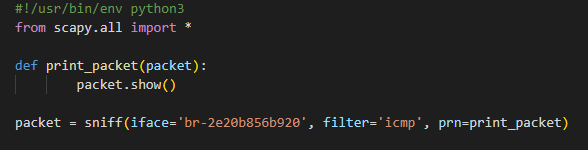
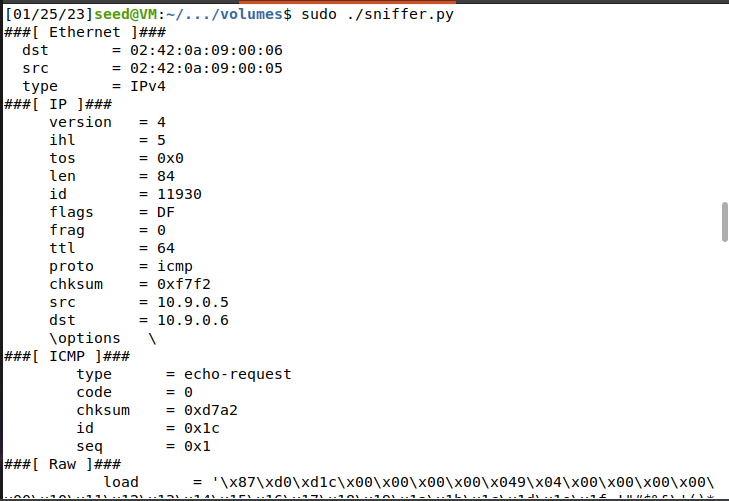
**Crpyto and Network security**

**Lab-2**

Task 1.1 A:

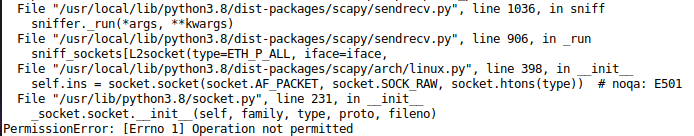


Output:



Program output for sniffing ICMP ECHO request packet when pinged from Host-A(10.9.0.5) to Host-B(10.9.0.6)

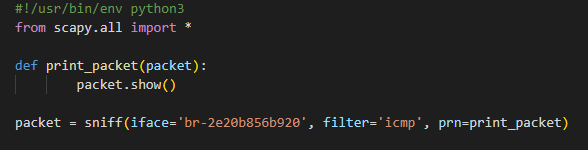
Without sudo:

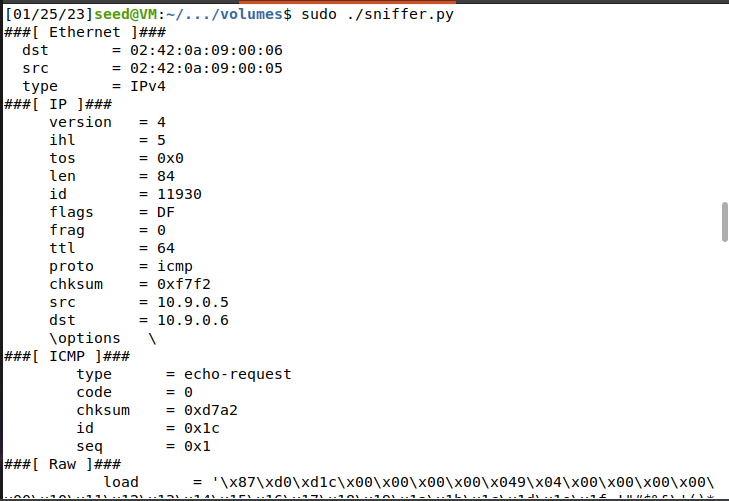


Without root privileges, sniffing the packages aren’t allowed. That is the reason, Permission error is occurred “Operation not permitted”. Scapy uses the Python socket library, hence in order to create raw sockets, root privileges are required.

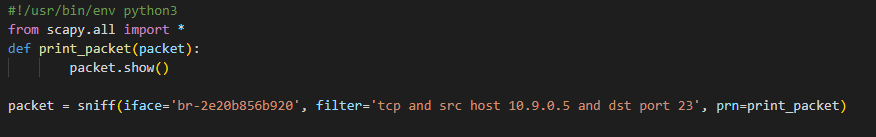
Task 1.1 B:

I: With ICMP filter

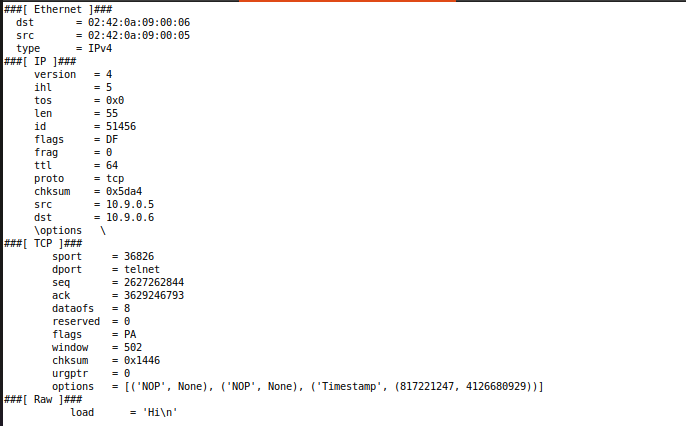


Output:

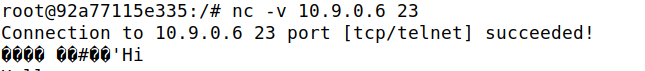
II: TCP filter with fixed source IP and destination port 23



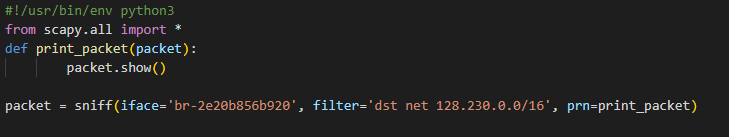
Output:



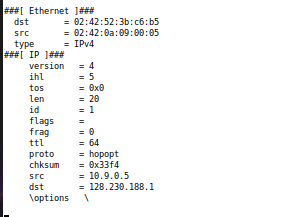
Sending “HI” message using TCP packets by Netcat utility:



III: Filter for packets going to 128.230.0.0/16 (different subnet)

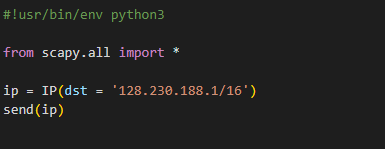


Output:

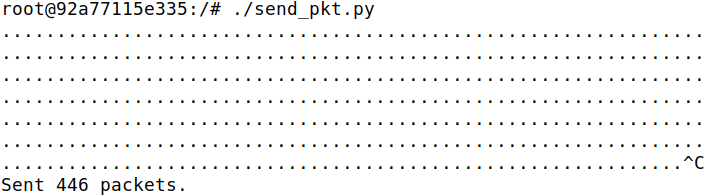


The only way to simulate a packet originating from another subnet is to send it using another Scapy code. Sniffer\_subnet.py executes this code and sniffs the appropriate packet.

Send\_packet.py:

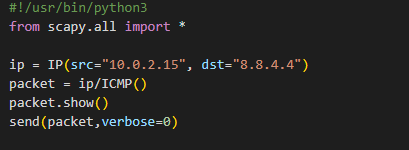


Output:



Task 1.2:

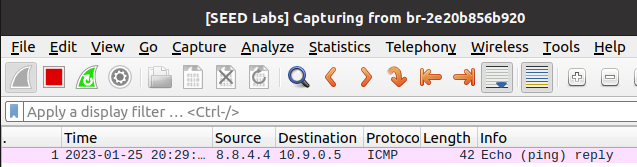
Spoofing ICMP packets



Output:

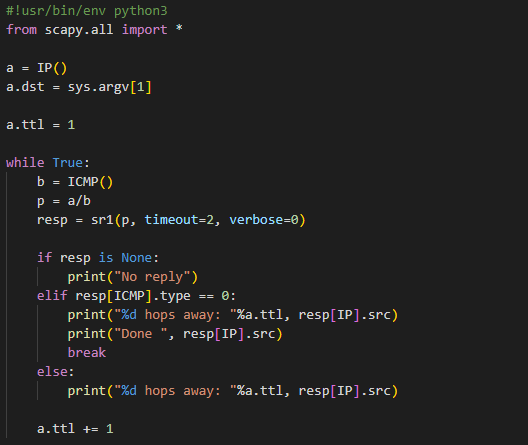


With Wireshark:

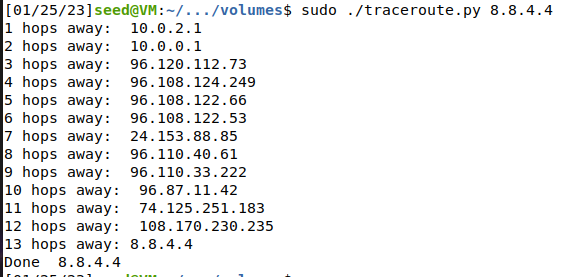


A faked ICMP request was issued from the virtual machine and was picked up by Wireshark, as shown in the screenshot. The ICMP request has 8.8.4.4 as its source and 10.9.0.5 as its destination, both of which are invalid IP addresses.

Task 1.3:

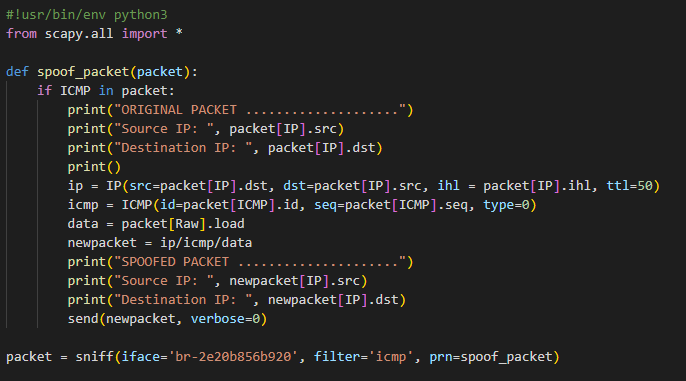


Output:

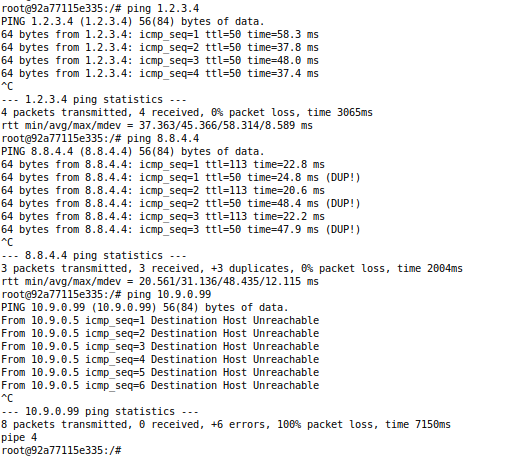


The traceroute program repeatedly sends an ICMP request to a destination IP while increasing the time-to-live attribute by 1 with each request. In this manner, the IP address of the server at each hop between the source and the destination is tracked using the answer to the ICMP packet that is dropped at each hop. This continues up until the ICMP echo reply (type = 0), at which point the loop is broken.

Task 1.4:



Output:



Ping 1: 1.2.3.4

The gateway receives a request from a destination host on the internet that doesn't exist, and our VM can sniff the ping and spoof a response to it. That is why the first portion of the screenshot above shows spoofed responses with ttl=50.

Ping 2: 8.8.4.4

A gateway receives a request from an active destination host on the internet. The actual 8.8.4.4 server and the code both begin responding to the ping, which explains why some of the responses have the (DUP!) signal in the second part of the screenshot above because we are receiving duplicate responses from our malicious program.

Ping 3: 10.9.0.99

Prior to sending the ICMP request, an attempt is made to reach a non-existent destination host on the LAN via the Address Resolution Protocol. Because the host does not exist, there is no response to the ARP request, and we receive the error "Destination Host Unreachable" as seen in the third section of the screenshot.