Методи боротьби з DoS/DDoS атаками

Виконав: ст. гр. СН-41
Симчак В. С.

Історія

Вперше термін DoS-атака з'явився в 1996 році, проте до широких мас цей тип дійшов лише в 1999році, коли один за іншим попадали web-сайти Amazon, Yahoo, CNN і eBay.

DoS-атаки

Локальні

1) експлойти
2) форк-бомби
3) циклічні програми

Віддалені

1) віддалена експл. помилок
2) Flood

1. Icmp-флуд.

Дуже примітивний метод забивання смуги пропускання і створення навантажень на мережевий стек через монотонну посилку запитів ICMP ECHO (пінг). Легко виявляється за допомогою аналізу потоків трафіку в обидві сторони: під час атаки типа Icmp-флуд вони практично ідентичні. Майже безболісний спосіб абсолютного захисту заснований на відключенні відповідей на запити ICMP ECHO:

```
# sysctl net.ipv4.icmp_echo_ignore_all=1
```

Або за допомогою брандмаузера:

```
# iptables -A INPUT -p icmp -j DROP --icmp-type 8
```

2. SYN-флуд.

Один з поширених способів не лише забити канал зв'язку, але і ввести мережевий стек операційної системи в такий стан, коли він вже не зможе приймати нові запити на підключення. Заснований на спробі ініціалізації великого числа одночасних TCP-з'єднань через посилку SYN-пакету з неіснуючою зворотньою адресою.

Оборонні заходи зазвичай включають:

Збільшення черги "напіввідкритих" tcp-з'єднань:

```
# sysctl -w net.ipv4.tcp_max_syn_backlog=1024
```

Зменшення часу утримання "напіввідкритих" з'єднань:

```
# sysctl -w net.ipv4.tcp_synack_retries=1
```

Включення механізму TCP syncookies:

```
# sysctl -w net.ipv4.tcp_syncookies=1
```

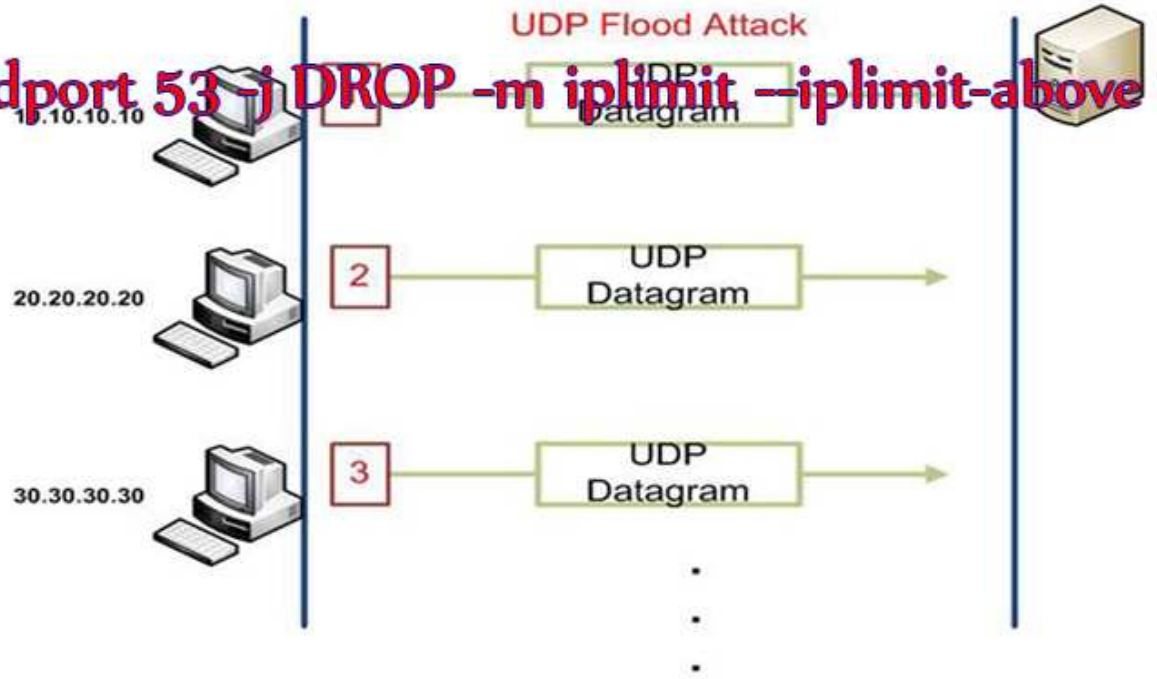
Обмеження максимального числа "напіввідкритих" з'єднань з одного IP до конкретного порту:

```
# iptables -i INPUT -p tcp --syn --dport 80 -m iplimit --iplimit-above  10 -j DROP
```

3. UDP-флуд.

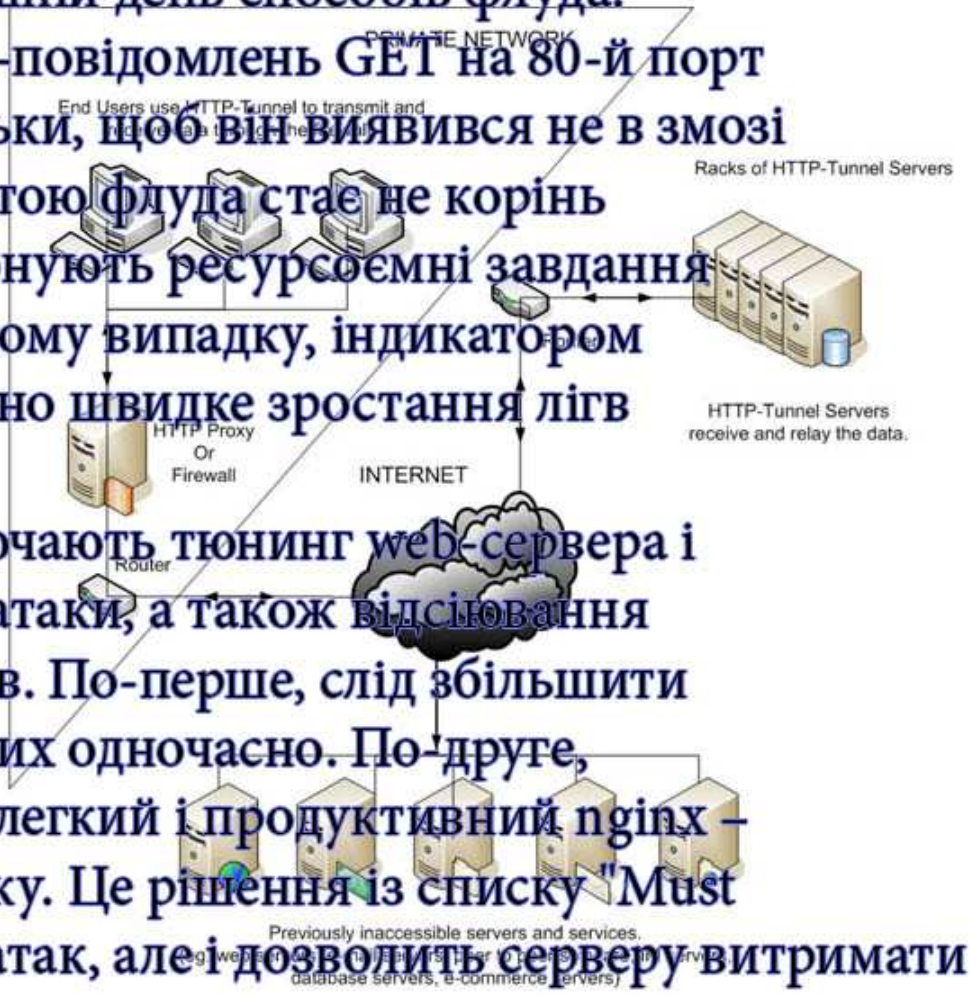
Типовий метод захаращення смуги пропускання. Заснований на безконечній посилці udp-пакетів на порти різних udp-сервісів. Легко усувається за рахунок відрізання таких сервісів від зовнішнього світу і установки ліміту на кількість з'єднань в одиницю часу до dns-сервера на стороні шлюзу:

```
# iptables -i INPUT -p udp --dport 53 -j DROP -m iplimit --iplimit-above 1
```



4. HTTP-флуд.

Один з найпоширеніших на сьогоднішній день способів флуда. Заснований на безконечній посилці http-повідомлень GET на 80-й порт з метою завантажити web-сервер настільки, щоб він виявився не в змозі обробляти всі останні запити. Часто метою флуда стає не корінь web-сервера, а один із скриптів, що виконують ресурсоємні завдання або що працює з базою даних. У будь-якому випадку, індикатором атаки, що почалася, служитиме аномально швидке зростання лігв web-сервера.



Методи боротьби з Http-флудом включають тюнинг web-сервера і бази даних з метою понизити ефект від атаки, а також відсіювання DoS-ботів за допомогою різних прийомів. По-перше, слід збільшити максимальне число з'єднань до бази даних одночасно. По-друге, встановити перед web-сервером Apache легкий і продуктивний nginx – він кешуватиме запити і видавати статику. Це рішення із списку "Must have", яке не лише понизить ефект DoS-атак, але і дозволить серверу витримати величезні нагрузки.

```
# vi /etc/nginx/nginx.conf
# Збільшує максимальну кількість використовуваних файлів worker_rlimit_nofile 80000;
events {
# Збільшує максимальну кількість з'єднань
worker_connections 65536;
# Використовувати ефективний метод метод epoll для обробки з'єднань
use epoll;
}
http {
gzip off;
# Відключаєм таймаут на закриття keep-alive з'єднань
keepalive_timeout 0;
# Не віддавати версію nginx в заголовку відповіді
server_tokens off;
# Зкидати з'єднання по таймауту
reset_timedout_connection on;
}
# Стандартні настройки для роботи в якості проксі
server {
listen 111.111.111.111 default deferred;
server_name host.com www.host.com;
log_format IP $remote_addr;
location / {
proxy_pass http://127.0.0.1/;
}
location ~* \.(jpeg|jpg|gif|png|css|js|pdf|txt|tar)$ {
root /home/www/host.com/httpdocs;
}}
```

Універсальні поради

Щоб не попасти в безвихідь під час обвалення DDoS-штурму на системи, необхідно ретельно підготувати їх до такої ситуації:

1. Всі сервера, що мають прямий доступ в зовнішню мережу, мають бути підготовлені до простої і швидкої віддаленої. Великим плюсом буде наявність другого, адміністративного, мережевого інтерфейсу, через який можна дістати доступ до сервера в разі затурканості основного каналу.
2. ПЗ, використовуване на сервері, завжди повинно знаходитися в актуальному стані. Всі дірки - пропатчені, оновлення встановлені. Це захистить тебе від DoS-атак, експлуатуючих баги в сервісах.
3. Всі слухаючі мережеві сервіси, призначені для адміністративного використання, мають бути заховані брандмаузером від всіх, хто не повинен мати до них доступу. Тоді той, що атакує не зможе використовувати їх для проведення DoS-атаки або брутфорса.
4. На підходах до сервера (найближчому маршрутизаторі) має бути встановлена система аналізу трафіку (Netflow в допомогу), яка дозволить своєчасно дізнатися про атаку, що починається, і вчасно прийняти заходи по її запобіганню.

Додай в /etc/sysctl.conf наступні рядки:

```
# vi /etc/sysctl.conf
# Захист від спуфінга
net.ipv4.conf.default.rp_filter = 1
# Перевіряти TCP-з'єднання кожну хвилину. Якщо на іншій стороні - легальна машина, вона зразу відповість. Значення по замовчуванні - 2 години.
net.ipv4.tcp_keepalive_time = 60
# Повторити попитку через десять секунд
net.ipv4.tcp_keepalive_intvl = 10
# Кількість повірок перед закриттям з'єднання
net.ipv4.tcp_keepalive_probes = 5
```

Боротьба з DDoS в FREEBSD

Зменшуємо час чекання у відповідь пакету на запит SYN-ACK (захист від Syn-флуда):

sysctl net.inet.tcp.msl=7500

Перетворюємо сервер на чорну діру. Так ядро не слатиме у відповідь пакети при спробі підключитися до незайнятих портів (знижує навантаження на машину під час DDoS'а на випадкові порти):

sysctl net.inet.tcp.blackhole=2

sysctl net.inet.udp.blackhole=1

Обмежуємо число відповідей на icmp-повідомлення 50 в секунду (захист від Icmp-флуда):

sysctl net.inet.icmp.icmplim=50

Збільшуємо максимальну кількість підключень до сервера (захист від всіх видів DDoS):

sysctl kern.ipc.somaxconn=32768

Включаємо Device_polling - самостійний опит мережевого драйвера ядром на високих навантаженнях (істотно знижує навантаження на систему під час DDoS'а):

- Збираємо заново ядро з опцією "options Device_polling";
- Активуємо механізм полінгу: "sysctl kern.polling.enable=1";
- Додаємо запис "kern.polling.enable=1" у /etc/sysctl.conf.

Слід в історії:

1997 рік - dDoS-атака на web-сайт Microsoft. Один день мовчання.

1999 рік – "поза зоною дії" виявилися web-сайти Yahoo, CNN, ebay і ін.

Жовтень 2002 - атака на кореневі dns-сервері інтернету.
На деякий час були виведені з буд 7 з 13 серверів.

21 лютого 2003 року - dDoS-напад на Livejournal.com. Два дні сервіс знаходився в паралізованому стані, лише інколи подаючи ознаки життя.