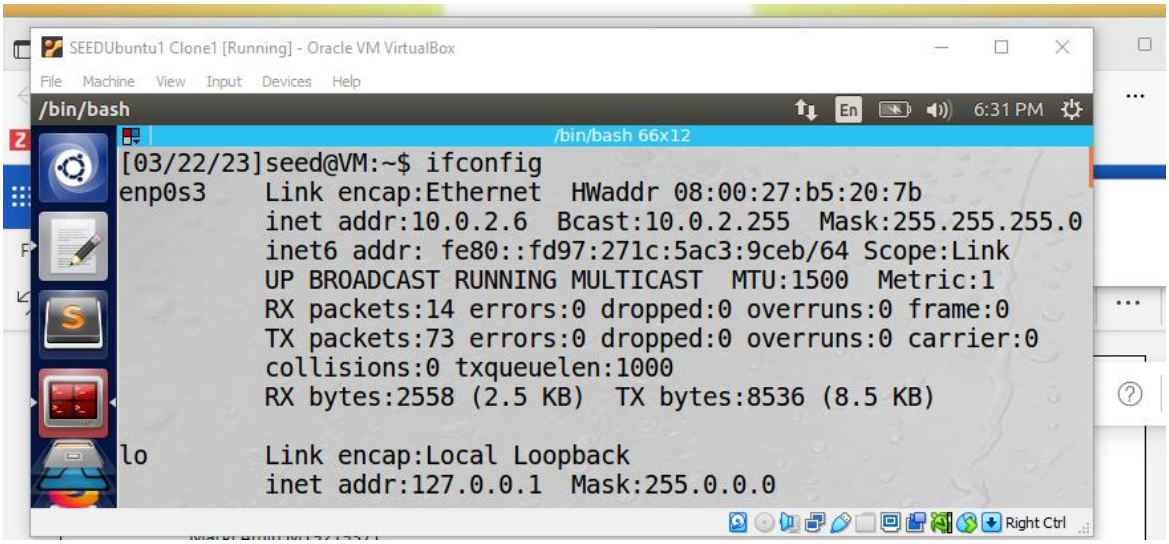
CS 5153/6053 Network Security, Spring 2023 Project 2: Buffer Overflow Attack

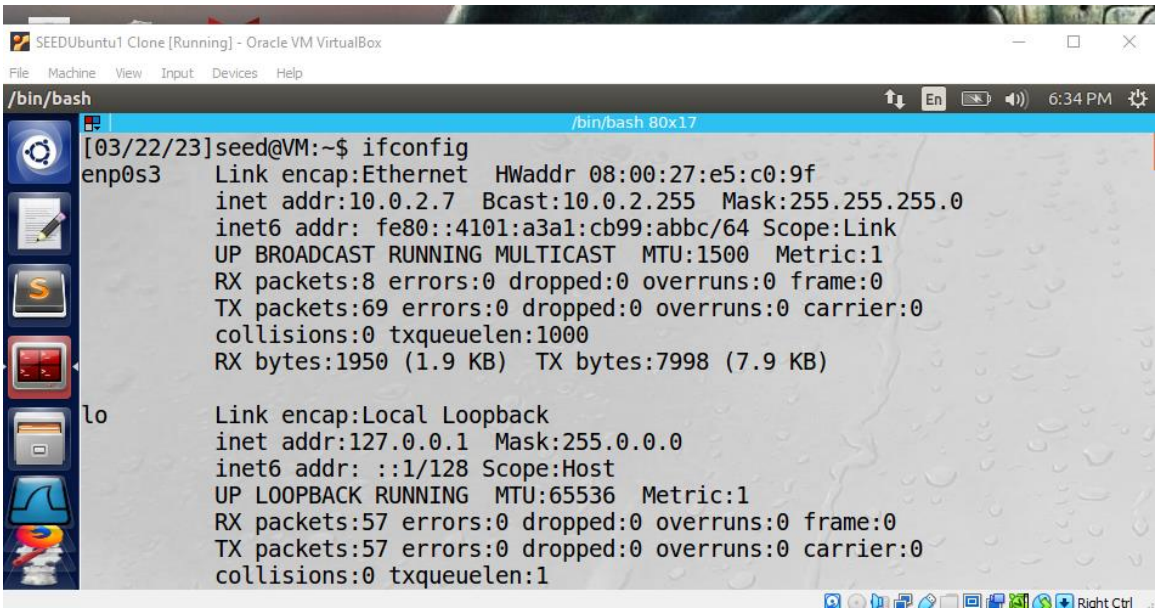
Margi Amin M19219371

I successfully set up a three virtual machines according to the instructions provided in the paper.

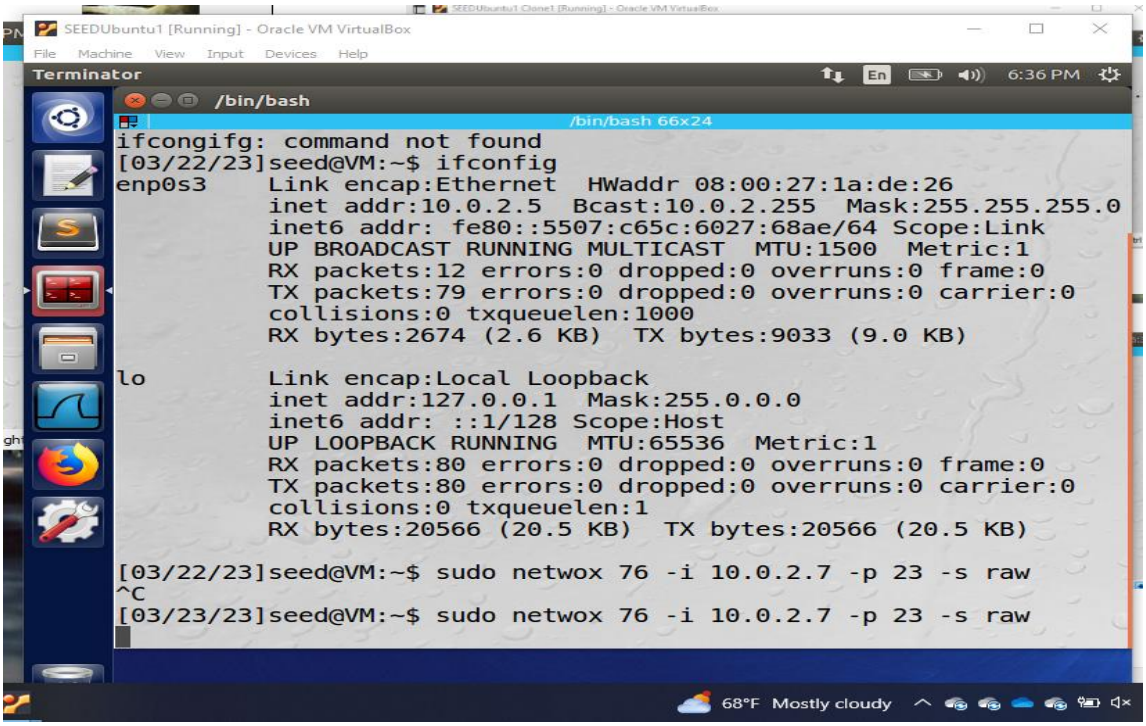
This is my user machine with IP address of 10.0.2.6



This is my server machine with IP address of 10.0.2.7



This is my attacker's machine with 10.0.2.5



Task 1 : SYN flooding attack

Step 1: turn SYN cookies off

In server run following command:

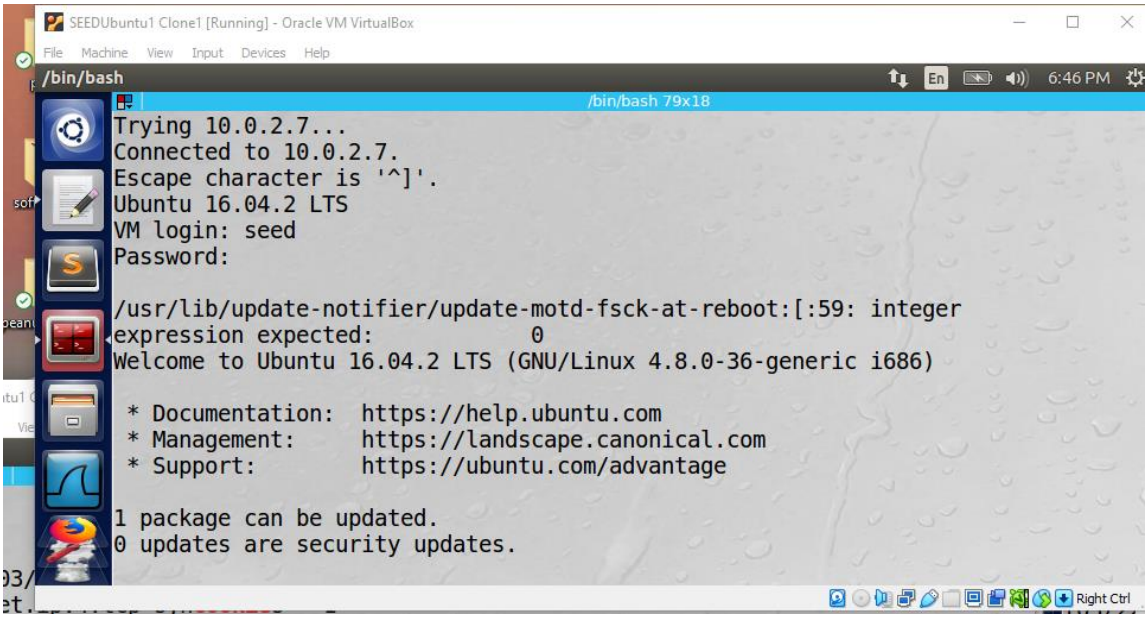
Sudo sysctl -w net.ipv4.tcp_syncookies=0

Step 2: connect user machine by telnet

In user run following command:

Telnet 10.0.2.7

My output with login id : seed and password: dees

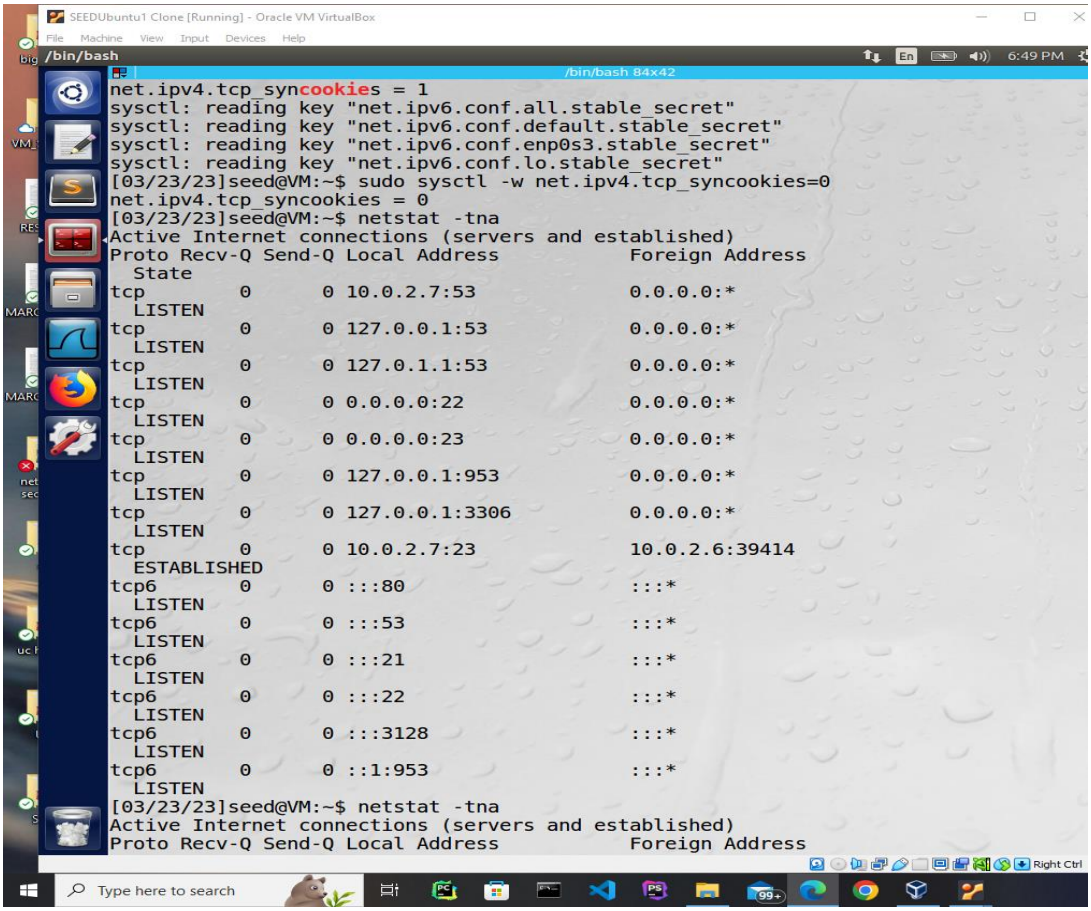


Step 3: in server machine cheack tcp connection

In server run following command:

Netstat –tna

My output:



Here we can see only one connection established betwwen 10.0.2.7 and 10.0.2.6.

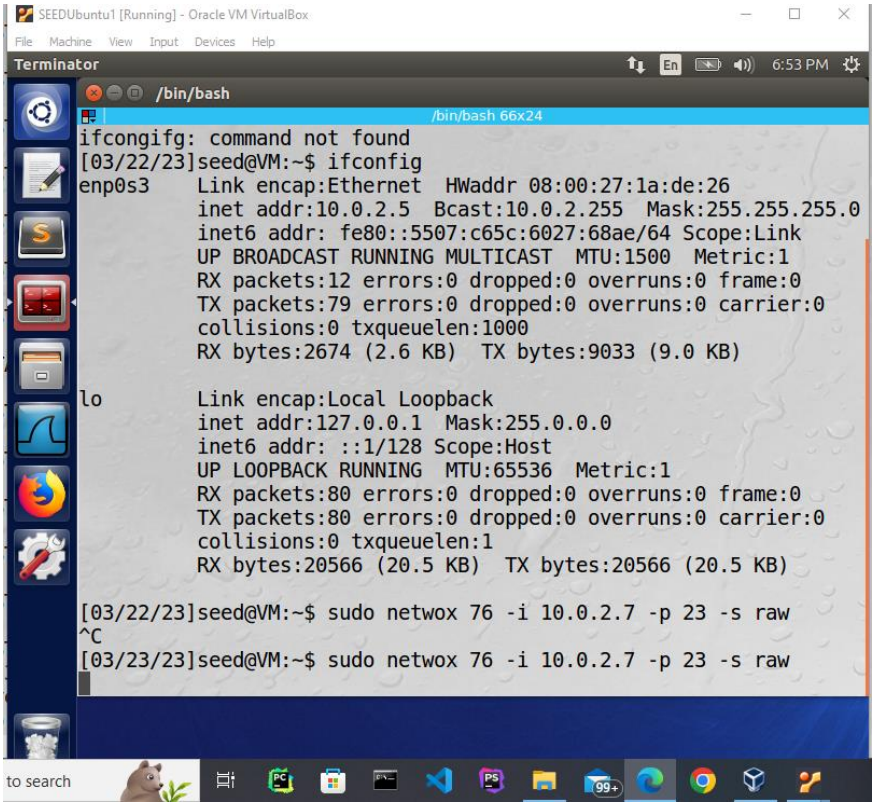
Step 4: attack server

In attaker run following command:

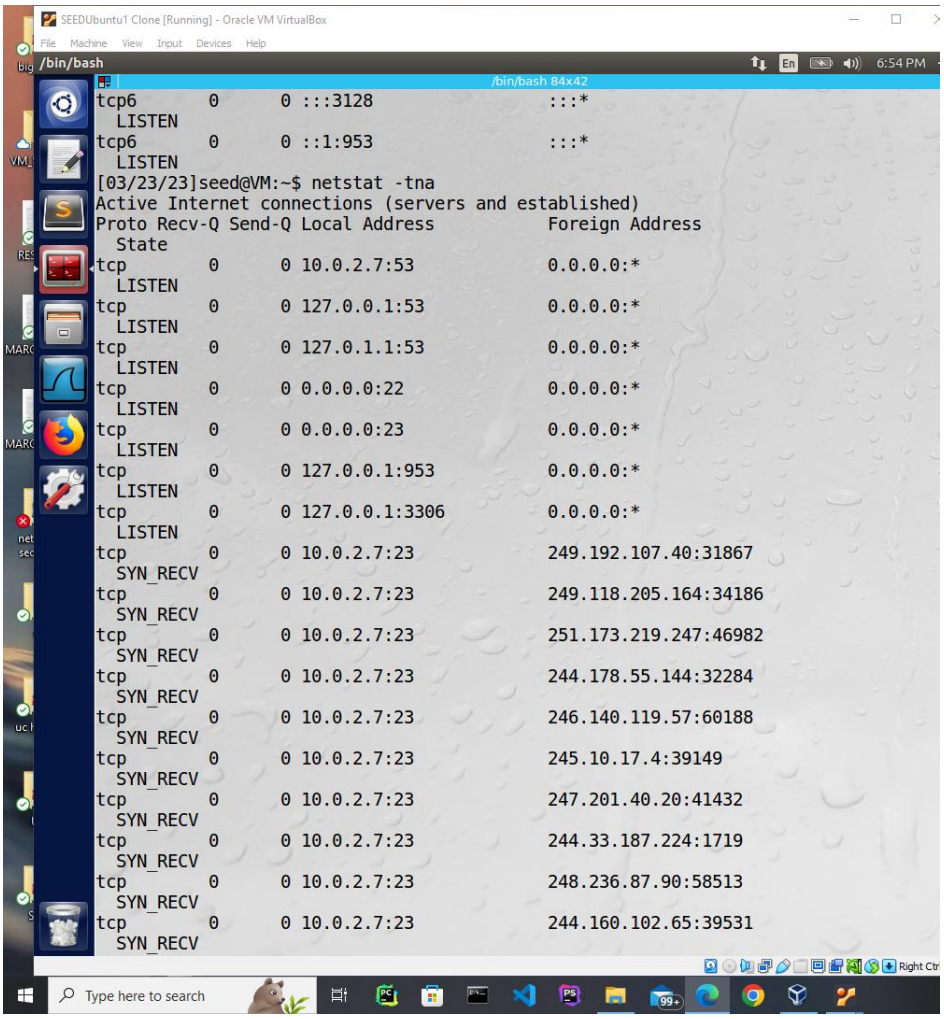
Sudo network 76 -I 10.0.2.7 -p 23 –s raw

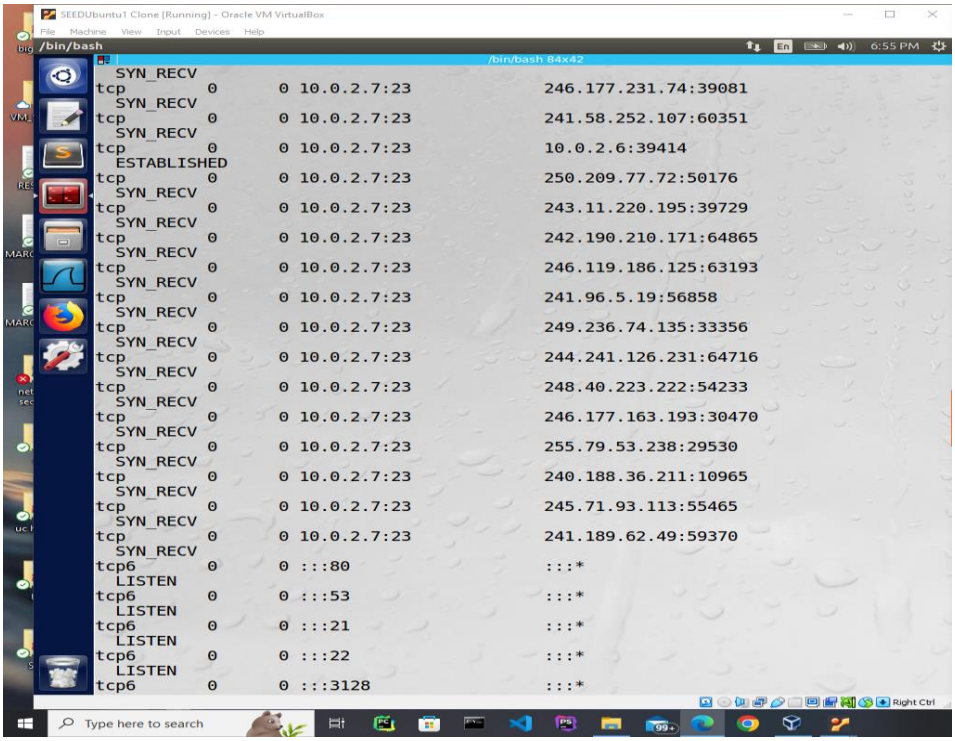
My output:

In attackers:



In server after repeting step 3:

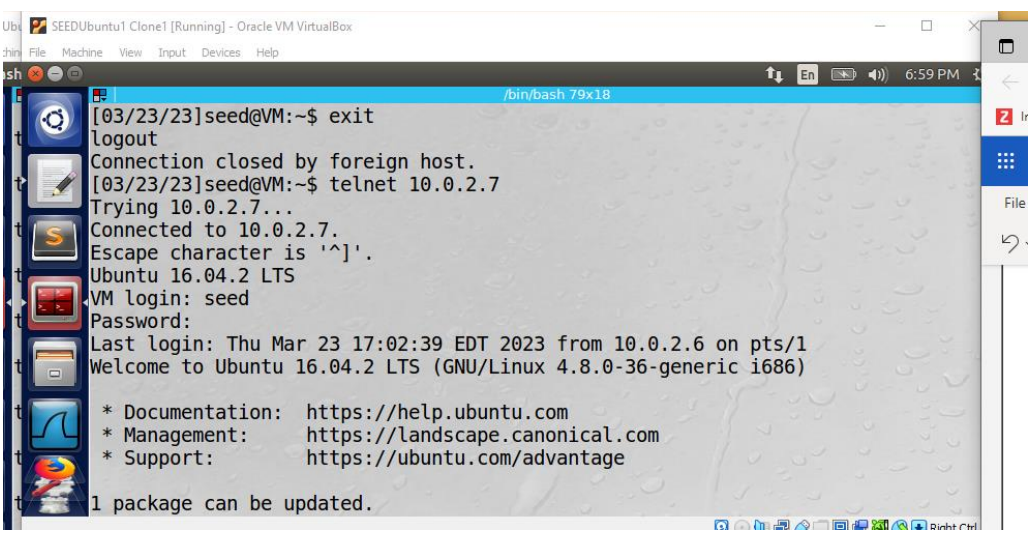

SEEDUbuntu1 Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
6:54 PM
/bin/bash 84x42
tcp6 0 0 :::3128 :::*
LISTEN
tcp6 0 0 ::1:953 :::*
LISTEN
[03/23/23]seed@VM:~$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address
State
tcp 0 0 10.0.2.7:53 0.0.0.0:*
LISTEN
tcp 0 0 127.0.0.1:53 0.0.0.0:*
LISTEN
tcp 0 0 127.0.1.1:53 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
tcp 0 0 10.0.2.7:23 249.192.107.40:31867
SYN_RECV
tcp 0 0 10.0.2.7:23 249.118.205.164:34186
SYN_RECV
tcp 0 0 10.0.2.7:23 251.173.219.247:46982
SYN_RECV
tcp 0 0 10.0.2.7:23 244.178.55.144:32284
SYN_RECV
tcp 0 0 10.0.2.7:23 246.140.119.57:60188
SYN_RECV
tcp 0 0 10.0.2.7:23 245.10.17.4:39149
SYN_RECV
tcp 0 0 10.0.2.7:23 247.201.40.20:41432
SYN_RECV
tcp 0 0 10.0.2.7:23 244.33.187.224:1719
SYN_RECV
tcp 0 0 10.0.2.7:23 248.236.87.90:58513
SYN_RECV
tcp 0 0 10.0.2.7:23 244.160.102.65:39531
SYN_RECV
Type here to search



Step 5 : try to connect user machine by telnet again

Follow step 2 and could not able to connect.

Output:



So we can say that attack ws successful.

Also tried with SYN cookies on and was able to connect.

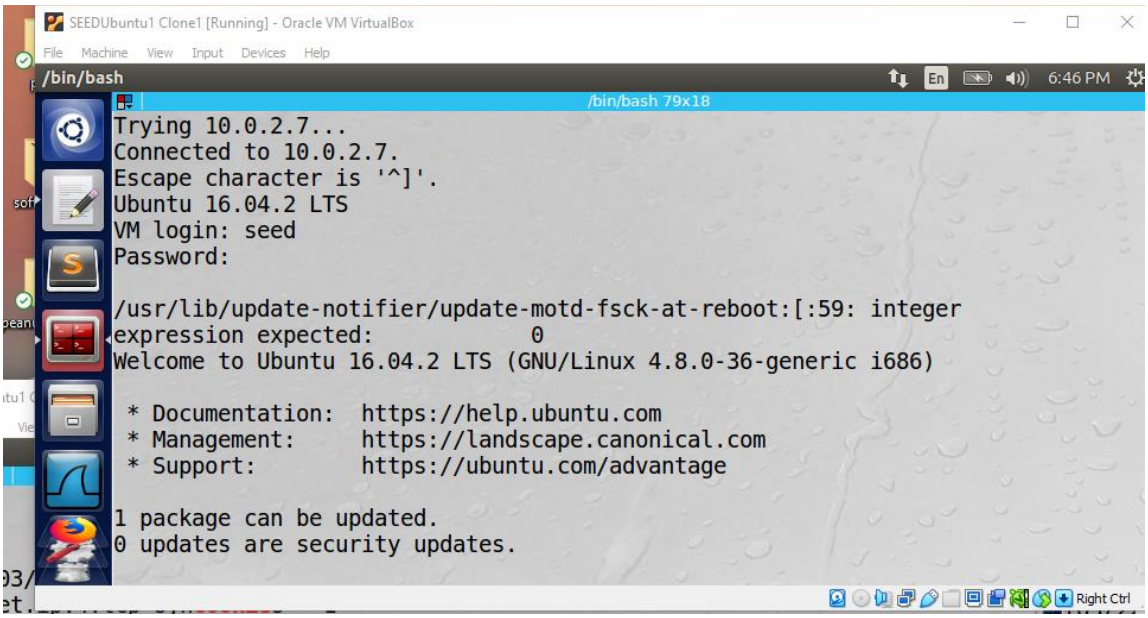
Task 2: TCP RST Attack on telnet

Step 1: connect user machine by telnet

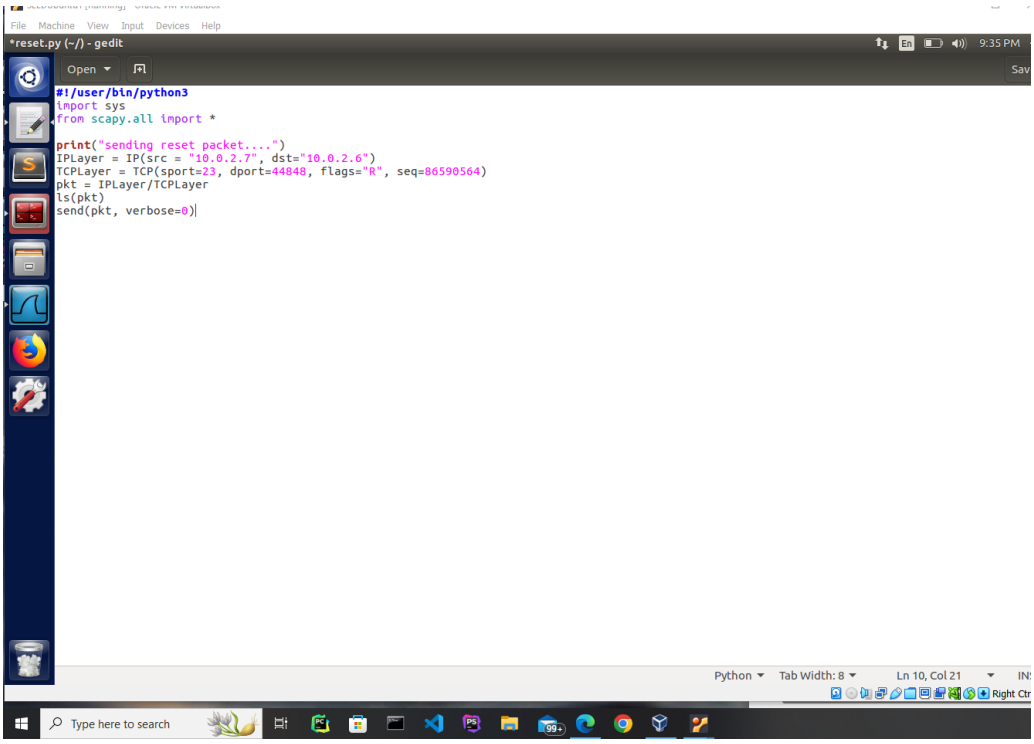
In user run following command:

Telnet 10.0.2.7

My output with login id : seed and password: dees



Step 2: Install pip3 and scapy and run following command:



Step 3:

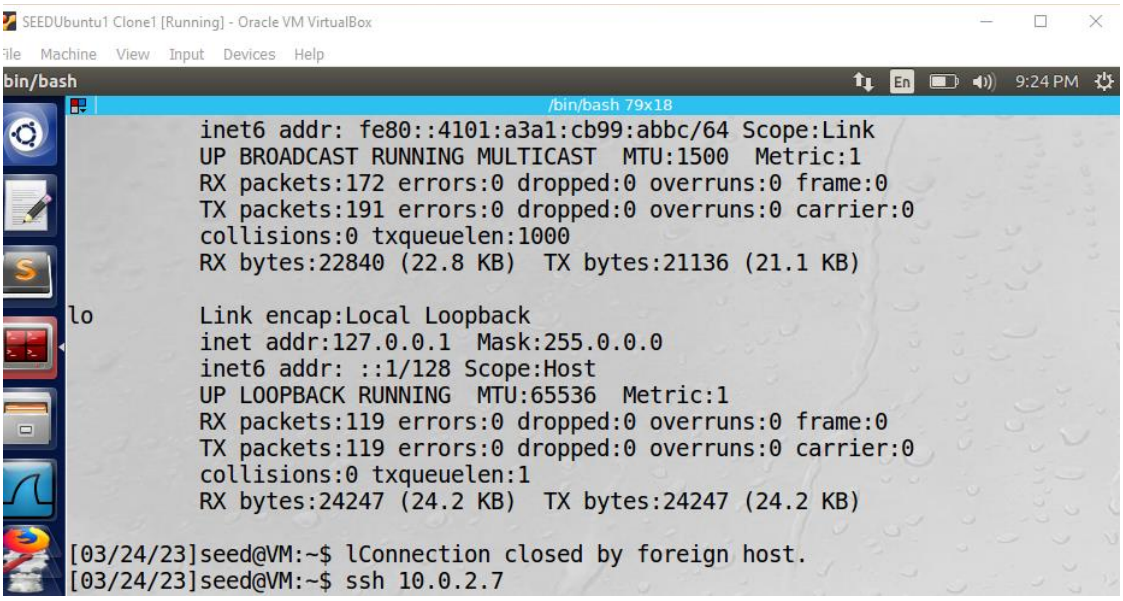
Run following command in attacker:

Sudo python reset.py

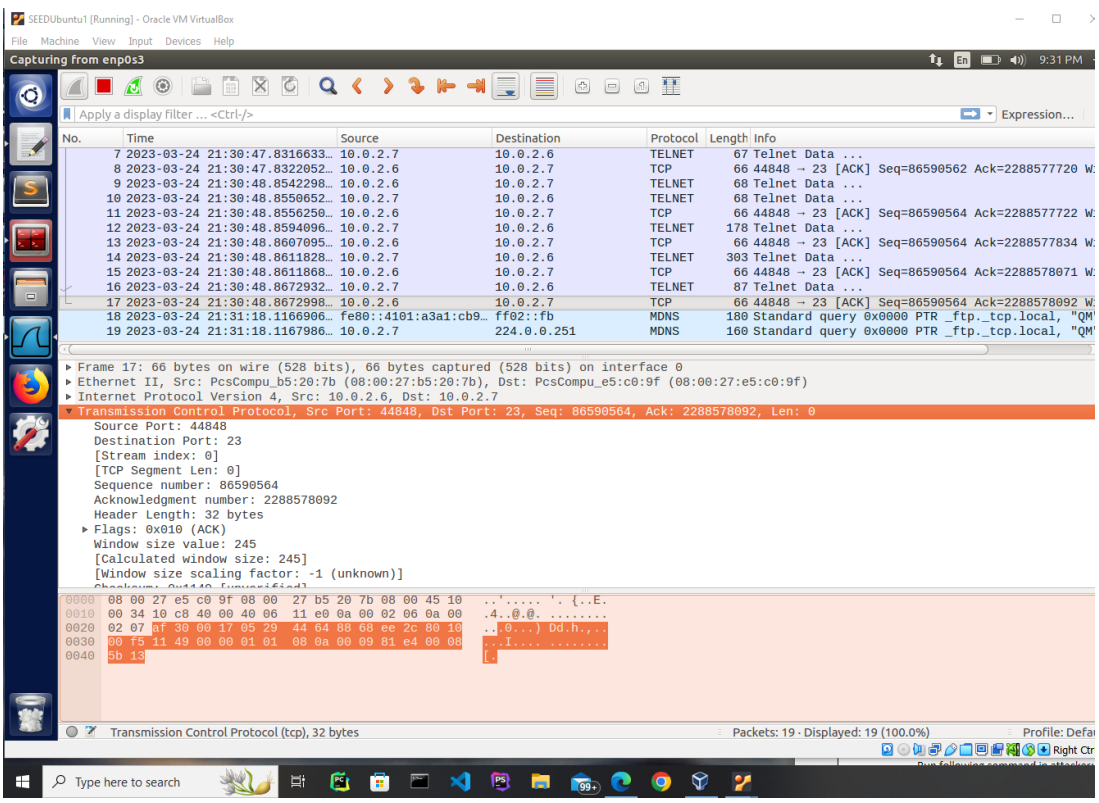
Step 4:

Attack successful

Output: It says connection closed by foreign host.



For sequence used wireshark:



Task 4:TCP Hijacking

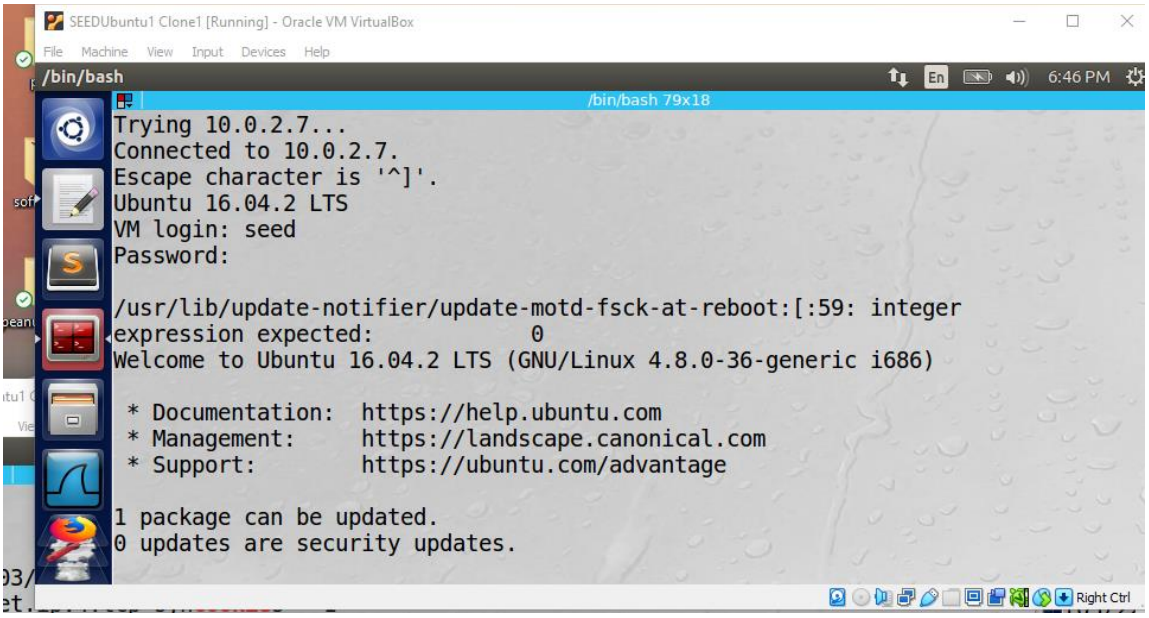
Step 1:create secret.txt file in server.

Step 2: connect user machine by telnet

In user run following command:

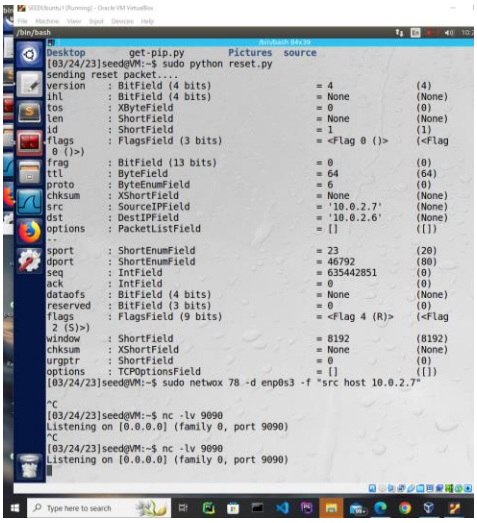
Telnet 10.0.2.7

My output with login id : seed and password: dees

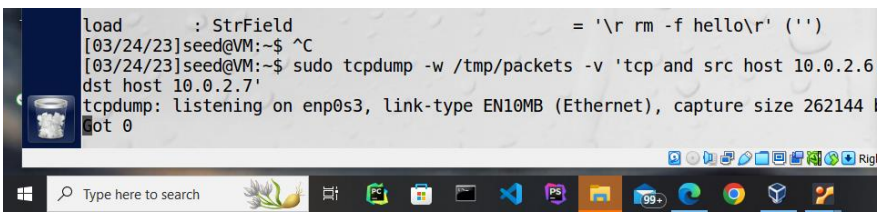


Step 3:connect by following command :

Nc –lv 9090



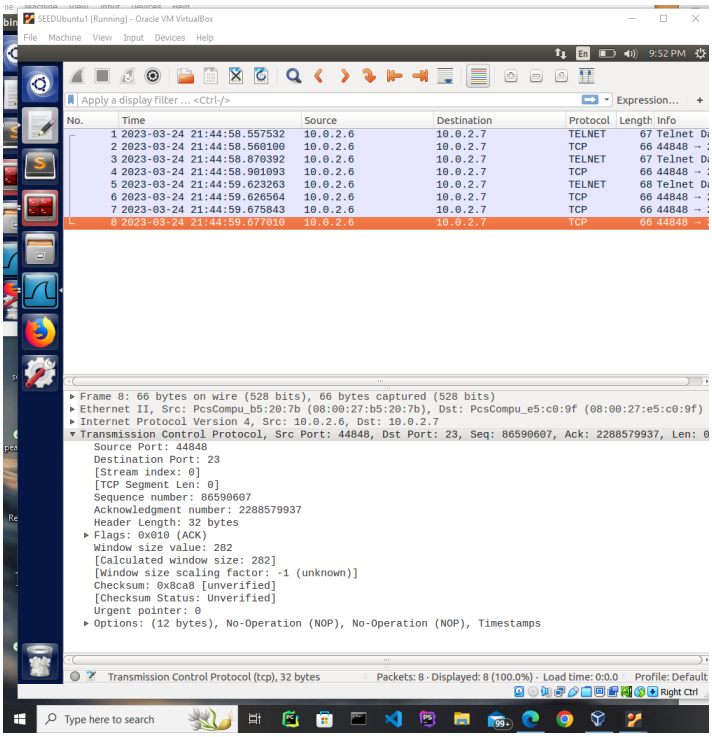
Step 4: in new terminal in attacker do following command:



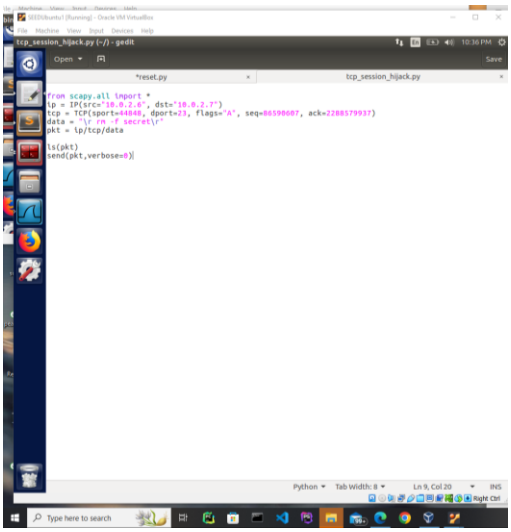
Step 5: do following command In attacker:

Wireshark /tmp/packets

Output:



Step 6 : do following command in attacker after editing all the numbers from the above step:

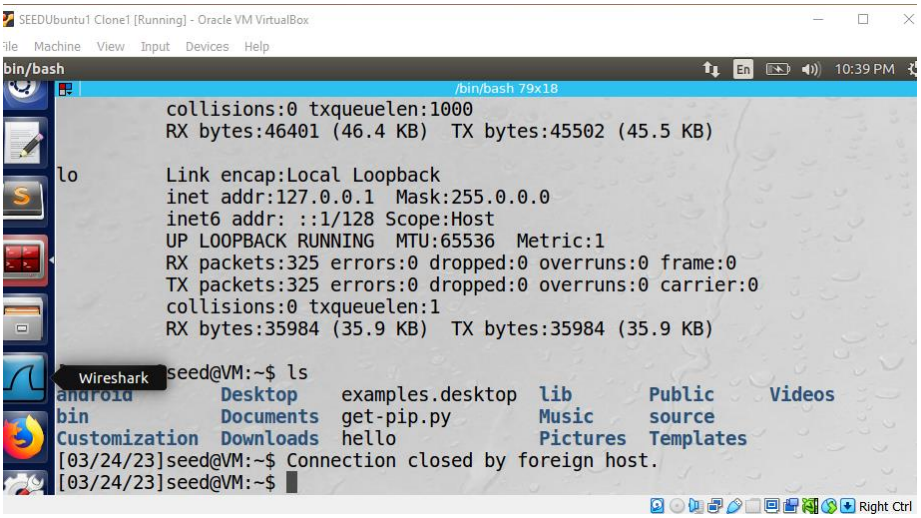


Step 7:

Do following command in attacker:

Sudo python tcp_session_hijack.py

Output:



We can not right any thing in user terminal.

And can not find the file in the server terminal.

So attack is successful.

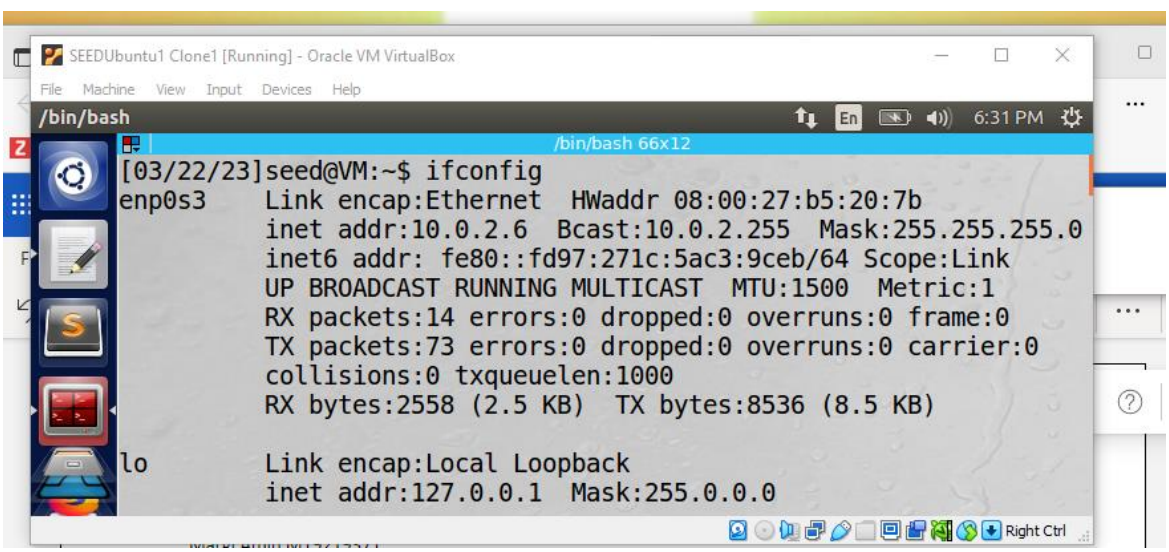
Task 5: shell reverse

Step 1: connect user machine by telnet

In user run following command:

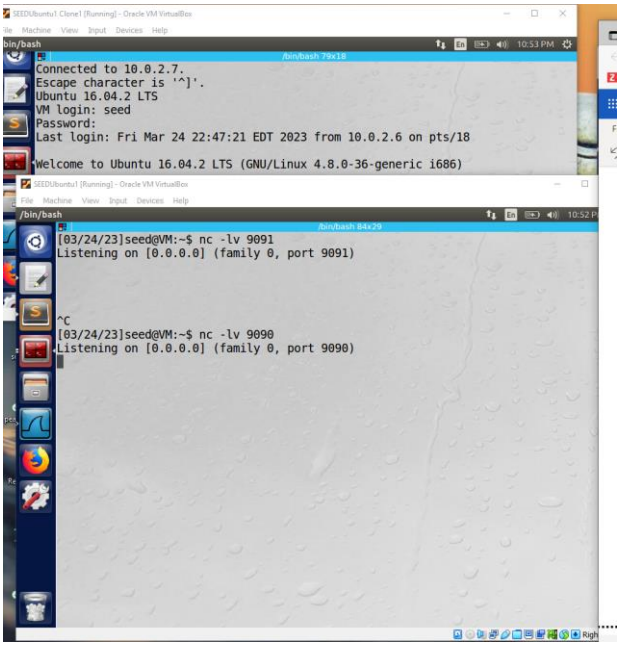
Telnet 10.0.2.7

My output with login id : seed and password: dees



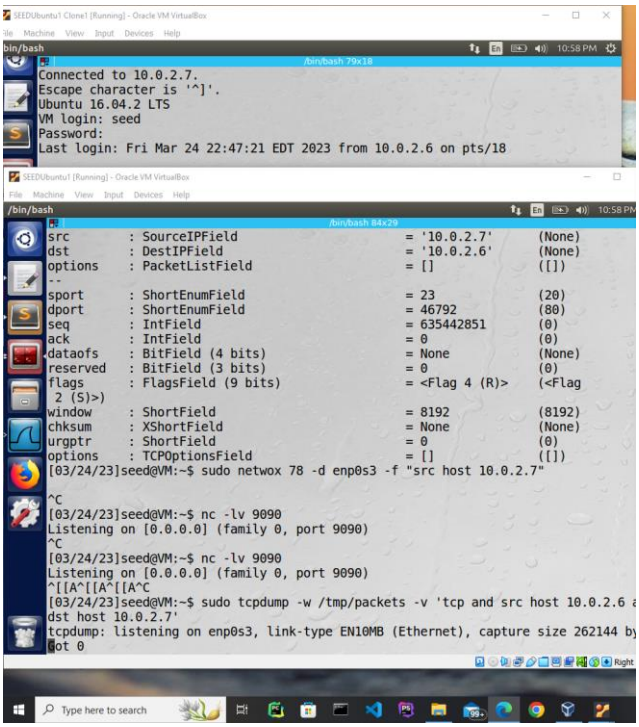
Step 2: build connection by following command:

Nc –lv 9090

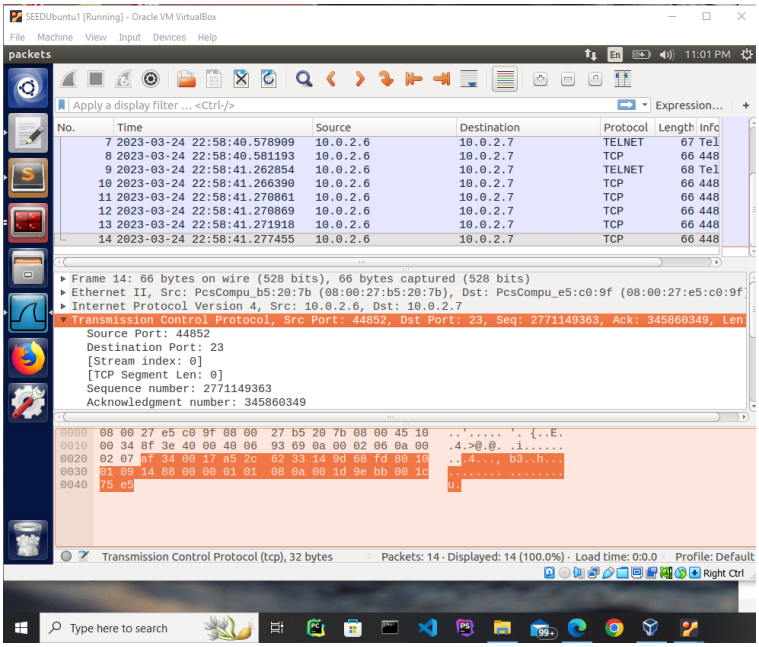


Step 3: in new terminal in attacker do following command :

Sudo tcpdump –w /tmp/packets -v ‘tcp and src host 10.0.2.6 and dst host 10.0.2.7’



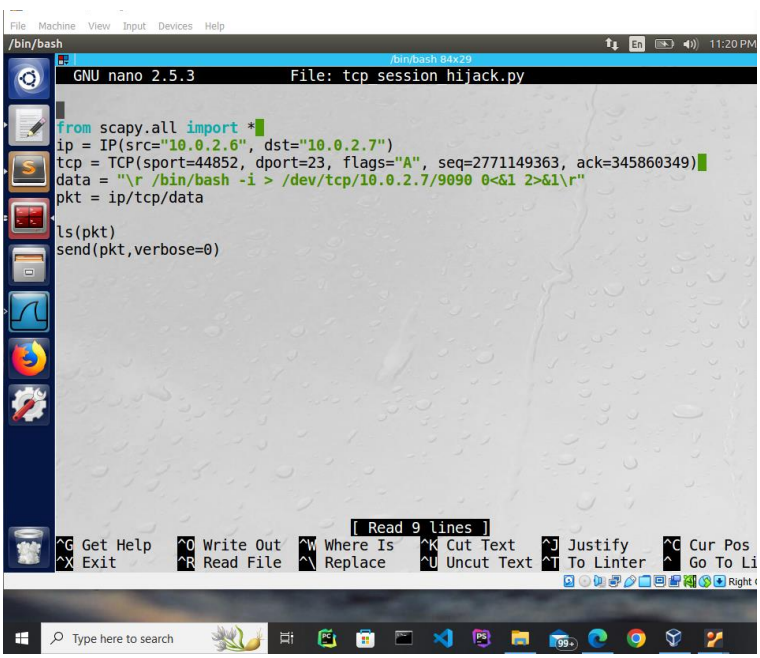
Step4 : do a simple command In user and then open wireshark in attacker.

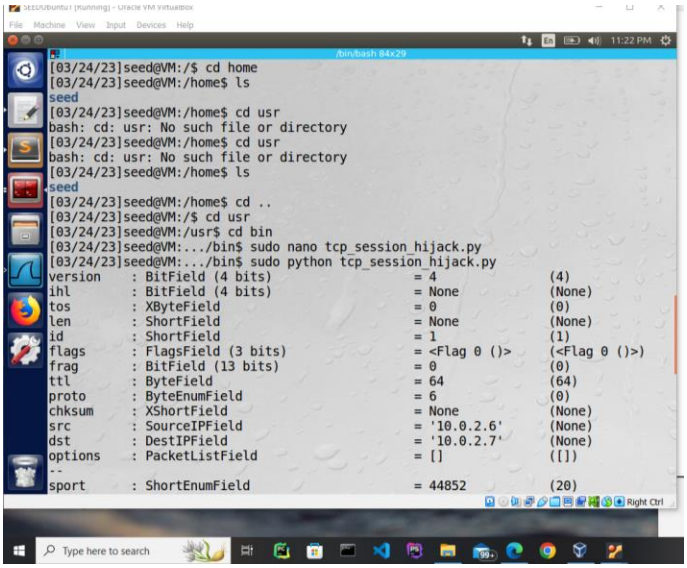


Step 5: do following command in bin directory in attacker:

Sudo nano tcp_session_hijack.py

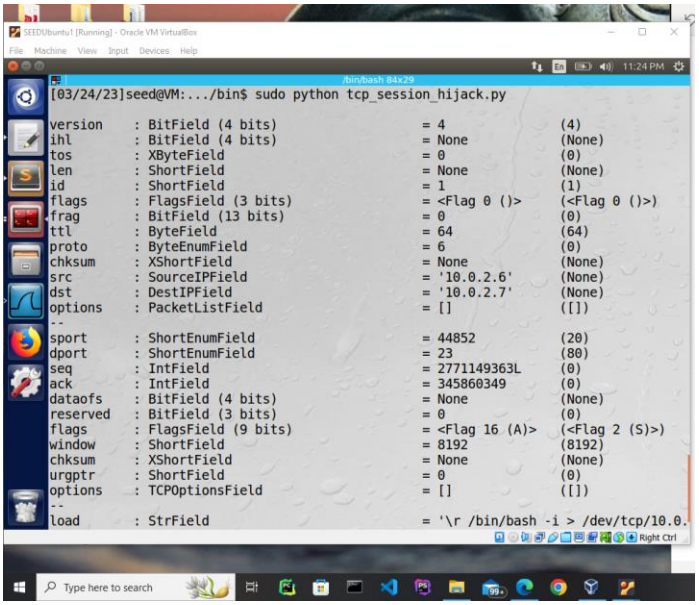
Output:





Step 6 : run python command:

Sudo python tcp_session_hijack.py



Step 7: now the 9090 port is connected .