

ВТОРОЕ ИЗДАНИЕ

Изучаем Kali Linux

*Проверка защиты, тестирование
на проникновение, этичный хакинг*

Рик Мессье

SPRINT
book

2025

Краткое содержание

Предисловие	16
Глава 1. Основы Kali Linux.....	23
Глава 2. Основы тестирования сетевой безопасности	67
Глава 3. Разведка.....	112
Глава 4. Поиск уязвимостей.....	160
Глава 5. Автоматизированные эксплойты.....	203
Глава 6. Освоение Metasploit	231
Глава 7. Тестирование беспроводных сетей.....	264
Глава 8. Тестирование веб-приложений.....	303
Глава 9. Взлом паролей.....	348
Глава 10. Продвинутое техники и концепции	378
Глава 11. Реверс-инжиниринг и анализ программ.....	407
Глава 12. Цифровая криминалистика	445
Глава 13. Создание отчетов	484
Об авторе	509
Иллюстрация на обложке.....	510

Оглавление

Предисловие	16
О чем пойдет речь в этой книге.....	16
Новое в этом издании	19
На кого рассчитана книга	20
Ценность и важность этики	20
Условные обозначения, используемые в книге	21
Благодарности	22
От издательства.....	22
О научном редакторе русского издания	22
Глава 1. Основы Kali Linux	23
Наследие Linux	23
Появление Linux	25
Загрузка и установка Kali Linux	28
Виртуальные машины.....	30
Дешевые вычисления.....	31
Подсистема Windows для Linux.....	32
Среды рабочего стола.....	34
Xfce	35
GNOME.....	36
Вход в систему через менеджер рабочего стола.....	38
Cinnamon и MATE.....	39
Использование командной строки.....	42
Управление файлами и каталогами	43
Управление процессами	48
Прочие утилиты	52
Управление пользователями	53
Управление службами.....	54
Управление пакетами.....	56

Удаленный доступ	59
Управление журналом	62
Резюме	65
Полезные ресурсы	66
Глава 2. Основы тестирования сетевой безопасности	67
Тестирование безопасности	68
Тестирование сетевой безопасности	70
Мониторинг	70
Слои	73
Стресс-тестирование	76
Средства для реализации атак типа «отказ в обслуживании»	84
Тестирование шифрования	91
Захват пакетов	97
Использование программы tcpdump	98
Пакетные фильтры Беркли	101
Программа Wireshark	102
Атаки типа «отравление»	106
ARP-спуфинг	107
DNS-спуфинг	109
Резюме	110
Полезные ресурсы	111
Глава 3. Разведка	112
Что такое разведка	112
Разведка по открытым источникам	114
Google-хакинг	116
Автоматизация сбора информации	119
Фреймворк Recon-ng	125
Программа Maltego	128
DNS-разведка и программа whois	132
DNS-разведка	132
Региональные интернет-регистраторы	138
Пассивная разведка	141

Сканирование портов	144
TCP-сканирование.....	145
UDP-сканирование	145
Сканирование портов с помощью программы nmap	146
Высокоскоростное сканирование.....	151
Сканирование служб	154
Ручное тестирование.....	156
Резюме.....	159
Полезные ресурсы.....	159
Глава 4. Поиск уязвимостей	160
Что такое уязвимости	160
Типы уязвимостей	162
Переполнение буфера	162
Состояние гонки	164
Проверка входных данных.....	165
Контроль доступа	166
Сканирование на уязвимости.....	167
Локальные уязвимости.....	171
Поиск локальных уязвимостей с помощью сканера Lynis	172
Поиск локальных уязвимостей с помощью программы OpenVAS	175
Руткиты.....	178
Удаленные уязвимости	180
Быстрый старт с OpenVAS.....	182
Создание задачи сканирования	184
Отчеты OpenVAS.....	187
Уязвимости сетевых устройств	192
Аудит устройств.....	192
Уязвимости баз данных.....	196
Выявление новых уязвимостей	197
Резюме.....	202
Полезные ресурсы.....	202

Глава 5. Автоматизированные эксплойты	203
Что такое эксплойт.....	203
Атаки на оборудование Cisco.....	204
Протоколы управления	206
Другие устройства	208
База данных эксплойтов.....	209
Фреймворк Metasploit.....	212
Начало работы с Metasploit	213
Работа с модулями Metasploit.....	214
Импорт данных	216
Эксплуатация систем.....	221
Приложение Armitage	225
Социальная инженерия.....	227
Резюме	229
Полезные ресурсы.....	230
Глава 6. Освоение Metasploit	231
Сканирование в поисках целей.....	231
Сканирование портов	231
SMB-сканирование	235
Сканирование на уязвимости.....	237
Эксплуатация уязвимости целевой системы	239
Использование оболочки Meterpreter	241
Основы работы с Meterpreter.....	242
Информация о пользователе.....	243
Манипулирование процессами	247
Повышение привилегий	249
Проброс трафика в другие сети	253
Поддержание доступа.....	256
Заметание следов.....	261
Резюме.....	262
Полезные ресурсы.....	263

Глава 7. Тестирование беспроводных сетей	264
Сфера беспроводных технологий	264
Стандарт 802.11	265
Протокол Bluetooth	266
Протокол Zigbee	267
Атаки на сети Wi-Fi и инструменты для тестирования.....	267
Терминология и принцип работы стандарта 802.11	268
Идентификация сетей.....	269
Атаки на WPS.....	272
Автоматическое выполнение нескольких тестов.....	275
Инъекционные атаки	278
Взлом паролей от сети Wi-Fi	278
Инструмент besside-ng	279
Программа coWPAtty	281
Инструмент aircrack-ng	282
Приложение Fern	284
Использование фальшивых точек доступа	286
Хостинг для точки доступа	287
Фишинговые атаки на пользователей	289
Беспроводная ловушка.....	293
Тестирование Bluetooth.....	293
Сканирование	294
Идентификация служб	296
Другие способы тестирования Bluetooth.....	299
Тестирование устройств для умного дома	301
Резюме.....	301
Полезные ресурсы.....	302
Глава 8. Тестирование веб-приложений	303
Архитектура веб-приложения.....	303
Брандмауэр	305
Балансировщик нагрузки	305
Веб-сервер.....	306

Сервер приложений.....	306
Сервер базы данных.....	307
Нативная облачная архитектура.....	308
Веб-атаки.....	309
Внедрение SQL-кода.....	309
Внедрение XML-сущностей.....	310
Внедрение команд.....	312
Межсайтовый скриптинг.....	313
Подделка межсайтовых запросов.....	315
Перехват сеанса.....	316
Использование прокси-серверов.....	318
Программа Burp Suite.....	318
Инструмент Zed Attack Proxy.....	322
Инструмент WebScarab.....	326
Инструмент Paros.....	328
Автоматизированные веб-атаки.....	328
Разведка с помощью программы skipfish.....	329
Сканер nikto.....	332
Инструмент wapiti.....	333
Программы dirbuster и gobuster.....	334
Серверы приложений на базе Java.....	336
Атаки, основанные на внедрении SQL-кода.....	337
Тестирование систем управления контентом.....	342
Инструменты для решения специфических задач.....	344
Резюме.....	346
Полезные ресурсы.....	347
Глава 9. Взлом паролей.....	348
Хранение паролей.....	348
Диспетчер учетных записей безопасности.....	350
Подключаемые модули аутентификации и криптография.....	351
Получение паролей.....	353
Взлом паролей в автономном режиме.....	356

Инструмент John the Ripper.....	358
Радужные таблицы	361
Программа HashCat.....	367
Взлом паролей в режиме онлайн	369
Инструмент Hydra.....	370
Программа Patator	371
Взлом веб-приложений	373
Резюме.....	376
Полезные ресурсы.....	377
Глава 10. Продвинутое техники и концепции	378
Основы программирования.....	379
Компилируемые языки	379
Интерпретируемые языки.....	384
Промежуточные языки	385
Компиляция и сборка	387
Ошибки программирования	389
Переполнение буфера	389
Переполнение кучи.....	392
Возвращение к библиотеке libc	393
Написание модулей Nmap	395
Расширение функциональности Metasploit.....	398
Поддержание доступа и заметание следов	402
Заметание следов с помощью Metasploit.....	402
Закрепление в системе	403
Резюме.....	405
Полезные ресурсы.....	406
Глава 11. Реверс-инжиниринг и анализ программ	407
Управление памятью	408
Структуры программ и процессов	411
Переносимый исполняемый файл	412
Формат исполняемых и компоуемых файлов	417

Отладка	421
Дизассемблирование	425
Декомпиляция Java-кода	428
Реверс-инжиниринг	430
Фреймворк Radare2.....	431
Программа Cutter	438
Программа Ghidra	441
Резюме	444
Полезные ресурсы.....	444
Глава 12. Цифровая криминалистика	445
Диски, файловые системы и образы.....	446
Файловые системы	450
Создание образа диска	452
Инструментарий The Sleuth Kit.....	455
Использование программы Autopsy	460
Анализ файлов.....	464
Получение файла из образа диска	465
Восстановление удаленных файлов	467
Поиск данных	470
Скрытые данные	474
Анализ PDF-файлов	475
Стеганография	477
Криминалистический анализ памяти.....	479
Резюме	482
Полезные ресурсы.....	483
Глава 13. Создание отчетов.....	484
Определение потенциала и уровня серьезности угрозы	485
Написание отчетов	487
Аудитория	487
Резюме для руководства	488
Методология.....	490
Результаты.....	491

Управление результатами	492
Текстовые редакторы	493
Редакторы с графическим интерфейсом.....	495
Программа Notes	497
Программа Cherry Tree	498
Сбор данных.....	500
Организация данных	502
Фреймворк Dradis	502
Инструмент CaseFile	505
Резюме.....	507
Полезные ресурсы.....	508
Об авторе	509
Иллюстрация на обложке.....	510