"Innovations in Science and Technologies" scientific electronic journal
www.innoist.uz
ISSN : 3030-3451
Volume 1
№ 1
February, 2024

ОБЗОР И РАЗЛИЧИЯ МЕЖДУ DOS И DDOS АТАКАМИ

***Исаков Аброр Фахриддинович**, заместитель начальника кафедры Информационных технологии Академия МВД*

***Абдужаппоров Шахбоз Музаффар угли**, курсант Академия МВД*

***Исокова Мухлиса Фахриддин кизи**, студент Ташкентского университета информационных технологий имени Мухаммада Аль-Хорезми*

Аннотация. В данной статье рассматриваются атаки на компьютерные системы, известные как DoS (отказ в обслуживании) и DDoS (распределенный отказ в обслуживании). Оба типа атак направлены на нарушение нормальной работы целевой системы, но имеют существенные различия в способе осуществления и масштабе последствий.

В разделе, посвященном DoS-атакам, описывается, что они представляют собой попытку перегрузить целевую систему, делая ее недоступной для легитимных пользователей. DoS-атаки могут осуществляться различными способами, включая флуд запросами, использование уязвимостей программного обеспечения или перегрузку сетевых ресурсов. Однако важно отметить, что в отличие от DDoS-атак, DoS-атаки выполняются с использованием одного источника, что ограничивает их масштаб и эффективность.

В разделе, посвященном DDoS-атакам, обсуждаются их отличительные особенности. DDoS-атаки осуществляются при помощи ботнета, то есть сети захваченных компьютеров, известных как "зомби". Зомби-компьютеры используются для одновременного направления огромного количества запросов на целевую систему, что приводит к перегрузке и ее недоступности. DDoS-атаки могут быть распределенными по различным географическим областям, что делает их более сложными для обнаружения и смягчения.

В заключении подчеркивается важность защиты от DoS и DDoS-атак. Это может включать использование фаерволов, систем обнаружения вторжений (IDS) и систем предотвращения вторжений (IPS), а также распределенных служб обнаружения и отключения (DDoS-защита). Кроме того, важно постоянно обновлять программное обеспечение и применять практики безопасности для уменьшения уязвимостей системы перед атакой.

Ключивые слова: DoS (отказ в обслуживании), DDoS (распределенная атака отказом в обслуживании), кибератаки, нарушение доступности, ресурсоемкие запросы, ботнет, злоумышленники, отказ в обслуживании, сетевая безопасность, защитные меры, инфраструктура сети, ответное время, пропускная способность, масштабируемость, уязвимости, методы атак, идентификация и фильтрация трафика, мониторинг сетевой активности, серверная защита, предотвращение атак.

В современном цифровом мире существует множество угроз информационной безопасности, и одной из наиболее распространенных являются атаки на сети и сервера, известные как DoS (от англ. Denial of Service) и DDoS (от англ. Distributed Denial of Service). В этой статье мы рассмотрим основные концепции и различия между этими двумя видами атак.

Что такое DoS атака?DoS атака - это попытка нарушить нормальную работу сети, сервера или компьютера, делая их недоступными для легитимных пользователей. Она основывается на перегрузке ресурсов целевой системы, таких как пропускная способность сети, процессорное время или доступная память. Атакующий отправляет большое количество запросов или злоумышленный трафик на целевую систему, вынуждая ее тратить ресурсы на обработку этих запросов и, в конечном итоге, приводя к отказу в обслуживании легитимных пользователей.

Примеры DoS атак включают в себя атаку с помощью флуда (флуд-атака), когда злоумышленник отправляет большое количество запросов на определенный сервис или сервер, перегружая его ресурсы и вызывая отказ в обслуживании. Еще одним примером является атака с использованием отказа в обслуживании, когда злоумышленник злоупотребляет уязвимостями в программном обеспечении или настройках сети, чтобы вызвать сбой в работе системы.

Что такое DDoS атака?DDoS атака - это расширенная версия DoS атаки, в которой атакующий использует несколько компьютеров или устройств, называемых ботнетом, для выполнения атаки. Ботнет - это сеть зараженных компьютеров, которые контролируются злоумышленником без ведома владельцев компьютеров. Каждый компьютер в ботнете, известный как зомби, служит для отправки огромного количества запросов или злоумышленного трафика на целевую систему.

DDoS атаки имеют преимущество перед DoS атаками в своей способности создавать намного больший объем трафика и превышать

пропускную способность сети или ресурсы целевой системы. Кроме того, распределение атаки между множеством компьютеров делает ее более сложной для обнаружения и пресечения.

Ресурсы и объем трафика: В DoS атаках один компьютер или источник генерирует атакующий трафик, в то время как в DDoS атаках используется ботнет, состоящий из множества компьютеров, что позволяет генерировать гораздо больший объем трафика.

Распределение и координация: В DoS атаках атакующий должен быть в состоянии справиться с атакой самостоятельно, в то время как в DDoS атаках атакующий использует множество компьютеров, чтобы создать координированную атаку, что значительно усложняет обнаружение и защиту от нее. Масштаб атаки: DDoS атаки имеют потенциал создавать более мощные и разрушительные атаки, способные перегрузить даже самые мощные сети и серверы.

Сложность источника: В DoS атаках источником атаки обычно является один компьютер или адрес IP, что делает его более легким для идентификации и блокирования. В DDoS атаках источником атаки являются множество компьютеров, что затрудняет их отслеживание и блокирование.

Защита от DoS и DDoS атак:Защита от DoS и DDoS атак требует комплексного подхода, который включает в себя следующие меры: Использование специализированных аппаратных или программных решений, которые способны обнаруживать и отвечать на атаки. Фильтрация сетевого трафика для блокирования подозрительного или злоумышленного трафика перед его достижением целевой системы. Конфигурация сетевых устройств и серверов для улучшения их устойчивости к атакам. Мониторинг и анализ сетевой активности для обнаружения необычного поведения или аномалий, которые могут указывать на атаку. Распределение сетевой нагрузки и использование CDN (Content Delivery Network), чтобы распределить трафик между несколькими серверами или узлами и снизить возможность перегрузки.

DoS и DDoS атаки представляют серьезную угрозу для сетей и серверов, и их последствия могут быть разрушительными для организаций и пользователей. Понимание различий между этими двумя видами атак и принятие соответствующих мер по защите помогут укрепить информационную безопасность и обеспечить бесперебойное функционирование сетей и систем.

Защита от DoS и DDoS атак требует комплексного подхода и применения различных мер безопасности. Вот некоторые из них:

Использование средств обнаружения и предотвращения атак: Установка специализированного программного обеспечения (например, фаервола) или аппаратных устройств, способных обнаруживать и блокировать атаки DoS и DDoS. Настройка систем мониторинга сетевой активности, чтобы обнаруживать аномальные или подозрительные паттерны трафика.

Фильтрация и ограничение трафика: Использование мер фильтрации сетевого трафика, чтобы блокировать известные источники злоумышленного трафика. Ограничение частоты запросов от одного и того же источника, чтобы предотвратить перегрузку ресурсов. Установка ограничений на размер передаваемых данных и объем трафика с целью предотвращения атак, основанных на переполнении памяти или пропускной способности.

Распределение сетевой нагрузки: Использование Content Delivery Network (CDN), чтобы распределить трафик между несколькими серверами или узлами и снизить возможность перегрузки одного центрального сервера. Использование балансировщиков нагрузки для равномерного распределения запросов между несколькими серверами.

Конфигурация сетевых устройств и серверов: Оптимизация настроек сетевых устройств и серверов для повышения их устойчивости к атакам, например, путем настройки максимального количества одновременных соединений или установки временных ограничений на обработку запросов. Использование механизмов защиты, таких как IP-фильтрация, чтобы блокировать известные источники атак.

Анализ и реагирование на атаки: Мониторинг сетевой активности и реагирование на аномальное поведение или атаки в реальном времени. Создание и регулярное обновление плана реагирования на атаки, который включает шаги по митигации атак и восстановлению после них.

Повышение общей безопасности сети: Регулярное обновление программного обеспечения и патчей, чтобы устранить уязвимости, которые могут быть использованы злоумышленниками. Использование сильных паролей и механизмов аутентификации для предотвращения несанкционированного доступа к системам. Обучение пользователей и сотрудников о мерах безопасности, чтобы предотвратить социальную инженерию и атаки, основанные на человеческом факторе.

Важно отметить, что защита от DoS и DDoS атак требует постоянного мониторинга, анализа и обновления мер безопасности, так как методы атак постоянно совершенствуются. Использование облачных служб: Переносить некоторые сервисы и ресурсы на облачные платформы может помочь

распределить нагрузку и предотвратить прямые атаки на ваши физические серверы.

Планирование пропускной способности: Оценка и планирование достаточной пропускной способности сети и хостинг-ресурсов для справления с возможными атаками на пиковых нагрузках. Использование систем капчи: Включение системы капчи на веб-страницах или других точках входа может помешать автоматизированным ботам участвовать в атаках.

Проверка на наличие зомби-компьютеров: Регулярно проверять компьютеры в сети на наличие зловредного ПО, такого как трояны и ботнеты, которые могут быть использованы для запуска DDoS атак. Использование сервисов CDN и WAF: Веб-приложения и сайты могут получить значительную защиту от DDoS атак, используя услуги Content Delivery Network (CDN) и Web Application Firewall (WAF). Резервное копирование данных: Регулярное создание резервных копий данных поможет минимизировать ущерб от атак и облегчить восстановление после них.

Планирование тестов на уязвимости: Регулярное проведение тестов на уязвимости и пентестинга поможет выявить слабые места в системе и принять соответствующие меры по их исправлению.

Сотрудничество с провайдером услуг: Связывайтесь с вашим интернет-провайдером для обсуждения мер безопасности и возможности использования их инфраструктуры для фильтрации вредоносного трафика.

Постоянное обновление мер безопасности: Атаки и методы злоумышленников постоянно эволюционируют. Поэтому важно регулярно обновлять и адаптировать меры безопасности, чтобы оставаться защищенным. Помните, что защита от DoS и DDoS атак - это непрерывный процесс. Реализация этих мер безопасности в сочетании с постоянным мониторингом и анализом сетевой активности поможет снизить риск и минимизировать воздействие атак на вашу инфраструктуру.

Механизмы ограничения ресурсов: Настройте механизмы ограничения ресурсов на серверах и сетевых устройствах, чтобы предотвратить перегрузку системы. Это может включать ограничение пропускной способности, числа одновременных соединений или ресурсов, выделяемых для каждого соединения.

Использование технологий кэширования: Применение технологий кэширования, например, кэширование статических содержимого или использование прокси-серверов, может снизить нагрузку на серверы и

повысить производительность, что поможет справиться с некоторыми видами атак.

Тестирование отказоустойчивости: Проверка и тестирование отказоустойчивости вашей инфраструктуры помогут выявить узкие места и проблемы, которые могут быть использованы злоумышленниками. Убедитесь, что ваша система способна справиться с повышенной нагрузкой и имеет план аварийного восстановления.

Использование фильтров пакетов: Настройка фильтров пакетов на сетевом оборудовании позволяет блокировать или ограничивать определенные типы трафика, включая трафик, связанный с атаками DoS и DDoS.

Географическое распределение серверов: Распределение серверов по разным географическим регионам может помочь справиться с атаками, направленными на конкретные локации или ресурсы. Это позволяет перенаправлять трафик на другие серверы в случае атаки на один из них.

Обновление безопасности приложений: Постоянно обновляйте и усиливайте безопасность ваших веб-приложений. Это включает в себя регулярное патчирование уязвимостей, использование безопасных библиотек и фреймворков, а также проведение аудита кода на наличие уязвимостей. Обучение пользователей: Обучайте ваших пользователей о безопасности в сети. Это поможет предотвратить социальную инженерию и атаки, основанные на ошибках пользователей, таких как фишинговые письма и вредоносные ссылки.

Сотрудничество с CERT/CSIRT: Сотрудничайте с местной командой реагирования на компьютерные инциденты (CERT) или службой реагирования на компьютерные инциденты в вашей стране (CSIRT), чтобы обмениваться информацией о существующих угрозах и получать рекомендации по защите от атак. Запомните, что комбинация этих мер безопасности и их постоянное обновление являются основой для эффективной защиты от DoS и DDoS атак.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. https://ddos-guard.net/ru/blog/dos-i-ddos-ataki.
2. https://www.reg.ru/blog/dos-vs-ddos-ataka-otlichiya-i-profilaktika/
3. https://powerdmarc.com/ru/dos-vs-ddos-attacks/
4. https://timeweb.com/ru/community/articles/otlichie-dos-atak-ot-ddos-ataki
5. https://blog.ingate.ru/seo-wikipedia/dos-i-ddos/

6. https://docs.mevspace.com/ru/articles/articles-content/dos-and-ddos-attacks
7. https://selectel.ru/blog/ddos-attacks/
8. https://www.iseo.ru/glossary/ddos-ataka/
9. https://eternalhost.net/blog/hosting/dos-i-ddos-ataki