

Оглавление

Об авторе	16
О научном редакторе	17
Благодарности	18
Введение	19
О чем эта книга.	20
Сопутствующие файлы	22
Как связаться с автором	22
От издательства.....	22
Глава 1. Освоение окна терминала	23
Файловая система Kali Linux	24
Основные команды терминала.....	25
Окно терминала Tmux	28
Управление пользователями и группами в Kali	32
Пользовательские команды	32
Команды управления группами.....	36
Управление паролями в Kali	37
Управление файлами и папками в Kali Linux	37
Отображение файлов и папок	39
Права доступа	40
Управление файлами в Kali	41
Поиск файлов	42
Сжатие файлов	44
Управление каталогами в Kali	45
Монтирование каталога	46
Управление текстовыми файлами в Kali Linux	47
Vim в сравнении с Nano	49
Поиск и фильтрация текста	50
Удаленные подключения в Kali	51
Протокол удаленного рабочего стола	52
Безопасная командная оболочка	52

SSH с учетными данными	53
SSH без пароля	55
Управление системой Kali Linux	58
Информация о хосте Linux	58
Информация об ОС Linux	58
Информация об аппаратном обеспечении Linux	60
Управление запущенными сервисами	61
Управление пакетами	62
Управление процессами	64
Сеть в Kali Linux	65
Сетевой интерфейс	66
DNS	69
Установленные соединения	70
Передача файлов	71
Резюме	72
Глава 2. Сценарии Bash	73
Базовые сценарии Bash	74
Вывод на экран в Bash	74
Переменные	76
Переменные команд	78
Параметры сценария	78
Пользовательский ввод	80
Функции	80
Условия и циклы	81
Условия	82
Циклы	84
Резюме	86
Глава 3. Сканирование сетевых хостов	88
Основы построения сетей	88
Сетевые протоколы	89
IP-адресация	92
Сетевое сканирование	95
Определение живых хостов	95
Сканирование портов и перечисление сервисов	97
Основы использования сканера Nmap	99
Перечисление сервисов	100
Отпечатки операционной системы	102
Сценарии Nmap	103

Перечисление DNS	107
DNS Brute-Force	107
Передача зоны DNS	108
Инструменты для работы с поддоменами DNS	109
Резюме.	110
Глава 4. Сбор информации в интернете	111
Пассивный сбор информации и разведка	112
Поисковые системы в интернете	112
Сбор информации с помощью Kali Linux	116
Резюме.	125
Глава 5. Атаки методом социальной инженерии	126
Целевые фишинговые атаки	126
Отправка электронного письма	127
Полезная нагрузка и слушатели	132
Прямое и обратное подключение	132
Социальная инженерия с помощью USB Rubber Ducky	137
Обратный шелл с помощью USB Rubber Ducky и PowerShell на практике	139
Создание сценария PowerShell	139
Резюме.	143
Глава 6. Этап продвинутого перечисления	145
Протоколы передачи	146
FTP (порт 21)	146
SSH (порт 22)	150
Telnet (порт 23)	154
Протоколы электронной почты	156
SMTP (порт 25)	157
POP3 (порт 110) и IMAP4 (порт 143)	161
Протоколы баз данных	161
Microsoft SQL Server (порт 1433)	162
Сервер базы данных Oracle (порт 1521)	162
MySQL (порт 3306)	163
Протоколы CI/CD	163
Docker (порт 2375)	163
Jenkins (порт 8080/50000)	165
Подбор учетных данных веб-портала с помощью Hydra	167
Веб-протоколы 80/443	171

Графические протоколы удаленного взаимодействия	172
RDP (порт 3389)	172
VNC (порт 5900)	173
Протоколы обмена файлами	174
SMB (порт 445)	174
SNMP (порт UDP 161)	177
Резюме	178
Глава 7. Фаза эксплуатации	179
Оценка уязвимостей	179
Рабочий процесс оценки уязвимостей	180
Сканирование уязвимостей с помощью OpenVAS	182
Исследование эксплойтов	187
Эксплуатация сервисов	191
Эксплуатация сервиса FTP	191
Эксплуатация сервиса SSH	196
Эксплуатация сервиса Telnet	198
Эксплуатация почтового сервера	202
Эксплуатация Docker	204
Эксплуатация Jenkins	208
Способы получения обратной командной оболочки	212
Эксплуатация протокола SMB	214
Резюме	216
Глава 8. Уязвимости веб-приложений	217
Рабочий процесс оценки уязвимостей	218
Установка Mutillidae	218
Межсайтовое выполнение сценариев (Cross-site scripting)	220
SQL-инъекция	227
Инъекция команд	236
Внедрение файла	237
Подделка межсайтовых запросов	240
Загрузка файла	243
OWASP Top 10	248
Резюме	249
Глава 9. Тестирование веб-приложений на проникновение и жизненный цикл безопасной разработки программного обеспечения	250
Перечисление в веб-приложениях и эксплуатация	250
Burp Suite Pro	251

Больше перечислений	265
Контрольный список для ручного тестирования на проникновение веб-приложений	267
Жизненный цикл безопасной разработки программного обеспечения	270
Этап анализа/архитектуры	270
Этап разработки	274
Этап тестирования	275
Рабочая среда (окончательное развертывание)	275
Резюме	276
Глава 10. Повышение привилегий в Linux	277
Введение в эксплойты ядра и ошибки в конфигурации	278
Эксплойты ядра	278
Эксплойты ядра: Dirty Cow	278
Использование SUID	281
Переопределение файла пользователей Passwd	283
Повышение привилегий через задачи CRON	284
Основы CRON	285
Перечисление и использование CRON	287
Файл конфигурации sudoers	288
Повышение привилегий через sudo	288
Эксплуатация запущенных сервисов	290
Автоматизированные сценарии	291
Резюме	292
Глава 11. Повышение привилегий в Windows	293
Перечисление системы Windows	293
Системная информация	293
Архитектура Windows	295
Список дисковых накопителей	295
Установленные исправления	295
Кто я	296
Список пользователей и групп	296
Сетевая информация	299
Отображение слабых разрешений	301
Список установленных программ	302
Список задач и процессов	303
Передача файлов	303
Место назначения — хост Windows	303
Назначение — хост Linux	304

Эксплуатация системы Windows	305
Эксплойты ядра Windows	306
Эксплуатация приложений Windows	312
Эксплуатация сервисов в Windows	316
Использование запланированных задач	321
Автоматизированные инструменты Windows PrivEsc	321
Резюме.	323
Глава 12. Пивотинг и горизонтальное перемещение	324
Дамп хешей Windows	325
Хеши Windows NTLM	325
Mimikatz	327
Дамп хешей Active Directory	329
Повторное использование паролей и хешей	329
Пивотинг с перенаправлением портов	331
Идея переадресации портов	331
Туннелирование SSH и переадресация локальных портов	333
Переадресация удаленного порта с помощью SSH	334
Динамическая переадресация портов	335
Резюме.	337
Глава 13. Криптография и взлом хешей	338
Основы криптографии.	338
Основы хеширования	339
Алгоритм безопасного хеширования (SHA)	342
Хеширование паролей	343
Код проверки подлинности сообщения на основе хеша	344
Основы шифрования	345
Асимметричное шифрование	348
Взлом паролей с помощью Hashcat	351
Тестирование производительности	352
Взлом хешей в действии	354
Режимы атаки	355
Рабочий процесс взлома	362
Резюме.	363
Глава 14. Отчетность	364
Обзор отчетов при тестировании на проникновение	364
Оценка критичности	365
Общая система оценки уязвимостей, версия 3.1	365

Презентация отчета	368
Обложка	369
Хронология	369
Сводка отчета	370
Раздел с обнаруженными уязвимостями	370
Резюме	370
Глава 15. Язык ассемблера и реверс-инжиниринг	371
Регистры процессора	371
Общие регистры ЦП	372
Индексные регистры	373
Регистры указателей	373
Сегментные регистры	374
Флаговые регистры	374
Инструкции ассемблера	375
Little endian	378
Типы данных	378
Сегменты памяти	379
Режимы адресации	379
Пример реверс-инжиниринга	379
Код Visual Studio для C/C++	380
Отладчик Immunity для реверс-инжиниринга	381
Резюме	386
Глава 16. Переполнение буфера/стека	387
Основы пополнения стека	387
Обзор стека	387
Эксплуатация пополнения стека	396
Описание лаборатории	396
Этап 1. Тестирование	397
Этап 2. Размер буфера	399
Этап 3. Управление EIP	401
Этап 4. Внедрение полезной нагрузки и получение удаленной командной оболочки	403
Резюме	406
Глава 17. Программирование на Python	407
Основы Python	407
Запуск сценариев Python	408
Отладка сценариев Python	409
Установка VS Code на Kali	409

Практика в Python	410
Базовый синтаксис Python	411
Python Shebang	411
Комментарии в Python	411
Отступ строки и импорт модулей	412
Ввод и вывод	412
Переменные	413
Числа	414
Арифметические операторы	415
Строки	415
Списки	417
Кортежи	418
Словарь	418
Дополнительные приемы в Python	419
Функции	419
Глобальные переменные	420
Условия	421
Операторы сравнения	422
Итерации цикла	423
Управление файлами	424
Обработка исключений	425
Экранирование символов	425
Резюме	427
Глава 18. Автоматизация пентеста с помощью Python	428
Робот для тестирования на проникновение	428
Как работает приложение	428
Резюме	443
Приложение А. Kali Linux Desktop: краткий обзор	444
Скачивание и запуск виртуальной машины Kali Linux	444
Первая загрузка виртуальной машины	445
Рабочий стол Kali Xfce	446
Меню Kali Xfce	446
Менеджер настроек Kali Xfce	450
Практический пример настройки рабочего стола	470
Установка Kali Linux с нуля	475
Резюме	484

Приложение Б. Создание лабораторной среды с помощью Docker	485
Технология Docker	485
Основы Docker	487
Установка Docker	487
Образы и реестры	488
Контейнеры	489
Контейнер Docker Mutillidae	493
Резюме.	494