

Подробное руководство по защите Вашей сети

Эта книга, получившая признание как всеобъемлющее практическое руководство по защите информации, займет достойное место в вашей профессиональной библиотеке по безопасности. Бестселлер «Защита от хакеров корпоративных сетей» продемонстрирует Вам, что единственный способ остановить хакера — думать как он.

- 1 Законы безопасности**
Узнайте об авторских методиках исследования проблем безопасности и обнаружения брешей в защите при аудите или проектировании системы.
- 2 Семь категорий атак**
Убедитесь на наглядных примерах, как отказ в обслуживании, утечка информации, доступ к файловым системам и базам данных, дезинформация, удаленное выполнение кода и получение статуса привилегированного пользователя может принести вам реальные неприятности.
- 3 Предотвращение прослушивания**
Познакомьтесь, как сравнение программ, библиотек или файлов до или после выполнения некоторых действий может повлиять на данные в Вашей сети.
- 4 Стандартные алгоритмы шифрования**
Проверьте, насколько защищены ваши зашифрованные файлы и надежны пароли.
- 5 Последовательности уязвимостей**
Узнайте о новейших приемах хакеров.
- 6 Сессии пиратских подключений**
Прочтите о расширенном применении мониторинга сетевых коммуникаций и атаках типа «злоумышленник посередине» (man-in-the-middle).
- 7 Туннелирование сетевого трафика**
Познакомьтесь с механизмами создания враждебного сетевого окружения для перехвата сетевого трафика. OpenSSH как один из лучших современных пакетов для создания сквозных туннелей.
- 8 Защита Вашего оборудования**
Создание продуктов с встроенными механизмами защиты: сопротивление, доказательство вторжения, поиск уязвимостей, обнаружение и ответная реакция. один из лучших современных пакетов для создания сквозных туннелей.

ISBN 598453015-5



SYNGRESS®



www.dmk.ru
www.abook.ru



www.academy.it.ru
www.infobooks.ru



ЗАЩИТА ОТ ХАКЕРОВ КОРПОРАТИВНЫХ СЕТЕЙ



SYNGRESS®

SYNGRESS®

ЗАЩИТА ОТ ХАКЕРОВ

КОРПОРАТИВНЫХ СЕТЕЙ

**ВТОРОЕ
ИЗДАНИЕ**

**Единственный способ остановить
хакера — думать как он**

Ф. Уильям Линч
Стив Манзуик
Райян Пемех
Кен Пфеил
Рэйн Форест Паппи
Райян Расселл
Дэн «Эффугас» Камински

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



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
К2
Дэн «Эффугас» Камински



Академия
АйТи

СМК
издательство

Москва

УДК 004.056
ББК 32.973.202
А95

А95 Дэвид М. Ахмад, Идо Дубравский, Хал Флинн, Джозеф «Кингпин» Гранд, Роберт Грэм, Норис Джонсон, К2, 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. – 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. Освещаются 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

Original English language edition published by Singress Publishing, Inc. Copyright © by Singress Publishing, 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.

Материал, изложенный в данной книге, многократно проверен. Но поскольку вероятность технических ошибок все равно существует, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. В связи с этим издательство не несет ответственности за возможные ошибки, связанные с использованием книги.

ISBN 1-928994-70-9 (англ.) Copyright © by Singress Publishing, Inc.
ISBN 5-98453-015-5 (АйТи) © Перевод на русский язык. Компания АйТи
© Оформление, издание. ДМК-Пресс

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

8 Защита от хакеров корпоративных сетей

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

10 Защита от хакеров корпоративных сетей

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

Методы поиска и устранения уязвимостей, обусловленных непредвиденными входными данными	259
Тестирование методом «черного ящика»	259
Анализ исходных текстов программ	264
Контроль данных	265
Пропуск символов	265
Язык Perl	266
Язык разметки COLD Fusion	267
Технология ASP	267
Язык PHP	268
Защита запросов SQL	269
Удалять неверные данные или сообщить об ошибке?	270
Функции контроля непредвиденных данных	270
Подмена значений	271
Использование средств безопасности языков программирования для обработки непредвиденных данных	271
Язык Perl	272
Система программирования PHP	273
Язык разметки ColdFusion	274
Технология ASP	274
Система управления базами данных MySQL	275
Инструментарий обработки непредвиденных данных	276
Программа Web Sleuth	276
Программа CGIAudit	276
Инструментарий RATS	276
Сценарий Flawfinder	277
Сканер Retina	277
Программа Hailstorm	277
Программа Pudding	277
Резюме	279
Конспект	280
Часто задаваемые вопросы	281

12 Защита от хакеров корпоративных сетей

Глава 8. Переполнение буфера	283
Введение	284
Стек	284
Дамп стека	287
Разнообразие стеков	289
Стековый фрейм функции	290
Основные сведения	290
Передача параметров в функцию.	
Простой пример	291
Стековый фрейм и соглашения о вызове функций	295
Основы переполнения буфера	296
Простое неуправляемое переполнение: программа-пример	298
Пример программы, уязвимой к переполнению буфера	302
Программа, уязвимая к переполнению буфера	302
Программа переполнения буфера	305
Современные способы переполнения буфера	339
Фильтрация входных данных	339
Перезапись указателя функции в стеке	342
Переполнения области динамически распределяемой памяти	343
Новаторские принципы построения программного кода полезной нагрузки	346
Использование того, что у вас есть	347
Резюме	351
Конспект	352
Часто задаваемые вопросы	355
Глава 9. Ошибки форматирующей строки	357
Введение	358
Уязвимость форматирующей строки	361
Как и почему возникают ошибки форматирующей строки?	365