26. Обеспечение безопасности систем, входящих в состав глобальных сетей: межсетевые экраны, виртуальные частные сети

Под доверенным объектом понимается элемент сети (компьютер, межсетевой экран, маршрутизатор и т.п.), имеющий легальное подключение, и которому присвоены права для доступа к сетевым ресурсам информационной системы.

Осуществление атаки "подмена доверенного объекта сети" и передача по каналам связи сообщений от его имени с присвоением его прав доступа возможна в системах, где используются нестойкие алгоритмы идентификации и аутентификации хостов. Типичным примером является перехват TCP-сессии.

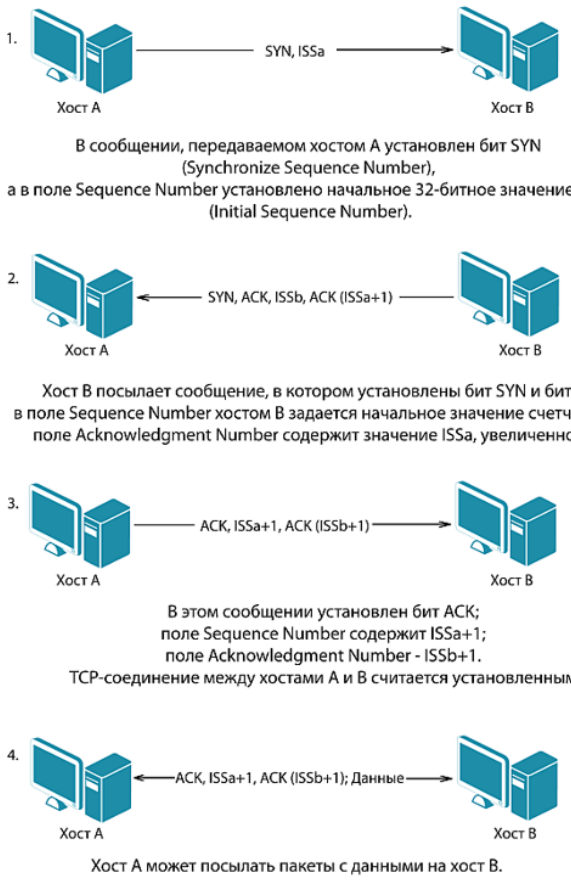
Протокол TCP является одним из базовых протоколов транспортного уровня сети Интернет. Он позволяет исправлять ошибки, которые могут возникнуть в процессе передачи пакетов, устанавливая логическое соединение – виртуальный канал. По этому каналу передаются и принимаются пакеты с регистрацией их последовательности, осуществляется управление информационным потоком, организовывается повторная передача искаженных пакетов, а в конце сеанса канал разрывается.

Для идентификации TCP-пакета в TCP-заголовке существуют два 32-разрядных идентификатора – Sequence Number (номер последовательности) и Acknowledgment Number (номер подтверждения), которые также играют роль счетчиков пакетов

Существуют две разновидности процесса осуществления удаленной атаки типа "подмена доверенного объекта сети":

- атака с установлением виртуального канала;
- атака без установления виртуального канала.

Процесс осуществления атаки с установлением виртуального канала состоит в присвоении прав доверенного пользователя, что позволяет злоумышленнику вести сеанс работы с объектами системы от имени доверенного пользователя. Для формирования ложного TCP-пакета атакующему достаточно подобрать соответствующие текущие значения идентификаторов TCP-пакета (ISSa и ISSb, см. рисунок 1.4) для данного TCP-соединения (например, FTP- или TELNET-подключение).



Так как для служебных сообщений в распределенных сетях часто используется передача одиночных сообщений, не требующих подтверждения, виртуальное соединение не создается. Атака без установления виртуального канала заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) о ложном изменении маршрутно-адресных данных.

Идентификация передаваемых сообщений осуществляется только по сетевому адресу отправителя, который легко подделать. Типовая удаленная атака, использующая навязывание ложного маршрута, основана на описанной идее.

Подмена доверенного объекта сети является активным воздействием, совершаемым с целью нарушения конфиденциальности и целостности информации. Данная удаленная атака может являться как внутрисегментной, так и межсегментной, как с обратной связью, так и без обратной связи с атакуемым объектом и осуществляется на сетевом и транспортном уровнях модели OSI.

Удаленная атака "ложный объект"

Архитектура Интернета создавалась в условиях, когда внутри сети существовало доверие к действиям отдельных участников. В распределенных сетях механизмы идентификации сетевых управляющих устройств (маршрутизаторов) не обеспечивают безопасное использование протоколов управления сетью.

Если участник сети (маршрутизатор) заявляет, что он владеет блоком адресного пространства, остальная часть IP-сети верит ему на слово и адресует ему весь соответствующий трафик. Значит, можно создать любой сетевой блок и запустить его в IP-сети, придав анонимность любой атаке, связанной с изменением маршрутизации и внедрением в систему ложного объекта. Такой тип воздействия на сетевую информационную систему ещё называют атакой типа MITM (man in the middle, "человек посередине").

Для перехвата трафика злоумышленники используют уязвимости, присущие протоколам различных уровней стека TCP/IP: сетевому, транспортному и прикладному.

На сегодняшний день в подавляющем большинстве применяются стандартные протоколы семейства TCP/IP, среди которых к наиболее уязвимым относятся следующие: протокол управления передачей TCP, межсетевого взаимодействия IP, эмуляции терминала Telnet, передачи файлов FTP, разрешения адресов ARP, службы доменных имен DNS, управляющих сообщений сети Интернет ICMP и сетевого управления SNMP.

Кроме того, для обеспечения эффективной и оптимальной маршрутизации в сетях применяются динамические протоколы RIP и OSPF, позволяющие маршрутизаторам обмениваться информацией друг с другом и обновлять таблицы маршрутизации.

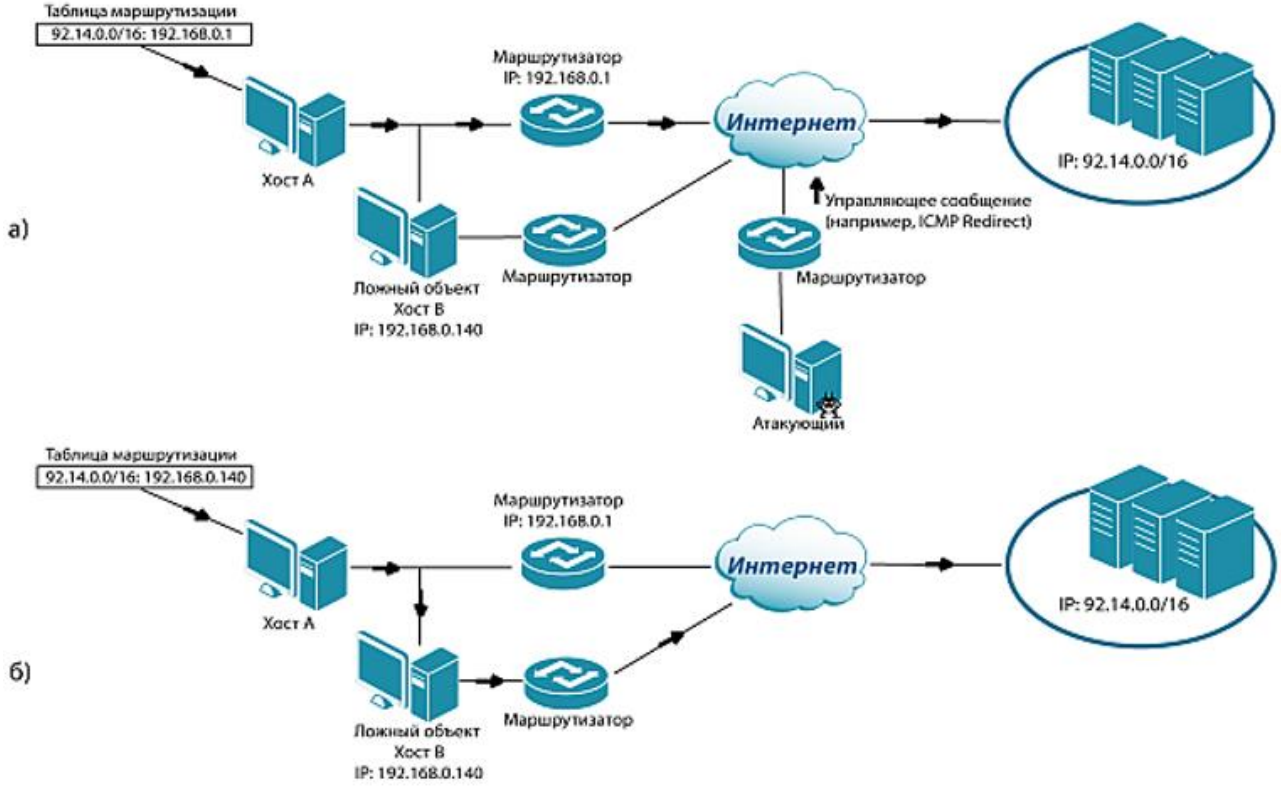
Атакующий ставит целью внедрение ложного объекта в сеть путем изменения таблиц маршрутизации и навязывания ложного маршрута.

Основная задача злоумышленника – не только прервать сообщение между сетями, а в первую очередь **перевести трафик через свой хост, чтобы извлечь полезную информацию**.

Реализация атаки основывается на уязвимостях или ошибках настройки протоколов маршрутизации (RIP, OSPF) и управления сетью (ICMP, SNMP). При этом злоумышленник посылает в сеть управляющее сообщение от имени сетевого управляющего устройства (например, маршрутизатора).

Рисунок 1.5 иллюстрирует реализацию удаленной атаки "навязывание ложного маршрута" с использованием протокола ICMP. Пакеты с запросами в сеть 92.14.0.0/16 с хоста A проходят через маршрутизирующее устройство с IP-адресом 192.168.0.1 (рисунок 1.5а). Атакующий посылает управляющее сообщение ICMP Redirect о наилучшем маршруте в сеть 92.14.0.0/16 и получает возможность изменения таблиц маршрутизации хоста A.

В результате весь трафик с хоста A, направляющийся в сеть 92.14.0.0/16, проходит через ложный объект хост B.



Относительно недавно разработчиками израильского центра Electronic Warfare Research and Simulation Center была обнаружена брешь в сетевом протоколе OSPF. Как утверждают исследователи, уязвимость существует из-за того, что сам протокол допускает прием поддельных запросов новых таблиц маршрутизации.

Например, при помощи ноутбука, можно отправить периодический запрос Link State Advertisement (LSA) на обновление таблиц маршрутизации. После чего маршрутизатор опознает запрос как легальный, поскольку в подтверждение он проверяет лишь порядковые номера запросов, которые также можно подделать. В результате подобной манипуляции, у злоумышленника будет полный доступ к сети в течение примерно 15-ти минут, пока маршрутизатор опять не обновит таблицы.

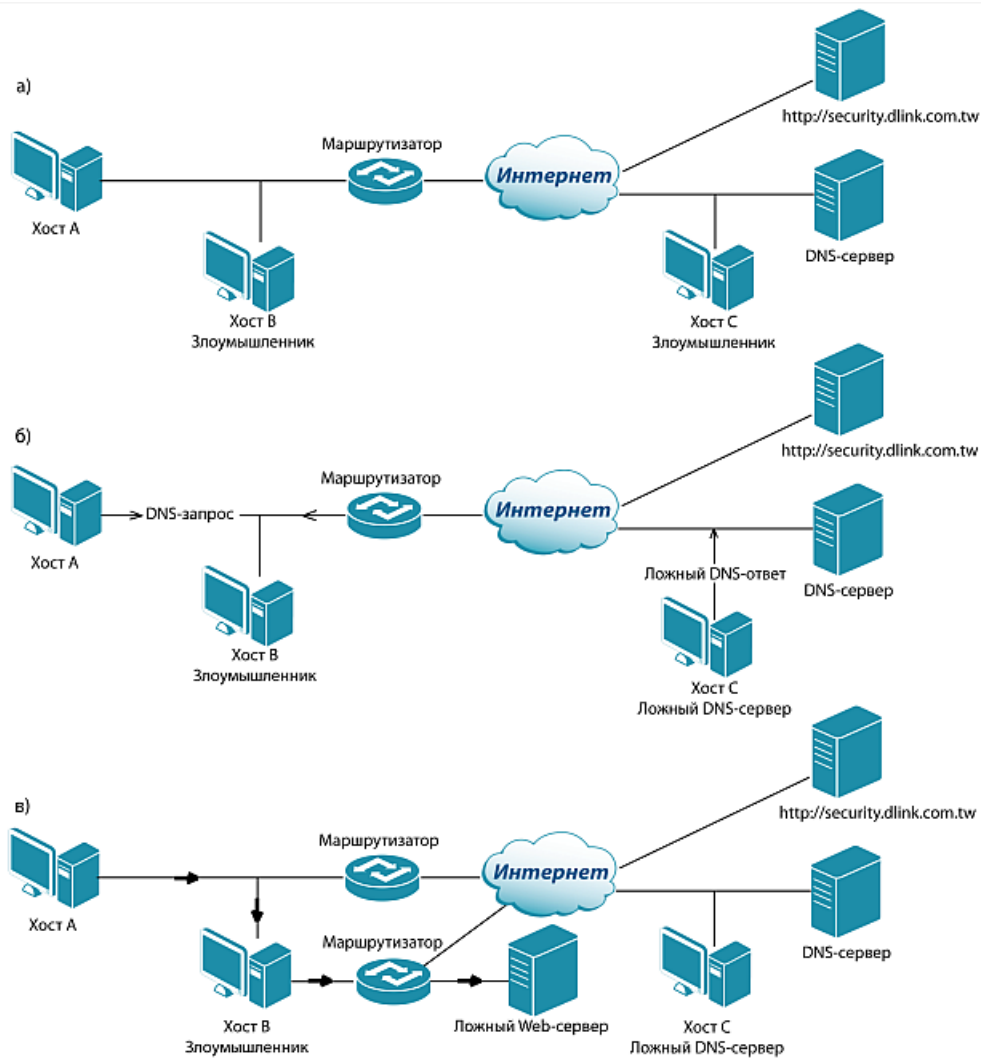
Также успешной может оказаться удаленная атака, использующая уязвимости сервисов, установленных на хостах (серверах). Для преобразования адресов из одного формата в другой в распределенных сетях используются протоколы удаленного поиска, заключающиеся в передаче по сети специальных запросов и получения на них ответов с искомой информацией.

Так, в сетях Ethernet протокол ARP решает вопрос отображения MAC-адреса (6 байтов) в пространство сетевых IP-адресов (4 байта) и наоборот; протокол DNS используется при преобразовании текстового доменного имени в IP-адрес.

При этом существует возможность перехвата злоумышленником поискового запроса и выдачи на него ложного ответа, использование которого приведет к изменению маршрутно-адресных данных. В результате весь сетевой трафик жертвы будет проходить через ложный объект.

На рисунке 1.6 представлена схема реализации атаки "внедрение ложного DNS-сервера" путем перехвата DNS-запроса. Атакующий (может находится либо на хосте B, либо на хосте C) ожидает DNS-запрос от хоста A (рисунок 1.6а). После перехвата поискового запроса от хоста A, атакующий посылает ему ложный DNS-ответ (рисунок 1.6б).

Особенно стоит отметить возможность преднамеренного искажения информации: вместо ресурса http://security.dlink.com.tw хост A в результате запроса может получить ресурс с таким же Web-интерфейсом, как и у запрашиваемого, только с искаженной информацией (рисунок 1.6в).



Перехват пользовательского сетевого трафика через ложный объект дает злоумышленнику возможность проведения анализа данных, передаваемых по сети, модификации информации, а также полной ее подмены.

Ниже приведены примеры некоторых наиболее распространенных атак, связанных с внедрением ложного объекта.

- **Одним из способов внедрения ложного объекта может быть SQL-инъекция** – это один из распространённых способов взлома сайтов и программ, работающих с базами данных, основанный на внедрении в запрос произвольного SQL-кода.

Атакующий использует индексы поисковых систем для идентификации уязвимых сайтов. Злоумышленники ищут сайты, использующие распространенные системы управления контентом и другое ПО, содержащее уязвимости процессов обработки входных данных, применяемых в SQL-запросах.

Результатом одной из последних атак такого рода стало то, что пользователи, посещающие зараженные страницы переводятся на другие сайты и на сервер Lilupophilupop.com, где им предлагается загрузить вредоносное ПО под видом Adobe Flash Player или несуществующего антивируса.

С использованием SQL-инъекций злоумышленник может не только получить закрытую информацию из базы данных, но и, при определенных условиях, внести туда изменения.

В целом, атаки, связанные с различного рода инъекциями, возможны ввиду недостаточной проверки входных данных и подразумевают внедрение сторонних команд или данных в работающую систему (чаще всего это связано с Web-сайтами) с целью изменения хода её работы, а в результате – получение доступа к закрытым ресурсам и информации, либо дестабилизации работы системы в целом.

- **Техника Clickjacking заключается в создании специального тега iFrame, который создает кнопку-подделку.** При нажатии (или автоматически, без действия пользователя) на эту кнопку в невидимый iFrame загрузится специальная страница с вредоносным кодом.

  Спрятанная страница может быть подделкой текущей, где будет предложено вновь ввести идентификационные данные пользователя, которые при повторном вводе сохраняться на хосте злоумышленника.
- Как рассматривалось выше, существует множество вредоносных программ, которые инфицировав сетевой компьютер, обеспечивают злоумышленникам удаленный доступ и полное управление этим компьютером, а также возможность использовать его в качестве ложного объекта сети, выдавая себя за легального пользователя.

  Люки (Backdoors) – программы, обеспечивающие вход в систему или получение привилегированной функции (режима работы) в обход существующей системы полномочий. Часто используются для обхода системы безопасности. Люки не инфицируют файлы, но прописывают себя в реестр, модифицируя, таким образом, ключи реестра. *BackDoor.Bitsex – троянская программа, представляющая собой полноценный сервер для удаленного управления инфицированным компьютером.*
- **Атака ARP-spoofing** – применяется преимущественно в сетях Ethernet, но возможна и в других сетях, использующих протокол ARP. Данная атака основана на использовании такой уязвимости протокола ARP, как отсутствие системы аутентификации пользователей.

  Она состоит в том, что злоумышленник посылает ложные ARP-пакеты с целью убедить компьютер жертвы в том, что ложный объект и есть легальный конечный адресат. Далее пакеты пересылаются реальному получателю, MAC-адрес отправителя в них подменяется, чтобы ответные пакеты тоже шли через ложный объект.

  Злоумышленник получает возможность прослушивать трафик, например, общение по ICQ, почту жертвы и др. При этом в случае прохождения через ложный объект трафика многих пользователей может возникнуть переполнение ARP-таблиц и сетевой отказ в обслуживании.

Достаточно часто злоумышленник проводит атаку на систему с целью ее отказа в работе.

Получив контроль над проходящим потоком информации между объектами, ложный объект вычислительной сети может применять различные методы воздействия на перехваченную информацию, например:

- **селекция потока информации** и сохранение ее на ложном объекте (нарушение конфиденциальности);
- **модификация информации:**
  - модификация данных (нарушение целостности),
  - модификация исполняемого кода и внедрение разрушающих программных средств – программных вирусов (нарушение доступности, целостности);
  - подмена информации (нарушение целостности).

Удаленная атака "отказ в обслуживании"

Одной из возможностей сетевой операционной системы (ОС), установленной на каждом объекте распределенной сети, является наличие сетевых служб, позволяющих удалённым пользователям использовать ресурсы данного объекта. Программа-сервер (например, FTP-сервер или Web-сервер), запущенная в сетевой ОС компьютера, обеспечивает удаленный доступ к FTP- или Web-ресурсам этого компьютера.

Пользователь отправляет запросы на предоставление услуги, ОС обрабатывает приходящие извне запросы, пересылает их на соответствующий сервер (FTP или Web), а сервер отвечает на них по созданному виртуальному каналу.

Любая операционная система имеет ограничения по количеству открытых виртуальных соединений и существует предел ответов на поступающие запросы. Данные ограничения зависят от системных ресурсов, основными из которых являются вычислительные мощности,

оперативная память, дисковое пространство или пропускная способность каналов связи. Если какой-то из ресурсов достигнет максимальной загрузки, приложение будет недоступно.

Как правило, атаки типа DoS (Denial of service) направлены на исчерпание критичных системных ресурсов, что приводит к прекращению функционирования системы, т.е. к отказу в обслуживании и невозможности доступа к серверу удаленных пользователей.

Выделяется два типа отказа в обслуживании: первый, основанный на ошибке в приложении, и второй, основанный на плохой реализации или уязвимости протокола.

Отказ в обслуживании приложения становится возможен, если уязвимости приложения ведут к получению контроля над машиной (например, с помощью переполнения буфера обмена). Приложение станет недоступным либо из-за нехватки ресурсов, либо из-за аварийного завершения. Уязвимость приложения может быть использована и для нарушения работоспособности других компонентов системы, таких как сервер СУБД или сервер аутентификации.

Сетевой отказ в обслуживании основывается на особенностях стека протоколов TCP/IP.

Если атака выполняется одновременно с большого числа хостов, говорят о распределённой атаке типа "отказ в обслуживании" – DDoS-атаке (Distributed Denial of Service). В некоторых случаях к DDoS-атаке приводит легальное действие, например, на популярном Интернет-ресурсе указана ссылка на сайт, размещённый на не очень производительном сервере (так называемый слэшдот-эффект).

Большой наплыв пользователей приводит к превышению допустимой нагрузки на сервер, и он очень быстро становится недоступным или доступ к нему затрудняется в результате перегруженности.

Ниже представлены некоторые типы подобных атак, однако, это всего лишь малая часть от существующих на сегодняшний день вариантов **DoS-атак**, информация о которых постоянно обновляется на специализированных Web-сайтах.

- **SYN-flood.**

  Выше был рассмотрен механизм установления TCP-соединения (рисунок 1.4). Атака типа SYN-flood использует именно этот механизм. TCP-соединение включает три состояния: отправка SYN-пакета, получение пакета SYN-ACK и посылка ACK-пакета.

  Идея атаки состоит в создании большого количества не до конца установленных TCP-соединений. Для реализации этого злоумышленник отправляет на сервер-жертву множество запросов на установление соединения (пакеты, с выставленным флагом SYN), машина-жертва отвечает пакетами SYN-ACK.

  Злоумышленник же игнорирует эти пакеты, не высылая ответные, либо подделывает заголовок пакета таким образом, что ответный SYN-ACK отправляется на несуществующий адрес. Процесс установки соединения не завершается, а остается в полуоткрытом состоянии, ожидая подтверждения от клиента.

  А так как под каждый полученный SYN-пакет сервер резервирует место в своем буфере, то при огромном количестве запросов, буфер достаточно быстро переполняется. В результате, вновь поступающие SYN-запросы, в том числе от легальных пользователей, не обрабатываются, и новые соединения не устанавливаются.

- **UDP-flood.**

  Данный метод основан на применении UDP-протокола и обычно используется для того, чтобы максимально загрузить канал связи сервера-жертвы бесполезными данными.

  Злоумышленник генерирует большое количество UDP-датаграмм (UDP-шторм), направленных на определенную машину. В результате происходит перегрузка сети и недоступность сервера-жертвы.

  В протоколе TCP есть механизмы предотвращения перегрузок: если подтверждения приема пакетов приходят со значительной задержкой, передающая сторона замедляет скорость передачи TCP-пакетов. Так как в протоколе UDP такой механизм отсутствует, то после начала атаки UDP-трафик "захватывает" практически всю доступную полосу пропускания.

Вредоносное ПО LOIC (Low Orbit Ion Cannon) выполняет распределённую атаку на отказ в обслуживании путём постоянной отправки TCP и UDP пакетов на целевой сайт или сервер.

Это ПО создано для организации DDoS-атак на Web-сайты с участием тысяч анонимных пользователей, пользующихся программой. Атаки производятся на такие сайты, как Visa.com или Mastercard.com.

- **ICMP-flood (ICPM-smurfing).**

Принцип работы такой DDoS-атаки довольно прост. Злоумышленник, изменяя адрес источника, посылает пакет ICMP Echo Request (больше известный как ping) к конкретным хостам.

Эти хосты отвечают пакетом ICMP Echo Reply, отправляя его на тот IP-адрес, который злоумышленник указал как источник. Часто для усиления атаки используются локальные сети (LAN) с включенной опцией направленной широковещательной рассылки (directed broadcast) в ответ на команду "ping" с каждого хоста в составе сети. Например, на один запрос будет отправлено 100 ответов. В результате вся сеть подвергается отказу из-за перегрузки.

- **Mailbombing.**

Суть атаки сводится к тому, чтобы генерировать большое количество сообщений с разных источников для почтового сервера (почтового ящика) с тем, чтобы реализовать ограничение доступа (или полный отказ) к этому почтовому серверу (ящику).

- **Атаки, основанные на уязвимостях протоколов управления.**

Например, утилита THC-SSL-DOS, которую некоторые злоумышленники применяют в качестве инструмента для проведения DoS-атак на SSL-серверы, использует уязвимость в функции повторного подтверждения SSL (SSL renegotiation).

Функция, предназначенная для обеспечения большей безопасности SSL, на самом деле делает его более уязвимым перед атакой.

Программы Backdoors способны производить DDoS атаку.

Например, троян Backdoor.IRCBot.ADEQ представляет собой вредоносное ПО, которое распространяется как регулярное обновление для Java платформы, и являет собой чрезвычайно опасный инструмент для инициации распределенной атаки "отказ в обслуживании".

Данная программа имеет возможность установки ссылки целевого ресурса, назначения времени атаки, интервала и частоты запросов.

Удаленная атака типа "отказ в обслуживании" является активным воздействием, осуществляемым с целью нарушения работоспособности системы, безусловно относительно цели атаки.

Данная удалённая атака является однонаправленным воздействием, как межсегментным, так и внутрисегментным, осуществляемым на транспортном и прикладном уровнях модели OSI.