Удалённые атаки на хосты в Internet

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

Артамонов П. А., 319 группа
12.04.2007

Основной особенностью любой сетевой системы, как Internet, является то, что ее компоненты распределены в пространстве, а связь между ними осуществляется физически, при помощи сетевых соединений, и программно, при помощи механизма сообщений. При этом все управляющие сообщения и данные, пересылаемые между такой системы, передаются по сетевым соединениям в виде пакетов обмена. Эта особенность и является основной для рассматриваемых в этом эссе удаленных атак на хосты сети Internet.

Существующие на сегодня атаки можно классифицировать по следующим признакам:

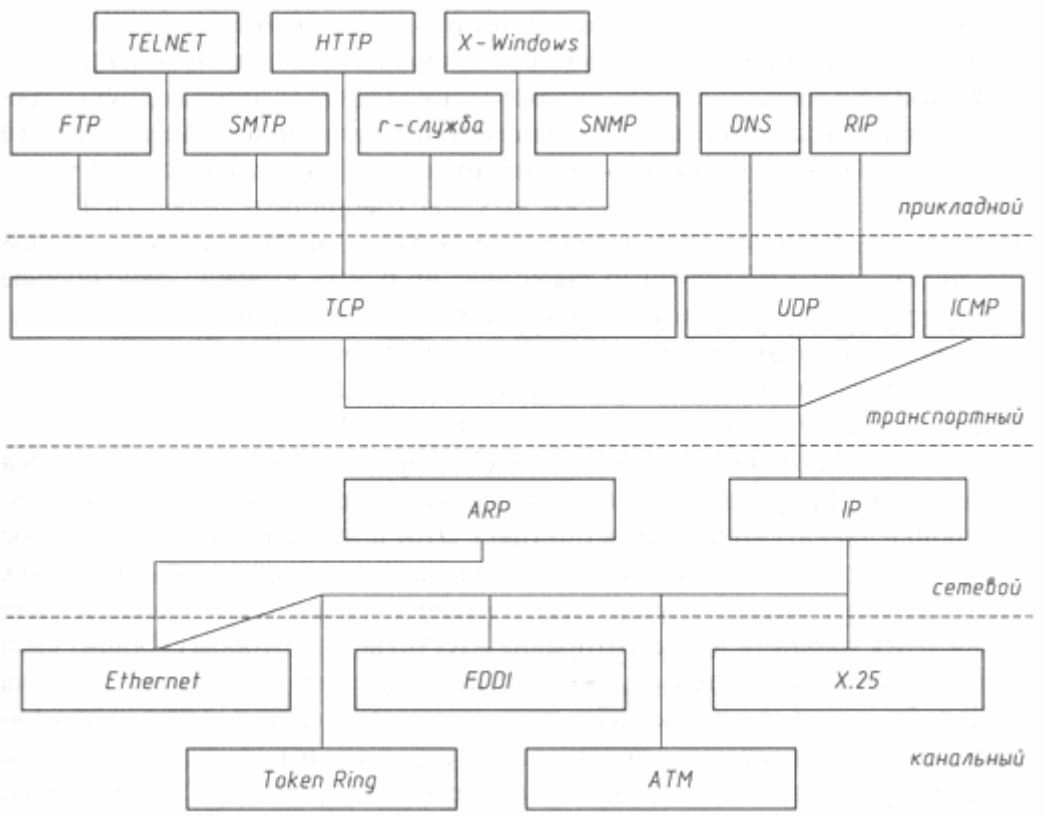
1. По характеру воздействия:
   - пассивное;
   - активное.
2. По цели воздействия:
   - нарушение конфиденциальности информации либо ресурсов;
   - нарушение целостности информации;
   - нарушение работоспособности (доступности) системы.
3. По условию начала осуществления воздействия:
   - атака по запросу от атакуемого объекта;
   - атака по наступлению ожидаемого события на атакуемом объекте;
   - безусловная атака.
4. По наличию обратной связи с атакуемым объектом:
   - с обратной связью;
   - без обратной связи (однонаправленная атака).
5. По расположению субъекта атаки относительно атакуемого объекта:
   - внутрисегментное;
   - межсегментное.
6. По уровню эталонной модели ISO/OSI, на котором осуществляется воздействие:
   - физический;
   - канальный;
   - сетевой;
   - транспортный;
   - сеансовый;
   - представительный;
   - прикладной.

Далее рассмотрим основные (исторические) виды атак на хосты Internet.

Анализ сетевого трафика сети Internet

Одним из способов получения паролей и идентификаторов пользователей в сети Internet, а также и другой передаваемой информации, является анализ сетевого трафика. Анализ передаваемых пакетов и выделение среди них необходимого осуществляется с помощью специальных программ. Так, например, сетевой анализ протоколов FTP и TELNET показывает, что TELNET пересылает пароль по одному символу, т.е. по символу в одном пакете, а FTP пересылает пароль целиком в одном пакете. Также, при не использовании в приложениях опций безопасной передачи пароля, в открытую передаются пароли электронной почты, ICQ и другие данные, необходимые, например, для доступа к какому-нибудь сайту.

Ложный ARP-сервер в сети Internet



Иерархия протоколов сети Internet в проекции на модель OSI

4-bit Version	4-bit Header Length	8-bit Type of Service	16-bit Total Length
16-bit Identification		3-bit Flags	13-bit Fragment Offset
8-bit Time to Live	8-bit Protocol	16-bit Header Checksum	
32-bit Source Address			
32-bit Destination Address			
Options & Padding			
Data			

Формат IP-пакета(v4)

Базовым сетевым протоколом обмена в Internet является протокол IP (Internet Protocol). Однако IP-пакет находится внутри аппаратного пакета, поэтому каждый пакет в конечном счете посылается на аппаратный адрес сетевого адаптера, непосредственно осуществляющего прием и передачу пакетов в сети. В сети Internet для решения этой задачи используется протокол ARP (Address Resolution Protocol). Так для Ethernet он позволяет получить взаимно однозначное соответствие IP- и Ethernet-адресов для хостов, находящихся внутри одного сегмента.

Схема создания ложного ARP-сервера выглядит следующим образом:

1. Ожидание ARP-запроса (широковещательного).
2. При получении такого запроса - передача по сети на запросивший хост ложного ARP-ответа, где указывается адрес сетевого адаптера ложного ARP-сервера. При этом необязательно указывать в ложном ARP-ответе свой настоящий адрес, так как сетевой адаптер можно запрограммировать на прием пакетов на любой адрес.
3. Прием, анализ, воздействие на пакеты обмена и передача их между взаимодействующими хостами.

Так как поисковый ARP-запрос кроме атакующего получит и маршрутизатор, то в его таблице окажется соответствующая запись об IP- и Ethernet-адресе атакуемого хоста. Для избежания того, чтобы пакеты с маршрутизатора шли напрямую на атакуемый хост можно,

например, получив ARP-запрос, можно самому послать такое же сообщение и присвоить себе данный IP-адрес или послать ARP-запрос, указав в качестве своего IP-адреса любой свободный в данном сегменте IP-адрес, и в дальнейшем вести работу с данного IP-адреса как с маршрутизатором, так и с атакуемым.

Ложный DNS-сервер в сети Internet

В современной сети Internet хост при обращении к удаленному серверу обычно знает его имя, но не IP-адрес, который необходим для непосредственной адресации. Решением задачи поиска IP-адреса сервера по имени и занимается служба DNS (Domain Name System) на базе протокола DNS.

Для осуществления атаки такого типа надо знать некоторые особенности работы службы DNS: служба DNS функционирует на базе протокола UDP (хотя возможен её перевод на протокол TCP); начальное значение поля "порт отправителя" в UDP-пакете >= 1023 и увеличивается с каждым переданным DNS-запросом; значение идентификатора (ID) DNS-запроса зависит от конкретного сетевого приложения, вырабатывающего запрос (оно может быть константой, так и изменяться с каждым новым запросом).

1. Перехват DNS-запроса

Рассмотрим обобщенную схему создания ложного DNS-сервера:

1. Ожидание DNS-запроса.
2. Извлечение из полученного сообщения необходимых сведений и передача по сети на запросивший хост ложного DNS-ответа от имени (с IP-адреса) настоящего DNS-сервера с указанием в этом ответе IP-адреса ложного DNS-сервера.
3. В случае получения пакета от хоста - изменение в IP-заголовке пакета его IP-адреса на IP-адрес ложного DNS-сервера и передача пакета на сервер.
4. В случае получения пакета от сервера - изменение в IP-заголовке пакета его IP-адреса на IP-адрес ложного DNS-сервера и передача пакета на хост.

Таким образом ложный DNS-сервер является для атакуемого настоящим сервером, а для настоящего сервера – обращающимся к нему хостом, а следовательно весь трафик между хостом и сервером будет проходить через ложный сервер.

Для успеха такой атаки необходимо, чтобы атакующий находился либо на пути основного трафика к серверу, либо в одном сегменте с DNS-сервером.

2. Направленный шторм ложных DNS-ответов на атакуемый хост

Это вторая разновидность атаки, основанной на ложном DNS-сервере, но в данном случае атакующему уже не обязательно находиться на пути следования трафика.

Для того, чтобы хост принял ответ от DNS-сервера необходимо выполнение следующих условий: IP-адрес отправителя ответа должен совпадать с IP-адресом DNS-сервера; имя в DNS-ответе - с именем в DNS-запросе; DNS-ответ должен направляться на тот же UDP-порт, с которого было послан запрос; поле идентификатора (ID) в заголовке DNS-ответа должно быть тем же, что и в запросе. Отсюда вытекают две проблемы: задание номера UDP-порта и значение ID запроса. Фактически, обе они решаются перебором: для UDP-порта перебираются все значения >=1023, а значение двухбайтового идентификатора либо равно 1, либо имеет не на много большее значение.

Схема предложенной удаленной атаки выглядит следующим образом:

1. Постоянная передача атакующим ложных DNS-ответов на различные UDP-порты атакуемого хоста и, возможно, с различными ID от имени (с IP-адреса) настоящего DNS-сервера, в которых указаны имя интересующего сервера и его ложный IP-адреса (IP-адрес хоста атакующего).
2. Если хост всё-таки принимает ложный DNS-ответ и отправляет пакет на IP-адрес атакующего, то в IP-заголовке пакета заменяется его IP-адреса на IP-адрес атакующего и пакет уже передаётся на реальный сервер.
3. При получении пакета от сервера в IP-заголовке пакета заменяется IP-адрес сервера на IP-адрес ложного сервера и пакет передаётся на атакуемый хост.

Ложный сервер снова является для атакуемого настоящим, а для настоящего сервера – обращающимся к нему хостом.

3. Перехват DNS-запроса или создание направленного шторма ложных DNS-ответов на DNS-сервер

Этот тип атаки уже направлен не на хост клиента, а на DNS-сервер.

Если DNS-сервер, получив запрос, не обнаружил указанное имя в своей базе имен, то такой запрос отсылается им на один из ответственных за домены верхних уровней DNS-серверов, адреса которых содержатся в файле настроек сервера, т.е. сам DNS-сервер является инициатором DNS-поиска, и изложенные выше схемы атаки могут быть применены в данной ситуации с переменой ролей: DNS-сервер – атакуемый хост, корневой DNS-сервер – реальный сервер. В данном случае ложные DNS-ответы будут направляться атакующим от имени корневого DNS-сервера на атакуемый DNS-сервер. Фактически, сам атакующий может спровоцировать DNS-сервер для ускорения процесса.

Также эта атака интересна тем, что, если принять во внимание кэширование DNS-сервером таблицы известных ему имён и IP-адресов хостов, а также добавление в эту таблицу новых имён и адресов, полученных в процессе работы, то обмануть можно не только один атакуемый хост, но и множество других, использующих этот DNS-сервер.

Конечно, здесь тоже не обходится без сложностей. В том случае, когда взломщик не может перехватить DNS-запрос на корневой сервер, для реализации атаки ему необходим шторм ложных DNS-ответов. При общении DNS-серверов исчезает проблема подбора порта, так как все запросы передаются на порт 53, но сложность подбора ID возрастает, так как его значение уже может доходить до 2^{16}.

Навязывание хосту ложного маршрута с использованием протокола ICMP

8-bit Type	8-bit Code	16-bit Checksum
32-bit Gateway Internet Address		
Internet Header + 64 bits of Original Data Datagram		

Заголовок сообщения ICMP Redirect Message

В сети Internet существует управляющий протокол ICMP (Internet Control Message Protocol), одной из функций которого является удаленное управление таблицей маршрутизации на хостах внутри сегмента сети. Таблица маршрутизации хоста состоит из пяти колонок: сетевой адрес (Network Destination), сетевая маска (Netmask), адрес маршрутизатора (Gateway), интерфейс (Interface) и метрика (Metric). Удаленное управление маршрутизацией реализовано в виде передачи с маршрутизатора на хост управляющего ICMP-сообщения Redirect Message. Для изменения маршрутизации на хосте второй байт заголовка ICMP Redirect Message должен быть равен 1. Этим можно воспользоваться с целью несанкционированного изменения маршрутизации на хосте, прислав от имени маршрутизатора IP-адрес хоста, для которого нужна смена маршрута (Destination), и новый IP-адрес маршрутизатора. Важным является то, что новый IP-адрес маршрутизатора должен принадлежать той же подсети, что и атакуемый хост.

В случае нахождения атакующего в том же сегменте сети, что и атакуемый хост, схема атаки выглядит следующим образом:

1. Передача на атакуемый хост ложного ICMP-сообщсния Redirect Datagrams for the Host.
2. Если пришел ARP-запрос от атакуемого хоста, то посылается ARP-ответ.
3. Если пришел пакет от атакуемого хоста, то он переправляется на настоящий маршрутизатор.
4. Если пришел пакет от маршрутизатора, то он переправляется на атакуемый хост.
5. При приеме пакета возможно воздействие на его содержание.

Общение хоста с сервером, маршрут к которому подменили, полностью происходит через хост атакующего.

В случае если атакующий находится за пределами сегмента атакуемого, то он может довольствоваться лишь тем, что нарушит работоспособность хоста, перенаправив его запросы к какому-нибудь серверу на другой хост подсети, который естественно не является маршрутизатором.

Подмена одного из субъектов TCP-соединения в сети Internet

<table>
<tr><td colspan="3">16-bit Source Port Number</td><td>16-bit Destination Port Number</td></tr>
<tr><td colspan="4">32-bit Sequence Number</td></tr>
<tr><td colspan="4">32-bit Acknowledgement Number</td></tr>
<tr><td>4-bit Header Length</td><td>6-bit Reserved</td><td>6-bit Flags</td><td>16-bit Window Size</td></tr>
<tr><td colspan="3">16-bit TCP Checksum</td><td>16-bit Urgent Pointer</td></tr>
<tr><td colspan="4">Options & Padding</td></tr>
<tr><td colspan="4">Data</td></tr>
</table>

Формат TCP-пакета

Transmission Control Protocol (TCP) является одним из базовых протоколов транспортного уровня сети Internet. Для идентификации TCP-пакета в его заголовке существуют два 32-разрядных идентификатора (счётчики пакетов) - Sequence Number (Номер последовательности) и Acknowledgment Number (Номер подтверждения). Также в пакете устанавливаются следующие флаги (слева направо): URG - Urgent Pointer Field Significant (Значение поля безотлагательного указателя), ACK - Acknowledgment Field Significant (Значение поля подтверждения), PSH - Push Function, RST - Reset the Connection (Восстановить соединение), SYN - Synchronize Sequence Numbers (Синхронизировать числа последовательности), FIN - No More Data from Sender (Конец передачи данных от отправителя).

Для установления соединения между хостами A и B по протоколу TCP используется следующая схема:

1. A >>> SYN, ISSa >>> B (ISSa - Initial Sequence Number хоста A)
2. A <<< SYN, ACK, ISSb, ACK(ISSa+l) <<< B (ACK - Acknowledgment Number)
3. A >>> ACK, ISSa+l, ACK(ISSb+l) >>> B
4. Передача данных в виде ACK, ISSa+l, ACK(ISSb+l); DATA.

Для осуществления подмены одного из хостов необходимо послать на другой хост пакет, в TCP-заголовке которого стояли бы правильные идентификаторы, а IP-заголовке IP-адрес атакующего, с которым и будет проходить дальнейшее общение. Если атакующий имеет возможность анализировать трафик между хостами, то задача подбора ISSa и ISSb является тривиальной. В противном случае их можно попробовать математически предсказать, опираясь на особенности генерации операционной системой Initial Sequence Number (ISN), либо просто получив это ISN, установив соединение с атакуемым хостом.

Фактически, атакующему может и не удастся заменить собой второй хост (если, например, атакуемый устанавливает соединения только с доверенными хостами), но при этом у него остаётся возможность, нейтрализовав второй хост, посылать от его имени пакеты атакуемому, например с какими-либо командами.

Направленный шторм ложных TCP-запросов на создание соединения

Для нарушения работоспособности хоста можно использовать направленный шторм TCP-запросов. Атака заключается в постоянной передаче на объект атаки ложных TCP-запросов на создание соединения от имени любого хоста. При этом в исходом атаки может быть как отказ в обслуживании, так и зависание системы. Это связано с тем, что атакуемая система должна сохранить в памяти полученную в ложных сообщениях информацию и

ответить на каждый запрос, что приводит к переполнению очереди запросов и необходимости для системы заниматься только ими. Также возможна другая ситуация, при которой не требуется постоянная передача запросов: получив максимальное число ложных TCP-запросов на подключение, система ответит на них и будет в течении некоторого периода времени (например 10 минут) ждать ответа от несуществующих хостов, не принимая новые запросы на соединения.

В эссе использованы материалы из книги «Атака на Internet» (http://bugtraq.ru/library/books/attack/)