16. МЕХАНИЗМЫ РЕАЛИЗАЦИИ УДАЛЕННЫХ АТАК В ГЛОБАЛЬНОЙ СЕТИ INTERNET

В настоящее время возможности по реализации удаленных атак в сети Internet настолько многообразны, что рассмотреть их все непредставляется возможным. Исследованиям уязвимостей отдельных операционных систем и особенностям функционирования операционных систем посвящено большое количество соответсвующей литературы. Цель данного раздела, не производя исчерпующего анализа механизмов отдельных удаленных атак, на отдельных простых примерах продемонстрировать реализации типовых уязвимостей рабочих станций в сети Internet.

16.1 Анализ сетевого трафика

В сети Internet основными базовыми протоколами удаленного доступа являются TELNET и FTP (File Transfer Protocol). TELNET - это протокол виртуального терминала (ВТ), позволяющий с удаленных хостов подключаться к серверам Internet в режиме ВТ. FTP - протокол, предназначенный для передачи файлов между удаленными хостами. Для получения доступа к серверу по данным протоколам пользователю необходимо пройти на нем процедуру идентификации и аутентификации. В качестве информации, идентифицирующей пользователя, выступает его идентификатор (имя), а для аутентификации используется пароль. Особенностью протоколов FTP и TELNET является то, что пароли и идентификаторы пользователей передаются по сети в открытом, незашифрованном виде. Таким образом, необходимым и достаточным условием для получения удаленного доступа к хостам по протоколам FTP и TELNET являются имя и пароль пользователя.

Одним из способов получения паролей и идентификаторов пользователей в сети Internet является анализ сетевого трафика. Сетевой анализ осуществляется с помощью специальной программы-анализатора пакетов, перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль (рис. 16.1). Сетевой анализ протоколов FTP и TELNET показывает, что TELNET разбивает пароль на символы и пересылает их по одному, помещая каждый символ из пароля в соответствующий пакет, а FTP, напротив, пересылает пароль целиком в одном пакете.

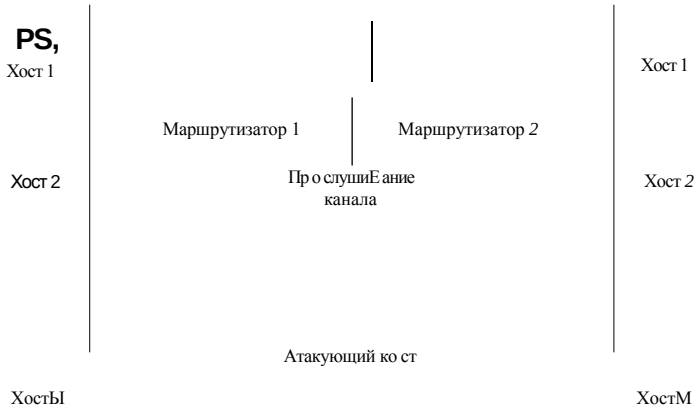

Рис. 16.1 - Анализ сетевого трафика

16.2 Ложный ARP-сервер

В вычислительных сетях связь между двумя удаленными хостами осуществляется путем передачи по сети сообщений, которые заключены в пакеты обмена. В общем случае передаваемый по сети пакет независимо от используемого протокола и типа сети (Token Ring, Ethernet, X.25 и др.) состоит из заголовка пакета и поля данных. В заголовок пакета обычно заносится служебная информация, определяемая используемым протоколом обмена и необходимая для адресации пакета, его идентификации, преобразования и т. д. В поле данных помещаются либо непосредственно данные, либо другой пакет более высокого уровня OSI.

Так, например, пакет транспортного уровня может быть вложен в пакет сетевого уровня, который, в свою очередь, вложен в пакет канального уровня. Таким образом, пакет TCP (транспортный уровень) вложен в пакет IP (сетевой уровень), который, в свою очередь, вложен в пакет Ethernet (канальный уровень). Схема на рис. 16.2 наглядно иллюстрирует как выглядит, например, TCP-пакет в сети Internet.

Ethernet-заголовок

IP-заголовок

TCP-заголовок

Данные

Рис. 16.2 - Структура TCP-пакета

Базовым сетевым протоколом обмена в сети Internet является протокол IP (Internet Protocol). Протокол IP - это межсетевой протокол, позволяющий передавать IP-пакеты в любую точку глобальной сети. Для адресации на сетевом уровне (IP-уровне) в сети Internet каждый хост имеет уникальный 32-разрядный IP-адрес. Для передачи IP-пакета на хост необходимо указать в IP-

заголовке пакета в поле Destination Address IP-адрес данного хоста. Однако, как видно из рис. 16.2, IP-пакет находится внутри Ethernet-пакета, поэтому каждый пакет в конечном счете адресуется на аппаратный адрес сетевого адаптера, непосредственно осуществляющего прием и передачу пакетов в сеть (при рассмотрении Ethernet-сети).

То есть, для адресации IP-пакетов в сети Internet кроме IP-адреса хоста необходим еще либо Ethernet-адрес его сетевого адаптера (в случае адресации внутри одной подсети), либо Ethernet-адрес маршрутизатора (в случае межсетевой адресации). Первоначально хост может не иметь информации о Ethernet-адресах других хостов, находящихся с ним в одном сегменте, в том числе и о Ethernet-адресе маршрутизатора. Следовательно, перед хостом встает стандартная проблема, решаемая с помощью алгоритма удаленного поиска.

В сети Internet для решения проблемы удаленного поиска Ethernet-адресов используется протокол ARP (Address Resolution Protocol). Протокол ARP позволяет получить взаимно однозначное соответствие IP- и Ethernet-адресов для хостов, находящихся внутри одного сегмента.

Это достигается следующим образом:

- При первом обращении к сетевым ресурсам хост отправляет широковещательный ARP-запрос на Ethernet-адрес FFFFFFFFFFFFh, в котором указывает IP-адрес маршрутизатора и просит сообщить его Ethernet-адрес. Этот широковещательный запрос получат все станции в данном сегменте сети, в том числе и маршрутизатор.
- Получив данный запрос, маршрутизатор внесет запись о запросившем хосте в свою ARP-таблицу, а затем отправит на запросивший хост ARP-ответ, в котором сообщит свой Ethernet-адрес.
- Полученный в ARP-ответе Ethernet-адрес будет занесен в ARP-таблицу, находящуюся в памяти операционной системы на запросившем хосте и содержащую записи соответствия IP- и Ethernet-адресов для хостов внутри одного сегмента.

В случае использования в РВС алгоритмов удаленного поиска существует возможность осуществления в такой сети типовой удаленной атаки «Ложный объект РВС». Из анализа безопасности протокола ARP становится ясно, что, перехватив на атакующем хосте внутри данного сегмента сети широковещательный ARP-запрос, можно послать ложный ARP-ответ, в котором объявить себя искомым хостом (например, маршрутизатором), и в дальнейшем активно контролировать и воздействовать на сетевой трафик «обманутого» хоста по схеме «Ложный объект РВС».

Рассмотрим обобщенную функциональную схему ложного ARP-сервера (рис. 16.3):

- ожидание ARP-запроса;

- при получении ARP-запроса передача по сети на запросивший хост ложного ARP-ответа, в котором указывается адрес сетевого адаптера атакующей станции (ложного ARP-сервера) или тот Ethernet-адрес, на котором будет принимать пакеты ложный ARP-сервер (совершенно необязательно указывать в ложном ARP-ответе свой настоящий Ethernet-адрес, так как при работе непосредственно с сетевым адаптером его можно запрограммировать на прием пакетов на любой Ethernet-адрес);
- прием, анализ, воздействие и передача пакетов обмена между взаимодействующими хостами, а также по возможности воздействие на перехваченную информацию.

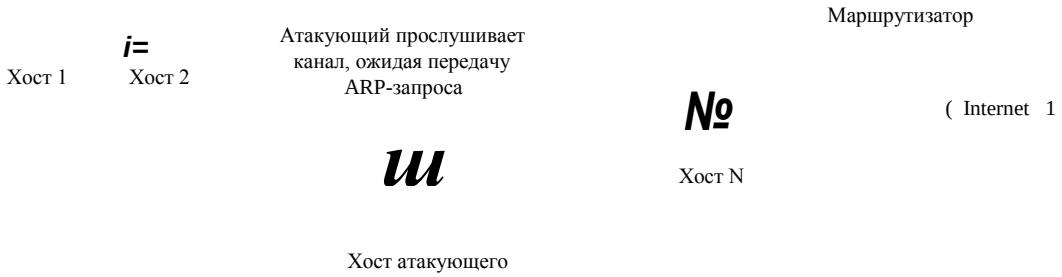

Рис. 16.3а - Фаза ожидания ARP-запроса

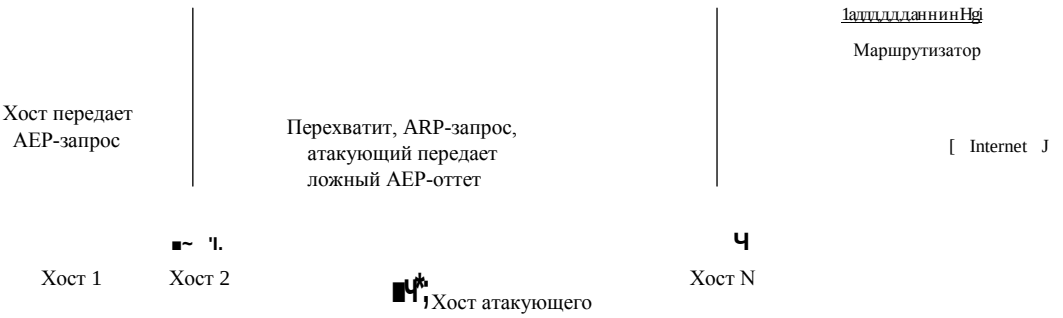

Рис. 16.3б - Фаза атаки

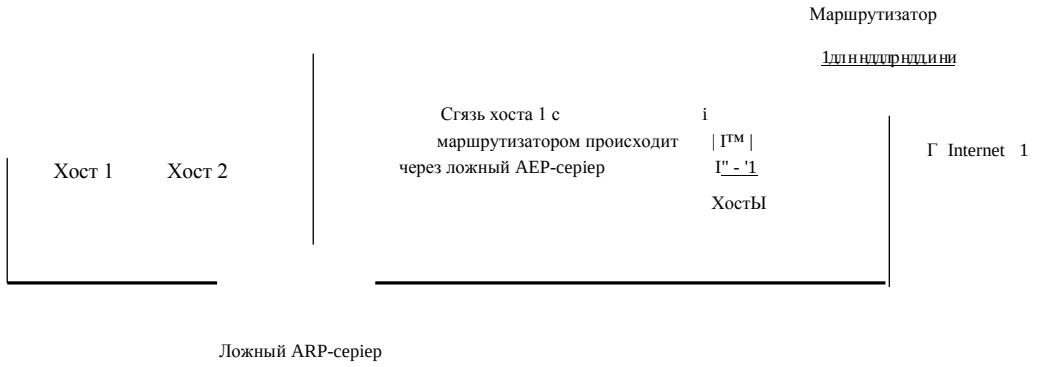

Рис. 16.3в - Фаза приема, анализа, воздействия и передачи перехваченной информации на ложном ARP-сервере

Рис. 16.3 - Ложный ARP-сервер

В заключение необходимо отметить, что, во-первых, причина успеха данной удаленной атаки кроется, не столько в Internet, сколько в широковещательной среде Ethernet и, во-вторых, очевидно, что эта удаленная атака является внутрисегментной и поэтому представляет угрозу только в случае нахождения атакующего внутри вашего сегмента сети.

16.3 Ложный DNS-сервер

Как известно, для обращения к хостам в сети Internet используются 32-разрядные IP-адреса, уникально идентифицирующие каждый сетевой компьютер в этой глобальной сети. Однако, для пользователей применение IP-адресов при обращении к хостам является не слишком удобным и далеко не самым наглядным. Использование в Internet породило проблему преобразования имен в IP-адреса. Такое преобразование необходимо, так как на сетевом уровне адресация пакетов идет не по именам, а по IP-адресам, следовательно, для непосредственной адресации сообщений в Internet имена не годятся. Для решения задачи преобразования мнемонически понятных для пользователей имен в IP-адреса была создана система преобразования имен, позволяющая хосту в случае отсутствия у него информации о соответствии имен и IP-адресов получить необходимые сведения от ближайшего информационно-поискового сервера – DNS (Domain Name System)-сервера.

Основной задачей, решаемой службой DNS является поиск по имени удаленного хоста его IP-адреса, который и необходим для непосредственной адресации.

Рассмотрим DNS-алгоритм удаленного поиска IP-адреса по имени в сети Internet.

- Хост посылает на IP-адрес ближайшего DNS-сервера (он устанавливается при настройке сетевой ОС) DNS-запрос, в котором указывает имя сервера, IP-адрес которого необходимо найти.
- DNS-сервер, получив запрос, просматривает свою базу имен на наличие в ней указанного в запросе имени. В случае, если имя найдено, а, следовательно, найден и соответствующий ему IP-адрес, то на запросивший хост DNS-сервер отправляет DNS-ответ, в котором указывает искомый IP-адрес.
- В случае, если указанное в запросе имя DNS-сервер не обнаружил в своей базе имен, то DNS-запрос отсылается DNS-сервером на один из корневых DNS-серверов и описанная в этом пункте процедура повторяется, пока имя не будет найдено (или не найдено).

Анализируя с точки зрения безопасности уязвимость этой схемы удаленного поиска с помощью протокола DNS, можно сделать вывод о возможности осуществления в сети, использующей протокол DNS, типовой удаленной атаки «Ложный объект РВС». Практические изыскания и

критический анализ безопасности службы DNS позволяют предложить три возможных варианта удаленной атаки на эту службу.

16.3.1 Внедрение в сеть Internet ложного DNS-сервера путем перехвата DNS-запроса

Для реализации атаки путем перехвата DNS-запроса атакующему необходимо перехватить DNS-запрос, извлечь из него номер UDP-порта отправителя запроса, двухбайтовое значение ID идентификатора DNS-запроса и искомое имя и затем послать ложный DNS-ответ на извлеченный из DNS-запроса UDP-порт, в котором указать в качестве искомого IP-адреса настоящий IP-адрес ложного DNS-сервера. Это позволит в дальнейшем полностью перехватить трафик между атакуемым хостом и сервером и активно воздействовать на него по схеме «Ложный объект РВС».

Рассмотрим обобщенную схему работы ложного DNS-сервера (рис. 16.4):

- ожидание DNS-запроса;
- извлечение из полученного запроса необходимых сведений и передача по сети на запросивший хост ложного DNS-ответа, от имени (с IP-адреса) настоящего DNS-сервера, в котором указывается IP-адрес ложного DNS-сервера;
- 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 (то есть ложный DNS-сервер ведет работу с сервером от своего имени);
- 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 (для хоста ложный DNS-сервер и есть настоящий сервер).

Необходимым условием осуществления данного варианта атаки является перехват DNS-запроса. Это возможно только в том случае, если атакующий находится либо на пути основного трафика, либо в сегменте настоящего DNS-сервера. Выполнение одного из этих условий местонахождения атакующего в сети делает подобную удаленную атаку трудно осуществимой на практике. Однако в случае выполнения этих условий возможно осуществить ***межсегментную*** удаленную атаку на сеть Internet.

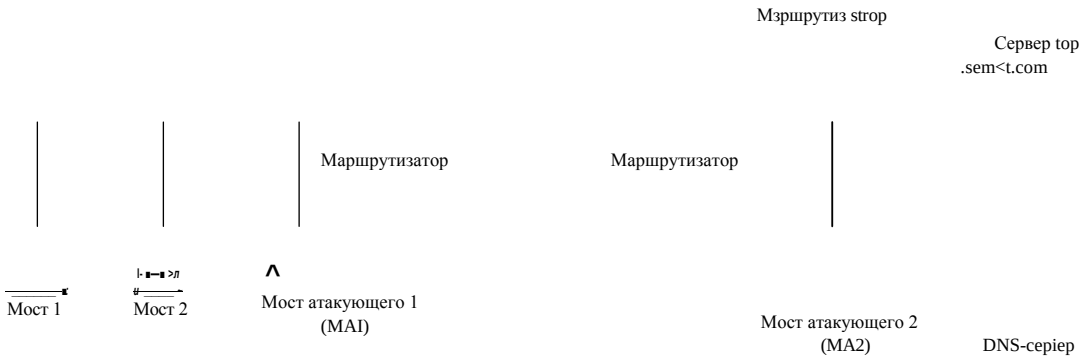

Рис. 16.4 а - Фаза ожидания атакующим DNS-запроса (он находится на ХА1, либо на ХА2)

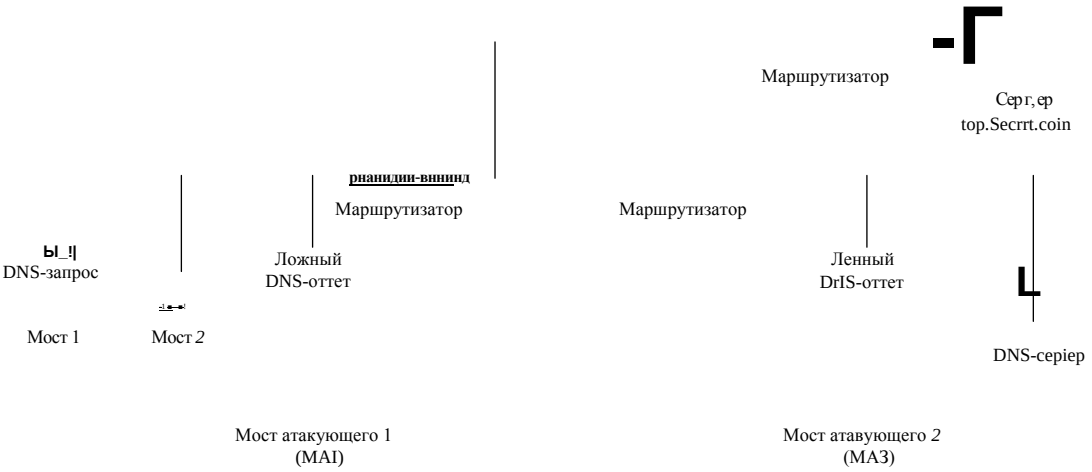

Рис. 16.4 б - Фаза передачи атакующим ложного DNS-ответа

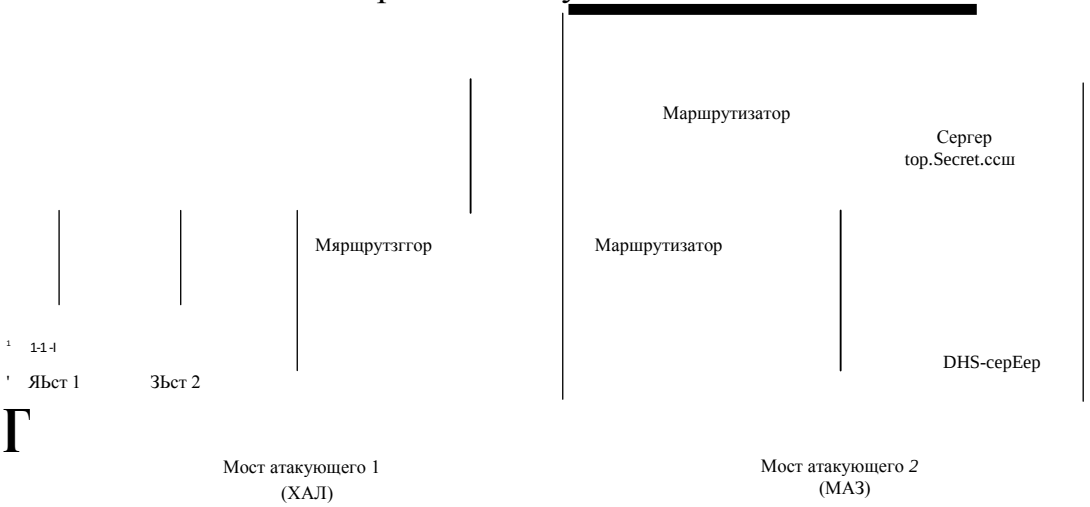

Рис. 16.4 в - Фаза приема, анализа, воздействия и передачи перехваченной информации на ложном сервере

Рис. 16.4 - Функциональная схема ложного DNS-сервера

16.3.2 Внедрение в сеть Internet ложного сервера путем создания направленного «шторма» ложных DNS-ответов на атакуемый хост

Другой вариант осуществления удаленной атаки, направленной на службу DNS, основан на второй разновидности типовой УА «Ложный объект РВС» (при использовании недостатков алгоритмов удаленного поиска). В этом случае атакующий осуществляет постоянную передачу на атакуемый хост заранее подготовленного ложного DNS-ответа от имени настоящего DNS-сервера *без приема DNS-запроса*! Другими словами, атакующий создает в сети Internet направленный «шторм» ложных DNS-ответов.

Это возможно, так как обычно для передачи DNS-запроса используется протокол UDP, в котором отсутствуют средства идентификации пакетов. Критериями, предъявляемыми сетевой ОС хоста к полученному от DNS-сервера ответу, является:

- совпадение IP-адреса отправителя ответа с IP-адресом DNS-сервера;
- DNS-ответ должен содержать то же имя, что и в DNS-запросе,
- DNS-ответ должен быть направлен на тот же UDP-порт, с которого был послан DNS-запрос (в данном случае это первая проблема для атакующего),
- в DNS-ответе поле идентификатора запроса в заголовке DNS (ID) должно содержать то же значение, что и в переданном DNS-запросе (а это вторая проблема).

В данном случае, так как атакующий не имеет возможности перехватить DNS-запрос, то основную проблему для него представляет номер UDP-порта, с которого был послан запрос. Однако, как было отмечено ранее, номер порта отправителя принимает ограниченный набор значений ($\geq$ 1023), поэтому атакующему достаточно действовать простым перебором, направляя ложные ответы на соответствующий перечень портов. На первый взгляд, второй проблемой может быть двухбайтовый идентификатор DNS-запроса, но, в связи с особенностями функционироания протокола DNS он либо равен единице, либо в случае DNS-запроса от Netscape Navigator (например) имеет значение близкое к нулю (один запрос - ID увеличивается на 1).

Поэтому для осуществления данной удаленной атаки атакующему необходимо выбрать интересующий его хост (например, ***top.secret.com***), маршрут к которому требуется изменить так, чтобы он проходил через ложный сервер - хост атакующего. Это достигается постоянной передачей (направленным «штормом») атакующим ложных DNS-ответов на атакуемый хост от имени настоящего DNS-сервера на соответствующие UDP-порты. В этих ложных DNS-ответах указывается в качестве IP-адреса хоста ***top.secret.com*** IP-адрес атакующего.

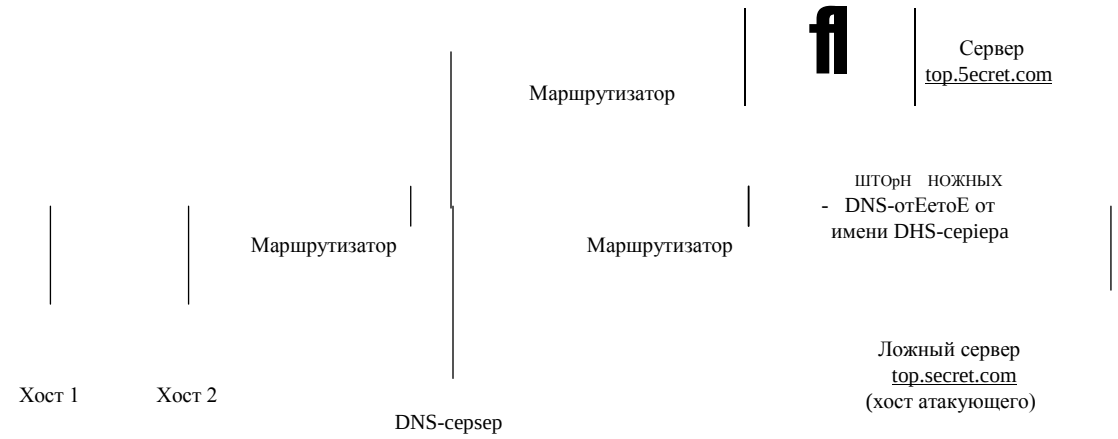

Рис. 16.5 а - Атакующий создает направленный «шторм» ложных DNS-ответов на Хост 1

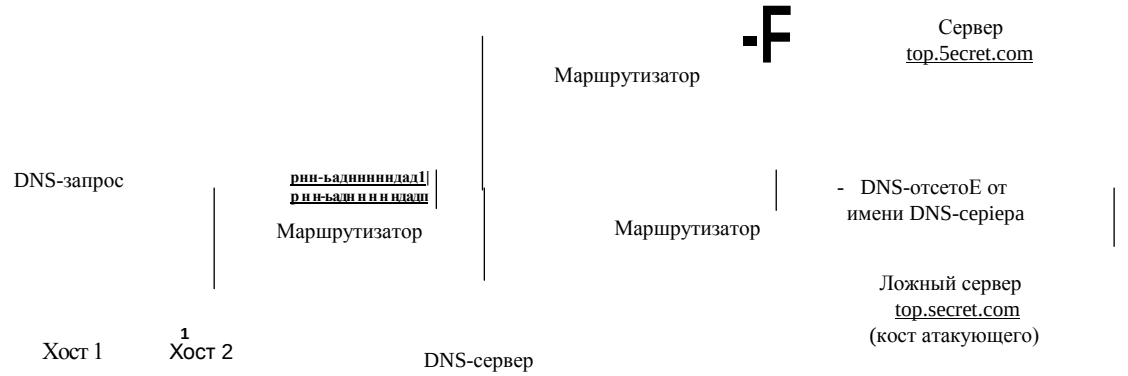

Рис. 16.5 б - Хост 1 посылает DNS-запрос и немедленно получает ложный DNS-ответ

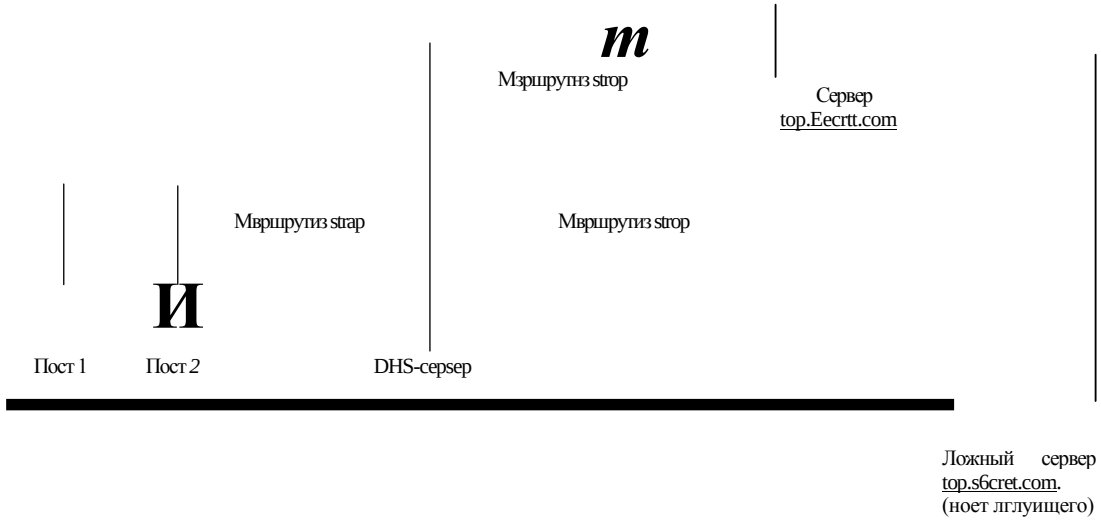

Рис. 16.5 в - Фаза приема, анализа, воздействия и передачи перехваченной информации на ложном сервере

Рис. 16.5 - Внедрение в Internet ложного сервера путем создания направленного «шторма» ложных DNS-ответов на атакуемый хост

Далее атака развивается по следующей схеме. Как только цель атаки (атакуемый хост) обратится по имени к хосту ***top.secret.com***, то от данного

хоста в сеть будет передан DNS-запрос, который атакующий никогда не получит, но этого ему и не требуется, так как на хост сразу же поступит постоянно передаваемый ложный DNS-ответ, что и будет воспринят ОС атакуемого хоста как настоящий ответ от DNS-сервера. Все! Атака состоялась, и теперь атакуемый хост будет передавать все пакеты, предназначенные для ***top.secret.com***, на IP-адрес хоста атакующего, который, в свою очередь, будет переправлять их на ***top.secret.com***, воздействуя на перехваченную информацию по схеме «Ложный объект РВС».

Рассмотрим функциональную схему предложенной удаленной атаки на службу DNS:

- постоянная передача атакующим ложных DNS-ответов на атакуемый хост на различные UDP-порты и, возможно, с различными ID, от имени (с IP-адреса) настоящего DNS-сервера с указанием имени интересующего хоста и его ложного IP-адреса, которым будет являться IP-адрес ложного сервера - хоста атакующего;
- в случае получения пакета от хоста, изменение в IP-заголовке пакета его IP-адреса на IP-адрес атакующего и передача пакета на сервер (то есть ложный сервер ведет работу с сервером от своего имени - со своего IP-адреса);
- в случае получения пакета от сервера, изменение в IP-заголовке пакета его IP-адреса на IP-адрес ложного сервера и передача пакета на хост (для хоста ложный сервер и есть настоящий сервер).

Таким образом, реализация данной удаленной атаки, использующей пробелы в безопасности службы DNS, позволяет из любой точки сети Internet нарушить маршрутизацию между двумя заданными объектами (хостами)! Данная удаленная атака осуществляется межсегментно по отношению к цели атаки и угрожает безопасности любого хоста Internet, использующего обычную службу DNS.

16.3.3 Внедрение в сеть Internet ложного сервера путем перехвата DNS-запроса или создания направленного «шторма» ложных DNS-ответов на атакуемый DNS-сервер

Из рассмотренной схемы удаленного DNS-поиска следует, что в том случае, если указанное в запросе имя DNS-сервер не обнаружил в своей базе имен, то запрос отсылается сервером на один из корневых DNS-серверов, адреса которых содержатся в файле настроек сервера ***root.cache***.

Итак, в случае, если DNS-сервер не имеет сведений о запрашиваемом хосте, то он сам, пересылая запрос далее, является инициатором удаленного DNS-поиска. Поэтому ничто не мешает атакующему, действуя описанными в предыдущих пунктах методами, *перенести свою атаку непосредственно на DNS-сервер*. В качестве цели атаки теперь будет выступать не хост, а DNS-

сервер и ложные DNS-ответы будут направляться атакующим от имени корневого DNS-сервера на атакуемый DNS-сервер.

При этом важно учитывать следующую особенность работы DNS-сервера. Для ускорения работы каждый DNS-сервер кэширует в области памяти свою таблицу соответствия имен и IP-адресов хостов. В том числе в кэш заносится динамически изменяемая информация об именах и IP-адресах хостов, найденных в процессе функционирования DNS-сервера, а именно, если DNS-сервер, получив запрос, не находит у себя в кэш-таблице соответствующей записи, он пересылает ответ на следующий сервер и, получив ответ, заносит найденные сведения в кэш-таблицу в память. Таким образом, при получении следующего запроса DNS-серверу уже не требуется вести удаленный поиск, так как необходимые сведения уже находятся у него в кэш-таблице.

Из анализа только что подробно описанной схемы удаленного DNS-поиска становится очевидно, что в том случае, если в ответ на запрос от DNS-сервера атакующий направит ложный DNS-ответ (или в случае «шторма» ложных ответов будет вести их постоянную передачу), то в кэш-таблице сервера появится соответствующая запись с ложными сведениями и в дальнейшем все хосты, обратившиеся к данному DNS-серверу, будут дезинформированы, и при обращении к хосту, маршрут к которому атакующий решил изменить, связь с ним будет осуществляться через хост атакующего по схеме «Ложный объект РВС». И, что хуже всего, с течением времени эта ложная информация, попавшая в кэш DNS-сервера, будет распространяться на соседние DNS-серверы высших уровней, а, следовательно, все больше хостов в Internet будут дезинформированы и атакованы!

В том случае, если атакующий не может перехватить DNS-запрос от DNS-сервера, то для реализации атаки ему необходим «шторм» ложных DNS-ответов, направленный на DNS-сервер. При этом возникает следующая проблема, отличная от проблемы подбора портов в случае атаки, направленной на хост. Как уже отмечалось ранее, DNS-сервер, посылая запрос на другой DNS-сервер, идентифицирует этот запрос двухбайтовым значением (ID). Это значение увеличивается на единицу с каждым передаваемым запросом. Узнать атакующему это текущее значение идентификатора DNS-запроса не представляется возможным. Поэтому предложить что-либо, кроме перебора 2^{16} возможных значений ID, достаточно сложно. Зато исчезает проблема перебора портов, так как все DNS-запросы передаются DNS-сервером на 53 порт.

Следующая проблема, являющаяся условием осуществления этой удаленной атаки на DNS-сервер при направленном «шторме» ложных DNS-ответов, состоит в том, что атака будет иметь успех только в случае, если DNS-сервер пошлет запрос на поиск имени, которое содержится в ложном DNS-ответе. DNS-сервер посылает этот столь необходимый и желанный для атакующего запрос в том и только том случае, когда на него приходит DNS-

запрос от какого-либо хоста на поиск данного имени и этого имени не оказывается в кэш-таблице DNS-сервера. В принципе, этот запрос может возникнуть когда угодно, и атакующему придется ждать результатов атаки неопределенное время. Однако, ничто не мешает атакующему, не дожидаясь никого, самому послать на атакуемый DNS-сервер подобный DNS-запрос и ***спровоцировать*** DNS-сервер на поиск указанного в запросе имени. Тогда эта атака с большой вероятностью будет иметь успех практически сразу же после начала ее осуществления.

Для примера вспомним скандал (28 октября 1996 года) с одним из московских провайдеров Internet - компанией РОСНЕТ, когда пользователи данного провайдера при обращении к обычному информационному WWW-серверу попадали, как было сказано в телевизионном репортаже, WWW-сервер «сомнительного» содержания. В связи с абсолютным непониманием случившегося как журналистами (их можно понять - они не специалисты в этом вопросе), так и теми, кто проводил пресс-конференцию (специалистов к общению с прессой, наверное, просто не допустили) информационные сообщения о данном событии были настолько убоги, что понять, что случилось, было толком невозможно. Тем не менее, этот инцидент вполне укладывается в только что описанную схему удаленной атаки на DNS-сервер. С одним исключением: вместо адреса хоста атакующего в кэш-таблицу DNS-сервера был занесен IP-адрес хоста ***www.playboy.com***.

Рис. 16.6 а - Фаза ожидания атакующим DNS-запроса от DNS-сервера (для ускорения атакующий генерирует необходимый DNS-запрос)

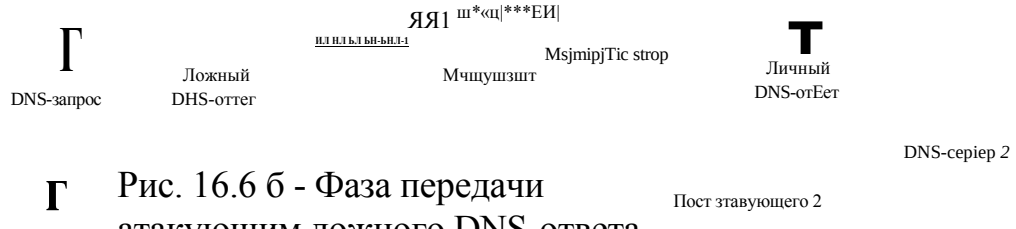

Рис. 16.6 б - Фаза передачи атакующим ложного DNS-ответа на DNS-сервер 1

Рис. 16.6 - Внедрение в Internet ложного сервера путем перехвата DNS-запроса от DNS-сервера

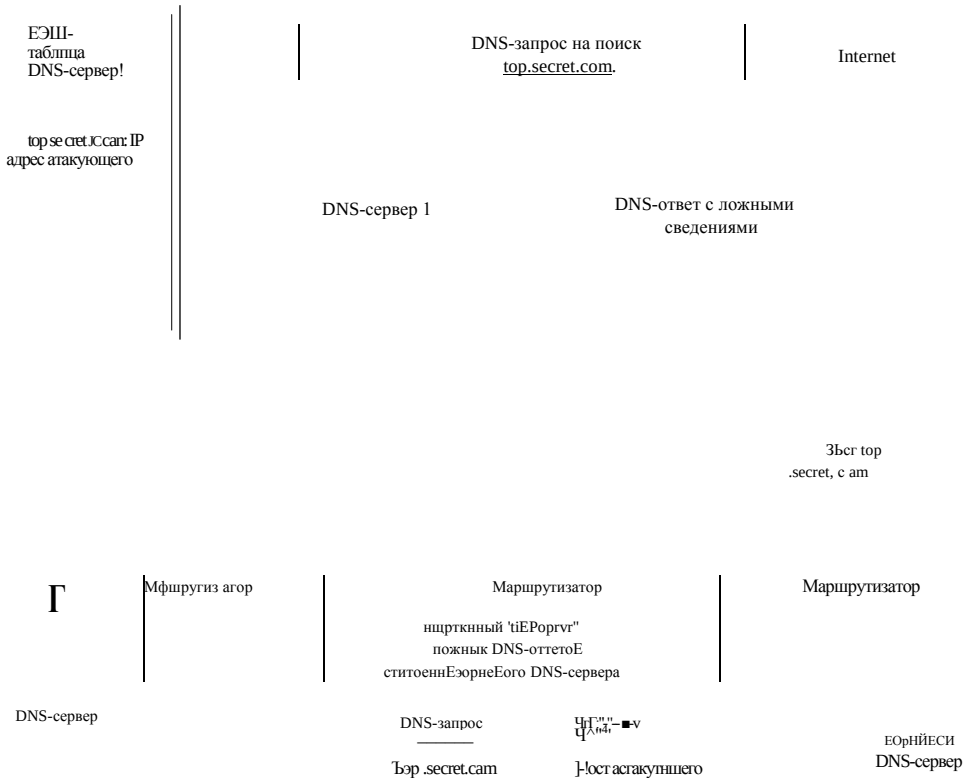

Рис16.7 а - Атакующий создает направленный «шторм» ложных DNS-ответов от имени одного из корневых DNS-серверов и при этом провоцирует атакуемый DNS-сервер, посылая DNS-запрос

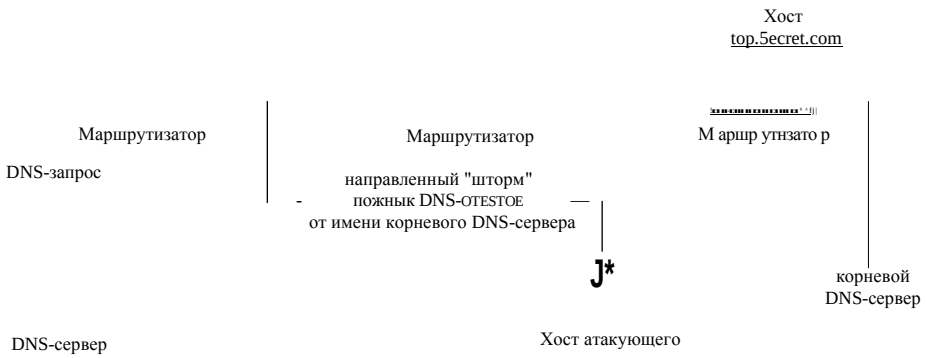

Рис16.7 б - DNS-сервер передает DNS-запрос на корневой DNS-сервер и немедленно получает ложный DNS-ответ от атакующего

Рис. 16.7 - Внедрение в Internet ложного сервера путем создания направленного «шторма» ложных DNS-ответов на атакуемый DNS-сервер

Использование в сети Internet службы удаленного поиска DNS позволяет атакующему организовать в Internet удаленную атаку на любой хост, пользующийся услугами данной службы, и может пробить серьезную брешь в безопасности этой и так отнюдь не безопасной глобальной сети.

16.4 Навязывание хосту ложного маршрута с использованием протокола ICMP с целью создания в сети Internet ложного маршрутизатора

В сети Internet используется управляющий протокол ICMP, одной из функций которого является удаленное управление маршрутизацией на хостах внутри сегмента сети. Удаленное управление маршрутизацией необходимо для предотвращения возможной передачи сообщений по неоптимальному маршруту. В сети Internet удаленное управление маршрутизацией реализовано в виде передачи с маршрутизатора на хост управляющего ICMP-сообщения: Redirect Message. Исследование протокола ICMP показало, что сообщение Redirect бывает двух типов:

- Первый тип сообщения носит название Redirect Net и уведомляет хост о необходимости смены адреса маршрутизатора, то есть default-маршрута.
- Второй тип - Redirect Host - информирует хост о необходимости создания нового маршрута к указанной в сообщении системе и внесения ее в таблицу маршрутизации. Для этого в сообщении указывается IP-адрес хоста, для которого необходима смена маршрута (адрес будет занесен в поле Destination), и новый IP-адрес маршрутизатора, на который необходимо направлять пакеты, адресованные данному хосту (этот адрес заносится в поле Gateway).

Необходимо обратить внимание на важное ограничение, накладываемое на IP-адрес нового маршрутизатора: он должен быть в пределах адресов данной подсети!

Что касается управляющего сообщения ICMP Redirect Host, то единственным идентифицирующим его параметром является IP-адрес отправителя, который должен совпадать с IP-адресом маршрутизатора, так как это сообщение может передаваться только маршрутизатором. Особенность протокола ICMP состоит в том, что он не предусматривает никакой дополнительной аутентификации источников сообщений. Таким образом, ICMP-сообщения передаются на хост маршрутизатором однонаправлено, без создания виртуального соединения.

Следовательно, ничто не мешает атакующему послать ложное ICMP-сообщение о смене маршрута от имени маршрутизатора. Приведенные выше факты позволяют осуществить типовую удаленную атаку «Внедрение в РВС ложного объекта путем навязывания ложного маршрута”.

Для осуществления этой удаленной атаки необходимо подготовить ложное ICMP Redirect Host сообщение, в котором указать конечный IP-адрес маршрута (адрес хоста, маршрут к которому будет изменен) и IP-адрес ложного маршрутизатора. Далее это сообщение передается на атакуемый хост от имени маршрутизатора. Для этого в IP-заголовке в поле адреса отправителя указывается IP-адрес маршрутизатора. В принципе, можно предложить два варианта данной удаленной атаки.

В первом случае атакующий находится в том же сегменте сети, что и цель атаки. Тогда, послав ложное ICMP-сообщение, он в качестве IP-адреса нового маршрутизатора может указать либо свой IP-адрес, либо любой из адресов данной подсети. Это даст атакующему возможность изменить маршрут передачи сообщений, направляемых атакованным хостом на определенный IP-адрес, и получить контроль над трафиком между атакуемым хостом и интересующим атакующего сервером. После этого атака перейдет во вторую стадию, связанную с приемом, анализом и передачей пакетов, получаемых от «обманутого» хоста.

Рассмотрим функциональную схему осуществления этой удаленной атаки (рис 16.8):

- передача на атакуемый хост ложного ICMP Redirect Host сообщения;
- отправление ARP-ответа в случае, если пришел ARP-запрос от атакуемого хоста;
- перенаправление пакетов от атакуемого хоста на настоящий маршрутизатор;
- перенаправление пакетов от маршрутизатора на атакуемый хост;
- при приеме пакета возможно воздействие на информацию по схеме «Ложный объект РВС».

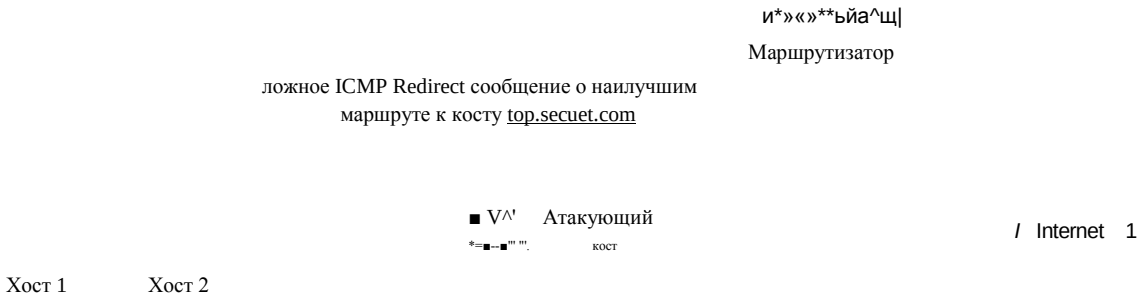

Рис16.8 а - Фаза передачи ложного ICMP Redirect сообщения от имени маршрутизатора.

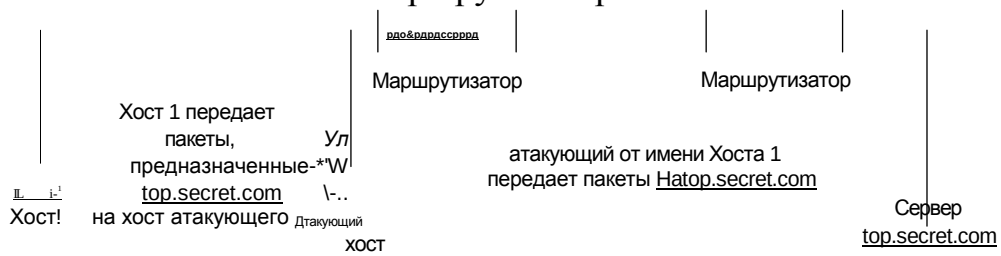

Рис 16.8 б - Фаза приема, анализа, воздействия и передачи перехваченной информации на ложном сервере

Рис. 16.8 -Внутрисегментное навязывание хосту ложного маршрута при использовании протокола ICMP

В случае осуществления второго варианта удаленной атаки атакующий находится в другом сегменте относительно цели атаки. Тогда, в случае передачи на атакуемый хост ложного ICMP Redirect сообщения, сам атакующий уже не сможет получить контроль над трафиком, так как адрес нового маршрутизатора должен находиться в пределах подсети атакуемого хоста, поэтому использование данного варианта этой удаленной атаки не позволит атакующему получить доступ к передаваемой по каналу связи информации. Однако, в этом случае атака достигает другой цели: нарушается работоспособность хоста.

Атакующий с любого хоста в Internet может послать подобное сообщение на атакуемый хост и в случае, если сетевая ОС на данном хосте не проигнорирует данное сообщение, то связь между данным хостом и указанным в ложном ICMP-сообщении сервером будет нарушена. Это произойдет из-за того, что все пакеты, направляемые хостом на этот сервер, будут отправлены на IP-адрес несуществующего маршрутизатора. Схема этой атаки приведена на рис. 16.9.

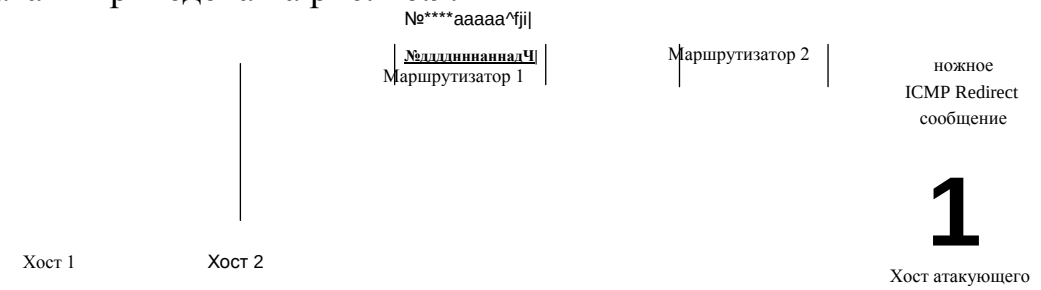

Рис. 16.9 а - Передача атакующим на хост 1 ложного ICMP Redirect сообщения от имени маршрутизатора 1

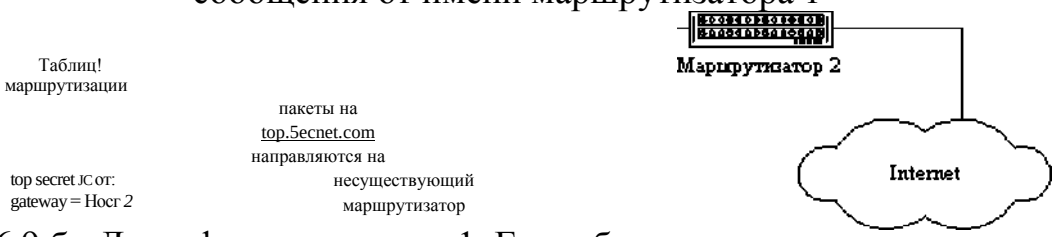

Рис. 16.9 б - Дезинформация хоста 1. Его таблица маршрутизации содержит формацию о ложном маршруте к хосту top.secret.com

Межсегментное навязывание хосту ложного маршрута
протокола ICMP, приводящее к отказу в обслуживании

С Хост 2), а,
следовательно,
СЕЯЗЬ с
top.5ecnet.com
нарушается

использовании

при

Оба варианта рассмотренной удаленной атаки удается осуществить (как межсегментно, так и внутрисегментно) на ОС Linux 1.2.8, Windows 95 и Windows NT 4.0. Остальные сетевые ОС (Linux 2.0.0 и защищенный по классу B1 UNIX), игнорировали данное ICMP Redirect сообщение (что, не

правда ли, кажется вполне логичным с точки зрения обеспечения безопасности).

16.5 Подмена одного из субъектов TCP-соединения в сети Internet

Протокол TCP (Transmission Control Protocol) является одним из базовых протоколов транспортного уровня сети Internet. Этот протокол позволяет исправлять ошибки, которые могут возникнуть в процессе передачи пакетов, и является протоколом с установлением логического соединения - виртуального канала. По этому каналу передаются и принимаются пакеты с регистрацией их последовательности, осуществляется управление потоком пакетов, организовывается повторная передача искаженных пакетов, а в конце сеанса канал разрывается. При этом протокол TCP является единственным базовым протоколом из семейства TCP/IP, имеющим дополнительную систему идентификации сообщений и соединения. Именно поэтому протоколы прикладного уровня FTP и TELNET, предоставляющие пользователям удаленный доступ на хосты Internet, реализованы на базе протокола TCP.

Для идентификации TCP-пакета в TCP-заголовке существуют два 32-разрядных идентификатора, которые также играют роль счетчика пакетов. Их названия - **Sequence Number** и **Acknowledgment Number**. Также нас будет интересовать поле, называемое **Control Bits**.

Это поле размером 6 бит может содержать следующие командные биты (слева направо):

- **URG**: Urgent Pointer field significant,
- **ACK**: Acknowledgment field significant,
- **PSH**: Push Function,
- **RST**: Reset the connection,
- **SYN**: Synchronize sequence numbers,
- **FIN**: No more data from sender.

Далее рассмотрим схему создания TCP-соединения (рис 16.10).
Предположим, что хосту **A** необходимо создать TCP-соединение с хостом **B**. Тогда **A** посылает на **B** следующее сообщение:

1. **A → B:** SYN, ISSa

Это означает, что в передаваемом **A** сообщении установлен бит SYN *(synchronize sequence number),* а в поле *Sequence Number* установлено начальное 32-битное значение *ISSa (Initial Sequence Number).*

2. B отвечает:

B → A: SYN, ACK, ISSb, ACK(ISSa+1) В ответ на полученный от **A** запрос **B** отвечает сообщением, в котором установлен бит SYN и установлен бит ACK; в поле *Sequence Number* хостом

B устанавливается свое начальное значение счетчика - *ISSb;* поле *Acknowledgment Number* содержит значение *ISSa,* полученное в первом пакете от хоста **A** и увеличенное на единицу.

3. A, завершая рукопожатие (handshake), посылает:

A → B: ACK, ISSa+1, ACK(ISSb+1) В этом пакете установлен бит *ACK;* поле *Sequence Number* содержит *ISSa + 1;* поле *Acknowledgment Number* содержит значение ISSb + 1. Посылкой этого пакета на хост **B** заканчивается трехступенчатый handshake, и TCP-соединение между хостами **A** и **B** считается установленным.

4. Теперь хост **A** может посылать пакеты с данными на хост **B** по только что созданному виртуальному TCP-каналу:

A → B: ACK, ISSa+1, ACK(ISSb+1); DATA

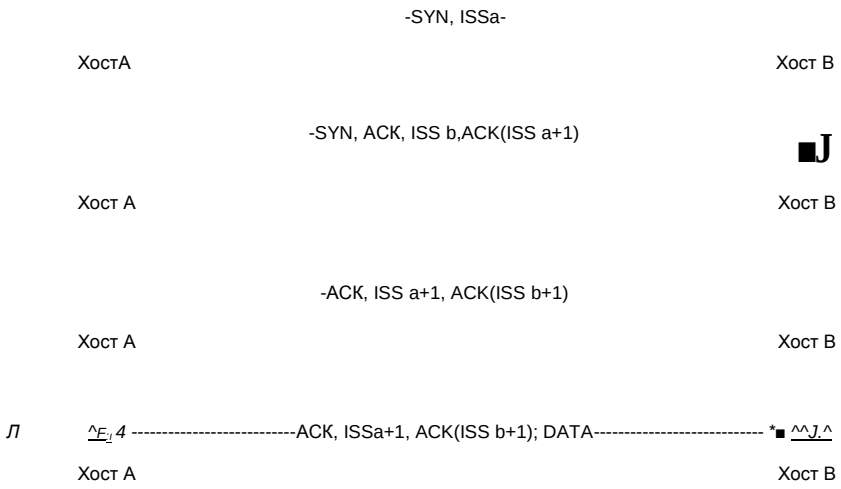

Рис. 16.10 - Схема создания TCP-соединения

Из рассмотренной выше схемы создания TCP-соединения видно, что единственными идентификаторами TCP-абонентов и TCP-соединения являются два 32-бит-ных параметра *Sequence Number* и *Acknowledgment Number*. Следовательно, для формирования ложного TCP-пакета атакующему необходимо знать текущие идентификаторы для данного соединения - *ISSa* и *ISSb.*

Проблема возможной подмены TCP-сообщения становится еще более важной, так как анализ протоколов FTP и TELNET, реализованных на базе протокола TCP, показал, что проблема идентификации FTP- и TELNET-пакетов целиком возлагается данными протоколами на транспортный уровень, то есть на TCP. Это означает, что атакующему достаточно, подобрав соответствующие текущие значения идентификаторов TCP-пакета для данного TCP-соединения (например, данное соединение может представлять собой FTP- или TELNET-подклю-чение), послать пакет с *любого хоста в*

сети Internet от имени одного из участников данного соединения (например, от имени клиента), и данный пакет будет воспринят как верный! К тому же, так как FTP и TELNET ***не проверяют*** IP-адреса отправителей, от которых им приходят сообщения, то в ответ на полученный ложный пакет, *FTP- или TELNET-сервер отправит ответ на указанный в ложном пакете настоящий IP-адрес атакующего, то есть атакующий начнет работу с FTP- или TELNET-сервером со своего IP-адреса, но с правами легально подключившегося пользователя, который, в свою очередь, потеряет связь с сервером из-за рассогласования счетчиков.*

16.6 Нарушение работоспособности хоста в сети Internet при использовании направленного «шторма» ложных TCP-запросов на создание соединения, либо при переполнении очереди запросов

Из рассмотренной в предыдущем пункте схемы создания TCP-соединения следует, что на каждый полученный TCP-запрос на создание соединения операционная система должна сгенерировать начальное значение идентификатора ISN и отослать его в ответ на запросивший хост. При этом, так как в сети Internet (стандарта IP v.4) не предусмотрен контроль за IP-адресом отправителя сообщения, то невозможно отследить истинный маршрут, пройденный IP-пакетом, и, следовательно, у конечных абонентов сети нет возможности ограничить число возможных запросов, принимаемых в единицу времени от одного хоста. Поэтому возможно осуществление типовой УА «Отказ в обслуживании», которая будет заключаться в передаче на атакуемый хост как можно большего числа ложных TCP-запросов на создание соединения от имени любого хоста в сети (рис. 16.11).

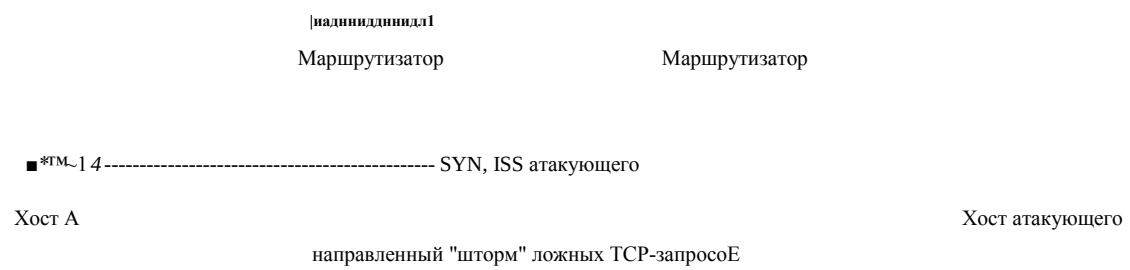

Рис. 16.11 - Нарушение работоспособности хоста в Internet, использующее направленный шторм ложных TCP-запросов на создание соединения

При этом атакуемая сетевая ОС в зависимости от вычислительной зависимости от мощности компьютера
либо - в худшем случае - практически зависает, либо -в лучшем случае - перестает реагировать на легальные запросы на подключение (отказ в обслуживании). Это происходит из-за того, что для всей массы полученных ложных запросов система должна, во-первых, сохранить в памяти полученную в каждом запросе информацию и, во-вторых, выработать и отослать ответ на каждый запрос. Таким образом, все

ресурсы системы «съедаются» ложными запросами: переполняется очередь запросов и система занимается только их обработкой. Эффективность данной удаленной атаки тем выше, чем больше пропускная способность канала между атакующим и целью атаки, и тем меньше, чем больше вычислительная мощь атакуемого компьютера (число и быстродействие процессоров, объем ОЗУ и т. д.).

Другая разновидность атаки «Отказ в обслуживании» состоит в передаче на атакуемый хост нескольких десятков (сотен) запросов на подключение к серверу, что может привести к временному (до 10 минут) переполнению очереди запросов на сервере. Это происходит из-за того, что некоторые сетевые ОС устроены так, чтобы обрабатывать только первые несколько запросов на подключение, а остальные - игнорировать. То есть при получении N запросов на подключение, ОС сервера ставит их в очередь и генерирует соответственно N ответов. Далее, в течение определенного промежутка времени, сервер будет дожидаться от предполагаемого клиента сообщения, завершающего handshake и подтверждающего создание виртуального канала с сервером. Если атакующий пришлет на сервер количество запросов на подключение, равное максимальному числу одновременно обрабатываемых запросов на сервере, то в течение тайм-аута остальные запросы на подключение будут игнорироваться и к серверу будет невозможно подключиться.

Необходимо отметить, что в существующем стандарте сети Internet IP v4 нет приемлемых способов надежно обезопасить свои системы от этой удаленной атаки. К счастью, атакующий в результате осуществления описанной атаки не сможет получить несанкционированный доступ к вашей информации. Он сможет лишь «съесть» вычислительные ресурсы вашей системы и нарушить ее связь с внешним миром. Остается надеяться, что нарушение работоспособности вашего хоста просто никому не нужно.