Содержание:

Введение

Одновременно с колоссальным ростом популярности Интернета возникает беспрецедентная опасность разглашения персональных данных, критически важных корпоративных ресурсов, государственных тайн и т.д. Каждый день хакеры подвергают угрозе эти ресурсы, пытаясь получить к ним доступ при помощи специальных атак, которые постепенно становятся, с одной стороны, более изощренными, а с другой — простыми в исполнении. Этому способствуют два основных фактора.

Во-первых, это повсеместное проникновение Интернета. Сегодня к Сети подключены миллионы устройств, и многие миллионы устройств будут подключены к Интернету в ближайшем будущем, поэтому вероятность доступа хакеров к уязвимым устройствам постоянно возрастает. Кроме того, широкое распространение Интернета позволяет хакерам обмениваться информацией в глобальном масштабе. Простой поиск по ключевым словам типа «хакер», «взлом», «hack», «crack» или «phreak» даст вам тысячи сайтов, на многих из которых можно найти вредоносные коды и способы их использования.

Во-вторых, это широчайшее распространение простых в использовании операционных систем и сред разработки. Данный фактор резко снижает уровень необходимых хакеру знаний и навыков. Раньше, чтобы создавать и распространять простые в использовании приложения, хакер должен был обладать хорошими навыками программирования. Теперь, чтобы получить доступ к хакерскому средству, нужно только знать IP-адрес нужного сайта, а для проведения атаки достаточно щелкнуть мышью.

Сетевая атака - некоторый набор действий (активность), имеющий целью произвести с компьютером (сервером) какие-то действия удаленно. Действия, обычно, являются нежелательными.

1. СЕТЕВЫЕ АТАКИ

Сетевые атаки столь же многообразны, как и системы, против которых они направлены. Некоторые атаки отличаются большой сложностью, другие по силам обычному оператору, даже не предполагающему, к каким последствиям может привести его деятельность. Для оценки типов атак необходимо знать некоторые ограничения, изначально присущие протоколу TPC/IP. Сеть Интернет создавалась для связи между государственными учреждениями и университетами с целью оказания помощи учебному процессу и научным исследованиям. Создатели этой сети не подозревали, насколько широкое распространение она получит. В результате в спецификациях ранних версий Интернет-протокола (IP) отсутствовали требования безопасности. Именно поэтому многие реализации IP являются изначально уязвимыми. Через много лет, после множества рекламаций (Request for Comments, RFC), наконец стали внедряться средства безопасности для IP. Однако ввиду того, что изначально средства защиты для протокола IP не разрабатывались, все его реализации стали дополняться разнообразными сетевыми процедурами, услугами и продуктами, снижающими риски, присущие этому протоколу. Далее мы кратко рассмотрим типы атак, которые обычно применяются против сетей IP, и перечислим способы борьбы с ними.

2. КЛАССИФИКАЦИЯ СЕТЕВЫХ АТАК

2.1 Сниффер пакетов

Сниффер пакетов представляет собой прикладную программу, которая использует сетевую карту, работающую в режиме promiscuous mode (в этом режиме все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки). При этом сниффер перехватывает все сетевые пакеты, которые передаются через определенный домен. В настоящее время снифферы работают в сетях на вполне законном основании. Они используются для диагностики неисправностей и анализа трафика. Однако ввиду того, что некоторые сетевые приложения передают данные в текстовом формате (Telnet, FTP, SMTP, POP3 и т.д.), с помощью сниффера можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли).

Перехват имен и паролей создает большую опасность, так как пользователи часто применяют один и тот же логин и пароль для множества приложений и систем. Многие пользователи вообще имеют единый пароль для доступа ко всем ресурсам и приложениям. Если приложение работает в режиме «клиент-сервер», а аутентификационные данные передаются по сети в читаемом текстовом формате, то эту информацию с большой вероятностью можно использовать для доступа к другим корпоративным или внешним ресурсам. Хакеры слишком хорошо знают и используют человеческие слабости (методы атак часто базируются на методах социальной инженерии). Они прекрасно представляют себе, что мы пользуемся одним и тем же паролем для доступа к множеству ресурсов, и потому им часто удается, узнав наш пароль, получить доступ к важной информации. В самом худшем случае хакер получает доступ к пользовательскому ресурсу на системном уровне и с его помощью создает нового пользователя, которого можно в любой момент использовать для доступа в Сеть и к ее ресурсам.

Снизить угрозу сниффинга пакетов можно с помощью следующих средств:

• Аутентификация. Сильные средства аутентификации являются важнейшим способом защиты от сниффинга пакетов. Под «сильными» мы понимаем такие методы аутентификации, которые трудно обойти. Примером такой аутентификации являются однократные пароли (One-Time Passwords, OTP). OTP — это технология двухфакторной аутентификации, при которой происходит сочетание того, что у вас есть, с тем, что вы знаете. Типичным примером двухфакторной аутентификации является работа обычного банкомата, который опознает вас, во-первых, по вашей пластиковой карточке, а во-вторых, по вводимому вами пин-коду. Для аутентификации в системе OTP также требуются пин-код и ваша личная карточка. Под «карточкой» (token) понимается аппаратное или программное средство, генерирующее (по случайному принципу) уникальный одномоментный однократный пароль. Если хакер узнает данный пароль с помощью сниффера, то эта информация будет бесполезной, поскольку в этот момент пароль уже будет использован и выведен из употребления. Отметим, что этот способ борьбы со сниффингом эффективен только в случаях перехвата паролей. Снифферы, перехватывающие другую информацию (например, сообщения электронной почты), не теряют своей эффективности.

• Коммутируемая инфраструктура. Еще одним способом борьбы со сниффингом пакетов в вашей сетевой среде является создание коммутируемой инфраструктуры. Если, к примеру, во всей организации используется коммутируемый Ethernet, хакеры могут получить доступ только к трафику,

поступающему на тот порт, к которому они подключены. Коммутируемая инфраструктура не устраняет угрозы сниффинга, но заметно снижает ее остроту.

• Антиснифферы. Третий способ борьбы со сниффингом заключается в установке аппаратных или программных средств, распознающих снифферы, работающие в вашей сети. Эти средства не могут полностью ликвидировать угрозу, но, как и многие другие средства сетевой безопасности, они включаются в общую систему защиты. Антиснифферы измеряют время реагирования хостов и определяют, не приходится ли хостам обрабатывать лишний трафик. Одно из таких средств, поставляемых компанией LOpht Heavy Industries, называется AntiSniff.

• Криптография. Этот самый эффективный способ борьбы со сниффингом пакетов хотя и не предотвращает перехвата и не распознает работу снифферов, но делает эту работу бесполезной. Если канал связи является криптографически защищенным, то хакер перехватывает не сообщение, а зашифрованный текст (то есть непонятную последовательность битов). Криптография Cisco на сетевом уровне базируется на протоколе IPSec, который представляет собой стандартный метод защищенной связи между устройствами с помощью протокола IP. К другим криптографическим протоколам сетевого управления относятся протоколы SSH (Secure Shell) и SSL (Secure Socket Layer).

2.2 IP-спуфинг

IP-спуфинг происходит в том случае, когда хакер, находящийся внутри корпорации или вне ее, выдает себя за санкционированного пользователя. Это можно сделать двумя способами: хакер может воспользоваться или IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам. Атаки IP-спуфинга часто являются отправной точкой для прочих атак. Классический пример — атака DoS, которая начинается с чужого адреса, скрывающего истинную личность хакера.

Как правило, IP-спуфинг ограничивается вставкой ложной информации или вредоносных команд в обычный поток данных, передаваемых между клиентским и серверным приложением или по каналу связи между одноранговыми устройствами. Для двусторонней связи хакер должен изменить все таблицы маршрутизации, чтобы направить трафик на ложный IP-адрес. Некоторые хакеры, однако, даже не пытаются получить ответ от приложений — если главная задача заключается в

получении от системы важного файла, то ответы приложений не имеют значения.

Если же хакеру удается поменять таблицы маршрутизации и направить трафик на ложный IP-адрес, он получит все пакеты и сможет отвечать на них так, как будто является санкционированным пользователем.

Угрозу спуфинга можно ослабить (но не устранить) с помощью перечисленных ниже мер.

• Контроль доступа. Самый простой способ предотвращения IP-спуфинга состоит в правильной настройке управления доступом. Чтобы снизить эффективность IP-спуфинга, настройте контроль доступа на отсечение любого трафика, поступающего из внешней сети с исходным адресом, который должен располагаться внутри вашей сети. Правда, это помогает бороться с IP-спуфингом, когда санкционированными являются только внутренние адреса; если же санкционированными являются и некоторые адреса внешней сети, данный метод становится неэффективным.

• Фильтрация RFC 2827. Вы можете пресечь попытки спуфинга чужих сетей пользователями вашей сети (и стать добропорядочным сетевым гражданином). Для этого необходимо отбраковывать любой исходящий трафик, исходный адрес которого не является одним из IP-адресов вашей организации. Данный тип фильтрации, известный под названием RFC 2827, может выполнять и ваш провайдер (ISP). В результате отбраковывается весь трафик, который не имеет исходного адреса, ожидаемого на определенном интерфейсе. К примеру, если ISP предоставляет соединение с IP-адресом 15.1.1.0/24, он может настроить фильтр таким образом, чтобы с данного интерфейса на маршрутизатор ISP допускался только трафик, поступающий с адреса 15.1.1.0/24. Отметим, что до тех пор, пока все провайдеры не внедрят этот тип фильтрации, его эффективность будет намного ниже возможной. Кроме того, чем дальше от фильтруемых устройств, тем труднее проводить точную фильтрацию. Например, фильтрация RFC 2827 на уровне маршрутизатора доступа требует пропуска всего трафика с главного сетевого адреса (10.0.0.0/8), тогда как на уровне распределения (в данной архитектуре) можно ограничить трафик более точно (адрес — 10.1.5.0/24).

Наиболее эффективный метод борьбы с IP-спуфингом — тот же, что и в случае со сниффингом пакетов: необходимо сделать атаку абсолютно неэффективной. IP-спуфинг может функционировать только при условии, что аутентификация происходит на базе IP-адресов. Поэтому внедрение дополнительных методов

аутентификации делает подобные атаки бесполезными. Лучшим видом дополнительной аутентификации является криптографическая. Если она невозможна, хорошие результаты может дать двухфакторная аутентификация с использованием одноразовых паролей.

2.3 Отказ в обслуживании(DoS)

Denial of Service (DoS), без сомнения, является наиболее известной формой хакерских атак. Кроме того, против атак такого типа труднее всего создать стопроцентную защиту.

Среди хакеров атаки DoS считаются детской забавой, а их применение вызывает презрительные усмешки, поскольку для организации DoS требуется минимум знаний и умений.

Тем не менее именно простота реализации и огромные масштабы причиняемого вреда привлекают к DoS пристальное внимание администраторов, отвечающих за сетевую безопасность. Если вы хотите больше узнать об атаках DoS, вам следует рассмотреть их наиболее известные разновидности, а именно:

TCP SYN Flood;

Ping of Death;

Tribe Flood Network (TFN) и Tribe Flood Network 2000 (TFN2K);

Trinco;

Stacheldracht;

Trinity.

рекрасным источником информации по вопросам безопасности является группа экстренного реагирования на компьютерные проблемы (Computer Emergency Response Team, CERT), опубликовавшая отличную работу по борьбе с атаками DoS. Эту работу можно найти на сайте www.cert.org/tech_tips/denial_of_service.html. Атаки DoS отличаются от атак других типов.

Они не нацелены ни на получение доступа к вашей сети, ни на получение из этой сети какой-либо информации, но атака DoS делает вашу сеть недоступной для

обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения.

В случае использования некоторых серверных приложений (таких как Web-сервер или FTP-сервер) атаки DoS могут заключаться в том, чтобы занять все соединения, доступные для этих приложений, и держать их в занятом состоянии, не допуская обслуживания рядовых пользователей. В ходе атак DoS могут использоваться обычные Интернет-протоколы, такие как TCP и ICMP (Internet Control Message Protocol).

Большинство атак DoS рассчитано не на программные ошибки или бреши в системе безопасности, а на общие слабости системной архитектуры. Некоторые атаки сводят к нулю производительность сети, переполняя ее нежелательными и ненужными пакетами или сообщая ложную информацию о текущем состоянии сетевых ресурсов.

Данный тип атак трудно предотвратить, так как для этого требуется координация действий с провайдером. Если не остановить у провайдера трафик, предназначенный для переполнения вашей сети, то сделать это на входе в сеть вы уже не сможете, поскольку вся полоса пропускания будет занята. Когда атака данного типа проводится одновременно через множество устройств, мы говорим о распределенной атаке DoS (distributed DoS, DDoS).

Угроза атак типа DoS может быть снижена тремя способами:

• Функции антиспуфинга. Правильная конфигурация функций антиспуфинга на ваших маршрутизаторах и межсетевых экранах поможет снизить риск DoS. Эти функции как минимум должны включать фильтрацию RFC 2827. Если хакер не сможет замаскировать свою истинную личность, он вряд ли решится провести атаку.

• Функции анти-DoS. Правильная конфигурация функций анти-DoS на маршрутизаторах и межсетевых экранах способна ограничить эффективность атак. Эти функции часто ограничивают число полуоткрытых каналов в любой момент времени.

• Ограничение объема трафика (traffic rate limiting). Организация может попросить провайдера (ISP) ограничить объем трафика. Этот тип фильтрации позволяет ограничить объем некритического трафика, проходящего по вашей сети. Типичным примером является ограничение объемов трафика ICMP, который используется

только для диагностических целей. Атаки (D)DoS часто используют ICMP.

2.4 Парольные атаки

Хакеры могут проводить парольные атаки с помощью целого ряда методов, таких как простой перебор (brute force attack), троянский конь, IP-спуфинг и сниффинг пакетов. Хотя логин и пароль зачастую можно получить при помощи IP-спуфинга и сниффинга пакетов, хакеры нередко пытаются подобрать пароль и логин, используя для этого многочисленные попытки доступа. Такой подход носит название простого перебора (brute force attack).

Часто для такой атаки используется специальная программа, которая пытается получить доступ к ресурсу общего пользования (например, к серверу). Если в результате хакеру предоставляется доступ к ресурсам, то он получает его на правах обычного пользователя, пароль которого был подобран. Если этот пользователь имеет значительные привилегии доступа, хакер может создать себе «проход» для будущего доступа, который будет действовать, даже если пользователь изменит свои пароль и логин.

Еще одна проблема возникает, когда пользователи применяют один и тот же (пусть даже очень хороший) пароль для доступа ко многим системам: к корпоративной, персональной и к системам Интернета. Поскольку устойчивость пароля равна устойчивости самого слабого хоста, то хакер, узнавший пароль через этот хост, получает доступ ко всем остальным системам, где используется тот же пароль.

Парольных атак можно избежать, если не пользоваться паролями в текстовой форме. Одноразовые пароли и/или криптографическая аутентификация могут практически свести на нет угрозу таких атак. К сожалению, не все приложения, хосты и устройства поддерживают вышеуказанные методы аутентификации.

При использовании обычных паролей старайтесь придумать такой, который было бы трудно подобрать. Минимальная длина пароля должна быть не менее восьми символов. Пароль должен включать символы верхнего регистра, цифры и специальные символы (#, %, $ и т.д.). Лучшие пароли трудно подобрать и трудно запомнить, что вынуждает пользователей записывать их на бумаге. Чтобы избежать этого, пользователи и администраторы могут использовать ряд последних технологических достижений.

Так, например, существуют прикладные программы, шифрующие список паролей, который можно хранить в карманном компьютере. В результате пользователю нужно помнить только один сложный пароль, тогда как все остальные будут надежно защищены приложением. Для администратора существует несколько методов борьбы с подбором паролей. Один из них заключается в использовании средства L0phtCrack, которое часто применяют хакеры для подбора паролей в среде Windows NT. Это средство быстро покажет вам, легко ли подобрать пароль, выбранный пользователем. Дополнительную информацию можно получить по адресу http://www.l0phtcrack.com/.

2.5 Атаки типа Man-in-the-Middle

Для атаки типа Man-in-the-Middle хакеру нужен доступ к пакетам, передаваемым по сети. Такой доступ ко всем пакетам, передаваемым от провайдера в любую другую сеть, может, к примеру, получить сотрудник этого провайдера. Для атак данного типа часто используются снифферы пакетов, транспортные протоколы и протоколы маршрутизации. Атаки проводятся с целью кражи информации, перехвата текущей сессии и получения доступа к частным сетевым ресурсам, для анализа трафика и получения информации о сети и ее пользователях, для проведения атак типа DoS, искажения передаваемых данных и ввода несанкционированной информации в сетевые сессии.

Эффективно бороться с атаками типа Man-in-the-Middle можно только с помощью криптографии. Если хакер перехватит данные зашифрованной сессии, у него на экране появится не перехваченное сообщение, а бессмысленный набор символов. Отметим, что если хакер получит информацию о криптографической сессии (например, ключ сессии), то это может сделать возможной атаку Man-in-the-Middle даже в зашифрованной среде.

2.6 Сетевая разведка

Сетевой разведкой называется сбор информации о сети с помощью общедоступных данных и приложений. При подготовке атаки против какой-либо сети хакер, как правило, пытается получить о ней как можно больше информации. Сетевая разведка проводится в форме запросов DNS, эхо-тестирования и сканирования портов. Запросы DNS помогают понять, кто владеет тем или иным доменом и какие

адреса этому домену присвоены. Эхо-тестирование адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты реально работают в данной среде. Получив список хостов, хакер использует средства сканирования портов, чтобы составить полный список услуг, поддерживаемых этими хостами. И наконец, хакер анализирует характеристики приложений, работающих на хостах. В результате он добывает информацию, которую можно использовать для взлома.

Полностью избавиться от сетевой разведки невозможно. Если, к примеру, отключить эхо ICMP и эхо-ответ на периферийных маршрутизаторах, то вы избавитесь от эхо-тестирования, но потеряете данные, необходимые для диагностики сетевых сбоев. Кроме того, сканировать порты можно и без предварительного эхо-тестирования — просто это займет больше времени, так как сканировать придется и несуществующие IP-адреса. Системы IDS на уровне сети и хостов обычно хорошо справляются с задачей уведомления администратора о ведущейся сетевой разведке, что позволяет лучше подготовиться к предстоящей атаке и оповестить провайдера (ISP), в сети которого установлена система, проявляющая чрезмерное любопытство.

• пользуйтесь самыми свежими версиями операционных систем и приложений и самыми последними коррекционными модулями (патчами);

• кроме системного администрирования, пользуйтесь системами распознавания атак (IDS) — двумя взаимодополняющими друг друга технологиями IDS:

- сетевая система IDS (NIDS) отслеживает все пакеты, проходящие через определенный домен. Когда система NIDS видит пакет или серию пакетов, совпадающих с сигнатурой известной или вероятной атаки, она генерирует сигнал тревоги и/или прекращает сессию;

- хост-система IDS (HIDS) защищает хост с помощью программных агентов. Эта система борется только с атаками против одного хоста.

В своей работе системы IDS пользуются сигнатурами атак, которые представляют собой профили конкретных атак или типов атак. Сигнатуры определяют условия, при которых трафик считается хакерским. Аналогами IDS в физическом мире можно считать систему предупреждения или камеру наблюдения. Самым большим недостатком IDS является их способность генерировать сигналы тревоги. Чтобы минимизировать количество ложных сигналов тревоги и добиться корректного функционирования системы IDS в сети, необходима тщательная настройка этой системы.

2.7 Переадресация портов

Переадресация портов представляет собой разновидность злоупотребления доверием, когда взломанный хост используется для передачи через межсетевой экран трафика, который в противном случае был бы обязательно отбракован.

Представим себе межсетевой экран с тремя интерфейсами, к каждому из которых подключен определенный хост. Внешний хост может подключаться к хосту общего доступа (DMZ), но не к тому, что установлен с внутренней стороны межсетевого экрана.

Хост общего доступа может подключаться и к внутреннему, и к внешнему хосту. Если хакер захватит хост общего доступа, он сможет установить на нем программное средство, перенаправляющее трафик с внешнего хоста прямо на внутренний.

Хотя при этом не нарушается ни одно правило, действующее на экране, внешний хост в результате переадресации получает прямой доступ к защищенному хосту.

Примером приложения, которое может предоставить такой доступ, является netcat. Более подробную информацию можно получить на сайте http://www.avian.org.

Основным способом борьбы с переадресацией портов является использование надежных моделей доверия (см. предыдущий раздел). Кроме того, помешать хакеру установить на хосте свои программные средства может хост-система IDS (HIDS).

2.8 Несанкционированный доступ

Несанкционированный доступ не может быть выделен в отдельный тип атаки, поскольку большинство сетевых атак проводятся именно ради получения несанкционированного доступа.

Чтобы подобрать логин Telnet, хакер должен сначала получить подсказку Telnet на своей системе. После подключения к порту Telnet на экране появляется сообщение «authorization required to use this resource» («Для пользования этим ресурсом нужна авторизация»). Если после этого хакер продолжит попытки доступа, они будут

считаться несанкционированными. Источник таких атак может находиться как внутри сети, так и снаружи.

Способы борьбы с несанкционированным доступом достаточно просты. Главным здесь является сокращение или полная ликвидация возможностей хакера по получению доступа к системе с помощью несанкционированного протокола.

В качестве примера можно рассмотреть недопущение хакерского доступа к порту Telnet на сервере, который предоставляет Web-услуги внешним пользователям. Не имея доступа к этому порту, хакер не сможет его атаковать. Что же касается межсетевого экрана, то его основной задачей является предотвращение самых простых попыток несанкционированного доступа.

сетевой протокол вирус сниффер

2.9 Вирусы и приложения типа «троянский конь»

Рабочие станции конечных пользователей очень уязвимы для вирусов и троянских коней. Вирусами называются вредоносные программы, которые внедряются в другие программы для выполнения определенной нежелательной функции на рабочей станции конечного пользователя.

В качестве примера можно привести вирус, который прописывается в файле command.com (главном интерпретаторе систем Windows) и стирает другие файлы, а также заражает все другие найденные им версии command.com.

Троянский конь — это не программная вставка, а настоящая программа, которая на первый взгляд кажется полезным приложением, а на деле исполняет вредную роль.

Примером типичного троянского коня является программа, которая выглядит, как простая игра для рабочей станции пользователя. Однако пока пользователь играет в игру, программа отправляет свою копию по электронной почте каждому абоненту, занесенному в адресную книгу этого пользователя. Все абоненты получают по почте игру, вызывая ее дальнейшее распространение.

Борьба с вирусами и троянскими конями ведется с помощью эффективного антивирусного программного обеспечения, работающего на пользовательском уровне и, возможно, на уровне сети. Антивирусные средства обнаруживают

большинство вирусов и троянских коней и пресекают их распространение.

Получение самой свежей информации о вирусах поможет бороться с ними более эффективно. По мере появления новых вирусов и троянских коней предприятие должно устанавливать новые версии антивирусных средств и приложений.

2.10 Атаки на уровне приложений

Атаки на уровне приложений могут проводиться несколькими способами. Самый распространенный из них — использование хорошо известных слабостей серверного программного обеспечения (sendmail, HTTP, FTP). Используя эти слабости, хакеры могут получить доступ к компьютеру от имени пользователя, работающего с приложением (обычно это бывает не простой пользователь, а привилегированный администратор с правами системного доступа). Сведения об атаках на уровне приложений широко публикуются, чтобы дать администраторам возможность исправить проблему с помощью коррекционных модулей (патчей). К сожалению, многие хакеры также имеют доступ к этим сведениям, что позволяет им совершенствоваться.

Главная проблема при атаках на уровне приложений заключается в том, что хакеры часто пользуются портами, которым разрешен проход через межсетевой экран. К примеру, хакер, эксплуатирующий известную слабость Web-сервера, часто использует в ходе атаки TCP порт 80. Поскольку web-сервер предоставляет пользователям Web-страницы, то межсетевой экран должен обеспечивать доступ к этому порту. С точки зрения межсетевого экрана атака рассматривается как стандартный трафик для порта 80.

Полностью исключить атаки на уровне приложений невозможно. Хакеры постоянно открывают и публикуют в Интернете новые уязвимые места прикладных программ. Самое главное здесь — хорошее системное администрирование. Вот некоторые меры, которые можно предпринять, чтобы снизить уязвимость для атак этого типа:

• читайте лог-файлы операционных систем и сетевые лог-файлы и/или анализируйте их с помощью специальных аналитических приложений;

• подпишитесь на услуги по рассылке данных о слабых местах прикладных программ: Bugtrad (http://www.securityfocus.com) и CERT (http://www.cert.com);

ЗАКЛЮЧЕНИЕ

И так, в данной работе, мы ознакомились, какие разновидные бывают сетевые атаки, узнали их уязвимые места и способы их устранения, либо предотвращения. Стоит задуматься, о безопасности своего компьютера, так как никто не может обезопасить свой компьютер, как сам пользователь, а зная врага в лицо, можно предотвратить все угрозы со стороны сетевых атак.

Не желательно недооценивать хакеров в наше время, как говориться «К любой двери есть запасной ключ», так и к любой информации есть дополнительные ходы её получения, но затруднить либо практически предотвратить её получение можно, стоит лишь постараться.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. Ральников М.А. Повышение безопасности среды передачи данных в интегрированных системах управления предприятиями. Автореферат. - Кострома: РИО КГТУ, 2004.

2. Лукацкий А.В. Обнаружение атак. - СПб.: «БХВ-Петербург», 2001.

3. Кадер М. Типы сетевых атак, их описания, средства борьбы// Cisco.

4. Windows под прицелом// Security Lab, декабрь 2004.

5. http://lagman-join.narod.ru/spy/CNEWS/cisco_attacks.html

6. http://ru.wikipedia.org/wiki/