Эссе по курсу "Защита информации", кафедра радиотехники, Московский физико-технический институт (ГУ МФТИ), http://www.re.mipt.ru/infsec

Безопасность tcp/ip.

Фатихов Айрат Винерович
116 группа
19.04.2005

Содержание

1. Введение

Для начала несколько слов о том, что такое tcp/ip. В переводе с ангийского tcp/ip (Transmission Control Protocol/Internet Protocol) означает Протокол управления

передачей/Протокол Интернет, откуда становится понятным для каких целей предназначен этот протокол. В первую очередь для построения intranet и Internet (глобальный) сетей. А теперь дадим более точное определение каждого из рассматриваемых протоколов:

IP- протокол низкого уровня, направляет данные в виде пакетов по отдельным сетям, которые связаны через роутеры для формирования Интернет или интрасети.

TCP -протокол для работы с подключениями, передает данные в виде потоков байтов. Этот протокол является надежным (поскольку используется контрольная сумма для удостоверения целостности данных и отправка подтверждений для гарантии того, что данные при передаче не исказились).

Кстати, tcp/ip зародился в результате исследований проводимых под покровительством правительства США (а точнее Advanced Research Project Agency). Разработки велись с целью объединить вычислительные базы научных центров в одну большую виртуальную сеть.

Несмотря на то, что tcp/ip сети нынче весьма популярны, они не являются неуязвимыми и подвержены различным атакам. Это видимо произошло потому, что он создавался в те времена, когда о возможных атаках и не думали, а следовательно и защита была такой необходимой.

Например, ip-шники и хосты серверов могут не соответствовать друг другу, так как обмануть кэш-память DNS сервера весьма просто. На этом основываются атаки типа фишинга.

В данной статье не будут рассматриваться физические атаки (мы же не в каменном веке живем), рассмотрим программную реализацию тех или иных атак, методы их обнаружения и устранения их возможности.

2. Пассивные атаки и защита

Атаки можно разделить на два типа: пассивные и активные.
При пассивных атаках злоумышленник не взаимодействует с системой напрямую и его нельзя обнаружить. При такой атаке злоумышленнику становятся доступны передаваемые данные для анализа.

2.1 Подслушивание (sniffing)

Эта атака заключается в том, что злоумышленник перехватывает сетевой поток и анализирует его.

Для осуществления такого подслушивания злоумышленнику необходимо иметь доступ к машине на пути сетевого потока, который необходимо анализировать (например, к роутеру или PPP-серверу на базе UNIXa). Тогда, имея необходимые права на этой машине, он сможет просматривать весь трафик (с помощью специальных программ), проходящий через данную машину.

Другой вариант этой атаки – это когда злоумышленник получает доступ к машине из одного сегмента сети с системой, у которой имеется доступ к сетевому потоку. Известно,

что в "тонком ethernet'е" сетевая карточка может работать в таком режиме, в котором она получает все пакеты, циркулирующие по сети, в том числе и те, которые ей не адресовались.

Злоумышленники (с использованием соответствующего инструментария) могут перехватывать TCP/IP-пакеты telnet сессий (так как TCP/IP-трафик чаще всего не шифруется , то это не составит большого труда) и извлекать из этих пакетов имена пользователей и пароли.

Защита от подслушивания

Этот тип атаки невозможно отследить без доступа к системе злоумышленника, так как при этом сетевой поток не меняется. Надежной защитой от подслушивания может служить шифрование TCP/IP-потока или же использование одноразовых паролей. Другой вариант решения этой проблемы - использование умных свитчей (это получается почти роутер), в результате каждая машина в сети получает только трафик адресованный ей и какой больше.

Хотя , вообще говоря, подслушивание может быть и необходимо для работы сети. Например, данный метод используется при анализе работы сети (оценка загруженности, работоспособности и т.п.), помогающем админам сети.

3. Активные атаки и защита

Активные атаки более интеллектуальные и изощренные и распространены они тоже больше. Такие атаки основываются на формирования произвольных (точнее требуемых злоумышленнику) IP-пакетов.

При данном виде атак злоумышленник взаимодействует с системой-получателем, системой-отправителем или промежуточными системами, изменяет или удаляет часть содержимого TCP/IP-пакетов.

Активные атаки можно разделить на два вида:

1) В первом случае злоумышленник перехватывает и модифицирует сетевой поток или же выдает себя за другую (дружественную) систему

2) Во втором случае злоумышленник хочет привести систему-жертву в нерабочее состоянии.

Почти в любой ОС злоумышленник может вручную (или же с помощью каких-либо программных средств) формировать произвольные IP-пакеты и передавать их по сети (в том числе и заголовок пакета может быть сформирован «как надо»). Получатель такого пакета, не сможет на 100% определить, кто действительно был его отправителем.

Рассмотрим несколько конкретных примеров таких атак

3.1. Пассивное сканирование

Сканирование применяется для того, чтобы выявить, на каких TCP-портах работают демоны, отвечающие на запросы из сети. Программа-сканер последовательно открывает соединения с различными портами. Если соединение устанавливается, то программа сбрасывает его и сообщает номер порта. Но в этом случае атака может быть легко обнаружена: демоны выдают сообщения при большом числе сразу же прерванных соединений.

Более хитрый метод - пассивное сканирование ("passive scan"). Злоумышленник (а точнее программа, которую он использует) посылает TCP/IP SYN-пакет на все порты. Порты, которые принимают внешние соединения, возвратят SYN/ACK-пакет (приглашение на продолжение тройного рукопожатия), которые не принимают - вернут RST-пакеты. Злоумышленнику становится известным на каких портах работают программы. В ответ на SYN/ACK-пакеты он может ответить RST-пакетом (установки соединения не будет) или же за него ответит реализация tcp/ip, но через некоторое время. Отсюда и способы, которыми можно детектировать такую атаку:

1) в первом случае - частое получение RST-пакета в ответ на SYN/ACK

1) во втором - большое количество сессий в syn_recieved-состоянии

Но если злоумышленник не дурак, то он будет сканировать порты не так быстро или будет сканировать какие-то конкретные порты – в общем делать так, чтобы все выглядело как обычные попытки установить соединение – и тогда такую атаку практически не возможно выявить.

В качестве защиты можно применить грубую силу - закрыть на firewall’е все сервисы, к которым не требуется внешний доступ.

Небольшое отступление в сторону тройного рукопожатия (3-way handshake):

Суть этого рукопожатия на примере клиент-сервер такова. Клиент выбирает и передает серверу sequence number (C-SYN). Сервер в ответ передает клиенту пакет данных, содержащий подтверждение (C-ACK) и собственный sequence number (S-SYN). Клиент высылает подтверждение (S-ACK). После того, как все это проделано, соединение установлено и начинается обмен данными. Каждый передаваемый пакет будет иметь в заголовке поле sequence number и acknowledge number. Эти числа увеличиваются с течением обмена данными и с помощью них контролируется корректность передачи данных.

3.2 Предсказание TCP sequence number (ip-spoofing)

Допустим, что возможно угадать значение sequence numbera’ от сервера (S-SYN). Есть два способа как это сделать: зная конкретную реализацию tcp/ip (в том числе и алгоритм генерации sequence number), можно с нескольких попыток просто угадать S-SYN; если же алгоритм неизвестен, то можно несколько раз послать пакеты серверу и из анализа его ответов предсказать S-SYN.

Пусть есть две системы A и B, которые доверяют друг другу, и злоумышленник C, задача которого - выдать себя за одну из систем, например B. Если быть ближе к жизни, то A-сервер (который доверят только B), B и C – клиенты.

Что делает C в первую очередь – так это выводит систему B из строя или же приводит ее в состояние, когда она не может отвечать на сетевые запросы (в простейшем случае можно дождаться перезагрузки B). Теперь C притворяется системой B:

1) C высылает несколько пакетов с запросами на соединение с A , для того чтобы выяснить значение sequence number'a у сервера.
2) C высылает пакет с обратным адресом B
3) A в ответ высылает пакет со значением sequence number'a , он предназначается для B, но тот его уже не получит...и C его к сожалению тоже не получит, но зато он сможет предсказать sequence number высланный для B.
4) C подтверждает получение (которого на самом деле не было) пакета от A, для этого высылает от имени B пакет с предполагаемым **S-ACK**. Если злоумышленнику очень повезло и sequence number сервера C был угадан верно, соединение считается установленным.

Ну а теперь злоумышленник может делать «все что хочет» (до тех пор пока не «проснулся» B).

Как обнаружить и защититься от такой атаки?

Можно лишить злоумышленника ключевого элемента атаки - угадывание sequence number - намного усложнить или вообще сделать невозможным это угадывание . Например, можно увеличить скорость изменения sequence number или выбирать скорость увеличения sequence number случайным образом (желательно, с помощью криптографически стойких алгоритмов).

Можно добавить firewall'у правила, по которым все пакеты, пришедшие извне и имеющие локальные обратные адреса, не пропускаются внутрь нашей сети. Кроме того, следует минимизировать доверие машин друг другу.

3.3 Затопление SYN-пакетами

Вспоминаем, как работает протокол TCP/IP для входящих соединений. На пришедший C-SYN система отвечает S-SYN/C-ACK-пакетом , переводит сессию в состояние syn_recieved и заносит ее в очередь. Если от клиента придет пакет S-ACK, то соединение устанавливается (established), а если же в течение некоторого времени от клиента не придет пакет S-ACK, то соединение удаляется.

Допустим, что очередь входных соединений уже заполнена, но система получает SYN-пакет, тогда он будет проигнорирован без какого либо оповещения.

BSD-системах, каждый порт имеет свою собственную очередь из 16 элементов, а система SunOS имеет большую общую очередью. Соответственно, для того, что бы сделать бездейственным WWW-порт на BSD необходимо 16 SYN-пакетов, а для Solaris'а намного больше. По истечению некоторого времени, зависящего от реализации, запросы из очереди удаляются. Но злоумышленник немного сообразив может посылать пакеты

постоянно. А также злоумышленник может использовать чужие обратные ip'шники, для того чтобы скрыть свои действия.

Обнаружить такую атаку несложно, это можно сделать по большому количество соединений в syn_recieved-состоянии.

В качестве защиты можно прорежать очереди (например, случайным образом удалять сессии из очереди). Или же настроить сеть так, чтобы все входящие соединения устанавливал firewall, а потом перекидывал их на систему, для которой это соединение предназначалось.

3.4 ip-hijacking

При этой атаке злоумышленник перехватывает и модифицирует сетевой трафик произвольным образом, являясь при этом как бы «посредником» между клиентом и сервером. Для этого соединение между сервером и клиентов вводится в десинхронизованное состояние, то есть когда sequence number и acknowledge number будут не правильными для сервера и клиента (полученный сервером от клиента number не совпадает с ожидаемым , и аналогично для клиента). Далее злоумышленник становится «посредине» между сервером и клиентом: прослушивает линию, отправляет пакеты серверу и клиенту и перехватывает ответы (вобщем выдает себя за клиента для сервера и наоборот). Что касается пакетов с неправильным sequence number и acknowledge number, то в ответ на них будут отправлены ACK-пакеты (вообще говоря, это может вызвать ACK-бурю).

Имеется два способа осуществления десинхронизации:

A. Ранняя десинхронизация при установке соединения: Злоумышленник прослушивает сеть и, дождавшись от сервера S-SYN пакета, посылает RST-пакет (который сбрасывает сессию) с правильным sequence number, а затем C-SYN-пакет от имени клиента. Сервер открывает новую сессию (с новым sequence number) и отправляет свой S-SYN-пакет клиенту. Далее злоумышленник, прослушивающий линию, высылает серверу S-ACK-пакет от имени клиента. Соединение установлено, но десинхронизировано.

B. Десинхронизация с нулевыми данными: Злоумышленник прослушивает уже установленную сессию и посылает серверу пакет с нулевыми данными (они будут проигнорированы на уровне выше). Аналогичный пакет шлется клиенту.

Ip-hijacking можно выследить по вызываемой ACK-буре. Она возникает из-за того, что когда сессия десинхронизирована, на неправильный пакет от сервера клиент тоже отвечает ACK пакетом, который для сервера неправильный; и так продолжается долго. Таким образом, можно анализируя загруженность сети, отслеживать ACK-бури.

3.5 DNS spoofing

Что такое DNS ? Работа системы DNS (Domain Name System) заключается в преобразовании доменных имен серверов в IP-адреса и наоборот. Атака DNS spoofing

проводится для получения требуемого злоумышленнику соответствия между IP адресом и доменным именем в кэше DNS сервера. На запрос клиента будет выдан адрес сайта злоумышленника, на котором может находиться копия настоящего сайта, и таким образом если это сайт какого-либо банка можно украсть конфиденциальную информацию клиента.

Каждый DNS-пакет содержит идентификатор (DNS ID) для соответствия запросов и ответов. Требуется послать свой ответ на DNS-запрос до того, как это сделает настоящий DNS-сервер, поэтому для этого нужно угадать DNS ID. Атака состоит из четырех последовательных шагов:

1. злоумышленник шлет DNS-запрос от имени www.haker.com к DNS-серверу ns.haked.com

2. целевой DNS-сервер перенаправляет запрос к серверу ns.haker.com

3. злоумышленник прослушивает запросы на предмет получения идентификаторов
4. злоумышленник фальсифицирует IP-адрес соответствующий имени.

Данная атака характерна большим количеством DNS пакетов с одинаковыми доменными именами(это связано с необходимостью угадывания параметров DNS обмена).

Для обеспечения достоверной передачи DNS-данных в систему DNS вводятся расширения, называемые DNSSEC (RFC-2535, 2536, 2537, 2541, 3008). Основная идея DNSSEC состоит в использовании асимметричного шифрования для присоединения цифровой подписи к передаваемым данным.

3.6 Smurf-атаки

Smurf-атаки используют шировещательный адрес IP-сети в качестве адреса назначения. Атакующий высылает пакет ICMP ECHO, причем адрес источника этого пакета заменяется адресом жертвы, чтобы представить дело так, будто именно целевая система инициировала запрос. Поскольку пакет ECHO послан по широковещательному адресу, все системы усиливающей сети возвращают жертве свои ответы и тогда жертва не сможет продолжить нормальную работу, поскольку будет полностью занята вся полоса пропускания линии.

Для избежания таких атак нужно запретить прямую широковещательную рассылку на всех граничных маршрутизаторах (чтобы предотвратить эффект усиления). Дополнительно можно установить в операционной системе режим "тихого" отброса широковещательных эхо-пакетов ICMP.

3.7 DoS- атаки

Предыдущие атаки (3.3, 3.5, 3.6) относятся к DoS-атакам Само название - DoS означает Denial of Service (с английского Отказ от Обслуживания).
Сущность DoS-атаки заключается в том, чтобы лишить пользователей какого-либо сервиса или службы. Это можно осуществить несколькими способами:
- перегрузка сети передачей "мусора" и другого паразитного трафика;

- физическое разрушение связи между двумя машинами;
- лишение доступа к службе пользователя (например лишение этого пользователя привилегий доступа);
- выведение сервиса из строя

Что можно посоветовать , для защиты от таких атак? Вот несколько самых важных пунктов:
- Постоянно следить за обновлениями ПО и обнаружением новых "дыр" в используемом ПО.
- Поставить ограничение на входящий трафик.
- Проверять все компьютеры в сети, так как их чаще взламывают, чем сам сервер.
- Закрыть неиспользуемые и ненужные порты.
- Установить FireWall, так как практически все хакеры стараются обходить его стороной из-за многопротокольной проверки пакетов с учётом состояния протокола (SMLI).

4. Пара слов об ipv6 и ipsec

ipv6 и ipsec относятся к VPN-технологиям (Virtual Private Networ).

ipv6 - это просто другая форма адресации и он не имеет мер безопасности. Но у него есть возможность поддержки защиты(например, там есть ipsec). Подробности об IPv6 есть на http://www.bieringer.de/linux/IPv6. Linux уже поддерживает IPv6 в полном объеме (одна из немногих OS, в которых это реализовано)

ipsec — это набор протоколов с шифрованием, аутентификацией и обеспечением защиты при транспортировке ip-пакетов. Архитектура ipsec включает в себя 3 алгоритмически-независимые основополагающие спецификации: "Архитектура безопасности IP", "Аутентифицирующий заголовок (AH)", "Инкапсуляция зашифрованных данных (ESP)".

5. Использованная литература

1. «Безопасность tcp/ip», В. Колонцов, 2000г . (http://www.citforum.ru/internet/securities/tcpip.shtml)