Атака на Internet

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

Илья Медведовский

Атака на Internet

«ДМК Пресс»

Медведовский И. Д.

Атака на Internet / И. Д. Медведовский — «ДМК Пресс»,

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.

Содержание

Илья Давидович Медведовский, Павел Валентинович Семьянов, Дмитрий Геннадьевич Леонов Атака на Internet

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 оче-

редь, 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.

Часть I
Хакеры и кракеры

Глава 1
О хакерах и не только…

Но сначала нам надо с тобой договориться, как именно мы определим, о чем мы советуемся, дабы не выходило, что я разумею одно, ты же – другое…
Платон. Диалоги

В последние полтора-два года книжные прилавки стали заполняться всевозможными книгами и журналами, в названиях которых присутствует слово «Internet». Это свидетельство того, что Internet пришел в Россию. Появились пользователи и провайдеры, с каждым днем растет количество всевозможных сайтов, начали формироваться свои службы, да и престиж заставляет некоторых людей подключаться к Сети. Появился и спрос на специальную литературу.

Практически в каждой такой книге имеется глава, раздел или параграф, посвященный безопасности. Однако анализ этого материала показывает, что главные вопросы – безопасна ли глобальная сеть и как защитить свой компьютер, подключенный к ней, – так и остаются без ответа.

Предлагаемая читателю книга целиком посвящена проблеме безопасности Internet. В отличие от других подобных изданий, она построена по принципу анализа возможных и существующих уязвимостей Сети, которые реализуются или могут быть реализованы в Internet. В книге рассматривается практически все, что грозит пользователю при работе с Internet, что поджидает каждого в этом удивительно интересном, но, подчеркиваем, опасном путешествии по Сети.

Основные понятия компьютерной безопасности

Для того чтобы рассматривать в дальнейшем вопросы защиты в Internet, необходимо напомнить основные понятия, которыми оперирует теория компьютерной безопасности. Вообще говоря, их всего три: это угрозы, уязвимости и атаки. Хотя искушенному читателю смысл их и так хорошо ясен, постараемся пояснить его.

Итак, *угроза* безопасности компьютерной системы – это потенциально возможное происшествие, неважно, преднамеренное или нет, которое может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней. Иначе говоря, угроза – это нечто плохое, что когда-нибудь может произойти.

Уязвимость компьютерной системы – это некая ее неудачная характеристика, которая делает возможным возникновение угрозы. Другими словами, именно из-за наличия уязвимостей в системе происходят нежелательные события.

Наконец, *атака* на компьютерную систему – это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости. Таким образом, атака – это реализация угрозы. Заметим, что такое толкование атаки (с участием человека, имеющего злой умысел) исключает присутствующий в определении угрозы элемент слу-

чайности, но, как показывает опыт, различить преднамеренные и случайные действия бывает невозможно и хорошая система защиты должна адекватно реагировать на любое из них.

Исследователи обычно выделяют три основных вида угроз безопасности – это угрозы раскрытия, целостности и отказа в обслуживании.

Угроза *раскрытия* заключается том, что информация становится известной тому, кому не следовало бы ее знать. В терминах компьютерной безопасности угроза раскрытия имеет место всякий раз, когда получен доступ к некоторой конфиденциальной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой. Иногда вместо слова «раскрытие» используются термины «кража» или «утечка».

Угроза *целостности* включает в себя любое умышленное изменение (модификацию или даже удаление) данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую. Обычно считается, что угрозе раскрытия подвержены в большей степени государственные структуры, а угрозе целостности – деловые или коммерческие.

Угроза *отказа в обслуживании* возникает всякий раз, когда в результате определенных действий блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным, так чтобы запрашиваемый ресурс никогда не был получен, или может вызвать только задержку, достаточно долгую для того, чтобы он стал бесполезным. В таких случаях говорят, что ресурс исчерпан. В локальных вычислительных системах (ВС) наиболее частыми являются угрозы раскрытия и целостности, а в глобальных, как будет показано далее, – на первое место выходит угроза отказа в обслуживании.

Особенности безопасности компьютерных сетей

Основной особенностью любой сетевой системы является то, что ее компоненты распределены в пространстве, а связь между ними осуществляется физически, при помощи сетевых соединений (коаксиальный кабель, витая пара, оптоволокно и т. п.), и программно, при помощи механизма сообщений. При этом все управляющие сообщения и данные, пересылаемые между объектами распределенной вычислительной системы, передаются по сетевым соединениям в виде пакетов обмена.

К сетевым системам, наряду с *обычными* (локальными) атаками, осуществляемыми в пределах одной компьютерной системы, применим специфический вид атак, обусловленный распределенностью ресурсов и информации в пространстве, – так называемые *сетевые* (или удаленные) атаки (remote или network attacks). Они характеризуются, во-первых, тем, что злоумышленник может находиться за тысячи километров от атакуемого объекта, и, во-вторых, тем, что нападению может подвергаться не конкретный компьютер, а информация, передающаяся по сетевым соединениям. С развитием локальных и глобальных сетей именно удаленные атаки становятся лидирующими как по количеству попыток, так и по успешности их применения, и, соответственно, обеспечение безопасности ВС с точки зрения противостояния сетевым атакам приобретает первостепенное значение.

Под *удаленной* атакой обычно понимается информационное разрушающее воздействие на распределенную ВС, программно осуществляемое по каналам связи. Такое определение охватывает обе особенности сетевых систем – распределенность компьютеров и распределенность информации. Поэтому далее будут рассмотрены два подвида таких атак – это удаленные атаки на инфраструктуру и протоколы сети и удаленные атаки на операционные системы и приложения. При этом под инфраструктурой сети мы понимаем сложившуюся систему организации отношений между объектами сети и используемые в сети сервисные службы, а под операционными системами и приложениями – все программное обеспечение, работающее на удаленном компьютере, которое тем или иным образом обеспечивает сетевое взаимодействие.

Что такое хорошо и что такое плохо

Просматривая большое количество статей (главным образом, в электронных журналах) о проблемах компьютерного взлома, нельзя не обратить внимание на тот факт, что ни в одной из них не проводится та грань, которая, как нам кажется, четко разделяет всех, так или иначе связанных с компьютерной безопасностью. В основном мнение компьютерного мира по этому поводу либо сугубо негативное (хакеры – это преступники), либо скромно-позитивное (хакеры – «санитары леса»). На самом деле у этой проблемы существует, по меньшей мере, две стороны, положительная и отрицательная, и между ними проходит четкая граница. Эта граница разделяет всех профессионалов, связанных с информационной безопасностью, на *хакеров* (hackers) и *кракеров* (crackers). И те, и другие во многом занимаются решением одних и тех же задач – поиском уязвимостей в вычислительных системах и осуществлением на них атак («взломом»).

Принципиальное различие между хакерами и кракерами состоит в целях, которые они преследуют. Основная задача хакера в том, чтобы, исследуя вычислительную систему, обнаружить слабые места (уязвимости) в ее системе безопасности и информировать пользователей и разработчиков системы с целью последующего устранения найденных уязвимостей. Другая задача хакера – проанализировав существующую безопасность вычислительной системы, сформулировать необходимые требования и условия повышения уровня ее защищенности.

С другой стороны, основная задача кракера состоит в непосредственном осуществлении взлома системы *с целью получения несанкционированного доступа* к чужой информации – иначе говоря, для ее кражи, подмены или для объявления факта взлома. Кракер, по своей сути, ничем не отличается от обычного вора, взламывающего чужие квартиры и крадущего вещи. Он взламывает вычислительные системы и крадет чужую информацию. Итак, кардинальное различие между хакерами и кракерами в том, что первые – исследователи компьютерной безопасности, а вторые – просто воры или вандалы. Хакер в данной терминологии – это специалист. В качестве доказательства приведем определение из словаря Guy L. Steele.

> **HACKER,** *сущ.* **1.** Индивидуум, который получает удовольствие от изучения деталей функционирования компьютерных систем и от расширения их возможностей, в отличие от большинства пользователей компьютеров, которые предпочитают знать только необходимый минимум. **2.** Энтузиаст программирования; индивидуум, получающий удовольствие от самого процесса программирования, а не от теоретизирования по этому поводу.

Данная трактовка термина «хакер» отличается от принятой в средствах массовой информации, которые, собственно, и привели к подмене понятий. В последнее время многие специалисты по компьютерной безопасности (особенно на Западе) стали аккуратнее относиться к этим терминам, и мы в подобной трактовке терминов уже не одиноки.

Низменность мотивов кракеров и отсутствие стремления к профессиональному росту приводят к тому, что 90 % из них являются «чайниками», которые взламывают плохо администрируемые системы, в основном используя чужие программы (обычно такая программа называется *exploit).* Причем это мнение тех самых 10 % профессиональных кракеров – бывших хакеров, ставших на путь нарушения закона. Их, в отличие от кракеров-«чайников», остановить действительно очень сложно, но, как показывает практика, отнюдь не невозможно (см. противоборство Митника и Шимомуры в главе 4). Очевидно, что для предотвращения возможного взлома или устранения его последствий требуется пригласить квалифицированного специалиста по информационной безопасности – профессионального хакера.

Однако было бы несправедливо смешать в одну кучу всех кракеров, однозначно назвав их ворами. По нашему мнению, кракеров можно разделить на три следующих класса в зави-

симости от цели, с которой осуществляется взлом: вандалы, «шутники» и профессиональные взломщики.

Вандалы – самая известная (во многом благодаря широкому распространению вирусов, а также творениям некоторых журналистов) и, надо сказать, самая малочисленная (к счастью) часть кракеров. Их основная цель – взломать систему для ее дальнейшего разрушения. К ним можно отнести, во-первых, любителей команд типа rm – f – d *, del *.*, format c:/U и т. д. и, во-вторых, специалистов в написании вирусов или «троянских» коней. Совершенно естественно, что весь компьютерный мир ненавидит кракеров-вандалов лютой ненавистью. Эта стадия кракерства характерна для новичков и быстро проходит, если кракер продолжает совершенствоваться (ведь довольно скучно осознавать свое превосходство над беззащитными пользователями). Кракеров, которые даже с течением времени не миновали эту стадию, а только все более оттачивали свои навыки разрушения, иначе, чем социальными психопатами, не назовешь.

«Шутники» – наиболее безобидная часть кракеров (конечно, в зависимости от того, насколько злые они предпочитают шутки), основная цель которых – известность, достигаемая путем взлома компьютерных систем и внесения туда различных эффектов, выражающих их неудовлетворенное чувство юмора. К «шутникам» также можно отнести создателей вирусов с различными визуально-звуковыми эффектами (музыка, дрожание или переворачивание экрана, рисование всевозможных картинок и т. п.). «Шутники», как правило, не наносят существенного ущерба компьютерным системам и их администраторам (разве что моральный). На сегодняшний день в Internet это наиболее распространенный класс кракеров, обычно осуществляющих взлом Web-серверов, чтобы оставить там упоминание о себе. Все это либо невинные шалости начинающих, либо рекламные акции профессионалов.

Взломщики – профессиональные кракеры, пользующиеся наибольшим почетом и уважением в кракерской среде. Их основная задача – взлом компьютерной системы с серьезными целями, например с целью кражи или подмены хранящейся там информации. Как правило, для того чтобы осуществить взлом, необходимо пройти три основные стадии: исследование вычислительной системы с выявлением в ней изъянов (уязвимостей), разработка программной реализации атаки и непосредственное ее осуществление. Естественно, настоящим профессионалом можно считать только того кракера, который для достижения своей цели проходит все три стадии. С небольшой натяжкой профессионалом можно также считать того кракера, который, используя добытую третьим лицом информацию об уязвимости в системе, пишет ее программную реализацию (exploit). Осуществить третью стадию, используя чужие разработки, очевидно, может практически каждый.

Если абстрагироваться от предмета кражи, то работа взломщиков – это обычное воровство. К сожалению, в России все не так просто. Конечно, взлом компьютерных систем ни в коем случае нельзя назвать достойным делом, но в стране, где большая часть находящегося у пользователей программного обеспечения является пиратским (хотя ситуация, наконец, меняется в лучшую сторону – становится модным использовать легальное ПО), то есть украденным не без помощи тех же взломщиков, почти никто не имеет морального права «бросить в них камень».

В этой книге мы ограничимся рассмотрением хакеров-кракеров с позиций распределенных систем, однако не нужно забывать, что самая многочисленная категория кракеров занимается более обыденными вещами, а именно: снятием защиты с коммерческих версий программных продуктов, изготовлением регистрационных ключей (registration key) для условно бесплатных программ (shareware) и т. п.

Цели кракера

Итак, какие же цели преследует кракер, атакующий извне ваш компьютер? Очевидно, их может быть несколько:

• получить доступ к важной информации, хранящейся у вас. Вероятно, вы крупная компьютерная шишка, и за вами серьезно охотятся (если, конечно, этой информацией не является несколько гигабайт изображений высокого разрешения);

• получить доступ к ресурсам вашей системы. Это может быть как процессорное время (особенно, если вы обладаете суперкомпьютером), так и дисковое пространство (например, для организации пиратского ftp-сайта). В этом случае вы не только ничего не потеряете, но и, возможно, приобретете честно украденное программное обеспечение стоимостью много тысяч долларов;

• нарушить работоспособность вашего хоста без реализации угрозы раскрытия. Это бывает опасно, если ваш хост должен обеспечивать бесперебойное обслуживание клиентов;

• иметь плацдарм для осуществления вышеназванных целей, но для атаки на другой компьютер – тогда в журналах атакованного компьютера будет значиться, что атака осуществлялась с вашего адреса. Вы, конечно, будете доказывать, что вы тут ни при чем, и, вероятно, докажете это, но инцидент доставит вам несколько неприятных минут и вы услышите обидные слова об уровне защиты вашего хоста;

• запустить пробный шар, отладить механизмы атак на другие системы. Не расстраивайтесь, ведь это доказательство того, что вы не так уж бесполезны в сети, в отличие от других хостов, на которые никогда никто не нападал и которые остро ощущают свою ненужность.

Сетевая информационная безопасность: мифы и реальность

Всемогущество хакеров

Глубокое непонимание большинством обывателей проблем, связанных с информационной безопасностью в вычислительных системах, с течением времени сформировало определенный миф о всемогуществе хакеров и повсеместной беззащитности компьютерных систем. Действительно, современные вычислительные системы и сети общего назначения имеют серьезнейшие проблемы с безопасностью. Но, подчеркнем, именно вычисли тельные системы общего назначения. Там же, где требуется обработка критической информации и обеспечение высшего уровня защиты и секретности (например, в военной области, в атомной энергетике и т. п.), используются специализированные защищенные ВС, которые (и это чрезвычайно важно!) в основном изолированы от сетей общего назначения (от сети Internet, например). Поэтому необходимо развеять первый миф, исключительно популярный в художественной литературе, кино, а также в средствах массовой информации: кракер не может проникнуть извне в вычислительную систему стратегического назначения (например, в ВС атомной станции или пункта управления стратегическими вооружениями).

Новую жизнь в этот миф вдохнул последний военный конфликт в Югославии. Согласно сообщениям российских СМИ, складывалось ощущение, что военные сети НАТО полностью беззащитны и полный контроль над ними имеют «отважные хакеры». Естественно, что если такие перлы попадали в электронные эхо-конференции, то только в разделы юмора.

Тем не менее мы говорим лишь о невозможности получения несанкционированного удаленного доступа именно извне. В том случае, если нанести ущерб системе вознамерится кракер из состава персонала защищенной ВС, то сложно абстрактно судить, насколько успешны будут его попытки.

В качестве примера напомним случай на Игналинской АЭС, когда местный системный программист внедрил в ВС программную закладку («троянского» коня), которая чуть не привела к аварии на станции. Однако, как утверждает статистика, нарушения безопасности системы собственным персоналом составляют около 90 % от общего числа нарушений. Итак,

критические вычислительные системы нельзя назвать неуязвимыми, но реализовать на них успешную удаленную атаку практически невозможно.

Прочитав этот раздел, недоверчивый читатель может заметить, что он лично встречал заметки о том, как «кракеры проникли в компьютер Пентагона или НАСА». Все дело в том, что любая уважающая себя организация, будь то ЦРУ, АНБ или НАСА, имеет свои WWW– или ftp-серверы, находящиеся в открытой сети и доступные всем. И кракеры в этом случае проникали именно в них (а ни в коем случае не в секретные или закрытые сети), используя, может быть, один из механизмов, описанных в нашей книге.

Защита банковских систем

Другим и, пожалуй, наиболее устойчивым мифом является миф о всеобщей беззащитности банковских вычислительных систем. Да, действительно, в отличие от ВС стратегического назначения, банки из-за конкурентной борьбы между собой вынуждены для обеспечения удобства и быстродействия работы с клиентами предоставлять им возможность удаленного доступа из сетей общего пользования к своим банковским вычислительным системам. Однако, во-первых, для связи в этом случае используются защищенные криптопротоколы и разнообразные системы сетевой защиты (например, Firewall), и, во-вторых, предоставление клиенту возможности удаленного доступа отнюдь не означает, что клиент может получить доступ непосредственно к внутренней банковской сети. По мнению специалистов, зарубежные банковские ВС (про отечественные мы не говорим, пока еще не достигнут соответствующий уровень автоматизации расчетов) являются наиболее защищенными после ВС стратегического назначения.

Однако в последние годы некоторым журналистам, в том числе и отечественным, в погоне за сенсацией удалось (и не без успеха, особенно на основе реально имевшего место дела Левина) придумать миф о всеобщей беззащитности банковских систем. Яркий пример подобных творений – статья г-на А. Какоткина «Компьютерные взломщики», опубликованная в еженедельнике «Аргументы и Факты» в феврале 1997 года. Вывод из этой статьи, перефразируя слова ее автора, можно сделать следующий: «Каждому хакеру – по бронежилету и запасному процессору». Не нужно быть крупным специалистом по компьютерной безопасности, чтобы, прочитав эту статью, понять, что она неправдоподобна от начала и до конца (особенно смешно читать «подробности» взлома банковской сети). Возможно, впрочем, что недостаточно просвещенного в этой области журналиста некие люди ввели в заблуждение (или, что неудивительно, он просто чего-то не понял).

Более интересным, на наш взгляд, вопросом является то, насколько надежно на самом деле защищены банковские сети, особенно в том случае, если к ним предусмотрен удаленный доступ из сети Internet. К сожалению, мы не можем дать точного ответа, пока специализированные системы безопасности банковских ВС (естественно, под такими системами не имеются в виду операционные системы типа Novell NetWare, Windows NT или 95, UNIX, которые хоть и часто применяются в банковской среде, но специализированными уж никак не являются) не будут сертифицированы. Единственное, что можно гарантировать, – то, что с вероятностью около 99,9 % подобные системы будут подвергаться угрозе отказа в обслуживании, которая рассмотрена далее.

Сетевые кракеры

Недоверие к описанным в средствах массовой информации способам того, как кракеры осуществляют взлом, и того, *к каким* результатам это приводит, побудило нас подробнее рассмотреть вопрос: а реальны ли вообще такие взломы?

Так вот, ни одного подтвержденного факта осуществления целенаправленного взлома с помощью программных средств (а не с помощью подкупа и т. п.) нам не удалось найти ни в России, ни за рубежом.

Да, почти каждый день вскрываются WWW-серверы каких-то компаний. Но здесь жертва выбирается не целенаправленно, а большей частью случайно: «повезет – не повезет». Более того, подмена некоторых WWW-страниц часто вовсе не означает, как будет показано в следующих главах, полного контроля над атакованным хостом, злоумышленник может вообще не иметь к нему никакого доступа, а просто подменять эти страницыс помощью перемаршрутизации. Собственно, взлом WWW-серверов и составляет 90 % всех проявлений якобы всемогущих кракеров, обсуждаемых в сетевой и несетевой прессе.

Легендарный Кевин Митник был по большей части именно легендарным. Его самая известная (и, возможно, единственная реальная) атака обсуждается в четвертой главе этой книги. Даже если принять эту атаку так, как она преподносится (обратите внимание на наши сомнения по поводу квалификации Митника!), очевиден тот факт, что она была придумана не им и осуществлена в то время, когда в Internet меньше всего беспокоились о безопасности.

Можно вспомнить еще дело Левина. Очень туманное дело. Если Левин (или кто-то еще) действительно вскрыл CityBank, пользуясь только своей головой и руками, то мы готовы взять свои слова обратно. Но на сегодняшний день наиболее убедительной является версия, что у него все же были сообщники в этом банке, которые предоставили ему входное имя и пароль. Косвенным подтверждением этого служит факт, что «гениальный взломщик банков» почему-то был гениален только в самом процессе взлома и вел себя, скажем, не очень умно при сокрытии своих следов и противоборстве с правоохранительными органами.

Все это позволяет нам предположить, что проблема сетевых кракеров в том виде, как она обычно преподносится СМИ, на самом деле отсутствует. Да, много сил должно уделяться защите компьютерных систем от «псевдохакеров», которые считают себя профессионалами, умея запускать различные «нюки» (nuke) или подбирать пароли типа «guest». Они способны нанести этим определенный урон. Существуют, безусловно, и более квалифицированные группы кракеров, занимающиеся, например, взломом WWW-серверов для «увековечивания» собственного имени. Но у нас вызывает большое сомнение существование профессионалов, а тем более налаженной индустрии, которая допускает взлом любого более-менее защищенного хоста «на заказ». По собственному опыту мы можем предположить, что цена такого взлома должна быть в несколько раз больше, чем ценность находящейся там информации, поэтому в ход идут старые проверенные методы типа вербовки или подкупа.

Резюмируя, мы считаем, что никаких сетевых кракеров, специализирующихся на вскрытии хостов за деньги или с целью использования полученной информации для собственного обогащения, не существует. Их квалификация должна быть настолько высока, что во всем мире таких людей можно без труда пересчитать, и они наверняка являются хакерами, а не кракерами.

Межсетевые экраны Firewall как панацея от всех угроз

И последний миф – это миф о системах Firewall, как о «единственном надежном средстве обеспечения безопасности» сегмента IP-сети. Да, сама суть методики Firewall является абсолютно непогрешимой и логичной. Основной ее постулат заключается в создании *bastion host* (выделенный бастион), обеспечивающего контроль за безопасностью в защищаемом сегменте сети и осуществляющего связь данного сегмента с внешним миром. Но это все действует пока только в теории. На практике же все известные нам сегодня системы Firewall *неспособны к отражению большинства из описанных удаленных атак как на протоколы и инфраструктуру сети, так и на операционные системы и приложения.*

Это, конечно, отнюдь не означает, что отразить данные удаленные атаки принципиально невозможно, – именно в направлении обнаружения и отражения сетевых атак сейчас наиболее активно развивается современная наука. По-видимому, все дело в том, что большинство разработчиков систем Firewall, как это часто случается с разработчиками систем защиты ВС, никогда не были хакерами и, следовательно, смотрели на проблему защиты IP-сетей не с точки зрения взломщика, а с точки зрения пользователя.

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

Для тех, кто хочет посмотреть на проблему безопасности с другой стороны, со стороны кракера, напоминаем, что с 1997 года начали действовать новые статьи УК РФ, где, к сожалению, довольно расплывчато и нечетко описывается возможная уголовная ответственность за «преступления в сфере компьютерной информации» (глава 28 УК РФ):

Статья 272. *Неправомерный доступ к компьютерной информации.*

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, – наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, – наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы, или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. *Создание, использование и распространение вредоносных программ для ЭВМ.*

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами, – наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, – наказываются лишением свободы на срок от трех до семи лет.

Статья 274. *Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.*

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, – наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, – наказывается лишением свободы на срок до четырех лет.

По своей сути данный закон должен быть направлен именно на кракеров, однако такое правонарушение, как взлом программного обеспечения, даже не упоминается. С другой стороны, расплывчатость формулировок статей закона, в случае их формальной трактовки, позволяет привлечьк уголовной ответственности практически любого программиста или системного администратора (например, допустившего ошибку, которая повлекла за собой причинение определенного законом ущерба). Так что программы теперь лучше вообще не писать.

Если же говорить серьезно, то применение на практике приведенных статей Уголовного кодекса чрезвычайно затруднено. Это связано, во-первых, со сложной доказуемостью подобных дел (судя по зарубежному опыту) и, во-вторых, с естественным отсутствием у следователей высокой квалификации в данной области. Поэтому, видимо, пройдет еще не один год, пока мы дождемся успешного уголовного процесса над преступникамив сфере компьютерной информации.

Проблема 2000года в свете информационной безопасности

Новое издание нашей книги выходит в 1999 году, и вполне естественным нашим желанием является обратить внимание читателей на проблему 2000 года (Y2K), которую мы рассматриваем в несколько менее традиционном аспекте – как с точки зрения информационной безопасности проблема Y2K повлияет на киберпространство.

Большинство исследований, посвященных этой проблеме, в основном содержат анализ причин возможных отказов в работе прикладного или системного программного обеспечения, потери от таких отказов и меры по предотвращению сбоев в работе программного обеспечения. Однако нельзя забывать о целом классе программных средств, основная задача которых – обеспечение информационной безопасности (ПСОИБ – программные средства обеспечения информационной безопасности). В этом разделе мы рассмотрим виды ПСОИБ, потенциально наиболее уязвимые по отношению к проблеме Y2K (программные средства, которые обрабатывают данные, связанные с системной датой), выделим различные модули ПСОИБ и рассмотрим возможные причины, по которым проблема Y2K может иметь к ним непосредственное отношение.

Возможные проблемы в модулях ПСОИБ

1. Проблемы с системами шифрования/цифровой подписи.

При шифровании/дешифрировании сообщений, формировании или проверке электронной подписи, при проверке подлинности сертификата, подтверждающего личность пользователя, программные реализации криптосистем могут некорректно обрабатывать год создания сообщений, тем самым приводя к их частичной или полной потере. Это может привестик нарушению функциональности криптосистем, вплоть до полной невозможности отправлять или читать шифрограммы.

Рассмотрим подробнее сущность данной проблемы. Любая криптосистема содержит в своей основе систему анализа, хранения и распределения ключевой информации (сертификатов), предназначенной для шифрования сообщений и идентификации/аутентификации пользователей. Все сообщения, передаваемые криптосистемой, так или иначе шифруются с использованием данного сертификата, который, как правило, выдается на определенный срок и, следовательно, с течением времени устаревает. Как следствие, системы шифрования обязательно обладают встроенными модулями «временного» анализа, задача которых – сопоставлять дату сертификата с текущей, указанной в шифрограмме, для того чтобы отфильтровать

устаревшие или повторные сообщения. Например, известная атака на криптосистемы связана с повторной передачей ранее перехваченных зашифрованных сообщений. В случае успеха атаки, если данное сообщение будет воспринято системой, можно вызвать повторную реакцию криптосистемы на данное сообщение, что приведет, например, к переполнениюи сбою системы (в случае *направленного шторма* повторными сообщениями). В связи с этим криптосистемы обычно имеют встроенную защиту от подобных атак и, анализируя дату приходящих сообщений, не допускают прием повторных сообщений или сообщений, зашифрованных с использованием устаревших ключей. В том случае, если в системе модуль «временного» анализа разработан без учета проблемы Y2K, криптосистема в целом может дать сбой, что приведет к приему повторных сообщений или полному выходу системы из строя.

2. Проблемы с модулями автоматизированного контроля безопасности системы.

Одной из стандартных функций ПСОИБ является автоматизированный контроль за безопасностью системы. Обычно данные модули осуществляют динамический контроль за состоянием АС, что вынуждает их использовать и протоколировать в log file (журнал аудита) время и дату обнаруженного контролируемого события. В стандартную поставку данных систем входят модули анализа журнала аудита. Сбои в этих модулях при попытке автоматизированного анализа базы данных, содержащей журнал аудита, могут привести к неверной реакции системы обеспечения информационной безопасности. Примером в данном случае являются системы Firewall, одна из задач которых – постоянное ведение журнала аудита, в который, помимо информации о попытках создания сетевых соединений, заносится информацияо времени создания соединения. Использование средств автоматизированного анализа журнала аудита, разработанных без учета Y2K, может вызвать их сбой и привести как к аварийному завершению процесса, осуществляющего анализ, так и к аварийному завершению работы всей системы в целом.

3. Проблемы с модулями реализации авторизованного доступа к ресурсам системы.

Одним из модулей, который присутствует практически в любой системе обеспечения компьютерной безопасности, является модуль контроля и предоставления авторизованного доступа к ресурсам системы. Данный модуль обеспечивает/запрещает доступ в систему в зависимости от даты и времени его осуществления. Например, функциями Account Expires и Logon Hours в Windows NT 4.0 можно разрешить пользователю доступ в систему с (или до) определенной даты или в определенные часы. Соответственно, в том случае, если в данном модуле о проблеме Y2K разработчики «забыли» (отметим, что эти службы приведены просто для примера), то такая забывчивость может привести к невозможности получения авторизованного доступа в систему в лучшем случае только для пользователя с установленным Account Expires, а в худшем – для всех пользователей системы, если сбой при входе в систему одного пользователя повлечет за собой сбой в работе модуля в целом.

4. Проблемы с модулями автоматизированного анализа безопасности и поиска вирусных сигнатур.

Другой разновидностью ПСОИБ являются средства автоматизированного анализа безопасности, основная задача которых состоит в анализе системы на предмет наличия в ней известных уязвимостей (сетевые сканеры безопасности, например SATAN, Internet Security Scanner и т. д.) или вирусов (антивирусов). Эти средства сетевого анализа широко применяются администраторами безопасности крупных корпоративных сетей с постоянно видоизменяемой инфраструктурой, что позволяет им выявлять внесение в ВС новых объектов, содержащих уязвимости или вирусы. Одной из стандартных функций ПСОИБ данного вида является возможность ихзапуска в определенное время. В связи с этим данный тип программного обес-

печения (ПО) также становится уязвимым из-за проблемы Y2K, что приведет к невозможности анализа безопасности системы и проникновению в нее кракеров или заражению ее вирусами.

5. Проблемы со встроенными системами на основе License Key (защита от нелегального использования).

Одной из особенностей ПСОИБ является практически повсеместное применение в них систем защиты от нелегального использования, обычно основанных на временных лицензиях. Те средства, которые в качестве «привязки» используют данные о системной дате в компьютере, могут быть подвержены сбоям, связанным с неправильной интерпретацией «нулевой» даты при достижении 2000 года.

Например, лицензия (сертификат) на работу данного программного средства рассчитана на 1 год и дается с 05.05.1999 по 05.05.2000. Следовательно, после наступления 2000 года система защиты от нелегального использования может дать сбой, и ПСОИБ откажутся далее функционировать вплоть до устранения проблемы.

6. Проблемы с операционными системами, в которых функционируют ПСОИБ.

Подавляющее большинство программных средств защиты функционируют под управлением различных операционных систем. Поэтому сбой операционной системы, в которой функционируют ПСОИБ, может косвенно повлиять на функционирование самой системы защиты и привести к ее дальнейшей некорректной работе или полному выходу из строя вплоть до устранения проблемы, связанной с управляющей операционной системой. Например, сбой в сервере ntp (network time protocol), в случае использования данного сервера, может привести к сбою системы защиты в целом.

7. Проблемы с аппаратными средствами защиты.

Общепризнанным является тот факт, что в сфере информационной безопасности используются комплексные решения, включающие в себя не только программные средства обеспечения безопасности, но также и аппаратные средства.

Существующие аппаратные средства защиты, разграничивающие доступ в систему на основе различной идентифицирующей информации (сетчатка глаза, отпечатки пальцев, электронные ключи и т. д.), могут дать аппаратный сбой, связанный с неверной обработкой системной даты при идентификации пользователя. Например, сбой электронного идентификатора «Touch Memory» может сделать невозможной идентификацию/аутентификацию пользователя, и дальнейший вход в контролируемую систему будет запрещен или разрешен в зависимости от реакции системы на данный сбой.

Возможные последствия проблемы Y2K

Оценим на основе вышеизложенного возможные последствия нарушения работоспособности автоматизированных систем обеспечения информационной безопасности в связи с проблемой Y2K. Данная оценка приводитсяс учетом основных функций ПСОИБ, заключающихся в предоставлении авторизованного доступа к ресурсам системы, в шифровании/дешифрировании конфиденциальной информации, в контроле за безопасностью системы, в анализе безопасности системы.

Итак, автоматизированным системам, использующим ПСОИБ, угрожают следующие опасности:

1. Невозможность получения доступа в систему для авторизованных пользователей.
2. Предоставление доступа неавторизованным пользователям.
3. Нарушение работоспособности АС, использующей ПСОИБ.
4. Невозможность в создании/передаче/чтении конфиденциальной информации, зашифрованной ПСОИБ.

5. Невозможность контроля за безопасностью системы оставит незамеченными как предварительный анализ атакующим ресурсов системы, так и возможные успешные попытки получения неавторизованного доступа к ресурсам контролируемой АС.

6. Невозможность выявления имеющихся недостатков в системе обеспечения безопасности, а также вирусов в ПО, что может в дальнейшем повлечь за собой нарушение безопасности системы или заражение ее компьютерными вирусами.

Возможные пути решения обозначенных проблем

1. Самостоятельное тестирование ПСОИБ путем установки новой системной даты.

Это, очевидно, наиболее простой способ самостоятельной проверки, однако использовать его нужно с определенной осторожностью. Дело в том, что выданные сертификаты (лицензии), подтверждающие легальную работу ПСОИБ или личность пользователя, после изменения системной даты и запуска ПСОИБ могут оказаться просроченными и в дальнейшем (даже после восстановления текущей даты) потерять свою силу. Данный факт серьезно затрудняет тестирование систем, однако проблема решается путем хранения эталонных сертификатов на отдельных носителях (если это возможно) и тестирования *только* макетов АС, а ни в коем случае не реально действующих систем.

2. Обращение к производителям ПСОИБ.

Пользователям, обладающим средствами ПСОИБ, имеет смысл обратиться к фирмам-производителям за получением в связи с проблемой Y2K соответствующих рекомендаций, разъяснений и патчей к программным средствам.

Информационная безопасность России и проблема Y2K

В российских условиях проблема Y2K с точки зрения информационной безопасности, на первый взгляд, выглядит несколько неактуальной в связи с относительно слабым развитием систем телекоммуникаций, особенно по сравнению со странами с более развитой экономической структурой. Но это только на первый взгляд! В наших условиях с точки зрения безопасности на первый план выходят не современные автоматизированные системы, о которых имеется достаточно информации, а всевозможные устаревшие программы, разработанные более десяти лет назад, отвечающие за обеспечение надежной работы систем управления и доступ к объектам стратегического назначения, таким как атомные станции, военные системы управления ракетами и т. д. Об их безопасности в связи с проблемой Y2K в данном случае судить достаточно сложно, но можно предположить, что программы, созданные в прошедших десятилетиях, содержат немало ошибок, связанных с неправильной обработкой системной даты. К каким последствиям это может привести – ответ очевиден. Примером сбоя ПО стратегического назначения служит известная авария французского ракетоносителя Ariane 5, произошедшая 4 июня 1996 года из-за тривиальной ошибки переполнения переменной и принесшая только прямых убытков на 500 миллионов долларов.

Глава 2
Социальная инженерия и ее применение

Все-таки желательно, гражданин артист, чтобы вы незамедлительно разоблачили бы перед зрителями технику ваших фокусов.
М. Булгаков. Мастер и Маргарита

В процессе написания этой части возник вопрос, как можно корректно перевести Social Engineering… В электронном переводчике Socrat мы нашли, что это – «общественное проектирование». Наверное, корректнее сказать «социальное исследование» или «социальная проработка», но оба термина совершенно неблагозвучны. Пожалуй, оставим так – «социальная инженерия» (СИ). Дело в том, что до сих пор этой проблеме в отечественной прессе не уделялось внимания, и потому соответствующего термина не существует.

Итак, что такое социальная инженерия в контексте информационной безопасности? Словарь хакерского жаргона сообщает: «Социальная инженерия – термин, использующийся взломщиками и хакерами для обозначения несанкционированного доступа к информации иначе, чем взлом программного обеспечения; цель – обхитрить людей для получения паролей к системе или иной информации, которая поможет нарушить безопасность системы. Классическое мошенничество включает звонки по телефону в организацию для выявления тех, кто имеет необходимую информацию, и затем звонок администратору, эмулируя служащего с неотложной проблемой доступа к системе».

Да, действительно, самое простое средство проведения СИ – телефон. Все исследование основывается на одной маленькой детали: в крупных компаниях лица, ответственные за систему, не знают всех сотрудников, поэтому появляется возможность манипулировать действиями администраторов. Телефон облегчает эту задачу, так как администратор не видит абонента, который может звонить даже из другого города или страны.

В западной прессе часто мелькают сообщения о том, что кто-то где-то что-то взломал. Немалая часть этих взломов как раз и была проведена с помощью СИ. В идеальных условиях у взломщика должны быть:

- телефон, воспроизводящий шум офиса;
- автоопределитель номера;
- устройство для изменения голоса;
- возможность использовать чужую телефонную линию.

Все эти вещи необходимы для успешного применения теоретических знаний на практике, но в нашей стране получить сразу все не представляется возможным, так что потенциальным взломщикам приходится довольствоваться простыми подручными средствами. Первый инструмент заменяется обыкновенным шумом в комнате или магнитофонной записью. Второй не составит труда отыскать. Третий – самое сложное. Проблема в том, что качественный аппарат способен преобразовывать голос как угодно: в женский, в детский, в старческий… Такие устройства очень редки, поэтому полностью использовать возможности СИ вряд ли получится. Конечно, ничто не помешает постучать ложкой о тарелку и сделать вид, что люди в офисе обедают. Можно позвать тетю Машу, дать ей шоколадку и попросить позвонить… Об использовании чужой линии, наверное, и заикаться не стоит. Единственное, что сразу приходит в голову, – это телефонная трубка с номеронабирателем и ближайший телефон-автомат. Но тогда придется использовать еще и анти-АОН.

Классификация атак класса СИ

Обычно атаки класса СИ представляют собой комбинацию некоторых средств, методов и «параметров окружения». Основные разновидности можно разделить на следующие категории.

По средствам применения:

- телефон;
- электронная почта;
- разговор по Internet в «реальном времени»;
- обыкновенная почта;
- личная встреча.

В первом случае основную сложность представляет голос. Если объект знаком с тем, кем вы представились, то необходимо сделать так, чтобы ваш голос почти не отличался от его голоса. При использовании электронной почты проблема голоса отпадает, зато появляется стиль письма, которого нужно придерживаться от начала и до конца. То же самое утверждение можно отнести к третьему и четвертому пунктам данной классификации. В последнее время быстро развивается новый вид общения – **ICQ,** некая смесь электронной почты, разговора в реальном времени и организатора межсетевых взаимодействий между пользователями. Эта программа иногда позволяет в большей степени ввести в заблуждение пользователей, но об этом потом. Следующий вид контактов – личностный. Лично можно воздействовать только на тех людей, которые не смогут утверждать, что вы не тот, за кого себя выдаете. В этом случае необходимо иметь приятный голос и уметь нравиться людям. Конечно, при сложных комбинациях может быть использовано не одно средство, а, возможно, даже все, но человек, осуществляющий такую атаку, должен быть не просто хорошим, а отличным психологом.

По уровню социального отношения к объекту:

- официальный;
- товарищеский;
- дружеский.

Разумеется, для того чтобы атака оказалась успешной, нужно выбрать соответствующий стиль общения для каждого случая. При официальном стиле общения недопустимы нотки пренебрежения или дружественности. Необходимо, чтобы все выглядело так, как должно. Если был выбран товарищеский тон, то предполагается, что вы знаете хотя бы имя человека, с которым собираетесь разговаривать. Последний, дружеский уровень дается с большими усилиями. Желательно не просто много знать о человеке, но и представлять, кем вы собираетесь выглядеть. Это самый сложный вид атаки, но после его успешного применения можно добиться самых высоких результатов.

По степени доступа объекта к информационной системе:

- администратор – высокая;
- начальник – средняя;
- пользователь – низкая;
- знакомый администратора, начальника или пользователя – отсутствие доступа.

Здесь предполагается разделение по результату атаки. Соответственно, в первом случае результат наибольший, а в последнем – наименьший. Но это – с точки зрения промежуточного результата (см. табл. 2.1). На практике работа с пользователем и знакомыми оказывается легче, чем с администратором и начальником: больше вероятность, что последние знают того, кем вы собираетесь представиться.

Таблица 2.1. Вероятность успешного проведения атаки в зависимости от навыков выполняющего (низкая-1, средняя-2 высокая-3)

Класс атаки / Подготовленность злоумышленника	Новичок	Любитель	Профессионал
СРЕДСТВАяПРИМЕНЕНИЯ			
Телефон	3	3	3
Электроннаяпочта	2	3	3
Обыкновеннаяпочта	1	3	3
РазговорячеяInternet	3	3	3
Личнаявстреча	1	2	3
УРОВЕНЬяОБЩЕНИЯя(ОТНОШЕНИЯ)			
Официальный	2	3	3
Товарищеский	3	3	3
Дружеский	1	2	3
СТЕПЕНЬяДОСТУПА			
Администратор	1	2	3
Начальник	1	2	3
Пользователь	3	3	3
Знакомый	2	3	3

Краткое введение в психологию СИ

«На свете есть только один способ побудить кого-либо что-то сделать. Задумывались ли вы когда-нибудь над этим? Да, только один способ. И он заключается в том, чтобы заставить другого человека захотеть это сделать. Помните – другого способа нет», – писал Дейл Карнеги.

Знаете… а ведь он прав! Конечно, все это и так интуитивно понятно, но если разобраться глубже, то оказывается, что есть способы, позволяющие этого достичь. Один из наиболее видных психологов XX века, Зигмунд Фрейд, говорил, что в основе всех наших поступков лежат два мотива – сексуальное влечение и желание стать великим, причем последнее трактуется как «желание быть значительным» или «страстное стремление быть оцененным». В принципе это одно и то же. Дайте человеку понять, что вы его цените и уважаете! Мы не призываем вас при разговоре с администратором сети льстить и сыпать комплиментами, хотя «льстить – значит говорить человеку именно то, что он думает о себе». Конечно, умный человек это заметит, и такое отношение ему может не понравиться. Но если заранее постараться признать для себя достоинства того, с кем вы собираетесь разговаривать, то собеседник почувствует вашу искренность.

Попробуйте произнести такие слова: «Я понимаю, что вы ужасно заняты, но не могли бы вы.» Обычно подобная фраза говорится с юмористическим оттенком или с тоном пренебрежения. Но если вы попробуете представить себе, что человек действительно занят и у него нет никакого желания с вами разговаривать, то ваш тон моментально изменится. Поверьте, такой прием подействует, только если говорить искренне!

Примеры проникновения в систему

Наверняка все в детстве баловались с телефонами. Ну кто не знает таких шуток, как: «Алло, это зоопарк?» – «Нет». – «А почему обезьяна у телефона?». Совершенно безобидный пример издевательства над людьми. А вот еще один подобный пример, но с элементами СИ:

Шутник: Алло! Вас беспокоят с телефонной станции. Измерьте, пожалуйста, длину шнура от трубки к телефону.

Жертва: Метр.

Ш.: Хорошо, для того, чтобы повеситься, хватит.

Следующий звонок.

Ш.: Алло! Это милиция. Вам сейчас хулиганы не звонили?

Ж.: Да, да! Звонили! Разберитесь с ними, пожалуйста!

Ш.: Про трубку и провод спрашивали?

Ж.: Да!

Ш.: И он у вас метр?

Ж.: Да!

Ш.: А почему до сих пор не висим?

Это было лирическое отступление на тему того, как методы СИ используются детьми на бессознательном уровне, в качестве шутки. Рассмотрим простейший пример СИ для проникновения в систему.

Звонок администратору системы.

Взломщик: Здравствуйте, вы администратор?

Администратор: Да.

В.: Я понимаю, что вы ужасно заняты, извините, что отрываю вас от дел, но я не могу войти в сеть.

А.: *(Про себя: ЁПРСТ!!! Поработать не дают!)* А что компьютер говорит по этому поводу?

В.: Как это – «говорит»???

А.: *(Ха!)* Ну, что там написано?

В.: Написано «вронг пассворд».

А.: *(Ну-ну, еще бы…)* А-а-а-а… А вы пароль правильно набираете?

В.: Не знаю, я его не совсем помню.

А.: Какое имя пользователя?

В.: anatoly.

А.: Ладно, ставлю вам пароль… мммм… art25. Запомнили? *(Если опять не войдет – убью!)*

В.: Постараюсь. Спасибо. *(Вот дурак-то!)*

Конец разговора. Все!

На самом деле это упрощение ситуации, но в некоторых случаях такое может сработать. Какие ошибки допустил администратор? С его точки зрения – никаких. В подобных случаях редко спрашиваются имя, фамилия, должность звонящего, особенно если звонит девушка с приятным голосом (для этого и используются преобразователи голоса). Администраторы часто сталкиваются с забывчивостью пользователей, особенно если сотрудники редко «входят»

в систему. В таких случаях ответственное лицо старается побыстрее положить трубку, и ему хватает того, что пользователь знает свое имя входа в систему. Однако в этом случае взломщик уже знал некоторые сведения о своей цели. Рассмотрим пример с первоначальными нулевыми знаниями.

1. Выберем цель по телефонной книге – организацию, где есть телефон секретаря.

2. Звоним секретарю и узнаем имя персоны, с кем можно проконсультироваться по поводу некоторых проблем с работой системы.

3. Звоним любому другому человеку, чей номер телефона имеется в книге, предполагая, что он имеет доступ к системе.

4. Представляемся (разумеется, вымышленным именем) как помощник той персоны, имя которой мы узнали из первого звонка. Говорим, что в связи с перестановкой системы администратор дал задание поменять пароли всем пользователям.

5. Узнаем имя входа, прежний пароль, говорим новый пароль. Все!

6. В том случае, если доступ к системе происходит посредством телефонных линий, звоним секретарю, говорим, что не получается дозвониться до системы, и просим назвать правильный номер телефона.

В принципе этот пример немногим отличается от предыдущего, но есть большая вероятность получения доступа в систему вследствие оперирования в разговоре конкретными именами и должностями.

После того как взломщик получает доступ к системе в виде простого пользователя, ему не составляет большого труда получить полное право на нее с помощью тех способов, которые описаны в главе 9. Но можно и дальше развить СИ для получения привилегий администратора. Вот пример на UNIX-системе.

Пусть каким-либо образом взломщик узнал, что у администратора в переменную окружения PATH включена «.» (это значит выполнение программ из текущего каталога, многие так делают для удобства работы).

Звонок администратору.

Хакер: Здравствуйте, вы администратор?

Администратор: Да.

Х.: Извините, что отвлекаю. Не могли бы вы мне помочь?

А.: *(Ну что еще ему надо?)* Да, конечно.

Х.: Я не могу в своем каталоге выполнить команду ls.

А.: *(Как будто ему это надо!)* В каком каталоге?

Х.: /home/anatoly.

А.: *(Вот ведь глупый юзер!)* Сейчас посмотрю. *(Заходит в этот каталог и набирает команду ls, которая успешно выполняется и показывает наличие нормальных прав на каталог.)*

А.: Все у вас должно работать!

Х.: Хммм… Подождите. О! А теперь работает. Странно…

А.: *(Рррррр!!!)* Да? Хорошо!

Х.: Спасибо огромное. Еще раз извиняюсь, что помешал.

А.: *(Ну наконец!)* Да не за что. *(Отстань, противный!)* До свидания.

Конец разговора.

Заметили криминал? Вроде бы ничего особенного. Даже с точки зрения опытного администратора. Что же произошло на самом деле? В каталоге /home/anatoly среди множества других файлов лежал измененный вариант программы ls. Как раз его-то администратор и запустил. Все дело в том, что при выполнении этого файла у запускающего (администратора) имелись

все права на систему, и, соответственно, все программы, которые он запускает, могут делать с системой практически все, что угодно. Что было в этом файле, кроме возможности показывать список файлов в каталоге, теперь только взломщику и известно.

Разумеется, эти случаи годятся для организации со средним уровнем защиты. В банках или военных учреждениях наверняка так просто ничего не получится. Там могут спросить имя звонящего, его адрес, номер паспорта или предложат оставить номер телефона для последующего уведомления о смене пароля (для этого и нужна возможность использовать чужую линию, чего позволяют добиться офисные мини-АТС, которыми можно оперировать с удаленного терминала или из сети Internet). В таком случае взломщики обычно заранее собирают информацию о потенциальных жертвах. Как это делается? Пожалуйста, еще один пример из телефонных шуток.

Звонок на совершенно незнакомый номер.

Взломщик: Алло, извините, вас беспокоят с телефонной станции. Это номер такой-то?

Жертва: Да.

В.: У нас идет перерегистрация абонентов, не могли бы вы сообщить, на кого у вас зарегистрирован телефон? Имя, фамилию и отчество, пожалуйста.

Ж.: *(Говорит информацию.)*

В.: Спасибо! Так. секундочку. Хорошо, ничего не изменилось. А место работы?

Ж.: *(С некоторым сомнением называет, а если человек очень подозрительный, то спрашивает, зачем.)*

В.: Это сведения для новой телефонной книги. По вашему желанию можем внести не одно имя, а всех, кого можно найти по этому телефону.

Ж.: *(Тут с радостью называются имена всех членов семьи с их положением в ней, хотя это и не требовалось.)*

Информации уже достаточно для попытки взлома. Таким же образом становятся известными номера паспортов и т. д. После такого разговора можно звонить сотрудникам хозяина телефона от имени его родственников и получать дальнейшую информацию.

Еще один пример.

Взломщик: Алло, это приемная?

Жертва: Да.

В.: Это администрация сети. Мы сейчас меняли сетевую систему защиты. Необходимо проверить, все ли у вас нормально работает. Как вы обычно регистрируетесь в системе?

Ж.: Ввожу свои имя и пароль.

В.: Хорошо… Так… *(Пауза)* Какое имя?

Ж.: anna.

В.: Анна… *(Пауза)* Так… какой у вас раньше был пароль?

Ж.: ienb48.

В.: Та-а-а-ак… Хорошо. Попробуйте сейчас перерегистрироваться.

Ж.: *(Пауза)* Все нормально. Работает.

В.: Отлично. Спасибо!

Разумеется, в маленьких организациях, где все знают администратора, это не сработает, зато в больших есть пространство для применения своих способностей.

Вот как использовали СИ такие люди, как Кевин Митник и Роско:

«И Роско, и Кевин гордились своим умением общаться с людьми. На их взгляд, в любом разговоре можно было подчинить себе собеседника, если говорить авторитетным тоном зна-

тока, даже если в этой области ты ничего не смыслишь. Время от времени они названивали в отдел дистанционной связи какой-нибудь компании и недовольным начальственным голосом требовали объяснить, почему тот или иной номер АТС не удается набрать из города. И напуганный оператор объяснял им, как набрать интересующий их номер.

Обычно в таких случаях Кевин предпочитал импровизировать, полагаясь на свою интуицию, а Роско возвел свое умение разговаривать с людьми чуть ли не в ранг искусства. Он вел специальную записную книжку, куда вписывал имена и должности телефонисток и операторов разных фирм и их начальников. Там же он помечал, новички они или опытные работники, насколько хорошо информированы, расположены к разговорам или нет. Заносил он в книжку и сведения, так сказать, личного характера, добытые в течение долгих часов разговоров по телефону: увлечения, имена детей, любимые виды спорта и места, где они любят бывать в отпуске и по выходным» [5].

Конец ознакомительного фрагмента.