

Linux для сетевых инженеров

Безопасная настройка и управление сетевыми
службами Linux в корпоративной среде

Роб Ванденбринк



Санкт-Петербург • Москва • Минск

2025

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 НЕПОЛАДOK

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 НЕПОЛАДОК

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/proxy.....	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