COMPUTER NETWORKS SECURITY LABORATORY
ASSIGNMENT 2

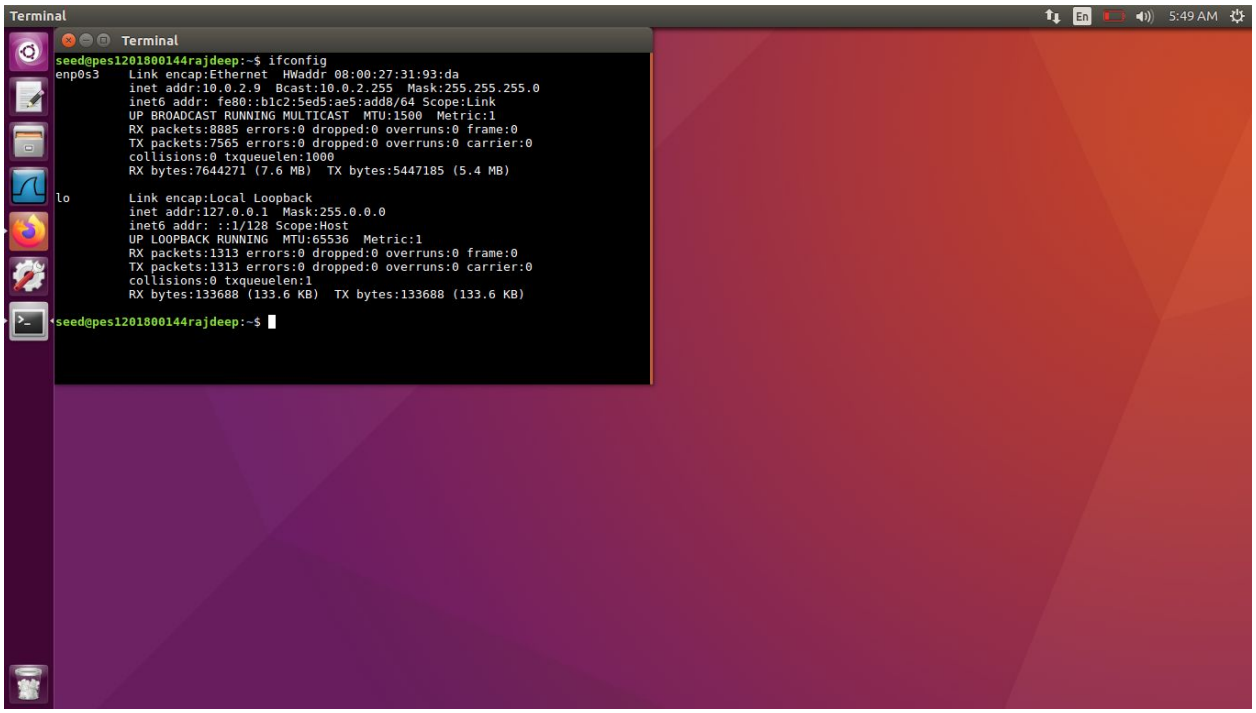
BY: RAJDEEP SENGUPTA
SRN: PES1201800144
SECTION: C

NOTE: Please find my SRN 'PES1201800144rajdeep' as the terminal username.

MY CONFIGURATIONS:

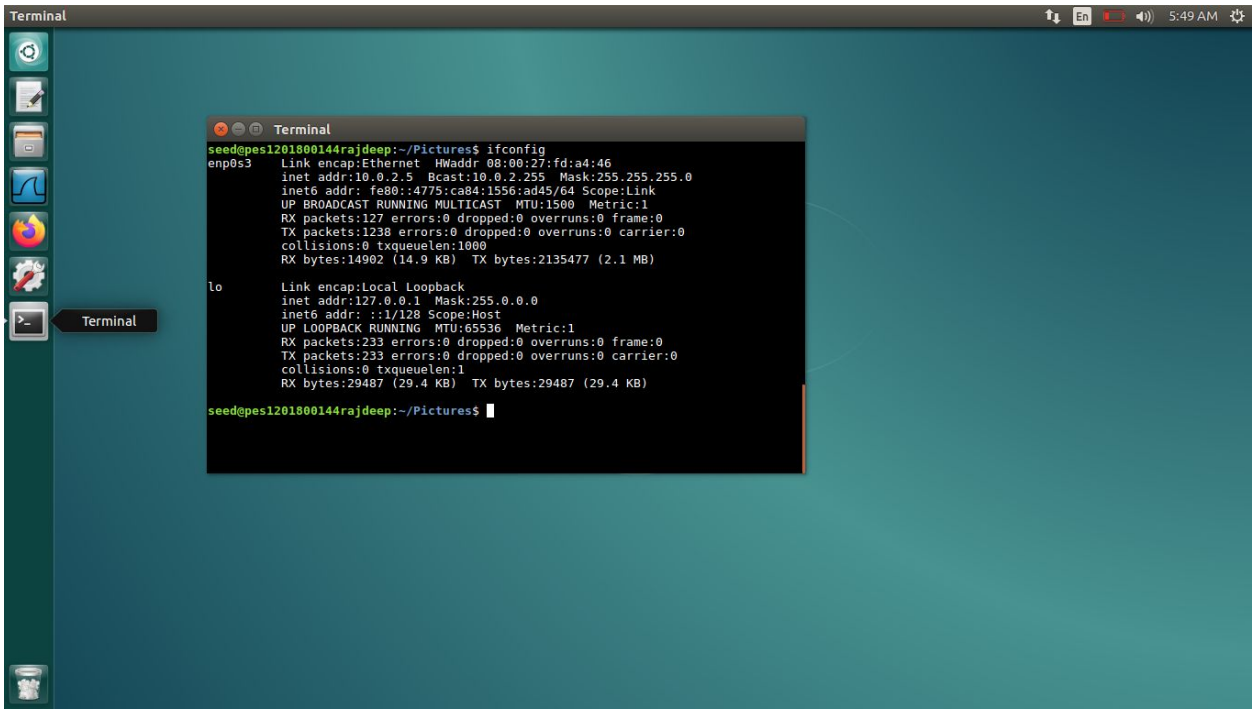
VM1 (Attacker)

IP Address: 10.0.2.9

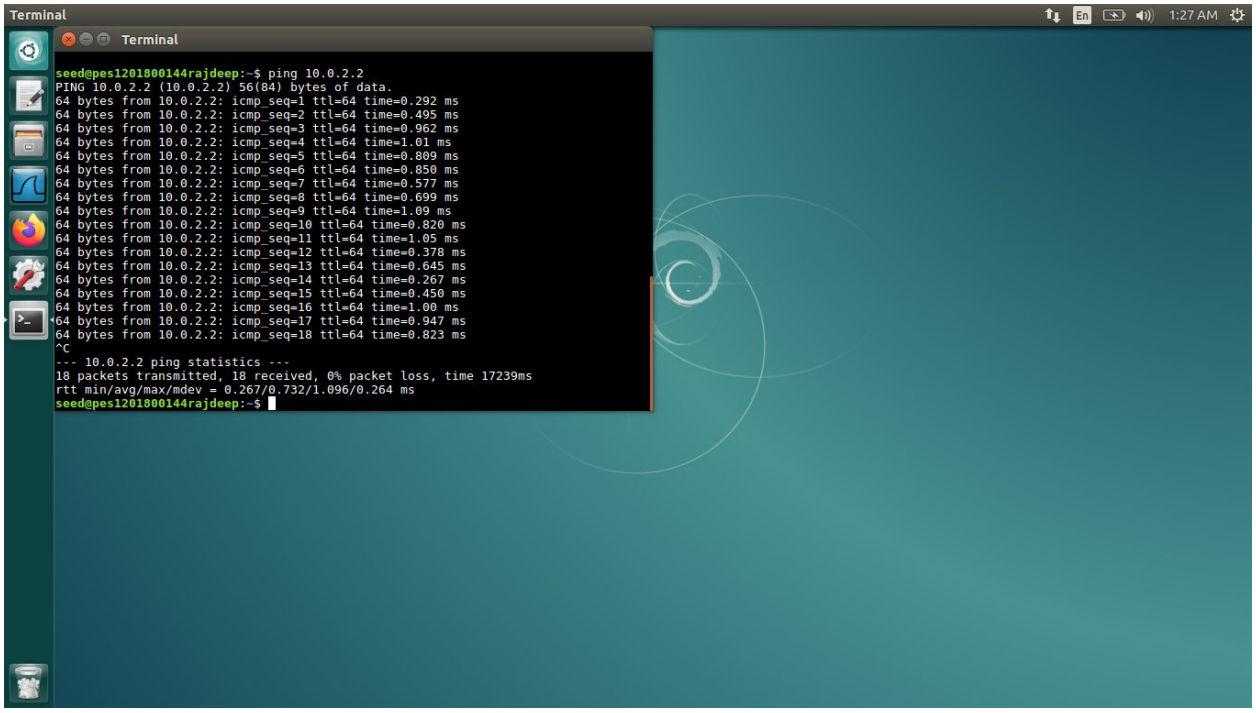


VM2 (Victim)

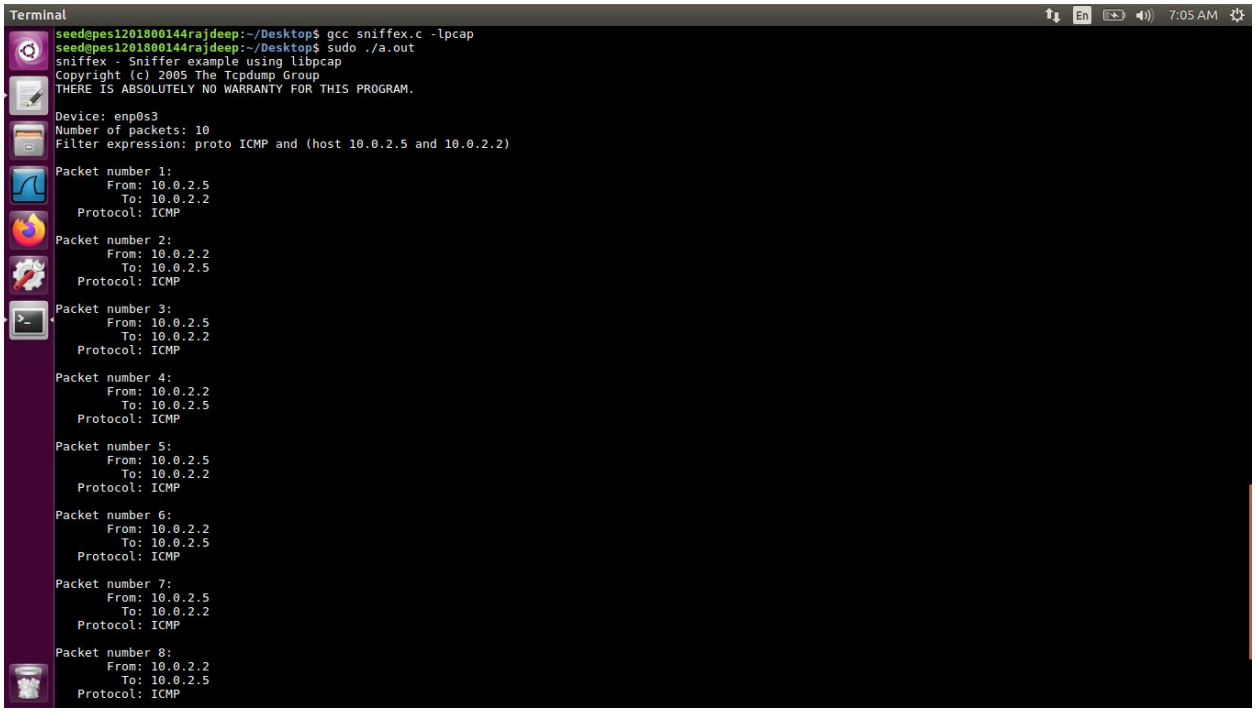
IP Address: 10.0.2.5



TASK 1.1A



Victim machine(10.0.2.5) pinging to 10.0.2.2



Attacker machine(10.0.2.9) sniffing the packets from victim machine(10.0.2.5) to a host(10.0.2.2)

Ques 1. Please use your own words to describe the sequence of the library calls that are essential for sniffer programs. This is meant to be a summary, not detailed explanation like the one in the tutorial.

Sol 1. **The library calls made and their uses are:**

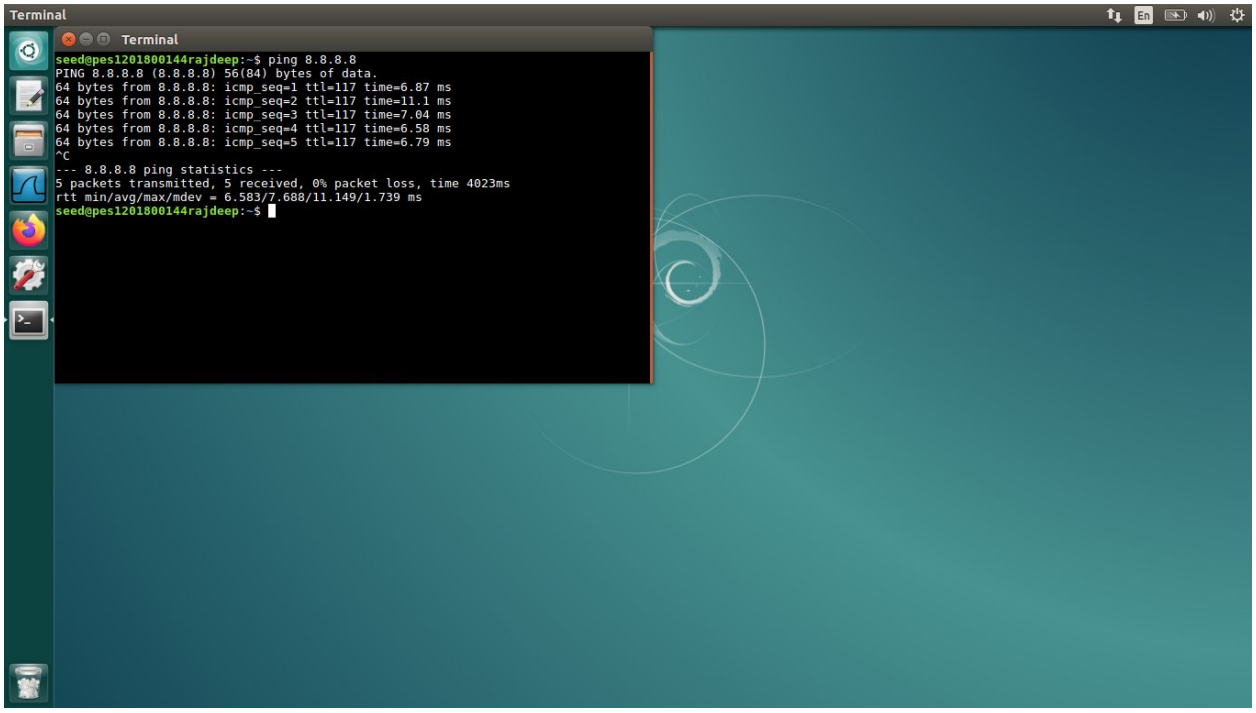
- **pcap - provides packet capture and filtering engines**
- **pcap_open_live() - start session on a device in the network to initiate sniffing**
- **pcap_compile() - compile filter expression stored in a string**
- **pcap_setfilter() - set the compiled filter to filter the packets to be sniffed**
- **pcap_loop() - to make the program wait for multiple packets for being sniffed**
- **pcap_close() - close the sniffing session**

Ques 2. Why do you need the root privilege to run sniffex? Where does the program fail if executed without the root privilege?

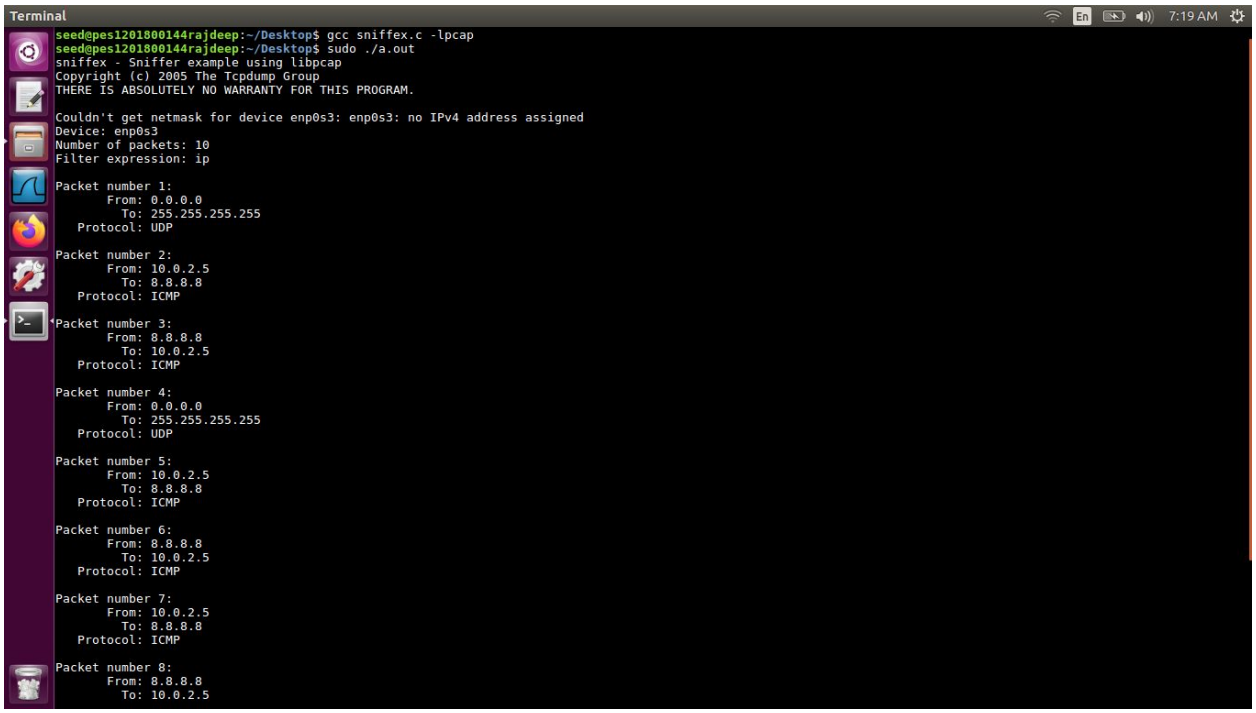
Sol 2. **When sniffex code is executed without root privilege, the terminal responds with "Permission denied". In this code, pcap library is used which tries to access the NIC(Network Interface Card) to sniff packets within the network even if the packets are not meant for the attacker machine(promiscuous mode).**

Ques 3> Promiscuous Mode On/Off Demonstration:

Promiscuous Mode On:

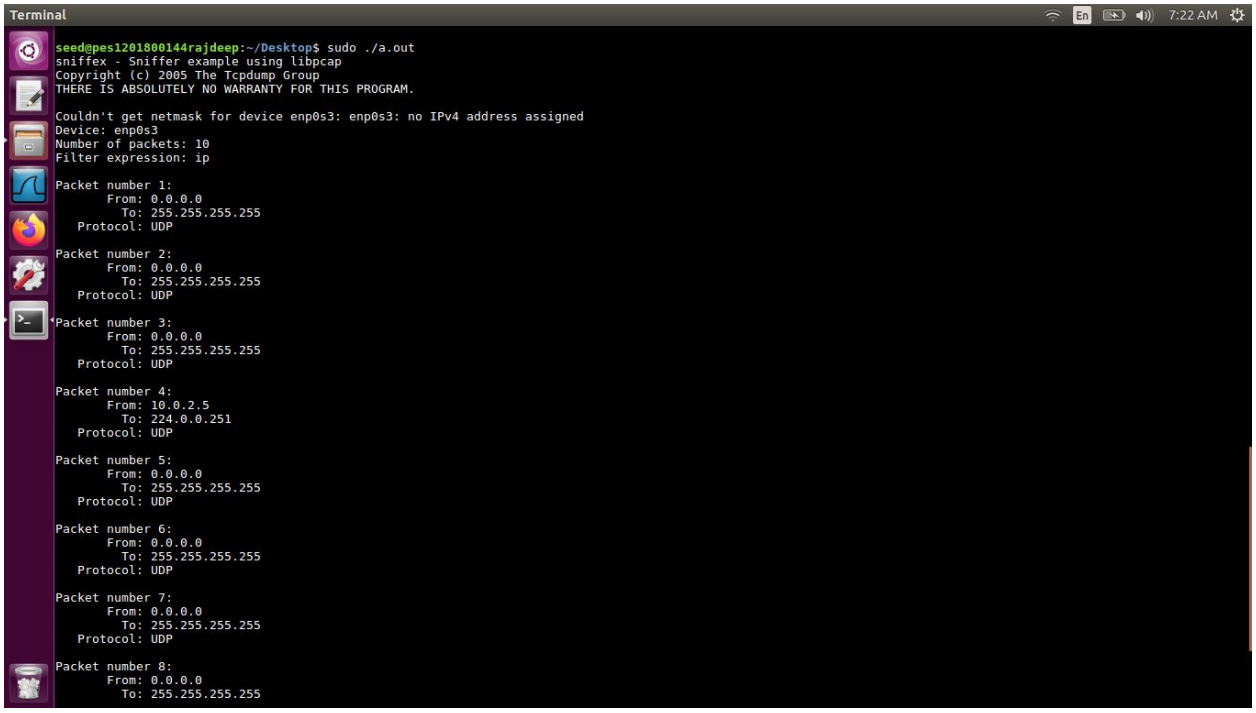


Victim machine(10.0.2.5) pinging to 8.8.8.8

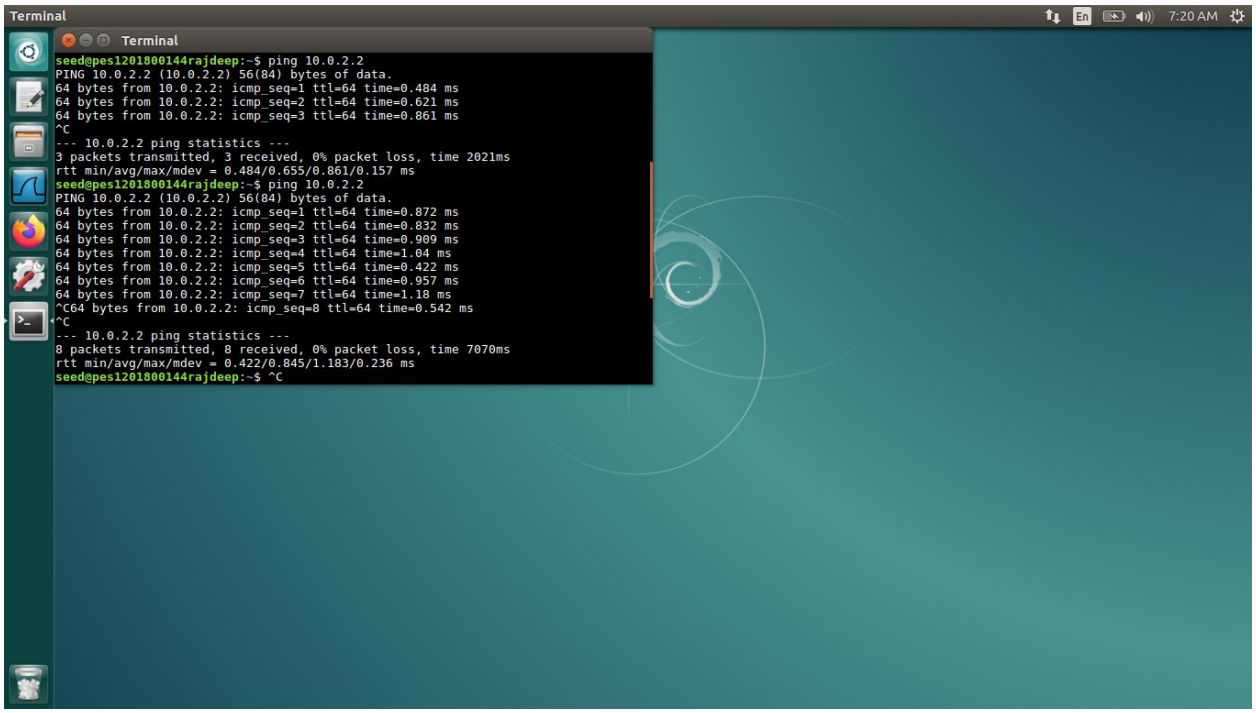


Attacker Machine(10.0.2.9) sniffing ICMP ping packets from victim machine(10.0.2.5) to Google server(8.8.8.8)

Promiscuous Mode Off:



Attacker machine (10.0.2.9) cannot sniff packets that don’t involve it’s IP address in source or destination.



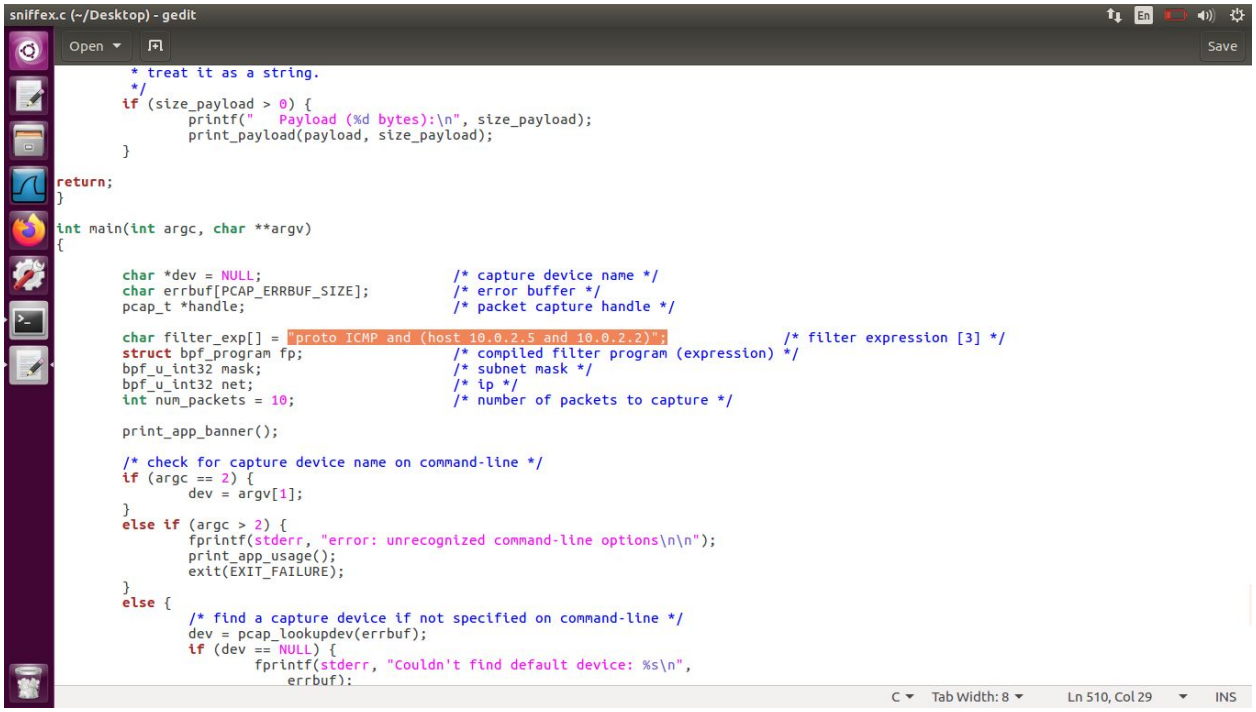
The victim pings to a host other than the attacker machine and the attacker cannot sniff this connection(in the screenshot above) since the promiscuous mode is off in the attacker machine.

When promiscuous mode is turned on, the attacker machine can sniff all the packets in the network may those be for the attacker machine or not. On the other hand, when the promiscuous mode is turned off, the attacker machine only captures the packets in which it itself is the source or destination.

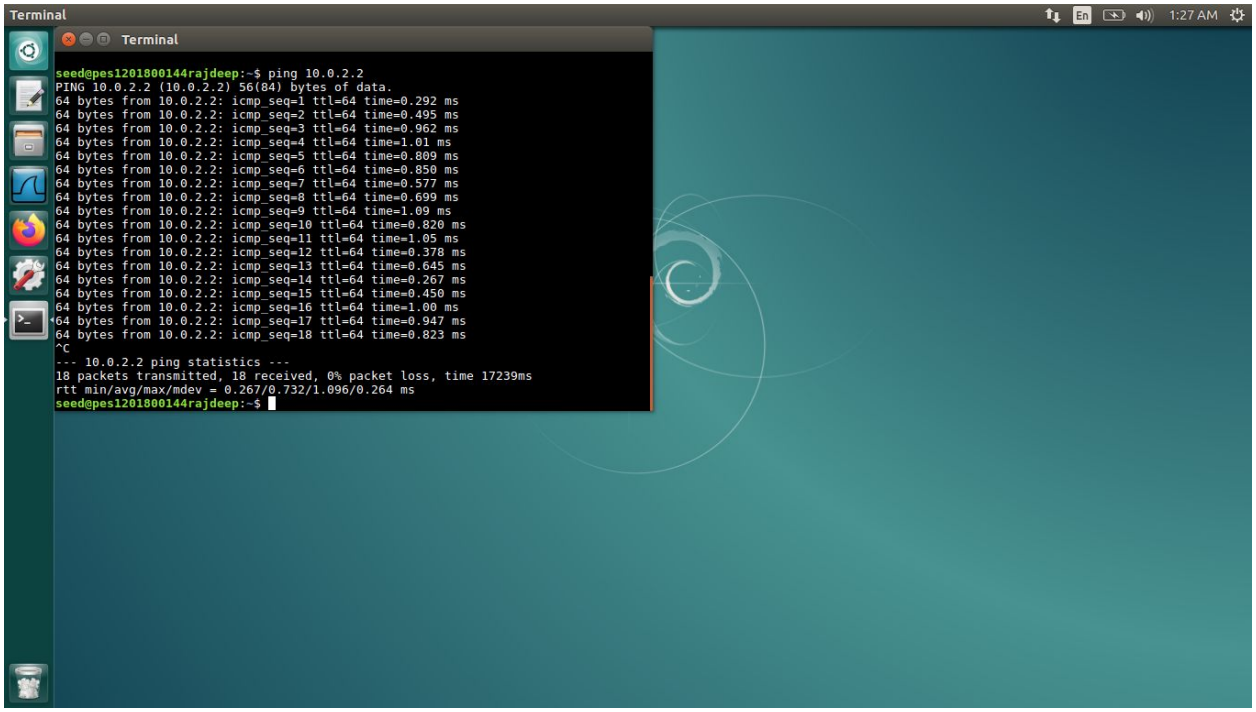
==========

TASK 1.2B

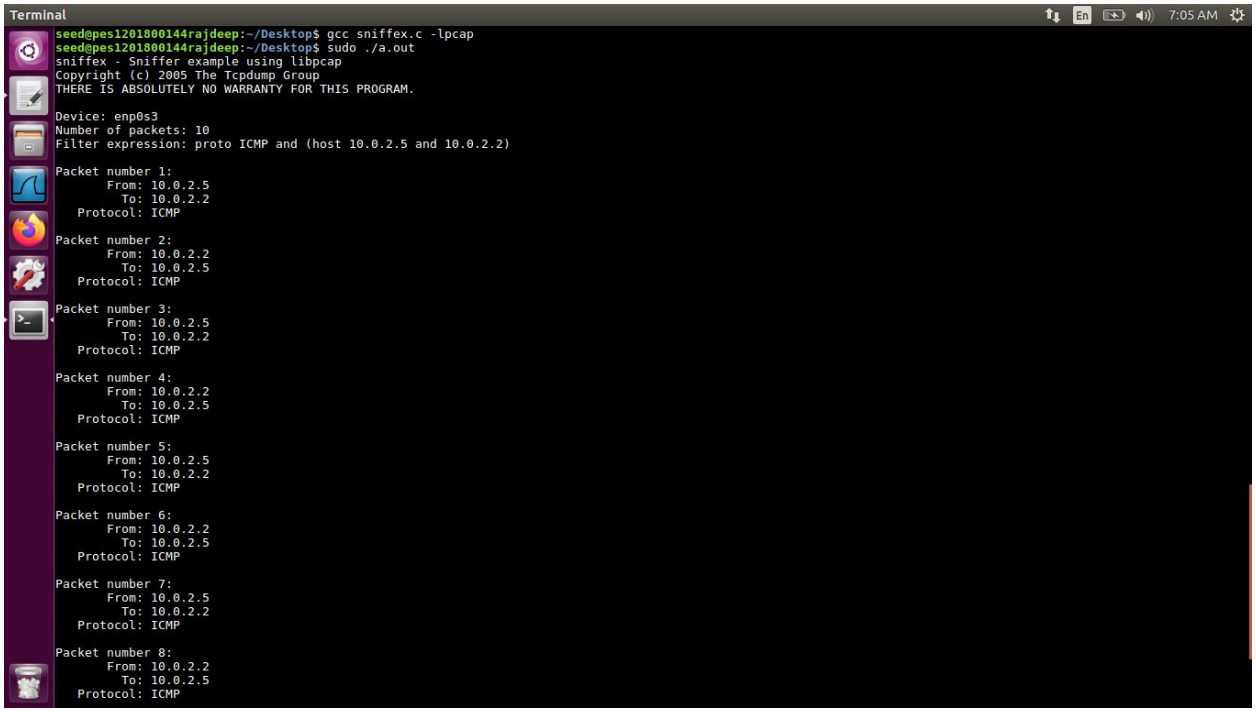
ICMP Connection:



Filter set to → “proto ICMP and (host 10.0.2.5 and 10.0.2.2)”



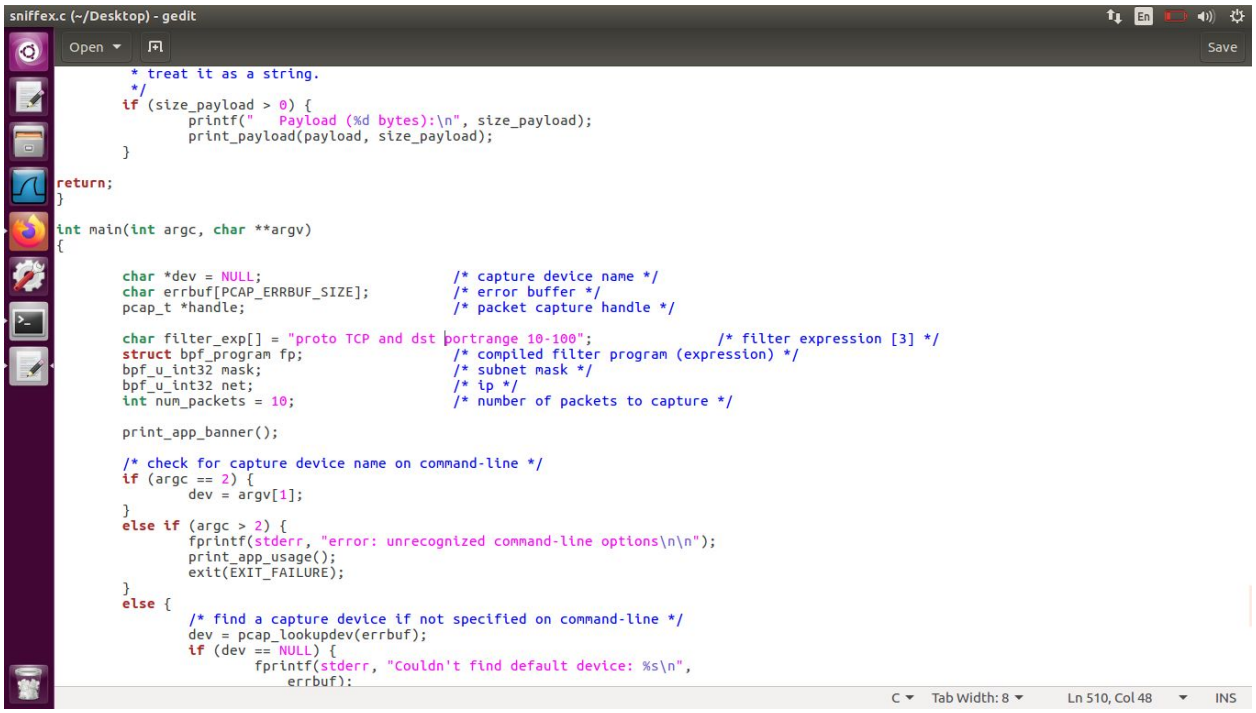
Victim machine(10.0.2.5) pings to 10.0.2.2



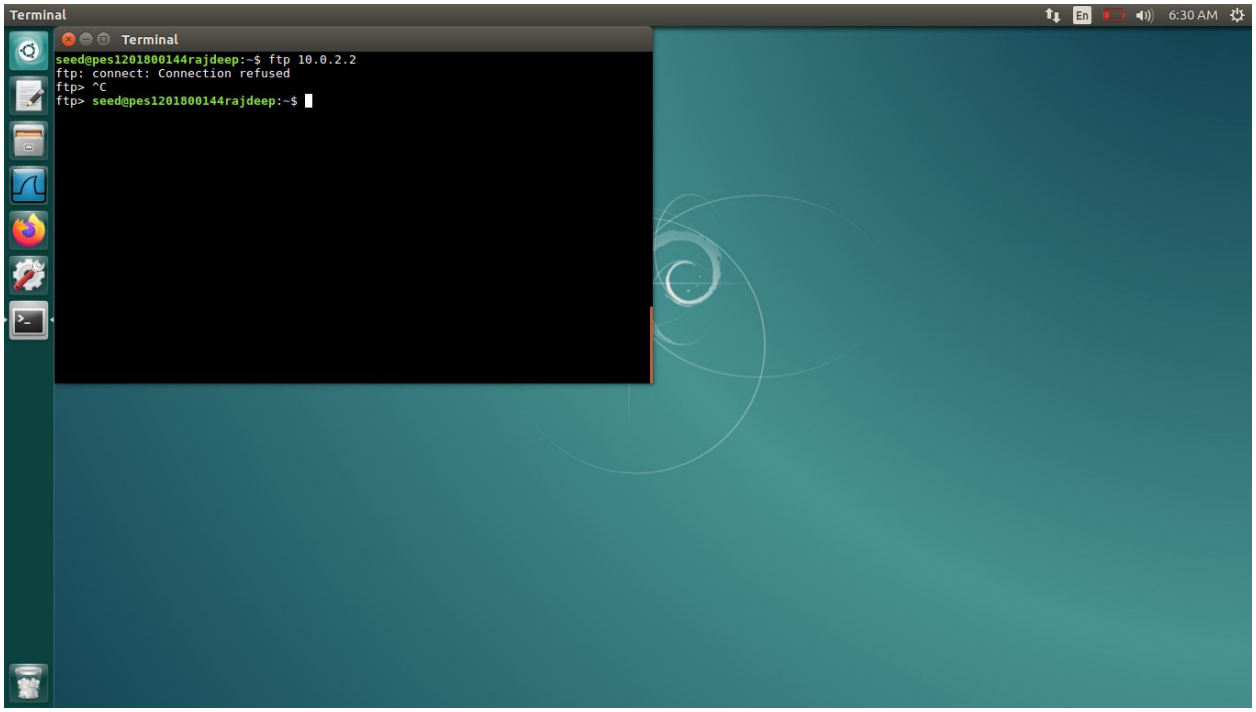
Attacker machine(10.0.2.9) captures ICMP packets from victim machine(10.0.2.5)

When the filter is set to “proto ICMP and (host 10.0.2.5 and 10.0.2.2)” then the attacker machine filters the sniffed packets and only receives the ICMP packets.

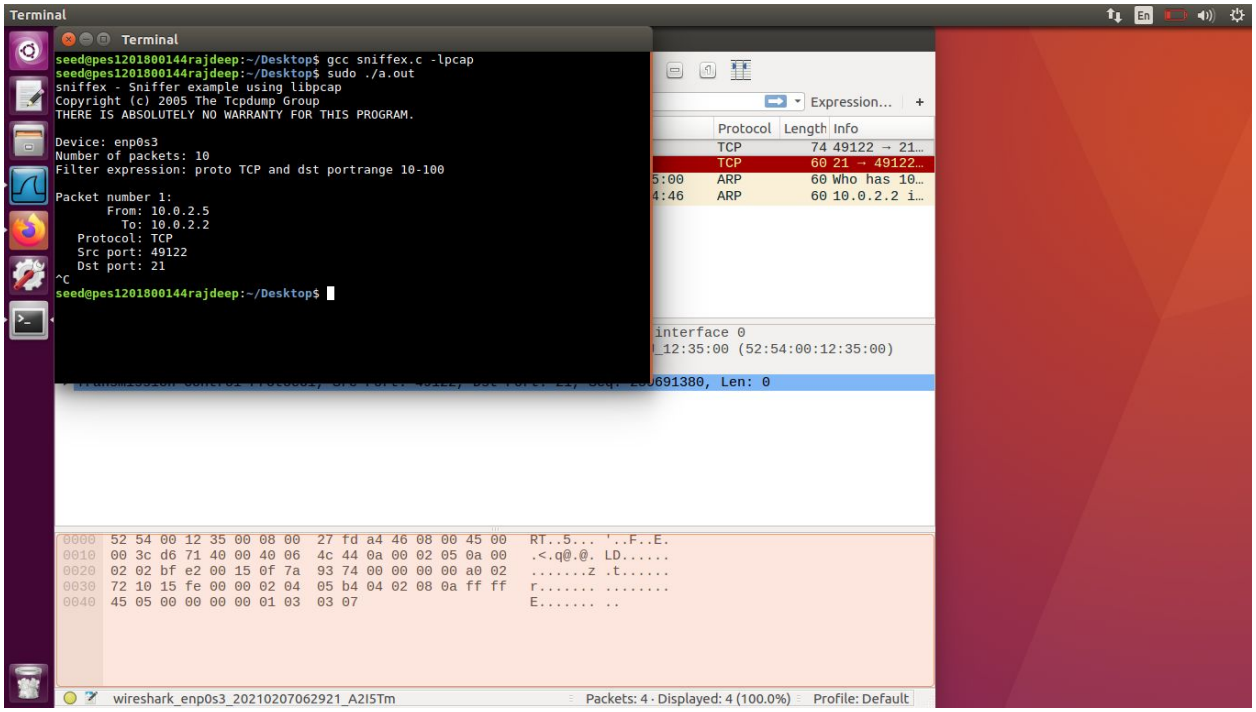
FTP Connection:



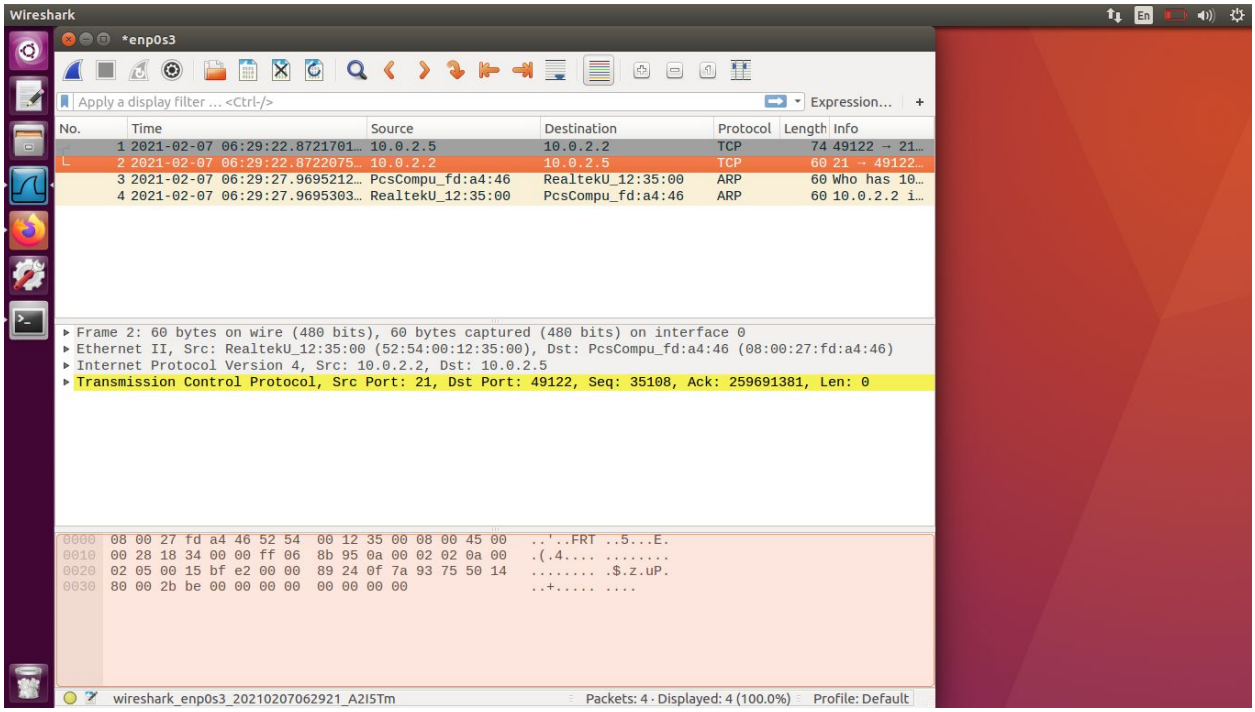
Filter set to → “proto TCP and dst portrange 10-100”



Victim machine(10.0.2.5) connecting through FTP protocol which uses TCP through port 21



Attacker machine(10.0.2.9) sniffs the FTP connection and captures username and password

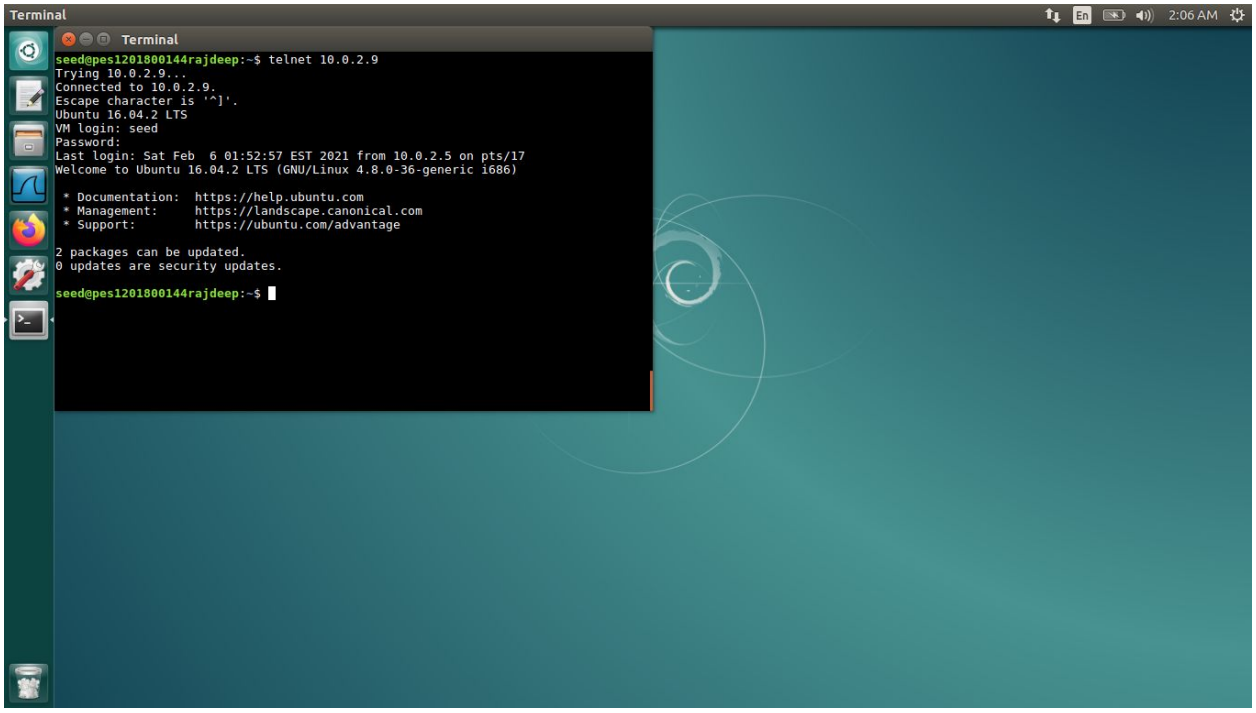


On wireshark in the attacker machine, the port number can be found as 21.

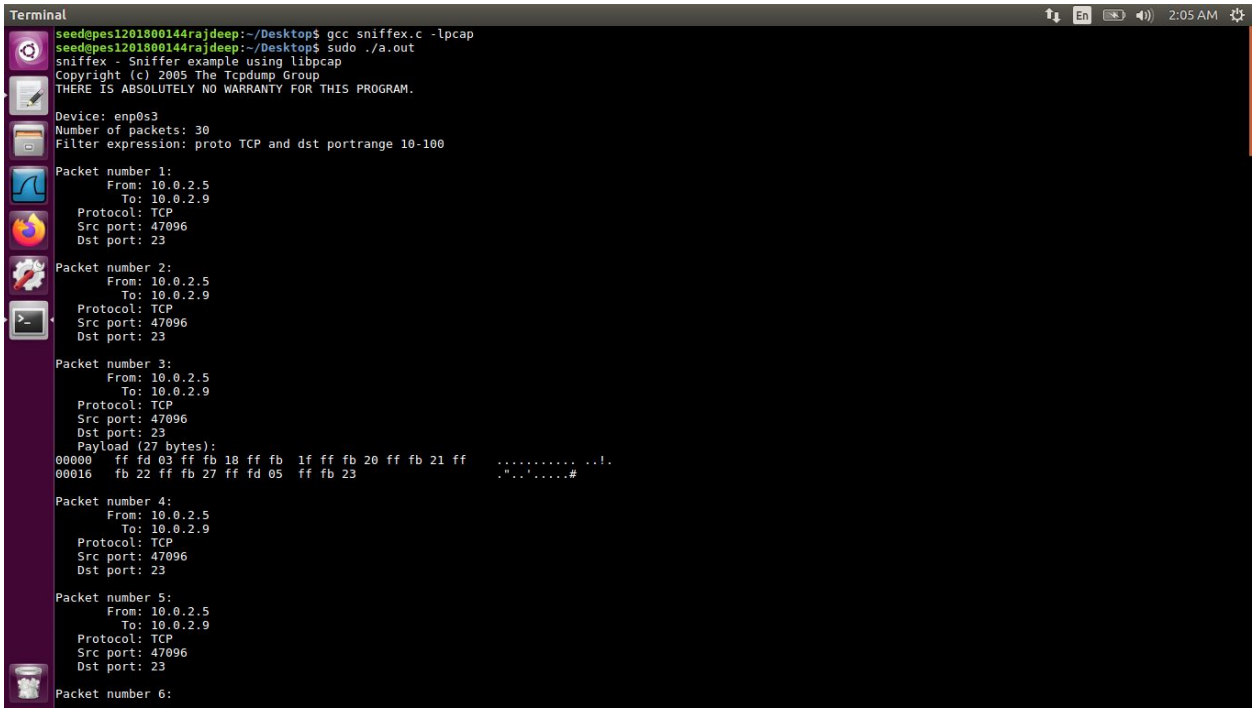
When the filter is set to “proto TCP and dst portrange 10-100” then the attacker machine filters the sniffed packets and only receives the TCP packets with port numbers in the range 10 to 100. These include FTP, telnet, SMTP, HTTP connections.

==========

TASK 1.2C



Victim machine(10.0.2.5) connecting to the telnet server



Attacker machine(10.0.2.9) sniffs the connection

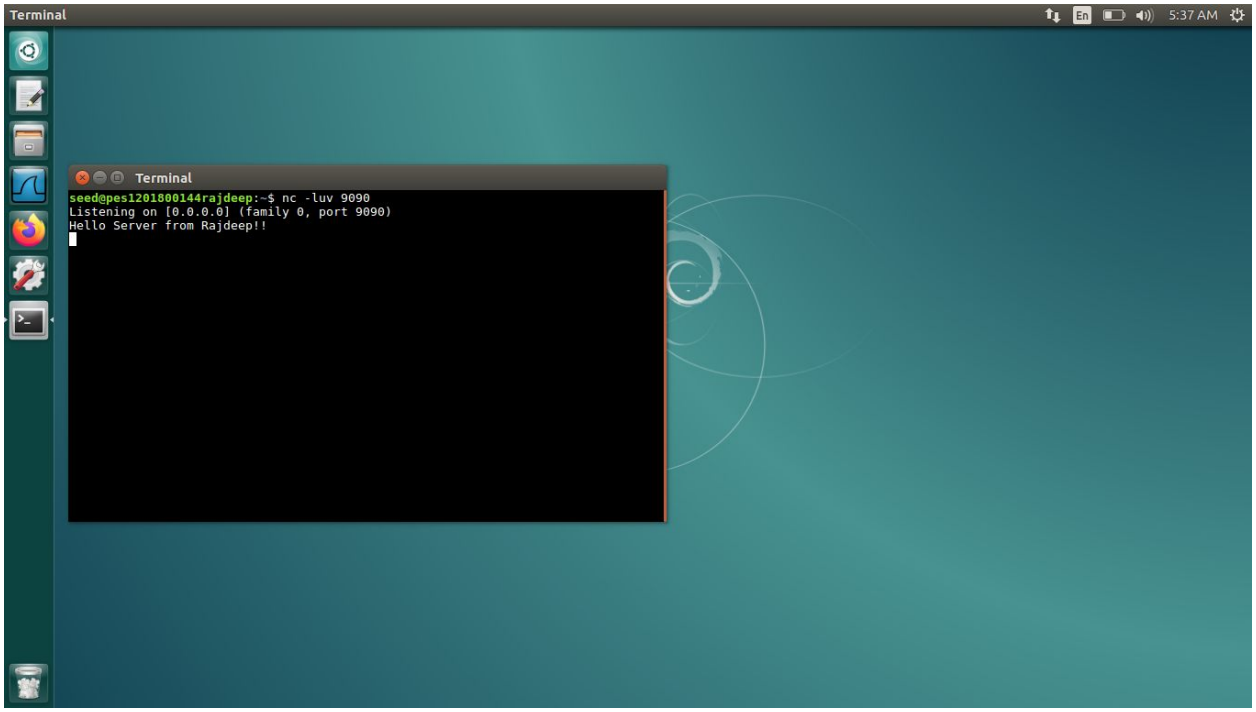
Further, on the terminal, we can find the username as ‘seed’ on the right side

Then we can find the password as ‘dees’ on scrolling down the terminal

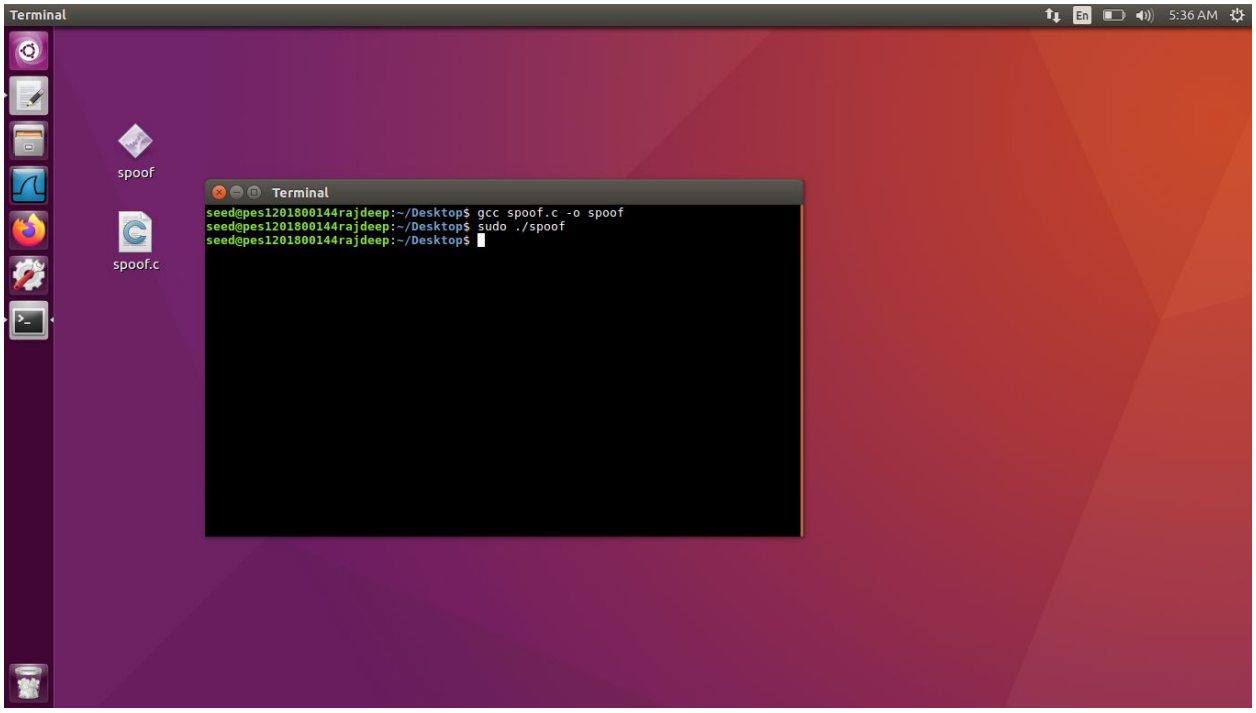
Since telnet connection runs on TCP port 23, all the traffic is sniffed by the code and the username and password is displayed in the terminal.

TASK 2

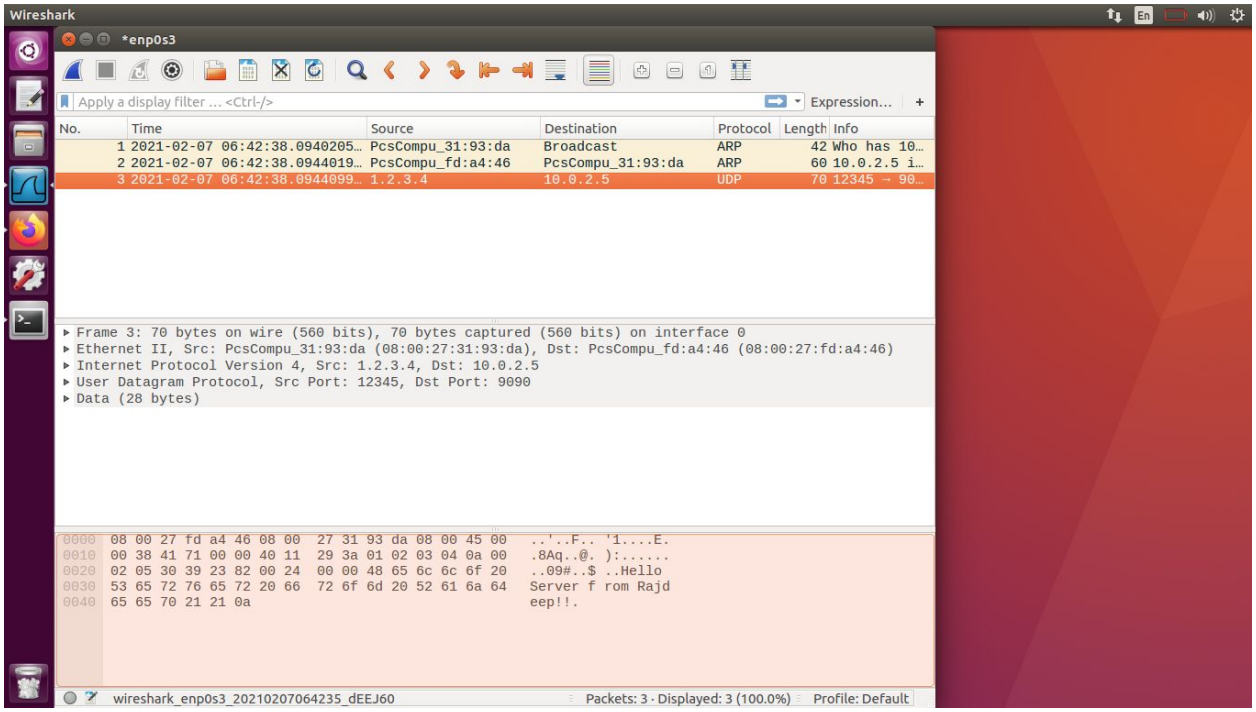
The spoof.c full code



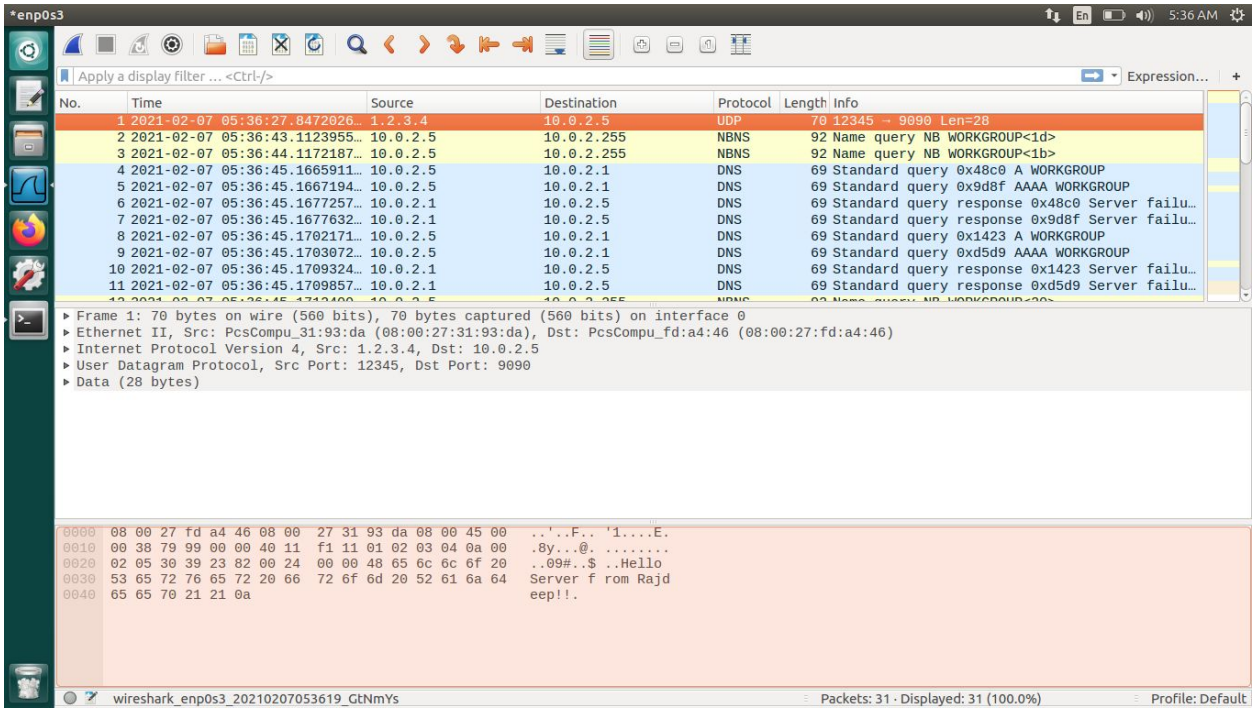
Victim machine listens on port 9090



Attacker machine executing the spoof.c code



Wireshark on attacker machine



Wireshark on victim machine

The server machine(10.0.2.5) listens using netcat command on port 9090. The attacker machine(10.0.2.9) sends a spoofed UDP packet to the victim machine(10.0.2.5) from the IP address 1.2.3.4. This is also shown using wireshark screenshots.

==========