

Юрген Эбнер

ЭТИЧНЫЙ ХАКИНГ
ИНСТРУМЕНТЫ ТЕСТИРОВАНИЯ
НА ВЗЛОМ И ОБЕСПЕЧЕНИЕ
ИТ-БЕЗОПАСНОСТИ

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

© 2024 mitp Verlags GmbH & Co. KG, Frechen

Published in German Language as: *Einstieg in Ethical Hacking — Penetration Testing & Hacking-Tools fuer die IT-Security* by Jürgen Ebner, 1st Edition 2024 by MITP Verlag, Germany / All Rights Reserved. Published with arrangements made by Maria Pinto-Peuckmann, Literary Agency — World Copyright Promotion, Kaufering, Germany

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

Все права защищены. Книга или любая ее часть не может быть скопирована, воспроизведена в электронной или механической форме, в виде фотокопии, записи в память ЭВМ, репродукции или каким-либо иным способом, а также использована в любой информационной системе без получения разрешения от издателя. Копирование, воспроизведение и иное использование книги или ее части без согласия издателя является незаконным и влечет уголовную, административную и гражданскую ответственность.

Научно-популярное издание
МИРОВОЙ КОМПЬЮТЕРНЫЙ БЕСТСЕЛЛЕР

Эбнер Юрген

ЭТИЧНЫЙ ХАКИНГ

ИНСТРУМЕНТЫ ТЕСТИРОВАНИЯ НА ВЗЛОМ И ОБЕСПЕЧЕНИЕ ИТ-БЕЗОПАСНОСТИ

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

12+

БОМБОРА
ИЗДАТЕЛЬСТВО

БОМБОРА – лидер на рынке полезных и вдохновляющих книг. Мы любим книги и создаем их, чтобы вы могли творить, открывать мир, пробовать новое, расти. Быть счастливыми. Быть на волне.

🌐 bombora.ru 📖 bomborabooks 📱 bombora



eksmo.ru
Официальный интернет-магазин издательства «Эксмо»



Хочешь стать автором «Эксмо»?



ТЕРИТОРИЯ
КНИЖНЫЙ МАГАЗИН
Официальное франшиза издательства «Эксмо»



9 785042 180811 >



ЧИТАЙТЕ И СЛУШАЙТЕ
в Литрес

ООО «Издательство «Эксмо»
123336, 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
Финдирект: «Издательство «Эксмо» ЖШҚ
123336, 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.kz
Интернет-магазин: www.book24.kz
Интернет-дүкен: www.book24.kz
Импортер в Республику Казахстан ТОО «РДЦ-Алматы»
Казахстан Республикасына импорттаушы «РДЦ-Алматы» ЖШС.
Дистрибутор и представитель по приему претензий на продукцию в Республике Казахстан: ТОО «РДЦ-Алматы»
ТОО РДЦ Алматы, Алматы, ул. Домбровскийго, 3-а, литер Б, офис 1.

Дистрибутор және Қазақстан Республикасында өнімге шағындар келдіруді жүзеге асыратын өзі: «РДЦ-Алматы» ЖШС.
Алматы қ., Домбровский кеші, 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
Республикасында өндірілген
Сертификаттауа жатпайды

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

ЧИТАЙТЕ
ГОРОД

ISBN 978-5-04-218081-1

© Семашко М.В., перевод на русский язык, 2025
© Оформление. ООО «Издательство «Эксмо», 2025

Содержание

Введение.....	9
Часть 1. Основы этичного взлома	13
1 Что такое этичный взлом	15
1.1 Определение	15
1.2 Что такое «хакер»?	16
1.3 Типы хакеров и их мотивация	17
1.4 Роль этичного хакера	19
1.5 Как стать хакером или хакершей?.....	23
1.6 Сбор информации об инструментах.....	24
1.7 Руководящие принципы, соответствие требованиям и нормативные аспекты.....	25
1.8 Зачем взламывать себя?.....	26
1.9 Стратегия и методология в этичном взломе	27
1.10 Понимание опасностей	29
1.11 Резюме.....	30
2 Операционные системы для хакеров	32
2.1 Kali Linux	32
2.2 Backbox	32
2.3 Parrot OS	33
2.4 BlackArch	34
2.5 Deft Linux.....	35
2.6 Pentoo Linux.....	35
2.7 CAINE	36
2.8 Fedora Security Spin	37
2.9 Резюме.....	38
3 Подготовка операционной системы	39
3.1 Установка Kali-Linux	39
3.2 Автономная установка.....	44
3.3 Kali Linux в качестве виртуальной машины.....	57
4 Основы (Kali-)Linux	64
4.1 Что такое Linux?	64
4.2 Управление оборудованием.....	66
4.3 Стандартизированная файловая система.....	67
4.4 Управление процессами	68
4.5 Командная строка (Command Line)	69
4.6 Файловая система Kali	72
4.7 Управление правами	74
4.8 Полезные команды для командной строки	78
4.9 Службы.....	82
4.10 Резюме.....	83

5	Начало работы и создание хакерской лаборатории с Kali Linux	84
5.1	Первый шаг с Kali Linux	84
5.2	Установка инструментов и обновлений	90
6	Введение в оценку уровня безопасности	95
6.1	Что означает «безопасность», когда речь идет об информационных системах?	95
6.2	Виды оценок	97
6.3	Стандартизация оценок	108
6.4	Виды атак	109
6.5	Резюме.....	113
7	Введение в программирование и shell-скрипты	115
7.1	Языки программирования для этичного хакинга	115
7.2	Программирование на языке Python	117
7.3	Bash-скрипты	124
7.4	Резюме.....	129

Часть 2. Проведение тестов на проникновение 131

8	Тест на проникновение	133
8.1	Сфера применения теста на проникновение (Scope).....	136
8.2	Вопросы для определения объема теста на проникновение.....	140
8.3	Цель	144
8.4	Бизнес-анализ	144
8.5	Указание диапазонов IP-адресов и доменов.....	145
8.6	Взаимодействие с третьими лицами	145
8.7	Определение приемлемых предложений для социальной инженерии	147
8.8	DoS-тесты.....	147
8.9	Условия оплаты.....	147
8.10	Установка каналов связи	148
8.11	Правила оформления заказа.....	150
8.12	Существующие функции и технологии	153
8.13	Резюме.....	154
9	Сбор информации (разведка)	155
9.1	Введение	155
9.2	Исследование	156
9.3	Определение целей	158
9.4	Пассивное сканирование против активного.....	158
9.5	Инструменты для сбора информации.....	159
9.6	Анализ информации и поиск целей	180
9.7	Как вы можете отработать эти действия?.....	181
9.8	Резюме.....	182
10	Активное сканирование	183
10.1	Введение	183
10.2	Обнаружение активных хостов с помощью ping	186

10.3	Portscan	187
10.4	Автоматизация сбора информации с помощью legion	199
10.5	Сканирование уязвимостей.....	201
10.6	Siege — проверка производительности веб-сайтов	212
10.7	Как вы можете практиковать эти действия?	213
10.8	Каковы дальнейшие действия?	214
10.9	Резюме.....	214
11	Вторжение через локальную сеть.....	215
11.1	Доступ к удаленным сервисам.....	216
11.2	Захват системы	219
11.3	Взлом паролей.....	229
11.4	Пароли из каталога Active Directory.....	240
11.5	Слежка за сетевым трафиком (Sniffing).....	244
11.6	Armitage — взлом с помощью «пулемета»	253
11.7	Как вы можете отработать этот шаг?	256
11.8	Каковы дальнейшие действия?	258
11.9	Резюме.....	260
12	Вторжение через веб-интерфейс	261
12.1	Основы веб-взлома.....	261
12.2	Поиск уязвимостей в веб-приложениях.....	263
12.3	WebScarab — анализ веб-сайтов (паук).....	270
12.4	Инъекция кода.....	275
12.5	Когда браузеры доверяют веб-сайтам — XSS-атаки	278
12.6	ZAP — Zed Attack Proxy, инструмент «все в одном».....	281
12.7	Как вы можете отработать этот шаг?	284
12.8	Каковы дальнейшие действия?	286
12.9	Резюме.....	286
13	Социальная инженерия	288
13.1	Основы SET	288
13.2	Целевая фишинг-атака	290
13.3	Веб-сайт как вектор атаки	290
13.4	Credential Harvester/Сбор учетных данных	296
13.5	Дополнительные опции в SET.....	297
13.6	Резюме.....	300
14	Пост-обработка и сохранение доступа	301
14.1	Netcat — швейцарский армейский нож	302
14.2	Cryptcat — криптографический кузен Netcat	307
14.3	Руткиты	308
14.4	Meterpreter — молоток, который делает гвоздь из чего угодно	311
14.5	Как вы можете отработать этот шаг?	314
14.6	Каковы дальнейшие действия?	315
14.7	Резюме.....	316
15	Завершение теста на проникновение.....	317
15.1	Инструменты для отчета.....	317

15.2	Отчет о тестировании.....	324
15.3	Каковы дальнейшие действия?.....	329
15.4	Резюме.....	330
Приложение А.....		331
	Эпилог.....	331
	Совет на будущее.....	331
	Заключительное замечание.....	333
	Предметный указатель.....	333

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 ИТ-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 ИТ-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 репозитория. 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.jurgenebner.com/](https://www.jurgenebner.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.....	15
■ Глава 2	
Операционные системы для хакеров.....	32
■ Глава 3	
Подготовка операционной системы.....	39
■ Глава 4	
Основы (Kali-)Linux.....	64
■ Глава 5	
Начало работы и создание хакерской лаборатории с Kali Linux	84
■ Глава 6	
Введение в оценку уровня безопасности	95
■ Глава 7	
Введение в программирование и shell-скрипты.....	115

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 игровой, 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.