Кристиан Барнс, Тони Боутс, Дональд Лойд, Эрик Уле,
Джеффри Посланс, Дэвид М. Зенджан, Нил О'Фаррел

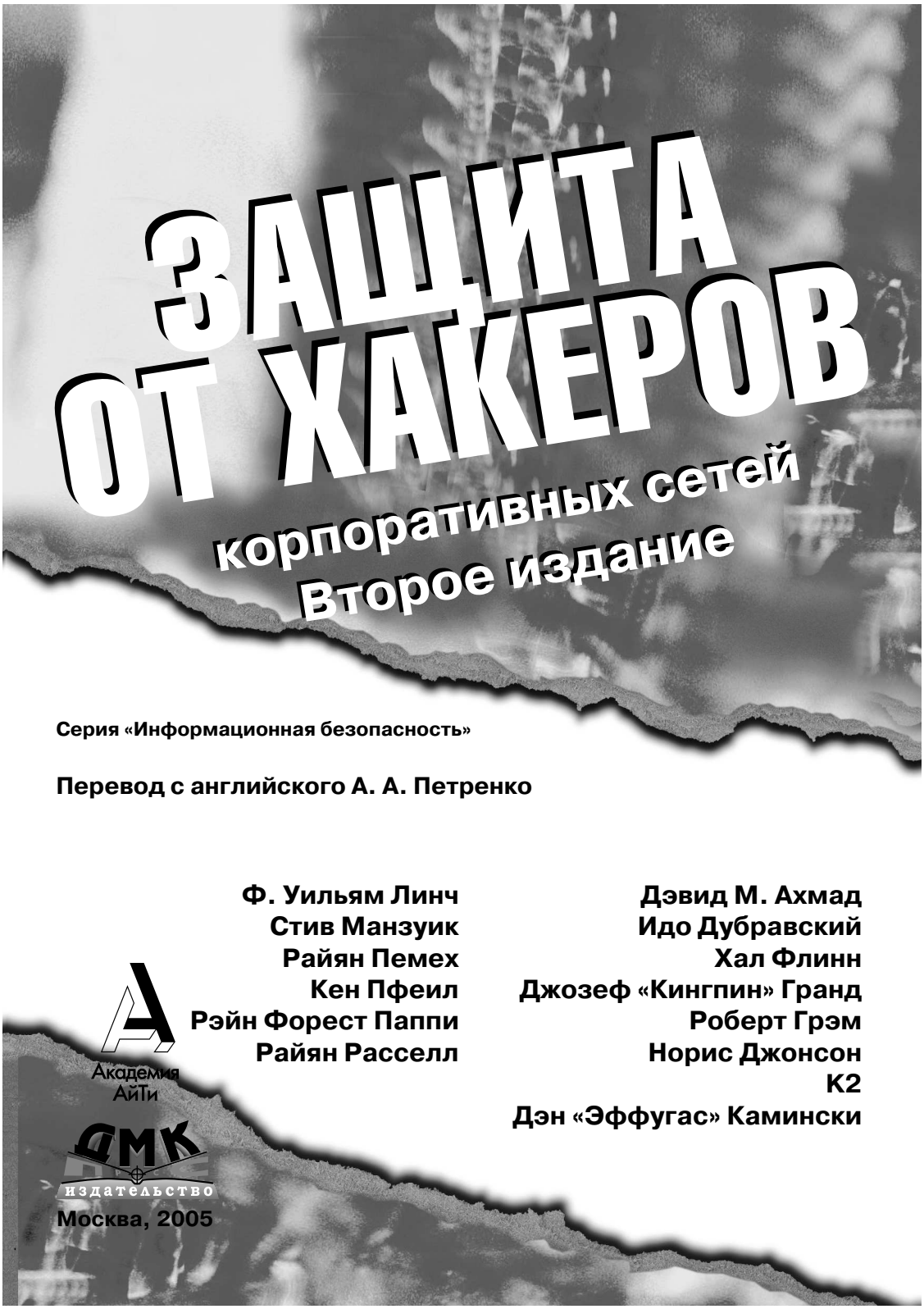
Защита от хакеров корпоративных сетей

Второе издание
(обновленное и дополненное новыми фактами,
ставшими известными по прошествии года после 1-го издания)

The Only Way to Stop a Hacker is to Think Like One

David R. Mirza Ahmad
Ido Dubrawsky
Hal Flynn
Joseph «Kingpin» Grand
Robert Graham
Norris L. Johnson, Jr.
K2
Dan «Effugas» Kaminsky
F. William Lynch
Steve W. Manzuik
Ryan Permeh
Ken Pfeil
Rain Forest Puppy
Ryan Russell Technical Editor

SYNGRESS®



ЗАЩИТА ОТ ХАКЕРОВ

корпоративных сетей
Второе издание

Серия «Информационная безопасность»

Перевод с английского А. А. Петренко

Ф. Уильям Линч
Стив Манзуик
Райян Пемех
Кен Пфеил
Рэйн Форест Паппи
Райян Расселл

Дэвид М. Ахмад
Идо Дубравский
Хал Флинн
Джозеф «Кингпин» Гранд
Роберт Грэм
Норис Джонсон
K2
Дэн «Эффугас» Камински

Академия АйТи

ДМК издательство

Москва, 2005

УДК 004.056
ББК 32.973.202
А95

А95 **Дэвид М. Ахмад, Идо Дубравский, Хал Флинн, Джозеф «Кингпин» Гранд, Роберт Грэм, Норис Джонсон, K2, Дэн «Эффугас» Камински, Ф. Уильям Линч, Стив Манзуик, Райян Пемех, Кен Пфеил, Рэйн Форест Паппи, Райян Расселл**
Защита от хакеров корпоративных сетей: Пер. с англ. А. А. Петренко. Второе издание. – М.: Компания АйТи; ДМК-Пресс, 2005. – 864 с.: ил. (Серия «Информационная безопасность»).

ISBN 5-98453-015-5

В книге рассматривается современный взгляд на хакерство, реинжиниринг и защиту информации. Авторы предлагают читателям список законов, которые определяют работу систем компьютерной безопасности и как можно применять эти законы в хакерских технологиях. Описываются типы атак и возможный потенциальный ущерб, который они могут нанести компьютерным системам. В книге широко представлены различные методы хакинга, такие как поиск различий, методы распознавания шифров, основы их вскрытия и схемы кодирования. Освящаются проблемы безопасности, возникающие в результате непредсказуемого ввода данных пользователем, методы использования машинно-ориентированного языка, возможности применения мониторинга сетевых коммуникаций, механизмы туннелирования для перехвата сетевого трафика. В книге представлены основные сведения о хакерстве аппаратных средств, вирусах, троянских конях, и червях. В этой книге читатель узнает о методах, которые в случае неправильного их применения приведут к нарушению законодательства и связанным с этим последствиям.

Лучшая защита – это нападение. Другими словами, единственный способ остановить хакера заключается в том, чтобы думать как он. Эти фразы олицетворяют подход, который, по мнению авторов, позволит наилучшим образом обеспечить безопасность информационной системы.

УДК 004.056
ББК 32.973.202

ISBN 1-928994-70-9 (англ.)
ISBN 5-98453-015-5 (АйТи)

Благодарности

Авторы книги хотели бы выразить свою признательность следующим людям, благодаря доброжелательности и поддержке которых стало возможным появление этой книги.

Ральфа Троупа (Ralph Troupe), Ронда Ст. Джона (Rhonda St. John) и коллектив Callisma за бесценную способность вникнуть в суть сложных задач проектирования, развертывания и поддержки сетей учреждений мирового класса.

Карена Кросса (Karen Cross), Ланса Тилфорда (Lance Tilford), Мегхана Канигхэма (Meaghan Cunningham), Кима Вилли (Kim Wylie), Гарри Кирчнера (Harry Kirchner), Кевина Вотела (Kevin Votel), Кента Андерсона (Kent Anderson), Фрида Яра (Frida Yara), Билла Геца (Bill Getz), Джона Мейеса (Jon Mayes), Джона Месджака (John Mesjak), Пега О'Доннелли (Peg O'Donnell), Сандру Паттерсона (Sandra Patterson), Бетти Редмонда (Betty Redmond), Роя Ремера (Roy Remer), Роя Шапиро (Ron Shapiro), Патрисию Келли (Patricia Kelly), Андреа Тетрика (Andrea Tetrick), Дженнифера Паскаля (Jennifer Pascal), Дуга Реила (Doug Reil) и Дэвида Дахла (David Dahl) из Западной группы издателей (Publishers Group West) за обмен потрясающим опытом в области маркетинга и экспертизу.

Жакью Шанахэм (Jacquie Shanahan) и ЭнХелен Линдехолм (AnnHelen Lindeholm) из Elsevier Science за придание нам уверенности в правоте нашего дела.

Анабел Дент (Annabel Dent) и Паулю Барри (Paul Barry) за все то, что они для нас сделали.

Дэвиду Букланду (David Buckland), Венди Вонгу (Wendi Wong), Мэри Чиенгу (Marie Chieng), Люси Чонгу (Lucy Chong), Лесли Лиму (Leslie Lim), Одри Гану (Audrey Gan) и Джозефу Чану (Joseph Chan) из Transquest Publishers за энтузиазм, с которым они просматривают наши книги.

Квон Шунг Джун (Kwon Sung June) из Acorn Publishing за поддержку.

Етан Аткин (Ethan Atkin) из Cranbury International за помощь в расширении программы Syngress.

Джекки Гросса (Jackie Gross), Гейла Войсея (Gayle Voycey), Алексия Пенни (Alexia Penny), Аник Робитэйла (Anik Robitaille), Крэга Сиддалла (Craig Siddall), Дарлен Моррою (Darlene Morrow), Иолану Миллер (Iolanda Miller),

Джан Макей (Jane Mackay) и Мэри Скелли (Marie Skelly) из Jackie Gross & Associates за помощь и энтузиазм, с которым они представляют книгу в Канаде.

Лоиса Фрасера (Lois Fraser), Конни Макменеми (Connie McMenemy), Шэннона Рассела (Shannon Russell) и других талантливых сотрудников из Jaguar Book Group за их помощь в распространении книг издательства в Канаде.

Слова благодарности от технического редактора Райана Рассела (Ryan Russel)

Я хотел бы посвятить свою работу своей замечательной жене и детям, не будь которых не было бы смысла работать над книгой. Я люблю тебя, Сара, с Днем святого Валентина тебя! Я также хотел бы поблагодарить Брайена Мартина (Brian Martin) за помощь при редактировании и, конечно, авторов, которые нашли время написать книгу. Особенно хочется поблагодарить авторов первого издания за их идеи по улучшению книги.

Райан Рассел

Содержание

От автора. Предисловие (версия 1.5) 23

Глава 1. Хакерские методы 27

Введение 28

Что понимают под «хакерскими методами» 28

Зачем применяют хакерские методы? 29

Обзор содержимого книги 30

Правовое обеспечение хакинга 33

Конспект 35

Часто задаваемые вопросы 35

Глава 2. Законы безопасности 37

Введение 38

Обзор законов безопасности 38

Закон 1. Невозможно обеспечить безопасность клиентской части 40

Закон 2. Нельзя организовать надежный обмен ключами шифрования без совместно используемой порции информации 42

Закон 3. От кода злоумышленника нельзя защититься на 100% 45

Закон 4. Всегда может быть создана новая сигнатура кода, которая не будет восприниматься как угроза 48

Закон 5. Межсетевые экраны не защищают на 100% от атаки злоумышленника 50

Социотехника 53

Нападение на незащищенные сервера 53

Прямое нападение на межсетевой экран 55

Бреши в системе безопасности клиентской части 55

Закон 6. От любой системы обнаружения атак можно уклониться 56

Закон 7. Тайна криптографических алгоритмов не гарантируется 58
Закон 8. Без ключа у вас не шифрование, а кодирование 61
Закон 9. Пароли не могут надежно храниться у клиента, если только они не зашифрованы другим паролем 63
Закон 10. Для того чтобы система начала претендовать на статус защищенной, она должна пройти независимый аудит безопасности 67
Закон 11. Безопасность нельзя обеспечить покровом тайны 69
Резюме 72
Конспект 73
Часто задаваемые вопросы 76

Глава 3. Классы атак 77

Введение 78
Обзор классов атак 78
Отказ в обслуживании 78
Утечка информации 89
Нарушения прав доступа к файлу 95
Дезинформация 98
Доступ к специальным файлам / базам данных 102
Удаленное выполнение программ 106
Расширение прав 108
Методы тестирования уязвимостей 111
Доказательство возможности нападения 111
Стандартные методы исследования 114
Резюме 126
Конспект 128
Часто задаваемые вопросы 129

Глава 4. Методология 131

Введение 132
Суть методологии исследования уязвимости 133

Анализ исходного текста программы 134
Анализ двоичного кода 136
Значение экспертизы исходного текста программы 138
Поиск функций, подверженных ошибкам 139
Технологии реинжиниринга 146
Дизассемблеры, декомпиляторы и отладчики 153
Тестирование методом «черного ящика» 158
Чипы 159
Резюме 161
Конспект 162
Часто задаваемые вопросы 163

Глава 5. Поиск различий 165

Введение 166
Суть поиска различий 166
Почему нужно знать о различиях файлов? 168
Просмотр исходного текста программы 169
Исследование инструментария поиска различий 176
Применение инструментария сравнения файлов 176
Работа с шестнадцатеричными редакторами 179
Использование инструментария мониторинга файловой системы 183
Другие инструментальные средства 188
Поиск неисправностей 191
Проблемы контрольных сумм и кэширования 191
Проблемы сжатия и шифрования 193
Резюме 195
Конспект 196
Часто задаваемые вопросы 198

Глава 6. Криптография 199

Введение 200
Концепции криптографии 200

Историческая справка 201
Типы криптосистем 201
Стандарты алгоритмов шифрования 204
Симметричные алгоритмы 204
Асимметричные алгоритмы 209
«Грубая сила» 212
Основы метода «грубой силы» 213
Применение метода «грубой силы» для расшифровки паролей 214
Неверное использование алгоритмов шифрования 218
Неверно организованный обмен ключами 219
Кэширование пароля по частям 221
Генерация длинного ключа из короткого пароля 222
Ошибки хранения частных или секретных ключей 222
Любительская криптография 225
Классификация зашифрованного текста 225
Моноалфавитные шифры 228
Другие способы скрытия информации 228
Резюме 236
Конспект 237
Часто задаваемые вопросы 239

Глава 7. Непредвиденные входные данные 241

Введение 242
Опасность непредвиденных входных данных 243
Поиск обусловленных непредвиденными входными данными уязвимостей 244
Локальные приложения и утилиты 244
Протокол HTTP и язык разметки HTML 245
Непредвиденные данные в запросах SQL 248
Аутентификация приложений 252
Маскировка непредвиденных данных 257