Лекция 10

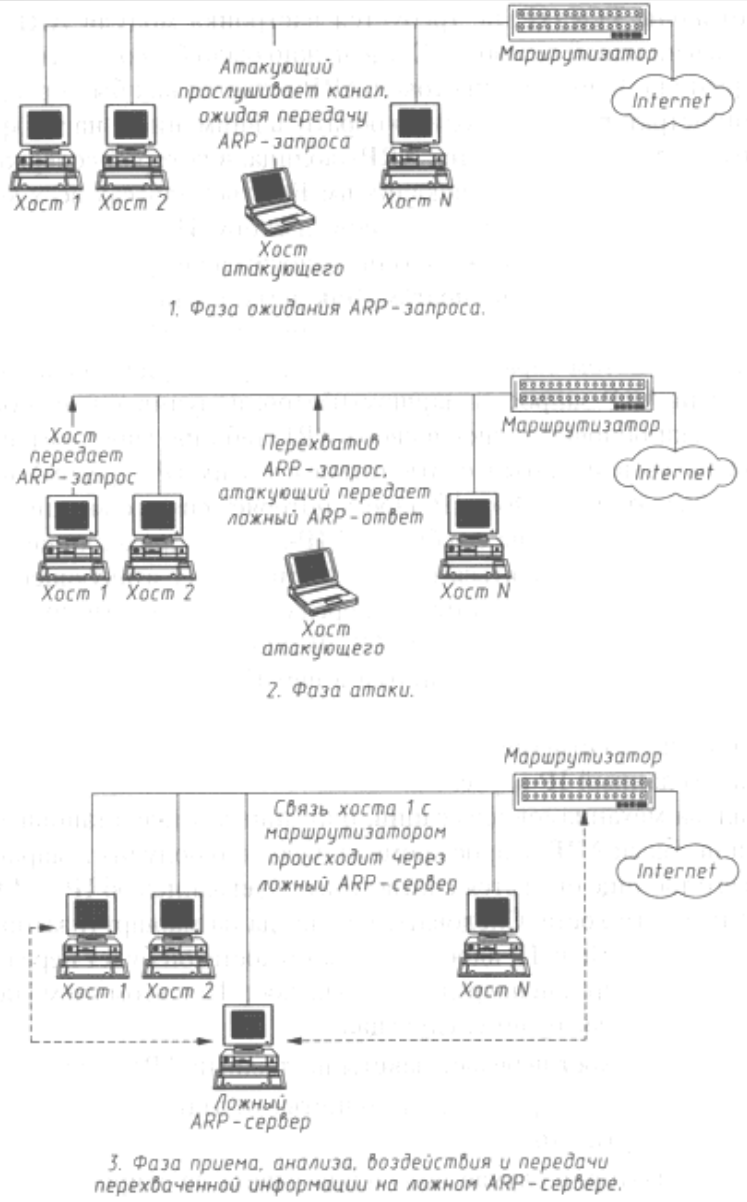
Активные сетевые атаки

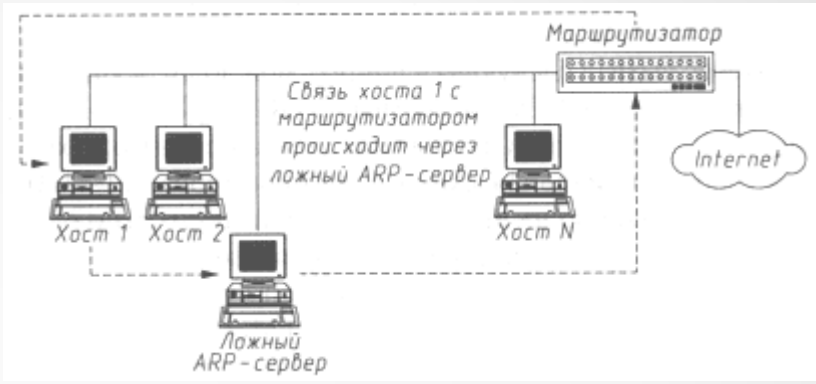
Ложный ARP-сервер

Анализ безопасности протокола ARP показывает, 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 сетевой трафик дезинформированного хоста.

1. Ожидание ARP-запроса от жертвы.
2. При получении такого запроса - передача по сети на запросивший хост ложного ARP-ответа, где 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.
3. Прием, анализ, воздействие на пакеты обмена и передача их между взаимодействующими хостами.

Ложный ARP-сервер



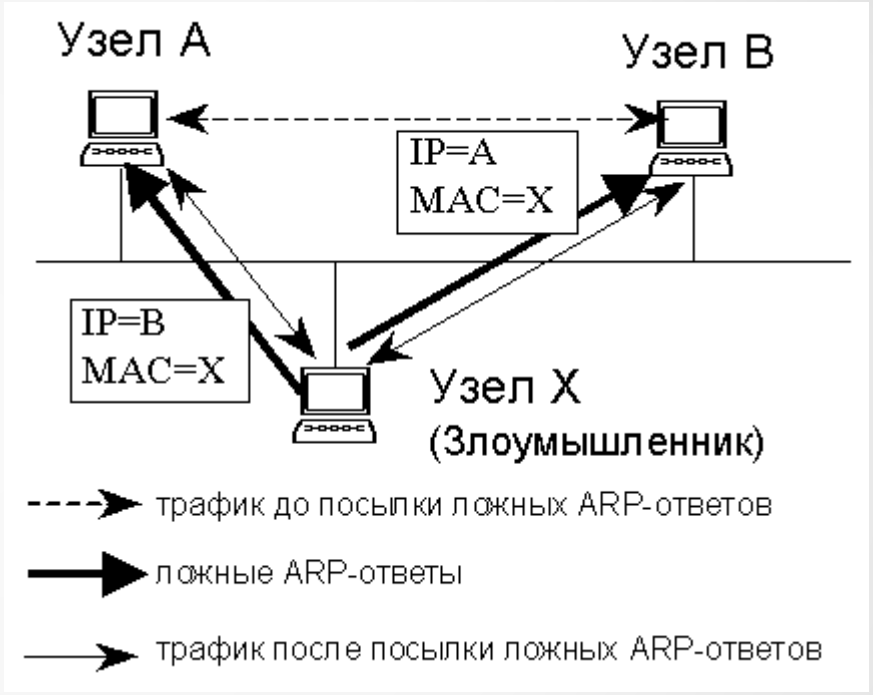


Из анализа механизмов адресации, описанных выше, становится ясно: так как поисковый ARP-запрос кроме атакующего получит и маршрутизатор, то в его таблице окажется соответствующая запись об IP- и Ethernet-адресе атакуемого хоста. Следовательно, когда на маршрутизатор придет пакет, направленный на IP-адрес атакуемого хоста, он будет передан не на ложный ARP-сервер, а непосредственно на хост.

Ложный ARP-сервер

Для перехвата трафика между узлами A и B, расположенными в одной IP-сети, злоумышленник использует протокол ARP. Он рассылает сфальсифицированные ARP-сообщения так, что каждый из атакуемых узлов считает MAC-адрес злоумышленника адресом своего собеседника

Введенные в заблуждение узлы A и B пересылают свой трафик через узел X, полагая, что сообщаются друг с другом непосредственно. Злоумышленник может просто прослушивать трафик или изменять передаваемые данные в своих интересах. Узел B может быть шлюзом сети, в которой находится узел A. В этом случае злоумышленник может перехватывать весь трафик между узлом A и Internet. Также злоумышленник может вообще не передавать кадры узла A узлу B, а выдавать себя за узел B, фабрикуя ответы от его имени и отсылая их в A.



Ложный DNS-сервер в сети Internet

Особенности работы DNS

Во-первых, по умолчанию служба DNS функционирует на базе протокола UDP (хотя возможно и использование протокола TCP для переноса информации о зонах между DNS-серверами), что, естественно, делает ее менее защищенной. Протокол UDP (в отличие от TCP) вообще не предусматривает средства создания виртуального канала, а, следовательно, отсутствуют какие-либо средства идентификации сообщений.

Во-вторых, начальное значение поля "порт отправителя" в UDP-пакете >= 1023 и увеличивается с каждым переданным DNS-запросом.

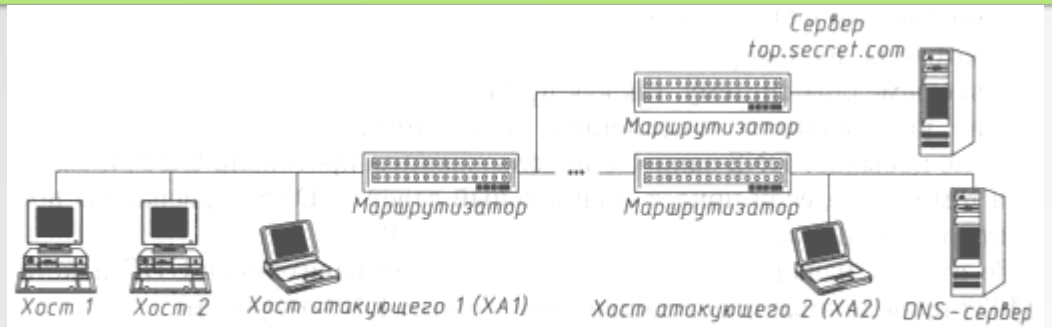
В-третьих, значение идентификатора (ID) DNS-запроса устанавливается следующим образом. В случае передачи DNS-запроса с хоста оно зависит от конкретного сетевого приложения, вырабатывающего DNS-запрос. Эксперименты показали, что если запрос посылается из оболочки командного интерпретатора (SHELL) операционных систем Linux и Windows (например, ftp nic.funet.fi), то это значение всегда равняется единице. Если же DNS-запрос передается из Netscape Navigator или его посылает непосредственно DNS-сервер, то с каждым новым запросом сам браузер или сервер увеличивает значение идентификатора на единицу. Эти моменты имеют значение в случае атаки без перехвата DNS-запроса.

Перехват DNS-запроса

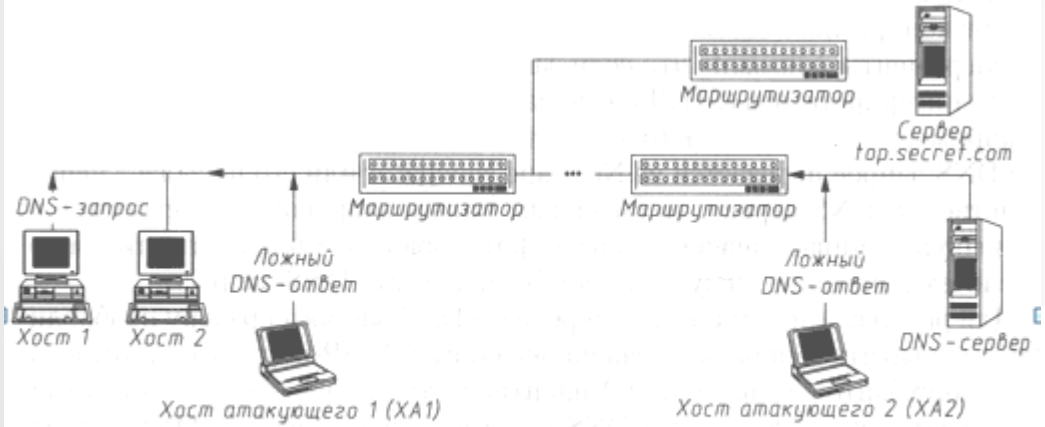
Для реализации атаки путем перехвата DNS-запроса злоумышленнику необходимо перехватить запрос, извлечь из него номер UDP-порта хоста отправителя, двухбайтовое значение ID-идентификатора DNS-запроса и искомое имя, а затем послать ложный DNS-ответ на извлеченный из DNS-запроса UDP-порт, где в качестве искомого IP-адреса указать настоящий IP-адрес ложного DNS-сервера. Такой вариант атаки в дальнейшем позволит полностью перехватить трафик между атакуемым хостом и сервером и активно воздействовать на него.

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, то есть ложный DNS-сервер ведет работу с сервером от своего имени.
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, для атакованного для хоста ложный DNS-сервер выглядит как настоящий сервер.

Перехват DNS-запроса

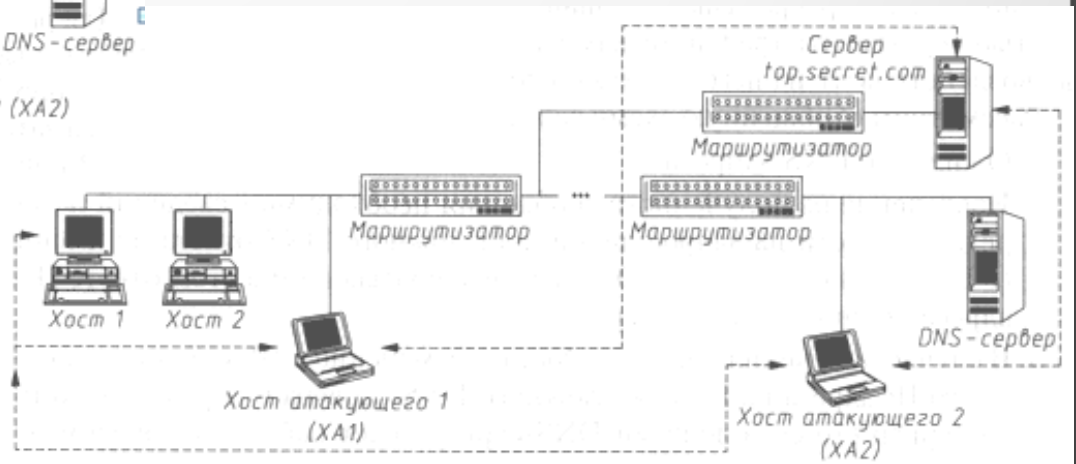


1. Фаза ожидания атакующим DNS-запроса (он находится либо на XA1, либо на XA2)



2. Фаза передачи атакующим ложного DNS-ответа

Необходимым условием осуществления данного варианта атаки является возможность перехвата DNS-запроса, а это возможно только в том случае, если атакующий находится, либо на пути следования запроса к DNS-серверу, либо в одном сегменте с DNS-сервером.



3. Фаза приема, анализа, воздействия и передачи перехваченной информации на ложном сервере

Направленный шторм ложных DNS-ответов

Другой вариант осуществления удаленной DNS-атаки - внедрение в сеть Internet ложного сервера путем создания направленного шторма ложных DNS-ответов на атакуемый хост. В этом случае злоумышленник осуществляет постоянную передачу на атакуемый хост заранее подготовленного ложного DNS-ответа от имени настоящего DNS-сервера без предыдущего приема DNS-запроса.

Но IP-адрес отправителя ответа должен совпадать с IP-адресом DNS-сервера, а имя в DNS-ответе - с именем в DNS-запросе; кроме того, DNS-ответ следует направить на тот же UDP-порт, с которого было послано сообщение (в данном случае это первая проблема для взломщика), и поле идентификатора запроса (ID) в заголовке DNS-ответа должно содержать то же значение, что и в переданном запросе (а это вторая проблема).

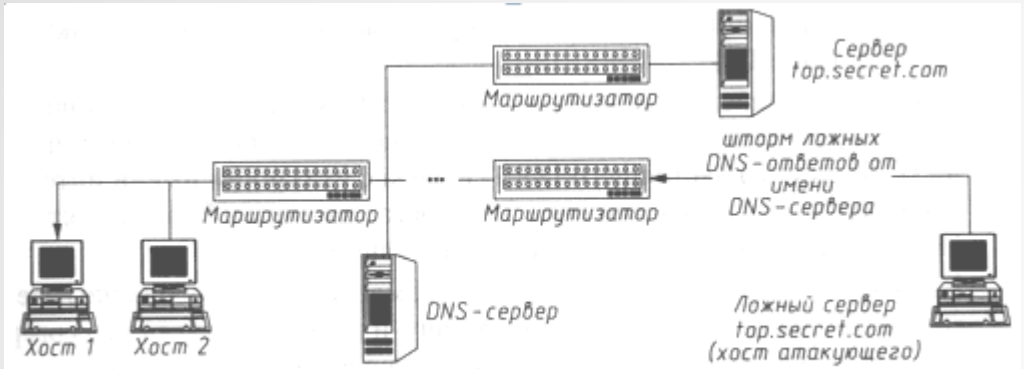
Можно использовать описанные выше особенности DNS.

Направленный шторм ложных DNS-ответов

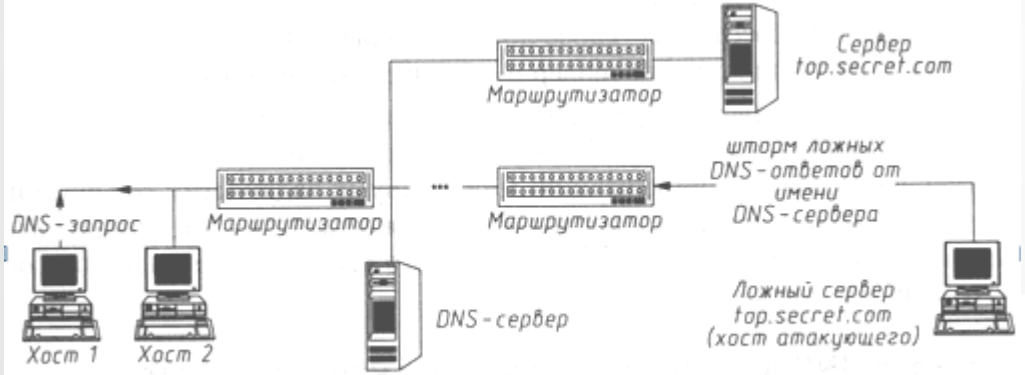
Вариантом осуществления данной удаленной атаки злоумышленнику необходимо выбрать интересующий его объект (например, сервер top.secret.com), маршрут к которому требуется изменить так, чтобы он проходил через ложный сервер. Это достигается постоянной передачей (направленным штормом) ложных DNS-ответов на соответствующие UDP-порты атакуемого объекта. В этих ложных DNS-ответах в качестве IP-адреса хоста top.secret.com указывается IP-адрес атакующего.
Далее атака развивается по следующей схеме. Как только атакуемый обратится по имени к хосту top.secret.com, то от данного хоста в сеть будет передан DNS-запрос, который атакующий никогда не получит. Однако злоумышленнику этого и не требуется, так как на объект атаки сразу же поступит постоянно передаваемый ложный DNS-ответ, что и будет воспринято ОС атакуемого хоста как настоящий ответ от DNS-сервера. Теперь жертва будет передавать все пакеты, предназначенные для top.secret.com, на IP-адрес хоста взломщика.

Конечно, условием успеха этой атаки будет получение объектом атаки ложного DNS-ответа ранее настоящего ответа от ближайшего DNS-сервера. Поэтому для повышения вероятности ее успеха желательно нарушить работоспособность ближайшего DNS-сервера (например, путем создания направленного шторма UDP-запросов на 53-й порт).

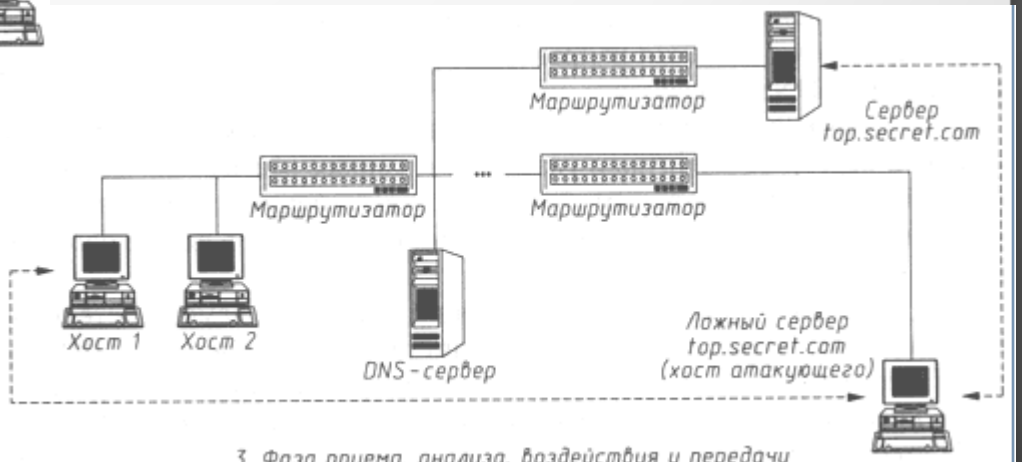
Перехват DNS-запроса



1. Атакующий создает направленный шторм ложных DNS-ответов на Хост 1



2. Хост 1 посылает DNS-запрос и немедленно получает ложный DNS-ответ



3. Фаза приема, анализа, воздействия и передачи перехваченной информации на ложном сервере

Перехват DNS-запроса

1. Постоянная передача злоумышленником ложных DNS-ответов на различные UDP-порты атакуемого хоста 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.
2. 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).
3. 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). Такая атака осуществляется межсегментно по отношению к цели атаки и угрожает безопасности любого хоста Internet, использующего обычную службу DNS.

Атака на DNS-сервер

Для внедрения в сеть Internet ложного сервера путем перехвата DNS-запроса или создания направленного шторма ложных DNS-ответов на атакуемый DNS-сервер можем использовать схему взаимодействия DNS серверов.

Из схемы удаленного DNS-поиска следует, что если DNS-сервер не обнаружил указанное в запросе 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. если DNS-сервер не имеет сведений о запрашиваемом хосте, то он сам, пересылая запрос далее, является инициатором удаленного DNS-поиска.

Поэтому ничто не мешает нарушителю, действуя описанными в предыдущих пунктах методами, перенести свой действия непосредственно на DNS-сервер. В таком случае ложные DNS-ответы будут направляться атакующим от имени корневого DNS-сервера на атакуемый DNS-сервер.

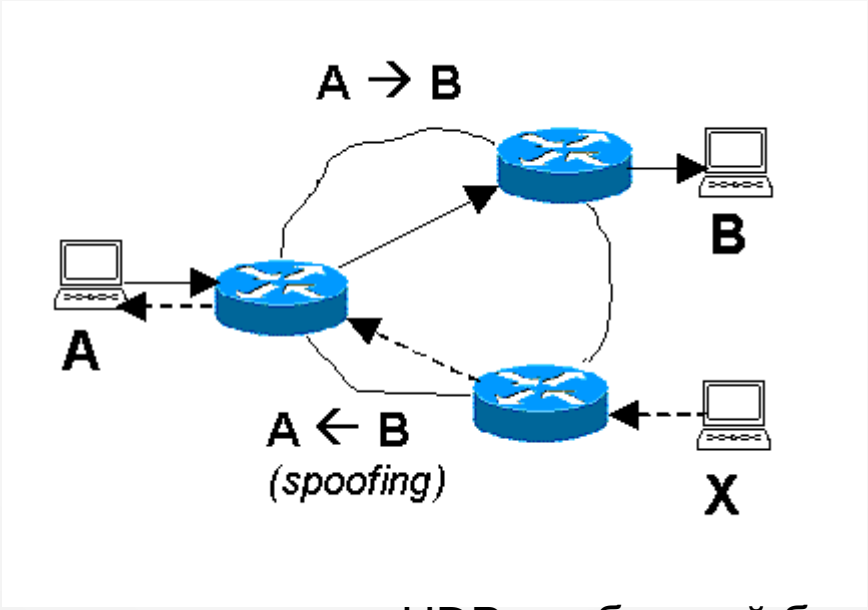
Имперсонация

Предположим, что узел A обменивается IP-датаграммами с узлом B, при этом узлы идентифицируют друг друга по IP-адресам, указываемым в датаграммах. Предположим далее, что узел B имеет особые привилегии при взаимодействии с A: то есть A предоставляет B некоторый сервис, недоступный для других хостов Internet. Злоумышленник на узле X, желающий получить такой сервис, должен имитировать узел B — такие действия называются *имперсонацией* узла B узлом X.

1. A, B и X находятся в одной IP-сети (ARP-атака);
2. A и X находятся в одной сети, а B — в другой (навязывание ложного маршрутизатора);
3. A и B находятся в разных сетях, а X находится на пути между ними (или включает себя в маршрут путем атаки на протокол маршрутизации).

Имперсонация без обратной связи

Пусть узел X находится в сети, не имеющей никакого отношения к узлам A и B и не лежащей между ними (A и B могут находиться как в одной, так и в разных сетях).



Легко видеть, что имперсонация UDP-сообщений без обратной связи является тривиальной -- злоумышленник должен только сфабриковать датаграмму, адресованную от узла B узлу A, и отправить ее по назначению.

Имперсонация без обратной связи

Для TCP соединений:

- ❑узел X от имени B отправляет в A сегмент с битом SYN, где указывает начальный номер ISN(B)
- ❑узел A отвечает узлу B SYN-сегментом, в котором подтверждает получение предыдущего сегмента, и устанавливает свой начальный номер ISN(A). Этот сегмент злоумышленник никогда не получит.

- ➢ узел B, получив от A ответ на SYN-сегмент, который он никогда не посылал, отправит узлу A сегмент с битом RST

➢Первая проблема решается относительно просто: злоумышленник проводит против узла B атаку типа «отказ в обслуживании» с тем расчетом, чтобы узел B не был способен обрабатывать сегменты, приходящие из A.

- ➢ узел X все равно не сможет отправить в A следующий сегмент (как раз это должен быть сегмент с данными), потому что в этом сегменте узел X должен подтвердить получение SYN-сегмента от A, то есть поместить в поле ACK SN заголовка своего сегмента значение ISN(A)+1. Но злоумышленник не знает номера ISN(A), потому что соответствующий сегмент ушел к узлу B.

➢Для решения второй проблемы злоумышленник должен уметь предсказывать значения ISN(A).

Имперсонация без обратной связи

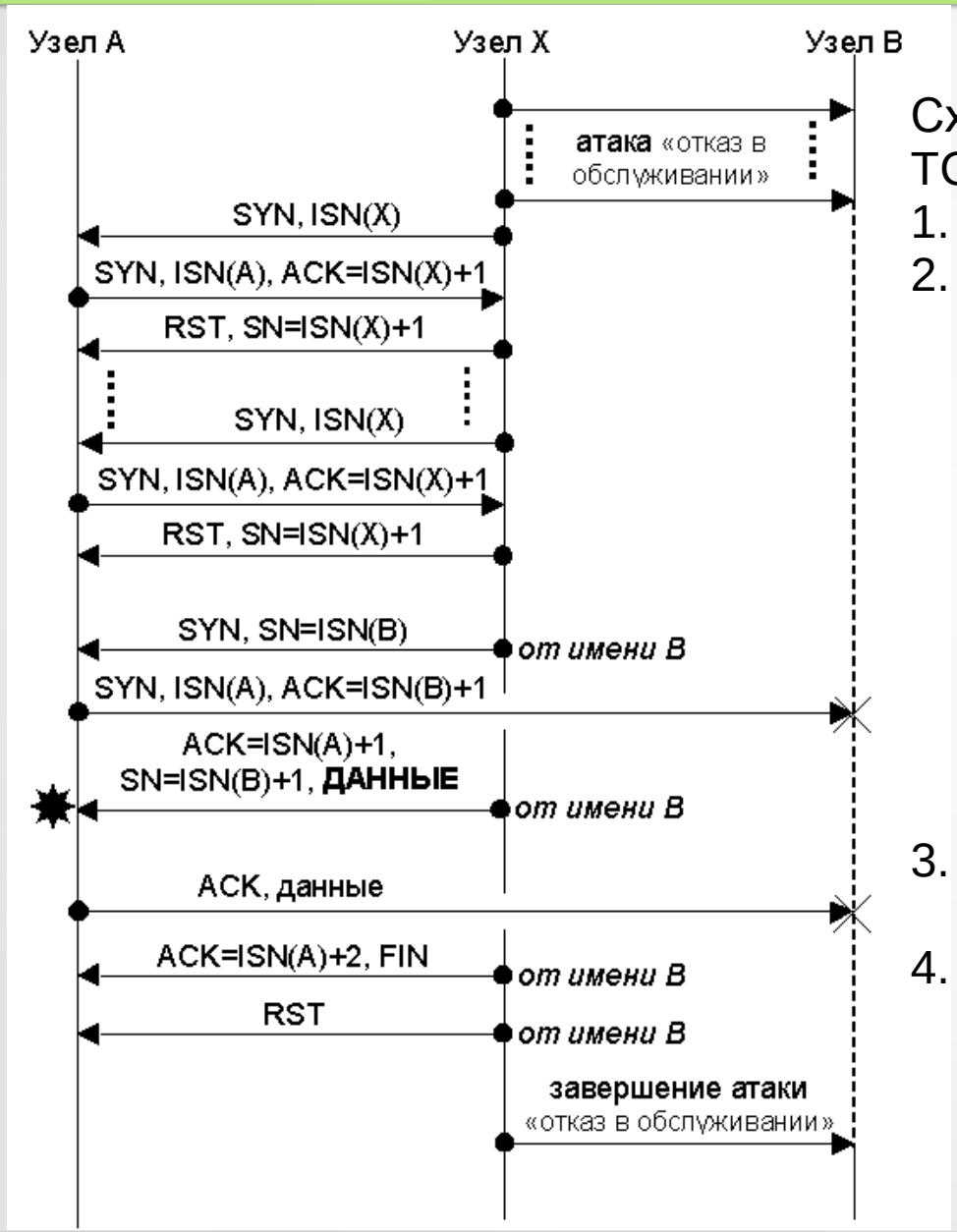
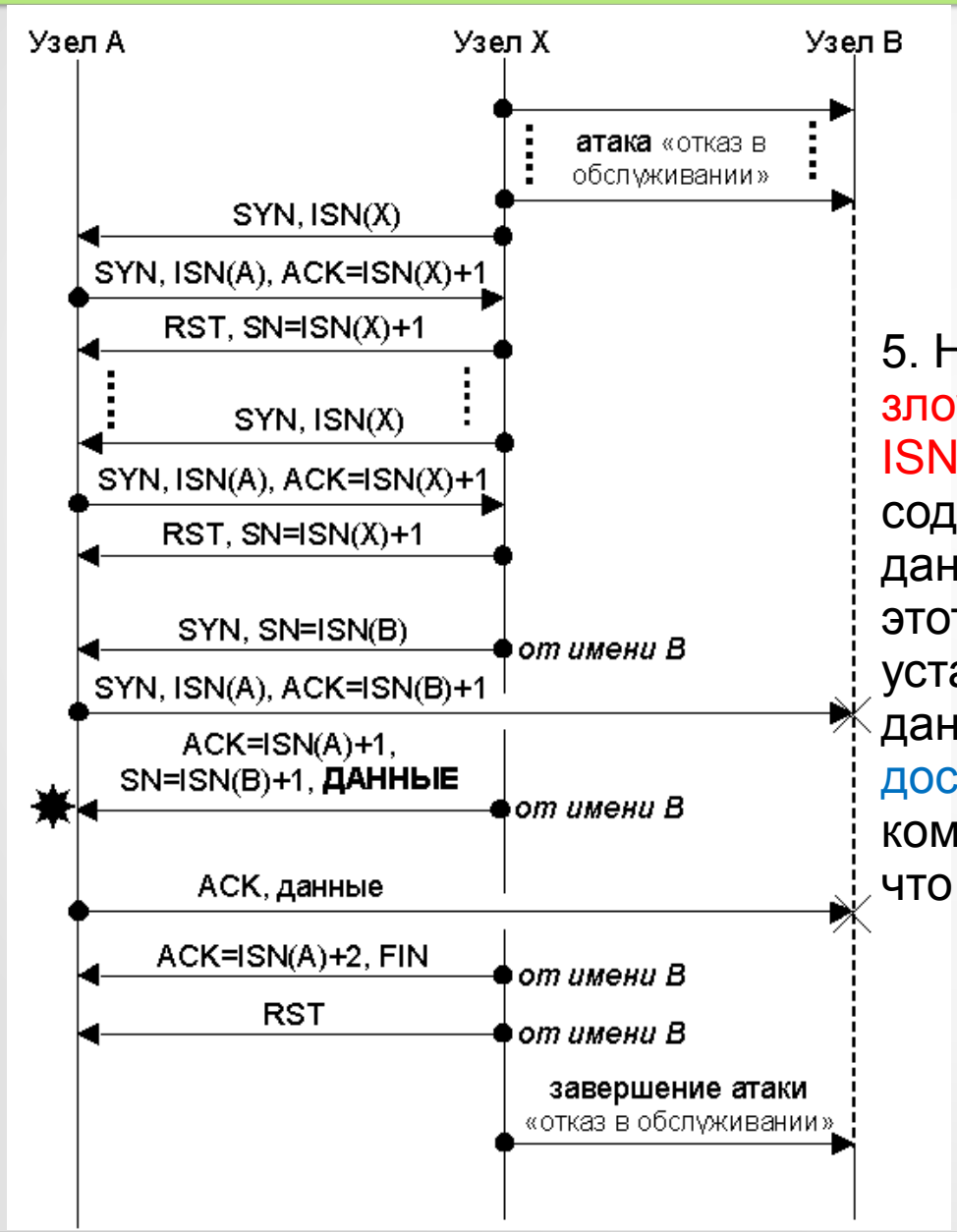


Схема атаки с имперсонацией TCP-соединения без обратной связи

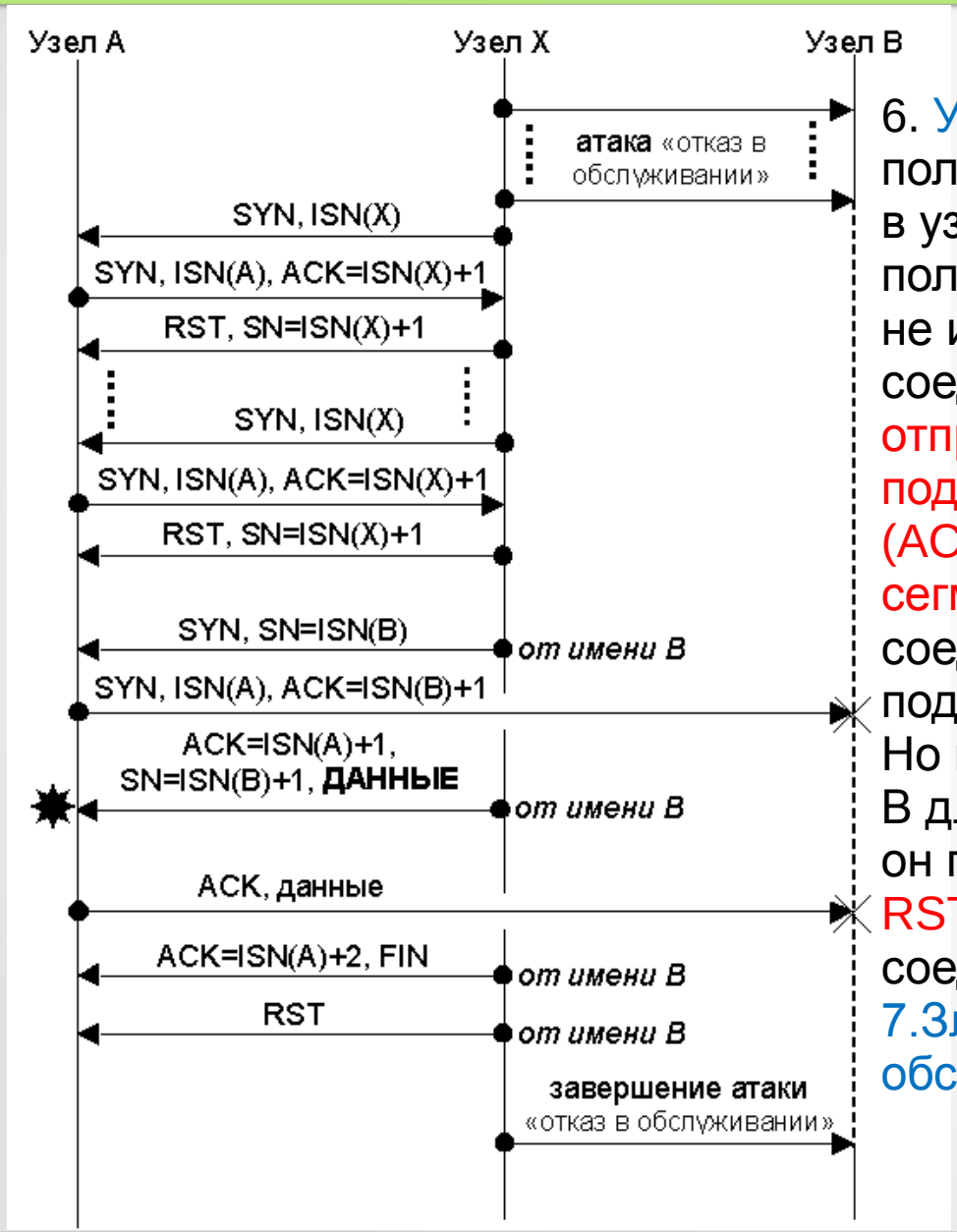
1. Злоумышленник выводит из строя узел B.
2. Злоумышленник делает несколько пробных попыток установить соединения с узлом A с целью получить от A последовательность значений ISN(A). Сразу после поступления SYN-сегмента от A злоумышленник разрывает наполовину установленное соединение посылкой сегмента с флагом RST. Проанализировав полученные значения ISN(A), злоумышленник определяет закон формирования этих значений.
3. Злоумышленник отправляет в A SYN-сегмент от имени B.
4. Узел A отвечает узлу B свои SYN-сегментом, подтверждающим получение SYN-сегмента от B, и указывает значение ISN(A) для этого соединения. Злоумышленник не видит этого сегмента.

Имперсонация без обратной связи



5. На основе ранее полученных данных злоумышленник предсказывает значение ISN(A) и отправляет в A сегмент от имени B, содержащий подтверждение ISN(A)+1 и данные для прикладного процесса. Получив этот сегмент, узел A считает соединение с B установленным и передает поступившие данные прикладному процессу. Цель атаки достигнута. Данные могут быть, например, командой, которую узел A выполняет, потому что она поступила от доверенного узла B.

Имперсонация без обратной связи



6. Узел A отправляет подтверждение получения данных и, возможно, свои данные в узел B. Злоумышленник этих сегментов не получит, но они его (по условиям задачи) и не интересуют. Чтобы корректно закрыть соединение, злоумышленник может вслепую отправить в узел A от имени узла B подтверждение получения одного октета (ACK SN=ISN(A)+2), а следом выслать сегмент с флагом FIN. Для полного закрытия соединения злоумышленник должен подтвердить получение FIN-сегмента от A. Но поскольку данные, передаваемые из A в B для злоумышленника ценности не имеют, он просто отправляет в A сегмент с флагом RST, тем самым полностью ликвидируя соединение.

7.Злоумышленник завершает атаку "отказ в обслуживании" против узла B.

Десинхронизация TCP-соединения

Злоумышленник X, находящийся в одном сегменте сети с узлами A и B или на пути между A и B, может произвести десинхронизацию TCP-соединения между A и B для установления полного контроля над соединением, то есть, злоумышленник получит возможность действовать как от имени A, так и от имени B. Для обозначения имперсонации, выполняемой таким методом, в англоязычной литературе используется термин TCP hijacking.

При установленном соединении каждый из узлов A и B знает, октеты с какими номерами может прислать ему другая сторона в данный момент: если последнее подтверждение, высланное узлом A, было ACK_{AB} и при этом узел A объявил окно W_{AB}, то A ожидает от B октетов с номерами SN_{BA}, попадающими в объявленное окно, то есть: $ACK_{AB} <= SN_{BA} <= ACK_{AB} + W_{AB}$

Аналогично в узле B ожидается от A: $ACK_{BA} <= SN_{AB} <= ACKBA + W_{BA}$

Если, например, узел A по какой-то причине получает от B сегмент с номером SN_{BA}, не попадающим в окно, то этот сегмент уничтожается, а в ответ A отправляет в B сегмент с SN_{AB}, ACK_{AB}, W_{AB}, чтобы указать узлу B, какие именно октеты ожидает получить A, , где SN_{AB} — номер следующего октета данных, который A когда-либо вышлет в B.

Десинхронизация TCP-соединения

Злоумышленник X, находящийся в одном сегменте сети с узлами A и B или на пути между A и B, может произвести десинхронизацию TCP-соединения между A и B для установления полного контроля над соединением, то есть, злоумышленник получит возможность действовать как от имени A, так и от имени B. Для обозначения имперсонации, выполняемой таким методом, в англоязычной литературе используется термин TCP hijacking.

При установленном соединении каждый из узлов A и B знает, октеты с какими номерами может прислать ему другая сторона в данный момент: если последнее подтверждение, высланное узлом A, было ACK_{AB} и при этом узел A объявил окно W_{AB}, то A ожидает от B октетов с номерами SN_{BA}, попадающими в объявленное окно, то есть: $ACK_{AB} <= SN_{BA} <= ACK_{AB} + W_{AB}$

Аналогично в узле B ожидается от A: $ACK_{BA} <= SN_{AB} <= ACKBA + W_{BA}$

Если, например, узел A по какой-то причине получает от B сегмент с номером SN_{BA}, не попадающим в окно, то этот сегмент уничтожается, а в ответ A отправляет в B сегмент с SN_{AB}, ACK_{AB}, W_{AB}, чтобы указать узлу B, какие именно октеты ожидает получить A, , где SN_{AB} — номер следующего октета данных, который A когда-либо вышлет в B.

Десинхронизация TCP-соединения

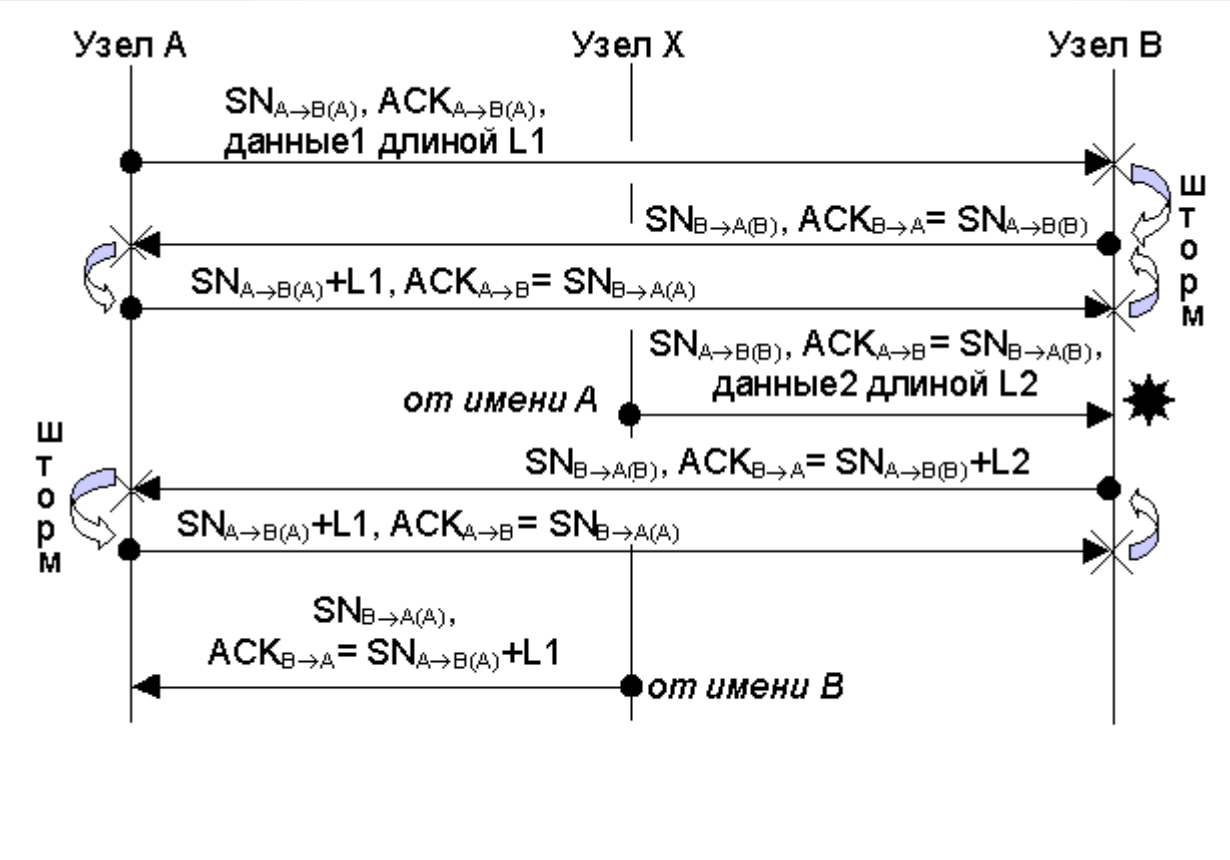
Будем использовать обозначения вида $SN_{AB(B)}$, что означает «приемлемый SN_{AB} с точки зрения B».

Теперь, если B посылает в A сегмент с неким номером $SN_{BA(B)}$, адекватным с точки зрения B, но уже не попадающим в окно в узле A, то A возвращает узлу B подтверждение со своим значением $ACK_{AB}=SN_{BA(A)}$.

Однако в этом же сегменте имеется номер $SN_{AB(A)}$, который теперь уже B рассматривает как не попадающий в свое окно и отправляет в A подтверждение $SN_{BA(B)}$, $ACK_{BA}=SN_{AB(A)}$.

Номер $SN_{BA(B)}$, как и раньше, неприемлем для A, и узел A вновь отправляет в B подтверждение,
……
и этот цикл, называемый ACK-шторм, теоретически продолжается до бесконечности, а практически — до тех пор, пока один из ACK-сегментов не потеряется в сети. Чем сильнее шторм, тем больше загрузка сети, тем выше процент потерь, следовательно, тем быстрее шторм прекратится.

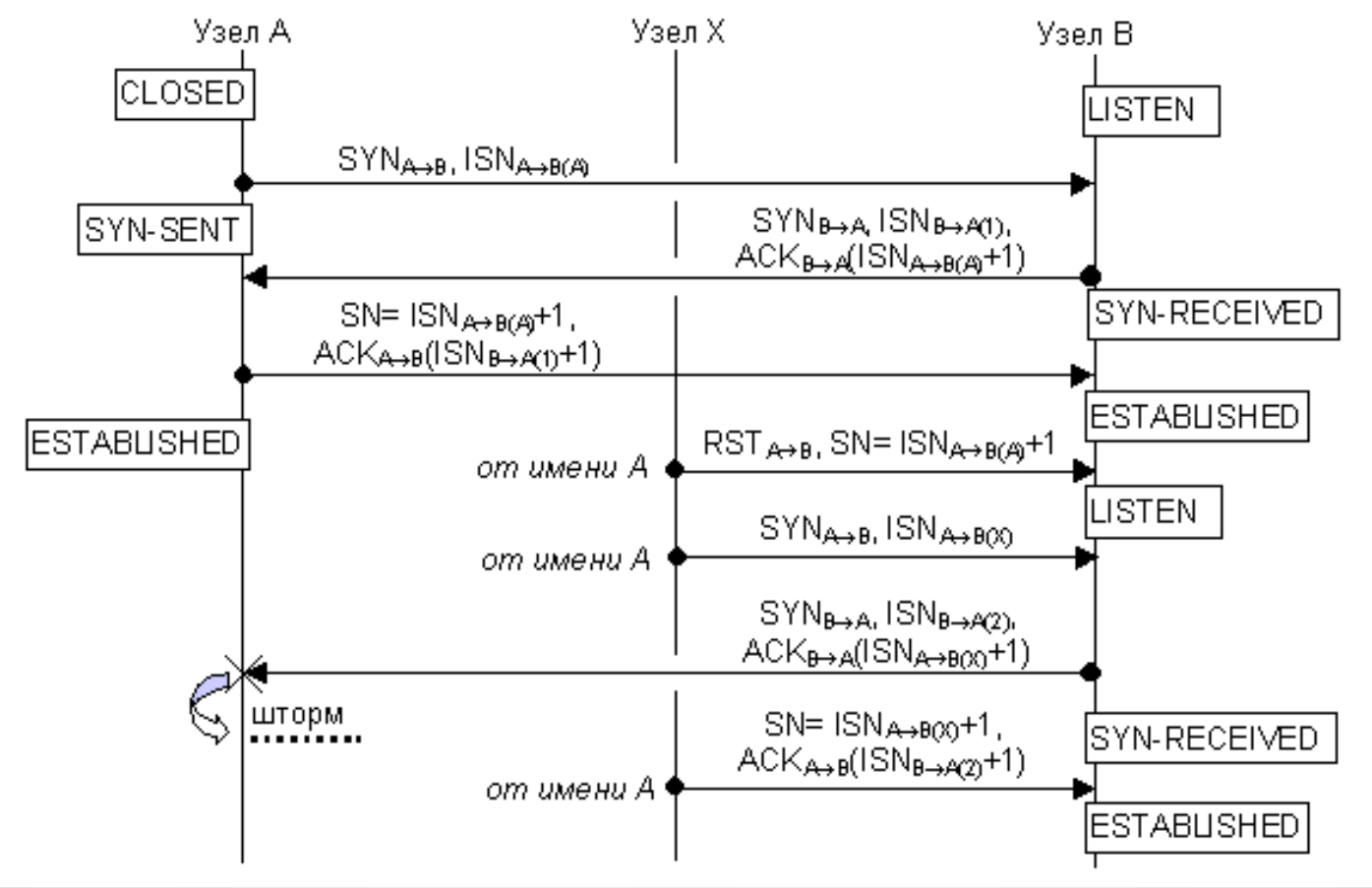
Десинхронизация TCP-соединения



В это время злоумышленник, знающий «правильные» номера с точки зрения обоих узлов, берет на себя функции посредника.

Ранняя десинхронизация

Ранняя десинхронизация: злоумышленник, прослушивая сеть, обнаруживает момент установления соединения между A и B, от имени A сбрасывает соединение RST-сегментом и тут же открывает его заново, но уже с новыми номерами ISN.



Ранняя десинхронизация

После этого оба узла A и B находятся в состоянии ESTABLISHED, но соединение десинхронизировано.

	следующий $SN_{A \to B}$	следующий $SN_{B \to A}$
С точки зрения A	$ISN_{A \to B(A)}+1$ (A будет отправлять)	$ISN_{B \to A(1)}+1$ (A ожидает получить)
С точки зрения B	$ISN_{A \to B(X)}+1$ (B ожидает получить)	$ISN_{B \to A(2)}+1$ (B будет отправлять)

Атаки, направленные на отказ в обслуживании

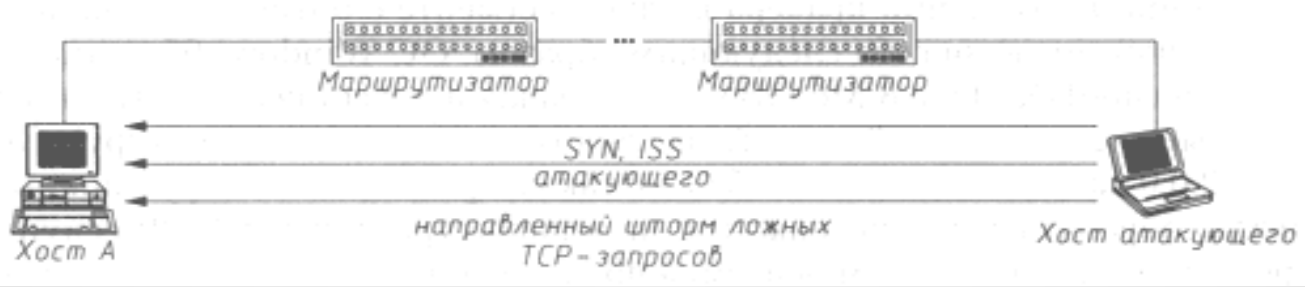
DoS-атаки можно условно поделить на три группы:

1. атаки большим числом формально корректных, но, возможно, сфальсифицированных пакетов, направленные на истощение ресурсов узла или сети;
2. атаки специально сконструированными пакетами, вызывающие общий сбой системы из-за ошибок в программах;
3. атаки сфальсифицированными пакетами, вызывающими изменения в конфигурации или состоянии системы, что приводит к невозможности передачи данных, сбросу соединения или резкому снижению его эффективности.

Атаки DoS используются как в комплексе с другими (имперсонация), так и сами по себе.

Направленный шторм ложных TCP-запросов на создание соединения

Из схемы создания TCP-соединения следует, что на каждый полученный TCP-запрос (TCP SYN) операционная система должна сгенерировать начальное значение идентификатора ISN и отослать его на запросивший хост. Но так как в Internet (стандарта IPv4) не предусмотрен контроль за IP-адресом отправителя сообщения, то проследить истинный маршрут, пройденный IP-пакетом, невозможно; и, следовательно, у конечных абонентов сети нет способа ограничить число запросов, принимаемых в единицу времени от одного хоста. Возможно осуществление типовой удаленной атаки "отказ в обслуживании", которая будет заключаться в передаче на объект атаки как можно большего числа ложных TCP-запросов на создание соединения от имени любого хоста в сети (направленный шторм запросов TCP SYN- «TCP SYN Flooding and IP Spoofing Attacks»). Разумеется, злоумышленник, чтобы скрыть себя, будет посылать сегменты от имени несуществующего (выключенного) узла и принимать ответные сегменты от атакуемого узла методом прослушивания.



Атака передачей широковещательного запроса от имени "жертвы"

Для создания шквала злоумышленник направляет несколько сфальсифицированных Echo-запросов от имени жертвы на широковещательные адреса нескольких сетей, которые выступят в роли усилителей.

Потенциально большое число узлов, находящихся в сетях-усилителях и поддерживающих обработку широковещательных Echo-запросов, одновременно отправляет ответы на атакуемый узел.

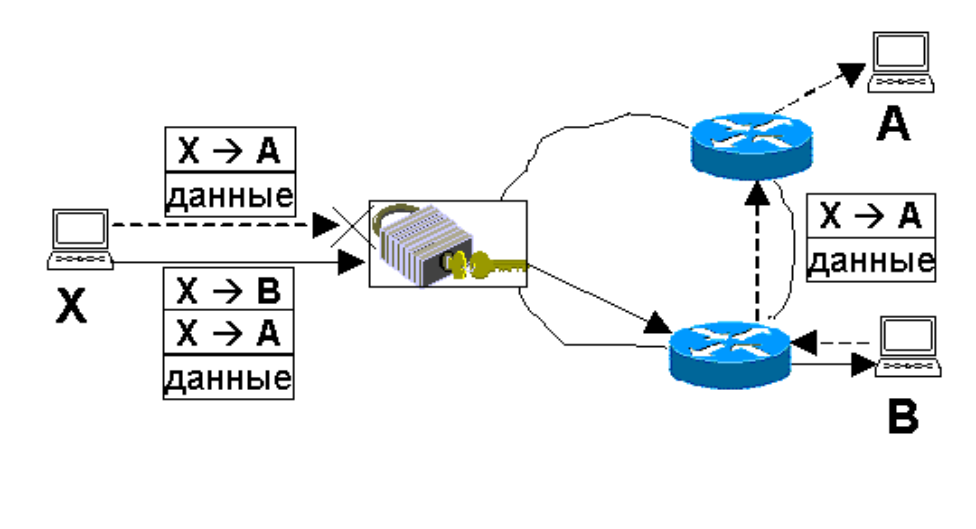
В результате атаки сеть, в которой находится жертва, сам атакуемый узел, а также и сети-усилители могут быть временно заблокированы шквалом ответных сообщений.

Более того, если атакуемая организация оплачивает услуги провайдера Internet пропорционально полученному трафику, ее расходы могут существенно возрасти.

«Тунелирование»

Пусть злоумышленник хочет отправить данные с узла X узлу A, находящемуся за пределами его сети, однако правила фильтрации на маршрутизаторе запрещают отправку датаграмм узлу A. В то же время разрешена отправка датаграмм узлу B, также находящемуся за пределами охраняемой сети.

Злоумышленник использует узел B как ретранслятор датаграмм, направленных в A. Для этого он создает датаграмму, направленную из X в B, в поле Protocol которой помещается значение 4 («IP»), а в качестве данных эта датаграмма несет другую IP-датаграмму, направленную из X в A. Фильтрующий маршрутизатор пропускает сформированную датаграмму, поскольку она адресована разрешенному узлу B, а IP-модуль узла B извлекает из нее вложенную датаграмму. Видя, что вложенная датаграмма адресована не ему, узел B отправляет ее по назначению, то есть узлу A



Атака крошечными фрагментами (Tiny Fragment Attack)

В случае, когда на вход фильтрующего маршрутизатора поступает фрагментированная датаграмма, маршрутизатор производит досмотр только первого фрагмента датаграммы (первый фрагмент определяется по значению поля IP-заголовка Fragment Offset=0). Если первый фрагмент не удовлетворяет условиям пропуска, он уничтожается. Остальные фрагменты можно безболезненно пропустить, не затрачивая на них вычислительные ресурсы фильтра, поскольку без первого фрагмента датаграмма все равно не может быть собрана на узле назначения.

При конфигурировании пакетного фильтра перед сетевым администратором часто стоит задача: разрешить соединения с TCP-сервисами Internet, инициируемые компьютерами внутренней сети, но запретить установление соединений внутренних компьютеров с внешними по инициативе последних. Для решения поставленной задачи фильтр конфигурируется на запрет пропуска TCP-сегментов, поступающих из внешней сети и имеющих установленный бит SYN в отсутствии бита ACK; сегменты без этого бита беспрепятственно пропускаются в охраняемую сеть, поскольку они могут относиться к соединению, уже установленному ранее по инициативе внутреннего компьютера.

Атака крошечными фрагментами (Tiny Fragment Attack)

Злоумышленник формирует искусственно фрагментированную датаграмму с TCP-сегментом, при этом первый фрагмент датаграммы имеет минимальный размер поля данных — 8 октетов (напомним, что размеры фрагментов указываются в 8-октетных блоках).

В поле данных датаграммы находится TCP-сегмент, начинающийся с TCP-заголовка.

В первых 8 октетах TCP-заголовка находятся номера портов отправителя и получателя и поле Sequence Number, но значения флагов не попадут в первый фрагмент.

Следовательно, фильтр пропустит первый фрагмент датаграммы, а остальные фрагменты он проверять не будет. Таким образом, датаграмма с SYN-сегментом будет успешно доставлена на узел назначения и после сборки передана модулю TCP.

Атака крошечными фрагментами (Tiny Fragment Attack)