**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**федеральное государственное бюджетное образовательное учреждение**

**высшего образования**

**«Российский экономический университет имени Г.В. Плеханова»**

**Институт цифровой экономики иинформационных технологий**

**Реферат**

**по дисциплине «Основы информационной безопасности»**

**Тема: «Удаленные атаки на интрасети»**

Выполнил:

студент группы 4310

**Хоанг Хай**

Научный руководитель:

**Алейников Вячеслав Владимирович**

*- Москва, 2021 -*

**Содержание**

[Введение 3](#_Toc83029342)

[I. Что такое удалённая сетевая атака? Ее цель 4](#_Toc83029343)

[II. Классификация атак 5](#_Toc83029344)

[1. Анализ сетевого трафика 6](#_Toc83029345)

[2. Подмена доверенного субъекта 7](#_Toc83029346)

[3. Введение ложного объекта компьютерной сети 7](#_Toc83029347)

[4. Отказ в обслуживании. 7](#_Toc83029348)

[5. Сканирование компьютерных сетей 8](#_Toc83029349)

[III. Краткое описание некоторых сетевых атак 9](#_Toc83029350)

[IV. Технологии обнаружения атак 14](#_Toc83029351)

[Список литературы 16](#_Toc83029352)

# Введение

Для организации коммуникаций в неоднородной сетевой среде применяются набор протоколов TCP/IP, обеспечивая совместимость между компьютерами разных типов. Данный набор протоколов завоевал популярность благодаря совместимости и предоставлению доступа к ресурсам глобальной сети Интернет и стал стандартом для межсетевого взаимодействия. Однако повсеместное распространение стека протоколов TCP/IP обнажило и его слабые стороны. В особенности из-за этого удалённым атакам подвержены распределённые системы, поскольку их компоненты обычно используют открытые каналы передачи данных, и нарушитель может не только проводить пассивное прослушивание передаваемой информации, но и модифицировать передаваемый трафик.

Трудность выявления проведения удалённой атаки и относительная простота проведения(из-за избыточной функциональности современных систем) выводит этот вид неправомерных действий на первое место по степени опасности и препятствует своевременному реагированию на осуществлённую угрозу, в результате чего у нарушителя увеличиваются шансы успешной реализации атаки.

# Что такое удалённая сетевая атака? Ее цель

**Удалённая сетевая атака** — информационное разрушающее воздействие на распределённую вычислительную систему (ВС), осуществляемое программно по каналам связи.

Интранет — в отличие от Интернета, это внутренняя частная сеть организации или крупного государственного ведомства. Как правило, интранет — это Интернет в миниатюре, который построен на использовании протокола IP для обмена и совместного использования некоторой части информации внутри этой организации. Таким образом, интранет — это «частный» Интернет, ограниченный виртуальным пространством отдельно взятой организации. Intranet допускает использование публичных каналов связи, входящих в Internet, (VPN), но при этом обеспечивается защита передаваемых данных и меры по пресечению проникновения извне на корпоративные узлы.

Цель предпринимаемых злоумышленниками атак на компьютеры из интрасетей, подключенных к Интернет, состоит в получении доступа к их информационным и сетевым ресурсам. Примером первого типа ресурсов бывают базы данных, файл-серверы и т. д. Ко второму типу ресурсов относятся сетевые сервисы, к примеру – Интернет, электронная почта͵ телеконференции и т. д.

Принципиальным отличием атак, осуществляемых злоумышленниками в открытых сетях, является фактор расстояния от ПК, выбранного в качестве жертвы, или "прослушиваемого" канала связи до местоположения злоумышленника. Этот фактор нашел выражение в определении подобного вида атак как "удаленных".

Под удаленной атакой принято понимать несанкционированное информационное воздействие на распределенную вычислительную систему, программно осуществляемое по каналам связи.

Для удаленной атаки можно выделить наиболее общие схемы их осуществления. Такие удаленные атаки получили название типовых.

# Классификация атак

Тогда типовая удаленная атака - это удаленное несанкционированное информационное воздействие, программно осуществляемое по каналам связи и характерное для любой распределенной вычислительной системы. Объектом удаленных атак могут стать следующие виды сетевых устройств: оконечные устройства; каналы связи, промежуточные устройства: ретрансляторы, шлюзы, модемы и т.п. Рассмотрим классификацию удаленных атак по следующим шести основным критериям:

1. По характеру воздействия удаленные атаки делятся на пассивные и активные (примером первого типа атак является, к примеру, прослушивание каналов связи и перехват вводимой с клавиатуры информации; примером второго типа является атака "третий посередине", когда злоумышленник может к примеру, подменять данные информационного обмена между двумя пользователями и/или интрасети или между пользователем и запрашиваемым им сетевым сервисом, пересылаемые в обоих направлениях),

2. По цели воздействия, ᴛ.ᴇ. исходя из нарушения трех базовых возможных свойств информации и информационных ресурсов - их конфиденциальности, целостности и доступности, плюс нарушение доступности всей системы или ее отдельных служб (пример атаки - "отказ в обслуживании");

3. По условию начала осуществления воздействия атака должна быть безусловной (предпринимается злоумышленником в любом случае), или может активизироваться либо при посылке определенного запроса от атакуемого объекта͵ либо при наступлении ожидаемого события на атакуемом объекте;

4. По наличию обратной связи с атакуемым объектом различают атаки с обратной связью или без обратной связи (такая атака принято называть однонаправленной);

5. По расположению субъекта атаки относительно атакуемого объекта бывают внутрисегментными (средства взлома сети или, к примеру, прослушивания каналов связи должны располагаться в том же сегменте сети, который интересует злоумышленника) или межсегментными (в данном случае дальность расстояния от жертвы до злоумышленника не имеет значения);

6. По уровню эталонной модели взаимосвязи открытых систем 0SI Международной Организации Стандартизации (ISO), на котором осуществляется воздействие. Атака может реализовываться на всех семи уровнях - физическом, канальном, сетевом, транспортном, сеансовом, представительном и прикладном. Средства обеспечения безопасности интрасетей на базе такой модели регламентируются стандартом ISO7492-2. Эти же рекомендации могут применяться и для разработки, создания аналогичных механизмов в Интернет-сетях, так как группа протоколов ТСР/IР соответствует уровням 1-4 модели, а прикладной уровень в сетях соответствует верхним уровням (5-7).

Среди выше перечисленных УА можно выделить пять базовых и наиболее часто предпринимаемых в настоящее время типовых удаленных атак:

## Анализ сетевого трафика

Анализ сетевого трафика путем его перехвата (сниффинга) является внутрисегментной атакой и направлен на перехват и анализ информации, предназначенной для любого ПК, расположенного в том же сегменте сети, что и злоумышленник. Злоумышленник может захватить все проходящие через себя пакеты путем перевода своей сетевой платы в смешанный режим (promiscuous mode).

Реализация данной атаки позволяет злоумышленнику изучить логику работы сети (для получения информации, помогающей ему осуществить последующий взлом) либо перехватить конфиденциальную информацию, которой обмениваются узлы компьютерной сети. Многие протоколы (например, POP3, FTP и пр.) передают информацию об используемых паролях доступа по каналу связи в открытом виде. Анализ трафика позволяет злоумышленнику перехватить эти пароли доступа (например, к электронной почте, к FTP серверу) и использовать их в дальнейшем для выполнения несанкционированных действий.

## Подмена доверенного субъекта

Подмена доверенного субъекта и передача сообщений по каналам связи от его имени позволяет получить злоумышленнику доступ к удаленной системе от имени этого доверенного субъекта. Подобные атаки эффективно реализуются в системах с нестойкими алгоритмами идентификации и аутентификации хостов и пользователей. Например, подобные атаки эффективны для систем, использующих аутентификацию источника по его IP адресу, для злоумышленника в этом случае нетрудно формировать пакеты с IP адресами, которым «доверяет» удаленный узел.

## Введение ложного объекта компьютерной сети

Реализация данной атаки позволяет навязать ложный маршрут потока информации так, чтобы этот маршрут лежал через компьютер злоумышленника, позволяет «заманить» легального пользователя на ПК злоумышленника (например, подменив WEB-сайт) с целью получения конфиденциальной информации.

## Отказ в обслуживании.

Атака должна быть предпринята͵ если нет средств аутентификации адреса отправителя и с хоста на атакуемый хост можно передавать бесконечное число анонимных запросов на подключение от имени других хостов. В этом способе проникновения используется возможность фрагментирования пакетов, содержащаяся в спецификации IР. Нападающий передает чересчур много фрагментов пакетов, которые должны быть смонтированы принимающей системой. В случае если общий объём фрагментов превышает максимально допустимый размер пакета͵ то система "зависает" или даже выходит из строя.

Результатом осуществления данной атаки может стать:

* Нарушение работоспособности соответствующей службы предоставления удаленного доступа на атакуемый хост;
* Передача с одного адреса такого количества запросов на подключение к атакуемому хосту, какое максимально может "вместить" трафик (атака - направленный "шторм запросов"), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

## Сканирование компьютерных сетей

Сетевое сканирование осуществляется злоумышленником на предварительной стадии атаки. Сканирование компьютерной сети позволяет получить злоумышленнику такую информацию, необходимую для дальнейшего взлома, как типы установленных ОС, открытые порты и связанные с ними сервисы, существующие уязвимости. Сам факт сетевого сканирования лишь говорит о реализации стадии, предваряющей атаку, и является важной информацией для сетевого администратора.

# Краткое описание некоторых сетевых атак

**Фрагментация данных**

При передаче пакета данных протокола IP по сети может осуществляться деление этого пакета на несколько фрагментов. Впоследствии, при достижении адресата, пакет восстанавливается из этих фрагментов. Злоумышленник может инициировать посылку большого числа фрагментов, что приводит к переполнению программных буферов на приемной стороне и, в ряде случаев, к аварийному завершению системы.

**Атака Ping flooding**

Данная атака требует от злоумышленника доступа к быстрым каналам в Интернет.

Программа ping посылает ICMP-пакет типа ECHO REQUEST, выставляя в нем время и его идентификатор. Ядро машины-получателя отвечает на подобный запрос пакетом ICMP ECHO REPLY. Получив его, ping выдает скорость прохождения пакета.

При стандартном режиме работы пакеты высылаются через некоторые промежутки времени, практически не нагружая сеть. Но в «агрессивном» режиме поток ICMP echo request/reply-пакетов может вызвать перегрузку небольшой линии, лишив её способности передавать полезную информацию.

**Нестандартные протоколы, инкапсулированные в IP**

Пакет IP содержит поле, определяющее протокол инкапсулированного пакета (TCP, UDP, ICMP). Злоумышленники могут использовать нестандартное значение данного поля для передачи данных, которые не будут фиксироваться стандартными средствами контроля информационных потоков.

**Атака smurf**

Атака smurf заключается в передаче в сеть широковещательных ICMP запросов от имени компьютера-жертвы. В результате компьютеры, принявшие такие широковещательные пакеты, отвечают компьютеру-жертве, что приводит к существенному снижению пропускной способности канала связи и, в ряде случаев, к полной изоляции атакуемой сети. Атака smurf исключительно эффективна и широко распространена.

Противодействие: для распознавания данной атаки необходимо анализировать загрузку канала и определять причины снижения пропускной способности.

**Атака DNS spoofing**

Результатом данной атаки является внесение навязываемого соответствия между IP-адресом и доменным именем в кэш DNS сервера. В результате успешного проведения такой атаки все пользователи DNS сервера получат неверную информацию о доменных именах и IP-адресах. Данная атака характеризуется большим количеством DNS пакетов с одним и тем же доменным именем. Это связано с необходимостью подбора некоторых параметров DNS обмена.

Противодействие: для выявления такой атаки необходимо анализировать содержимое DNS трафика либо использовать DNSSEC.

**Атака IP spoofing**

Большое количество атак в сети Интернет связано с подменой исходного IP-адреса. К таким атакам относится и syslog spoofing, которая заключается в передаче на компьютер-жертву сообщения от имени другого компьютера внутренней сети. Поскольку протокол syslog используется для ведения системных журналов, путём передачи ложных сообщений на компьютер-жертву можно навязать информацию или замести следы несанкционированного доступа.

Противодействие: выявление атак, связанных с подменой IP-адресов, возможно при контроле получения на одном из интерфейсов пакета с исходным адресом этого же интерфейса или при контроле получения на внешнем интерфейсе пакетов с IP-адресами внутренней сети.

**Навязывание пакетов**

Злоумышленник отправляет в сеть пакеты с ложным обратным адресом. С помощью этой атаки злоумышленник может переключать на свой компьютер соединения, установленные между другими компьютерами. При этом права доступа злоумышленника становятся равными правам того пользователя, чье соединение с сервером было переключено на компьютер злоумышленника.

**Sniffing — прослушивание канала**

Возможно только в сегменте локальной сети.

Практически все сетевые карты поддерживают возможность перехвата пакетов, передаваемых по общему каналу локальной сети. При этом рабочая станция может принимать пакеты, адресованные другим компьютерам того же сегмента сети. Таким образом, весь информационный обмен в сегменте сети становится доступным злоумышленнику. Для успешной реализации этой атаки компьютер злоумышленника должен располагаться в том же сегменте локальной сети, что и атакуемый компьютер.

**Перехват пакетов на маршрутизаторе**

Сетевое программное обеспечение маршрутизатора имеет доступ ко всем сетевым пакетам, передаваемым через данный маршрутизатор, что позволяет осуществлять перехват пакетов. Для реализации этой атаки злоумышленник должен иметь привилегированный доступ хотя бы к одному маршрутизатору сети. Поскольку через маршрутизатор обычно передается очень много пакетов, тотальный их перехват практически невозможен. Однако отдельные пакеты вполне могут быть перехвачены и сохранены для последующего анализа злоумышленником. Наиболее эффективен перехват пакетов FTP, содержащих пароли пользователей, а также электронной почты.

**Навязывание хосту ложного маршрута с помощью протокола ICMP**

В сети Интернет существует специальный протокол ICMP (Internet Control Message Protocol), одной из функцией которого является информирование хостов о смене текущего маршрутизатора. Данное управляющее сообщение носит название redirect. Существует возможность посылки с любого хоста в сегменте сети ложного redirect-сообщения от имени маршрутизатора на атакуемый хост. В результате у хоста изменяется текущая таблица маршрутизации и, в дальнейшем, весь сетевой трафик данного хоста будет проходить, например, через хост, отославший ложное redirect-сообщение. Таким образом возможно осуществить активное навязывание ложного маршрута внутри одного сегмента сети Интернет.

**WinNuke**

Наряду с обычными данными, пересылаемыми по TCP-соединению, стандарт предусматривает также передачу срочных (Out Of Band) данных. На уровне форматов пакетов TCP это выражается в ненулевом urgent pointer. У большинства ПК с установленным Windows присутствует сетевой протокол NetBIOS, который использует для своих нужд три IP-порта: 137, 138, 139. Если соединиться с Windows машиной по 139 порту и послать туда несколько байт OutOfBand данных, то реализация NetBIOS-а, не зная, что делать с этими данными, попросту вешает или перезагружает машину. Для Windows 95 это обычно выглядит как синий текстовый экран, сообщающий об ошибке в драйвере TCP/IP, и невозможность работы с сетью до перезагрузки ОС. NT 4.0 без сервис-паков перезагружается, NT 4.0 с ServicePack 2 паком выпадает в синий экран. Судя по информации из сети подвержены такой атаке и Windows NT 3.51 и Windows 3.11 for Workgroups.

Посылка данных в 139-й порт приводит к перезагрузке NT 4.0, либо выводу «синего экрана смерти» с установленным Service Pack 2. Аналогичная посылка данных в 135 и некоторые другие порты приводит к значительной загрузке процесса RPCSS.EXE. На Windows NT WorkStation это приводит к существенному замедлению работы, Windows NT Server практически замораживается.

**Подмена доверенного хоста**

Успешное осуществление удалённых атак этого типа позволит злоумышленнику вести сеанс работы с сервером от имени доверенного хоста. (Доверенный хост — станция легально подключившаяся к серверу). Реализация данного вида атак обычно состоит в посылке пакетов обмена со станции злоумышленника от имени доверенной станции, находящейся под его контролем.

# Технологии обнаружения атак

Для защиты от **анализа сетевого трафика с использованием снифферов** известны следующие подходы:

* Диагностика перевода сетевой платы удаленного ПК в смешанный режим путем установки различных средств мониторинга. Данный подход к защите достаточно трудоемок и не является универсальным, поэтому используется недостаточно часто.
* Сегментация сетей - чем больше сегментов, тем меньше вероятность и последствия реализации внутрисегментной атаки.
* Шифрование сетевого трафика и использование безопасных протоколов удаленной аутентификации пользователей (S/KEY, CHAP и др.).

Для защиты от от **Подмены доверенного субъекта** необходимо применение стойких алгоритмов идентификации и аутентификации хостов и пользователей. Нельзя допускать в компьютерную сеть организации пакеты, посланные с внешних ПК, но имеющих внутренний сетевой адрес.

Для защиты от **Введения ложного объекта компьютерной сети**необходимо использовать более стойкие протоколы идентификации и аутентификации хостов и устройств.

Для защиты от **Отказа в обслуживании (DoS)** необходимо использовать стойкие протоколы аутентификации, ограничивать доступ в сеть с использованием межсетевых экранов, применять системы обнаружения вторжений, разрабатывать адекватные политики безопасности, использовать для поддержки сервисов программные продукты, в которых устранены уязвимости, позволяющие выполнить подобные атаки.

В настоящее время большую актуальность представляет защита от распределенных DoS атак (DDoS), реализуемых путем заражения («зомбирования») множества ничего не подозревающих ПК, которые в заданный момент времени начинают посылать «шторм запросов» на объект атаки.

Для защиты от **сетевого сканирования** необходимо применять подходы, позволяющие скрыть внутреннюю структуру сети и идентифицировать факт сканирования, например, использовать межсетевые экраны, системы обнаружения вторжений.

Таким образом, для защиты от рассмотренных выше атак используют:

* Межсетевые экраны;
* Виртуальные частные сети;
* Стойкие протоколы аутентификации;
* Системы обнаружения вторжений;
* Анализ журналов безопасности (аудита) компьютерных систем.

# Список литературы

1. Удалённые сетевые атаки / Wikipedia - Электрон. дан. - Режим доступа: <https://ru.wikipedia.org/wiki/%D0%A3%D0%B4%D0%B0%D0%BB%D1%91%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D1%8B%D0%B5_%D0%B0%D1%82%D0%B0%D0%BA%D0%B8>
2. Интранет / Wikipedia - Электрон. дан. - Режим доступа: <https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D1%80%D0%B0%D0%BD%D0%B5%D1%82>
3. Классификация типовых удаленных атак на интрасети / © Портал студенческих и научных материалов Ozlib.com (info{aт}ozlib.com) © 2017 - 2021 - Электрон. дан. - Режим доступа: <https://ozlib.com/974105/tehnika/klassifikatsiya_tipovyh_udalennyh_atak_intraseti>