А. Лукацкий

АТАКИ НА ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Типы и объекты воздействия

Соблюдение мер безопасности – норма повседневной жизни. Все следуют определенным правилам, когда переходят дорогу, отправляются в путешествия, просто поздно возвращаются домой. Новой реалией современного мира, такой же его частью, как города и автомобили, стал и интенсивный информационный обмен. И вместе с появлением информационных систем возникли проблемы, связанные с информационной безопасностью. Видимо, в связи с новизной их окружает множество мифов и абсолютно неверных суждений – от полного пренебрежения возможной угрозой до страха собственной тени. От легенд о злобных хакерах, поджидающих за каждым узлом сети и проникающих в каждый байт до отсутствия в системе простейших средств антивирусной защиты.

Лучшее средство от мифов – информация. В статье рассказывается об основных видах атак в информационных компьютерных сетях, точках их приложения и способах защиты. А кто знает про опасность – тот уже наполовину неуязвим.

ОБРАТНАЯ СТОРОНА МЕДАЛИ

Развитие современных информационных технологий ведет к постепенному объединению автономных компьютеров и локальных сетей в единую корпоративную сеть организации. Помимо явных преимуществ такой переход несет и ряд проблем, с которыми приходится сталкиваться как специалистам служб безопасности, так и сотрудникам управлений автоматизации. Можно выделить три группы причин появления этих проблем.

Прежде всего, ***высока сложность и разнородность используемого программного и аппаратного обеспечения.*** Сегодня почти не встречаются сети, построенные на основе только одной сетевой операционной системы (ОС). Например, в российских организациях, на рабочих станциях применяют ОС MS DOS, Windows 95 или Windows NT, а в качестве сетевой операционной системы используют Novell Netware и Windows NT. Большое число конфигурационных параметров различных ОС и аппаратуры затрудняет эффективную настройку и эксплуатацию информационных систем.

Другой источник проблем – ***территориальная распределенность корпоративных сетей, большое число их узлов, следствие чего – отсутствие времени для контроля всех настроек.*** Уже не редкость, когда узлы, объединенные в корпоративную сеть, расположены не только в пределах одного города, но и региона. Сетевые администраторы не в состоянии лично и своевременно контролировать деятельность пользователей системы на всех узлах и правильность настроек программного и аппаратного обеспечения.

Немало неприятностей могут доставить проблемы, связанные с ***подключением к сети Интернет и возможностью доступа внешних пользователей (клиентов, партнеров и пр.) в корпоративную сеть***. Все это затрудняет определение границ сети и всех подключенных к ней пользователей – возрастает опасность несанкционированного доступа к защищаемой информации.

Информационная система становится объектом воздействия со стороны очень многих лиц, своих и чужих, авторизованных и нет, предпринимающих санкционированные, злонамеренные и ошибочные действия. В итоге растет уязвимость корпоративной сети. Для защиты применяют различные механизмы и средства обеспечения безопасности – межсетевые экраны, системы обнаружения атак, системы шифрования трафика, системы контроля "мобильного кода" (Java, ActiveX) и т.п. Однако чем совершеннее средства защиты, тем дороже они стоят. Поэтому крайне важно правильно выбрать конфигурацию системы защиты, а для этого необходимо представлять основные источники опасности, наиболее уязвимые точки системы и виды возможного вредоносного воздействия.

БОЛЕВЫЕ ТОЧКИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Как правило, иерархия информационной системы (ИС) любой компании включает четыре уровня (рис. 1):

- ✦ уровень прикладного программного обеспечения (ПО), отвечающий за взаимодействие с пользователем (текстовый редактор WinWord, редактор электронных таблиц Excel, почтовая программа Outlook и т.д.);
- ✦ уровень системы управления базами данных (СУБД) – хранение и обработка данных ИС (СУБД Oracle, MS SQL Server, Sybase и даже MS Access);

Представляем автора статьи

ЛУКАЦКИЙ Алексей Викторович. Руководитель отдела Internet-решений, Научно-инженерное предприятие "Информзащита", Москва.

(095) 289-8998, luka@infosec.ru

✦ уровень операционной системы – обслуживание СУБД и прикладного программного обеспечения (ОС Microsoft Windows NT, Sun Solaris, Novell Netware и т.п.);

✦ уровень сети, обеспечивающий взаимодействие узлов информационной системы (протоколы TCP/IP, IPS/SPX и SMB/NetBIOS).

Структура информационных систем большинства небольших компаний в России, независимо от видов их деятельности, достаточно стандартна (рис. 2). Рабочие станции функционируют под управлением ОС Windows 9x или Windows NT. На файловом сервере, где хранятся различные документы, дистрибутивы программного обеспечения, базы данных, 1С:Бухгалтерия и т.д. используют, Windows NT и Novell Netware. Управляет сетью компьютер (контроллер домена) с ОС Windows NT Server или Novell Netware. База данных SQL хранится на отдельном сервере под управлением MS SQL Server, хотя может быть и другое программное обеспечение (например, Oracle или Sybase).

Рис. 1. Иерархия информационной системы

Организация может использовать в работе сеть Интернет, причем не только для электронной почты и "хождения" по Web-серверам, – как правило, у фирмы есть свое "представительство" в Интернете, Web- и FTP-серверы на территории Интернет-провайдера. Корпоративная сеть связана с Интернетом посредством proxy-серверов MS Proxy Server или Novell BorderManager, которые блокируют доступ внешних пользователей во внутреннюю сеть. Связь с Интернет-провайдером реализуется с помощью Dial-up-соединения (необходимо дозвониться до провайдера и произвести аутентификацию – ввести имя и пароль) через модем.

Знакомая ситуация, не правда ли? По такому сценарию строятся практически все сети с выходом в Интернет. Причем все защитные функции, как правило, ограничиваются применением proxy-сервера. Поэтому злоумышленники располагают широчайшим спектром возможностей для вредоносного воздействия на любом уровне иерархии ИС (рис. 1). Например, получить несанкционированный доступ к финансовой информации в базе данных MS Access можно, попытавшись:

✦ прочесть записи БД из MS Excel, которые открывают доступ к записям MS Access (уровень прикладного ПО);

✦ получить нужные данные средствами СУБД MS Access (уровень СУБД);

✦ прочесть файлы базы данных с расширением .mdb непосредственно на уровне операционной системы;

✦ отправить по сети пакеты с запросами на получение необходимых данных от СУБД (уровень сети).

Наиболее критичные с точки зрения безопасности участки ИС – это:

✦ контроллер домена (primary и backup) под управлением Windows NT или Novell Netware;

✦ MS Proxy Server под управлением Windows NT или Novell Border Manager;

✦ почтовый сервер под управлением MS Exchange;

✦ файловые серверы под управлением Windows NT и Netware;

✦ сервер базы данных под управлением MS SQL Server;

✦ сеть передачи данных.

Кроме этого, подвержены атакам и менее критичные элементы – рабочие станции под управлением Windows 9x и Windows NT (рис. 2).

ВИДЫ АТАК

По статистике, опубликованной институтом SANS (System Administration, Networking and Security, www.sans.org), к наиболее часто используемым атакам можно отнести несанкционированный доступ к паролю и конфиденциальной информации, несанкционированное удаленное выполнение команд вследствие ошибок типа "переполнение буфера", нарушение прав доступа, атаки типа "отказ в обслуживании" и загрузка враждебного содержания (программ типа "троянский конь", мобильного кода Java и ActiveX, вирусов).

Несанкционированный доступ к паролю

Эта атака заключается в краже или подборе пароля законного пользователя ИС. Для нее уязвим любой компонент ИС. Первоначально злоумышленник может получить доступ к паролю пользователя с незначительными правами (например, guest), но его конечной целью является пароль администратора контроллера домена, что позволит воздействовать на все компоненты ИС. Пароль либо крадут (узнают без разрешения владельца), либо подбирают. Основные способы кражи пароля:

• ***Подсматривание за пользователями во время ввода пароля***. Вспомним классический пример – фильм "Хакеры", в кото-

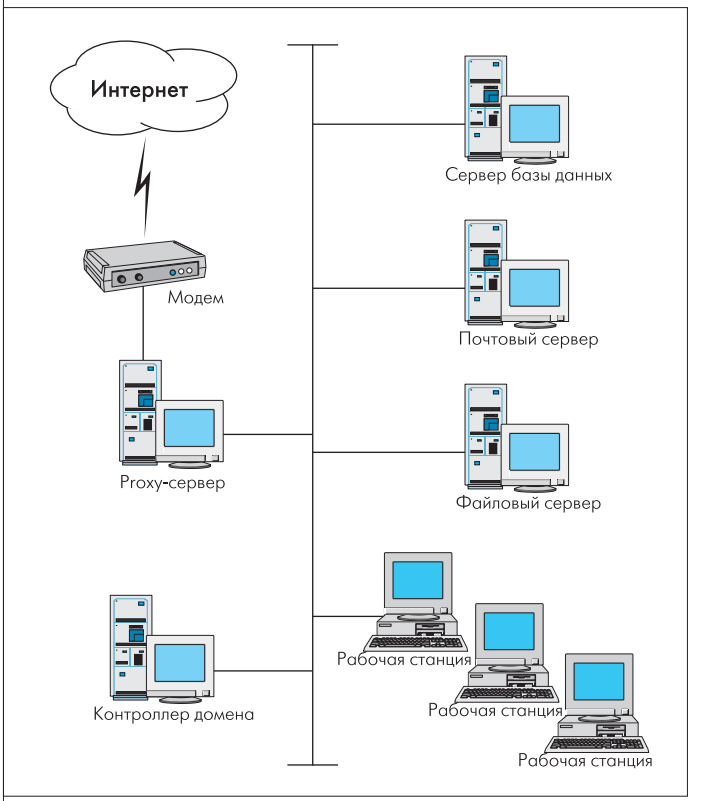

Рис. 2. Функциональная структура информационной системы

ром один из героев узнавал пароли, следя за движениями пальцев на клавиатуре. Для не обладающих подобными талантами существуют технические средства, например миниатюрные видеокамеры и режим покадрового просмотра. Во многих программах при вводе пароля его символы на экране заменяются звездочками. Но спасает это далеко не всегда, поскольку существуют свободно распространяемые программы, которые позволяют, скопировав замененный звездочками пароль в буфер обмена, восстановить его.

• ***Получение пароля из командной строки или командного файла,*** например, при выполнении командного файла или скрипта (сценария) сетевой аутентификации. Так, для аутентификации при удаленном управлении в Novell Netware в загрузочный файл AUTOEXEC.NCF включается команда LOAD REMOTE <пароль>. Злоумышленник может подсмотреть вводимый в открытом виде в командной строке пароль либо прочесть пароль из файла AUTOEXEC.NCF. Еще проще доступ к командным файлам в ОС Windows NT.

• ***Изучение "мусора" и иных источников (записных книжек, распечаток и т.п.).*** Этот путь к овладению паролем распространен гораздо шире, чем кажется.

• ***Кража внешнего носителя пароля*** (дискеты, таблетки "Touch Memory", смарт-карты и т.п.).

• ***Перехват пароля программной закладкой*** (например, "троянским конем" NetBus или BackOrifice) ***или в процессе передачи по каналу связи***. Последний вариант достаточно часто используется злоумышленниками, поскольку каналы связи трудно контролировать на всей их протяженности. Например, подключив модем в специальном режиме, можно перехватывать пароли аутентификации в сети Novell Netware или открыто передаваемые пароли в рамках протоколов Telnet, FTP, HTTP, SMTP и т.д.

Пароль не обязательно "подсматривать", его можно и подобрать. Иногда подбор происходит "вручную", на основе дополнительной информации о пользователе. Однако намного эффективнее автоматизированные методы. Например, программа L0phtCrack для Windows NT подбирает пароли как удаленно через сеть, так и локально. В последнем случае скорость подбора существенно возрастает (рис. 3).

От злоумышленников пароли можно защитить различными способами, начиная от запрета входа посторонних людей в помещения с вычислительной техникой или уничтожения всех бумаг и распечаток, и заканчивая различными техническими мерами. Для защиты от получения пароля из командной строки в Novell Netware в файл AUTOEXEC.NCF включается строка LOAD REMOTE -E <ключ>. В результате в командном файле хранится не пароль, а некий ключ, сам по себе доступа в систему не дающий.

Избежать перехвата пароля, передаваемого по каналам связи, поможет шифрование. Причем средства кодирования могут быть "встроенными" в операционную систему (команда SET ALLOW UNENCRYPTED PASSWORDS = OFF в Novell Netware) или дополнительными, как программа PGP или механизм HTTPS – защищенный HTTP-протокол. Для защиты от программ типа L0phtCrack необходимо шифровать сетевой трафик или запретить удаленный доступ к системному реестру Windows NT.

Несанкционированное выполнение команд

Данная атака, хотя и считается одной из самых распространенных, свою известность получила в связи с ОС Unix, которая в России пока массово не распространена. Однако известны случаи реализации этой атаки и для ОС Windows NT. Принцип атаки - использовать ошибки в операционных системах, проявляющиеся в том, что при переполнении входного буфера (например, при аутентификации) часть

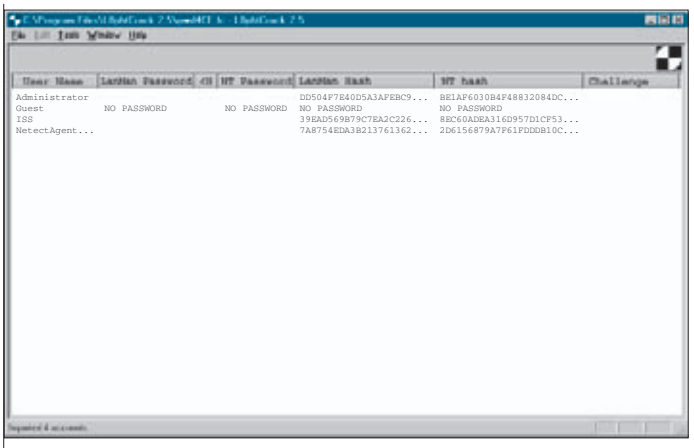

Рис. 3. Сеанс работы программы подбора паролей L0phtCrack

данных воспринимается как команда. Например, ранние версии Microsoft Internet Information Server (ПО Web-сервера) неправильно обрабатывали длинные URL (более 255 символов), что приводило к выполнению команд, задаваемых в таком URL. Реализоваться эта атака может на любом из компонентов информационной системы, за исключением сети передачи данных. Но наиболее часто ей подвергаются серверы под управлением ОС Unix или Web- и SMTP-сервера.

Для защиты от подобных атак необходимо периодически просматривать информационные бюллетени по безопасности, публикуемые различными организациями, например, X-Force (http:/xforce.iss.net). Так можно своевременно узнавать об обнаруженных "дырках" в программном обеспечении , которые позволяют использовать переполнение буфера. Однако в крупных территориально-распределенных сетях данный метод малоэффективен. В этом случае необходимо использовать средства анализа защищенности, которые ищут уязвимые места и устраняют их, или инструменты обнаружения атак [1].

Нарушение прав доступа

Превышение прав доступа – это самое распространенное нарушение политики безопасности. Неправильно заданные права доступа к ресурсам ИС (файлам, каталогам, логическим и сетевым дискам, модемам, компьютерам и т.д.) позволяют злоумышленнику или просто нерадивому сотруднику натворить немало бед. Например, неконтролируемое использование модемов сводит на нет применение таких защитных средств, как proxy-сервер и межсетевой экран (firewall). При несанкционированном доступе к исполняемым файлам или скриптам автозагрузки можно вольно или невольно внедрить в сеть закладку или вирус. Несколько лет назад была широко распространена ситуация, когда при помощи скрипта подключения к серверу Novell Netware на него внедрялся вирус OneHalf, в течение дня заражавший более 70% компьютеров всей организации. Наличие на контроллере домена Windows NT общедоступных (shared) ресурсов и неправильно заданные права доступа к ним могут привести к краже файла паролей пользователей ИС с соответствующими последствиями.

Данные атаки достаточно легко предотвратить или обнаружить при помощи продуманной конфигурации элементов ИС, а также встроенных в операционную систему защитных механизмов. Например, настройка прав доступа ко всем ресурсам компьютера, где установлен контроллер домена, позволит защититься от многих атак на уровне ОС, СУБД и прикладного ПО. Это можно сделать, например, при помощи программы User Manager, входящей в состав ОС Windows NT, или программ nwadmin, syscon, Filer в Novell Netware, а также вкладки Security подпункта Properties меню File программы Windows NT Explorer.

Для эффективной защиты также необходимо регистрировать все события в соответствующем журнале (Event Log для Windows NT или журналы аудита для Netware). Этот журнал следует просматривать не реже одного раза в сутки или настроить его таким образом, чтобы в нештатных ситуациях происходило оповещение администратора безопасности или сети.

Атаки типа "отказ в обслуживании"

Этот вид атак наиболее известен благодаря частому упоминанию в прессе. Характерный пример атак типа "отказ в обслуживании" (Denial of Service) – широко известные атаки WinNuke или SYN-Flood, которые сводятся к посылке нарушителем неправильно сформированного сетевого пакета или передаче большого числа специальных пакетов, обработка которых занимает все ресурсы контроллера домена, что блокирует обработку других запросов.

Рассмотрим принцип атаки SYN-Flood. Для связи между узлами сети по протоколу TCP устанавливается виртуальное соединение. При запросе на соединение один узел (например, клиент) направляет другому узлу (например, серверу) TCP-пакет с установленным флагом SYN (рис. 4). Сервер отвечает на это пакетом с установленными флагами SYN и ACK, и после получения от клиента подтверждения создается виртуальное соединение. В том случае, если подтверждение от клиента не пришло, сервер в течение некоторого времени ждет от него ответ, расходуя на это часть ресурсов. Атака SYN-Flood заключается в посылке большого числа SYN-пакетов на установление соединения без соответствующего подтверждения. В результате сервер выделяет слишком много ресурсов на несуществующие соединения и уже не может обрабатывать другие запросы – нарушается работоспособность узла.

Для защиты компонентов ИС от атак типа "отказ в обслуживании" могут применяться специальные системы обнаружения атак или межсетевые экраны. Пример средства обнаружения атак на уровне сети – система RealSecure компании ISS [1]. Она устанавливается на узел под управлением Windows NT или Solaris и не только обнаруживает все атаки в информационной системе, но и предотвращает их влияние на работу элементов ИС. Аналогичным образом действуют и межсетевые экраны, однако они защищают от меньшего числа атак.

Загрузка враждебного содержания

Под враждебным содержанием обычно понимаются программы типа "троянский конь", программы с мобильным кодом (Java и ActiveX), а также вирусы. Защита от вирусов – это тема отдельной статьи, поэтому основное внимание уделим первым двум типам атак.

Мобильный код сулит огромные возможности не только для построения более совершенных информационных систем, но и для вредоносного воздействия на них. Злоумышленник при помощи апплетов Java, управляющих элементов ActiveX или сценариев JavaScript способен получить доступ к конфиденциальной информации, модифицировать (нарушить или уничтожить) информацию при передаче ее по сети или на компьютере пользователя, нарушить работоспособность компьютера, несанкционированно использовать ресурсы компьютера, записать произвольные данные на локальный компьютер, наконец, просто досаждать пользователю и т.п.

Как средство для проведения атак мобильный код может быть реализован в виде:

- ✦ вируса, который вторгается в систему и уничтожает данные на локальных дисках, постоянно модифицируя свой код, что затрудняет его обнаружение и удаление;
- ✦ агента, перехватывающего пароли, номера кредитных карт и т.п.;
- ✦ программы, копирующей конфиденциальные файлы (деловая, финансовая информация и пр.).

Маскироваться такие программы могут под анимационные баннеры, интерактивные игры, звуковые файлы и т.п.

Наиболее часто (из-за простоты) мобильный код Java, ActiveX или JavaScript реализует атаки типа "отказ в обслуживании". Самые распространенные сценарии таких атак – создание высокоприоритетных процессов, выполняющих несанкционированные действия; генерация большого числа окон; захват значительного объема памяти и важных системных классов; загрузки процессора бесконечным циклом и т.п.

Ниже приведен пример HTML-страницы со сценарием на языке JavaScript. Стоит открыть такую страницу каким-либо броузером (Internet Explorer), как начинают циклически создаватся окна, которые невозможно закрыть. Для завершения цикла приходится выходить из броузера путем завершения задачи в Task Manager (для ОС Windows NT).

Пример атаки "отказ в обслуживании" при помощи мобильного кода

```
<HTML>
<HEAD>
<TITLE>Демонстрация атаки Denial of Service</TITLE>
</HEAD>
<BODY>
<CENTER>
<H1> Демонстрация атаки Denial of Service</H1>

<HR>Как дела?<BR>
<HR>
</CENTER>
<SCRIPT>
while(1){alert("Не все то золото, что блестит!")}
</SCRIPT>
</HTML>
```

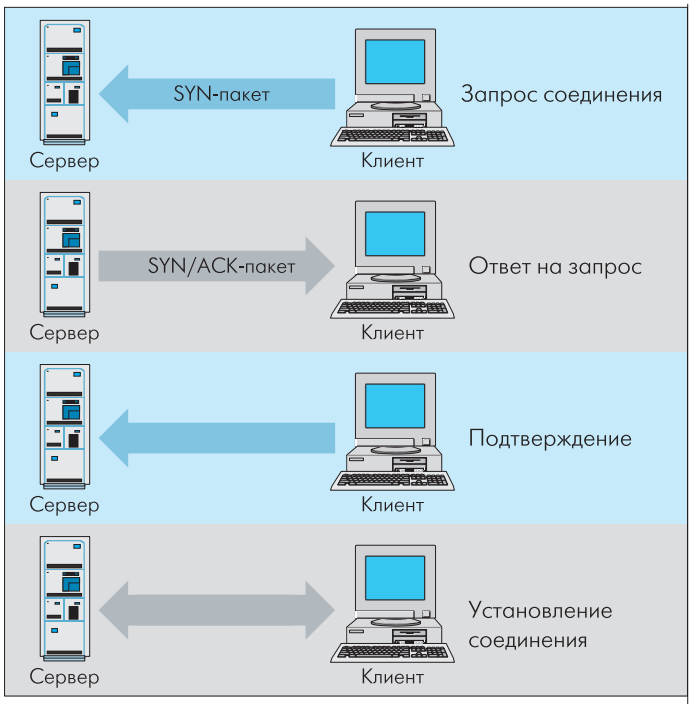

Рис. 4. Сценарий атаки SYN-Flood

Программы типа "троянский конь" сейчас у всех на слуху. Существует более 50 основных "троянских коней", которые выполняют огромное число функций, начиная от перехвата вводимой с клавиатуры информации и кражи паролей до удаленного управления узлом, на котором он установлен. Основная опасность такого рода программ заключается в том, что они работают незаметно (или почти незаметно) для пользователя. Недаром многие специалисты считают "троянских коней" разновидностью вирусов.

Название свое они получили за то, что внешне выглядят как привычная системная или прикладная (например, почтовый агент) программа. Однако кроме функций программы-прототипа "троянские кони" реализуют массу иных возможностей, например позволяют удаленному пользователю наблюдать все действия на компьютере с установленным "троянцем". При этом зачастую подменяются системные команды, такие как просмотр директории или списка выполняемых заданий – пользователь может долго не подозревать о том, что система взломана.

Российские провайдеры каждый день фиксируют попытки использования "троянцев", крадущих пароли не защищающих себя пользователей. Наиболее известными "троянскими конями" считаются Back Orifice и NetBus (рис. 5.). Эти две программы выполняют множество функций, и в некоторых организациях их даже используют как средство удаленного сетевого администрирования.

Самый простой механизм защиты от враждебного мобильного кода – правильная конфигурация узлов информационной системы. От многих проблем избавит запрет использования Java, ActiveX и JavaScript в броузерах на рабочих станциях. От "дырок" – ошибок в системе защиты программного обеспечения (броузеры, почтовые программы и т.д., особенно фирмы Microsoft) – спасает постоянное обновление программ при помощи "заплаток" (patch), которые регулярно публикуются фирмами-производителями ПО. Запрет несанкционированного изменения системного реестра не позволит многим "троянцам" запускаться на компьютере. В Интернете свободно распространяются программы для обнаружения и удаления многих из известных "троянцев", например NukeNabber или TrojanCleaner.

Кроме того, враждебный код обнаруживают и обезвреживают такие средства, как межсетевые экраны (блокировка применения Java и ActiveX), антивирусные системы (обнаружение программ типа "троянский конь"), системы контроля мобильного кода Java и ActiveX (например, продукты компаний Finjan, Security-7 Software или Digivity), системы обнаружения атак и анализа защищенности.

ОТКУДА ИСХОДИТ УГРОЗА?

Вопреки распространенным мифам о хакерах, наибольшую опасность представляют авторизованные пользователи (сотрудники, клиенты, партнеры и т.д.). До 75–80 % всех компьютерных инцидентов связано именно с теми, кому принято доверять. "Свои" пользователи по незнанию, ошибке или злому умыслу могут занести в информационную систему вирус, удалить тот или иной файл, или выполнить иные несанкционированные действия – что они регулярно и проделывают.

Что до хакеров, то, как ни странно, проблема заключается в том, что сегодняшний хакер в массе своей таковым не является – это не увлеченный фанатик, ведущий интеллектуальную борьбу с разработчиками средств защиты, а плохо образованный подросток 12–30 лет, сам ничего взломать не способный. Но он умеет запускать находящиеся в свободном доступе программы, которые сканируют сеть в поисках незащищенных серверов либо серверов с неустраненными "дырками" в защите. Найдя такой сервер, программа каким-либо образом воздействует на него, например внедряет "троянца". И все это происходит автоматически. Пишут программы-сканеры действительно специалисты, которые, однако, вашу сеть ломать не станут – недосуг (конечно, если ваше предприятие – не крупная финансовая компания, секретная лаборатория или министерство обороны). Беда, что таких программ достаточно много (обновляются по мере обнаружения новых "прорех" в ПО), немало и энтузиастов-ломателей. Поэтому корпоративная сеть может подвергнуться случайной, "сканирующей" атаке, что вовсе не уменьшает вред. Описан случай, когда при настройке был взломан подключенный к Интернету сервер. Его обнаружили и внедрили "троянца" за те 15 минут, когда он имел "дыры" в защите – уже был включен IP-роутинг, но не были доставлены новые "заплатки" [2]. За машиной никто специально не охотился, удачная атака – результат работы сканирующей программы.

Существует немало других источников опасности для ИС. Причем многие из них никак не связаны с предметной деятельностью предприятия и носят случайный характер. Поэтому не стоит полагаться на то, что информация в ИС фирмы не представляет для злоумышленников большой ценности. Отметим, что зачастую встроенные механизмы операционной системы не позволяют предотвра-

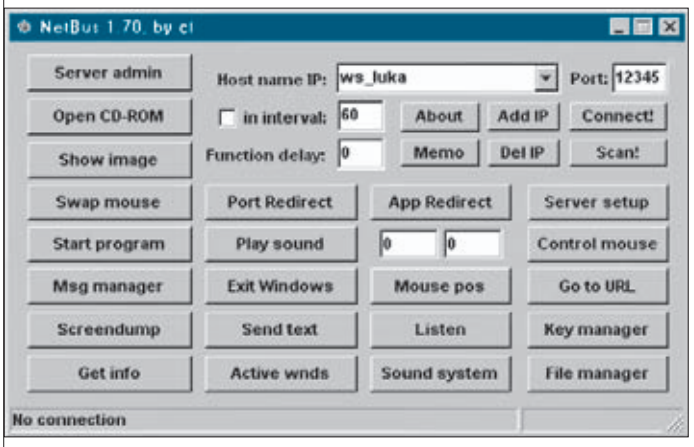

Рис. 5. Сеанс работы программы типа "троянский конь" NetBus

тить и даже обнаружить некоторые атаки. В этом случае необходимы дополнительные средства защиты. Из коммерческих российских средств можно назвать системы семейства SecretNet, разработанные Научно-инженерным предприятием "Информзащита" и обеспечивающие защиту от многих атак для ОС Windows 3.x/9x/NT, Novell Netware 3.x/4.x/5.0 и Unix.

Мы постарались рассказать о наиболее распространенных атаках и способах защиты от них. Необходимо еще раз отметить, что чисто техническими средствами решить задачу построения эффективной системы защиты невозможно. Необходим комплекс организационных, законодательных, физических и технических мер.❍

ЛИТЕРАТУРА

1. **Лукацкий А.** Системы обнаружения атак. Взгляд изнутри. – Электроника: НТБ, №5, 1999.
2. **Мошков М.** Безопасность для Интернет-дачников. – Журнал Интернет, №16.

Компании Ericsson и Intel объединяют усилия с целью разработки Интернет-устройств нового поколения

Корпорация Intel приступает к поставкам компании Ericsson высокопроизводительных модулей флэш-памяти нового поколения, предназначенных для сотовых телефонов. Эта акция началась в рамках достигнутого между фирмами соглашения об объединении усилий с целью разработки спецификации флэш-памяти, способной сохранять как программный код, так и различные данные (Web-страницы, сообщения электронной почты, голосовую информацию и даже музыку). Это необходимо для многих беспроводных устройств, например мобильных телефонов с доступом в Интернет.

По условиям договора Ericsson, как ведущий поставщик средств мобильной телефонии принимает на себя обязательство в течение трех лет приобретать модули флэш-памяти у Intel. Соглашение позволит компании Ericsson разработать и выпустить на рынок качественно новую продукцию, относящуюся к третьему поколению средств связи и телекоммуникаций. Речь, в частности, идет о беспроводных устройствах карманного формата, обеспечивающих голосовую связь и подключение к Интернету.

«Как производители, так и потребители получат новые, поистине колоссальные возможности с распространением преимуществ Интернета на средства мобильной телефонии и, в целом, беспроводной связи, а активное участие в разработке устройств беспроводного Интернета открывает перед Intel, без преувеличения, захватывающие перспективы», - отметил Рон Смит (Ron Smith), вице-президент корпорации и генеральный менеджер группы Intel по разработке беспроводных коммуникационных и вычислительных средств (Wireless Communications and Computing Group).

«Обширные знания и опыт, накопленные нами в таких смежных областях, как разработка сетей, системных решений и мобильных устройств, позволили компании Ericsson занять ведущие позиции в деле развертывания мобильной связи третьего поколения, - заявил вице-президент компании Ян Аренбринг (Jan Ahrenbring), руководитель службы маркетинга подразделения Ericsson по мобильным коммуникациям. – Сотрудничество Ericsson и Intel имеет для нас важнейшее значение, позволяя нам занять великолепные стартовые позиции в преддверии лавинообразного роста спроса на мобильные Интернет-устройства».

По сообщению фирм Intel и Ericsson