

Защита и укрепление Linux

Практическое руководство
по защите системы Linux
от кибератак

Дональд А. Тиволт



Содержание

От издательства.....	17
Об авторе.....	18
О рецензенте	19
Предисловие	20
 Часть I. ПОДГОТОВКА БЕЗОПАСНОЙ LINUX-СИСТЕМЫ.....	 23
 Глава 1. Запуск Linux в виртуальной среде	 24
Обзор угроз	25
Откуда берутся бреши?	26
Быть в курсе новостей по безопасности.....	26
Различия между физической, виртуальной и облачной системами.....	27
Знакомство с VirtualBox и Cygwin.....	28
Установка виртуальной машины в VirtualBox.....	29
Установка репозитория EPEL на виртуальную машину CentOS 7	33
Установка репозитория EPEL на виртуальные машины AlmaLinux 8/9	34
Конфигурирование сети для виртуальных машин в VirtualBox	35
Создание моментального снимка виртуальной машины в VirtualBox	36
Использование Cygwin для подключения к виртуальным машинам	37
Установка Cygwin на компьютер под управлением Windows.....	37
Использование клиента SSH в Windows 10 для взаимодействия с виртуальными машинами Linux.....	38
Использование клиента SSH в Windows 11 для взаимодействия с виртуальными машинами Linux.....	41
Сравнение Cygwin с оболочкой Windows	41
Поддержание систем Linux в актуальном состоянии.....	41
Обновление систем на основе Debian	42
Конфигурирование автоматического обновления в Ubuntu	43
Обновление систем на основе Red Hat 7	45

Обновление систем на основе Red Hat 8/9	49
Управление обновлениями на предприятии	50
Резюме	51
Вопросы	51
Для дополнительного чтения	52
Ответы	52
Присоединяйтесь к сообществу	52

Глава 2. Защита административных учетных записей..... 53

Риски входа в систему от имени root	53
Преимущества использования sudo	54
Задание привилегий sudo для пользователей с полными правами администратора	56
Добавление пользователей в предопределенную группу администраторов	56
Создание записи в файле политики sudo	58
Задание привилегий sudo для пользователей, которым делегирована только часть прав	59
Практикум: назначение ограниченных привилегий sudo	63
Дополнительные приемы работы с sudo	64
Таймер sudo	65
Просмотр своих привилегий sudo	65
Практикум: отключение таймера sudo	66
Предотвращение доступа к оболочке root со стороны пользователей	67
Предотвращение выхода пользователей в оболочку	67
Предотвращение запуска других опасных программ пользователями	70
Ограничение действий пользователя при вызове команд	71
Разрешение пользователям работать от имени других пользователей	72
Предотвращение злоупотреблений с помощью пользовательских скриптов оболочки	73
Обнаружение и удаление учетных записей по умолчанию	74
Новые возможности sudo	76
Особенности sudo в SUSE и OpenSUSE	76
Резюме	79
Вопросы	79
Для дополнительного чтения	80
Ответы	80

Глава 3. Защита обычных учетных записей 81

Защита домашних каталогов пользователей в Red Hat	81
Защита домашних каталогов пользователей в Debian Ubuntu	83
useradd в Debian/Ubuntu	83
adduser в Debian/Ubuntu	84
Практикум: создание зашифрованного домашнего каталога с помощью adduser	86

Задание критериев стойкости паролей	86
Установка и конфигурирование pwquality	87
Практикум: задание критериев сложности пароля	90
Задание срока действия пароля и учетной записи	91
Задание данных об истечении срока действия для useradd в системах типа Red Hat	92
Задание данных о сроке действия для каждой учетной записи в отдельности с помощью useradd и usermod	94
Задание данных о сроке действия для каждой учетной записи в отдельности с помощью chage	96
Практикум: задание данных о сроке действия для учетной записи и пароля	97
Предотвращение атак полным перебором	98
Конфигурирование PAM-модуля pam_tally2 в CentOS 7	99
Практикум: конфигурирование pam_tally2 в CentOS 7	100
Конфигурирование pam_faillock в AlmaLinux 8 и 9	101
Практикум: конфигурирование pam_faillock в AlmaLinux 8 и 9	102
Конфигурирование pam_faillock в Ubuntu 20.04 и Ubuntu 22.04	103
Практикум: конфигурирование pam_faillock в Ubuntu 20.04 и Ubuntu 22.04	104
Блокировка учетных записей	104
Блокировка учетной записи с помощью usermod	105
Блокировка учетной записи с помощью passwd	105
Блокировка учетной записи root	106
Настройка баннеров безопасности	107
Использование файла motd	107
Использование файла issue	108
Использование файла issue.net	109
Обнаружение скомпрометированных паролей	110
Практикум: обнаружение скомпрометированных паролей	113
Системы централизованного управления пользователями	114
Microsoft Active Directory	114
Samba в Linux	115
FreeIPA (управление идентификацией) в дистрибутивах типа RHEL	115
Резюме	116
Вопросы	117
Для дополнительного чтения	118
Ответы	118

Глава 4. Защита сервера с помощью брандмауэра, часть 1.....119

Технические требования	120
Обзор брандмауэров в Linux	120
Обзор iptables	121
Основы iptables	122
Блокирование ICMP с помощью iptables	126
Блокирование всего, что не разрешено, с помощью iptables	128

Практикум: основы работы с iptables.....	131
Блокирование недопустимых пакетов с помощью iptables	132
Восстановление удаленных правил	139
Практикум: блокирование недопустимых IPv4-пакетов	139
Защита IPv6.....	141
Практикум: работа с ip6tables	144
nftables – более универсальная система для построения брандмауэров	145
Таблицы и цепочки nftables	146
Конфигурирование nftables в Ubuntu	147
Использование команд nft	150
Практикум: работа с nftables в Ubuntu	155
Резюме	157
Вопросы	158
Для дополнительного чтения.....	159
Ответы	159

Глава 5. Защита сервера с помощью брандмауэра, часть 2..... 160

Технические требования.....	161
Uncomplicated Firewall для систем Ubuntu	161
Конфигурирование ufw.....	161
Работа с конфигурационными файлами ufw	163
Практикум: основы работы с ufw.....	167
firewalld для систем Red Hat	169
Проверка состояния firewalld.....	169
Работа с зонами firewalld	170
Добавление служб в зону по умолчанию	174
Добавление портов в зону firewalld	178
Блокирование ICMP.....	179
Использование режима паники	182
Протоколирование отброшенных пакетов.....	182
Использование развитых языковых правил firewalld	184
Правила iptables в firewalld для RHEL/CentOS 7	186
Создание прямых правил firewalld в RHEL/CentOS 7	188
Правила nftables для firewalld в RHEL/AlmaLinux 8 и 9	190
Создание прямых правил firewalld в RHEL/AlmaLinux	191
Практикум: команды firewalld.....	191
Резюме	195
Вопросы	195
Для дополнительного чтения.....	196
Ответы	196

Глава 6. Технологии шифрования

GNU Privacy Guard (GPG)	198
Практикум: создание собственных ключей GPG	199

Практикум: симметричное шифрование собственных файлов	201
Практикум: шифрование файлов открытыми ключами	204
Практикум: подписание без шифрования	208
Шифрование разделов с помощью Linux Unified Key Setup (LUKS)	209
Шифрование диска в процессе установки операционной системы	209
Практикум: добавление зашифрованного раздела с помощью LUKS	212
Конфигурирование автоматического монтирования раздела LUKS	216
Практикум: конфигурирование автоматического монтирования раздела LUKS	217
Шифрование каталогов с помощью eCryptfs	218
Практикум: шифрование домашнего каталога для учетной записи нового пользователя	218
Создание частного каталога внутри существующего домашнего каталога	219
Практикум: шифрование других каталогов с помощью eCryptfs	221
Шифрование раздела swap с помощью eCryptfs	223
Использование VeraCrypt для кросс-платформенного разделения зашифрованных контейнеров	224
Практикум: получение и установка VeraCrypt	224
Практикум: создание и монтирование тома VeraCrypt в консольном режиме	225
Работа с VeraCrypt в графическом режиме	228
OpenSSL и инфраструктура открытых ключей	229
Коммерческие удостоверяющие центры	230
Создание ключей, запросов на подписание сертификата и сертификатов	233
Создание самоподписанного сертификата с ключом RSA	233
Создание самоподписанного сертификата с эллиптическим ключом	235
Создание ключа RSA и запроса на подписание сертификата	235
Создание ЕС-ключа и CSR	237
Создание локального УЦ	238
Практикум: настройка УЦ Dogtag	239
Добавление УЦ в операционную систему	243
Практикум: экспорт и импорт сертификата УЦ Dogtag	243
Импорт УЦ в Windows	245
OpenSSL и веб-сервер Apache	245
Укрепление Apache SSL/TLS в Ubuntu	246
Укрепление Apache SSL/TLS в RHEL 9/AlmaLinux 9	247
Задание режима FIPS в RHEL 9/AlmaLinux 9	249
Укрепление Apache SSL/TLS в RHEL 7/CentOS 7	251
Настройка взаимной аутентификации	252
Введение в квантово-стойкие алгоритмы шифрования	252
Резюме	253
Вопросы	254
Для дополнительного чтения	255
Ответы	256

Глава 7. Укрепление SSH	257
Запрет протокола SSH 1.....	258
Создание и управление ключами для входа без пароля	258
Создание пользовательского набора ключей SSH	259
Перенос открытого ключа на удаленный сервер	262
Практикум: создание и перенос ключей SSH.....	264
Запрет входа от имени root	266
Запрет входа по имени пользователя и паролю	267
Практикум: запрет входа по имени пользователя и паролю	267
Включение двухфакторной аутентификации	268
Практикум: настройка двухфакторной аутентификации в Ubuntu 22.04	269
Практикум: использование Google Authenticator в сочетании с обменом ключами в Ubuntu	271
Практикум: настройка двухфакторной аутентификации в AlmaLinux 8.....	272
Практикум: использование Google Authenticator в сочетании с обменом ключами в AlmaLinux 8	274
Конфигурирование Secure Shell со стойкими алгоритмами шифрования	274
Что такое алгоритмы шифрования в SSH	275
Сканирование с целью узнать, какие алгоритмы SSH разрешены	278
Практикум: сканирование с помощью Nmap	278
Запрещение слабых алгоритмов шифрования SSH.....	280
Практикум: запрещение слабых алгоритмов шифрования SSH в Ubuntu 22.04	280
Практикум: запрет алгоритмов шифрования SSH в CentOS 7.....	281
Задание системных политик шифрования в RHEL 8/9 и AlmaLinux 8/9.....	283
Практикум: задание политик шифрования в AlmaLinux 9	284
Конфигурирование более подробного протоколирования	285
Практикум: конфигурирование более подробного протоколирования SSH.....	286
Конфигурирование управления доступом с помощью белых списков и TCP Wrappers.....	287
Конфигурирование белых списков в sshd_config	288
Практикум: конфигурирование белых списков в sshd_config	288
Конфигурирование белых списков с помощью TCP Wrappers.....	290
Конфигурирование автоматического выхода из системы и баннеров безопасности	291
Настройка автоматического выхода для локальных и удаленных пользователей	291
Настройка автоматического выхода в sshd_config	292
Создание предупредительного баннера безопасности	292
Конфигурирование прочих параметров безопасности.....	293
Запрет проброса X11	293
Запрет SSH-туннелей	294

Изменения порта SSH по умолчанию	295
Управление ключами SSH.....	296
Задание разных конфигураций для различных пользователей и групп.....	299
Задание разных конфигураций для различных узлов	300
Задание окружения chroot для пользователей SFTP	301
Создание группы и конфигурирование файла sshd_config	301
Практикум: задание каталога chroot для группы sftputers.....	303
Разделение каталога с помощью SSHFS	304
Практикум: разделение каталога с помощью SSHFS	305
Удаленное подключение с рабочего стола Windows.....	306
Резюме	311
Вопросы	312
Для дополнительного чтения.....	313
Ответы	314

Часть II. УПРАВЛЕНИЕ ДОСТУПОМ К ФАЙЛАМ И КАТАЛОГАМ

315

Глава 8. Избирательное управление доступом

316

Использование <code>chown</code> для изменения владельца файлов или каталогов	316
Использование <code>chmod</code> для задания прав доступа к файлам или каталогам.....	318
Символический способ задания прав доступа	319
Числовой способ задания прав доступа.....	320
Использование SUID и SGID для регулярных файлов	322
Последствия установки битов SUID и SGID с точки зрения безопасности	323
Нахождение посторонних SUID- и SGID-файлов.....	323
Практикум: поиск SUID- и SGID-файлов	325
Предотвращение использования SUID и SGID в разделе	326
Использование расширенных атрибутов для защиты важных файлов	326
Задание атрибута <code>a</code>	327
Задание атрибута <code>i</code>	328
Защита системных конфигурационных файлов.....	330
Резюме	333
Вопросы	333
Для дополнительного чтения.....	336
Ответы	336

Глава 9. Списки управления доступом и управление разделяемым каталогом

337

Создание ACL для пользователя или группы.....	337
Создание наследуемого ACL для каталога	340
Удаление конкретного права доступа с помощью маски ACL	342

Использование команды <code>tar --acls</code> для предотвращения потери ACL при создании резервной копии	343
Создание группы пользователей и добавление в нее членов	345
Добавление членов при создании их учетных записей	346
Использование <code>usermod</code> для добавления существующего пользователя в группу	346
Добавление пользователя в группу путем редактирования файла <code>/etc/group</code>	347
Создание разделяемого каталога	348
Установка бита SGID и бита закрепления для разделяемого каталога	349
Использование ACL для доступа к файлам в разделяемом каталоге	351
Задание прав доступа и создание ACL	352
Практикум: создание разделяемого каталога для группы	353
Резюме	355
Вопросы	355
Для дополнительного чтения	357
Ответы	357

Часть III. Дополнительные методы укрепления системы..... 358

Глава 10. Реализация мандатного управления доступом с помощью SELinux и AppArmor..... 359

Чем SELinux может быть полезна системному администратору	360
Настройка контекстов безопасности для файлов и каталогов	361
Установка инструментов SELinux	363
Создание файлов контента при включенной SELinux	364
Исправление неверного контекста SELinux	367
Использование <code>chcon</code>	367
Использование <code>restorecon</code>	368
Использование <code>semanage</code>	369
Практикум: установка типа SELinux	371
Использование <code>setroubleshoot</code> для отладки проблем в SELinux	372
Просмотр сообщений <code>setroubleshoot</code>	372
Использование графической утилиты <code>setroubleshoot</code>	373
Отладка в разрешительном режиме	375
Работа с политиками SELinux	378
Просмотр булевых признаков	378
Конфигурирование булевых признаков	380
Защита веб-сервера	381
Защита сетевых портов	382
Создание специальных модулей политики	385
Практикум: булевы признаки SELinux и порты	387
Чем AppArmor может быть полезна системному администратору	388
Знакомство с профилями AppArmor	389
Работа с командными утилитами AppArmor	392

Отладка проблем в AppArmor	395
Отладка профиля AppArmor – Ubuntu 16.04	395
Отладка профиля AppArmor – Ubuntu 18.04	398
Практикум: отладка профиля AppArmor	399
Отладка проблем Samba в Ubuntu 22.04	400
Эксплуатация системы с помощью вредоносного контейнера Docker	401
Практикум: создание вредоносного контейнера Docker	402
Резюме	404
Вопросы	405
Для дополнительного чтения	406
Ответы	407
 Глава 11. Укрепление ядра и изоляция процессов	408
Файловая система /proc	409
Просмотр процессов, работающих в режиме пользователя	409
Просмотр информации о ядре	411
Задание параметров ядра с помощью sysctl	413
Конфигурирование файла sysctl.conf	414
Конфигурирование sysctl.conf – Ubuntu	415
Конфигурирование sysctl.conf – CentOS и AlmaLinux	419
Задание дополнительных параметров для укрепления ядра	420
Практикум: сканирование параметров ядра с помощью Lynis	420
Запрет пользователям просматривать чужие процессы	423
Что такое изоляция процессов	424
Что такое контрольные группы	425
Что такое изоляция пространств имен	428
Что такое возможности ядра	430
Практикум: задание возможности ядра	433
SECCOMP и системные вызовы	434
Использование изоляции процессов при работе с контейнерами	
Docker	435
Организация песочницы с помощью Firejail	436
Практикум: работа с Firejail	439
Организация песочницы с помощью Snappy	440
Организация песочницы с помощью Flatpak	444
Резюме	447
Вопросы	447
Для дополнительного чтения	449
Ответы	450
 Глава 12. Сканирование, аудит и укрепление	451
Установка и обновление ClamAV и maldet	452
Практикум: установка ClamAV и maldet	453
Практикум: конфигурирование maldet	455

Обновление ClamAV и maldet	456
Сканирование с помощью ClamAV и maldet	459
Проблемы SELinux	460
Поиск руткитов с помощью Rootkit Hunter	460
Практикум: установка и обновление Rootkit Hunter	461
Поиск руткитов	462
Быстрый анализ на предмет вредоносности с помощью strings и VirusTotal	463
Анализ файла с помощью strings	464
Сканирование вредоносного файла с помощью VirusTotal	465
О демоне auditd	466
Создание правил аудита	467
Аудит изменений файла	467
Аудит каталога	469
Аудит системных вызовов	470
Использование ausearch и aureport	471
Поиск уведомлений об изменении файла	471
Поиск нарушений правил доступа к каталогам	474
Поиск нарушений правил системных вызовов	478
Генерирование отчетов об аутентификации	480
Использование предопределенных наборов правил	482
Практикум: использование auditd	483
Практикум: использование предопределенных правил для auditd	485
Аудит файлов и каталогов с помощью inotifywait	485
Применение политик OpenSCAP с помощью oscar	487
Установка OpenSCAP	487
Просмотр файлов профилей	488
Получение недостающих профилей для Ubuntu	489
Сканирование системы	489
Лечение системы	491
Использование SCAP Workbench	493
Выбор профиля OpenSCAP	496
Применение профиля OpenSCAP на этапе установки системы	497
Резюме	499
Вопросы	499
Для дополнительного чтения	501
Ответы	501
Глава 13. Протоколирование и защита журналов	502
Знакомство с системными журналами Linux	503
Системный журнал и журнал аутентификации	503
Файлы utmp, wtmp, btmp и lastlog	506
Знакомство с rsyslog	509
Правила протоколирования в rsyslog	509
Знакомство с journald	511
Упрощение работы с помощью Logwatch	514

Практикум: установка Logwatch.....	514
Настройка сервера удаленного протоколирования.....	516
Практикум: настройка простого сервера протоколирования	516
Создание зашифрованного подключения к серверу протоколирования.....	518
Создание подключения через stunnel в AlmaLinux 9 – сторона сервера	518
Создание подключения через stunnel в AlmaLinux 9 – сторона клиента.....	519
Создание подключения через stunnel в Ubuntu – сторона сервера.....	520
Создание подключения через stunnel в Ubuntu – сторона клиента	522
Разнесение сообщений клиентов по отдельным файлам	523
Обслуживание журналов на крупных предприятиях.....	524
Резюме	525
Вопросы	525
Для дополнительного чтения.....	527
Ответы	527

Глава 14. Поиск уязвимостей и обнаружение вторжений..... 528

Введение в Snort и Security Onion.....	529
Получение и установка Snort	529
Практикум: установка Snort с помощью контейнера Docker	530
Использование Security Onion	532
IPFire и встроенная в нее система предотвращения вторжений.....	534
Практикум: создание виртуальной машины IPFire	535
Сканирование и укрепление с помощью Lynis	539
Установка Lynis в Red Hat/CentOS.....	540
Установка Lynis в Ubuntu	540
Сканирование с помощью Lynis	540
Поиск уязвимостей с помощью Greenbone Security Assistant	544
Сканирование веб-сервера с помощью Nikto.....	552
Nikto в Kali Linux.....	552
Практикум: установка Nikto с Github	553
Сканирование веб-сервера с помощью Nikto	554
Резюме	556
Вопросы	556
Для дополнительного чтения.....	557
Ответы	557

Глава 15. Предотвращение запуска нежелательных программ..... 558

Монтирование разделов с параметрами по	559
Демон fapolicyd.....	565
Правила fapolicyd	568
Установка fapolicyd	570
Резюме	571

Для дополнительного чтения.....	571
Вопросы	571
Ответы	572

Глава 16. Полезные советы по безопасности

для неустойчивых тружеников	573
Технические требования.....	573
Аудит системных служб.....	574
Аудит системных служб с помощью systemctl	574
Аудит сетевых служб с помощью netstat.....	575
Практикум: просмотр сетевых служб с помощью netstat	580
Аудит сетевых служб с помощью Nmap.....	581
Состояния портов	582
Типы сканирования	582
Практикум: сканирование с помощью Nmap	587
Парольная защита начального загрузчика GRUB2	588
Практикум: сброс пароля	
для Red Hat/CentOS/AlmaLinux	589
Практикум: сброс пароля для Ubuntu.....	591
Предотвращение редактирования параметров ядра	
в Red Hat/CentOS/AlmaLinux	594
Предотвращение редактирования параметров ядра в Ubuntu.....	595
Отключение подменю для Ubuntu	598
Безопасное конфигурирование BIOS/UEFI	600
Контрольный список мер защиты конфигурации системы	602
Резюме	605
Вопросы	605
Для дополнительного чтения.....	607
Ответы	607
 Предметный указатель.....	 608