DDoS атака – борьба в FreeBSD

Кажется, началось. Что делать?

Перед непосредственным началом атаки боты “разогреваются”, постепенно
наращивая поток пакетов на атакуемую машину. Важно поймать момент и начать
активные действия. Поможет в этом постоянное наблюдение за маршрутизатором,
подключенным к внешней сети (анализ графиков NetFlow). На сервере-жертве
определить начало атаки можно подручными средствами.

Наличие SYN-флуда устанавливается легко – через подсчет числа “полуоткрытых”
TCP-соединений:

```
# netstat -na | grep ".80\ " | grep SYN_RCVD
```

В обычной ситуации их не должно быть совсем (или очень небольшое количество:
максимум 1-3). Если это не так – ты атакован, срочно переходи к дропанью
атакующих.

С HTTP-флудом несколько сложнее. Для начала нужно подсчитать количество
процессов Apache и количество коннектов на 80-ый порт (HTTP-флуд):

```
# ps aux | grep httpd | wc -l
# netstat -na | grep ".80\ " | wc -l
```

Значения, в несколько раз превышающие среднестатистические, дают основания
задуматься. Далее следует просмотреть список IP-адресов, с которых идут запросы

на подключение:

```
# netstat -na | grep ".80\ " | sort | uniq -c | sort -nr | less
```

Однозначно идентифицировать DoS-атаку нельзя, можно лишь подтвердить свои
догадки о наличии таковой, если один адрес повторяется в списке слишком много
раз (да и то, это может говорить о посетителях, сидящих за NAT’ом).
Дополнительным подтверждением будет анализ пакетов с помощью tcpdump:

```
# tcpdump -n -i eth0 -s 0 -w output.txt dst port 80 and host IP-сервера
```

Показателем служит большой поток однообразных (и не содержащих полезной
информации) пакетов от разных IP, направленных на один порт/сервис (например,
корень web-сервера или определенный cgi-скрипт).

Окончательно определившись, начинаем дропать неугодных по IP-адресам (будет
гораздо больше эффекта, если ты сделаешь это на маршрутизаторе):

```
# iptables -A INPUT -s xxx.xxx.xxx.xxx -p tcp --destination-port http -j
DROP
```

Или сразу по подсетям:

```
# iptables -A INPUT -s xxx.xxx.0.0/16 -p tcp --destination-port http -j
DROP
```

Это даст тебе некоторую фору (совсем маленькую; зачастую IP-адрес источника
спуфится), которую ты должен использовать для того, чтобы

обратиться к
провайдеру/хостеру (с приложенными к сообщению логами web-сервера, ядра,
брандмауэра и списком выявленных тобой IP-адресов). Большинство из них, конечно,
проигнорируют это сообщение (а хостинги с оплатой трафика еще и порадуются –
DoS-атака принесет им прибыль) или просто отключат твой сервер. Но в любом
случае это следует сделать обязательно, – эффективная защита от DDoS возможна
только на магистральных каналах. В одиночку ты справишься с мелкими нападками,
направленными на истощение ресурсов сервера, но окажешься беззащитным перед
более-менее серьезным DDoS’ом.

Борьба с DDoS во FreeBSD

Уменьшаем время ожидания ответного пакета на запрос SYN-ACK (защита от
SYN-флуда):

```
# sysctl net.inet.tcp.msl=7500
```

Превращаем сервер в черную дыру. Так ядро не будет слать ответные пакеты при
попытке подключиться к незанятым портам (снижает нагрузку на машину во время
DDoS’а на случайные порты):

```
# sysctl net.inet.tcp.blackhole=2
# sysctl net.inet.udp.blackhole=1
```

Ограничиваем число ответов на ICMP-сообщения 50-ю в секунду (защита от
ICMP-флуда):

```
# sysctl net.inet.icmp.icmplim=50
```

Увеличиваем максимальное количество подключений к серверу (защита от всех
видов DDoS):

```
# sysctl kern.ipc.somaxconn=32768
```

Включаем DEVICE_POLLING – самостоятельный опрос сетевого драйвера ядром на
высоких нагрузках (существенно снижает нагрузку на систему во время DDoS’a):

Пересобираем ядро с опцией "options DEVICE_POLLING";
Активируем механизм поллинга: "sysctl kern.polling.enable=1";
Добавляем запись "kern.polling.enable=1" в /etc/sysctl.conf.

Наивный Internet

Во времена своего рассвета DoS-атаки были настоящей катастрофой для серверов
и обычных рабочих станций. Web-сайт можно было легко завалить с помощью
одного-единственного хоста, реализующего атаку типа Smurf. Рабочие станции с
установленной ОС Windows падали, как доминошки, от атак типа Ping of Death, Land,
WinNuke. Сегодня всего этого не стоит опасаться.