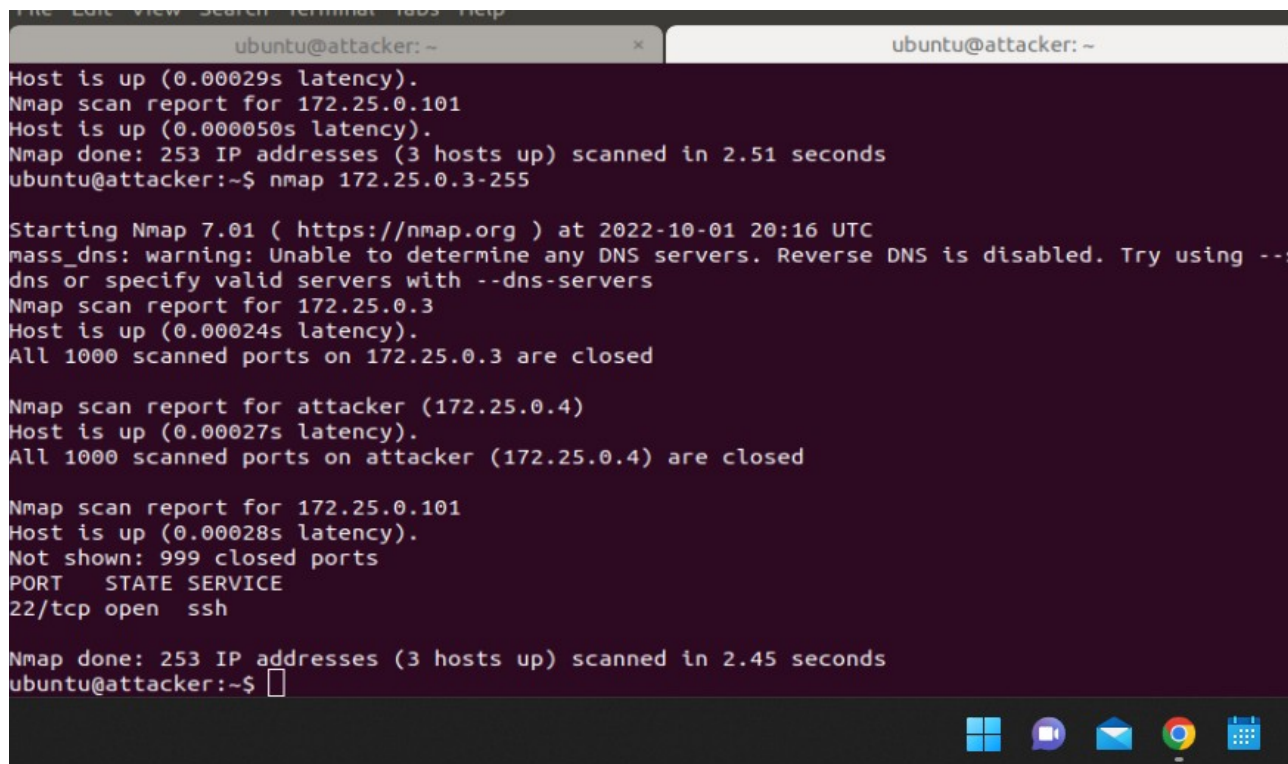


- This is an individual assignment and worth 20 points.
- The due date is **Saturday, October 1, midnight**.
- Please zoom in on the outputs.
- Use the accompanying output document to report your results.
- Follow the naming convention.
- **YOU ARE NOT ALLOWED TO DO THIS DURING THE CLASS.**

Homework 3: Attacks on TCP/IP

Task 1. Performing a Ping Sweeping



```
The Edit View Search Terminal Tabs Help
ubuntu@attacker: ~
Host is up (0.00029s latency).
Nmap scan report for 172.25.0.101
Host is up (0.000050s latency).
Nmap done: 253 IP addresses (3 hosts up) scanned in 2.51 seconds
ubuntu@attacker:~$ nmap 172.25.0.3-255

Starting Nmap 7.01 ( https://nmap.org ) at 2022-10-01 20:16 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --dns or specify valid servers with --dns-servers
Nmap scan report for 172.25.0.3
Host is up (0.00024s latency).
All 1000 scanned ports on 172.25.0.3 are closed

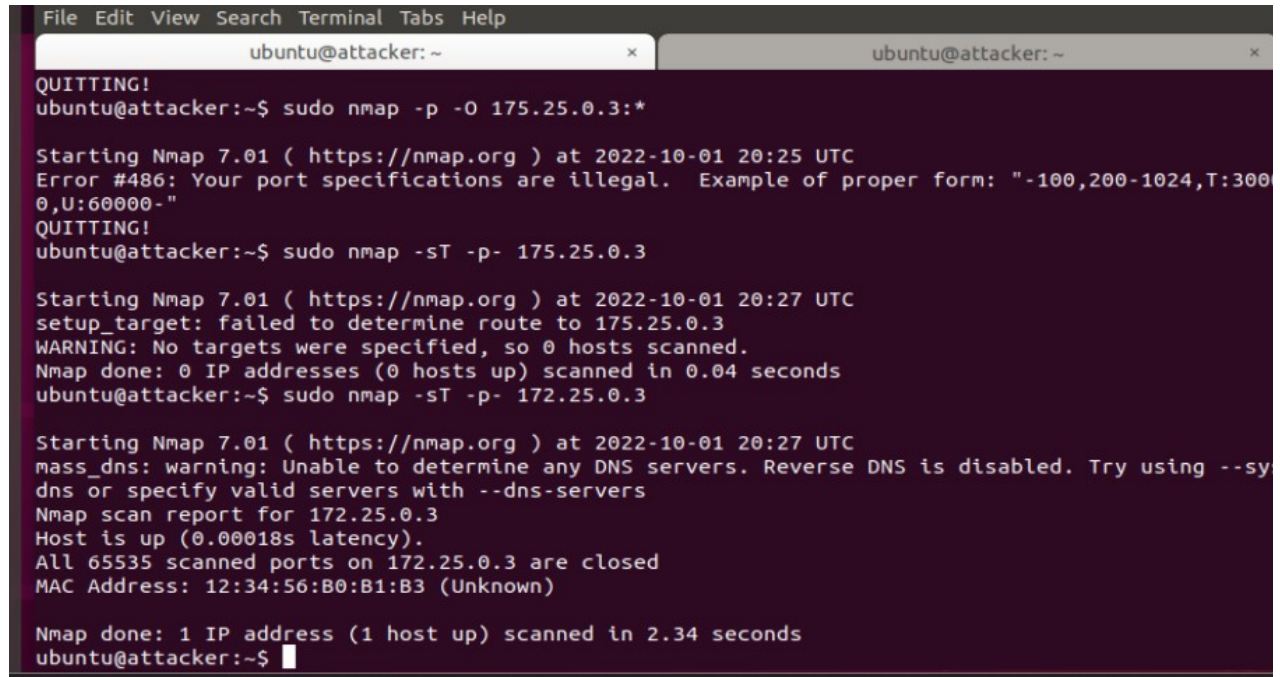
Nmap scan report for attacker (172.25.0.4)
Host is up (0.00027s latency).
All 1000 scanned ports on attacker (172.25.0.4) are closed

Nmap scan report for 172.25.0.101
Host is up (0.00028s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 253 IP addresses (3 hosts up) scanned in 2.45 seconds
ubuntu@attacker:~$
```

Task 2. Performing a Port Scanning

.



```
File Edit View Search Terminal Tabs Help
ubuntu@attacker: ~
QUITTING!
ubuntu@attacker:~$ sudo nmap -p -O 175.25.0.3:*

Starting Nmap 7.01 ( https://nmap.org ) at 2022-10-01 20:25 UTC
Error #486: Your port specifications are illegal. Example of proper form: "-100,200-1024,T:3000,U:60000-"
QUITTING!
ubuntu@attacker:~$ sudo nmap -sT -p- 175.25.0.3

Starting Nmap 7.01 ( https://nmap.org ) at 2022-10-01 20:27 UTC
setup_target: failed to determine route to 175.25.0.3
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds
ubuntu@attacker:~$ sudo nmap -sT -p- 172.25.0.3

Starting Nmap 7.01 ( https://nmap.org ) at 2022-10-01 20:27 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --syn
dns or specify valid servers with --dns-servers
Nmap scan report for 172.25.0.3
Host is up (0.00018s latency).
All 65535 scanned ports on 172.25.0.3 are closed
MAC Address: 12:34:56:B0:B1:B3 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.34 seconds
ubuntu@attacker:~$
```

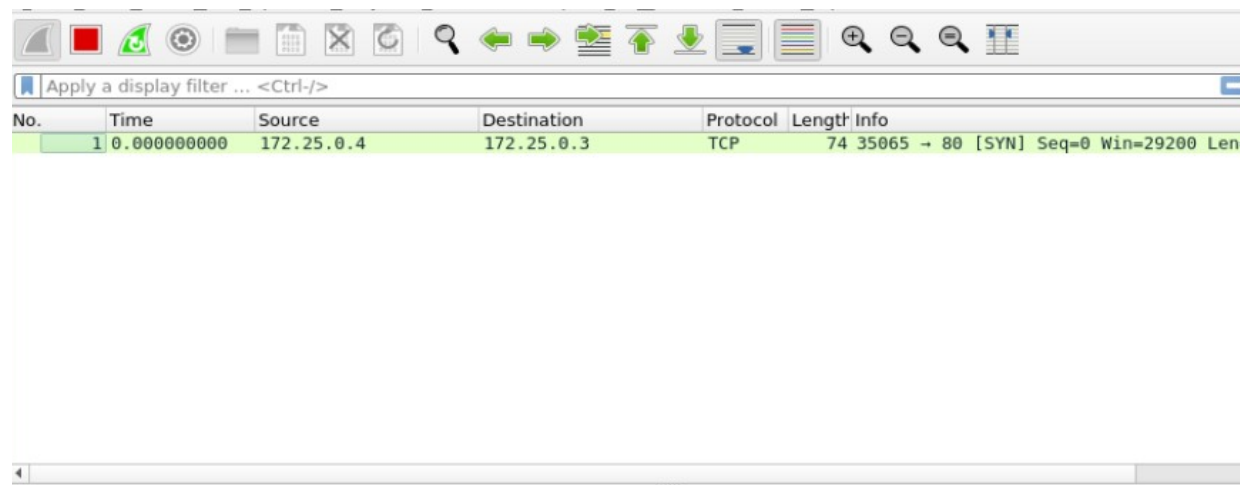
Task 3. Complete Task 1 of the Labtainer tcpip (SYN flooding attack)

```

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
TCP connection attempts: 20 | Successful connections: 0 | Failed: 20 (100.00%)
Nping done: 1 IP address pinged in 19.03 seconds
ubuntu@attacker:~$ nping -c 20 --source-ip 192.168.10.10 172.25.0.3

Starting Nping 0.7.01 ( https://nmap.org/nping ) at 2022-10-01 20:59 UTC
libnsock mksock_bind_addr(): Bind to 192.168.10.10:0 failed (IOD #1): Cannot assign requested address (99)
SENT (0.0060s) Starting TCP Handshake > 172.25.0.3:80
RECV (0.0061s) Possible TCP RST received from 172.25.0.3:80 --> Connection refused
libnsock mksock_bind_addr(): Bind to 192.168.10.10:0 failed (IOD #2): Cannot assign requested address (99)
SENT (1.0078s) Starting TCP Handshake > 172.25.0.3:80
RECV (1.0078s) Possible TCP RST received from 172.25.0.3:80 --> Connection refused
libnsock mksock_bind_addr(): Bind to 192.168.10.10:0 failed (IOD #3): Cannot assign requested address (99)
SENT (2.0091s) Starting TCP Handshake > 172.25.0.3:80
RECV (2.0091s) Possible TCP RST received from 172.25.0.3:80 --> Connection refused
libnsock mksock_bind_addr(): Bind to 192.168.10.10:0 failed (IOD #4): Cannot assign requested address (99)
SENT (3.0102s) Starting TCP Handshake > 172.25.0.3:80
RECV (3.0102s) Possible TCP RST received from 172.25.0.3:80 --> Connection refused
libnsock mksock_bind_addr(): Bind to 192.168.10.10:0 failed (IOD #5): Cannot assign requested address (99)
SENT (4.0115s) Starting TCP Handshake > 172.25.0.3:80
RECV (4.0115s) Possible TCP RST received from 172.25.0.3:80 --> Connection refused
libnsock mksock_bind_addr(): Bind to 192.168.10.10:0 failed (IOD #6): Cannot assign requested address (99)
SENT (5.0127s) Starting TCP Handshake > 172.25.0.3:80
RECV (5.0127s) Possible TCP RST received from 172.25.0.3:80 --> Connection refused
libnsock mksock_bind_addr(): Bind to 192.168.10.10:0 failed (IOD #7): Cannot assign requested address (99)
SENT (6.0143s) Starting TCP Handshake > 172.25.0.3:80
RECV (6.0143s) Possible TCP RST received from 172.25.0.3:80 --> Connection refused
libnsock mksock_bind_addr(): Bind to 192.168.10.10:0 failed (IOD #8): Cannot assign requested address (99)
SENT (7.0154s) Starting TCP Handshake > 172.25.0.3:80
RECV (7.0154s) Possible TCP RST received from 172.25.0.3:80 --> Connection refused
libnsock mksock_bind_addr(): Bind to 192.168.10.10:0 failed (IOD #9): Cannot assign requested address (99)
SENT (8.0171s) Starting TCP Handshake > 172.25.0.3:80
RECV (8.0171s) Possible TCP RST received from 172.25.0.3:80 --> Connection refused
libnsock mksock_bind_addr(): Bind to 192.168.10.10:0 failed (IOD #10): Cannot assign requested address (99)
SENT (9.0189s) Starting TCP Handshake > 172.25.0.3:80
RECV (9.0189s) Possible TCP RST received from 172.25.0.3:80 --> Connection refused

```



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.25.0.4	172.25.0.3	TCP	74	35065 → 80 [SYN] Seq=0 Win=29200 Len=0

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

```
ntu@router:~$  
  
admin@server:~$ wireshark  
libl error: failed to open /dev/dri/card0: Permission denied  
libl error: failed to open /dev/dri/card0: Permission denied  
libl error: failed to load driver: vmwgfx  
admin@server:~$ telnet  
-bash: telnet: command not found  
admin@server:~$ ifconfig -a  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 172.25.0.2 netmask 255.255.255.0 broadcast 172.25.0.255  
    ether 02:42:ac:19:00:02 txqueuelen 0 (Ethernet)  
    RX packets 2082 bytes 92743 (92.7 KB)  
    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  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 20 bytes 1000 (1000.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 20 bytes 1000 (1000.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
admin@server:~$  
  
ubuntu@attacker:~$  
  
File Edit View Search Terminal Tabs Help  
ubuntu@client:~$  
lo Link encap:Local Loopback  
    inet addr:127.0.0.1 Mask:255.0.0.0  
    UP LOOPBACK RUNNING MTU:65536 Metric:1  
    RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
    TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
    collisions:0 txqueuelen:1000  
    RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)  
  
ubuntu@client:~$ ip addr  
-su: ip: command not found  
ubuntu@client:~$ ip addr (ip a)  
-su: syntax error near unexpected token `('`  
ubuntu@client:~$ ip a  
-su: IP: command not found  
ubuntu@client:~$ wireshark  
-su: wireshark: command not found  
ubuntu@client:~$ wireshark  
-su: wireshark: command not found  
ubuntu@client:~$ sudo telnet 172.25.0.3  
Trying 172.25.0.3...  
telnet: Unable to connect to remote host: Connection refused  
ubuntu@client:~$
```

```
nslookup Bind to 192.168.10.10:0 failed (IOD #10): Cannot assign requested  
ress (99)  
IT (17.0339s) Starting TCP Handshake > 172.25.0.3:80  
V (17.0339s) Possible TCP RST received from 172.25.0.3:80 --> Connection refused  
nslookup Bind to 192.168.10.10:0 failed (IOD #19): Cannot assign requested  
ress (99)  
IT (18.0358s) Starting TCP Handshake > 172.25.0.3:80  
V (18.0358s) Possible TCP RST received from 172.25.0.3:80 --> Connection refused  
nslookup Bind to 192.168.10.10:0 failed (IOD #20): Cannot assign requested  
ress (99)  
IT (19.0377s) Starting TCP Handshake > 172.25.0.3:80  
V (19.0377s) Possible TCP RST received from 172.25.0.3:80 --> Connection refused  
  
rtt: N/A | Min rtt: N/A | Avg rtt: N/A  
connection attempts: 20 | Successful connections: 0 | Failed: 20 (100.00%)  
ng done: 1 IP address pinged in 19.04 seconds  
ntu@attacker:~$ telnet 172.25.0.3  
: telnet: command not found  
ntu@attacker:~$ sudo telnet 172.25.0.3  
: telnet: command not found  
ntu@attacker:~$ su -  
sword:  
Authentication failure  
ntu@attacker:~$
```