Автор: Administrator
19.03.10 14:19 - Последнее обновление 19.03.10 14:23

DDOS - что делать. Если сервер только один - Linux с Apache.

Сейчас перейдем к более практическим занятиям и посмотрим, каким образом можно защитить сервер от DDOS.
В качестве сервера будет взят обычный компьютер с x86 архитектурой и ОС Linux и веб-сервером apache.
Почему не FreeBSD? *На FreeBSD, насколько мне известно, аналога модуля iptables string нет* .
Почему не nginx или lighttpd? *Эти веб-сервера будут рассмотрены в следующих заметках. В этой заметке nginx выступает как фронтенд, а не как основной*
.

Важно знать! Для работы модуля iptables string, iptables должен быть не ниже версии 1.3.5, а ядро – не ниже 2.6.18, собранным с опцией CONFIG_NETFILTER_XT_MATCH_STRING=m

Рекомендую! ***Эти эти примеры помогут сохранить веб-сервер атак:***
Лимит на 20 запросов в секунду для интерфейса eth0
iptables --new-chain car
iptables --insert OUTPUT 1 -p tcp --destination-port 80 -o eth0 --jump car
iptables --append car -m limit --limit 20/sec --jump RETURN
iptables --append car --jump DROP
Максимум 10 одновременных соединений с одного IP
iptables -A INPUT-p tcp --dport 80 -m iplimit --iplimit-above 10 -j REJECT
Блокировка более 10 SYN
iptables -I INPUT -p tcp --syn --dport 80 -j DROP -m iplimit --iplimit-above 10
20 соединений на сеть класса C
iptables -p tcp --dport 80 -m iplimit --iplimit-above 20 --iplimit-mask 24 -j REJECT

Если на сервере предоставлен хостинг для множества сайтов

Наша задача - спасти все остальные сайты, потому что то все сайты, которые размещены на общем IP адресе с жертвой, будут недоступны.
Почему? *На этот вопрос даст ответ алгоритм атаки ботнета:*

- бот получает от координатора домен-жертву
- бот производит преобразование домена в IP
- бот отсылает по данному IP запрос "GET / HTTP/1.0" на веб-сервер жертвы

Как только замечены симптомы DDOS атаки, проверьте access_log веб-сервера apache. Если он забит записями вида "GET / HTTP/1.0", то это значит, что атака идет на IP адрес.
Что делать? Прежде всего временно отключите атакуемый IP адрес, лучше всего через iptables, командой iptables -A FORWARD -p tcp -s <атакуемый IP> --dport 80 -j REJECT. Это даст хоть какой-то шанс, что ботнет не успеет забить весь канал к серверу, после чего связь с ним будет потеряна. После отключения атакуемого домена доступ можно будет открыть обратно.
Для поиска атакуемого домена необходимо, чтоб его NS сервера находились на вашем сервере!
Почему? Так как атака идет по IP адресу, то единственным способом нахождения домена-жертвы может быть только анализ запросов к dns.
Как? С помощью утилиты ngrep. Эта утилита позволяет применить регулярные выражения к трафику. В нашем случае команда будет ngrep port 53. На 53 порт идут запросы на преобразование домена в IP. В течении нескольких десятков секунд визуально можно будет определить домен-жертву.
Другой вариант – настроить bind на запись всех запросов в лог и проверить, какой домен чаще всех запрашивается.
Следующее действие – это отключение домена. Наиболее простым и действенным методом будет блокировка запросов с именем домена. Это запретит преобразование домена, и боты не смогут получить IP домена-жертвы. Снова iptables поможет сделать это:
iptables -I INPUT 1 -p tcp --dport 53 -m string --string "domain.com" --algo kmp -j DROP
iptables -I INPUT 2 -p udp --dport 53 -m string --string "domain.com" --algo kmp -j DROP
Обратите внимание – блокируются TCP и UDP порты.
Другой вариант – вписать для домена-жертвы IP 127.0.0.1 и подождать пока запись разойдется, это зависит от настроек TTL, обычно 15 минут.
После отключения атакуемого домена все остальные сайты будут работать нормально.

Если на сервере предоставлен хостинг только для одного сайта (dedicated или vps хостинг)

Задача меняется – цель уже известна, а вот методы нужны иные. Цель защиты от DDOS на сайт – сохранить его работоспособность.
Проявите сразу заботу о защите своего сайта. Сделайте главную страницу сайта вида
http://hostinghelp.biz/node
с редиректом на нее при запросе вида
http://hostinghelp.biz/

Почему? *Это поможет защитить главную страницу сайта, отфильтровав все запросы от ботнета, так как боты не выполняют заход при редиректе и будут продолжать упорно долбить "GET / HTTP/1.0"*

Как? *Лучше всего поставить перед веб-сервером apache быстрый и легкий nginx и отдавать им статичные файлы. Создать статичный файл index.html в котором написать о том, что будет сделан переход на другую страницу и установите редирект с помощью метатега html.*

Когда начнется DDOS атака, то nginx сможет выдержать намного больше запросов к статичному файлу по сравнению с apache.

Если nginx не помогает, и сервер не выдерживает столько запросов - забивается канал, то на помощь нам снова приходит iptables.

Так как главная страница сайта известна посетителям и поисковым системам, то можно просто заблокировать страницу-редирект, и тем самым сделав недоступным сайт для запросов вида "GET / HTTP/1.0", оставить его работоспособным по всем остальным.

Как? iptables -I INPUT 1 -p tcp --dport 80 -m string --string "GET / HTTP/1.0" --algo kmp -j DROP

Таким образом сайт защищен от DDOS атаки и сохраняет работоспособность, пусть и ценой временного отключения страницы редиректа

В следующей заметке я расскажу о том, как защищать сайт от серьезных атак (более 100Mbit) с помощью нескольких серверов и фильтрации трафика

{jcomments on}