Лабораторна робота 5

Тема: Виявлення та захист від DOS/DDOS атак

Мета: Вивчити принципи мережевих атак типу DOS/DDOS, їх виявлення, вплив та принципи захисту

1. Теоретичні відомості

Для корпоративних інформаційних систем (КІС) важливим є захист так званого периметру комп'ютерної мережі. Основною загрозою є DOS / DDOS атаки, метою яких є зробити недоступними сервіси КІС.

DOS (Denial of Service) — відмова в обслуговуванні.

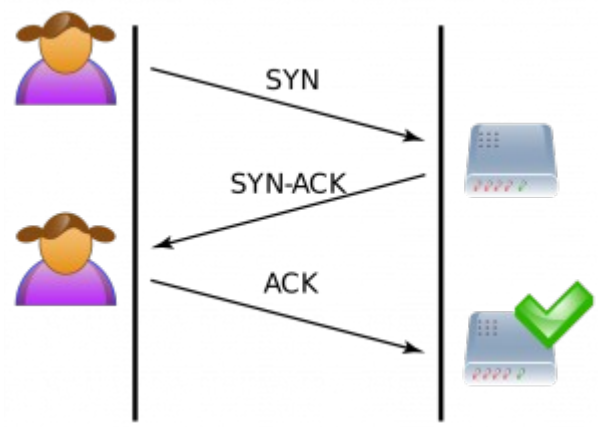
DDOS (Distributed Denial of Service) - розподілена відмова в обслуговуванні.

Відмінність між DOS та DDOS полягає в тому, що під час DoS атаки запускається атака з одного Інтернет з’єднання, а при DDoS атаках використовується трафік із кількох джерел, розподілених через Інтернет. Для того, щоб виконати захист комп’ютерної мережі КІС від такого роду атак слід вивчити можливості та характеристики інструментів їх здійснення.

DOS атаки можна розділити на дві основні категорії: атаки на прикладному рівні та атаки на мережевому рівні. DOS атаки спрямовані на транспортний і мережевий рівні зазвичай складаються із об’ємних атак, спрямованих на перевантаження цільової машини трафіком і споживання всіх ресурсів, а також зупинку сервера.

TCP SYN Flood

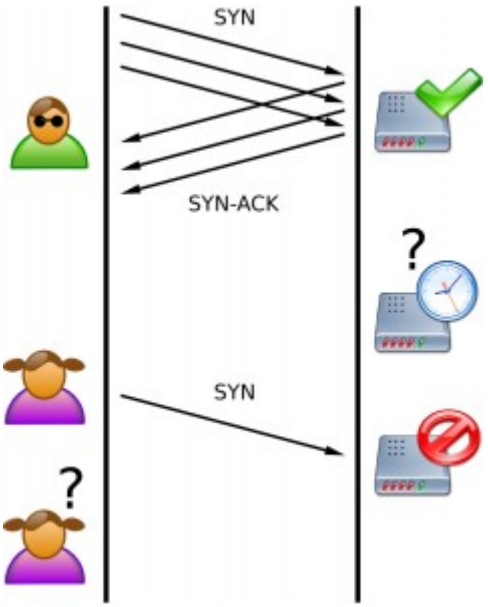
SYN Flood працює на транспортному рівні. З'єднання TCP встановлюється шляхом тристороннього рукостискання. Клієнт надсилає пакет SYN, щоб ініціювати з’єднання TCP. На сервері пакет SYN, що надійшов, передає «з’єднання» в стан SYN-RCVD. Після цього сервер відповідає SYN+ACK. Нарешті, клієнт відповідає на це ACK. Після цих 3 кроків TCP-з’єднання вважається встановленим.



Однак, якщо пакет ACK не досягає сервера, то він буде залишатиметься в стані SYN-RCVD для цього з’єднання та продовжуватиме очікувати ACK деякий час. Атаки SYN flood використовують цю поведінку сервера. Тому, метою SYN flood є надсилання великої кількості SYN-пакетів на сервер та ігнорування SYN+ACK пакетів, повернутих сервером. Це

змушує сервер використовувати свої ресурси (пул динамічних портів) протягом налаштованого періоду часу для очікування надходження пакетів ACK.

Якщо надіслати достатньо велику кількість SYN пакетів, то це перевантажить сервер, оскільки сервери обмежені в кількості одночасних TCP-з’єднань. Якщо сервер досягає свого ліміту, він не зможе встановити нові TCP-з’єднання, доки існуючі з’єднання, які перебувають у стані SYN-RCVD, перебувають у стані очікування.



Одним із інструментів для виконання TCP SYN Flood атак є hping3. В операційній системі Linux цей інструмент встановлюється із звичайний спосіб із його репозиторію. Формат використання після інсталяції має наступний вигляд:

```
~# hping3 -S --flood -V -p TARGET_PORT TARGET_SITE
```

Наприклад:

```
linuxhint@LinuxHint:~$ sudo hping3 -S --flood -V -p 80 170.155.9.185
using wlp3s0, addr: 192.168.0.103, MTU: 1500
HPING 170.155.9.185 (wlp3s0 170.155.9.185): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

де sudo — вказує на необхідні привілеї для запуску hping3;
hping3 — викликає програму hping3;
-S — визначає пакети SYN;
-flood — відповіді ігноруватимуться, а пакети надсилатимуться якомога швидше;
-V — багатослівність;
-p 80 — порт 80, на який виконується атака (може бути замінений для іншого сервісу);
170.155.9.185 — цільова IP адреса.

Також існують інші ключі та параметри, призначення яких можна дізнатись із довідки до hping3.

UDP Flood

Транспортному протоколу UDP не потрібно створювати сеанс між двома пристроями, у нього процес “рукостискання” відсутній. Тому UDP Flood не використовує вразливості, а його метою є створення та надсилання великої кількості дейтаграм UDP із підроблених IP адрес на цільовий сервер. Коли сервер отримує цей тип трафіку, він не може обробити кожен запит і використовує свою пропускну здатність, надсилаючи пакети ICMP із вмістом «адресат недоступний». Для створення UDP Flood також може використовуватись hping3:

```
~# hping3 --flood --rand-source --udp -p TARGET_PORT TARGET_IP
```

де - - flood — пакети надсилаються якомога швидше;
- - rand-source — випадкова адреса джерела;
- - udp - режим UDP;
-p TARGET_PORT - порт призначення (за замовчуванням 0)

Практичне завдання

1. Встановіть операційну систему для виконання атак на віртуальну машину.
2. Встановіть Web сервер, наприклад, http Apache. Та запустіть його. Перевірте, що сервер відповідає на запит на порт http.
3. Запустіть атаку TCP SYN Flood атаку на порт http цього серверу. Під час атаки перевірте чи дійсно Web-сервер перестає відповідати.
4. За допомогою команди **netstat v** визначте як займаються порти на боці Web-серверу до та під час атаки.
5. За допомогою програми Wireshark або tcpdump визначте типовий вміст пакету TCP SYN Flood.
6. Встановіть на віртуальній машині, що забезпечує сервіс Web-серверу, програму firewall та задайте на ній правило, що забороняє приймати запити з IP адресою вузла, з якого виконується атака.
7. Повторіть пункти 3 та 4.
8. Відмініть встановлене в п.6 правило та повторіть пп.3-7 для UDP Flood атаки.
9. Підготуйте звіт, до якого додайте скріншоти та коментарії до них. Зробіть висновки.