

Научная библиотека

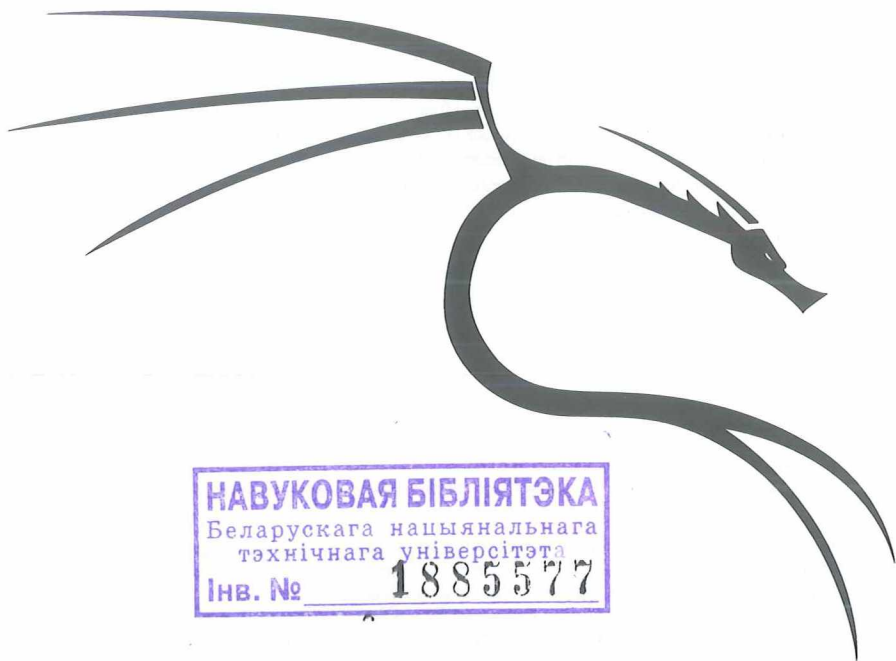
БНТУ



* 8 0 1 2 4 7 2 2 7 *

Рафаэль Херцог, Джим О'Горман, Мати Ахарони

КАЛІ LINUX ОТ РАЗРАБОТЧИКОВ



НАВУКОВАЯ БІБЛІЯТЭКА
Беларускага нацыянальнага
тэхнічнага ўніверсітэта
Інв. № **1885577**

 **ПИТЕР®**

Санкт-Петербург • Москва • Минск

2022

Краткое содержание

Предисловие.....	14
Вступление.....	21
Введение.....	23
Глава 1. О Kali Linux.....	27
Глава 2. Начало работы с Kali Linux.....	39
Глава 3. Основы Linux.....	65
Глава 4. Установка Kali Linux.....	83
Глава 5. Настройка Kali Linux.....	117
Глава 6. Самостоятельное решение проблем и получение помощи.....	135
Глава 7. Защита и контроль Kali Linux.....	161
Глава 8. Управление пакетами Debian.....	181
Глава 9. Расширенное использование системы.....	233
Глава 10. Kali Linux в организации.....	263
Глава 11. Оценка защищенности информационных систем.....	289
Глава 12. Резюме: дальнейший путь.....	313
Об авторах.....	316

Оглавление

Предисловие.....	14
Вступление.....	21
Введение.....	23
Почему именно эта книга?.....	23
Для вас ли эта книга?.....	24
Общий подход и структура издания.....	24
Благодарности от Рафаэля Херцога.....	25
Благодарности от Джима О'Гормана.....	25
Благодарности от Мати Ахарони.....	26
Глава 1. О Kali Linux.....	27
1.1. Немного истории.....	28
1.2. Взаимоотношения с Debian.....	30
Движение пакетов.....	30
Управление различиями с Debian.....	31
1.3. Предназначение и варианты использования.....	31
1.4. Основные характеристики Kali Linux.....	34
Live-система.....	34
Режим криминалистической экспертизы.....	35
Пользовательское ядро Linux.....	35
Полная настраиваемость.....	35

Надежная операционная система.....	36
Используется на широком диапазоне ARM-устройств	36
1.5. Политики Kali Linux	36
Один суперпользователь по умолчанию.....	36
Сетевые сервисы отключены по умолчанию.....	37
Коллекция приложений с сопровождением	37
1.6. Резюме.....	38
Глава 2. Начало работы с Kali Linux.....	39
2.1. Скачивание ISO-образа Kali	40
Где скачать.....	40
Что скачать.....	41
Проверка целостности и подлинности.....	43
Копирование образа на DVD- или USB-накопитель.....	45
2.2. Загрузка ISO-образа Kali в режиме Live	50
На реальном компьютере.....	50
В виртуальной машине.....	50
2.3. Резюме.....	64
Глава 3. Основы Linux	65
3.1. Что такое Linux и для чего она нужна	66
Управление оборудованием	66
Объединение файловых систем.....	67
Управление процессами.....	68
Управление правами.....	69
3.2. Командная строка	69
Как получить доступ к командной строке.....	69
Основы командной строки: просмотр дерева каталогов и управление файлами	71
3.3. Файловая система	73
Стандарт иерархии файловой системы.....	73
Личный каталог пользователя	73

3.4. Полезные команды.....	74
Отображение и изменение текстовых файлов.....	74
Поиск файлов и по содержимому файлов.....	75
Управление процессами.....	75
Управление правами.....	76
Получение системной информации и файлов регистрации.....	78
Обнаружение оборудования.....	80
3.5. Резюме.....	81
Глава 4. Установка Kali Linux.....	83
4.1. Минимальные требования к установке.....	84
4.2. Пошаговая установка на жесткий диск.....	84
Обычная установка.....	84
Установка на полностью зашифрованную файловую систему.....	103
4.3. Автоматическая установка.....	108
Автоматические ответы.....	108
Создание файла пресидинга.....	110
4.4. Установка на ARM-устройства.....	110
4.5. Устранение неполадок установки.....	112
4.6. Резюме.....	115
Глава 5. Настройка Kali Linux.....	117
5.1. Настройка сети.....	118
На рабочем столе с помощью инструмента NetworkManager.....	118
В командной строке с помощью пакета Ifupdown.....	119
В командной строке с помощью инструмента systemd-networkd.....	120
5.2. Управление пользователями и группами Unix.....	121
Создание учетных записей пользователей.....	121
Изменение существующей учетной записи или пароля.....	122
Отключение учетной записи.....	123
Управление Unix-группами.....	123

5.3. Настройка сервисов	124
Настройка конкретной программы	124
Настройка SSH для удаленного входа в систему.....	124
Настройка баз данных PostgreSQL.....	125
Настройка сервера Apache	128
5.4. Управление сервисами	131
5.5. Резюме.....	133
Глава 6. Самостоятельное решение проблем и получение помощи.....	135
6.1. Источники документации	136
Руководства	137
Документы формата info	138
Документация для пакетов	138
Сайты	139
Документация на сайте docs.kali.org.....	140
6.2. Сообщества Kali Linux.....	140
Веб-форумы на сайте forums.kali.org	140
Канал IRC #kali-linux в сети Freenode.....	141
6.3. Подача грамотно составленного отчета об ошибке	142
Общие рекомендации	142
Где регистрировать отчет об ошибке	145
Как подать отчет об ошибке	146
6.4. Резюме.....	158
Глава 7. Защита и контроль Kali Linux	161
7.1. Определение политики безопасности	162
7.2. Возможные меры безопасности	164
На сервере.....	164
На ноутбуке	164
7.3. Защита сетевых сервисов	165

7.4. Брандмауэр или фильтрация пакетов	166
Поведение сетевого фильтра Netfilter	166
Синтаксис команд iptables и ip6tables	169
Создание правил.....	172
Установка правил при каждой загрузке.....	173
7.5. Мониторинг и протоколирование	174
Мониторинг журналов с помощью программы logcheck	174
Мониторинг активности в режиме реального времени	175
Обнаружение изменений.....	176
7.6. Резюме.....	178
Глава 8. Управление пакетами Debian	181
8.1. Введение в APT	182
Взаимосвязь между APT и dpkg	182
Подробности о файле sources.list	184
Репозитории Kali	186
8.2. Основное взаимодействие пакетов в Debian.....	188
Инициализация APT	188
Установка пакетов	188
Обновление Kali Linux	191
Удаление и очистка пакетов	193
Проверка пакетов	194
Устранение проблем	199
Пользовательские интерфейсы: aptitude и synaptic	203
8.3. Дополнительная настройка и использование APT.....	207
Настройка APT	208
Управление приоритетами пакетов	209
Работа с несколькими дистрибутивами	212
Отслеживание автоматически установленных пакетов.....	213
Использование поддержки Multi-Arch	214
Проверка подлинности пакета	216

8.4. Справка по пакетам: погружение в систему пакетов Debian	218
Файл control	220
Сценарии конфигурации	225
Контрольные суммы, конфигурационные файлы	229
8.5. Резюме.....	230
Глава 9. Расширенное использование системы.....	233
9.1. Модификация пакетов Kali	234
Загрузка исходного кода	235
Установка зависимостей для сборки.....	238
Внесение изменений	239
Запуск сборки	243
9.2. Перекомпиляция ядра Linux	245
Подготовка и предварительные требования.....	245
Загрузка исходного кода	246
Настройка ядра.....	247
Компиляция и сборка пакета.....	248
9.3. Сборка собственных ISO-образов Kali	249
Предварительные требования к установке.....	250
Сборка live-образа с различными окружениями рабочего стола	250
Изменение набора установленных пакетов	251
Использование хуков для настройки содержимого образа.....	252
Добавление файлов в ISO-образ или в файловую live-систему.....	252
9.4. Добавление постоянного хранилища в live-образ Kali в формате ISO с помощью USB-накопителя	253
Особенности постоянного хранилища	253
Создание незашифрованного хранилища на USB-накопителе	254
Создание зашифрованного хранилища на USB-накопителе	256
Использование нескольких постоянных хранилищ	257

9.5. Резюме.....	259
Итоговые сведения по модификации пакетов	259
Итоговые сведения по сборке ядра Linux	260
Итоговые сведения по сборке собственных ISO-образов Kali.....	261
Глава 10. Kali Linux в организации	263
10.1. Установка Kali Linux через сеть (PXE Boot).....	264
10.2. Использование управления конфигурацией.....	267
Настройка SaltStack.....	267
Выполнение команд на миньонах.....	268
State-файлы salt и другие особенности	270
10.3. Расширение и настройка Kali Linux	274
Разветвление пакетов Kali.....	274
Создание пакетов конфигурации	275
Создание хранилища пакетов для APT	281
10.4. Резюме.....	285
Глава 11. Оценка защищенности информационных систем.....	289
11.1. Kali Linux в оценке защищенности	292
11.2. Типы оценок	293
Оценка уязвимости систем.....	294
Оценка систем на соответствие стандартам безопасности	299
Традиционное тестирование на проникновение	300
Оценка приложений.....	303
11.3. Формализация оценки	305
11.4. Типы атак.....	307
Атака типа «отказ в обслуживании» (DoS-атака)	307
Нарушение целостности информации в памяти.....	308
Атаки на веб-приложения	308
Взлом паролей.....	309
Атаки на клиентские системы.....	310
11.5. Резюме.....	310

Глава 12. Резюме: дальнейший путь	313
12.1. Отслеживание изменений.....	314
12.2. Демонстрация новоприобретенных знаний.....	314
12.3. Дальнейший путь	314
Системное администрирование	315
Тестирование на проникновение.....	315
Об авторах	316