
bhv
Александр Чайка
Практическая безопасность Linux
Основы архитектуры Linux
Сравнение дистрибутивов
Защита загрузчика и безопасная загрузка
Системы инициализации
Уровни безопасности и модели управления доступом
Аутентификация и авторизация
Мониторинг системы, сервисов и пользовательской активности
Песочницы для приложений
Сетевая безопасность
Защита данных и памяти
Расследование инцидентов безопасности
СИСАДМИН
СИСТЕМНЫЙ АДМИНИСТРАТОР

Оглавление

Предисловие **15**
Благодарности 15
О чем эта книга 15
Как устроена эта книга 16
Кому она будет полезна 16
Об авторе 17

Введение **18**
Основы информационной безопасности 18
Роль Linux в инфраструктуре 19
История и философия Linux 19
Мифы о безопасности Linux 19
Миф 1: «На Linux нет вирусов» 19
Миф 2: «Если не root — значит, безопасно» 20
Миф 3: «Открытый код — значит, безопасный» 20
Миф 4: «Linux безопасен по умолчанию» 20
Современные угрозы и векторы атак 20
Уязвимости в ядре и базовых сервисах 20
Злоупотребление доверенными механизмами 20
LOTL (Living Off The Land) 21
Контейнеры и облачные среды 21
Supply Chain: атаки на цепочку поставки 21
Edge и IoT 21
Модели угроз и их применение в безопасности Linux 22
STRIDE 22
DREAD 22
MITRE ATT&CK 22
Практический подход к безопасности 23
Этика и ответственность 23
Мотивация и призыв к действию 23

Глава 1. Основы архитектуры Linux **25**
Уровни привилегий 26
Пространства выполнения 26

Инициализация....27
Механизмы перехода....27
Архитектурные особенности....27
Ядро и его компоненты....28
Аудит и безопасность....28
Аудит системы с помощью Linux Audit Framework, Lynis и auditd....29
Встроенные механизмы аудита....30

Глава 2. Защита загрузчика и безопасная загрузка....32
Этапы загрузки Linux....32
Описание этапов....33
Загрузчик GRUB. Настройка безопасности....34
Методы защиты GRUB....34
Пароль на доступ к меню загрузки....34
Защита параметров загрузки....35
Подпись ядра и модулей....35
Шифрование конфигурации....35
Загрузчик Syslinux. Методы обеспечения безопасности....35
Методы защиты Syslinux....36
Пароль на доступ к меню загрузки....36
Ограничение доступа к консоли....36
Защита конфигурационных файлов....36
Загрузчик rEFInd. Безопасная настройка....36
Загрузчик systemd-boot. Настройки, повышающие безопасность....37
Методы защиты systemd-boot....37
Подпись ядра....37
Пароль UEFI....38
Шифрование дисков....38
UEFI и Secure Boot. Принципы, настройка, обход....38
Методы защиты....39
Цифровая подпись кода....39
Загрузка только проверенного ПО....39
Защита от руткитов и буткит-атак....39
Блокировка изменения загрузчика и ядра....40
Совместимость с современными методами криптографической защиты....40
Уровни доступа....40
Векторы атаки....40
Популярные атаки на UEFI....41
Защиты от записи в хранилище основной прошивки....41
Настройка Secure Boot....42
Пример. Полнодисковое шифрование с LUKS2 Argon2id на Debian 12....42
Практика. Настройка Secure Boot на своем устройстве....43

Глава 3. Уровни безопасности и модели управления доступом....44
Дискретная модель доступа DAC (Discretionary Access Control)....44
Мандатная модель доступа MAC (Mandatory Access Control)....44
SELinux: политика важнее root....45
AppArmor: контроль по именам....46
Smack: безопасность для встраиваемых систем....47
Tomoyo: контроль поведения....47

Классические модели: Biba, MLS, BSD Extended ... 48
Сертифицированный уровень: Astra Linux SE ... 48
Выводы ... 49

Глава 4. Аутентификация и авторизация ... 50
Права доступа. Углубленное руководство по *chmod*, *chown*, *chgrp* ... 50
Настройка пользовательских окружений для повышения безопасности ... 51
Методы аутентификации: от паролей до MFA ... 52
Система контроля доступа (ACL): расширяя стандартные права ... 53
Настройка PAM для повышения безопасности ... 53
Системы управления секретами. HashiCorp Vault ... 55

Глава 5. Мониторинг системы, сервисов и пользовательской активности в Linux ... 57
Исторический и событийный мониторинг ... 57
Метамониторинг ... 57
Время отклика и SLA ... 57
Контроль нагрузки от мониторинга ... 58
Мониторинг системных ресурсов ... 58
Мониторинг сетевых сервисов ... 58
Отслеживание активности пользователей ... 58
Централизованный сбор логов ... 59
Автоматизация оповещений ... 59
Пример. Базовая настройка Zabbix ... 59
Интерпретация данных и поведенческий анализ ... 60
Риски ложных срабатываний ... 60
Рекомендации ... 60

Глава 6. Песочницы для приложений ... 62
Что такое песочница. Какие принципы лежат в ее основе ... 62
Зачем использовать песочницы. Преимущества и случаи применения ... 63
Flatpak и Snap как системы распространения приложений со встроенными механизмами песочницы ... 64
Популярные решения ... 64
Firejail: легкая изоляция через пространства имен ... 64
gVisor: контейнеры с собственной реализацией системных вызовов ... 65
Как работает gVisor ... 65
bubblewrap: контейнеризация для десктопа и не только ... 66
chroot: изоляция по старинке ... 66
systemd-nspawn: изоляция на уровне systemd ... 66
seccomp и seccomp-bpf: фильтрация системных вызовов ... 67
Примеры настройки песочницы для приложений ... 67
Изоляция браузера Firefox с помощью Firejail ... 68
Усиление безопасности системного сервиса через systemd ... 68
Побег из песочницы: примеры выхода и защиты от этого ... 68
Практический выбор ... 69

Глава 7. Выбор ядра и дистрибутива ... 70
Виды ядра ... 70
Generic Stable Kernel ... 71

Libre Kernel ... 71
Hardened Kernel ... 71
Выводы ... 72
Выбор дистрибутива ... 72
Безопасные дистрибутивы: от изоляции к анонимности ... 72
Whonix: анонимность и защита от слежки ... 72
Qubes OS: модульная безопасность с помощью виртуализации ... 73
Сертифицированные решения и российские дистрибутивы ... 74
Astra Linux Special Edition (SE) ... 75
Реализация MAC в Astra Linux SE ... 75
Поддержка аппаратных токенов и доверенной загрузки ... 76
Администрирование и сопровождение ... 76
РЕД ОС ... 76
ALT Linux и ROSA ... 77
Подбор дистрибутива для специализированных задач ... 77

Глава 8. Системы инициализации ... 78
systemd: комплексная модель управления и безопасности ... 78
Архитектура ... 79
Механизмы безопасности ... 79
Анализ жесткой настройки ... 80
Контейнеризация и переносимость ... 80
OpenRC: модульная простота и ручной контроль ... 81
Архитектура ... 81
Безопасность и ограничения ... 81
Преимущества ... 82
Недостатки ... 82
Runit: скорость, надежность, минимум кода ... 82
Архитектура ... 82
Безопасность ... 83
Преимущества ... 83
Недостатки ... 83
s6: надежность, изоляция, контроль ... 83
Архитектура ... 83
Механизмы безопасности ... 84
Преимущества ... 84
Недостатки ... 85
Сравнение систем инициализации ... 85
Что выбирать и когда ... 85
Практика. Жесткая настройка инициализации для безопасности ... 86
systemd: контроль через unit-файлы ... 86
OpenRC: контроль через скрипты ... 87
Runit: контроль через chpst ... 87
s6: минимализм с предсказуемостью ... 87
Общие рекомендации ... 87

Глава 9. Безопасность виртуализации ... 89
Основные угрозы и уязвимости в системах виртуализации ... 89
Обеспечение безопасности гипервизора ... 90
Изоляция и безопасность виртуальных машин ... 90

Безопасность сети в виртуальных системах ... 91
Мониторинг и аудит в виртуальных системах ... 91
Особенности безопасности контейнерной виртуализации ... 92
Безопасность хоста ... 93
Rootless Docker и Podman ... 93
Безопасная сборка и запуск контейнеров ... 93
Изоляция и контроль ... 94
Сеть и доступ ... 94
Аудит и секреты ... 94

Глава 10. Безопасность сети и коммуникаций ... 95
Настройка сетевого стека ... 95
Диагностика соединений ... 95
iptables и nftables ... 96
iptables ... 96
Основные действия, которые могут быть выполнены с помощью iptables ... 96
nftables ... 97
Сравнение iptables и nftables: производительность и безопасность ... 98
Основные отличия iptables и nftables ... 98
Архитектура ... 98
Синтаксис ... 98
Производительность ... 98
Применение правил ... 98
Примеры безопасности ... 99
Настройка NAT и проброс портов ... 99
Пример NAT через iptables (SNAT, MASQUERADE) ... 99
Проброс порта на внутренний сервер (DNAT) ... 100
NAT на nftables ... 100
Фингерпринтинг и сетевые отпечатки ... 100
Защита от фингерпринтинга ... 100
Zero Trust: недоверие ко всем по умолчанию ... 101

Глава 11. Обеспечение целостности системы ... 102
Настройка Integrity Policy Enforcement (IPE) ... 102
Основные понятия IPE ... 102
Проверка поддержки IPE в ядре ... 103
Настройка и компиляция IPE (при необходимости) ... 103
Настройка политики IPE ... 103
Пример базовой политики IPE ... 104
Создание политики на основе хеша файлов ... 104
Настройка политик на основе подписей ... 104
Пример политики с разными правилами ... 104
Настройка GRUB ... 105
Режимы работы IPE ... 105
Режим аудита (Audit Mode) ... 105
Режим принуждения (Enforce Mode) ... 106
Мониторинг и журналирование ... 106
Тестирование ... 106

Применение атрибута *immutable* для контроля целостности системы 106
Мониторинг изменений: инструменты Tripwire, OSSEC, AIDE 107
Tripwire: настройка и использование для безопасности Linux 107
Инициализация базы данных 108
Конфигурация политики 108
Обработка отчетов 108
Советы по использованию 108
OSSEC 109
Установка OSSEC 109
Конфигурация OSSEC 109
Проверка целостности файлов 110
Уведомления и оповещения 110
Практическое использование и примеры 110
AIDE 110
Установка AIDE 111
Автоматизация и уведомления 111
Примеры использования AIDE для безопасности 112
Системы обнаружения вторжений (IDS): различные IDS, их настройка и использование 112
Snort 112
Установка Snort 112
Конфигурация Snort 112
Запуск Snort 113
Мониторинг и управление 113
Примеры использования Snort 113
Suricata 114
Установка Suricata 114
Основная настройка 114
Правила и политики 115
Мониторинг и анализ 115
Примеры использования Suricata 115
Защита от атак с помощью доверенных приложений (LOTL-атаки) 115
Мониторинг и логирование 116
Примеры использования LOTL-атак 117
Настройка dm-verity для проверки контрольных сумм файлов и обеспечения целостности 117
Принцип работы dm-verity 117
Установка и настройка dm-verity 117
Создание образа файловой системы только для чтения 117
Создание хеш-дерева 118
Монтирование с проверкой целостности 118
Обеспечение безопасности и целостности 118

Глава 12. Антивирусы и обнаружение руткитов 119
Зачем нужны антивирусы в Linux. Риски и случаи использования 119
Инструменты для обнаружения скрытых процессов и модулей ядра в Linux 120
Шифровальщики 120
Майнеры 121
Руткиты и буткиты в Linux: что это такое и как они угрожают безопасности 121
Методы обнаружения руткитов: rkhunter, chkrootkit 122

Примеры антивирусов для Linux ... 122
Как защититься от вирусов, руткитов и буткитов ... 124

Глава 13. Защита данных ... 125
Инфраструктура публичных ключей (PKI) и безопасность в Linux ... 125
Доверие в PKI ... 125
Управление сертификатами в Linux ... 126
Выбор библиотеки SSL: OpenSSL и LibreSSL ... 126
GNU Privacy Guard (GPG). Работа с ключами ... 127
Типы ключей ... 127
Генерация ключей ... 127
Импорт и экспорт ключей ... 128
Шифрование файловой системы ... 129
dm-crypt ... 129
eCryptfs ... 130
LUKS ... 131
VeraCrypt ... 133
Опции разбиения на разделы и монтирования ... 134
Разбиение на разделы ... 134
Опции монтирования ... 135
Файл /etc/fstab ... 135
FUSE и его применение ... 136
Применение FUSE-шифрования в контексте безопасности ... 137
Рекомендации по использованию FUSE-шифрования ... 137
Безопасность хранения информации: LVM и RAID ... 137
Резервное копирование и восстановление данных. Лучшие практики и инструменты ... 139
Инструменты для резервного копирования ... 140
Восстановление данных ... 140
План восстановления после аварий (DRP) ... 141
Безопасное удаление данных: инструменты и методы ... 142

Глава 14. Защита памяти в Linux ... 144
Уязвимости памяти в Linux ... 144
Address Space Layout Randomization (ASLR) ... 145
Data Execution Prevention (DEP/NX) ... 146
Stack Canaries в Linux ... 146
Настройка компилятора ... 147
Control Flow Integrity (CFI) в Linux ... 147
Примеры реализации CFI ... 148
Сравнение SLUB с другими аллокаторами памяти в Linux с точки зрения безопасности ... 149
Выбор аллокатора ... 150
hardened_malloc ... 150
Настройка и использование ... 151
Kernel Heap Hardening ... 152
SELinux или AppArmor ... 153
Безопасность файла подкачки ... 153
Основные меры по обеспечению безопасности файла подкачки ... 153
Шифрование файла подкачки ... 153
Регулярная очистка файла подкачки ... 154
Мониторинг и ограничение использования файла подкачки ... 154

Что такое атака холодной загрузки ... 154
Шифрование памяти ... 155
Шифрование памяти и управление доступом в Intel SGX ... 155
Шифрование памяти и управление доступом в AMD SEV ... 155
Сравнение Intel SGX и AMD SEV ... 156
Защита от атак DMA ... 156
Отключение неиспользуемых портов ... 157
Использование безопасности сетевых устройств ... 157
Мониторинг и обновления системы ... 157
Языки программирования, безопасные для памяти ... 157
Rust ... 157
Python ... 158
Java ... 158
Выводы ... 158

Глава 15. Усиление безопасности ядра Linux и компилятора ... 159
Kernel Self Protection Project (KSPP) и его роль в усилении безопасности ядра Linux ... 160
Использование патчей Grsecurity/PaX и их возможности ... 162
Утилита sysctl и ее роль в безопасности ядра Linux ... 163
Зачем использовать sysctl для безопасности ... 164
Основные параметры безопасности ядра, управляемые через sysctl ... 164
Защита от подмены IP-адреса ... 164
Отключение перенаправления ICMP (пингов) ... 164
Отключение отправки ICMP-перенаправлений ... 164
Защита от атак SYN-флуд ... 164
Отключение ответа на широковещательные запросы ... 165
Отключение IP-перенаправления ... 165
Ограничение доступа к памяти ядра ... 165
Управление ASLR ... 165
Отключение дампов памяти для suid/sgid-файлов ... 165
Защита от форк-бомб ... 166
Как применять настройки sysctl ... 166
Временное изменение параметров ... 166
Постоянное сохранение настроек ... 166
Использование отдельного файла в директории /etc/sysctl.d/ ... 166
Практические рекомендации по настройке sysctl для безопасности ... 166
Уменьшение поверхности атаки на ядро Linux ... 167
Способы уменьшения поверхности атаки на ядро ... 167
Практические примеры уменьшения поверхности атаки ... 168
Отключение дампов ядра и его роль в обеспечении безопасности системы ... 169
Причины отключения дампов ядра ... 169
Как отключить дампы ядра в Linux ... 169
Важные моменты при отключении дампов ядра ... 170
Альтернативы отключению дампов ... 170
Дополнительные рекомендации ... 171
Внесение модулей ядра в черный список и обеспечение безопасности системы ... 171
Почему важно блокировать определенные модули ядра ... 171
Внесение модулей в черный список ... 172
Способы блокировки модулей ... 172
Особенности и предостережения ... 173

Дополнительные меры безопасности ... 173
Практические примеры блокировки модулей ... 173
Самостоятельная компиляция ядра для усиления безопасности ... 174
Почему стоит самостоятельно компилировать ядро ... 174
Подготовка к компиляции ядра ... 175
Шаги по компиляции ядра ... 175
Ключевые настройки для усиления безопасности ... 176
Отключение ненужных модулей и функций ... 176
Включение механизмов безопасности ... 176
Отключение неиспользуемых системных вызовов ... 177
Включение Control Flow Integrity (CFI) ... 177
Включение Security Audit ... 177
Компиляция и установка ядра ... 177
Проверка работы нового ядра ... 178
Дополнительные меры для обеспечения безопасности ... 178
Защита процессора при конфигурировании ядра Linux ... 178
Понимание уязвимостей процессора ... 179
Настройка ядра Linux для защиты процессора ... 179
Включение изоляции таблиц страниц ядра (Kernel Page Table Isolation, KPTI) ... 179
Включение защиты от Spectre ... 179
Включение функции Microcode Update ... 180
Ограничение спекулятивного выполнения ... 180
Включение Rogue Data Cache Load (RDCL) Mitigations ... 180
Использование Control-flow Enforcement Technology (CET) ... 180
Обновление компилятора и использование защитных опций ... 181
Удаление устаревших и неиспользуемых функций ... 181
Ограничение доступа к отладочным интерфейсам ... 181
Отслеживание состояния защиты ... 181
Основы безопасности компиляции ... 182
Использование опций безопасности компилятора ... 182
Удаление отладочной информации из релизной версии ... 183
Обзор ключевых опций безопасности компилятора GCC ... 184
Ключевые опции безопасности в GCC ... 184
Защита стека (Stack Protector) ... 184
Усиление стандартных функций (Fortify Source) ... 185
Позиционно-независимый код (Position Independent Executable, PIE) ... 185
Защита разделов памяти (Relocation Read-Only, RELRO) ... 185
Address Sanitizer (ASan) ... 186
Undefined Behavior Sanitizer (UBSan) ... 186
Контроль потока управления (Control Flow Integrity, CFI) ... 186
Предупреждения компилятора ... 186
Ограничение размера исполняемых файлов ... 187
Лучшие практики при использовании опций безопасности GCC ... 187
Пример полной команды компиляции с опциями безопасности ... 187
Основные опции безопасности в Clang и их использование ... 188
Основные опции безопасности в Clang ... 188
Stack Canaries (Защита стека) ... 188
Address Sanitizer (ASan) ... 189
Undefined Behavior Sanitizer (UBSan) ... 189

Memory Sanitizer (MSan) ... 189
Control Flow Integrity (CFI) ... 190
SafeStack ... 190
Fortify Source ... 190
Position Independent Executables (PIE) и Position Independent Code (PIC) ... 190
Relocation Read-Only (RELRO) ... 191
Stack Clash Protection ... 191
Рекомендации по использованию опций безопасности ... 191
Пример полного использования опций безопасности ... 192
Сравнение библиотек C с точки зрения безопасности: musl, glibc и др. ... 192
Сравнение библиотек C в контексте безопасности ... 192
Рекомендации по обеспечению безопасности при выборе библиотеки C ... 193

Глава 16. Безопасность приложений ... 194
ModSecurity ... 194
Fail2Ban ... 195
Безопасные практики разработки. Принципы обеспечения безопасности на этапе разработки ... 196

Глава 17. Работа с уязвимостями ... 198
Обновление системы ... 198
Общий стандарт уязвимостей (CWE). Классификация и понимание типов уязвимостей ... 199
Использование Security Advisories и CVE. Поиск и использование информации об уязвимостях ... 201
Инструменты для сканирования уязвимостей. Обзор и использование популярных инструментов ... 202
Сравнение инструментов сканирования уязвимостей ... 202
Как использовать инструменты для сканирования уязвимостей ... 203
Практика применения сканера OpenSCAP для поиска уязвимостей ... 204
Анализ результатов ... 204
Использование разных профилей ... 204
Автоматизация и интеграция ... 205

Глава 18. Расследование инцидентов безопасности ... 206
Типы инцидентов. Классификация инцидентов и особенности каждого типа ... 207
Подготовка к расследованию инцидентов безопасности. Создание плана действий, сбор команды, инструменты ... 208
Сбор команды ... 209
Необходимые инструменты ... 209
Сбор и сохранение данных. Методы сбора логов, снапшотов системы, сетевого трафика ... 210
Сбор логов ... 210
Создание снимков системы (снапшотов) ... 210
Сбор сетевого трафика ... 211
Журналы системных служб ... 211
Журналы аутентификации ... 212
Журналы приложений ... 212
Инструменты для анализа логов ... 212
Рекомендации по анализу логов ... 212

Анализ сетевой активности. tcpdump и Wireshark — ваши защитники от нежелательного трафика в Linux 213
tcpdump: быстрый и эффективный снифер командной строки 213
Wireshark: мощный графический анализатор пакетов 214
Обнаружение подозрительного трафика 214
Обнаружение вредоносных процессов в Linux. Утилиты lsof, netstat и другие методы 215
Идентификация подозрительных процессов 215
lsof: список открытых файлов 215
netstat: информация о сетевых соединениях 216
Другие полезные утилиты 216
Форензика файловых систем Linux. Восстановление удаленных файлов и анализ временных меток 216
Восстановление удаленных файлов 217
Процесс восстановления 217
Анализ временных меток 218
Использование инструментов форензики: Volatility, Autopsy, Sleuth Kit 218
Volatility 218
Получение дампа памяти 219
Autopsy 220
The Sleuth Kit 221
Основные утилиты TSK 221
Работа с образами дисков 222
Документирование и отчетность в расследовании инцидентов безопасности Linux: от анализа к действиям 222
Этапы документирования 222
Структура отчета 223
Рекомендации по дальнейшим действиям 224
Восстановление системы Linux после инцидента безопасности 224
Постинцидентный анализ: уроки из прошлого, безопасность будущего 226
Правовые аспекты кибербезопасности Linux: взаимодействие с правоохранительными органами и сохранение цепочки доказательств 227
Приказы, регулирующие взаимодействие с компетентными органами 227
Приказ № 524 ФСБ (для организаций, обрабатывающих ПД) 227
Приказ № 17 ФСТЭК 228
Приказ № 21 ФСТЭК 228
Приказ № 31 (2024) ФСТЭК + приказ № 235 228
Взаимодействие с органами при расследовании 228
Легализация данных для расследования 229

Глава 19. Практические рекомендации 231
Создание и поддержание безопасной среды Linux: ключевые аспекты 231
Лучшие практики безопасности Linux: свод рекомендаций 232

Заключение 233
Будущее безопасности Linux: перспективы и новые технологии 233
Ресурсы для дальнейшего изучения безопасности Linux: книги, курсы и сообщества 234

Предметный указатель 236