COMPUTER NETWORKS SECURITY LABORATORY

WEEK 1

BY: RAJDEEP SENGUPTA

SRN: PES1201800144

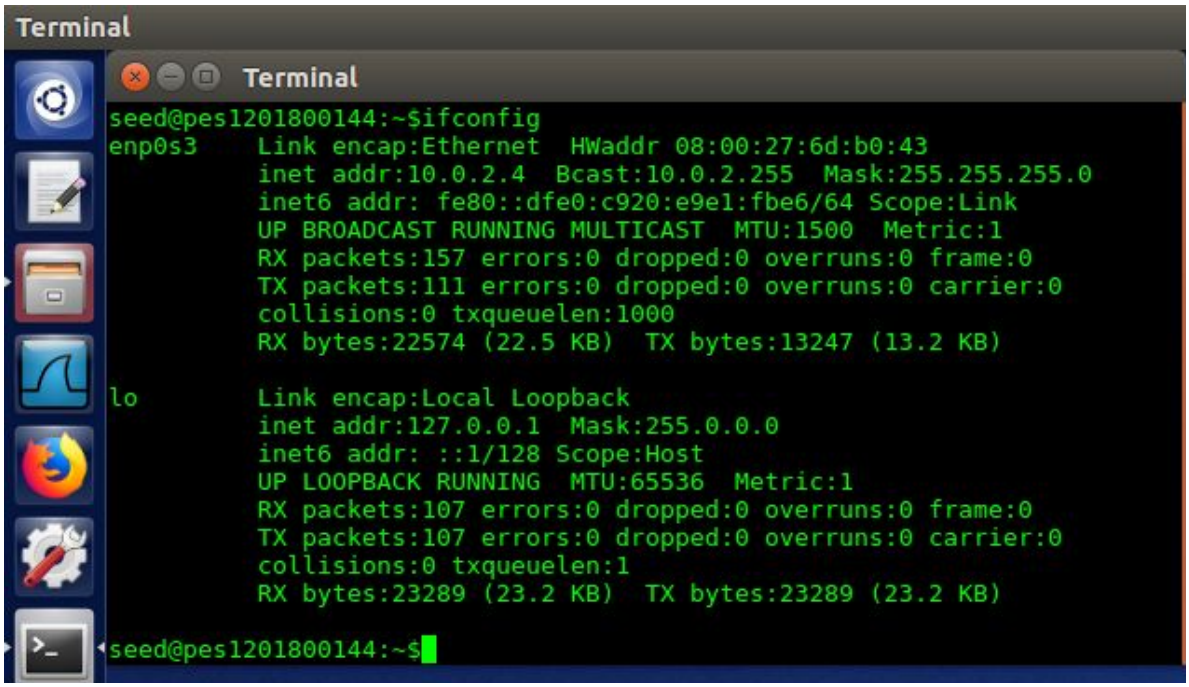
SECTION: C

NOTE: Please find my SRN 'PES1201800144' in all the screenshots attached below. Also find these screenshots in the attached folder in the 'attacker machine screenshots' and 'victim machine screenshots' directories.

MY CONFIGURATIONS:

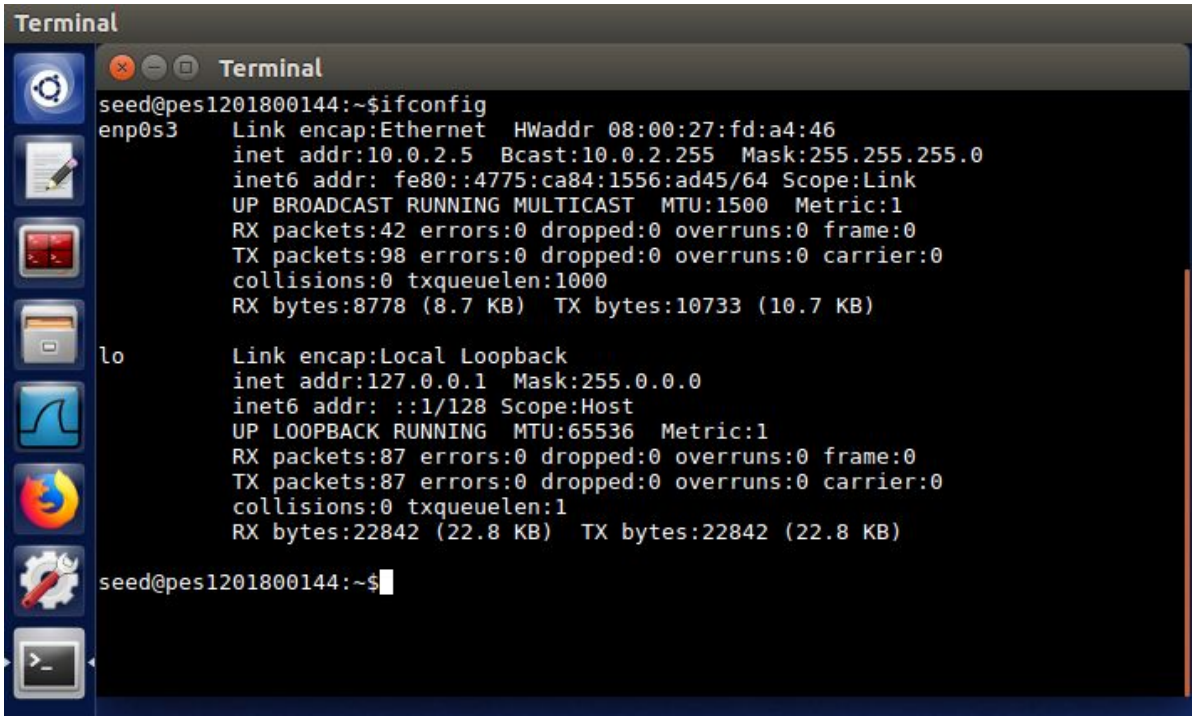
VM1 (Attacker)

IP Address: 10.0.2.4 WITH GREEN TERMINAL TEXT



VM2 (Victim)

IP Address: 10.0.2.5 WITH WHITE TERMINAL TEXT



TASKS

TASK 2.1.1

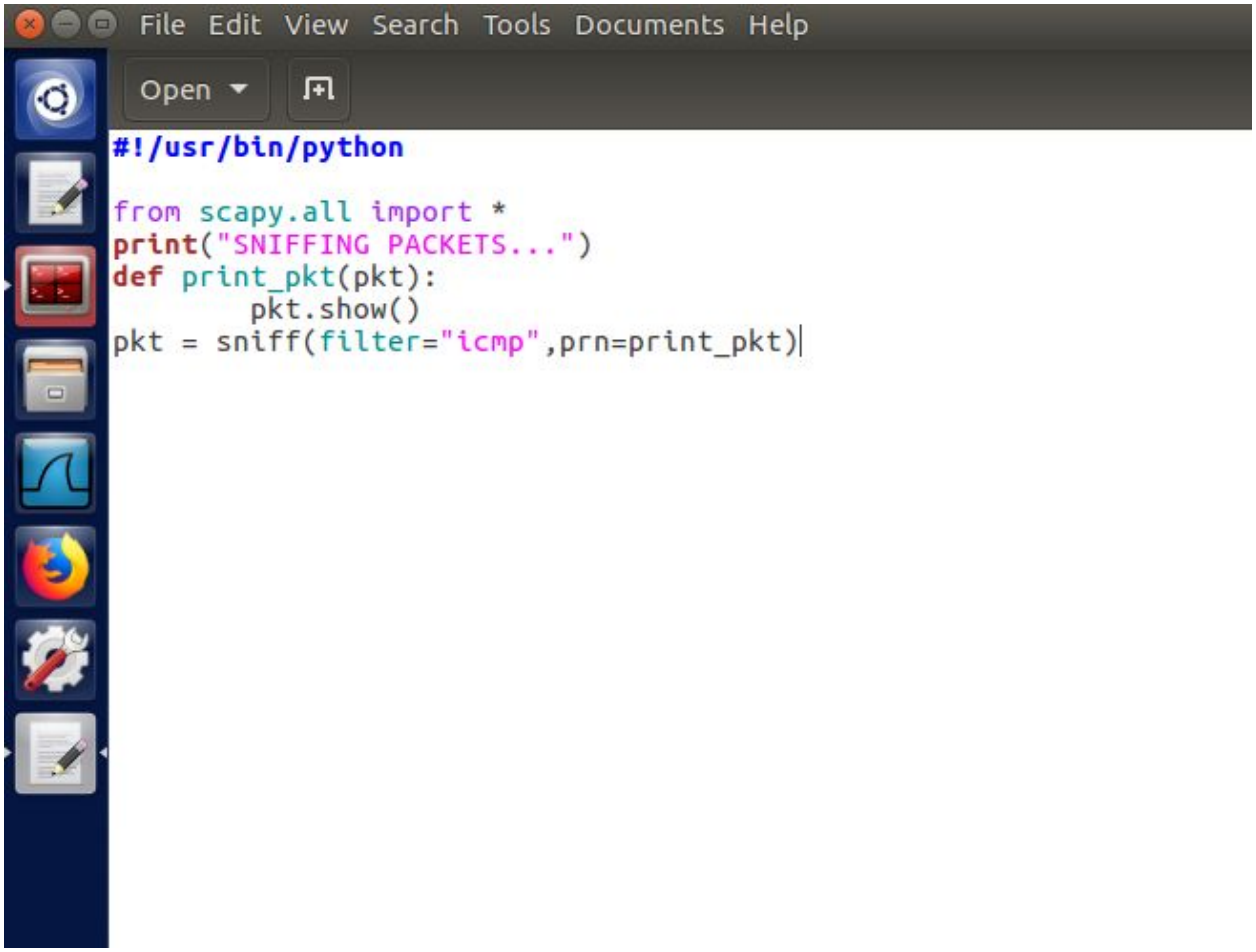


Figure: Code to capture ICMP packets

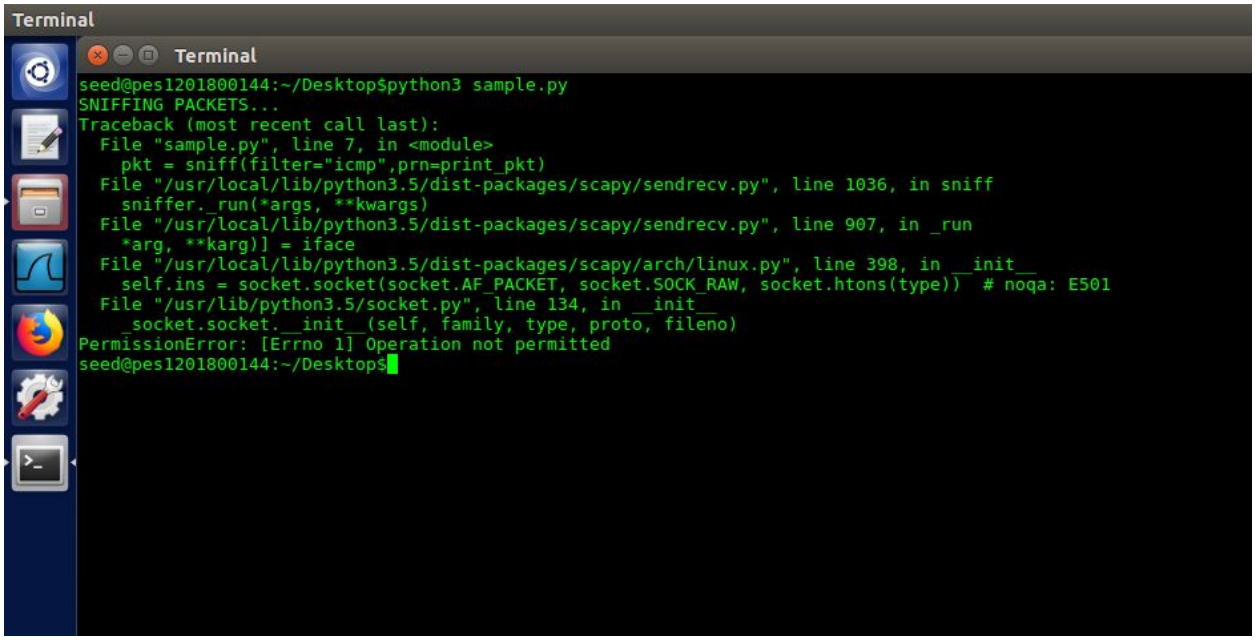


Figure: Running the code without sudo

TASK 2.1.2.1

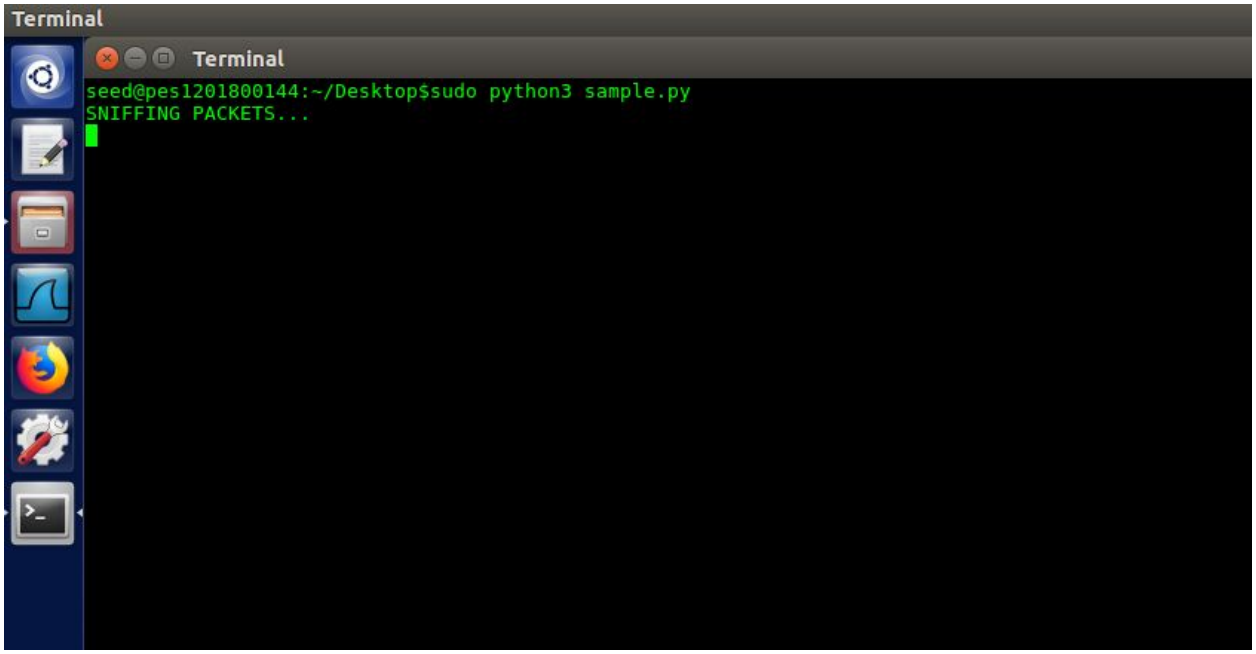


Figure: Running with sudo (root permission)

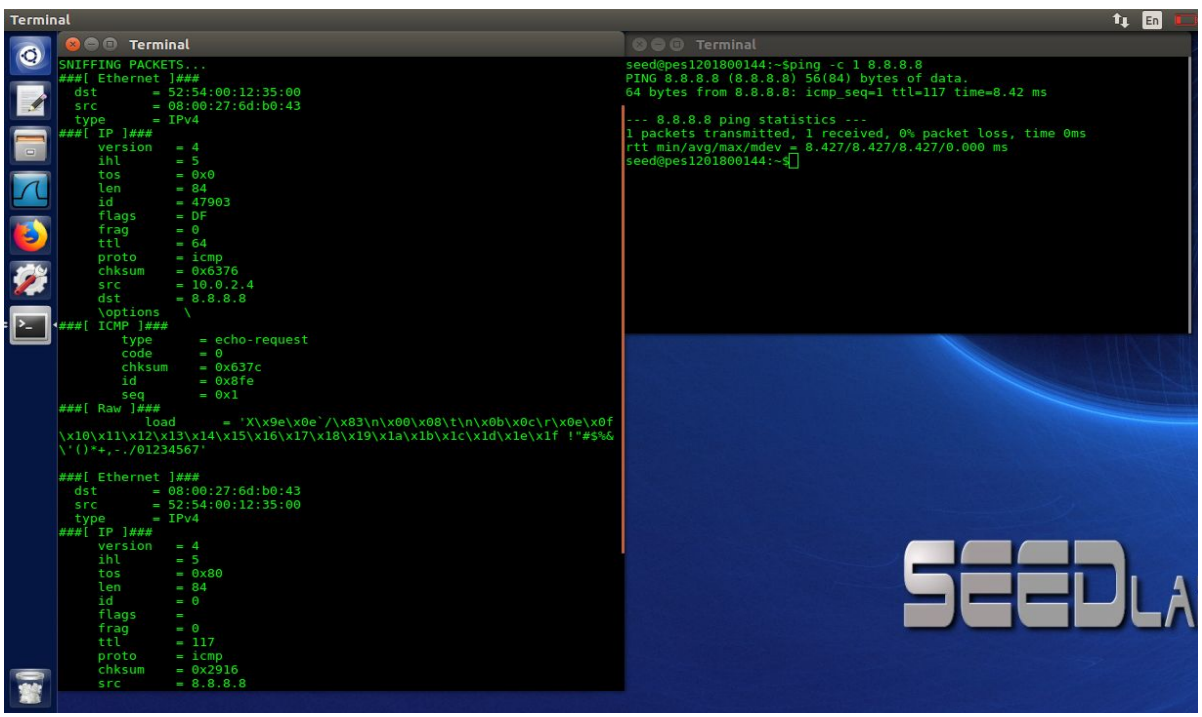


Figure: ICMP packets captured by sniffer program

TASK 2.1.2.2

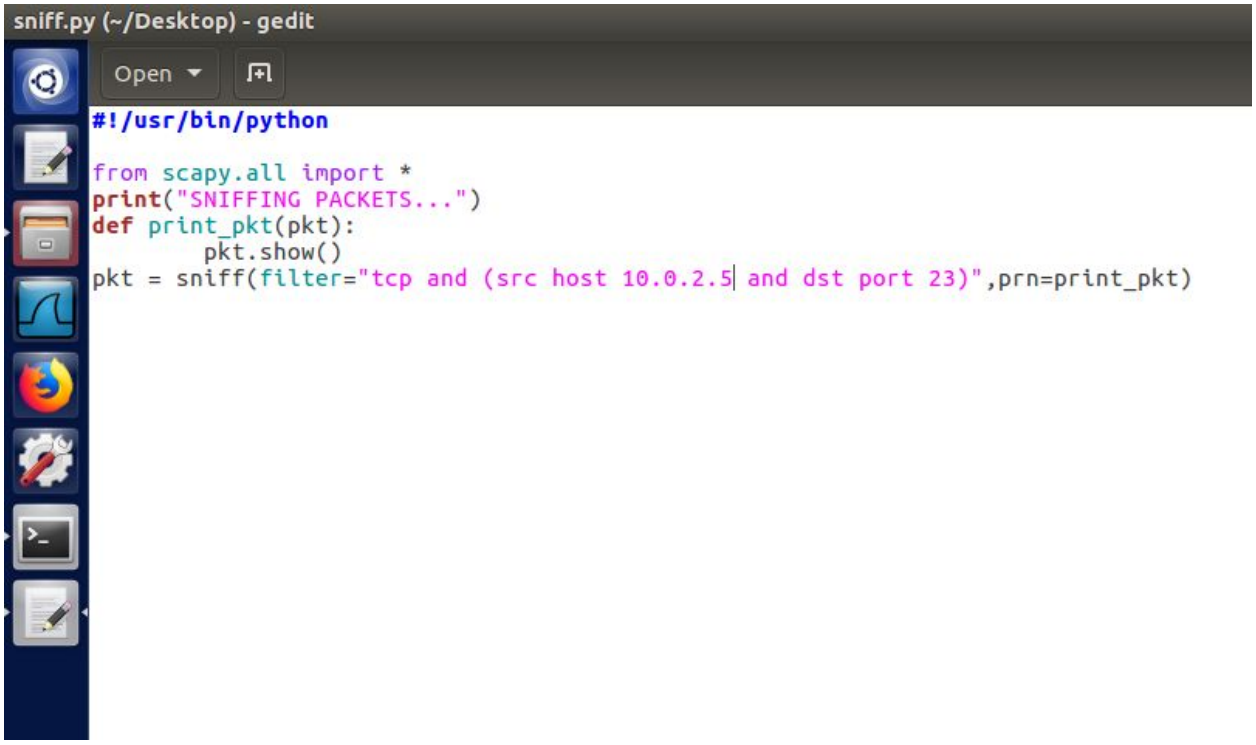


Figure: TCP sniffer code

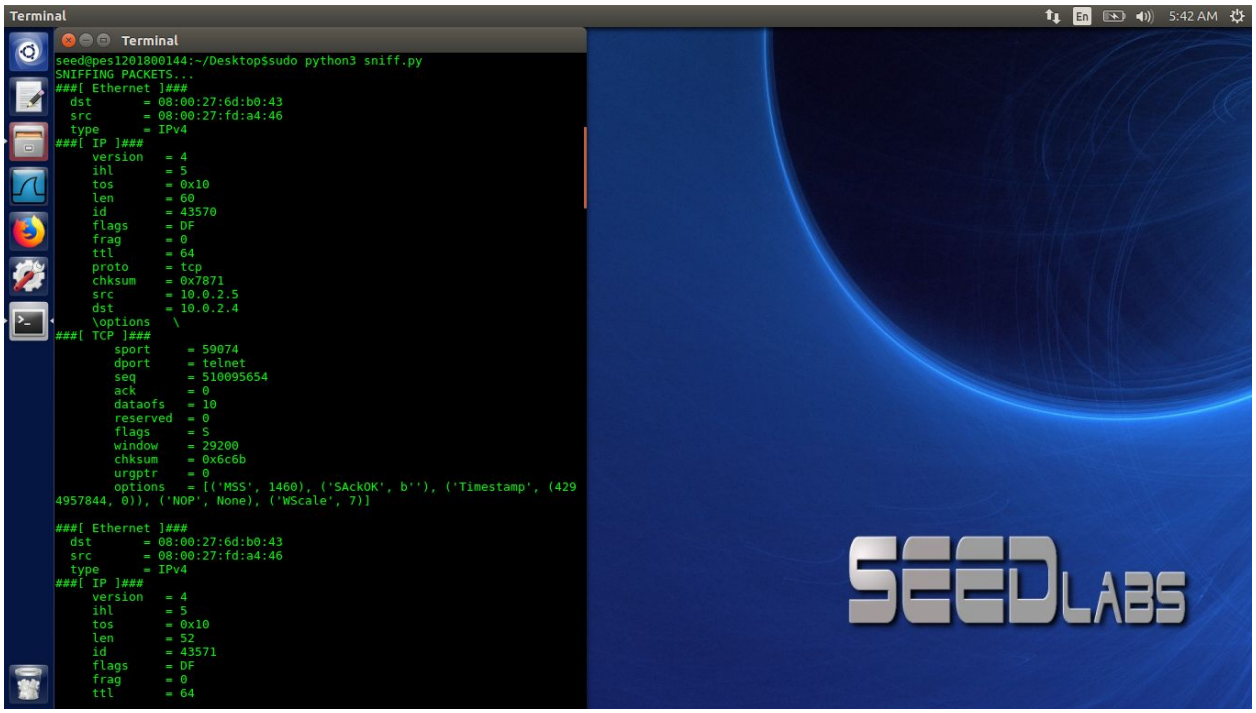


Figure: TCP packets captured by sniffer program

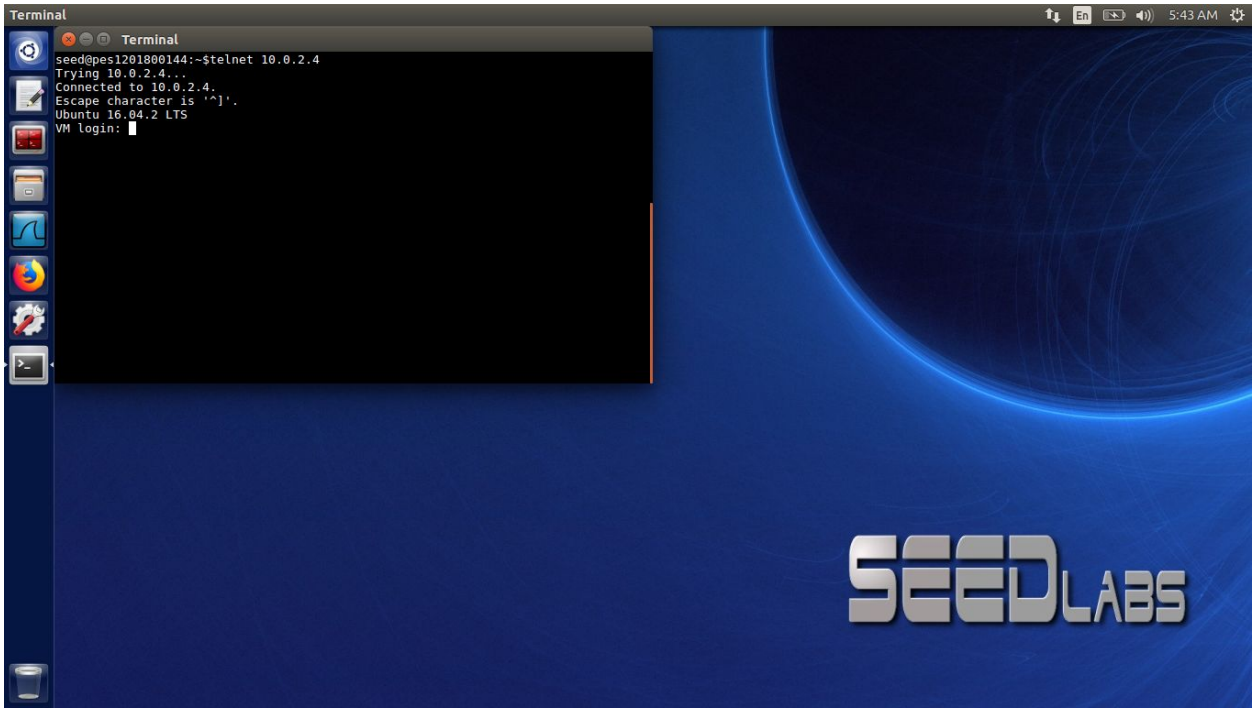


Figure: Telnet connecting from victim machine

TASK 2.1.2.2.1

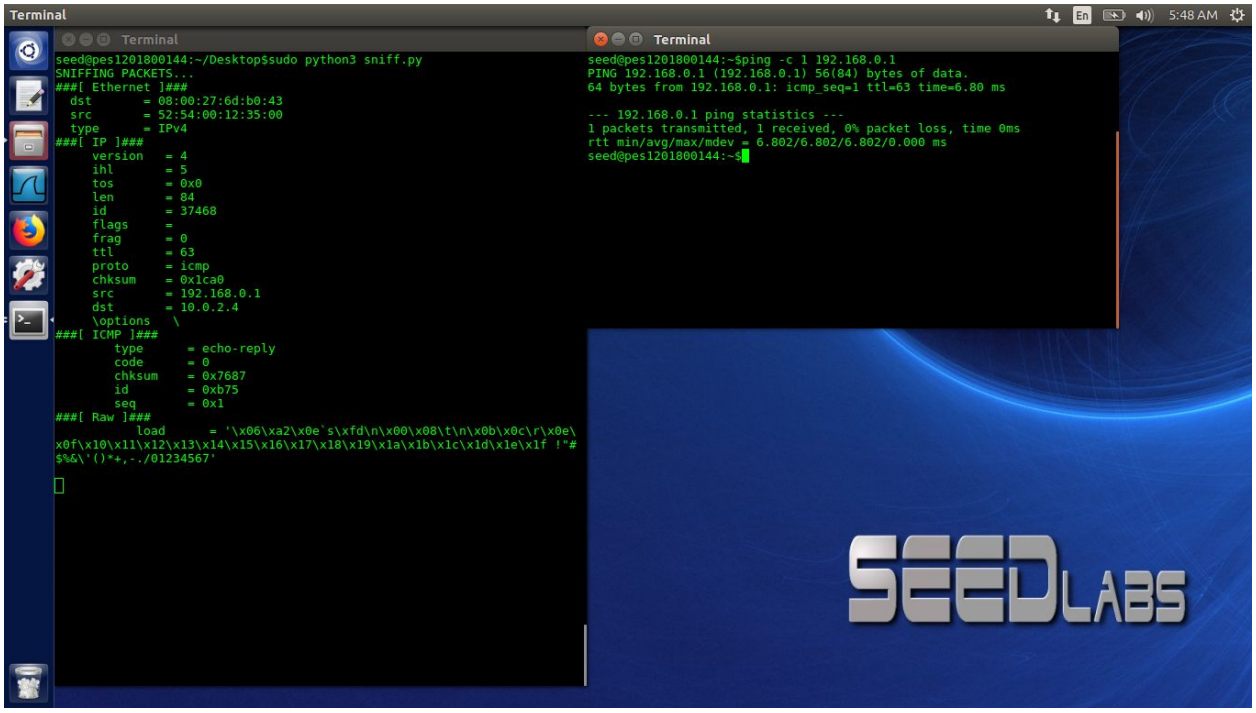


Figure: Capturing packets coming or going from a particular subnet

TASK 2.1.3

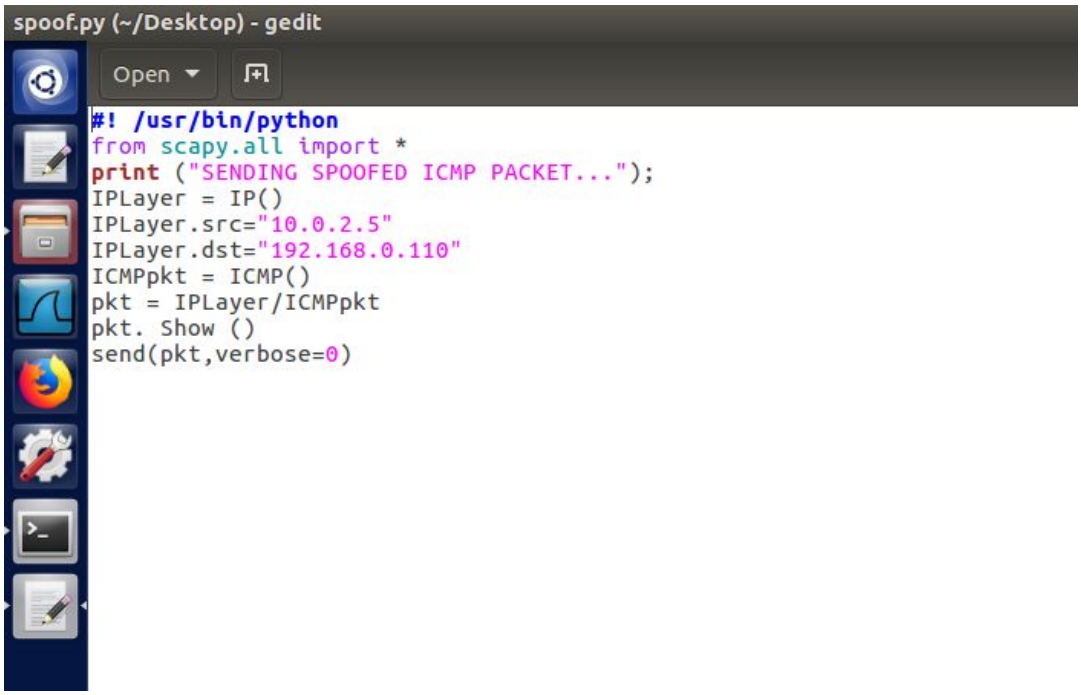


Figure: Code to spoof ICMP packets

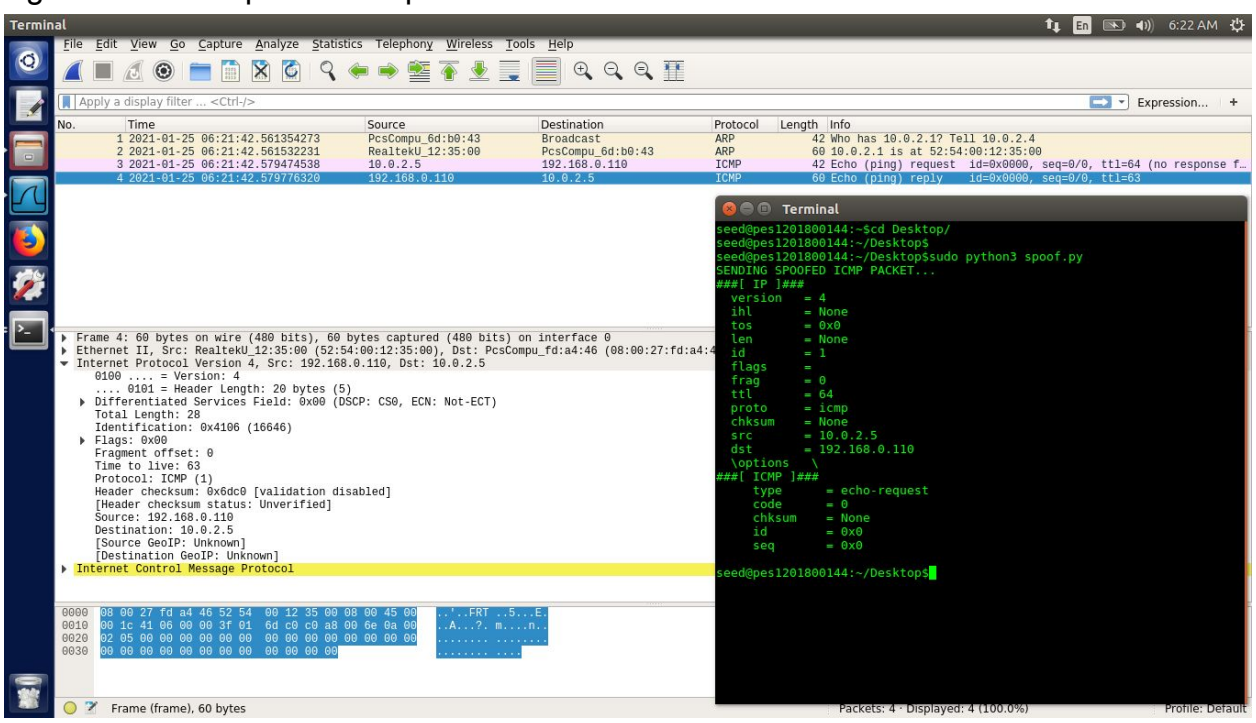
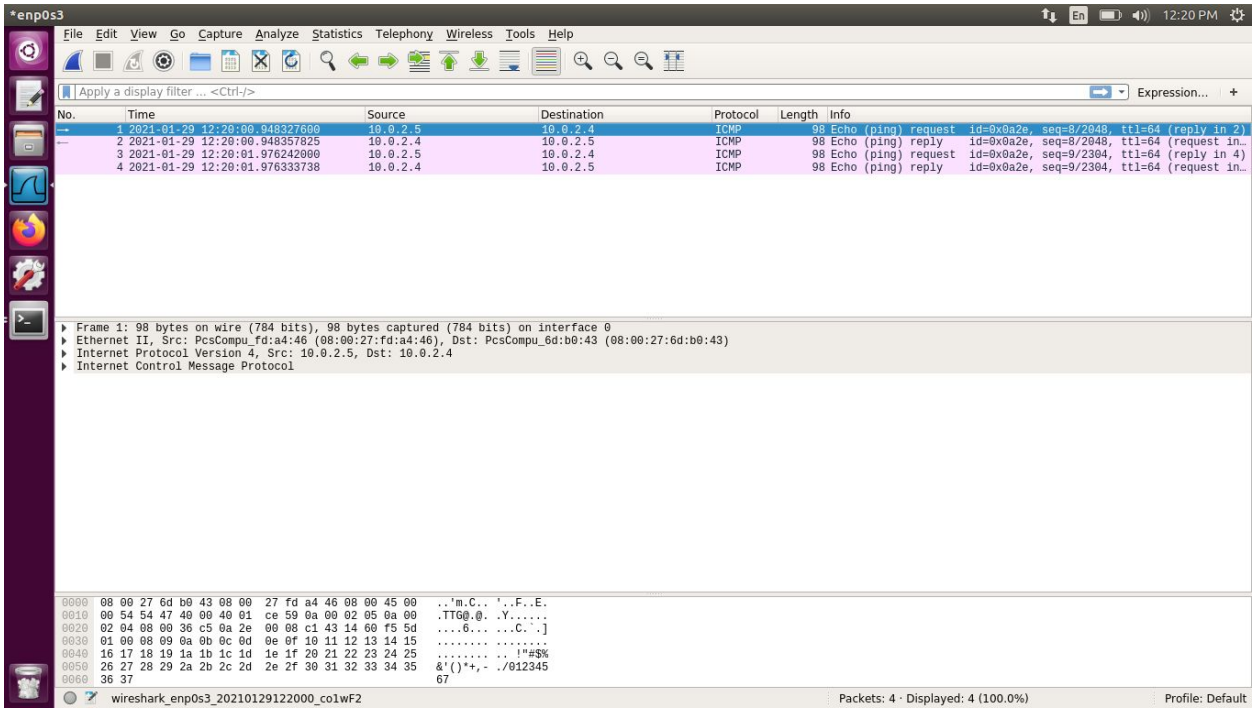


Figure: spoofing ICMP packets



Pinging to attacker 10.0.2.4

TASK 2.1.4

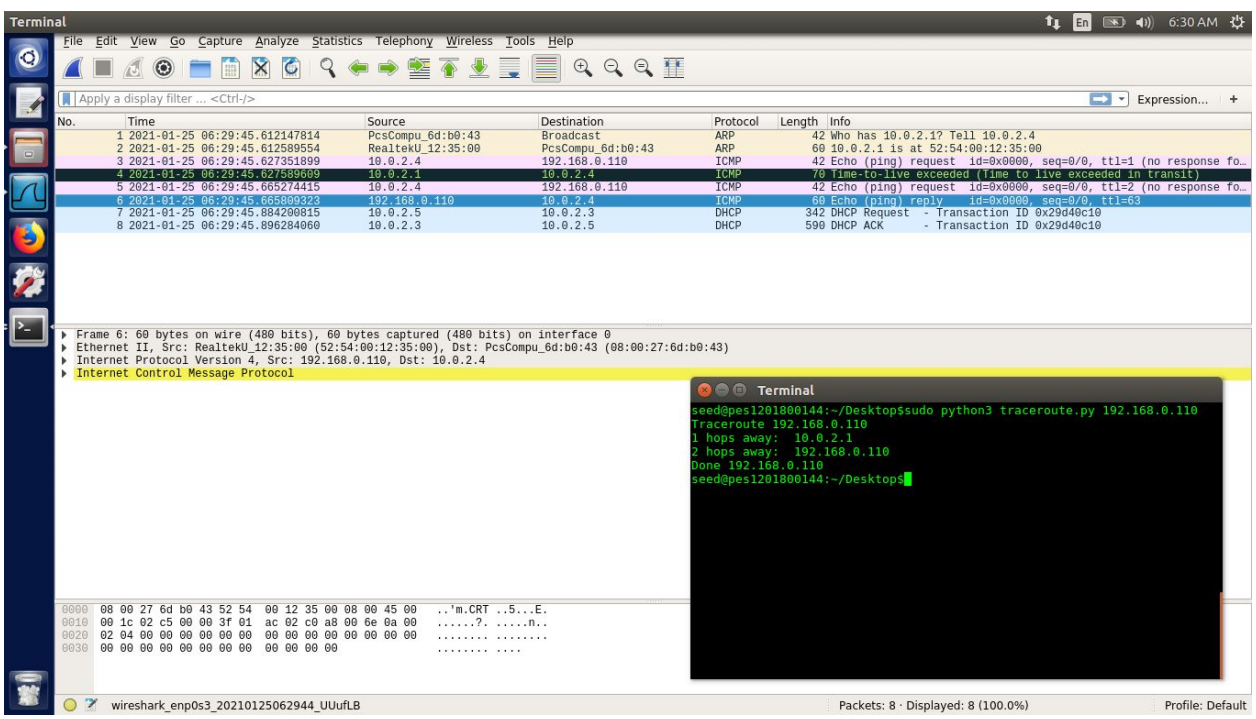


Figure: Capturing packets through wireshark and performing traceroute. TTL=1 and TTL=2 packets can be seen clearly. Also Time-To-Live exceeded response packet can also be seen clearly.

TASK 2.1.5

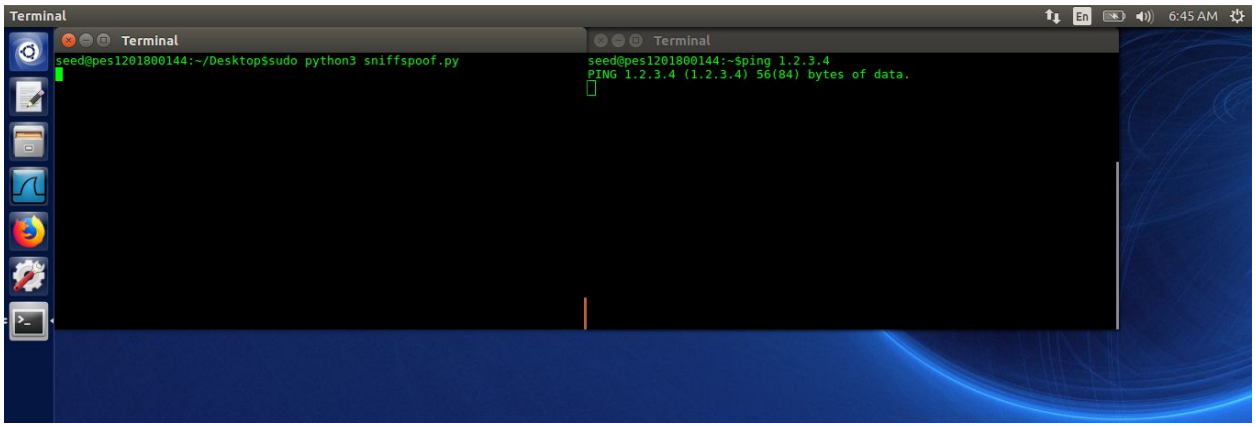


Figure: Spoofing an 1.2.3.4 from same machine(attacker machine)

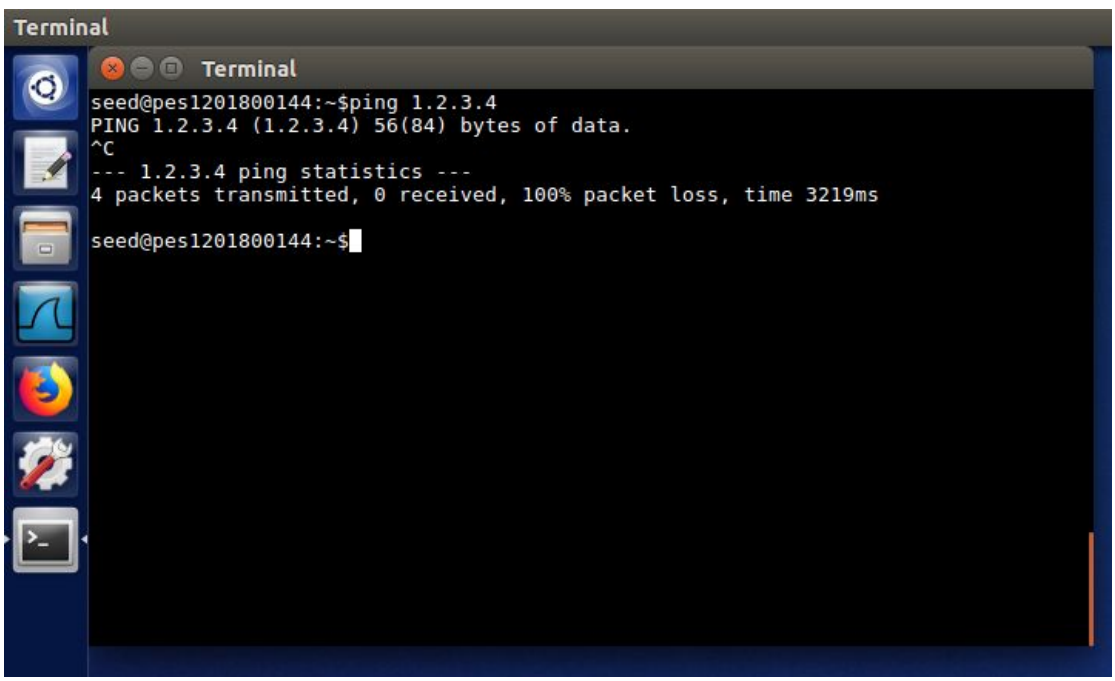


Figure: pinging 1.2.3.4 from victim machine without running spoofing code on attacker machine

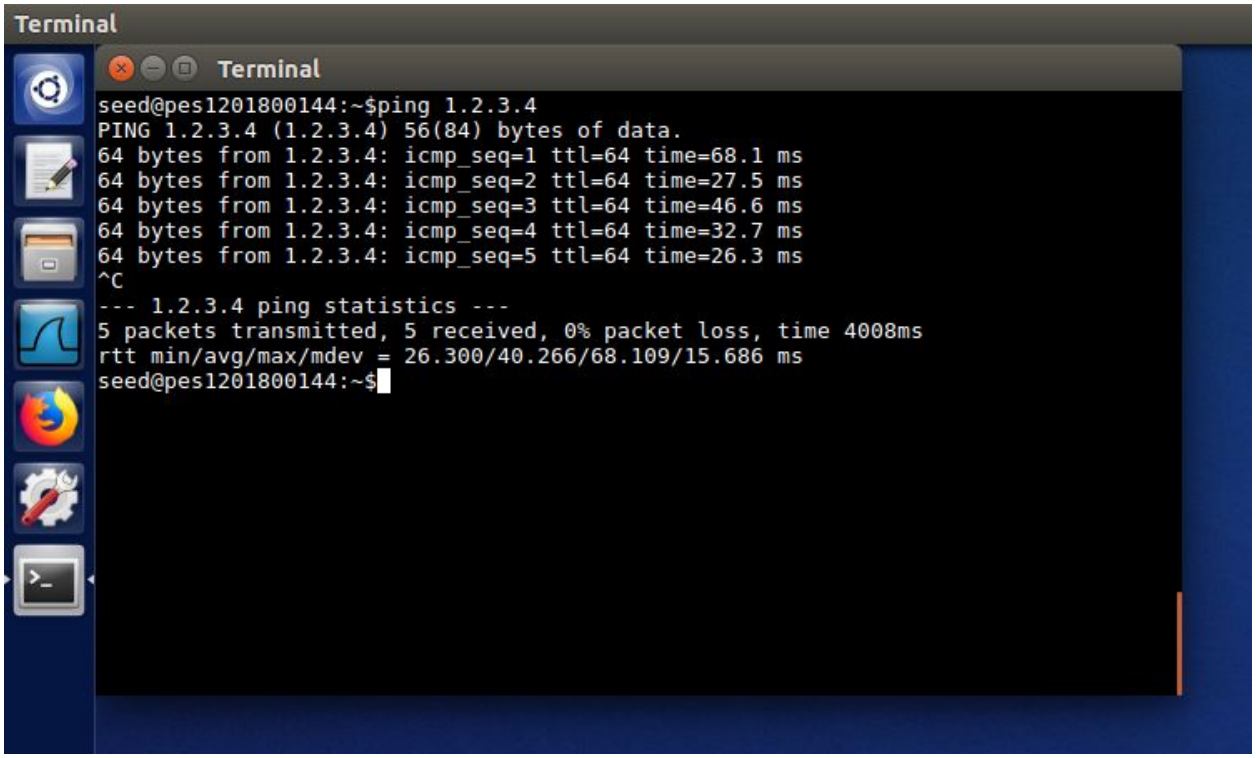
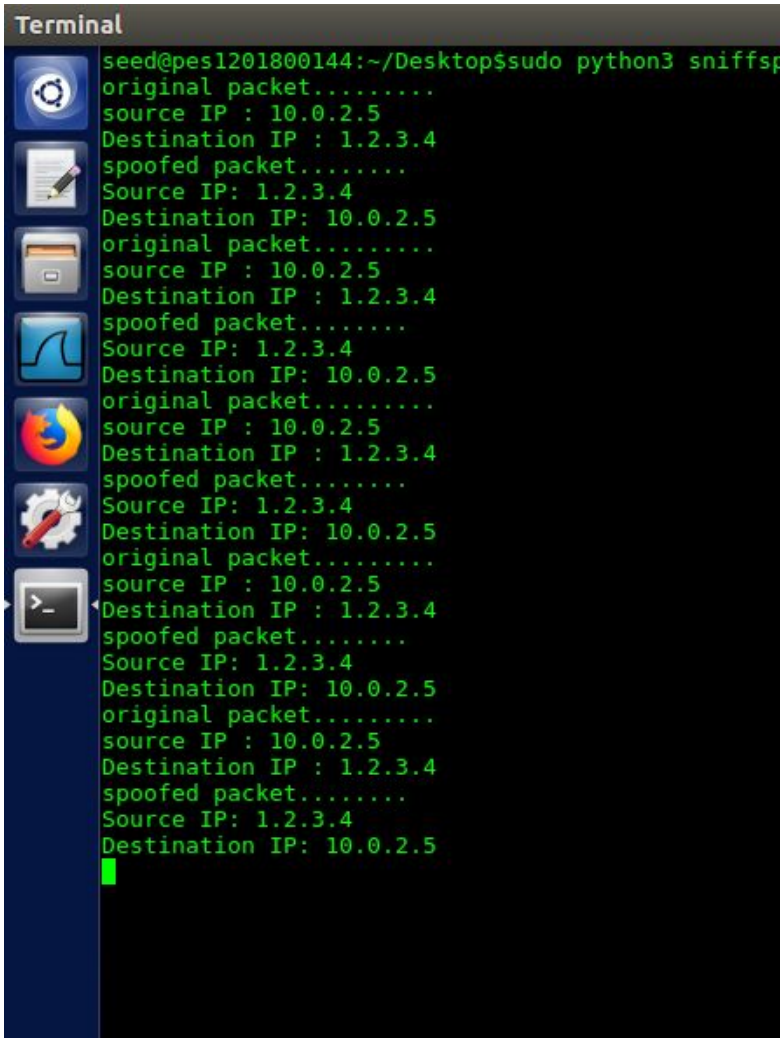


Figure: pinging 1.2.3.4 from victim machine while running spoofing code on attacker machine



```
seed@pes1201800144:~/Desktop$sudo python3 sniffsp
original packet.........
source IP : 10.0.2.5
Destination IP : 1.2.3.4
spoofed packet........
Source IP: 1.2.3.4
Destination IP: 10.0.2.5
original packet.........
source IP : 10.0.2.5
Destination IP : 1.2.3.4
spoofed packet........
Source IP: 1.2.3.4
Destination IP: 10.0.2.5
original packet.........
source IP : 10.0.2.5
Destination IP : 1.2.3.4
spoofed packet........
Source IP: 1.2.3.4
Destination IP: 10.0.2.5
original packet.........
source IP : 10.0.2.5
Destination IP : 1.2.3.4
spoofed packet........
Source IP: 1.2.3.4
Destination IP: 10.0.2.5
original packet.........
source IP : 10.0.2.5
Destination IP : 1.2.3.4
spoofed packet........
Source IP: 1.2.3.4
Destination IP: 10.0.2.5
```

Figure: attacker machine terminal while victim pings to 1.2.3.4

=============================**END**===============================