Computer Network Security
Lab 1
Packet sniffing and spoofing

-PES1201801948
-Bharath S Bhambore
-Section H

Lab Setup :

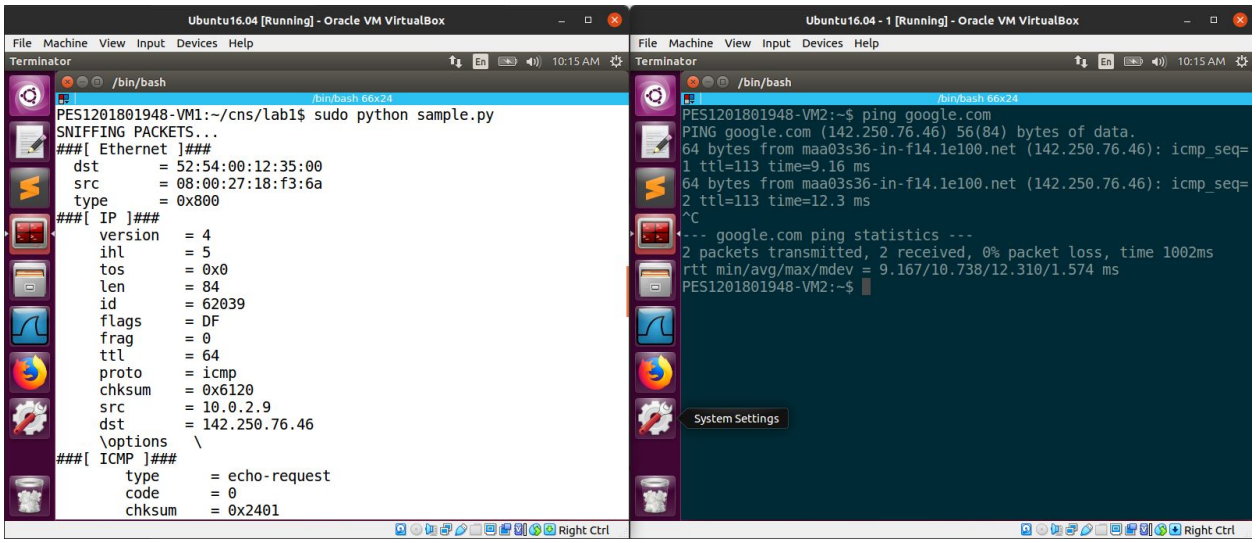
Attacker Machine :
Machine Name : Ubuntu 16.04 [White Terminal]
IP : 10.0.2.8

Victim Machine :
Machine Name : Ubuntu 16.04 -1 [Blue Terminal]
IP : 10.0.2.9

Task 1 : Sniffing Packets

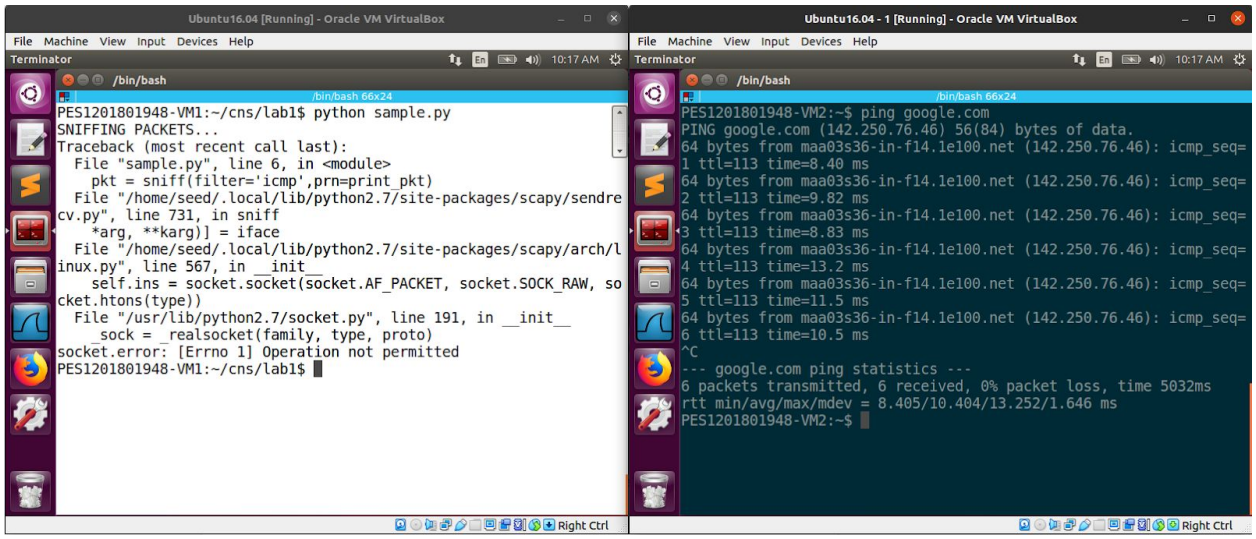
2.1.1 Task 1.1 : Sniffing packets using scapy

Command is run on the attacker machine [10.0.2.8] to sniff the ICMP request packets of the victim machine [10.0.2.9]on the network



As we can see in the attacker terminal [Left], it was able to capture the ICMP ping requests of the victim machine.

Running without Sudo :

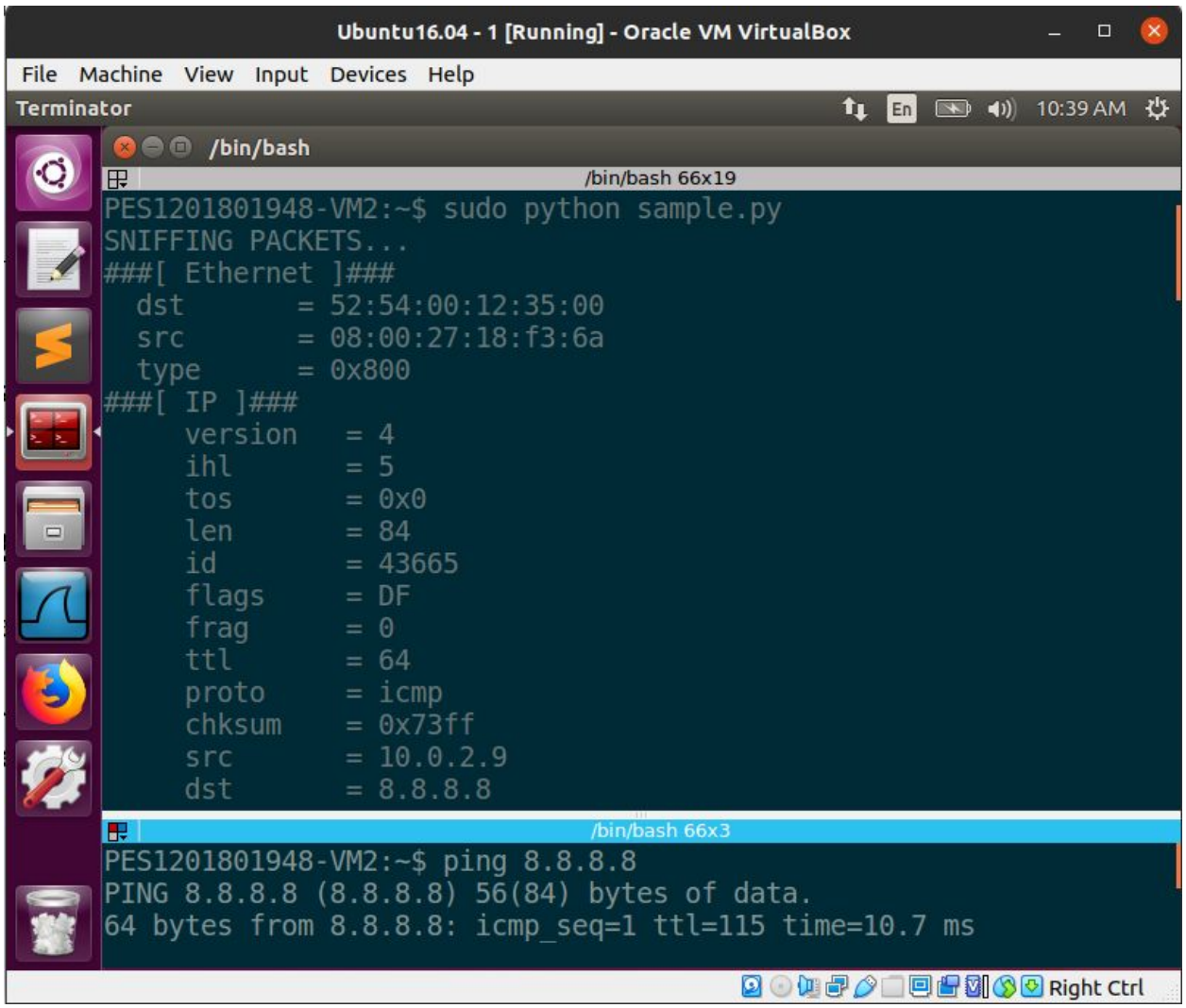


Error : Operation not permitted
Sniffing requires root privileges therefore the socket itself is not initialized, hence why it failed to capture the icmp packets

2.1.2 Task 1.2 Capturing ICMP, TCP packet and Subnet

2.1.2.1 Capture only the ICMP packet

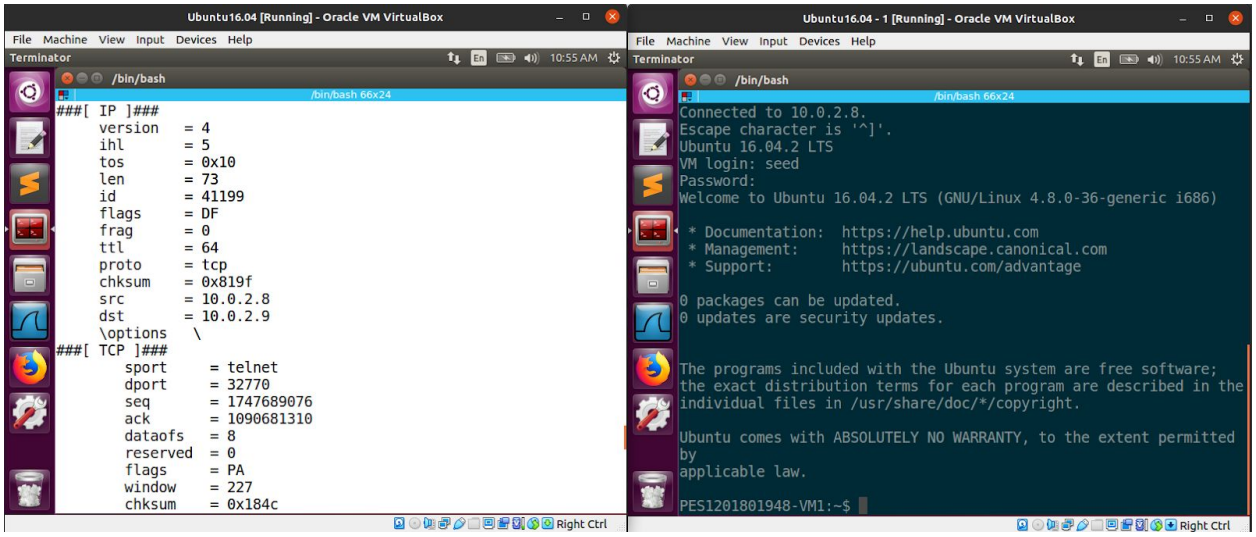
sample.py is run with the ICMP packet filter, ping is also run on the same machine



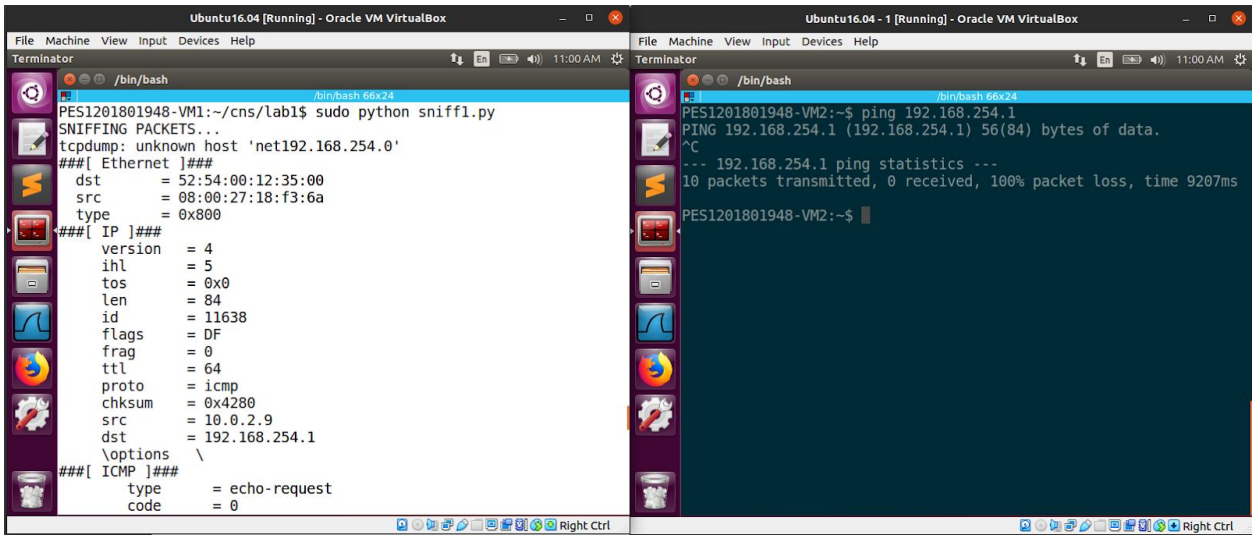
2.1.2.2 Capture any TCP packet that comes from a particular IP and with a destination port number 23

Telnet request uses TCP packets on port 23, therefore it is run on the Victim Machine [10.0.2.9], while the python script is run on the attacker machine [10.0.2.8] to sniff out the TCP packets.

Telnet is used to virtually access another machine and provide a 2 way channel between them.

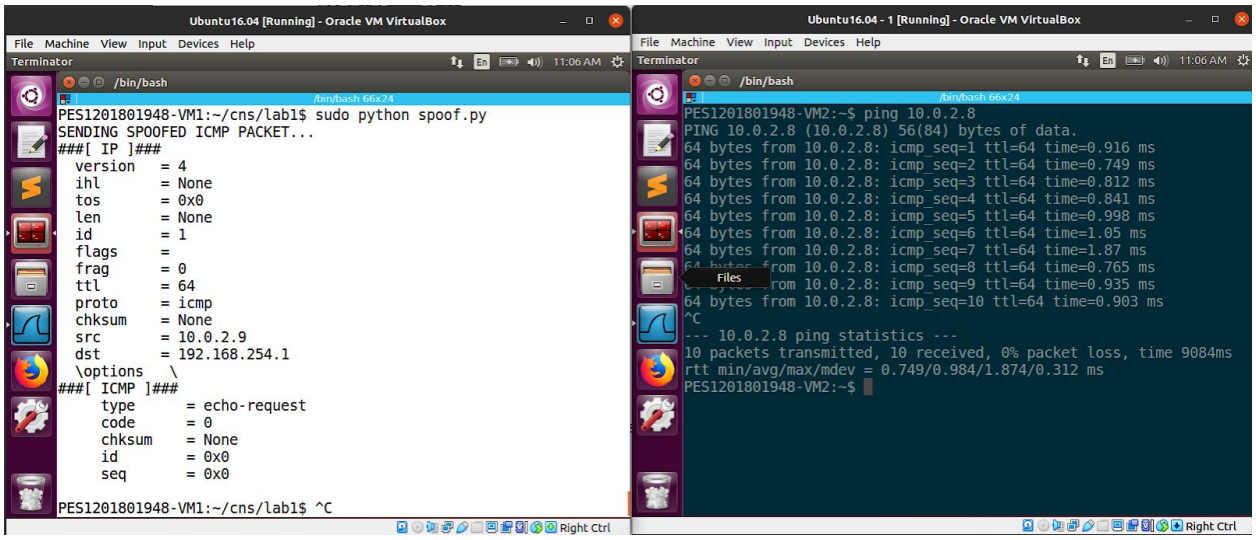


2.1.2.2.1 iii) Capture packets comes from or to go to a particular subnet

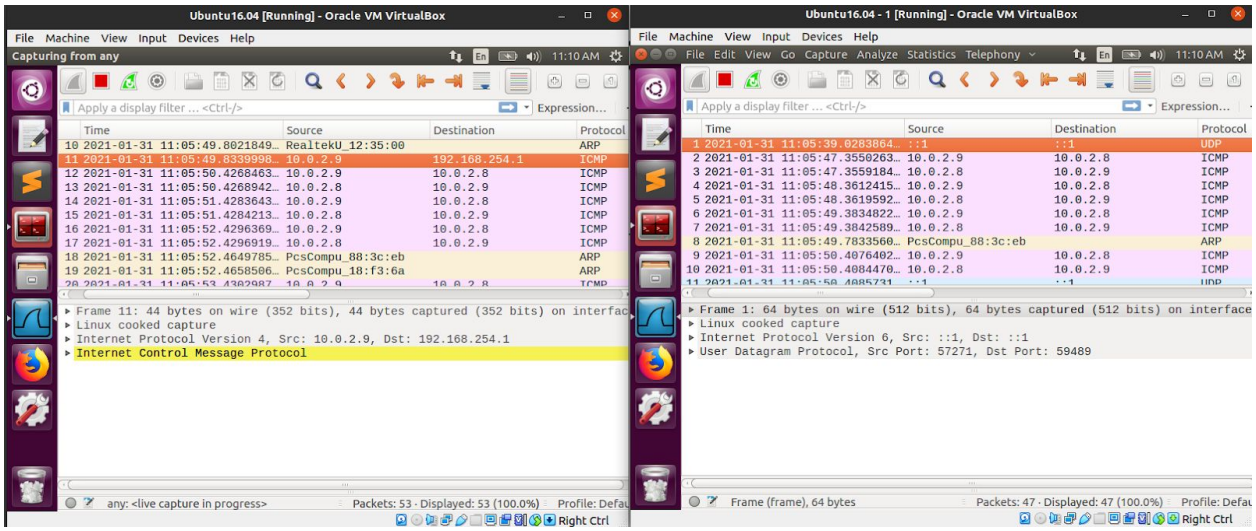


192.168.254.1 is the router's IP address that we ping from the victim machine, while the attacker machine is able to capture the packets transferred in the subnet specified.

2.1.3 Task 2: Spoofing

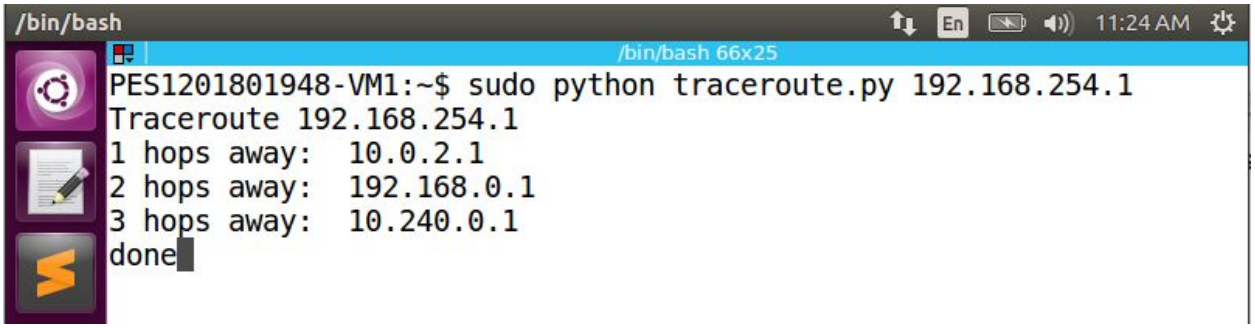


Wireshark capture of both machines :



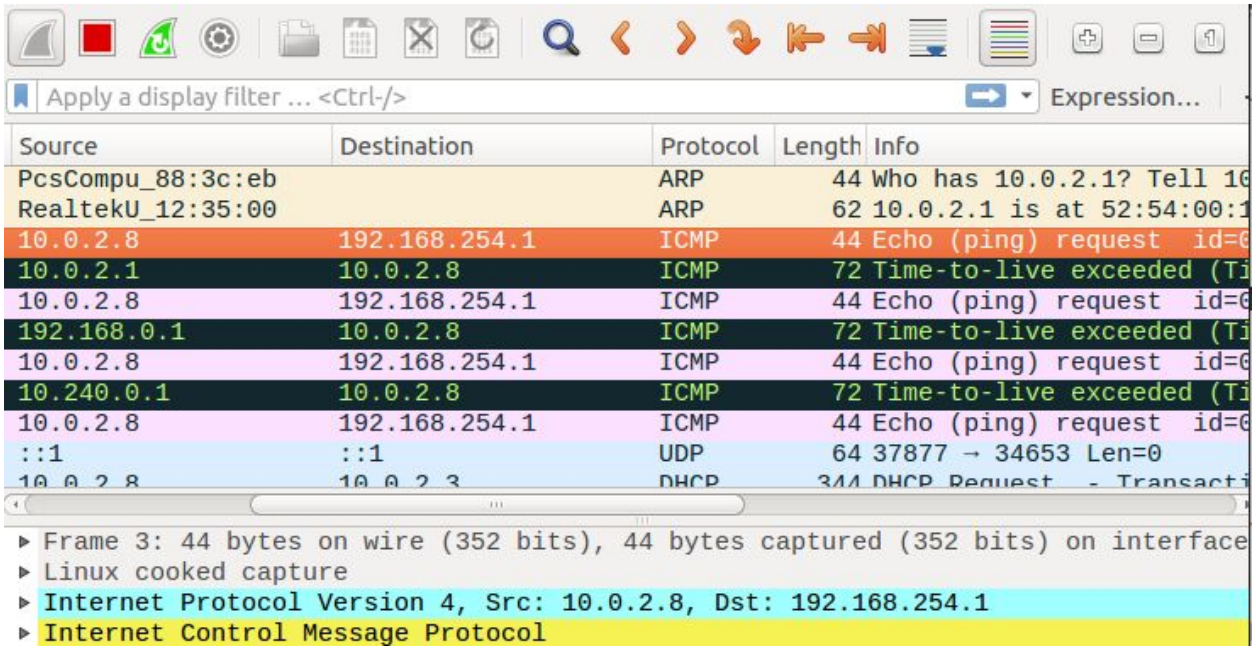
We can see that the destination is successfully spoofed in this attack.

2.1.4 Task 3: Traceroute

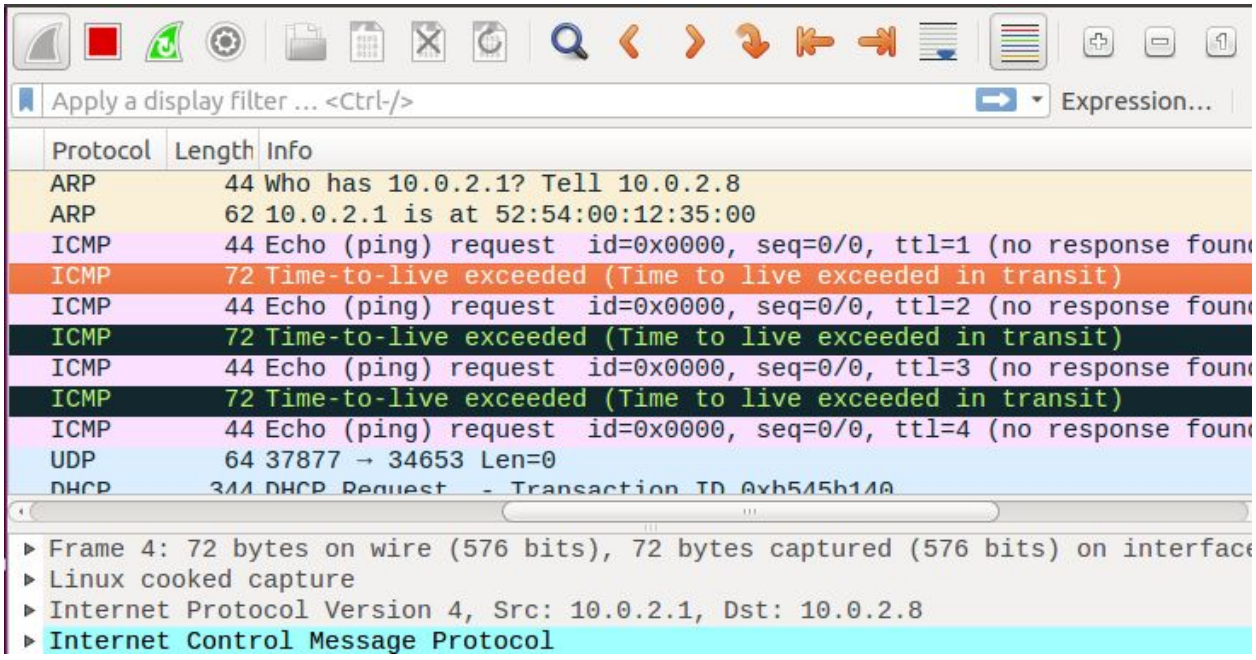


Traceroute of the router is found using the above script

Wireshark capture :



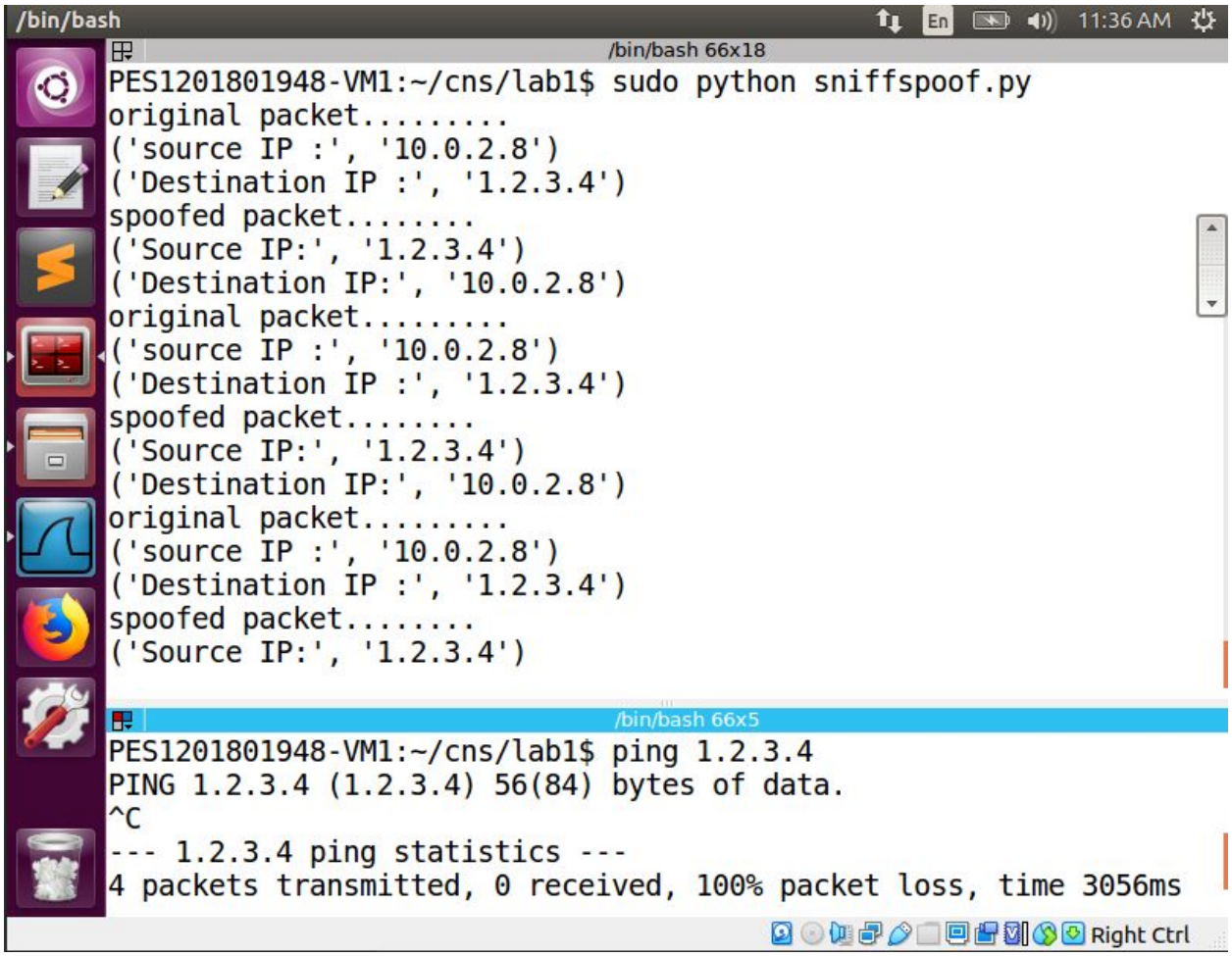
TTL exceeded response from router



As we can see, the TTL of the icmp packets is increasing

2.1.5 Task 4: Sniffing and-then Spoofing

Running in the same machine itself



We can also sniff and spoof packets sent from the victim machine instead of testing it on the same machine only.

As shown below,

The attack runs successfully implying that the victim, even though it pinged a non-existent IP address, the attacker was able to send spoofed ICMP packets.