Медведовский И. Д., Семьянов П. В.,
Леонов Д. Г.

Атака на Internet

Издание второе, переработанное и дополненное

ДМК
издательство
Москва

Атака на Internet / Медведовский И. Д., Семьянов П. В., Леонов Д. Г. –
А92 2-е изд., перераб. и доп. – М.: ДМК. – 336 с.: ил.

ISBN 5-89818-036-2

Эта книга является одним из первых специализированных изданий, написанных отечественными авторами, которое посвящено обстоятельному анализу безопасности сети Internet. В книге предлагаются и подробно описываются механизмы реализации основных видов удаленных атак как на протоколы TCP/IP и инфраструктуру Сети, так и на многие популярные сетевые операционные системы и приложения.

Особое внимание авторы уделили причинам возникновения и успеха удаленных атак, а также их классификации. Были также рассмотрены основные способы и методы защиты от удаленных атак.

Издание предназначено для сетевых администраторов и пользователей Internet, администраторов безопасности, разработчиков систем защит, системных сетевых программистов, студентов и аспирантов вузов, а также для всех интересующихся вопросами нарушения и обеспечения информационной безопасности компьютерных сетей.

ISBN 5-89818-036-2 © ДМК, Москва

Медведовский Илья Давидович
Семьянов Павел Валентинович
Леонов Дмитрий Геннадьевич

Атака на Internet

Главный редактор *Захаров И. М.*
Научный редактор *Орлов А. В.*
Литературный редактор *Космачева Н. А.*
Верстка *Чувилин И. А.*
Дизайн обложки *Антонов А. И.*

Гарнитура «Петербург». Печать офсетная.
Усл. печ. л. 21. Тираж 3000. Заказ №

Отпечатано с готовых диапозитивов в ППП «Типография “Наука”»
121099, Москва, Шубинский пер., 6.

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.

Содержание

Предисловие ... 8

Часть I

Хакеры и кракеры ... 11

Глава 1

О хакерах и не только... ... 12

Основные понятия компьютерной безопасности ... 12

Особенности безопасности компьютерных сетей ... 14

Что такое хорошо и что такое плохо ... 14

Цели кракера ... 17

Сетевая информационная безопасность: мифы и реальность ... 18

Всемогущество хакеров ... 18

Защита банковских систем ... 19

Сетевые кракеры ... 20

Межсетевые экраны Firewall как панацея от всех угроз ... 22

Статьи Уголовного кодекса Российской Федерации, связанные с преступлениями в сфере компьютерной информации ... 22

Проблема 2000 года в свете информационной безопасности ... 24

Возможные проблемы в модулях ПСОИБ ... 25

Возможные последствия проблемы Y2K ... 28

Возможные пути решения обозначенных проблем ... 28

Информационная безопасность России и проблема Y2K ... 29

Глава 2

Социальная инженерия и ее применение ... 30

Классификация атак класса СИ ... 31

Краткое введение в психологию СИ ... 33

Примеры проникновения в систему ... 34

Социальная инженерия посредством сети Internet ... 38

Беседы через Internet ... 38

Электронная почта ... 39

Программа-пейджер ... 41

Возможности защиты от социальной инженерии ... 42

Тесты на проникновение ... 42
Осведомленность ... 44

Часть II
Протоколы ... 47

Глава 3
Удаленные атаки на распределенные вычислительные системы ... 48
Классификация угроз безопасности распределенных вычислительных систем ... 48
Модели механизмов реализации типовых угроз безопасности PBC ... 55
Понятие типовой угрозы безопасности ... 55
Графовая модель взаимодействия объектов PBC ... 55
Моделирование механизмов реализации типовых угроз безопасности PBC ... 59

Глава 4
Удаленные атаки на хосты Internet ... 76
Анализ сетевого трафика Internet ... 76
Ложный ARP-сервер в сети Internet ... 78
Ложный DNS-сервер в сети Internet ... 85
Перехват DNS-запроса ... 86
Направленный шторм ложных DNS-ответов на атакуемый хост ... 89
Перехват DNS-запроса или создание направленного шторма ложных DNS-ответов на DNS-сервер ... 92
Навязывание хосту ложного маршрута с использованием протокола ICMP ... 96
Немного о ICMP ... 98
Подмена одного из субъектов TCP-соединения в сети Internet ... 103
Предсказание начального значения идентификатора TCP-соединения ... 106
Недостатки идентификации абонентов TCP-соединения ... 110
Направленный шторм ложных TCP-запросов на создание соединения ... 120
Направленный шторм запросов на ОС Windows NT 4.0 ... 123
Направленный мини-шторм запросов на 21, 25, 80, 110 и 139 порты ... 125
Мифические удаленные атаки в сети Internet ... 128
Фрагментация IP как способ проникновения через Firewall ... 128
Превышение максимально возможного размера IP-пакета, или Ping Death ... 131

Атаки, использующие ошибки реализации сетевых служб ... 134
Атака Land ... 134
Атаки teardrop и bonk ... 135
Атака передачей широковещательного запроса от имени «жертвы» ... 137
Атака Windows-систем передачей пакетов TCP/IP на открытый порт ... 137

Глава 5
Методы удаленного сканирования портов ... 138
Методы открытого сканирования ... 143
Сканирование TCP SYN ... 143
Сканирование TCP FIN ... 143
Сканирование с использованием IP-фрагментации ... 143
Сканирование TAP IDENT ... 144
Методы «невидимого» анонимного сканирования ... 145
Скрытая атака по FTP ... 145
Сканирование с использованием «немого» хоста ... 146
Сканирование через proxy-сервер ... 148

Глава 6
Причины успеха удаленных атак ... 151
Причины успеха угроз безопасности РВС ... 151
Отсутствие выделенного канала связи ... 152
Недостаточные идентификация и аутентификация ... 152
Отсутствие контроля за виртуальными каналами связи ... 154
Отсутствие возможности контролировать маршрут сообщений ... 155
Отсутствие полной информации об объектах РВС ... 156
Отсутствие криптозащиты сообщений ... 157
Причины успеха удаленных атак в сети Internet ... 157
Отсутствие выделенного канала связи между объектами сети Internet ... 157
Недостаточные идентификация и аутентификация ... 158
Невозможность контроля за виртуальными каналами связи ... 159
Отсутствие возможности контроля за маршрутом сообщений ... 159
Отсутствие полной информации об объектах Internet ... 159
Отсутствие криптозащиты сообщений ... 159

Глава 7
Безопасные распределенные вычислительные системы ... 161
Выделенный канал связи ... 161
Виртуальный канал связи ... 164

Контроль за маршрутом сообщения ... 167
Контроль за виртуальными соединениями ... 169
Проектирование распределенной ВС ... 171

Глава 8
Как защититься от удаленных атак в сети Internet ... 173

Административные методы защиты
от удаленных атак в сети Internet ... 175
Защита от анализа сетевого трафика ... 175
Защита от ложного ARP-сервера ... 176
Защита от ложного DNS-сервера ... 176
Защита от навязывания ложного маршрута ... 178
Защита от отказа в обслуживании ... 178
Защита от подмены одной из сторон ... 179

Программно-аппаратные методы защиты
от удаленных атак ... 180
Методика Firewall ... 180
Программные методы защиты ... 183

Часть III
Операционные системы и приложения ... 187

Глава 9
Прошлое и настоящее сетевых операционных систем ... 188

Классификация пользователей и типовых сценариев атак в UNIX ... 190
Начало, или До червя ... 195
Технология переполнения буфера ... 196
Червь ... 203
Стратегии вируса ... 205
После червя ... 216
Подбор пароля ... 216
Типичные атаки ... 221
Атаки на доверие ... 224
Современная ситуация ... 228
Ошибка в демоне telnetd ... 228
Снова sendmail ... 230
Уязвимости в wu-ftpd ... 231
Проникновение с помощью innd ... 232
Причины существования уязвимостей в UNIX-системах ... 233
Windows NT ... 236

Классификация причин уязвимости Windows NT ... 238
Переполнения буфера в системных сервисах ... 241
Разделение ресурсов и анонимный пользователь ... 245
Протокол SMB в глобальных сетях ... 249
Процедуры идентификации и аутентификации ... 251
Как защитить свой хост ... 256
Средства автоматизированного контроля безопасности ... 259
Программа SATAN ... 260
Семейство программ SAFEsuite ... 264
Сетевой монитор RealSecure ... 266
Глава 10
Атака через WWW ... 269
Атака на клиента ... 269
Безопасность браузеров ... 270
Безопасность Java-приложений ... 271
Суровая действительность ... 278
Безопасность других клиентских приложений ... 288
Вирусы и «троянские» кони ... 290
Атака на Web-сервер ... 293
Безопасность стандартного серверного ПО ... 294
Безопасность CGI-приложений ... 304
Общие сведения ... 305
Распространенные ошибки ... 307
Создание безопасных CGI-приложений ... 313
Ошибки в известных CGI-скриптах ... 316
Использование серверных приложений для атака на клиента ... 320
Безопасность личной информации ... 321
Проблемы идентификации ... 322
Заключение ... 327
Перечень информационных ресурсов Internet ... 329
Использованная литература ... 330
Алфавитный указатель ... 332

Предисловие

Предыдущая книга «Атака через Internet» вызвала широкий отклик у наших читателей. За прошедшие два года с момента ее выхода постоянно меняющийся мир Internet преподнес всем нам много нового в такой интересной и чрезвычайно динамичной области, как информационная безопасность вычислительных сетей. Мы не могли остаться в стороне от этого процесса – удивительный мир информационных воздействий сильно притягивает к себе, а однажды вступив на этот путь, уже невозможно остановиться, так как очень интересно узнать, что же там, за горизонтом...

Прошло два года – до горизонта все еще далеко, следовательно, у нашей науки есть настоящее и будущее: «Я мыслю – значит, я существую». Мы не оговорились, безопасность сетей – это именно наука, только она столь тесно переплетена с практикой, что многие об этом иногда забывают. Надеемся, что созданный нами в этой книге «сплав» науки и практики не оставит равнодушными наших читателей, и они смогут почерпнуть для себя много нового и интересного.

О чем эта книга

О безопасности сети Internet, а если точнее – о той опасности, которая угрожает всем пользователям Сети. Главная цель авторов – показать, что Internet как величайшее информационное достижение человечества помимо очевидных достоинств обладает рядом существенных недостатков в системе безопасности. Основываясь на своих практических исследованиях безопасности Сети и анализе доступной информации, мы попытались как можно более подробно и точно описать те возможные удаленные информационные разрушающие воздействия (удаленные атаки), о которых ходят слухи и мифы в среде пользователей Internet и которые в любой момент могут пожаловать к вам в качестве незваных гостей. А для того, чтобы оказать им достойную встречу, необходимо знать основные типы возможных атак и понимать механизмы их реализации. Авторам хотелось бы надеяться, что наша цель – повышение уровня информированности специалистов и пользователей Internet о тех угрозах информационной безопасности, которые таит в себе Сеть, – все-таки будет достигнута!

Отличия этой книги от других изданий по безопасности Internet

Неординарность подхода состоит в том, что его основу составляет анализ алгоритмических и технических особенностей реализации Internet, используемых нарушителями безопасности Сети.

Именно с этой точки зрения авторы, подробно изучив механизмы реализации удаленных атак, рассматривают возможные способы защиты от них.

По нашему мнению, предлагаемый подход позволяет указать на причины недостатков Сети и, тем самым, сосредоточиться на мерах, которые должны быть приняты в первую очередь, чтобы обеспечить опережающие действия для блокирования возможной атаки, а не устранения ее последствий.

Опережая возможные упреки в опасности раскрытия механизмов атак, мы считаем необходимым отметить следующее:

1. Знание механизмов атак позволяет в большинстве случаев предотвратить их путем правильного администрирования. Принцип «кто предупрежден – тот вооружен» оправдывает себя в данной ситуации и лишает нападающую сторону преимуществ внезапности и скрытности.
2. Информация об атаках в Сети основывается исключительно на открытых источниках. Правда об Internet, сопровождаемая понятными специалистам доводами, важнее для пользователя, чем неясные слухи о «страшных вторжениях в каждый компьютер» или рекламная информация о «достаточной мере защиты». Реальная оценка позволит точно установить риск использования Сети и требования к режиму ее использования.

Вопросы, оставшиеся за пределами данной книги

Осветить проблему безопасности сети Internet в целом не входило в наши планы. Мы не рассматривали безопасность электронной почты (программу PGP и т. п.), проблемы с безопасностью, возникающие при переходе на новый стандарт IPv6, почти не затронуты средства криптографической защиты (типа Kerberos). Кроме того, мы не стремились подробно описывать такие хорошо известные и, видимо, порядком уже поднадоевшие читателям методы и средства защиты в сети Internet, как Firewall, SSL, SKIP, S-HTTP.

Чем настоящее издание отличается от предыдущего «Атака через Internet»

Мы надеемся, что уважаемый читатель уже имел возможность познакомиться с предыдущей книгой «Атака через Internet». Тогда попробуем предвосхитить вопрос читателей об отличиях двух изданий и в этом разделе о них рассказать.

Во-первых, изменился состав авторов: вместо В. Платонова, написавшего в предыдущем издании вторую главу, появился новый автор – Д. Леонов, который написал десятую главу. Также в создании книги принимал участие Е. Ильченко – автор второй главы.

Во-вторых, существенно изменилось наполнение книги. Ее объем увеличен нами более чем в полтора раза за счет новых глав, посвященных Web-безопасности, социальной инженерии, методам сканирования, и отдельного раздела, написанного, по многочисленным пожеланиям наших читателей, о безопасности Windows NT. Кроме того, на основе проведенных нами исследований безопасности различных систем за два года, прошедших с момента выхода первой книги, существенно доработаны старые главы.

В-третьих, исправлены некоторые досадные технические ошибки и опечатки, присущие предыдущему изданию.

Авторы выражают благодарность всему коллективу кафедры информационной безопасности компьютерных систем Санкт-Петербургского государственного технического университета и отдельно Александру Монину за оформление большинства графических материалов книги, а также Евгению Ильченко – аспиранту Томского государственного университета – за помощь при составлении данной книги.

В завершение мы желаем всем нашим читателям обращать должное внимание на проблемы информационной безопасности и надеемся помочь вам как этой книгой, так и, возможно, лично в качестве независимых экспертов.

Специалистам понятна сложность в изложении столь деликатного вопроса, как безопасность сети, поэтому авторы будут благодарны читателям за отзывы.

Авторский коллектив:

Илья Медведовский – руководитель отдела информационной безопасности Notes Development, ведущий раздела «Информационная безопасность» журнала BYTE/Россия, ilya@blader.com;

Павел Семьянов – старший преподаватель кафедры информационной безопасности компьютерных систем СПбГТУ, psw@ssl.stu.neva.ru;

Дмитрий Леонов – главный редактор журнала «HackZone – территория взлома» и создатель одноименного сайта, web@hackzone.ru.

Условные обозначения



Эта пиктограмма обращает внимание на дополнительные сведения, связанные с обсуждаемой темой.



Пиктограмма обозначает утверждение.



Текст содержит следствие из предшествующего утверждения.