DoS Атаки
[Хакерство в Интернете]

Как и было обещано ранее, вот вам маленькое описание DoS атак. Скажу сразу ,что оно (описание) не претендует на полноту и т.д. А поясняет , что есть такое эти самые DoS атаки. Итак: название DoS не как не связано со старенькой мелкософтовской операционной системой, и являестя сокращением от следующей абривиатуры Denied of Service - что в переводе на русский язык звучит как "Отказ от Работы". Как видно из названия , атака предначначена не для получения паролей или еще какой нибуть информации, а направлена на то чтобы завалить,повесить,перезагрузить сервер. Вы конечно спросите а на №;% это надо ? Отвечу пригодица ! Данный вид атак используется (а примеру) в войнах на IRC, а так же для нанесения материального урона той или иной организации. Представьте на пример сколько баксов потеряет какая нибуть крупная компания, чья работа связана непосредственно с интернет, если ее сервер будет находится в "дауне" пол дня.

Продолжим. Все DoS атаки можно разделить на 2 основные группы:
1) DoS атаки связанные с ошибками в протоколах связи.
2) DoS атаки связанные с ошибками в программном обеспечении (web,ftp,smtp сервера).

DoS атаки связанные с ошибками в протоколах, мелее распространены, но наиолее опасны т.к. применение такого рода атак часто влечет за собой отказ от работы не одного сервера, а подсети (а иногда и не одной).

К примеру: не помню как называется атака, суть заключалась в следующем:
На сервер посылался пакет для установки соединения, с обратным адрессом самого сервера. Что приводило в зарасанию или тому подобному.
Таких рода атак насчитывается в данное время большое количество, но в основном такие атаки эффективны не большое количество времени, после ее обнаружения.

Второй же вид атак связанный с ошибками в программном обеспечении , наиболее распространен, связан он с так называемым переполнением буфера.

К примеру: какой нибуть ftp сервер, просит вас ввести свое имя для входа в систему, а вы ему на этот запрос посылаете строку длиной этак в 8000 символов. Результат ftp сервер падает.
Такие атаки наиболее распостранены, и находят их в программном обеспечении очень часто.

Так-же необходино упамянуть о распределенных DoS атаках. Для реализации такой атаки необходимо организовать определенную скорость (кол-во пакетов/муниту) посылки пакетов. Ну к примеру все наверное знают программку voidozer - против 9х Форточек. Но не кому не удавалось завалить машину друга через модем . Так вот сейчас я вам раскажу один приемчик. Эта атака основана на том , что форточки при определенной скорости приходящих пакетов PING не успевает, обрабатывать их и посылать пакеты, и тачка в форточками вешается. При использовании voidozera в локальной 10 мегабитной сетке , компы слетают как листья в дерева в осенний период. А реализовать на модеме эту фишку не удается по простой причине , необходимо как уже сказано обеспецить большую скорость передачи, даже если вы имеете соединени со скоростью 56К врядле вы завалите человера на 33.6К. Что же делать спросите вы . Да все очень просто , атаковать с нескольких модемов,шеллов одновременно.

Ну только прикиньте сидит человек на 33.6К. а вы его со своего 14.4+5 друзей 56к+еще с 2 шелов с каналом Т1. Во веселуха !

Между прочим так называемый flood на IRC , тоже можно использовать в целях убийства (отправление далеко и надолго) людей сидящих на канале.Но это уже история для другой статьи.

Кудинов Олег