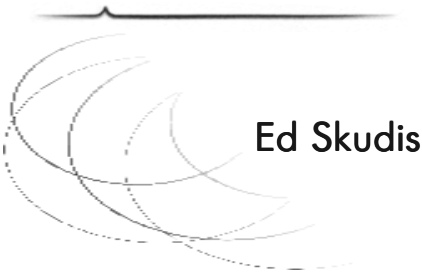
Эд Скудис

Противостояние хакерам

Пошаговое руководство по компьютерным атакам и эффективной защите

Counter Hack

A Step-by-Step Guide to
Computer Attacks and Effective Defenses



Ed Skudis



Prentice Hall PTR, Upper Saddle River, NJ 07458
www.phptr.com

Противостояние хакерам

Пошаговое руководство
по компьютерным атакам и эффективной защите



Эд Скудис

Серия
«Защита и администрирование»

ДМК Пресс
издательство
Москва

УДК 004.056.53
ББК 32.973.202
С46

Скудис Эд

С46 Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите: Пер. с англ. – М.: ДМК Пресс. – 512 с.: ил. (Серия «Защита и администрирование»).

ISBN 5-94074-170-3

Книга написана для системных и сетевых администраторов, профессионалов в области безопасности, а также для всех, кто хочет узнать о компьютерных атаках и способах их предотвращения. Стратегии атак и методы защиты, о которых здесь рассказывается, используются многими предприятиями и организациями, имеющими компьютерные сети.

Читая книгу, вы поймете, какими методами пользуется ваш противник при взломе: начиная от простого непрофессионального сканирования и заканчивая мощными атаками, которые финансируются криминальными группировками. Здесь детально рассматриваются наиболее часто встречающиеся стратегии реальных атак, а также даются советы, как защититься от возможных нападений.

Authorized translation from the English language edition, entitled COUNTER HACK: A STEP-BY-STEP GUIDE TO COMPUTER ATTACKS AND EFFECTIVE DEFENSES, 1st Edition by SKOUDIS, ED, published by Pearson Education, Inc, publishing as Prentice Hall, Copyright ©.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education, Inc.

RUSSIAN language edition published by DMK PUBLISHERS, Copyright ©.

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 владельца авторских прав.

Материал, изложенный в данной книге, многократно проверен. Но, поскольку вероятность технических ошибок все равно остается, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. В связи с этим издательство не несет ответственности за возможный ущерб любого вида, связанный с применением содержащихся здесь сведений.

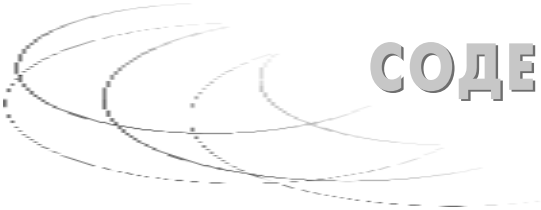
Все торговые знаки, упомянутые в настоящем издании, зарегистрированы. Случайное неправильное использование или пропуск торгового знака или названия его законного владельца не должно рассматриваться как нарушение прав собственности.

ISBN 0-13-033273-9 (англ.)

ISBN 5-94074-170-3 (рус.)

© Prentice Hall PTR
Prentice-Hall, Inc

© Перевод на русский язык,
оформление ДМК Пресс



СОДЕРЖАНИЕ

Предисловие 17

Вступление 18

Глава 1
Введение 22

Мир компьютеров и золотой век хакеров 23
Для чего нужна эта книга 24
Зачем рассказывать о специальных инструментах и стратегиях атак 25
Чем эта книга отличается от других 26
Не следует недооценивать противника 26
Навыки атакующего: от «сценаристов» до элиты 29
Кратко о терминологии и иконографии 30
Хакеры, взломщики и злоумышленники 30
Рисунки и сценарии 31
Имена разработчиков 32
Инструменты атак могут быть направлены и против вас 32
Создание лаборатории для исследования 33
Дополнительная информация 34
Структура книги 34
Современные технологии 34
Этапы атаки 35
Советы на будущее, выводы и справочная информация 36
Принятые обозначения 36
Резюме 36

Глава 2
Краткий обзор сети: все, что нужно знать о TCP/IP 38

Эталонная модель взаимодействия открытых систем и многоуровневое представление протоколов 39
TCP/IP в эталонной модели OSI 41
Понятие о TCP/IP 44
Протокол управления передачей (TCP) 45
Номера портов TCP 45
Контрольные биты TCP, трехэтапное квитирование и номера последовательности 48
Другие поля в TCP-заголовке 50
Протокол пользовательских датаграмм (UDP) 51
UDP менее надежен, чем TCP? 53
Internet-протокол (IP) и протокол управляющих сообщений Internet (ICMP) 53
Локальные сети и маршрутизаторы 54
IP-адреса 54
Сетевые маски 56
Фрагментация пакетов на IP-уровне 56
Другие составляющие IP-заголовка 57
Безопасность или ее отсутствие в традиционном протоколе IP 58
Протокол управляющих сообщений Internet (ICMP) 58
Другие вопросы, связанные с работой в сети 60
Маршрутизация пакетов 60
Трансляция сетевого адреса 61
Брандмауэры: регулировщики потока данных в сети и защитники 63
Персональные брандмауэры 70
Не забывайте о канальном и физическом уровнях! 72
Технология Ethernet – королева соединений 72
ARP, ARP, ARP! 73
Коммутаторы и концентраторы 74
Безопасность сетей 76
Безопасность на прикладном уровне 76

Протокол защищенных сокетов (SSL) ... 77
Безопасность на IP-уровне – IPSec ... 79
Выводы ... 83
Резюме ... 83

Глава 3
Краткий обзор UNIX: практически все, что нужно знать о UNIX ... 86

Понятие о UNIX ... 89
Архитектура ... 89
Структура файловой системы UNIX ... 89
Ядро и процессы ... 91
Автоматический вызов процессов init, inetd и cron ... 92
Процессы, запускаемые вручную ... 96
Взаимодействие с процессами ... 96
Учетные записи и группы ... 98
Файл /etc/passwd ... 98
Файл /etc/group ... 99
Root: права супервизора ... 100
Контроль привилегий – права в UNIX ... 100
SetUID-программы ... 103
Доверие UNIX ... 105
Системные журналы и аудит ... 105
Стандартные сетевые сервисы UNIX ... 107
Telnet: удаленный доступ с помощью командной строки ... 107
FTP: протокол передачи файлов ... 108
TFTP: простейший протокол передачи файлов ... 108
Web-серверы: HTTP ... 108
Электронная почта ... 108
R-команды ... 109
Сервер доменных имен ... 109
Сетевая файловая система (NFS) ... 109
Система X Window ... 110
Выводы ... 111
Резюме ... 111

Глава 4
Краткий обзор Windows NT/2000: все, что нужно знать о Windows ... 113

Краткая историческая справка ... 114
Основные концепции NT ... 114
Домены: объединение компьютеров ... 114
Общая зона – работа с удаленными ресурсами ... 115
Служебные пакеты и текущие исправления ... 115
Архитектура ... 116
Пользовательский режим ... 116
Форматы паролей в Windows NT ... 117
Режим ядра ... 118
Учетные записи и группы ... 120
Учетные записи ... 120
Группы ... 121
Контроль привилегий ... 123
Политики ... 124
Account Policy ... 124
Параметры User Properties ... 126
Доверие ... 127
Аудит ... 128
Контроль доступа и права доступа к объекту ... 129
Принадлежность ... 130
NTFS и права доступа в NTFS ... 130
Права доступа для общих папок ... 131
Локальный доступ ... 131
Слабость прав доступа по умолчанию и укрепление средств защиты ... 132
Безопасность сети ... 133
Ограничения базовых сетевых протоколов и API ... 133
Сервис удаленного доступа (RAS) ... 135
Windows 2000: добро пожаловать в новое тысячелетие ... 135
Что предлагает Windows 2000 ... 136
Вопросы безопасности в Windows 2000 ... 138
Архитектура: некоторые усовершенствования Windows NT ... 140

Учетные записи и группы ... 140
Контроль привилегий ... 141
Доверие Windows 2000 ... 143
Аудит ... 144
Контроль доступа к объекту ... 144
Безопасность сети ... 146
Выводы ... 146
Резюме ... 147

Глава 5
Этап 1: исследование ... 150

Простые методы исследования: социотехника, непосредственное вторжение и разгребание мусора ... 150
Социотехника ... 151
Непосредственное вторжение ... 153
Разгребание мусора ... 155
Обычный поиск в Web ... 156
Поиск на собственном сайте компании ... 156
Искусство применения поисковых систем ... 157
Просмотр сети Usenet ... 158
Способы защиты против Web-исследователей ... 159
Базы данных Whois: хранилище ценной информации ... 159
Исследование доменных имен .com, .net и .org ... 160
Исследование других доменных имен (не .com, .net и .org) ... 161
И что дальше? ... 163
Распределение IP-адресов через ARIN ... 165
Способы защиты против поиска в базах данных Whois ... 167
Доменная система имен ... 167
Опрос DNS-серверов ... 170
Способы защиты против DNS-исследования ... 172
Универсальные инструменты исследования ... 174
Sam Spade, универсальный клиентский инструмент исследования ... 174
Инструменты исследования на базе Web: порталы для исследований и атак ... 176
Выводы ... 178
Резюме ... 178

Глава 6
Этап 2: сканирование ... 180

War dialer ... 180
War dialer по сравнению с demon dialer ... 181
Опасное сочетание: модемы, программы для удаленного доступа и невежественные пользователи ... 181
Системные администраторы и незащищенные модемы ... 182
Бесплатные звонки по телефону ... 183
Телефонные номера для war dialer ... 184
Краткая история развития инструментов war dialer ... 184
THC-Scan 2.0 ... 185
Инструмент TBA от L0pht ... 188
Дальнейшие действия ... 188
Средства защиты против war dialer ... 190
Отображение сети ... 192
Поиск активных хостов ... 192
Трассировка маршрутов и транзитный узел ... 193
Cheops: отличный инструмент отображения сети и универсальный инструмент управления ... 196
Способы защиты против отображения сети ... 197
Сканирование открытых портов ... 197
Nmap: полнофункциональный инструмент сканирования ... 198
Способы защиты против сканирования портов ... 212
Опередите атакующих – первыми найдите открытые порты ... 213
Определение правил фильтрации брандмауэра с помощью Firewalk ... 215
Сканеры уязвимых мест ... 219
Список сканеров уязвимых мест ... 221
Nessus ... 222
Способы защиты против сканеров уязвимых мест ... 227
Обман системы обнаружения вторжений ... 228
Как работает сетевая IDS ... 229
Как обмануть сетевую IDS ... 229
Способы защиты против методов обмана IDS ... 238
Выводы ... 240
Резюме ... 240