Костюкова Нина Ивановна

БЕЗОПАСНОСТЬ В ОПЕРАЦИОННЫХ СИСТЕМАХ, СЕТЕВАЯ БЕЗОПАСНОСТЬ

Адрес статьи: www.gramota.net/materials/1/2011/7/13.html

Источник

Альманах современной науки и образования

Тамбов: Грамота, 2011. № 7 (50). С. 57-61. ISSN 1993-5552.

Адрес журнала: www.gramota.net/editions/1.html

Содержание данного номера журнала: www.gramota.net/materials/1/2011/7/

Комплексная стратегия защиты

Антивирус не убережет вас от хакерской атаки, так же как ***firewall*** не умеет искать вирусы, и оба они бессильны перед ***spyware***. Для обеспечения полной компьютерной безопасности необходимо использовать комплексную систему защиты: ***Antivirus + Firewall + Antispyware***.

Существуют системы безопасности, сделанные по принципу «все в одном». Одним из лучших представителей этого класса является ***Panda Security***. Однако, по данным сайта ***www.antivirus.ru***, за период с 03.2008 по 02.2009 г. ***Panda*** пропустила 125 вирусов из 283. Результат оставляет желать много лучшего.

Так же, при выборе антивируса не стоит забывать о том, что некоторые вирусы пишутся под определенный антивирус. К примеру, российские хакеры очень «любят» антивирус Касперского и ***DrWeb***.

Предлагаемая система защиты:

Antivirus: ***BitDefender*** либо ***A-SQUARED*** (есть бесплатная версия).

Firewall: ***Outpost firewall***.

Antispyware: ***Spyware Terminator*** (программа бесплатна, в некоторых случаях может заменить ***firewall***).

A-SQUARED

Бесплатное антивирусное решение ***a-squared Free Edition***, которое разрабатывает немецкая компания ***EMSI Software GmbH***, позволяет удалять с компьютера разного рода вредоносные программы, к которым относятся шпионы, рекламные программы, трояны, руткиты, звонилки и прочее. Бесплатная редакция включает в себя только сканер, которым вы сможете проверить свой компьютер и удалить вредоносные программы.

Outpost firewall

Персональный файрволл, проще говоря - программа для защиты компьютера от хакерских атак из Интернета. Кроме этого, Аутпост обеспечивает блокировку загрузки рекламы и активного содержимого вебстраниц, а тем самым - их более быструю загрузку.

С сайта разработчика можно скачать большое и подробное «Руководство пользователя» и не очень большое, но тоже полезное «Приступаем к работе» (оба документа - на русском языке). Стоимость 699 р.

Без регистрации ***Agnitum Outpost Firewall PRO*** работает 30 дней.

Spyware Terminator

Программа для обнаружения шпионских модулей и обеспечения компьютерной безопасности. ***Spyware Terminator*** может обнаружить и удалить практически все виды вредоносных программ. Доступно несколько видов сканирования: быстрое, полное и пользовательское. При полной проверке файлы проверяются наиболее тщательно. Выбрав свои персональные установки, можно найти оптимальный режим сканирования, наиболее подходящий пользователю по скорости и эффективности. Встроенная система безопасности включает защиту приложений и системы, а также ведет мониторинг утилит, непосредственно взаимодействующих с сетью. Таким образом, можно предотвратить заражение компьютера вредоносными программами и некоторыми вирусами. Тут имеется функция восстановления начальных настроек операционной системы, анализ подозрительных файлов и удаление защищенных файлов. Программа бесплатна.

УДК 519.6

Нина Ивановна Костюкова
Институт вычислительной математики и математической геофизики СО РАН

БЕЗОПАСНОСТЬ В ОПЕРАЦИОННЫХ СИСТЕМАХ, СЕТЕВАЯ БЕЗОПАСНОСТЬ©

Сетевые операционные системы

В компьютерных сетях персональные компьютеры могут взаимодействовать с другими сетевыми устройствами посредством кабельной системы и устройства связи. Однако одного аппаратного обеспечения недостаточно для работы сети. Для организации безопасного совместного использования файлов и оборудования серверам и рабочим станциям нужна операционная система (ОС), а для обмена информацией внутри сети требуется *протокол* (или язык), принятый в качестве стандарта.

Компьютерные сети - это нечто более сложное, чем группа ПК, соединенных кабелями и устройствами связи. Основная задача компьютерных сетей состоит в том, чтобы обеспечить совместное использование ресурсов (приложений, файлов, сообщений, принтеров, сканеров и так далее) между этими ПК. Такое совместное использование требует *операционной системы* (программного обеспечения), способной управлять множеством файлов и устройств, существующих в рамках этой компьютерной сети, и в то же время обеспечивать защиту этих ресурсов от несанкционированного использования. В этом заключается роль сетевой операционной системы (СОС).

Операционная система - «душа» любой компьютерной системы - в принципе является очень большой и сложной программой. Так что многие слабости программ присущи и операционным системам.

Однако есть ряд качеств, которые заставляют выделить обеспечения безопасности операционных систем в особую категорию.

Прежде всего операционная система часто содержит ряд встроенных механизмов, прямо или косвенно влияющих на безопасность всех программ и данных, работающих и обрабатываемых в среде данной операционной системы. Помимо этого, размер и сложность операционной системы как программы делает качественно более сложной атаку на поражение операционной системы. Чтобы испортить настроение администратору системы, вовсе не обязательно специально разрабатывать одну из ловушек. Нанести серьезный ущерб системе - и тем самым нарушить ее безопасность - можно и с помощью самых обычных программ и утилит. Например, удалить важный для кого-то файл можно с помощью одной команды операционной системы. Можно вообще отформатировать все доступные носители с помощью стандартной системной утилиты, уничтожив тем самым всю хранившуюся на них информацию и даже саму систему. Прочитать данные - то есть, которые вам читать не положено, - легче всего с помощью текстового редактора. Таким образом, мы подошли к одной из центральных проблем в обеспечении безопасности: проблеме несанкционированного (неавторизованного) доступа и способам его предотвращения. Вся проблема заключается в обеспечении такого порядка работы, при котором систему мог бы использовать только тот, кому ее разрешено использовать; чтобы каждый законный пользователь только со «своими» данными и не мог исказить, прочитать или удалить из системы данные, принадлежащие другому пользователю (если на то нет согласия хозяина); чтобы каждый законный пользователь мог выполнять только те операции, которые ему разрешено выполнять администратором системы. Вполне естественным является стремление не допустить работы в системе посторонних лиц: вы же не пускаете случайных прохожих в свой дом. Не менее естественно желание пользователей иметь гарантии, что их личные данные никто по ошибке или с умыслом не удалит, не исказит, не прочитает и так далее.

Средства поддержки сетевого режима

Прежде всего нужно понять способ, каким СОС обеспечивают поддержку сетей. Некоторые версии СОС просто добавляют сетевые компоненты поверх той операционной системы, которая установлена в персональном компьютере, тогда как другие версии полностью интегрируют сетевую поддержку в операционную систему компьютера, поэтому наличие автономной операционной системы в этом случае не требуется. Наверное, операционные системы *NetWare 4.x, 5x* фирмы *Novell* являются самыми известными и распространенными примерами СОС, в которых средства поддержки сетевого режима в клиентском компьютере добавляются поверх уже установленной ОС. Это означает, что настольному компьютеру необходимы обе операционные системы, для того чтобы он мог выполнять как внутренние, так и системные функцию.

Сервера

Основными компонентами любой информационной сети являются ***сервера*** и ***рабочие станции***. Сервера представляют информационные или вычислительные ресурсы, на рабочих станциях работает персонал. В принципе любая ЭВМ в сети может быть одновременно и сервером и рабочей станцией - в этом случае к ней применимы описания атак, посвященные и серверам и рабочим станциям. Основными задачами серверов являются хранение и представление доступа к информации и некоторые виды сервисов. Следовательно, и все возможные цели злоумышленников можно классифицировать как:

- получение доступа к информации;
- получение несанкционированного доступа к услугам;
- попытка вывода из рабочего режима определенного класса услуг;
- попытка изменения информации или услуг, как вспомогательный этап какой-либо более крупной атаки.

Проблема получения несанкционированного доступа к услугам принимает чрезвычайно разнообразные формы и основывается в основном на ошибках или недокументированных возможностях самого программного обеспечения, предоставляющего подобные услуги.

А вот проблема вывода из строя (нарушения нормального функционирования сервисов) довольно актуальна в современном компьютерном мире. Класс подобных атак получил название атака «отказ в сервисе» (англ. *Deny of service - DoS*). Атака «отказ в сервисе» может быть реализована на целом диапазоне уровней: ***физическом, канальном, сетевом, сеансовом***.

Изменение информации или услуг как часть более крупномасштабной атаки является также очень важной проблемой в защите серверов. В случае, если на сервере хранятся пароли пользователей или какие-либо данные, которые могут позволить злоумышленнику, или какие-либо данные, которые могут позволить злоумышленнику, изменив их, войти в систему (например, сертификаты ключей), то естественно, сама атака на систему начнется с атаки на подобный сервер. В качестве серверов услуг, наиболее часто подвергающимся модификации, следует назвать *DNS*-сервера.

DNS-служба (англ. *Domain Name System* - служба доменных имен) в сетях *Intra-* и *Internet* отвечает за сопоставление «произносимых» и легко запоминаемых доменных имен (например, *www.intel.com* или *mail.metacom.ru*) к их *IP*-адресам (например, 165.140.12.200 или 194.186.106.26). Пакеты между станциями всегда передаются только на основании *IP*-адресов (***маршрутизаторы*** ориентируются только на их значения при выборе направления отправки пакета - доменное имя вообще не включается в отправляемый пакет), а служба *DNS* была создана в основном для удобства пользователей сети. Как следствие и во многих сетевых программах имея удаленного компьютера для большей гибкости или для удобства операторов заносится не в

виде 4-байтового *IP*-адреса, а в виде доменного имени. Да, действительно, два указанных преимущества будут достигнуты в этом случае, а вот безопасность пострадает.

Дело в том, что, если злоумышленнику удастся заполучить права доступа к *DNS*-серверу, обслуживающему данный участок сети, то он вполне может изменить программу *DNS*-сервису. Обычно заполучить права доступа к *DNS*-серверу, обслуживающему данный участок сети, то он вполне может изменить программу *DNS*-сервиса. Обычно изменение делается таким образом, чтобы по некоторым видам запросов вместо правильного *IP*-адреса клиенту выдавался *IP*-адрес какой-либо вспомогательной машины злоумышленника, а все остальные запросы обрабатывались корректно. Это дает возможность изменять путь прохождения трафика, который возможно содержит конфиденциальную информацию, и делать так, что весь поток информации, который в нормальном режиме прошел бы вне досягаемости от прослушивания, теперь поступал сначала прямо в руки злоумышленника (а затем его уже можно переправлять по настоящему *IP*-адресу второго абонента).

Рабочие станции

Основной целью атаки рабочей станции является, конечно, получение данных, обрабатываемых, либо локально хранимых на ней. А основным средством подобных атак до сих пор остаются «троянские» программы. Эти программы по своей структуре ничем не отличаются от компьютерных вирусов, однако при попадании на ЭВМ стараются вести себя как можно незаметнее. При этом они позволяют любому постороннему лицу, знающему протокол работы с данной троянской программой, производить удаленно с ЭВМ любые действия. То есть основной целью работы подобных программ является разрушение системы сетевой защиты станции изнутри - пробивание в ней огромной бреши.

Для борьбы с троянскими программами используется как обычное антивирусное программное обеспечение, так и несколько специфичных методов, ориентированных исключительно на них. В отношении первого метода, как и с компьютерными вирусами, необходимо помнить, что антивирусное программное обеспечение обнаруживает огромное количество вирусов, но только таких, которые широко разошлись по стране и имели многочисленные прецеденты заражения. В тех же случаях, когда вирус или троянская программа пишется с целью получения доступа именно к вашей ЭВМ или корпоративной сети, то она практически с вероятностью 90% не будет обнаружена стандартным антивирусным программным обеспечением. Те троянские программы, которые постоянно обеспечивают доступ к зараженной ЭВМ, а, следовательно, держат на ней открытый порт какого-либо транспортного протокола, можно обнаруживать с помощью утилит контроля за сетевыми портами, например, для операционных систем клона *Microsoft Windows* такой утилитой является программа *NetStat*. Запуск с ключом *netstat*-а выведет на экран все активные порты ЭВМ. От оператора в этом случае требуется знать порты стандартных сервисов, которые постоянно открыты на ЭВМ, и тогда любая новая запись на мониторе должна привлечь его внимание. На сегодняшний день существует уже несколько программных продуктов, производящих подобный контроль автоматически. В отношении троянских программ, троянских программ, которые не держат постоянно открытых транспортных портов, а просто методически пересылают на сервер злоумышленника какую-либо информацию (например, файлы паролей или полную копию текста, набираемого с клавиатуры), возможен только сетевой мониторинг. Это достаточно сложная задача, требующая либо участия квалифицированного сотрудника, либо громоздкой системы принятия решений. Поэтому наиболее простой путь, надежно защищающий как от компьютерных вирусов, так и от троянских программ - это установка на каждой рабочей станции программ контроля за изменениями в системных файлах и служебных областях данных (реестре, загрузочных областях дисков) так называемых ***адвизоров*** (англ. *adviser*- уведомитель).

Средства передачи информации

Естественно, основным видом атак на среду передачи информации является ее прослушивание. В отношении возможности прослушивания все линии связи делятся на:

- широковещательные с неограниченным доступом;
- широковещательные с ограниченным доступом;
- каналы «точка-точка».

К первой категории относятся схемы передачи информации, возможность считывания информации с которых ничем не контролируется. Такими схемами, например, являются инфракрасные и радиоволновые сети. Ко второй категории относятся уже только проводные линии: чтение информации с них возможно либо всеми станциями, подключенными к данному проводу (широковещательная категория), либо только теми станциями и узлами коммутации через которые идет пакет от пункта отправки до пункта назначения (категория «точка-точка»).

К широковещательной категории сетей относятся сеть *TokenRing* и сеть *EtherNet* на коаксиальной жиле, а также на повторителях (хабах - англ. *hub*). Целенаправленную (защищенную от прослушивания другими рабочими станциями) передачу данных в сетях *EtherNet* производят сетевые коммутаторы типа *свич* (англ. *switch*) и различного рода маршрутизаторы (роутеры - англ. *router*). Сеть, построенная по схеме с защитой трафика от прослушивания смежными рабочими станциями, почти всегда будет стоить дороже, чем широковещательная топология, но за безопасность нужно платить.

В отношении прослушивания сетевого трафика подключаемыми извне устройствами существует следующий список кабельных соединений по возрастанию сложности их прослушивания:

- не витая пара - сигнал может прослушиваться на расстоянии в несколько сантиметров без непосредственного контакта;

- витая пара - сигнал несколько слабее, но прослушивание без непосредственного контакта также возможно;

- коаксиальный провод - центральная жила надежно экранирована оплеткой: необходим специальный контакт, раздвигающий или режущий часть оплетки, и проникающий к центральной жиле;

- оптическое волокно - для прослушивания информации необходимо вклинивание в кабель и дорогостоящее оборудование, сам процесс подсоединения к кабелю сопровождается прерыванием связи и может быть обнаружен, если по кабелю постоянно передается какой-либо контрольный блок данных.

Вывод систем передачи информации из строя (атака «отказ в сервисе) на уровне среды передачи информации возможен, но обычно он расценивается уже как внешнее механическое или электронное (а не программное) воздействие. Возможны физическое разрушение кабелей, постановка шумов в кабеле и в инфра- и радиотрактах.

Узлы коммутации сетей

Узлы коммутации сетей представляют для злоумышленников:

- инструмент маршрутизации сетевого трафика;
- необходимый компонент работоспособности сети.

В отношении первой цели получение доступа к таблице маршрутизации позволяет изменить путь потока возможно конфиденциальной информации в интересующую злоумышленника сторону. Дальнейшие его действия могут быть подобны атаке на DNS-сервер. Достичь этого можно либо непосредственным администрированием, если злоумышленник каким-либо получил права администратора (чаще всего узнал пароль администратора или воспользовался несмененным паролем по умолчанию). В этом плане возможность удаленного управления устройствами коммутации не всегда благо: получить физический доступ к устройству, управляемому только через физический порт, гораздо сложнее. Либо же возможен второй путь атаки с целью изменения таблицы маршрутизации - он основан на динамической маршрутизации пакетов, включенной на многих узлах коммутации. В таком режиме устройство определяет наиболее выгодный путь отправки конкретного пакета, основываясь на истории прихода определенных служебных пакетов сети - сообщений маршрутизации (протоколы ARP, RIP). В этом случае при фальсификации по определенным законам нескольких подобных служебных пакетов можно добиться того, что устройство начинает отправлять пакеты по пути, интересующем злоумышленника, думая, что это и есть самый быстрый путь к пункту назначения.

При атаке класса «отказ в сервисе» злоумышленник обычно заставляет узел коммутации либо передавать сообщения по неверному «тупиковому» пути, либо вообще перестать передавать сообщения. Для достижения второй цели обычно используют ошибки в программном обеспечении, запущенном на самом маршрутизаторе, с целью его «зависания». Так, например, совсем недавно было обнаружено, что целый модельный ряд маршрутизаторов одной известной фирмы при поступлении на его IP-адрес довольно небольшого потока неправильных пакетов протокола TCP либо перестает передавать все остальные пакеты до тех пор, пока атака не прекратится, либо вообще зацикливается.

Уровни сетевых атак согласно модели OSI

Эталонная модель взаимодействия открытых систем *OSI* (Ohtn Systems Interconnection) была разработана институтом стандартизации *OSI* с целью разграничить функции различных протоколов в процессе передачи информации от одного абонента другому. Подобных классов функций было выделено 7 - они получили название уровней. Каждый уровень выполняет свои определенные задачи в процессе передачи блока информации, причем соответствующий уровень на приемной стороне производит преобразования, точно обратные тем, которые производил тот же уровень на передающей стороне. Каждый уровень добавляет к пакету небольшой своей служебной информации - префикс. Некоторые уровни в конкретной реализации вполне могут отсутствовать. Данная модель позволяет провести классификацию сетевых атак согласно уровню их воздействия.

Физический уровень отвечает за преобразование электронных сигналов в сигналы среды передачи информации (импульсы напряжения, радиоволны, инфракрасные сигналы). На этом уровне основным классом атак является «отказ в сервисе». Постановка шумов по всей полосе пропускания канала может привести к «надежному» разрыву связи.

Канальный уровень управляет синхронизацией двух и большего количества сетевых адаптеров, подключенных к единой среде передачи данных. Примером его является протокол *EtherNet*. Воздействия на этом уровне также заключаются в основном в атаке «отказ в сервисе». Однако, в отличие от предыдущего уровня, здесь производится сбой синхропосылок или самой передачи данных периодической передачей «без разрешения и не в свое время».

Сетевой уровень отвечает за систему уникальных имен и доставку пакетов по этому имени, то есть за маршрутизацию пакетов. Примером такого протокола является протокол Интернет *IP*.

Транспортный уровень отвечает за доставку больших сообщений по линиям с коммутацией пакетов. Так как в подобных линиях размер пакета представляет собой обычно небольшое число (от 500 байт до 5 килобайт), то для передачи больших объемов информации их необходимо разбивать на передающей стороне и собирать на приемной. Транспортными протоколами в сети Интернет являются протоколы *UDP*, *TCP*. Реализация транспортного протокола - довольно сложная задача, а если еще учесть, что злоумышленник придумывает самые разные схемы составления неправильных пакетов, то проблема атак транспортного уровня вполне объяснима. Все дело в том, что пакеты на приемную станцию могут приходить и иногда приходят не в том порядке, в каком они были отправлены. Причина обычно состоит в потере некоторых пакетов из-за

ошибок или переполненности каналов, реже - в использовании для передачи потока двух альтернативных путей в сетях. А, следовательно, операционная система должна хранить некоторый буфер пакетов, дожидаясь прихода задержавшихся в пути. А если злоумышленник с умыслом формирует пакеты таким образом, чтобы последовательность была большой и заведомо неполной, то тут можно ожидать как постоянной занятости буфера, так и более опасных ошибок из-за его переполнения.

Сеансовый уровень отвечает за процедуру установления начала сеанса и подтверждение (квитирование) прихода каждого пакета от отправителя получателю. В сети Интернет протоколом сеансового уровня является протокол *TCP* (он занимает и 4, и 5 уровни модели *OSI*). В отношении сеансового уровня очень широко распространена специфичная атака класса «отказ в сервисе», основанная на свойствах процедуры установления соединения в протоколе *TCP*. Она получила название *SYN-Flood* (*flood* -«большой поток»).

При попытке клиента подключиться к серверу, работающему по протоколу *TCP* (а его используют более 80% информационных служб, в том числе *HTTP FTP SMTP POP3*), он посылает серверу пакет без информации, но с битом *SYN*, установленным в 1 в служебной области пакета - запросом на соединение. По получении такого пакета сервер обязан выслать клиенту подтверждение приема запроса, после чего с третьего пакета начинается собственно диалог между клиентом и сервером. Одновременно сервер может поддерживать в зависимости от типа сервиса от 20 до нескольких тысяч клиентов.

При атаке типа *SYN-Flood* злоумышленник начинает на своей ЭВМ создавать пакеты, представляющие собой запросы на соединение (то есть *SYN*-пакеты) от имени произвольных *IP*-адресов (возможно даже несуществующих) на имя атакуемого сервера по порту сервиса, который он хочет приостановить. Все пакеты будут доставляться получателю, поскольку при доставке анализируется только адрес назначения. Сервер, начиная соединение по каждому из этих запросов, резервирует под него место в своем буфере, отправляет пакет-подтверждение и начинает ожидать третьего пакета клиента в течение некоторого промежутка времени (1-5 секунд). Пакет-подтверждение уйдет по адресу, указанному в качестве ложного отправителя в произвольную точку Интернет и либо не найдет адресата вообще, либо чрезмерно «удивит» операционную систему на этом *IP*-адресе (поскольку она никаких запросов на данный сервер не посылала) и будет просто проигнорирован. А вот сервер, при достаточно небольшом потоке таких запросов, будет постоянно держать свой буфер заполненным ненужными ожиданием соединений, и даже *SYN*-запросы от настоящих легальных пользователей не будут помещаться в буфер. Сеансовый уровень просто не знает и не может узнать, какие из запросов фальшивые, а какие настоящие и могли бы иметь больший приоритет.

Атака *SYN-Flood* получила довольно широкое распространение, поскольку для нее не требуется никаких дополнительных подготовительных действий. Ее можно проводить из любой точки Интернет в адрес любого сервера, а для отслеживания злоумышленника потребуется совместные действия всех провайдеров, составляющих цепочку от злоумышленника до атакуемого сервера (к чести сказать, практически все фирмы-провайдеры, если они обладают соответствующим программным обеспечением и квалифицированным персоналом, активно участвуют в отслеживании атакующей стороны).

Заключение

Каждый квалифицированный программист должен знать:

1. Сетевые операционные системы.
2. Средства поддержки сетевого режима.
3. Сервера.
4. Рабочие станции.
5. Среду передачи информации.
6. Узлы коммутации сетей.
7. Уровни сетевых атак согласно модели *OSI*.

УДК 004.9:332.871

Анатолий Алексеевич Лукьянец, Артём Геннадьевич Чернов
Институт экономики и организации промышленного производства
Сибирское отделение Российской академии наук

Виктор Григорьевич Ротарь
Томский политехнический университет

ЗАДАЧИ ВНЕДРЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В КОММУНАЛЬНОМ ХОЗЯЙСТВЕ РЕГИОНА©

Коммунальное хозяйство крупного региона несомненно представляет собой сложную со своими уникальными особенностями систему. Качество процесса управления этой системой во многом определяет