

УДК 004.382
ББК 32.973.018
Ф73

Флоу С.

Ф73 Занимайся хакингом как невидимка / пер. с англ. В. С. Яценкова. – М.: ДМК Пресс, 2023. – 272 с.: ил.

ISBN 978-5-97060-977-4

Эта книга позволит вам примерить на себя роль хакера и атаковать вымышленную консалтинговую фирму Gretch Politico, чтобы на ее примере изучить стратегии и методы опытных взломщиков. Вы узнаете о том, как построить надежную хакерскую инфраструктуру, гарантирующую анонимность в интернете, рассмотрите эффективные приемы разведки, разработаете инструменты взлома с нуля и освоите низкоуровневые функции обычных систем.

Независимо от того, являетесь ли вы профессионалом в области безопасности или просто энтузиастом, это практическое руководство поможет вам научиться проводить реальные хакерские атаки и распознавать скрытые уязвимости облачных технологий.

УДК 004.382
ББК 32.973.018

Title of English-language original: *How to Hack Like a Ghost: Breaching the Cloud*, ISBN 9781718501263, published by No Starch Press Inc. 245 8th Street, San Francisco, California United States 94103. The Russian-Language 1st edition Copyright © 2022 by DMK Press Publishing under license by No Starch Press Inc. All rights reserved.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

ISBN 978-1-7185-0126-3 (англ.)
ISBN 978-5-97060-977-4 (рус.)

© Sparc Flow, 2021
© Перевод, издание, оформление, ДМК Пресс, 2022

СОДЕРЖАНИЕ

От издательства	10
Об авторе	11
О техническом обозревателе	11
Благодарности	12
Введение	13

ЧАСТЬ I ПОЙМАЙ МЕНЯ, ЕСЛИ СМОЖЕШЬ 18

1

Станьте анонимным в сети	19
VPN и его недостатки	20
Физическое местоположение	21
Рабочий ноутбук	22
Опорные серверы	23
Инфраструктура атаки	25
Дополнительные ресурсы	26

2

Сервер управления и контроля (C2)	27
Родословная C2	27
В поисках нового C2	28
Дополнительные ресурсы	36

3

Да будет инфраструктура!	37
Устаревший метод настройки	37
Контейнеры и виртуализация	39
Пространства имен	41
Файловая система UFS	44
Cgroups	47

6 Содержание

Маскировка IP-адресов	49
Автоматизация настройки сервера	50
Настройка сервера	55
Запуск сервера в работу	58
Дополнительные ресурсы	59

ЧАСТЬ II ЗА РАБОТУ!..... 61

4

Правильная атака в киберпространстве 62

Знакомство с Gretsch Politico.....	62
Поиск скрытых отношений	64
Просеивание GitHub	66
Извлечение веб-доменов	71
Информация из сертификатов	71
Поиск в интернете.....	73
Исследование используемой веб-инфраструктуры.....	75
Дополнительные ресурсы	76

5

Поиск уязвимостей..... 77

Практика – залог совершенства.....	77
Выявление скрытых доменов.....	78
Изучение URL-адресов S3.....	81
Безопасность бакета S3	82
Изучение бакетов	84
Поиск веб-приложения	87
Перехват с помощью WebSocket	89
Подделка запроса на стороне сервера	93
Изучение метаданных.....	93
Маленький грязный секрет API метаданных.....	95
AWS IAM	101
Изучение списка ключей	105
Дополнительные ресурсы	105

ЧАСТЬ III ПОЛНОЕ ПОГРУЖЕНИЕ107

6

Проникновение108

Инъекция шаблона на стороне сервера	110
Поиск характерных признаков фреймворка	111
Выполнение произвольного кода.....	113
Подтверждение принадлежности сайта	116
Бакеты для контрабанды.....	117
Качественный бэкдор с использованием S3.....	120

Создание агента	121
Создание оператора	123
Попытка вырваться на свободу	125
Проверка привилегированного режима	126
Возможности Linux	127
Сокет Docker	129
Дополнительные ресурсы	131

7

За кулисами	132
Обзор Kubernetes	133
Знакомство с подами	134
Балансировка трафика	139
Открытие приложения миру	140
Что у Kubernetes под капотом?	141
Дополнительные ресурсы	145

8

Побег из Kubernetes	147
Система RBAC в Kubernetes	148
Разведка, второй заход	151
Взлом хранилищ данных	156
Исследование API	159
Злоупотребление привилегиями роли IAM	163
Злоупотребление привилегиями учетной записи службы	164
Проникновение в базу данных	165
Redis и торги в реальном времени	168
Десериализация	170
Отравление кеша	172
Повышение привилегий Kubernetes	177
Дополнительные ресурсы	181

9

Стабильный доступ к командной оболочке	183
Стабильный доступ	186
Скрытый бэкдор	191
Дополнительные ресурсы	194

ЧАСТЬ IV ВРАГ ВНУТРИ	195
-----------------------------------	-----

10

Враг внутри	196
Путь к апофеозу	196
Захват инструментов автоматизации	202

8 Содержание

Jenkins Всемогущий.....	202
Адская кухня.....	204
Захват Lambda	212
Дополнительные ресурсы	216

11

Несмотря ни на что, мы продолжаем.....	217
Часовые AWS.....	217
Сохранение строжайшей конспирации	220
Приложение для запуска.....	221
Настройка Lambda	222
Настройка триггерного события.....	224
Заметаем следы.....	225
Восстановление доступа	226
Альтернативные (худшие) методы	227
Дополнительные ресурсы	228

12

Апофеоз.....	229
Сохранение доступа.....	232
Как устроен Spark.....	235
Вредоносный Spark	236
Захват Spark.....	241
Поиск необработанных данных	245
Кража обработанных данных	247
Повышение привилегий	248
Проникновение в Redshift	253
Дополнительные ресурсы	257

13

Финальная сцена.....	258
Взлом Google Workspace.....	259
Злоупотребление CloudTrail.....	263
Создание учетной записи суперадминистратора Google Workspace.....	265
Взгляд украдкой.....	267
Заключительное слово	269
Дополнительные ресурсы	269

Предметный указатель	270
-----------------------------------	------------