Юрген Эбнер

ЭТИЧНЫЙ ХАКИНГ

ИНСТРУМЕНТЫ ТЕСТИРОВАНИЯ НА ВЗЛОМ И ОБЕСПЕЧЕНИЕ ИТ-БЕЗОПАСНОСТИ

БОМБОРА
ИЗДАТЕЛЬСТВО
Москва 2025

УДК 004.056
ББК 32.973.26-018.2
Э13

Jürgen Ebner
Einstieg in Ethical Hacking: Penetration Testing und Hacking-Tools für die IT-Security

Книга предназначена исключительно для образовательных целей и направлена на обучение методам защиты компьютерных систем и сетей от несанкционированного доступа. Она соответствует законодательству Российской Федерации и международным нормам, регулирующим деятельность в области информационной безопасности. Использование полученных знаний должно осуществляться только в рамках закона и профессиональной этики. Автор и издательство не несут ответственности за неправомерное применение изложенных материалов и инструментов. Все практические задания и эксперименты рекомендуется проводить в специально созданных тестовых средах и лабораториях, исключающих риск нарушения прав третьих лиц и нанесения ущерба чужим ресурсам. Мы не поощряем и не оправдываем использование методов хакинга в целях незаконного проникновения, кражи данных или иных противоправных действий.

Эбнер, Юрген.

Э13 Этичный хакинг. Инструменты тестирования на взлом и обеспечение ИТ-безопасности / Юрген Эбнер ; [перевод с немецкого М. В. Семашко]. — Москва : Эксмо, 2025. — 336 с. — (Мировой компьютерный бестселлер).

Хотите стать специалистом по этичному хакингу и научиться эффективно защищать компьютерные системы? Изучайте основы белого взлома с этой книгой, осваивайте мощнейшие инструменты Kali Linux и создавайте собственную лабораторию для тестов. Узнайте секреты автоматизации процессов с помощью BASH-скриптов и Python-программирования. Шаг за шагом пройдите путь от начальной разведки до финального отчета о проверках. Научитесь проводить тестирование на взлом и обеспечение ИТ-безопасности законно, повышая свою квалификацию и профессионализм.

Книга подойдет как начинающим специалистам, так и опытным профессионалам, стремящимся систематизировать знания и освоить новые технологии обеспечения информационной безопасности.

УДК 004.056
ББК 32.973.26-018.2

Научно-популярное издание
МИРОВОЙ КОМПЬЮТЕРНЫЙ БЕСТСЕЛЛЕР

Эбнер Юрген

ЭТИЧНЫЙ ХАКИНГ

ИНСТРУМЕНТЫ ТЕСТИРОВАНИЯ НА ВЗЛОМ И ОБЕСПЕЧЕНИЕ ИТ-БЕЗОПАСНОСТИ

12+

Главный редактор *Р. Фасхутдинов*
Руководитель направления *В. Обручев*
Продюсер *Е. Бойцова*
Ответственный редактор *Л. Салихова*
Научный редактор *Н. Фидченко*
Литературный редактор *Е. Пригородова*
Младший редактор *М. Назаренко*
Художественный редактор *Д. Манжавидзе*
Компьютерная верстка *С. Никонорова*
Корректоры *Е. Ерошкина, Л. Макарова*

Страна происхождения: Российская Федерация
Шығарушы ел: Ресей Федерациясы

ООО «Издательство «Эксмо»
123308, Россия, г. Москва, ул. Зорге, д. 1, стр. 1, эт. 20, каб. 2013. Тел.: 8 (495) 411-68-86.
Home page: www.eksmo.ru E-mail: info@eksmo.ru
Өндіруші: «Издательство «Эксмо» ЖШҚ,
123308, Ресей, Мәскеу қаласы, Зорге көшесі, 1-үй, 1-құрылыс, 20 қабат, 2013-каб.
Тел.: 8 (495) 411-68-86. Home page: www.eksmo.ru E-mail: info@eksmo.ru.
Тауар белгісі: «Эксмо»
Интернет-магазин : www.book24.ru
Интернет-магазин : www.book24.kz
Интернет-дүкен : www.book24.kz

Импортёр в Республику Казахстан ТОО «РДЦ-Алматы».
Қазақстан Республикасына импорттаушы «РДЦ-Алматы» ЖШС.

Дистрибьютор и представитель по приему претензий на продукцию в Республике Казахстан: ТОО «РДЦ-Алматы»

ТОО РДЦ Алматы, Алматы, ул. Домбровского, 3«а», литер Б, офис 1.

Дистрибьютор жане Қазақстан Республикасында өнімге шағымдар қабылдау жөніндегі өкіл: «РДЦ-Алматы» ЖШС.

Алматы қ., Домбровский көш., 3 «а», литер Б, офис 1.
Тел.: 8 (727) 251-59-90/91/92. E-mail: RDC-Almaty@eksmo.kz

Сведения о подтверждении соответствия издания согласно законодательству РФ о техническом регулировании можно получить на сайте Издательства «Эксмо»: www.eksmo.ru/certification

Техникалық реттеу туралы РФ заңнамасына сай басылымның сәйкестігін растау туралы мәліметтерді мына адрес бойынша алуға болады: http://eksmo.ru/certification/

Произведено в Российской Федерации
Ресей Федерациясында өндірілген

Сертификаттауға жатпайды

Дата изготовления / Подписано в печать 08.10.2025.
Формат 70x100 1/16. Печать офсетная. Усл. печ. л. 27,22.
Тираж экз. Заказ

ISBN 978-5-04-218081-1

ISBN 978-5-04-218081-1

Содержание

Введение

Не так давно хакерство было скорее табу, и обучающие тренинги по этой теме не проводились. Однако сейчас пришло осознание, что «наступательный подход» обеспечивает дополнительную ценность для IT-безопасности. Этот новый метод приветствуется большими и малыми организациями различных отраслей деятельности: государственные учреждения теперь серьезно относятся к «наступательной» безопасности, а правительства официально признают, что работают в этом направлении.

Важную роль в концепции безопасности организации играют тесты на проникновение. Политика оценки рисков, планы чрезвычайных ситуаций и восстановление после катастроф стали неотъемлемыми мерами обеспечения IT-безопасности. Тестирование на проникновение также должно быть включено в общее планирование. С помощью таких тестов вы сможете узнать, как вас воспринимает противник. Это даст ключ к неожиданным открытиям и позволит вам выиграть драгоценное время для улучшения систем прежде, чем произойдет реальная атака.

В настоящее время существует множество хороших инструментов для взлома. Большинство из них не просто «существуют», но и стабильно запускаются благодаря многолетнему развитию. Еще более важно, что многие из этих инструментов доступны бесплатно.

Звучит заманчиво, но для начала вам нужно найти, скомпилировать и установить эти инструменты, прежде чем можно будет выполнить даже самый простой тест на проникновение. В современных операционных системах Linux это сделать относительно легко. Но для новичков данная задача может оказаться сложной. Даже для опытных пользователей сбор и установка всех инструментов — дело утомительное.

Сообщество безопасности, к счастью, активное и независимое. Несколько организаций неустанно работали над созданием различных дистрибутивов Linux для взлома и тестирования на проникновение. Дистрибутив (сокращенно Distro) — вариант Linux. Для тестирования взлома и проникновения существуют такие дистрибутивы Linux, как:

- Parrot Security OS;
- BlackBox;
- BlackArch;
- Fedora Security Spin;

- Samurai Web Testing Framework;
- Pentoo Linux;
- DEFT Linux;
- Caine;
- Network Security Toolkit (NST);
- Kali Linux.

Самый популярный Distro для тестов на проникновение — Kali Linux. Поэтому в этой книге мы также используем его в качестве инструмента взлома, который можно применить во всех других дистрибутивах Linux, а иногда даже в Windows. Благодаря Kali Linux, а также другим операционным системам для взлома, начинающие специалисты по безопасности, Pentester и IT-специалисты получают обширную платформу для планирования и проведения цифровых атак.

Зачем вам это нужно?

С одной стороны, для борьбы с потенциальными атаками на собственные системы, а с другой — для лучшего понимания внутренних и внешних уязвимостей.

«Хакерская операционная система», такая как Kali Linux & Co., уже по умолчанию наполнена инструментами, которые либо лишают сна специалистов по безопасности и IT-руководителей, либо заставляют их глаза блестеть.

На самом деле хакерские операционные системы не содержат ничего эксклюзивного. Вы можете установить любой инструмент, программное обеспечение и скрипт на всякий выбранный вами Linux (иногда даже на Windows), однако многие исследователи безопасности прибегают к Kali.

Причина, по которой часто используются дистрибутивы типа Kali & Co, заключается в том, что большинство программ, включая соответствующие настройки, уже активированы или могут быть просто установлены из репозиториев. Другая причина — Kali очень хорошо работает в изолированной среде. Если что-то пойдет не так, систему можно быстро переустановить и начать с нуля. Это гораздо лучше полного разрушения продуктивной среды.

Предупреждение

Неправильное применение инструментов безопасности в вашей сети, особенно без разрешения, может причинить непоправимый ущерб с серьезными последствиями. Никогда не тестируйте и не взламывайте системы без разрешения.

Об этой книге

Эта книга — практическое руководство для всех, кто интересуется этичным хакингом и тестированием на проникновение. Она предназначена как для начинающих, так и для опытных пользователей, которые хотят расширить свои навыки в области IT-безопасности. Книга объясняет основы этичного взлома, правовые и этические аспекты, а также основные методы и инструменты, используемые хакерами для обнаружения и использования уязвимостей в сетях и системах.

Я построил книгу таким образом, чтобы вы могли использовать ее, даже если у вас нет опыта в оценке безопасности или вы еще не работали с Linux. Прочитав ее, вы сможете успешно проводить оценки безопасности в качестве тестировщика на проникновение — даже если вы новичок.

В первой части книги вы найдете все основы, необходимые для этичного хакинга, в частности краткое введение в Kali Linux, создание хакерской лаборатории и самые важные основы Linux. Так что, если вы новичок в Linux, вы без проблем сможете следовать инструкциям в книге. Вы узнаете, какие существуют виды оценки безопасности и какую роль в них играет тестирование на проникновение. Вы также получите представление о BASH-скриптах и о том, как работает язык программирования Python. Они пригодятся для адаптации существующих инструментов взлома или их автоматизации.

Вторая часть книги посвящена планированию и проведению тестов на проникновение. Вы подробно изучите различные этапы тестирования, разнообразные атаки и подходящие инструменты для взлома. Также здесь поясняется, каких рекомендаций следует придерживаться при проведении тестов, чтобы взламывать безопасно и этично.

Дополнительная информация

На домашней странице (https:// www.jürgenebner.com/) вы найдете информацию об актуальных темах безопасности и изменениях в моих книгах. Также здесь можно оставлять отзывы, чтобы мы могли улучшить последующие издания.

Часть 1

Основы этичного взлома

В этой части книги вы узнаете все, что нужно для начала работы с этичным взломом. Мы рассмотрим различия между целями этичных хакеров и злоумышленников, а также разберем, как зародился и развивался этичный хакинг.

В книге мы будем работать с Kali Linux, но этот инструмент подходит не всем. Поэтому мы также рассмотрим, какие существуют альтернативы Kali Linux, чтобы в случае необходимости вы могли прибегнуть к ним.

Прежде чем приступить к взлому, вам необходимо настроить систему. Для этой книги мы выбрали быстрый старт, поэтому будем использовать Image для Virtual Box. Кроме того, здесь описана общая установка Kali Linux.

В этой части:

Глава 1

Что такое этичный взлом

С помощью этой книги вы сможете обнаружить слабые стороны на своем компьютере и в вашей сети и устранить их до того, как киберпреступники получат возможность воспользоваться ими.

Поскольку термин «этика» часто используется в неправильном ключе, посмотрим, как он определяется в словарях:

> *Совокупность моральных норм и принципов, на которых основывается {ответственное} отношение.*

Это определение отлично согласуется с данной книгой, а также с профессиональными тестами и методами безопасности, которые в ней рассматриваются. Специалисты в области информационных технологий и безопасности данных обязаны выполнять представленные здесь методы честно и **только с прямого разрешения владельцев систем**.

1.1 Определение

Судя по сообщениям СМИ, многие уже ощущают последствия кибератак. Большинство наверняка слышали о хакерах и злоумышленниках. Но кто эти люди? Что следует о них знать?

Чтобы избежать недоразумений, мы определяем здесь следующие термины:

- **Хакер.** Внешний злоумышленник, атакующий компьютеры с намерением украсть конфиденциальные данные для достижения незаконной цели.
- **Злоумышленники (Вредоносные пользователи**). Внутренние пользователи, которые атакуют компьютеры и конфиденциальные данные изнутри в качестве авторизованных и «доверенных» пользователей. Злоумышленник чаще всего атакует системы, чтобы отомстить, но в некоторых случаях преследует и незаконные цели.

  Атакующие могут быть как хакерами, так и злоумышленниками. И тех и других проще назвать хакерами. Различие между терминами мы проведем в том случае, если нам понадобится глубже изучить их инструменты, методы и способы мышления.
- **Этичные хакеры.** «Хорошие парни», которые взламывают системы, чтобы выявить слабые стороны и иметь возможность создавать средства защиты от несанкционированного доступа. Это могут быть консультанты по IT-безопасности или штатные сотрудники.

1.2 Что такое «хакер»?

Когда мы рассуждаем о хакере, на ум многим приходит типичный компьютерный ботаник в толстовке с капюшоном. Но что такое «хакер» на самом деле?

Лучшее описание, которое я слышал, имеет мало общего с компьютерами. Оно таково: *хакер — это человек, который решает проблему творческим способом*.

В первоначальном значении это человек, увлеченный технологиями в контексте игривой, самозабвенной преданности и с особым чувством креативности. Однако сегодня термин «хакер» чаще всего имеет негативный оттенок; под ним мы понимаем человека, который незаконно проникает в компьютерные системы. Он получает удовольствие от исследования программируемых систем и в процессе расширяет свои возможности. Ему нравится интеллектуальный вызов, который можно преодолеть и обойти творческими способами. Этот человек обладает знаниями в области технических устройств и интернета, и он пытается перехитрить, перепрофилировать или модифицировать технику.

Что отличает программистов или компьютерных ученых от хакеров? Это непростой вопрос, так как четкого определения нет. Программист — это обычная профессия, которой можно обучиться, не становясь хакером автоматически.

Есть несколько моментов, которые отличают хакеров от программистов: хакеры пробуют что-то новое, незадокументированное. Они экспериментируют и тестируют программное обеспечение или оборудование. Им необязательно знать, как все это работает: они пытаются разобраться с помощью своих тестов. Программисты и программистки придерживаются систем, которые знают. Хакеры пытаются заставить программное обеспечение вести себя так, как им нужно. Они ищут незадокументированные углы, что часто означает действовать методом проб и ошибок. Хакеры получают удовольствие от того, что у других обычно вызывает разочарование. Как правило, они принимают вызов и не дают себе отдыха, пока не поймут, что происходит.

Для улучшения осведомленности хакеры и хакерши часто делятся своими знаниями с сообществом. Они документируют свои шаги, чтобы и другие могли достичь данного уровня. Это помогает им выйти за рамки своих способностей.

Хакеров можно разделить на различные группы в зависимости от их деятельности:

- Hardware Hacker (модификация и создание аппаратного обеспечения);
- Open Source Software (программное обеспечение с открытым исходным кодом);

- Security (защита информации и систем от несанкционированного доступа и атак);
- Hacktivismus (проведение кибератак в политических целях);
- File Sharing (предоставление файлов в общий доступ);
- Cracking-Szene (несанкционированный взлом для обхода защиты или создания пиратских копий).

Этот список, безусловно, неполный. В сообществе пытались отделить незаконные действия от «хороших» хакеров — в частности, установить термин Cracker (взломщик). Но, к сожалению, он не прижился. Поэтому нам придется принять, что слово «хакер» стало обобщающим определением для многих описаний. В наше время этот термин обычно понимают неправильно. В разговорной речи он звучит негативно, но на самом деле означает высококвалифицированных компьютерных чудаков. Это люди, которые занимаются компьютерными системами и особенно любознательны. Они любят вызовы и с удовольствием изучают что-то новое. Хакера отличает творческий подход, умение развивать собственные идеи, создавать что-то новое и максимально креативно использовать свои навыки. Они готовы усердно работать, чтобы достичь своих целей, и делиться своими знаниями с единомышленниками. И это положительные качества, которые многие компании хотят видеть у своих сотрудников.

Как и везде, среди хакеров есть «паршивые овцы». Это специализированная группировка криминальных взломщиков, которые несут ответственность за негативный имидж хакеров. Они проникают в сети и компьютерные системы, крадут данные и взламывают пароли.

1.3 Типы хакеров и их мотивация

Термин «хакер» подразумевает и хороших хакеров, и тех, кто действует тайно. Поэтому часто говорят о «белых шляпах» и «черных шляпах» среди хакеров. Эта классификация берет начало из старых вестернов, в которых хорошие персонажи всегда носили белые шляпы, а злодеи — черные. Однако сейчас большинство людей связывают с термином «хакер» что-то негативное.

Примечание

Многие злоумышленники утверждают, что делают это ради блага общества и не хотят никому навредить. Будьте осторожны и не путайте сотрудника службы безопасности с преступным хакером. Первые занимаются взломами в честных интересах и также разрабатывают инструменты, которые помогают нам в работе. Они осознают свою ответственность и заботятся о том, чтобы их результаты и исходные коды программ были опубликованы.