

ДЖОН ЭРИКСОН

ХАКИНГ

ИСКУССТВО ЭКСПЛОЙТА

2-е ИЗДАНИЕ



Санкт-Петербург • Москва • Екатеринбург • Воронеж
Нижний Новгород • Ростов-на-Дону • Самара • Минск

2020

ББК 32.973.23-018-07
УДК 004.56.53
Э77

Эриксон Д.

Э77 Хакинг: искусство эксплойта. 2-е изд. — СПб.: Питер, 2020. — 496 с.: ил. — (Серия «Библиотека программиста»).

ISBN 978-5-4461-0712-4

Каждый программист по сути своей — хакер. Ведь первоначально хакингом называли поиск искусного и неочевидного решения. Понимание принципов программирования помогает находить уязвимости, а навыки обнаружения уязвимостей помогают создавать программы, поэтому многие хакеры занимаются тем и другим одновременно. Интересные нестандартные ходы есть как в техниках написания элегантных программ, так и в техниках поиска слабых мест.

С чего начать? Чтобы перезаписывать память с помощью переполнения буфера, получать доступ к удаленному серверу и перехватывать соединения вам предстоит программировать на Си и ассемблере, использовать шелл-код и регистры процессора, познакомиться с сетевыми взаимодействиями и шифрованием и многое другое.

Как бы мы ни хотели верить в чудо, программное обеспечение и компьютерные сети, от которых зависит наша повседневная жизнь, обладают уязвимостями.

Мир без хакеров — это мир без любопытства и новаторских решений. (Джон Эриксон)

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 978-1593271442 англ.

© 2008 by Jon Erickson.
Hacking: The Art of Exploitation, 2nd Edition, ISBN 978-1-59327-114-2,
published by No Starch Press.

ISBN 978-5-4461-0712-4

© Перевод на русский язык ООО Издательство «Питер», 2020
© Издание на русском языке, оформление ООО Издательство «Питер»,
2020
© Серия «Библиотека программиста», 2020

ОГЛАВЛЕНИЕ

Предисловие	10
Благодарности	11
От издательства	11
0x100 Введение	12
0x200 Программирование	17
0x210 Что такое программирование?.....	18
0x220 Псевдокод	19
0x230 Управляющие структуры	20
0x231 Конструкция if-then-else	20
0x232 Циклы while/until	22
0x233 Цикл for	22
0x240 Основные концепции программирования	24
0x241 Переменные.....	24
0x242 Арифметические операторы.....	25
0x243 Операторы сравнения	26
0x244 Функции.....	28
0x250 Практическое применение.....	32
0x251 Расширяем горизонты	33
0x252 Процессор x86.....	36
0x253 Язык ассемблера.....	38
0x260 Назад к основам.....	52
0x261 Строки	52
0x262 Базовые типы signed, unsigned, long и short	56
0x263 Указатели	58
0x264 Форматирующие строки	62
0x265 Приведение типов.....	66
0x266 Аргументы командной строки.....	73
0x267 Область видимости переменных.....	77

0x270	Сегментация памяти.....	85
0x271	Сегменты памяти в языке С.....	92
0x272	Работа с кучей.....	94
0x273	Функция malloc() с контролем ошибок.....	96
0x280	Дополнение к основам.....	98
0x281	Доступ к файлам.....	98
0x282	Права доступа к файлам.....	103
0x283	Идентификаторы пользователей.....	105
0x284	Структуры.....	114
0x285	Указатели на функции.....	117
0x286	Псевдослучайные числа.....	118
0x287	Азартные игры.....	120
0x300	Эксплуатация уязвимостей.....	133
0x310	Общий принцип эксплуатации уязвимостей.....	136
0x320	Переполнение буфера.....	136
0x321	Уязвимости переполнения буфера через стек.....	140
0x330	Эксперименты с оболочкой BASH.....	152
0x331	Работа с окружением.....	161
0x340	Переполнение в других сегментах памяти.....	169
0x341	Стандартное переполнение в куче.....	170
0x342	Перезапись указателя на функцию.....	176
0x350	Форматирующие строки.....	187
0x351	Параметры форматирования.....	187
0x352	Уязвимость строк форматирования.....	190
0x353	Чтение из произвольного места в памяти.....	192
0x354	Запись в произвольное место в памяти.....	193
0x355	Прямой доступ к параметрам.....	201
0x356	Запись значений типа short.....	203
0x357	Обход через секцию .ctors.....	205
0x358	Еще одна уязвимость в программе notesearch.....	210
0x359	Перезапись глобальной таблицы смещений.....	212
0x400	Сетевые взаимодействия.....	216
0x410	Сетевая модель OSI.....	216
0x420	Сокеты.....	219
0x421	Функции сокетов.....	220
0x422	Адреса сокетов.....	222
0x423	Сетевой порядок байтов.....	224
0x424	Преобразование интернет-адресов.....	224
0x425	Пример простого сервера.....	225

0x426	Пример с веб-клиентом.....	229
0x427	Маленький веб-сервер.....	235
0x430	Спускаемся к нижним слоям.....	239
0x431	Канальный уровень.....	240
0x432	Сетевой уровень.....	241
0x433	Транспортный уровень.....	243
0x440	Анализ сетевого трафика.....	246
0x441	Программа для перехвата raw-сокетов.....	248
0x442	Библиотека libpcap.....	250
0x443	Расшифровка уровней.....	253
0x444	Активный сниффинг.....	262
0x450	Отказ в обслуживании.....	275
0x451	SYN-флуд.....	275
0x452	Атака с помощью пингов смерти.....	280
0x453	Атака teardrop.....	280
0x454	Наводнение запросами.....	280
0x455	Атака с усилением.....	281
0x456	Распределенная DoS-атака.....	282
0x460	Перехват TCP/IP.....	282
0x461	Атака с добавлением бита RST.....	283
0x462	Дополнительные варианты перехвата.....	288
0x470	Сканирование портов.....	288
0x471	Скрытое SYN-сканирование.....	289
0x472	Сканирование с помощью техник FIN, X-mas и Null.....	289
0x473	Фальшивые адреса.....	290
0x474	Метод idle scan.....	290
0x475	Превентивная защита.....	292
0x480	Давайте взломаем что-нибудь.....	298
0x481	Анализ с помощью GDB.....	299
0x482	Почти успех.....	302
0x483	Шелл-код, привязывающий к порту.....	305
0x500	Шелл-код.....	308
0x510	Сравнение ассемблера и С.....	308
0x511	Системные вызовы Linux на языке ассемблера.....	311
0x520	Путь к шелл-коду.....	314
0x521	Инструкции ассемблера для стека.....	314
0x522	Использование GDB.....	317
0x523	Удаление нулевых байтов.....	318
0x530	Код запуска оболочки.....	323
0x531	Вопрос привилегий.....	328
0x532	Дополнительная оптимизация.....	330

0x540	Шелл-код, привязывающий к порту.....	332
0x541	Дублирование стандартных файловых дескрипторов.....	337
0x542	Управляющие структуры ветвлений.....	339
0x550	Шелл-код с обратным подключением.....	344
0x600	Меры противодействия.....	350
0x610	Средства обнаружения атак.....	351
0x620	Системные демоны.....	352
0x621	Обзор сигналов.....	353
0x622	Демон tinysweb.....	355
0x630	Инструментарий.....	360
0x631	Инструмент для эксплуатации уязвимости демона tinyswebd.....	360
0x640	Файлы журналов.....	366
0x641	Затеряться в толпе.....	366
0x650	Не видя очевидного.....	368
0x651	Пошаговая инструкция.....	369
0x652	Функционирование демона.....	373
0x653	Дочерний процесс.....	379
0x660	Усиленная маскировка.....	381
0x661	Подделка регистрируемого IP-адреса.....	381
0x662	Остаться незарегистрированным.....	386
0x670	Инфраструктура в целом.....	389
0x671	Повторное использование сокетов.....	389
0x680	Контрабанда вредоносного кода.....	394
0x681	Шифрование строк.....	394
0x682	Как скрыть дорожку.....	397
0x690	Ограничения буфера.....	398
0x691	Полиморфный шелл-код из отображаемых символов ASCII.....	401
0x6a0	Усиление противодействия.....	412
0x6b0	Неисполняемый стек.....	413
0x6b1	Атака возврата в библиотеку.....	413
0x6b2	Возврат в функцию system().....	413
0x6c0	Рандомизация стека.....	416
0x6c1	Анализ с помощью BASH и GDB.....	417
0x6c2	Возвращение из библиотеки linux-gate.....	421
0x6c3	Практическое применение знаний.....	425
0x6c4	Первая попытка.....	425
0x6c5	Уменьшаем риски.....	427

0x700	Криптология.....	430
0x710	Теория информации.....	431
0x711	Безусловная стойкость.....	431
0x712	Одноразовые блокноты.....	431
0x713	Квантовое распределение ключей.....	432
0x714	Вычислительная стойкость.....	433
0x720	Время работы алгоритма.....	434
0x721	Асимптотическая нотация.....	435
0x730	Симметричное шифрование.....	435
0x731	Алгоритм Гровера.....	437
0x740	Асимметричное шифрование.....	437
0x741	Алгоритм RSA.....	438
0x742	Алгоритм Шора.....	442
0x750	Гибридные шифры.....	443
0x751	Атака посредника.....	444
0x752	Разница цифровых отпечатков узлов в протоколе SSH.....	448
0x753	Нечеткие отпечатки.....	452
0x760	Взлом паролей.....	456
0x761	Перебор по словарю.....	458
0x762	Атаки с полным перебором.....	461
0x763	Поисковая таблица хэшей.....	462
0x764	Матрица вероятности паролей.....	463
0x770	Шифрование в протоколе беспроводной связи 802.11b.....	473
0x771	Протокол Wired Equivalent Privacy.....	473
0x772	Потоковый шифр RC4.....	475
0x780	Атаки на WEP.....	476
0x781	Полный перебор в автономном режиме.....	476
0x782	Повторное использование потока битов ключа.....	477
0x783	Дешифровка по словарным таблицам IV.....	478
0x784	Переадресация IP.....	478
0x785	Атака Флурера, Мантина, Шамира.....	480
0x800	Заключение.....	490
0x810	Ссылки.....	491
0x820	Источники.....	492