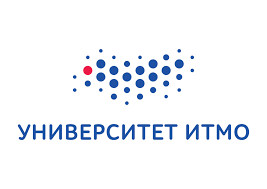
**Министерство науки и высшего образования Российской Федерации**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**



**Факультет безопасности информационных технологий**

**Дисциплина:**

«Теория информационной безопасности и методология защиты

информации»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №3**

«Экспертные оценки»

**Выполнили:**

Нгуен Тхи Маи, студент группы: N3245

*\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

**Проверил:**

Есипов Дмитрий Андреевич, ассистент ФБИТ

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(отметка о выполнении)

*\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

**Содержание**

[**Введение 3**](#_heading=h.gg4ihxnmmfqz)

[**1. Определение DoS-атаки 4**](#_heading=h.hqthl1jj2nv)

[**2. Цели DoS-атак 5**](#_heading=h.7ym9irpv5nls)

[**3. DoS атаки 6**](#_heading=h.lqac0yjraw74)

[**4. Как предотвратить DoS-атаки 9**](#_heading=h.oizpagroh9wo)

# **Введение**

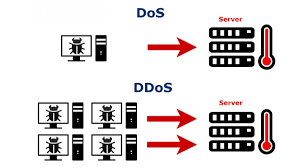
Цель работы: Исследование методов DoS/DDoS-атак:

* Определение DoS-атаки;
* Цели DoS-атак;
* DoS атаки;
* Как предотвратить DoS-атаки;

# Определение DoS-атаки

DoS-атака (Denial of Service) — это тип атаки, при которой человек делает систему непригодной для использования или существенно замедляет ее работу для обычных пользователей, перегружая ее системные ресурсы. Это самый простой тип атаки. Хотя DoS-атака не дает возможности получить доступ к реальным данным системы, она может нарушить работу служб, предоставляемых системой.

DDoS-атака (Distributed Denial of Service) — это форма DoS, но для проведения атаки злоумышленник использует несколько компьютеров. Промежуточные компьютеры, используемые для атак, называются зомби (компьютерами-призраками). В настоящее время пользователи компьютерных сетей, такие как мы, сталкиваются со многими более сложными методами, чем традиционные DDoS-атаки. Эти методы позволяют злоумышленнику контролировать чрезвычайно большое количество захваченных компьютеров (зомби) на удаленной станции, просто используя протокол IRC.



DoS-атака и DDoS-атака

Разница в том, что DoS — это атака из одного источника, а DDoS — из множества разных источников, поэтому и методы борьбы тоже немного отличаются.

Например: если вы обнаружите признаки DoS, вам нужно только найти и отключить действия или соединения, связанные с источником (только 1), но у DDoS много источников атаки, поэтому вы не можете этого сделать. Важным моментом является то, что если вы подверглись DDoS-атаке, вы не сможете от нее защититься.

# Цели DoS-атак

Целями DoS-атак являются:

* Занимая пропускную способность сети и переполняя сеть, сеть не сможет предоставлять другие услуги обычным пользователям.
* Разъединяет соединение между двумя машинами и предотвращает доступ к сервису.
* Запретить определенным пользователям доступ к определенной услуге
* Запретить доступ к услугам другим лицам.

# 3. DoS атаки

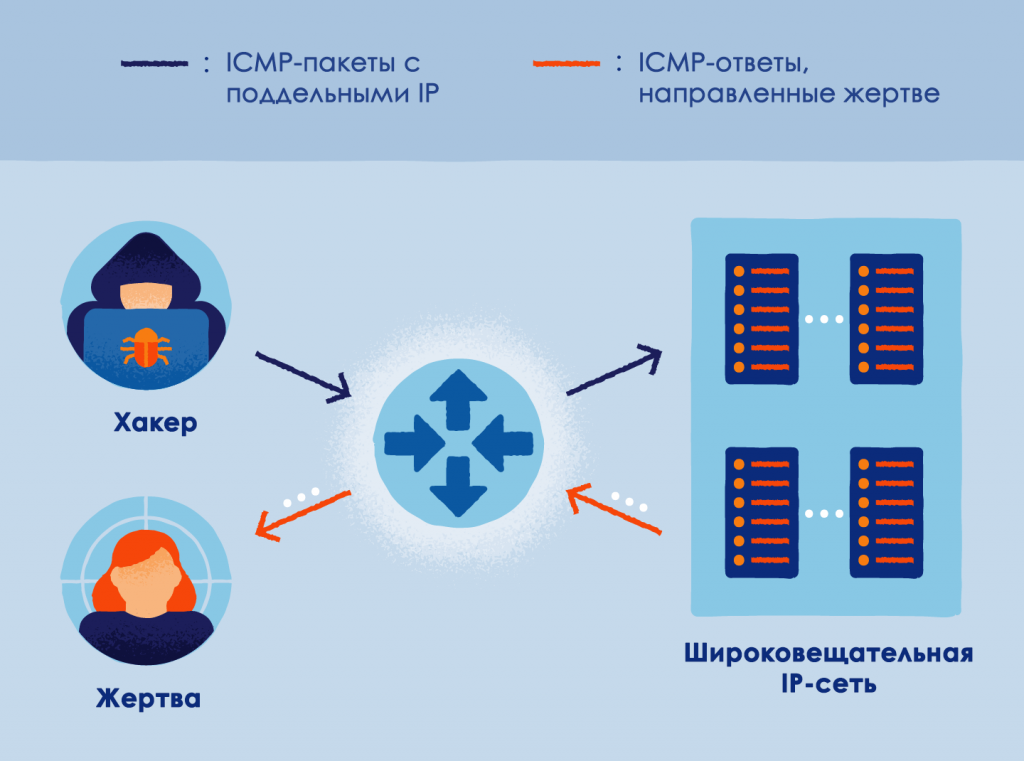
DoS-атаки бывают следующих типов:

Атаки типа « Denial of Service» делятся на два типа атак.

* DoS-атака: атака со стороны отдельного лица или группы лиц.
* DDoS-атака: это атака из компьютерной сети, предназначенная для атаки на конкретную цель.

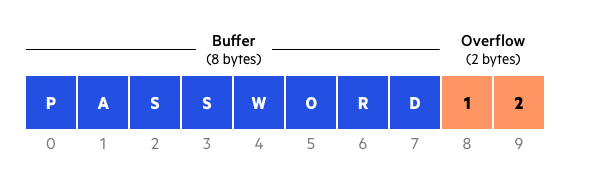
Winnuke - Этот тип DoS-атаки может применяться только к компьютерам под управлением Windows9x. Хакер отправляет пакеты с “Out of Band” данными на порт 139 целевого компьютера. (Порт 139 — это порт NetBIOS, этот порт принимает только пакеты с включенным флагом Out of Band). Когда компьютер получает этот пакет, жертве отображается синий экран ошибки, поскольку программа Windows получила эти пакеты, но не знает, как реагировать на данные Out Of Band, что приводит к “crash” системы.

Атака Smurf — это форма атаки типа «отказ в обслуживании» (DDOS). Злоумышленник пытается атаковать сервер жертвы с помощью пакета «Internet Control Message Protocol». Отправляя запросы с использованием IP-адреса, который выдает себя за сервер жертвы. Одновременно отправлять пакеты на один или несколько компьютеров в одной сети. Эти машины после получения запроса отправят ответный пакет на машину-жертву. Усиление этой атаки приведет к перегрузке сервера и приведет к отказу в обслуживании. Однако когда-то этот тип атаки считался уязвимостью операционных систем. Теперь он обновлен патчами, в которых этот метод атаки больше не используется.

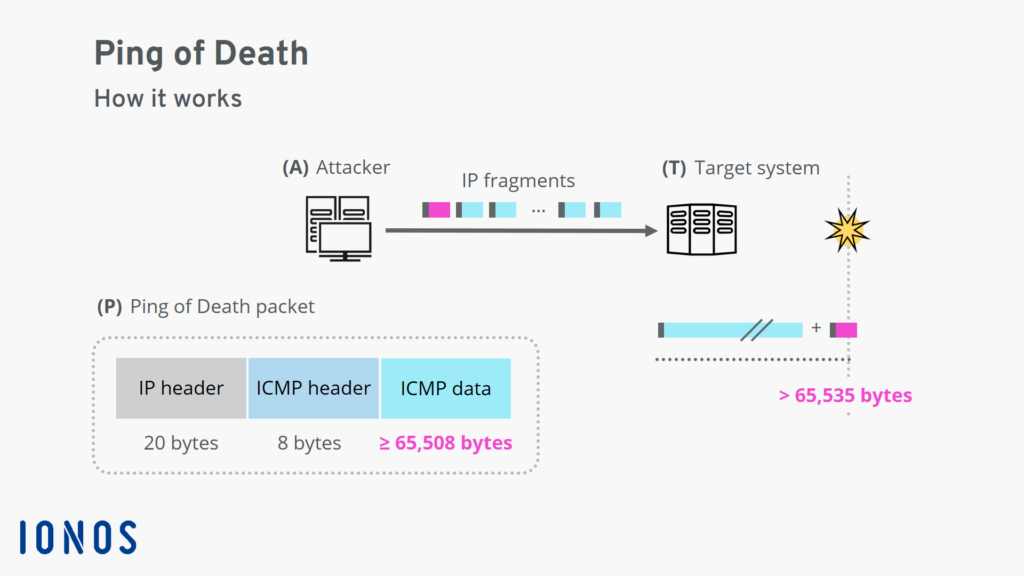


Атака Smurf

Buffer overflow — это ошибка, которая возникает, когда память в стеке перезаписывается несколько раз. Эта ошибка часто возникает из-за того, что пользователь отправляет большой объем данных на сервер приложений, что приводит к принудительной перезаписи данных соседними ячейками памяти. Это программная ошибка, которая может привести к исключению доступа к памяти компьютера и завершению работы программы. Кроме того, когда пользователи намеренно совершают саботаж, эта ошибка может быть использована для нарушения безопасности системы.



Ping of Death (PoD) — это тип атаки типа «отказ в обслуживании» (DoS), при которой злоумышленник пытается вывести из строя, дестабилизировать или заморозить целевой компьютер или службу, отправляя неправильно отформатированные или слишком большие пакеты с помощью простого пинг-запроса. команда. Размер правильно отформатированного пакета IPv4, включая IP-заголовок, составляет 65 535 байт, включая общую емкость полезной нагрузки 84 байта. Многие компьютерные системы прошлого просто не могли обрабатывать большие пакеты и при их получении происходили сбои. Эту ошибку легко эксплуатировать в ранних реализациях TCP/IP в различных операционных системах, включая Windows, Mac, Unix, Linux, а также в сетевых устройствах, таких как принтеры и маршрутизаторы. Поскольку отправка ping-пакета размером более 65 535 байт нарушает Интернет-протокол, злоумышленники обычно отправляют искаженные пакеты фрагментами. Когда целевая система пытается собрать фрагменты заново и в итоге получает слишком большой пакет, может произойти переполнение памяти, что приведет к различным системным проблемам, включая сбои в работе.



# 4. Как предотвратить DoS-атаки

Так как же можно предотвратить DDoS-атаку?

Выявляйте DDoS-атаки на ранней стадии. Если вы используете частный сервер, вам необходимо иметь возможность определить, когда на вас нападают. Потому что чем раньше вы обнаружите, что проблемы, возникающие на вашем сайте, вызваны DDoS-атакой, тем больше у вас шансов их решить. Чтобы это сделать, вам следует изучить профиль посещаемости вашего сайта; Чем лучше вы понимаете типичный поток трафика вашего веб-сайта, тем легче вам будет обнаружить риски, как только произойдут изменения. Большинство DDoS-атак начинаются с внезапного увеличения трафика, и этот профиль полезен для того, чтобы отличить внезапное увеличение количества законных посетителей от увеличения трафика. Вам также следует выбрать сотрудника, который будет нести основную ответственность за действия по предотвращению DDoS-атак, чтобы обеспечить своевременные меры реагирования в случае случайной атаки.

Резервная полоса пропускания. Вам следует использовать большую пропускную способность, чем необходимо для вашего веб-сервера. Таким образом, вы сможете реагировать на неожиданные всплески трафика – будь то рекламная кампания, специальная акция, которую проводит ваша компания, или название компании.Ваша компания упоминается в СМИ. Даже если вы используете на 100% или даже на 500% больше пропускной способности, чем вам действительно необходимо, это не обязательно предотвратит DDoS-атаку, но может дать вам несколько дополнительных минут на действия, прежде чем ваш компьютер выйдет из строя.Владелец перегружен. Существует ряд технических мер, которые вы можете предпринять, чтобы смягчить последствия атаки, особенно в первые минуты:

* Ограничьте маршрутизатор, чтобы предотвратить перегрузку веб-сервера.
* Добавьте фильтры на маршрутизатор для удаления поддельных пакетов из очевидных источников атак.
* Сокращение времени ожидания получения пакетов аутентификации увеличивает возможности подключения.
* Устраняет поддельные или поврежденные пакеты
* Установите более низкие пороговые значения совокупного отбрасывания SYN, ICMP и UDP.

Хотя вышеуказанные шаги были эффективными в прошлом, они не оказали существенного влияния на текущие DDoS-атаки из-за их большого масштаба. Единственное, на что вы можете надеяться, это то, что эти шаги дадут вам немного больше времени, прежде чем произойдет DDoS-атака.

Свяжитесь с вашим интернет-провайдером или хостингом. Следующий шаг — связаться с вашим интернет-провайдером (или хостинг-провайдером, если у вас нет собственного веб-сервера), сообщить ему, что вы подверглись атаке, и попросить о помощи. Всегда держите их связь на случай чрезвычайных ситуаций. В зависимости от силы атаки они, возможно, уже обнаружили ее или могут также начать быть подавленными атакой.По сравнению с использованием частного веб-сервера, у вас будет больше шансов предотвратить атаку. DDoS выше, если веб-сервер находится в хостинг-центре. Это потому, что эти центры имеют более высокую пропускную способность и более мощные маршрутизаторы, чем ваша компания, а их сотрудники будут иметь больше опыта борьбы с атаками. При размещении веб-сервера в хостинговой компании DDoS-трафик будет нацелен на веб-сервер этой компании и покинет локальную сеть вашей компании, таким образом, по крайней мере, часть вашего бизнеса, включая электронную почту и, возможно, услуги передачи голоса по IP, может работать нормально во время такой атаки. При достаточно масштабной DDoS-атаке первое, что может сделать хостинговая компания или интернет-провайдер, — это «направить» трафик на веб-сайт — в результате пакеты, предназначенные для веб-сервера, будут удалены до того, как они прибудут. Если вы остановитесь на этом этапе, DDos-атака будет успешной. Они терпят неудачу только тогда, когда ваш сайт снова работает нормально. Для этого интернет-провайдер или хостинговая компания могут перенаправить трафик в «скруббер», где вредоносные пакеты удаляются до того, как законные пакеты будут отправлены на веб-сервер. Создание разумного плана DDoS с вашим интернет-провайдером или хостинговой компанией может свести вредные последствия этой атаки к минимуму.

Свяжитесь с экспертами по DDoS. В случае крупных атак, возможно, лучший шанс вернуть ваш веб-сайт в сеть — это использовать компанию, которая специализируется на предотвращении DDoS-атак. Эти организации имеют крупномасштабную инфраструктуру и используют различные технологии, включая очистку данных, чтобы поддерживать ваш сайт в сети. В случае серьезной атаки вы можете напрямую связаться с компанией по предотвращению DDoS-атак или через свою хостинговую компанию/провайдера услуг, чтобы договориться с ними о партнерстве. Свяжитесь с экспертами по предотвращению DDoS-атак. Услуги по предотвращению DDoS-атак не бесплатны, поэтому все зависит от того, хотите ли вы платить за то, чтобы оставаться в сети и ждать, пока DDoS-атака утихнет, прежде чем продолжить свою деятельность. Подписка на постоянную услугу по предотвращению DDoS-атак может стоить несколько сотен долларов в месяц. Вы также можете подождать, пока на вас нападут, чтобы воспользоваться этой услугой, однако вам, возможно, придется заплатить больше и подождать дольше, прежде чем услуга запустится.

Создайте «Playbook DDoS» Лучший способ гарантировать, что ваша организация максимально быстро и эффективно отреагирует на DDoS-атаку, — это создать сценарий, документирующий каждый этап процесса и реагировать при обнаружении атаки. Сюда входят действия, описанные выше, с указанием контактных имен и номеров телефонов всех, кто должен присутствовать во время мероприятия. Компании, занимающиеся смягчением последствий DDoS-атак, могут помочь в этом, запустив симуляцию DDoS-атаки, что позволит вам быстро разработать и настроить процессы вашей компании в ответ на реальную атаку. Важная часть, которую не следует упускать из виду в вашем плане реагирования на DDoS-атаку, — это то, как вы будете общаться с клиентами. DDoS-атаки могут длиться до 24 часов, а хорошая связь может обеспечить минимальные затраты бизнеса во время атаки.