

ЭТИЧНЫЙ ХАКИНГ

практическое руководство по взлому



Дэниел Г. Грэм

Предисловие Хуана Гилберта



ЭТИЧНЫЙ ХАКИНГ

практическое руководство по взлому

Дэниел Г. Грэм



Санкт-Петербург • Москва • Минск

2023

ББК 32.973.23-018-07

УДК 004.56.53

Г91

Грэм Дэниел Г.

Г91 Этичный хакинг. Практическое руководство по взлому. — СПб.: Питер, 2023. — 384 с.: ил. — (Серия «Библиотека программиста»).

ISBN 978-5-4461-1952-3

Практическое руководство по взлому компьютерных систем с нуля, от перехвата трафика до создания троянов. Книга «Этичный хакинг» освещает современные проблемы кибербезопасности и помогает освоить навыки, необходимые любому этичному хакеру. Сделайте первый шаг в карьере пентестера, ознакомившись с методами взлома, которые используют эксперты.

16+ (В соответствии с Федеральным законом от 29 декабря 2010 г. № 436-ФЗ.)

ББК 32.973.23-018-07

УДК 004.56.53

Права на издание получены по соглашению с No Starch Press. Все права защищены. Никакая часть данной книги не может быть воспроизведена в какой бы то ни было форме без письменного разрешения владельцев авторских прав.

Информация, содержащаяся в данной книге, получена из источников, рассматриваемых издательством как надежные. Тем не менее, имея в виду возможные человеческие или технические ошибки, издательство не может гарантировать абсолютную точность и полноту приводимых сведений и не несет ответственности за возможные ошибки, связанные с использованием книги. Издательство не несет ответственности за доступность материалов, ссылки на которые вы можете найти в этой книге. На момент подготовки книги к изданию все ссылки на интернет-ресурсы были действующими.

ISBN 978-1718501874 англ.

© 2021 by Daniel G. Graham. Ethical Hacking: A Hands-on Introduction to Breaking In, ISBN 9781718501874, published by No Starch Press Inc. 245 8th Street, San Francisco, California United States 94103.

ISBN 978-5-4461-1952-3

Russian edition published under license by No Starch Press Inc.

© Перевод на русский язык, ООО «Прогресс книга», 2022

© Издание на русском языке, оформление, ООО «Прогресс книга», 2022

© Серия «Библиотека программиста», 2022

Краткое содержание

Об авторе	18
О научном редакторе	19
Благодарности	20
От издательства	21
Предисловие	22
Введение	23
Глава 1. Подготовка к работе	28

ЧАСТЬ I ОСНОВЫ СЕТЕВЫХ ТЕХНОЛОГИЙ

Глава 2. Перехват трафика с помощью ARP-спуфинга	44
Глава 3. Анализ перехваченного трафика	57
Глава 4. Создание TCP-оболочек и ботнетов	73

ЧАСТЬ II КРИПТОГРАФИЯ

Глава 5. Криптография и программы-вымогатели	92
Глава 6. Протокол TLS и алгоритм Диффи — Хеллмана	116

ЧАСТЬ III СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Глава 7. Фишинг и дипфейки	140
Глава 8. Сбор информации	159

**ЧАСТЬ IV
ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ**

Глава 9. Поиск уязвимостей нулевого дня188
Глава 10. Создание троянов217
Глава 11. Создание и установка руткитов в ОС Linux253
Глава 12. Кража и взлом паролей278
Глава 13. Эксплуатация уязвимостей межсайтового скриптинга304

**ЧАСТЬ V
ЗАХВАТ КОНТРОЛЯ НАД СЕТЬЮ**

Глава 14. Проброс трафика и повышение привилегий326
Глава 15. Перемещение по корпоративной сети Windows344
Глава 16. Дальнейшие шаги365

Оглавление

Об авторе	18
О научном редакторе	19
Благодарности	20
От издательства	21
Предисловие	22
Введение	23
Зачем нужна эта книга	23
Установка Python	24
О чем пойдет речь в книге	24
Часть I. Основы сетевых технологий	25
Часть II. Криптография	25
Часть III. Социальная инженерия	26
Часть IV. Эксплуатация уязвимостей	26
Часть V. Захват контроля над сетью	27
Глава 1. Подготовка к работе	28
Виртуальная лаборатория	28
Настройка VirtualBox	29
Настройка pfSense	30
Настройка внутренней сети	32
Конфигурирование параметров pfSense	33
Настройка Metasploitable	35
Настройка Kali Linux	37
Настройка Ubuntu Linux Desktop	38

Ваш первый взлом: эксплуатация бэкдора в Metasploitable	39
Получение IP-адреса сервера Metasploitable	40
Использование бэкдора для получения доступа	41

ЧАСТЬ I ОСНОВЫ СЕТЕВЫХ ТЕХНОЛОГИЙ

Глава 2. Перехват трафика с помощью ARP-спуфинга	44
Передача данных в интернете	44
Пакеты	44
MAC-адреса	45
IP-адреса	46
ARP-таблицы	47
Атака методом ARP-спуфинга	48
Выполнение ARP-спуфинга	49
Обнаружение признаков ARP-спуфинга	53
Упражнения	55
Проверка ARP-таблиц	55
Написание ARP-спуфера на языке Python	55
MAC-флудинг	56
Глава 3. Анализ перехваченного трафика	57
Пакеты и стек интернет-протоколов	57
Пятиуровневый стек интернет-протоколов	60
Просмотр пакетов с помощью Wireshark	63
Анализ пакетов, собранных межсетевым экраном	69
Перехват трафика на порте 80	69
Упражнения	71
pfSense	71
Анализ пакетов в Wireshark	72
Глава 4. Создание TCP-оболочек и ботнетов	73
Сокеты и взаимодействие процессов	73
TCP-рукопожатия	74
Обратная TCP-оболочка	76

Получение доступа к компьютеру жертвы	78
Сканирование открытых портов	79
Эксплуатация уязвимого сервиса	80
Написание клиента обратной оболочки	81
Написание TCP-сервера, прослушивающего клиентские соединения	83
Загрузка обратной оболочки на сервер Metasploitable	84
Ботнеты	85
Упражнения	87
Мультиклиентный бот-сервер	88
SYN-сканирование	89
Выявление признаков XMas-сканирования	90

ЧАСТЬ II

КРИПТОГРАФИЯ

Глава 5. Криптография и программы-вымогатели	92
Шифрование	92
Одноразовый блокнот	93
Генераторы псевдослучайных последовательностей	97
Ненадежные режимы работы алгоритмов блочного шифрования	98
Надежные режимы работы алгоритмов блочного шифрования	99
Шифрование и расшифровка файла	101
Шифрование электронной почты	102
Криптографическая система с открытым ключом	103
Теория Ривеста — Шамира — Адлемана	103
Математические основы алгоритма RSA	104
Шифрование файла с помощью алгоритма RSA	106
Оптимальное асимметричное шифрование с дополнением	108
Написание программы-вымогателя	109
Упражнения	112
Сервер для программы-вымогателя	112
Расширение возможностей программы-вымогателя	113
Нерасшифрованные послания	114

Глава 6. Протокол TLS и алгоритм Диффи — Хеллмана	116
Протокол защиты транспортного уровня	117
Проверка подлинности сообщений	118
Центры сертификации и подписи	119
Центры сертификации	120
Использование алгоритма Диффи — Хеллмана для вычисления общего ключа	122
Этап 1. Генерация общих параметров	123
Этап 2. Создание открытого и закрытого ключей	124
Почему хакер не может вычислить закрытый ключ	125
Этап 3. Обмен открытыми ключами и попсе-числами	126
Этап 4. Вычисление общего секретного ключа	127
Этап 5. Формирование ключа	128
Атака на протокол Диффи — Хеллмана	129
Протокол Диффи — Хеллмана на эллиптических кривых	129
Математика эллиптических кривых	130
Алгоритм удвоения и сложения	131
Почему хакер не может использовать G_{xy} и a_{xy} для вычисления закрытого ключа A	132
Написание TLS-сокетов	133
Защищенный клиентский сокет	133
Защищенный серверный сокет	135
Атака типа SSL stripping и обход HSTS	136
Упражнение: добавление шифрования на сервер для программы-вымогателя	137

ЧАСТЬ III СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Глава 7. Фишинг и дипфейки	140
Изощренная атака с применением социальной инженерии	141
Подделка электронных писем	141
Поиск данных почтового сервера в DNS	142
Обмен данными по протоколу SMTP	143
Написание спуффера электронной почты	145
SMTPS-спуфинг электронной почты	147

Подделка сайтов	149
Создание дипфейков	151
Получение доступа к Google Colab	152
Импорт моделей машинного обучения	153
Упражнения	156
Клонирование голоса	156
Масштабный фишинг	156
Аудит SMTP	157
Глава 8. Сбор информации	159
Анализ связей	159
Maltego	161
Утекшие базы данных	164
Угон SIM-карты	166
Google Dorking	167
Сканирование всей сети интернет	168
Masscan	168
Shodan	172
Ограничения, связанные с IPv6 и NAT	174
Интернет-протокол версии 6 (IPv6)	174
Технология NAT	175
Базы данных уязвимостей	176
Сканеры уязвимостей	179
Упражнения	182
Сканирование с помощью nmap	182
Discover	183
Создание OSINT-инструмента	185

ЧАСТЬ IV ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ

Глава 9. Поиск уязвимостей нулевого дня	188
Эксплуатация уязвимости Heartbleed в OpenSSL	188
Создание эксплойта	189
Начало программы	190
Написание сообщения Client Hello	191

Чтение ответа сервера	193
Создание вредоносного Heartbeat-запроса	195
Чтение утекших из памяти данных	196
Написание функции эксплойта	196
Собираем все вместе	197
Фаззинг	197
Упрощенный пример	198
Написание фаззера	199
American Fuzzy Lop	200
Символьное выполнение	204
Символьное выполнение тестовой программы	205
Пределы возможностей символьного выполнения	206
Динамическое символьное выполнение	207
Использование DSE для взлома пароля	210
Создание исполняемого двоичного файла	210
Установка и запуск Angr	211
Программа Angr	212
Упражнения	214
Захват флага с помощью Angr	214
Фаззинг веб-протоколов	214
Фаззинг программ с открытым исходным кодом	215
Реализуйте собственный механизм конколического выполнения	216
Глава 10. Создание троянов	217
Воссоздание программы Drovorub с помощью Metasploit	218
Создание сервера злоумышленника	219
Создание клиента жертвы	220
Загрузка импланта	221
Использование агента злоумышленника	222
Зачем использовать модуль ядра	222
Скрытие импланта в легитимном файле	223
Создание трояна	223
Размещение трояна	227

Скачивание зараженного файла	228
Управление имплантом	230
Обход антивируса с помощью кодировщиков	231
Кодировщик Base64	232
Написание модуля Metasploit	234
Кодировщик Shikata Ga Nai	236
Создание трояна для ОС Windows	237
Соккрытие трояна в Minesweeper	237
Соккрытие трояна в документе Word (или в другом безобидном файле)	238
Создание трояна для ОС Android	240
Разбор APK-файла для изучения импланта	240
Сборка и подписывание APK-файла	243
Тестирование трояна для ОС Android	244
Упражнения	248
Evil-Droid	248
Создание импланта на языке Python	250
Обфускация импланта	251
Создание исполняемого файла для конкретной платформы	252
Глава 11. Создание и установка руткитов в ОС Linux	253
Написание модуля ядра Linux	254
Резервное копирование виртуальной машины Kali Linux	254
Написание кода	255
Компиляция и запуск модуля ядра	256
Изменение системных вызовов	258
Принцип работы системных вызовов	259
Перехват системных вызовов	262
Перехват системного вызова Shutdown	262
Соккрытие файлов	267
Структура linux_dirent	267
Написание кода перехвата	268
Использование инструмента Armitage для эксплуатации хоста и установки руткита	269
Сканирование сети	271

Эксплуатация хоста	273
Установка руткита	274
Упражнения	274
Кейлоггер	274
Скрывающийся модуль	277
Глава 12. Кража и взлом паролей	278
SQL-инъекция	278
Кража паролей из базы данных сайта	280
Перечисление доступных на веб-сервере файлов	281
Проведение SQL-инъекции	282
Создание инструмента для выполнения SQL-инъекции	283
HTTP-запросы	284
Написание программы для внедрения кода	286
Использование SQLMap	288
Хеширование паролей	290
Анатомия хеш-функции MD5	291
Взлом хешей	294
Подсаливание хешей с помощью popse-числа	295
Создание инструмента для взлома соленых хешей	296
Популярные инструменты для взлома хешей и полного перебора	297
John the Ripper	297
Hashcat	297
Hydra	299
Упражнения	300
NoSQL-инъекция	300
Перебор учетных данных методом грубой силы	301
Burp Suite	302
Глава 13. Эксплуатация уязвимостей межсайтового скриптинга	304
Межсайтовый скриптинг	304
Как код JavaScript может быть вредоносным	306
Хранимые XSS-атаки	309
Отраженные XSS-атаки	311

Обнаружение уязвимостей с помощью OWASP Zed Attack Proxy	312
Использование полезных нагрузок инструмента BeEF	315
Внедрение скрипта BeEF Hook	315
Реализация атаки с помощью методов социальной инженерии	316
Переходим от браузера к компьютеру	318
Эксплуатация старой версии браузера Chrome	319
Установка руткитов путем эксплуатации уязвимостей сайтов	320
Упражнение: поиск ошибок в программе Bug Bounty	323

ЧАСТЬ V

ЗАХВАТ КОНТРОЛЯ НАД СЕТЬЮ

Глава 14. Проброс трафика и повышение привилегий	326
Проброс трафика с помощью устройства с двойной привязкой	327
Настройка устройства с двойной привязкой	327
Подключение машины к частной сети	330
Проброс трафика с помощью Metasploit	331
Создание атакующего прокси-сервера	335
Извлечение хешей паролей из памяти машины Linux	336
Где система Linux хранит имена пользователей и пароли	336
Уязвимость Dirty COW и атака на повышение привилегий	339
Упражнения	342
Настройка NAT на устройстве с двойной привязкой	342
Материалы по теме повышения привилегий в ОС Windows	343
Глава 15. Перемещение по корпоративной сети Windows	344
Создание виртуальной лаборатории Windows	345
Извлечение хешей паролей с помощью mimikatz	345
Передача хеша по протоколу NT LAN Manager	348
Исследование корпоративной сети Windows	350
Атака на сервис DNS	351
Атака на сервисы Active Directory и LDAP	353
Создание клиента для генерации LDAP-запросов	355
Использование инструментов SharpHound и Bloodhound для LDAP-перечисления	358

Атака на протокол Kerberos	359
Атака типа Pass-the-Ticket	362
Атаки типа Golden Ticket и DC Sync	363
Упражнение: Kerberoasting	364
Глава 16. Дальнейшие шаги	365
Создание укрепленной хакерской среды	365
Сохранение анонимности с помощью Tor и Tails	366
Настройка виртуального выделенного сервера	368
Настройка SSH-ключей	369
Установка хакерских инструментов	370
Укрепление сервера	372
Аудит укрепленного сервера	374
Дополнительные темы	375
Программно-определяемые радиосистемы	375
Атака на инфраструктуру сотовой связи	376
Воздушный зазор	376
Обратная разработка	377
Физические инструменты для взлома систем	377
Криминалистика	378
Взлом промышленных систем	378
Квантовые вычисления	379
Вступайте в сообщество	379