



ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ с KALI LINUX

ИЗУЧИТЕ ПЕНТЕСТ НА ПРАКТИКЕ С НУЛЯ

ДЖОШИ ПРАНАВ • ЧАНДА ДИПАЯН

Penetration Testing with Kali Linux

*Learn Hands-on Penetration Testing
Using a Process Driven Framework*

Pranav Joshi
Deepayan Chanda



www.bpbonline.com

Пранав Джоши
Дипаян Чанда

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ С KALI LINUX

Санкт-Петербург
«БХВ-Петербург»
2022

УДК 004.89
ББК 32.973.26-018
Д42

Джоши, П.

Д42 Тестирование на проникновение с Kali Linux: Пер. с англ. / П. Джоши, Д. Чанда. — СПб.: БХВ-Петербург, 2022. — 256 с.: ил.

ISBN 978-5-9775-1202-2

Подробно рассмотрен процесс тестирования на проникновение, его виды, этапы, юридический и практический аспекты. Даны советы по согласованию плана тестирования, выбору инструментария. Рассказано о возможностях дистрибутива Kali Linux, его настройке, принципах работы с командной строкой, показаны примеры вызова различных команд и написания скриптов для автоматизации рутинных процессов. Описан процесс сборки виртуальной лаборатории для тестирования на проникновение. С использованием инструментов Kali Linux максимально подробно и последовательно описываются все этапы пентеста: сбор информации, разведка и сканирование, перечисление работающих в целевых системах сервисов и служб, обнаружение уязвимостей, поиск эксплойтов, эксплуатация и постэксплуатация. Отдельный раздел посвящен правильному оформлению отчета о тестировании на проникновение и сопроводительной документации.

Для начинающих специалистов по информационной безопасности

УДК 004.89
ББК 32.973.26-018

Группа подготовки издания:

Руководитель проекта	<i>Павел Шалин</i>
Зав. редакцией	<i>Людмила Гауль</i>
Компьютерная верстка	<i>Ольги Сергиенко</i>
Оформление обложки	<i>Зои Канторович</i>

Copyright 2021 BPB Publications, India. All rights reserved.
First published in the English language under the title *Penetration Testing with Kali Linux*, ISBN 9789390684793 by BPB Publications India. (sales@bpbonline.com)
Russian translation rights arranged with BPB Publications, India

© 2021 BPB Publications, Индия. Все права защищены.
Впервые опубликовано на английском языке под названием *Penetration Testing with Kali Linux*, ISBN 9789390684793 издательством BPB Publications India. (sales@bpbonline.com)
Права на перевод на русский язык предоставлены издательством BPB Publications, Индия

Подписано в печать 29.07.22.
Формат 70×100^{1/16}. Печать офсетная. Усл. печ. л. 20,64.
Тираж 1000 экз. Заказ № 5075.
"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20
Отпечатано с готового оригинал-макета
ООО "Принт-М", 142300, М.О., г. Чехов, ул. Полиграфистов, д. 1

ISBN 978-93-90684-793 (англ.)
ISBN 978-5-9775-1202-2 (рус.)

© BPB Publications, India, 2021
© Перевод на русский язык, оформление. ООО "БХВ-Петербург",
ООО "БХВ", 2022

Оглавление

От рецензентов.....	11
Об авторах.....	17
О рецензентах.....	18
Благодарности.....	21
Предисловие	22
Глава 1. Основы тестирования на проникновение	25
Структура	25
Цели	25
Что такое тестирование на проникновение?	26
Предварительные действия для тестирования на проникновение	26
Этапы тестирования на проникновение	27
Сбор информации	28
Разведка и сканирование	28
Исследование уязвимостей	28
Эксплуатация и получение доступа	28
Постэксплуатация и поддержание доступа	28
Документация и отчетность	29
Виды тестирования на проникновение	29
Внутреннее тестирование	29
Внешнее тестирование	29
«Черный ящик», «белый ящик» и «серый ящик»	29
Настройка виртуальной лаборатории тестирования на проникновение	30
Установка VirtualBox	31
Настройка сети VirtualBox	33
Установка Kali Linux	34
Заключение.....	39
Вопросы.....	39
Глава 2. Лаборатория для тестирования на проникновение.....	41
Структура	41
Цели	41

Целевые машины	42
Настройка целей	43
Импорт виртуальных целей	44
Специальная инструкция по импорту Kioptrix: 2014	45
Концепции, охваченные упражнениями на тестирование	47
Заклочение.....	48
Контрольные вопросы.....	48
Глава 3. Знакомство с Kali Linux	49
Структура	49
Цели	49
Изменение пароля по умолчанию	51
Изменение часового пояса	51
Справка по командам	52
Установка, удаление и обновление пакетов.....	53
<i>apt search</i> <строка-поиска>	53
<i>apt show</i> <имя пакета>	54
<i>apt install</i> <имя пакета>	54
<i>apt remove</i> <имя пакета>	54
<i>apt update</i>	55
<i>apt upgrade</i>	56
<i>dpkg</i>	56
Поиск файлов	56
<i>locate</i> <имя файла>	56
<i>whereis</i> <имя файла>	57
<i>find</i> <каталог поиска> <критерий> <строка поиска>	57
Управление службами в Kali Linux.....	58
<i>service</i> <имя службы> <i>start</i>	58
<i>service</i> <имя службы> <i>restart</i>	58
<i>service</i> <имя службы> <i>status</i>	59
<i>service</i> <имя службы> <i>stop</i>	59
Обеспечение постоянной работы службы с помощью <i>update-rc.d</i>	60
Основы создания скриптов (сценариев) оболочки	60
Подстановка команд	60
Цепочка команд и перенаправление ввода, вывода, ошибки	61
Циклы	64
Плагины для браузера	65
HackBar V2	67
Cookie Quick Manager.....	67
Tamper Data for FF Quantum	67
Заклочение.....	68
Вопросы.....	68
Глава 4. Понимание этапов процесса тестирования	69
Структура	69
Цели	69
Важность структурированного тестирования на проникновение	70
Фреймворк для тестирования на проникновение	71
Этап 1: предварительные действия.....	72
Этап 2: планирование	73

Этап 3: сбор информации	74
Пассивный сбор информации	74
Активный сбор информации	75
Историческая информация	75
Этап 4: разведка	76
Этап 5: составление перечня служб	77
Получение информации NetBIOS	78
Получение информации SNMP	79
Получение информации DNS	79
Этап 6: исследование уязвимостей	79
Этап 7: эксплуатация	80
Этап 8: отчетность	80
Цели тестирования	81
Предполагаемые заинтересованные стороны	81
Краткое резюме	81
Методология	81
Выводы и связанные с ними подробности	81
Образцы и примеры	82
Уровни риска	82
Подробные выводы	83
Заключение	83
Вопросы	83
Глава 5. Планирование и разведка	85
Структура	85
Цели	85
Планирование теста на проникновение	85
Ожидания клиентов	86
Объем тестирования	86
Способы коммуникации	87
Иерархия эскалации в случае возникновения проблем	87
Ключевой персонал	87
Окно тестирования	88
Ограничения тестирования	88
Разведка	89
DC:7	90
Digitalworld.local:Joy	96
Kioptrix:5	100
HackInOS:1	103
Sunset:Nightfall	105
Mumbai:1	108
Заключение	110
Вопросы	110
Глава 6. Составление перечня и сканирование служб	111
Структура	111
Цели	111
DC-7	111
Digitalworld.local: Joy	116
Kioptrix:5	123
HackInOS:1	127

Sunset: Nightfall	131
Mumbai: 1	137
Заклочение.....	145
Вопросы.....	145
Глава 7. Исследование уязвимостей	147
Структура	147
Цели	147
DC-7	148
Digitalworld.local:Joy	153
Kioptrix:5	157
HackInOS:1	162
Sunset:Nightfall	167
Mumbai: 1	170
Заклочение.....	173
Вопросы.....	174
Глава 8. Эксплуатация	175
Структура	175
Цели	175
DC-7	176
Digitalworld.local:Joy	179
Kioptrix:5	187
HackInOS:1	192
Sunset:Nightfall	194
Mumbai: 1	196
Заклочение.....	198
Вопросы.....	198
Глава 9. Постэксплуатация	199
Структура	199
Цели	199
DC-7	200
Digitalworld.local:Joy	202
Kioptrix:5	206
HackInOS:1	209
Sunset:Nightfall	213
Mumbai: 1	218
Заклочение.....	222
Вопросы.....	222
Глава 10. Отчет	223
Структура	223
Цели	223
Составление отчетов	224
Заинтересованные стороны	224
Исполнительный менеджмент	224
Технический персонал	225
Аудиторы и службы надзора	225
Что можно и чего нельзя делать при тестировании на проникновение	225
Что можно делать	226
Определять приоритеты факторов риска.....	226

Повышать квалификацию	226
Не преуменьшать значение отчета	226
Участвовать в устранении обнаруженных уязвимостей	227
Обязательно сделать резервную копию всех ваших данных	227
Чего нельзя делать	228
Быть незэтичным	228
Не соглашаться с результатами тестирования	228
Не соблюдать ограничения объема тестирования	229
Устанавливать большие промежутки в графике тестирования или проводить тестирование исключительно для соблюдения требований соответствия	229
Использовать неавторизованные инструменты и скрипты	230
Заключение	230
Вопросы	230
ОТЧЕТ ПО РЕЗУЛЬТАТАМ ТЕСТА НА ПРОНИКНОВЕНИЕ (пример)	231
Детали проекта	233
Список версий	233
Список рассылки	233
Информация о команде тестирования	233
Информация о представителях заказчика	234
Объем работ	234
Сроки исполнения проекта	234
Окно тестирования	234
Ограничения теста	234
Методология тестирования	234
Этап 1: определение объема и планирование	235
Этап 2: сбор информации и разведка	235
Этап 3: составление перечня и сканирование служб	236
Этап 4: исследование уязвимостей	236
Этап 5: эксплуатация	236
Этап 6: отчетность	236
Стандартные определения	237
Рейтинг уязвимостей	237
Краткое резюме	238
Графическое представление результатов тестирования	238
Список уязвимостей	238
Обобщенный анализ	239
Стратегические рекомендации	239
Техническое резюме	240
Низкий уровень — 1	240
Низкий уровень — 2	241
Высокий уровень — 1	242
Высокий уровень — 2	244
Низкий уровень — 3	245
Средний уровень — 1	246
Средний уровень — 2	247
Высокий уровень — 3	248
Высокий уровень — 4	249
Ссылки	250
Предметный указатель	251