CNS (UE20CS326) LAB

Aryansh Bhargavan

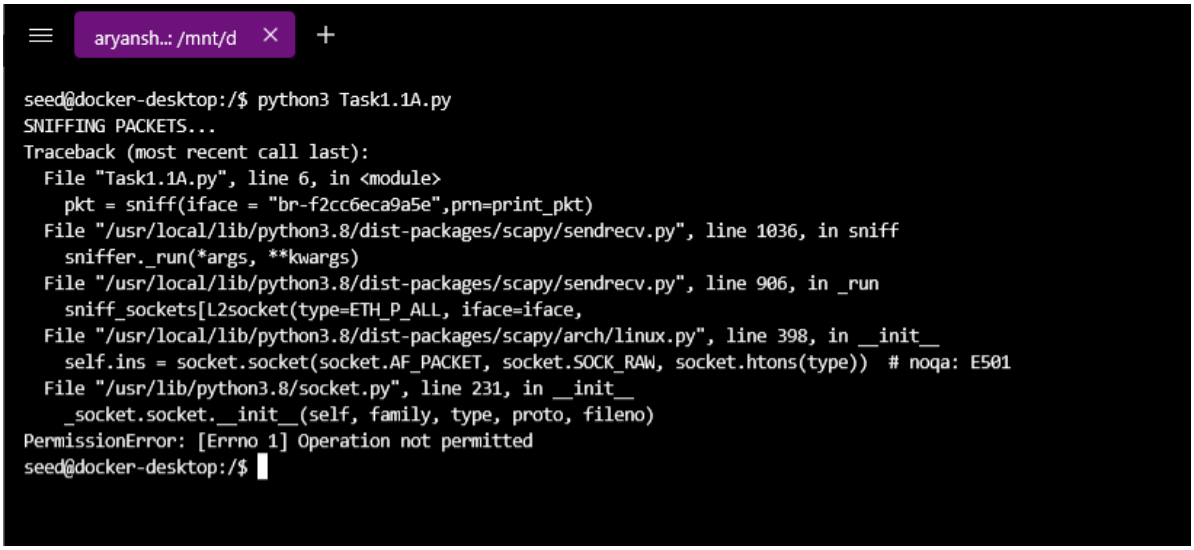
PES1UG20CS084

Task 1.1A Sniffing IP Packets using Scapy

Running as superuser

We ran this from the attacker's VM since the attacker is the one that is going to be intercepting and sniffing said packets.

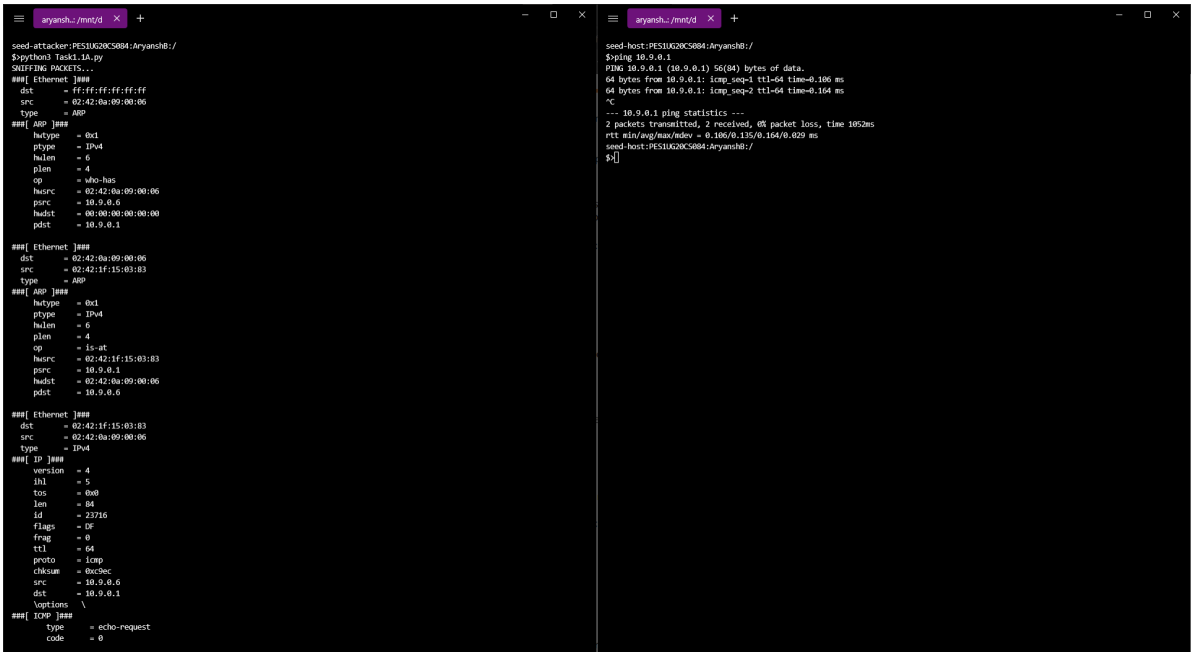
Running as non-superuser



Above program needs to be ran as superuser since a regular user would not be able to perform the tasks due to lack of privileges.

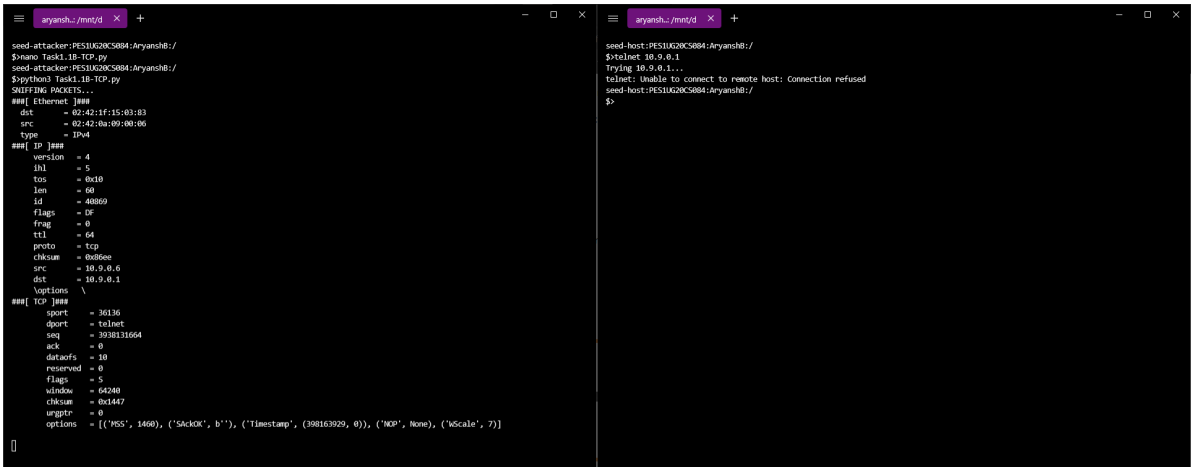
Task 1.1B Capturing ICMP, TCP packet and Subnet

ICMP



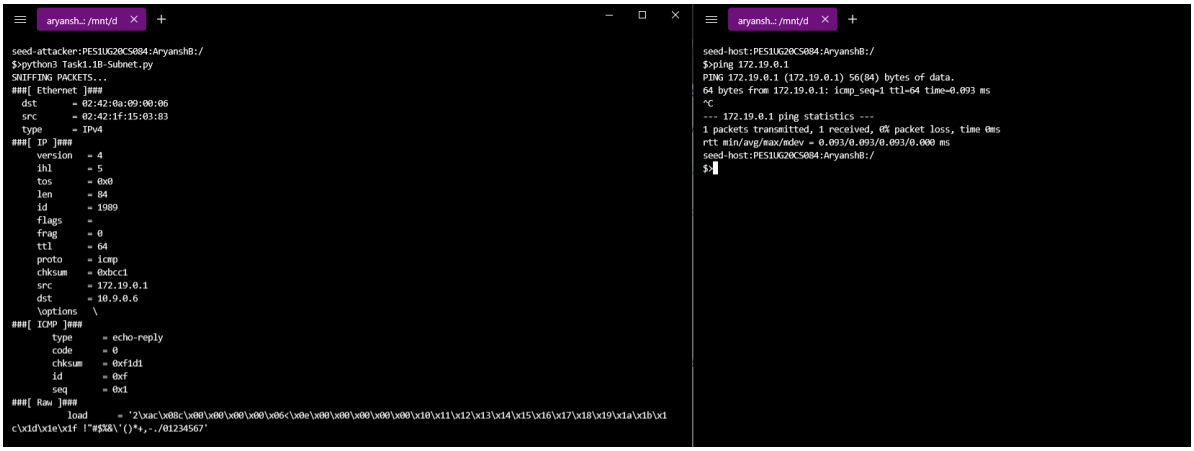
We can see that an ICMP Packet has been captured and can see the source and destination as well.

TCP



Telnet connection was refused but we received a singular packet

SUBNET

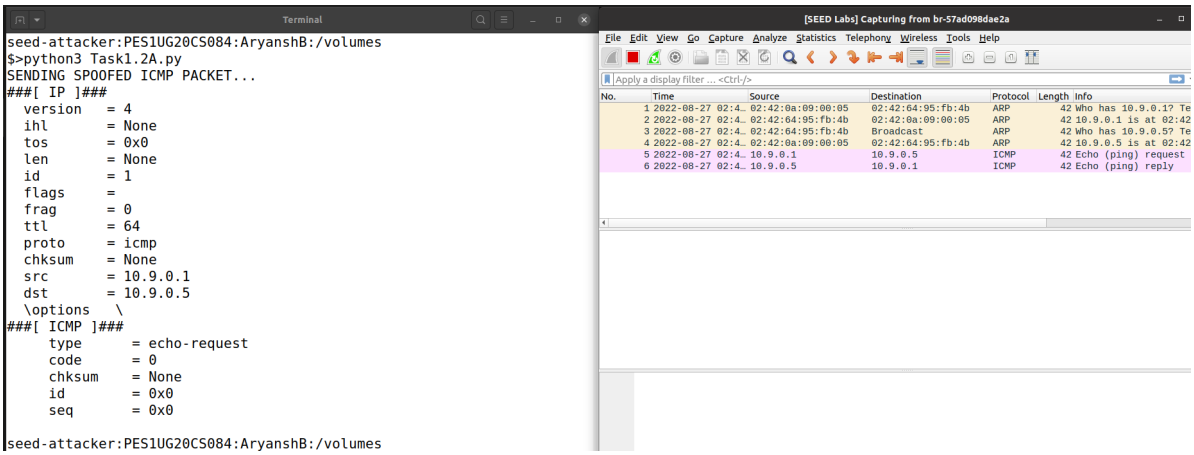


We have successfully captured a packet from 172.19.0.0 subnet

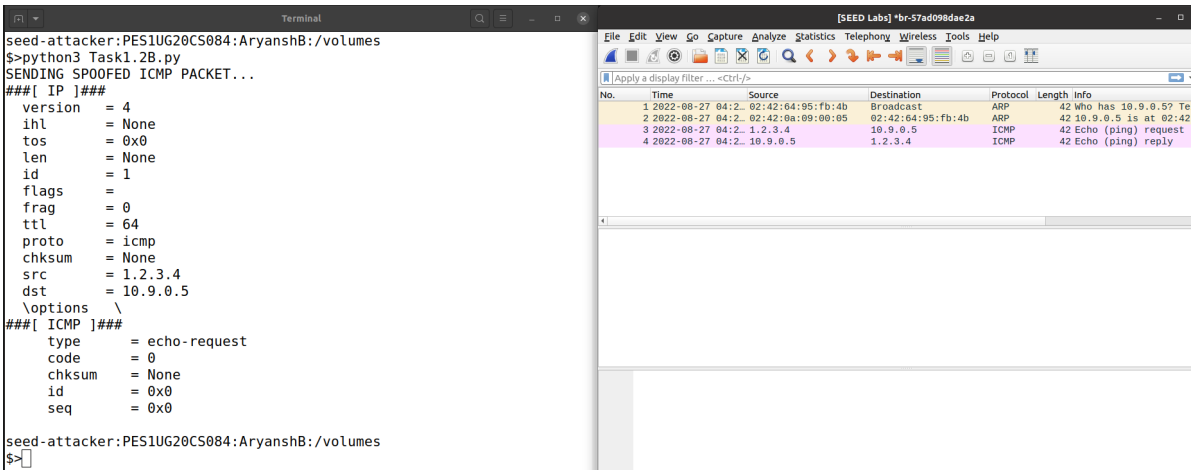
---

Task 1.2 Spoofing

1.2A



1.2B



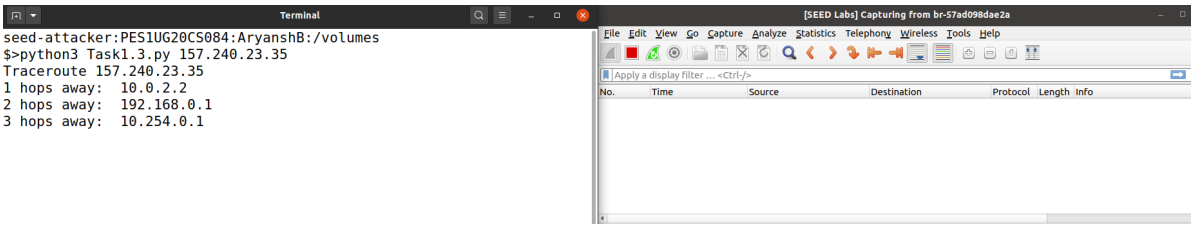
IP address 1.2.3.4 doesn't exist but it got spoofed and host machine (10.9.0.5) sent a reply which means the spoof was successful

---

Task 1.3 Traceroute

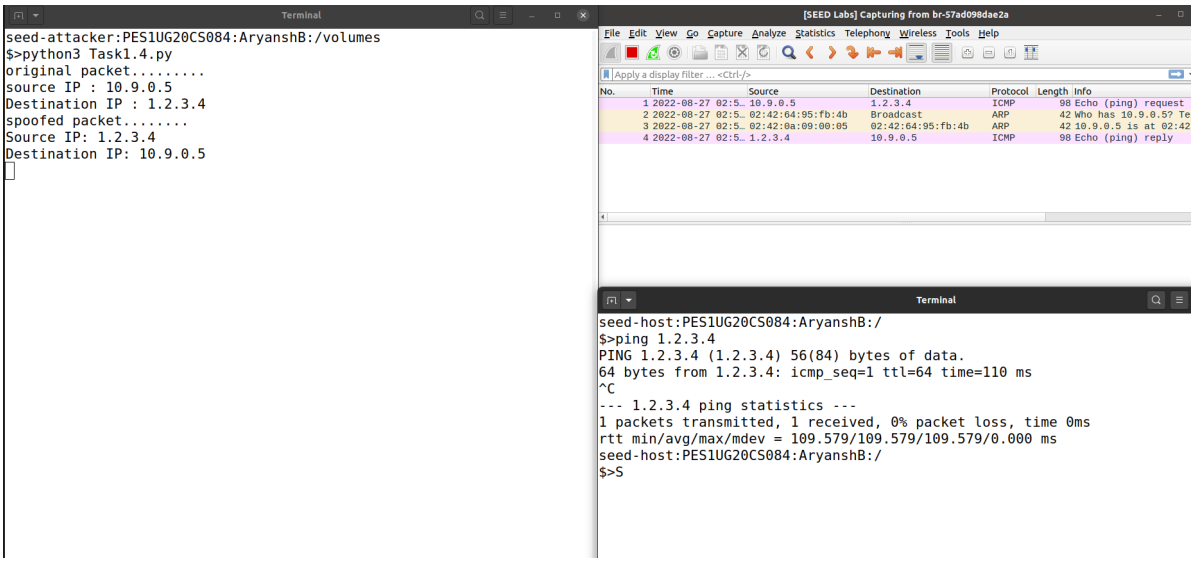
Unfortunately, traceroute was not working properly on college network and could not travel beyond a certain number of hops. I tried the same using my mobile data and home Wi-fi to no avail. Wireshark showed no captures and traceroute could only go travel one hop outside my subnet.

Screenshot for reference:



I tried writing my own traceroute program, which also faced a similar issue.

Task 1.4 Sniffing and then Spoofing



First we sniff a packet meant for IP address 1.2.3.4, then we use this packet and to send spoofed packets.
