Эссе по курсу
«Защита Информации»
Студента 212 гр.
Трушина Константина

TCP/IP: обзор возможных атак и способов защиты.

Содержание

1. Вступление

В постиндустриальном обществе функционирование экономики невозможно без обмена данными. Основным средством для этого на данный момент является Internet, построенный на протоколах TCP/IP. Поэтому вопросы стабильной и безопасной работы TCP/IP-сетей являются критическими для всей IT-инфраструктуры.

Для понимания сути многих атак необходимо кратко описать процесс установления TCP-соединения и передачи данных.

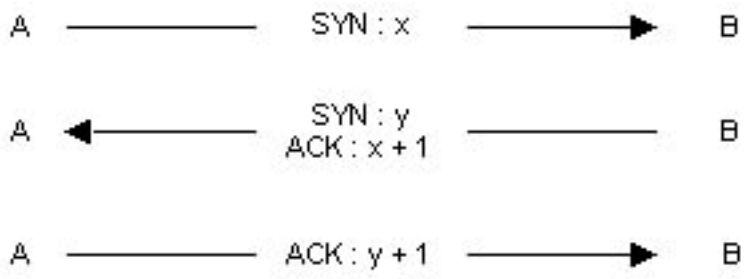

Рис 1. Установка соединения.

Машина A посылает SYN-пакет (запрос на соединение) машине B, в котором помимо адреса и порта назначения содержится так называемый sequence number машины A(пусть он например равен x), который используется для синхронизации и увеличивается в процессе обмена данными на количество переданных байт. Машина B отвечает SYN/ACK пакетом, в котором содержится подтверждение получения данных (бит ACK установлен в 1), acknowledge number x+1 и запрос на соединение с sequence number y. В ответ машина A посылает подтверждение с acknowledge number y+1.

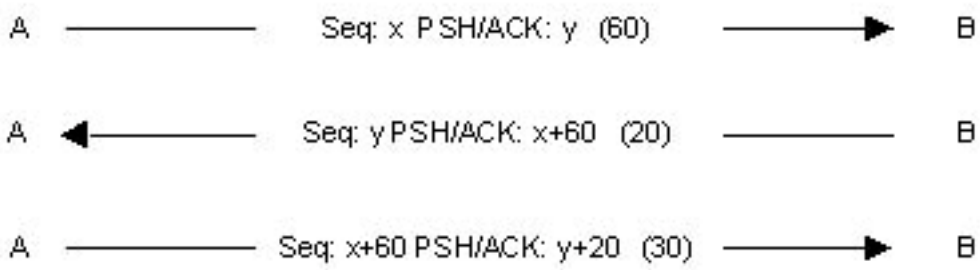

Рис 2. Передача данных

На рисунке 2 изображен схематически процесс передачи данных. Sequence number изображен после идентификатора Seq, флаг PSH означает, что данные должны быть переданы приложению, acknowledge number указан после идентификатора ACK. В скобках указана длина переданных данных в каждом из пакетов.

2. Пассивные Атаки

Данные атаки характеризуются тем, что злоумышленник никаким образом не ступает во взаимодействие с системами сети.

2.1 Sniffing

Sniffing – это подслушивание. При данной атаке злоумышленник только анализирует трафик, не меняя его. Осуществлять данную атаку имеет смысл только в тех сетях, где нет шифрования передаваемых данных (университетские сети, локальные сети районов городов).

Чтобы осуществить атаку злоумышленник должен иметь доступ с необходимыми правами к машине на пути потока трафика (например, маршрутизатору(router)).

Наиболее простой вариант в локальных сетях для внутреннего злоумышленника – это перевести сетевую карту в режим, когда она принимает весь входящий трафик , а не только адресованный ей конкретно, и использование специального программного обеспечения.

Выявить такую атаку невозможно ввиду того, что ни функционирование сети, ни трафик по ней не изменяются.

В качестве средств защиты можно использовать шифрование данных, а также использование более интеллектуальных коммутаторов(switch), которые данной машине направляют только трафик, адресованный ей.

Но здесь надо учесть, что подслушивание используется сетевыми администраторами для анализа работы сети.

3. Активные атаки

Атаки этого типа характеризуются тем, что злоумышленник тем или иным способом взаимодействует с одной или несколькими машинами в сети.

Отказ в обслуживании

Данная группа атак направлена на то, что физически заполнить всю полосу пропускания канала жертвы или всей сети.

3.1 SYN-flood

Атака заключается в создании не до конца установленных соединений. При получении SYN-пакета машина отвечает SYN/ACK-пакетом и заносит сессию в очередь. Если был получен ACK-пакет, то соединение считается установленным и удаляется из очереди. Если в течение некоторого времени ACK-пакет не получен, сессия также удаляется из

очереди. В случае если очередь заполнена, и пришел новый SYN-пакет, то он будет проигнорирован.

SYN-flood основан на переполнении очереди какого-либо сервера, после чего он уже не будет отвечать на запросы пользователей. Примечательно, что в старых версиях FreeBSD максимальный размер очереди соединений составлял всего 16 элементов. Таким образом злоумышленнику достаточно отправлять по 20-30 макетов за 1 минуту, чтобы фактически сделать сервер недоступным для пользователей в течение длительного времени.

Полной защиты от таких атак не существует. Для снижения риска необходимо закрыть на серверах все неиспользуемые порты для уменьшения «благодатной почвы» подобных атак.

Ныне основная работа по противодействию таким атакам возложена на маршрутизаторы сети. Когда извне приходит SYN-пакет, маршрутизатор не пропускает его во внутреннюю сеть, а сам отвечает на него от имени сервера назначения. Если соединение с внешним клиентом все же устанавливается, то маршрутизатор создает соединение с сервером от имени клиента, и в дальнейшем выступает как невидимый посредник, о котором ни внутренний сервер, ни внешний клиент не догадываются.

В случае, если ответ от клиента на SYN/ACK-пакет в определенный промежуток времени не получен, то оригинальный SYN-пакет умрет на маршрутизаторе и не будет передан внутрь сети.

Если же SYN-пакеты начинают поступать в большом количестве и с большой скоростью, то маршрутизатор переходит в так называемый «агрессивный» режим, когда время ожидания ответа на SYN/ACK-пакет резко сокращается, а каждый новый пришедший SYN-пакет выталкивает из очереди один из ранее полученных. При снижении потока запросов маршрутизатор возвращается в обычный режим работы. Данная техника применения маршрутизаторов в борьбе с SYN-flood, а не гораздо менее приспособленных для этого серверов, получила название TCP Intercept.

Использование маршрутизаторов в защитных целях эффективно с материальной точки зрения, когда в нужно защитить сегмент сети, в котором много серверов имеют устаревшие операционные системы и таким образом подвержены атакам типа «отказ в обслуживании». Если же на всех машинах установлены последние версии операционных систем, в которых реализована вышеописанная система защиты от SYN-flood с помощью перехода в «агрессивный» режим, то работа марширутизаторов по схеме TCP Intercept не имеет смысла.

3.2 UDP-flood

Многие системы поддерживают работу таких как 7 («эхо», отсылка обратно полученного пакета) и 19 («знакогенератор», в ответ на пришедший пакет отправителю высылается строка символов).

Злоумышленник посылает UDP-пакет с портом назначения 19 и портом-отправителем 7 (IP-адреса отправителя и получателя подменяются на адреса машин-жертв). На этот пакет 19 порт ответит строкой, которая будет послана на порт 7, а он в сою очередь отошлет ее на 19, и так до бесконечности. Таким образом, возникает UDP-буря.

Результат: ресурсы машин «съедены», а сеть загружена бесполезным трафиком. Буря прекращается при первой потери пакета, но в принципе ничто не мешает злоумышленнику отправить еще один пакет, инициирующий атаку.

В качестве защиты применяется закрытие на firewall всех сервисов и недопущение с сеть пакетов с внутренним адресом отправителя, но пришедших извне. Заметим, что последняя методика, примененная без первой, не поможет, если злоумышленник находится во внутренней сети.

3.3 Smurfing

Эта атака использует ICMP-протокол. Каждой машине сети постоянно посылаются ping-пакеты, в котором в качестве адреса отправителя указан адрес жертвы. Это можно сделать послав ICMP ECHO REQUEST по широковещательному адресу, например 10.255.255.255. Каждая машина сети ответит жертве пакетом ICMP ECHO REPLY. Таким образом жертва получит число пакетов, равное количеству машин в сети. В результате вся сеть оказывается перегруженной, а вычислительные ресурсы жертвы полностью занятыми. Чтобы противодействовать таким атакам, нужно запретить широковещательную рассылку на всех граничных маршрутизаторах сети. Это поможет предотвратить эффект усиления потока ICMP –пакетов. Также рекомендуется установить на операционных системах компьютеров сети режим отброса широковещательных ICMP –пакетов.

3.4 Fake DHCP clients

Во многих локальных сетях IP-адреса машинам выдает специальный сервер по протоколу DHCP(Dynamic Host Control Protocol) сразу после подключения машины к сети. Причем адресное пространство, с которым работает DHCP –сервер ограничено. Это дает возможность злоумышленнику сформировать множество фиктивных запросов к этому серверу от имени не существующих в сети машин. Таким образом, DHCP –сервер

истратит се множество адресов на ложных пользователей и как следствие легальные хосты лишаться возможности подключиться в сеть.
Для защиты от этой атаки обычно используется следующий механизм. DHCP –сервер настраивается так, чтобы конкретному хосту выдавался не случайный IP-адрес из пула, а всегда один и тот же. Это достигается поддержкой на сервере таблицы соответствия между MAC-адресом хоста и IP-адресом, который надо ему выдать. В этом случае все фиктивные запросы будут отброшены, и атака не возымеет успеха.
Существует метод обхода защиты только на основе таблицы соответствия MAC- IP. Если злоумышленник будет менять свой MAC-адрес на MAC-адрес легального пользователя сети (который в данный момент не подключен к сети), и уже от имени этого пользователя посылать запросы на получение IP-адреса, то атака пройдет. При этом необходимо заранее собрать статистику о легальных MAC-адресах в данном сегменте сети.
Чтобы защититься от смены MAC-адресов, на каждом поту в всех маршрутизаторов сегмента сети должна периодически просматриваться статистика по MAC-адресам. Это может делать программное обеспечение маршрутизатора. Если к какому-то порту подключалось много разных MAC-адресов (которых в обычном режиме быть не должно), то об этом ставится в известность администратор (например, по электронной почте), который может:

- отключить этот порт маршрутизатора
- по известному порту вычислить источник атаки и применить к нему меры карательного характера

4. Перехват Трафика

Злоумышленник вмешивается в процесс обмена данными между машинами, искажая их, перенаправляя трафик и т.д.

4.1 ARP Spoofing

Цель данной атаки – перенаправление трафика от одной или нескольких машин н машину злоумышленника с последующим изменением или без него.
Для понимания атаки необходимо кратко описать работу протокола ARP (Address Resolution Protocol). Чтобы было возможна передача данных по сети на канальном уровне, каждая машина должна иметь некий уникальный адрес. Обычно таковым служит MAC-адрес сетевого устройства. При посылке IP-пакета, машина-отправитель должна узнать MAC-адрес машины-получателя. Для этого она отправляет широковещательный ARP - запрос всем машинам сети, в котором спрашивается: «Какой MAC-адрес у машины с IP-

адресом x.x.x.x?». Машина-получатель, увидев свой IP-адрес, отвечает ARP-пакетом, содержащим ее MAC-адрес. Этот адрес некоторое время сохраняется в cache у отправителя, дабы не посылать запрос перед отправкой каждого пакета.
Данная атака изменяет cache целевой машины. Злоумышленник отправляет жертве ARP-ответы, в которых в качестве соответствия некоторому IP-адресу (например, IP-адресу шлюза) указан MAC-адрес машины злоумышленника. С высокой степенью вероятности этот пакет будет воспринят жертвой, в результате чего в ее cache попадет неверный MAC-адрес. Таким образом, трафик жертвы будет перенаправлен злоумышленнику, который может его прочитать/видоизменить и отправить к реальному целевому адресу.
Злоумышленник может поступить более хитро, перенаправляя трафик жертвы на несуществующий MAC-адрес и извлечения таких пакетов с помощью утилит прослушивания сети. Таким образом, MAC-адрес самого злоумышленника нигде не фигурирует, что позволяет остаться ему незамеченным.
Для обнаружения ARP-атак администратор должен вести таблицу соответствия MAC и IP адресов всех узлов сети, и использовать программное обеспечение, которое прослушивает сеть и сообщает о обнаруженных несоответствиях таблице. Использование статических ARP-таблиц (хотя бы на ключевых маршрутизаторах сети) защищает от атаки ценой увеличения нагрузки на узлы сети.
Заметим, что пользовательскому хосту, не снабженному статической ARP-таблицой почти невозможно обнаружить атаку.

4.2 IP Spoofing

Цель данной атаки состоит в том, чтобы выдать себя за другую машину в сети. Может использоваться двумя способами:
1 сокрытия источника атаки типа «отказ в обслуживании»
2 извлечение выгоды из доверия двух машин друг другу
Рассмотрим второй вариант атаки на примере таких сервисов как rsh (remote shell), в котором единственным средством аутентификации является IP-адрес клиента.
Для этого надо вспомнить, что в процессе установки TCP/IP-соединения используется так называемый sequence number. Если существует возможность угадать sequence number от сервера, то с высокой долей вероятности атака пройдет.
Сначала злоумышленник должен нейтрализовать легального клиента с помощью атаки типа «отказ в обслуживании» или просто дождавшись перезагрузки клиентской ситемы. Затем он посылает несколько запросов на соединение серверу, чтобы по ответным данным выяснить алгоритм генерации sequence number.

Злоумышленник высылает серверу пакет с обратным адресом легального клиента. В ответ сервер высылает *легальному клиенту* пакет с sequence number, который не дойдет до назначения, так как клиент нейтрализован. Заметим, что и злоумышленник не получит этого пакета, потому что он же сам выставил в качестве обратного IP-адрес клиента.
Затем злоумышленник должен подтвердить получение (которого в действительности не было) от имени легального клиента. Здесь и требуется угаданный sequence number сервера. Если подтверждение прошло удачно (sequence number был угадан верно), то соединение установлено, злоумышленник получает доступ на консоль сервера (напомним, рассматривается атака на rsh) и может делать фактически что угодно.
Как защититься? Ключевым элементом атаки является угадывание sequence number сервера, поэтому его генерацию надо как можно сильнее усложнить. Вместо зачастую используемой линейной скорости увеличения sequence number предлагается сделать ее случайной при помощи криптографически стойких алгоритмов.
Заметим, что если легальный пользователь и злоумышленник находятся в одной подсети, то последний может применить утилиту прослушивания сети, и таким образом поймать пакет, шедший от сервера к легальному пользователю и содержащий правильный sequence number сервера. В этом случае задача злоумышленника намного упрощается.
Атака работает до тех пор, пока машина легального клиента не станет работоспособной.

4.3 TCP Session Hijacking

В данной атаке злоумышленник перехватывает и модифицирует трафик между двумя машинами, выступая в роли невидимого посредника между ними: со стороны сервера он представляется клиентом, а со стороны клиента – сервером.
Для этого злоумышленнику необходимо ввести сессию между легальным клиентом и сервером в десинхронизованное состояние, когда клиент получает от сервера пакеты с sequence number и acknowledge number, отличными от ожидаемых, и наоборот. При этом злоумышленник генерирует пакеты с корректными sequence number и acknowledge number как для клиента, так и для сервера, что позволяет ему выступать в качестве посредника.

Рассмотрим один из методов десинхронизации соединения, получивший название «ранняя десинхронизация», когда соединение десинхронизируется во время установки.
Пусть легальный клиент посылает на сервер SYN-пакет, в ответ на который получает SYN/ACK-пакет, и соединение с его стороны переходит в установленное состояние. В этот момент злоумышленник посылает на сервер пакет типа RST, что приводит к сбрасыванию сессии на сервере. Вслед за этим злоумышленник посылает SYN-пакет от

имени клиента, в результате открывается новая сессия, но уже с другим sequence number. Сервер посылает легальному клиенту SYN/ACK-пакет, который является для него неприемлемым, так как содержит неподходящий sequence number(в этом случае возникает ACK-буря, о которой будет рассказано ниже). Теперь злоумышленник посылает серверу ACK-пакет подтверждения от имени клиента с угаданным sequence number, которое является корректным для сервера, и соединение на сервере переходит в установленное состояние. Таким образом, соединение на клиенте и сервере установлено, но десинхронизовано.

Еще один способ десинхронизации соединения заключается в том, что злоумышленник посылает легальному клиенту и серверу по пакеты с «нулевыми» дынными, которые будут проигнорированы на уровне приложений. Они, тем не менее, приведут соединение в десинхронизованное состояние.

Такой метод позволяет обойти системы защиты, основанные на одноразовых паролях, поскольку злоумышленник начинает работать уже после аутентификации легального клиента.

Особенностью данной атаки является то, что любой пакет, полученный клиентом или сервером в десинхронизованном состоянии вызывает ACK-бурю. Рассмотрим это подробнее. Пусть клиент получил от сервера пакет, но так как в этом соединение десинхронизовано, то в этом пакете стоит некорректный для клиента sequence number. Поэтому он ответит ACK-пакетом, который будет неприемлем уже для сервера. На этот пакет будет опять сгенерирован неприемлемый ответ и т.д. Так как в сетях допускается потеря пакетов, то неизбежно ACK-буря стихнет при первом же потерянном пакете.

Данную атаку можно детектировать, анализируя загруженность сети, отслеживая возникающие ACK-бури.

Наиболее эффективным методом защиты является шифрование TCP/IP-трафика с использованием secure shell или IPSec.

Заметим, что на некоторых реализациях TCP/IP атака никогда на сработает. По стандарту при получении RST-пакета сессия должна просто закрываться, но некоторые реализации вместе с этим посылают встречный RST-пакет, закрывая сессию на противоположном конце.

5. Список Использованной Литературы

1. М Мамаев, С. Петренко «Технологии защиты информации в Интернете» (СПб: «Питер», 2002) http://athena.vvsu.ru/net/book/security.html
2. Внешние Атаки. Eric Detoisien Перевод: Иван Песин http://gazette.linux.ru.net/rus/articles/externalAttacks.html#282lfindex5
3. Безопасность TCP/IP. Вадим Колонцов. http://www.citforum.ru/internet/securities/tcpip.shtml