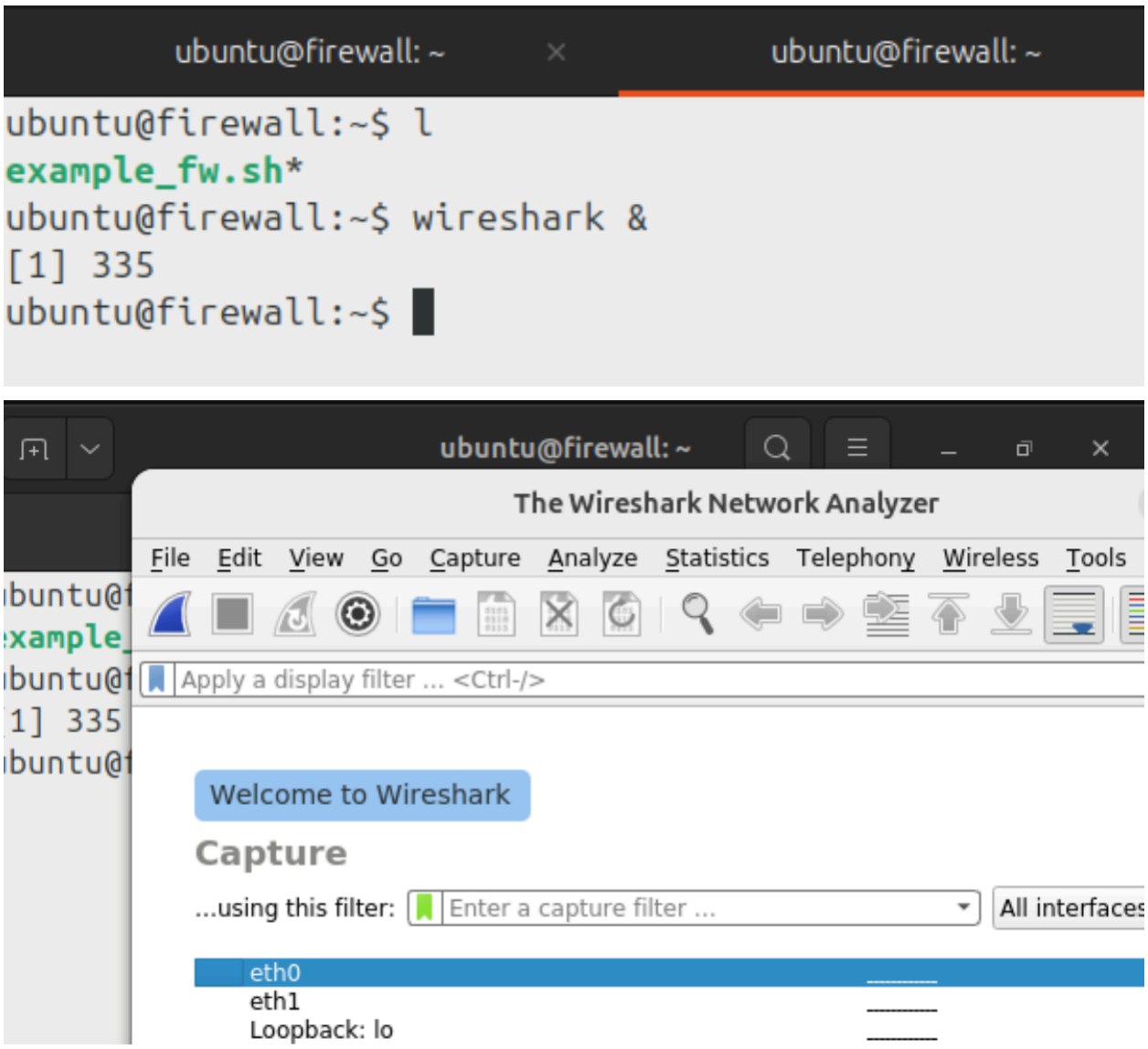
CSI4139 LAB 6 Report

Name: Iyanu Aketepe

Student No: 300170701

3.1



Wireshark has been opened in the firewall

0

```
ubuntu@client:~$ nmap server
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-24 20:41
 UTC
Nmap scan report for server (172.25.0.3)
Host is up (0.00055s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds
ubuntu@client:~$
```

Nmap has been used on the client side, three tcp ports are open.

```
Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds
ubuntu@client:~$ wget server &
[1] 472
ubuntu@client:~$
Redirecting output to 'wget-log'.
```

```
ubuntu@client:~$ cat wget-log
--2024-10-24 20:44:00--  http://server/
Resolving server (server)... 172.25.0.3
Connecting to server (server)|172.25.0.3|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 874 [text/html]
Saving to: 'index.html'

index.html     100%     874  --.-KB/s    in 0s

2024-10-24 20:44:00 (48.7 MB/s) - 'index.html' saved [874/8
74]

ubuntu@client:~$
```

```
ubuntu@client:~$ ssh server
The authenticity of host 'server (172.25.0.3)' can't be est
ablished.
ECDSA key fingerprint is SHA256:ZtE8xi5Y50aUktZ/XtgjIs1c5jx
YQB84Vq5ofmlgGng.
Are you sure you want to continue connecting (yes/no/[finge
rprint])? yes
Warning: Permanently added 'server,172.25.0.3' (ECDSA) to t
he list of known hosts.
ubuntu@server's password:
```

```
ubuntu@client:~$ telnet server
Trying 172.25.0.3...
Connected to server.
Escape character is '^]'.
Ubuntu 20.04.2 LTS
server login:
```

No.	Time	Source	Destination	Protocol
2104	376.584221786	172.24.0.3	172.25.0.3	TCP
2105	376.584815511	172.25.0.3	172.24.0.3	TCP
2106	376.585857059	172.24.0.3	172.25.0.3	TCP
2107	376.585978892	172.25.0.3	172.24.0.3	TCP

3.2

Text of Example_fw.sh script:

```
#!/bin/bash
#
#  This example IPTABLES firewall will only allow SSH traffic>
#  to be forwarded
#
IPTABLES=/sbin/iptables
```

```
#start and flush
$IPTABLES -F
$IPTABLES -t nat -F
$IPTABLES -X
#
#  By default, do not allow any forwarding or accept any t>
#  destined for the firewall.
#
$IPTABLES -P FORWARD DROP
$IPTABLES -P INPUT   DROP
$IPTABLES -P OUTPUT  DROP

# Allow forwarding of traffic associated with any establis>
$IPTABLES -A FORWARD -m conntrack --ctstate ESTABLISHED,RE>

# Allow SSH traffic on port 22
$IPTABLES -A FORWARD -p tcp --dport 22 -j ACCEPT

# loopback device (internal traffic)
iptables -A INPUT -i lo -p all -j ACCEPT

# log IPTABLES filtering actions
iptables -A FORWARD -j NFLOG -m limit --limit 2/min --nflog-prefix "IPTABLES DROPPED"
```

```
ubuntu@firewall:~$ sudo iptables -A FORWARD -p tcp --dpor
t 22 -j ACCEPT
ubuntu@firewall:~$ sudo iptables -A FORWARD -p tcp --dpor
t 80 -j ACCEPT
ubuntu@firewall:~$
```

Iptables has been used to only allow for ssh and http.

```
ubuntu@client:~$ telnet server
Trying 172.25.0.3...
```

Client tries to connect to server using telnet

```
ubuntu@firewall:~$ tail -f /var/log/iptables.log
Oct 24 21:21:11 firewall IPTABLES DROPPED IN=eth0 OUT=eth
1 MAC=02:42:ac:18:00:04:02:42:ac:18:00:03:08:00 SRC=172.2
4.0.3 DST=172.25.0.3 LEN=60 TOS=10 PREC=0x00 TTL=63 ID=13
554 DF PROTO=TCP SPT=39990 DPT=23 SEQ=1613553224 ACK=0 WI
NDOW=32120 SYN URGP=0 MARK=0
Oct 24 21:21:12 firewall IPTABLES DROPPED IN=eth0 OUT=eth
1 MAC=02:42:ac:18:00:04:02:42:ac:18:00:03:08:00 SRC=172.2
4.0.3 DST=172.25.0.3 LEN=60 TOS=10 PREC=0x00 TTL=63 ID=13
555 DF PROTO=TCP SPT=39990 DPT=23 SEQ=1613553224 ACK=0 WI
NDOW=32120 SYN URGP=0 MARK=0
```

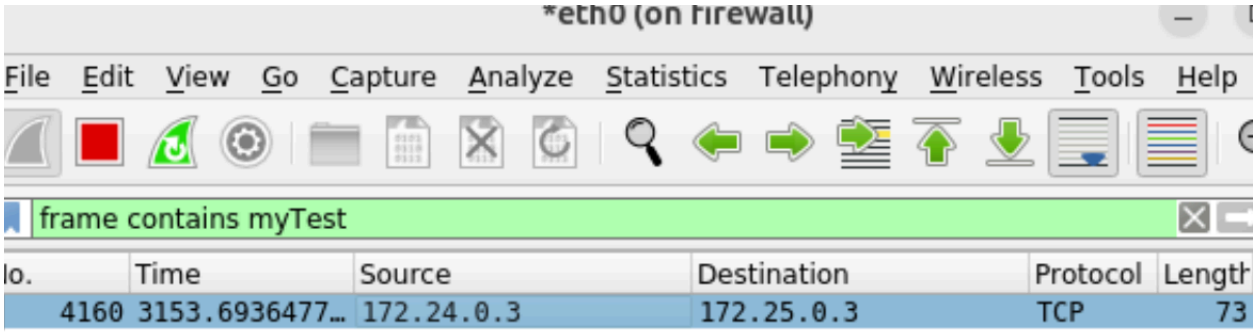
Firewall has dropped packets

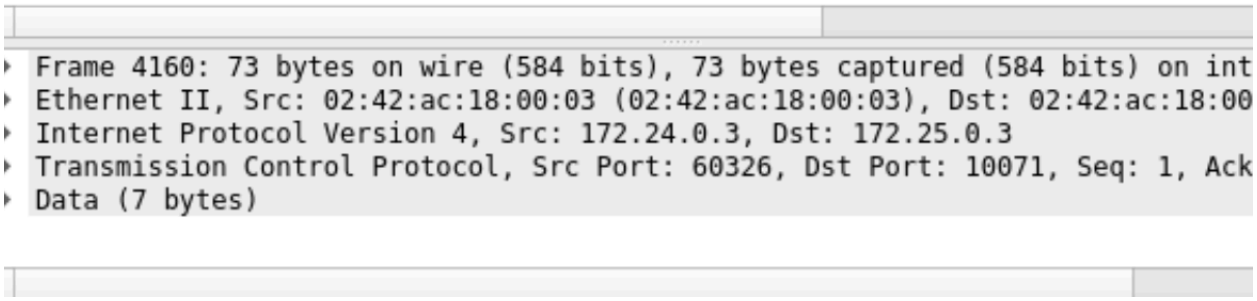
```
ubuntu@client:~$ nmap server
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-24 21:
22 UTC
Nmap scan report for server (172.25.0.3)
Host is up (0.0052s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 4.91 secon
ds
ubuntu@client:~$
```

Client uses nmap, and sees that telnet is no longer open

3.3

```
ubuntu@client:~$ ./wizbang myTest
Sending instruction myTest
bye
ubuntu@client:~$
```






```
ubuntu@firewall:~$ sudo iptables -A FORWARD -p tcp --dpor
t 10071 -j ACCEPT
ubuntu@firewall:~$
```

```
ubuntu@client:~$ nmap -p 10000-10100 server
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-24 21:
42 UTC
Nmap scan report for server (172.25.0.3)
Host is up (0.0010s latency).
Not shown: 100 filtered ports
PORT      STATE SERVICE
10071/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.89 secon
ds
ubuntu@client:~$
```