DoS-атаки и методы защиты от них

Выполнила студентка
группы И411
Сурков В. М.

Определение

DoS-атака (*Denial of Service – «отказ в обслуживании»*) и **DDoS-атака** (*Distributed Denial of Service* — «распределённый отказ обслуживания», когда атака производится одновременно с большого количества IP-адресов) — это разновидности атак злоумышленника на компьютерные системы.

Цель атак

Создание условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднён.

Чаще всего это просто блокирование доступа, иногда вывод этого ресурса из строя.

Иногда DoS-атака может являться частью акции, направленной на взлом ресурса.

Типы DoS-атак

1) Атаки типа "SYN-flood"

В основу данного типа атак заложена идея превышения ограничения на количество соединений, находящихся в состоянии установки.

Блокирование каналов связи и маршрутизаторов осуществляется с помощью мощного потока пакетов (flood), полностью забивающего всю ширину канала или входной маршрутизатор и не дающего возможности для прохождения пакетов пользователей.

Результатом является состояние системы, в котором она не может устанавливать новые соединения.

2) **Атаки, использующие ошибки в реализации стека протоколов TCP/IP в операционной системе**

Основной таких атак является генерация последовательности сетевых пакетов, при обработке которой проявляется искомая ошибка реализации.

Как результат можно получить стремящуюся к бесконечности загрузку процессора, захват ядром или приложением всей доступной памяти.

3) Атаки, направленные на переполнение ресурсов операционной системы или приложений

Поскольку каждая система или работающее на ней приложение имеют ограничения по множеству параметров (макс. количество одноврем. соединений, файловых дескрипторов) атакующий пытается заставить программу превысить этот ресурс.

Последствием обычно является неспособность атакуемого сервиса обслужить штатных абонентов, а в идеале – полная неспособность атакуемой системы к сетевой деятельности.

Иногда также подвергается входной маршрутизатор, который бомбардируется маленькими перекрывающимися фрагментами. В результате запросы пользователей не проходят к серверу, расположенному за маршрутизатором, из-за переполнения внутренних ресурсов маршрутизатора.

4) DoS-атаки основанные на протоколе ICMP

Большое количество DoS-атак основывается на протоколе ICMP.

Классическим примером является Smurf – атака, которая используется с целью нанесения финансового вреда конкурентам. Ее единственное назначение - сужение полосы пропускания жертвы.

Сценарий: посылается эхо-запрос с адресом источника, подмененным на адрес жертвы. Следовательно, эхо-ответ уже приходит к компьютеру-жертве. Если, к тому же, эхо-запрос является широковещательным для сети, на него могут отреагировать все компьютеры указанной сети и поток, направленный на жертву, уже становится огромным, приобретая лавинообразный характер.

Обнаружение DoS-атак

Методы обнаружения :

- сигнатурные — основанные на качественном анализе трафика;
- статистические — основанные на количественном анализе трафика;
- гибридные — сочетающие в себе достоинства двух предыдущих методов.

Механизмы защиты от DoS-атак

Меры противодействия DoS-атакам можно разделить на *пассивные и активные*, а также на *превентивные и реакционные*.

Основные методы защиты

- *Предотвращение*. Профилактика причин, побуждающих тех или иных лиц организовывать DoS-атаки.
- *Фильтрация и блэкхолинг*. Эффективность этих методов снижается по мере приближения к цели атаки и повышается по мере приближения к её источнику.
- *Устранение уязвимостей*. Не работает против атак типа *флуд*, для которых «уязвимостью» является конечность тех или иных ресурсов.
- *Наращивание ресурсов*.
- *Рассредоточение*. Построение распределённых и продублированных систем, которые не прекратят обслуживать пользователей даже если некоторые их элементы станут недоступны из-за атаки.
- *Уклонение*. Увод непосредственной цели атаки (доменного имени или IP-адреса) подальше от других ресурсов, которые часто также подвергаются воздействию вместе с непосредственной целью.
- *Активные ответные меры*. Воздействие на источники, организатора или центр управления атакой, как технического, так и организационно-правового характера.

Рекомендации

- Привлечение серьезных технических специалистов и специалистов в области информационной безопасности для наиболее сложных работ (выбор систем защиты, их настройка, информационное сопровождение, анализ статистики при взломе).
- Использование по возможности более широкого канала связи с провайдером.
- Использование "серьезного" провайдера, с хорошими каналами (желательно несколькими), грамотно и быстро отвечающими на запрос о помощи администраторами.
- Использование надежных и эффективных операционных систем на сервере, не прельщаясь графическими интерфейсами, проверенного матобеспечения.
- Использование квалифицированного системного администратора, желательно подчиняющегося службе безопасности.
- Наличие межсетевого экрана достаточной производительности и хорошими техническими характеристиками.

Спасибо за внимание!