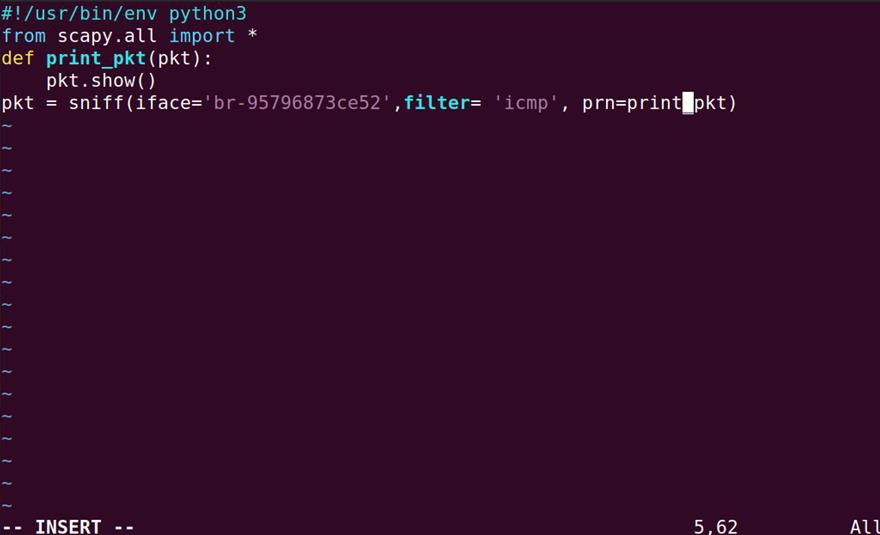
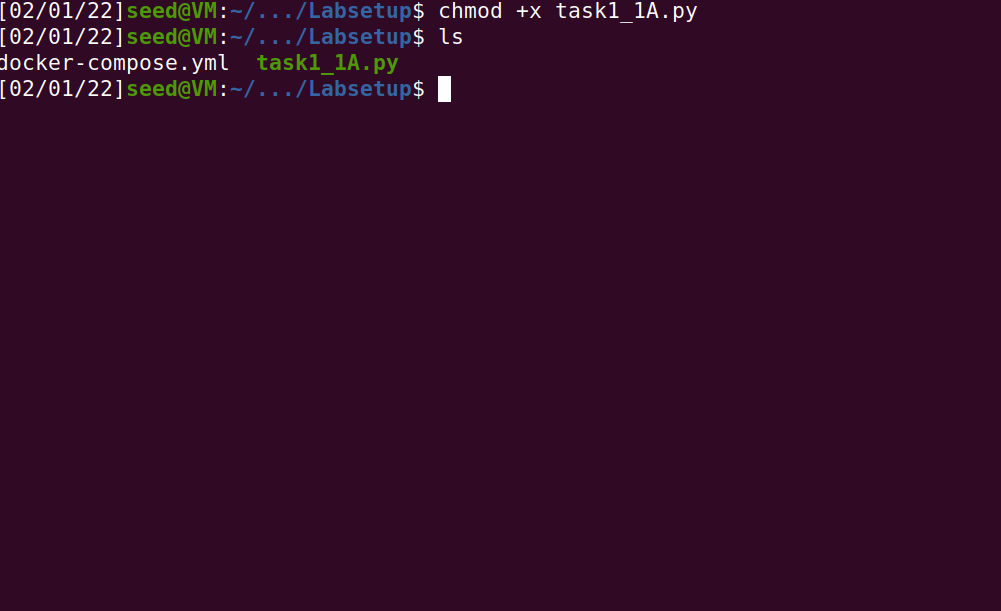
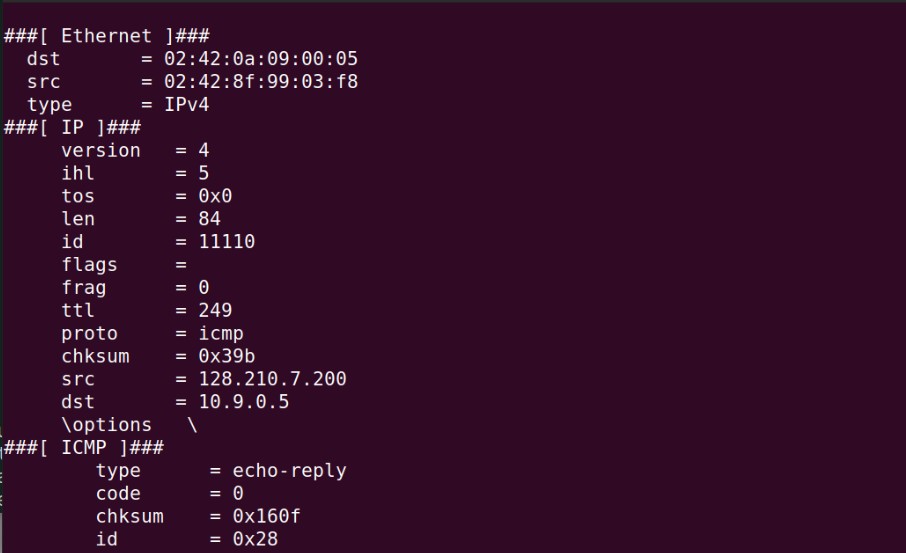
# Crypto & Network Security Lab 3

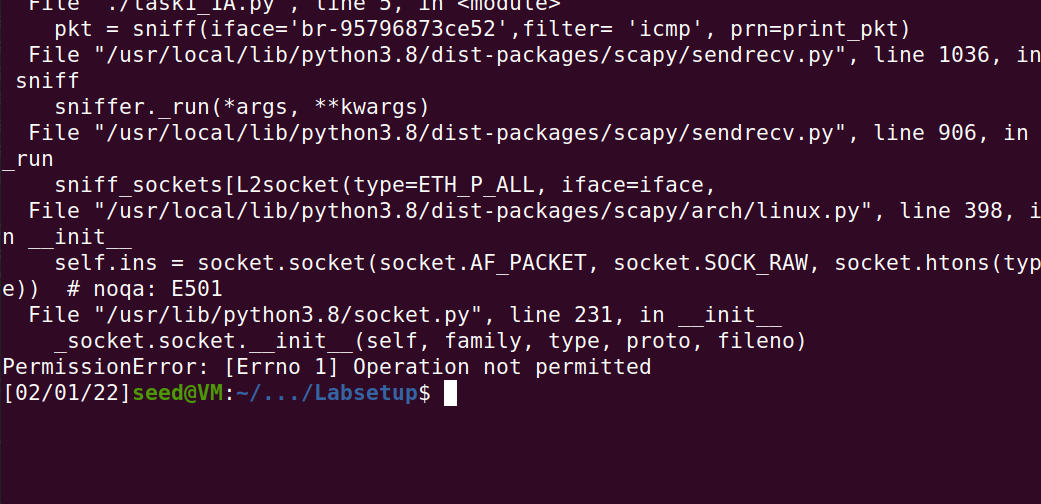
**1.1 A**

**ANS:** Sniffing ICMP packets



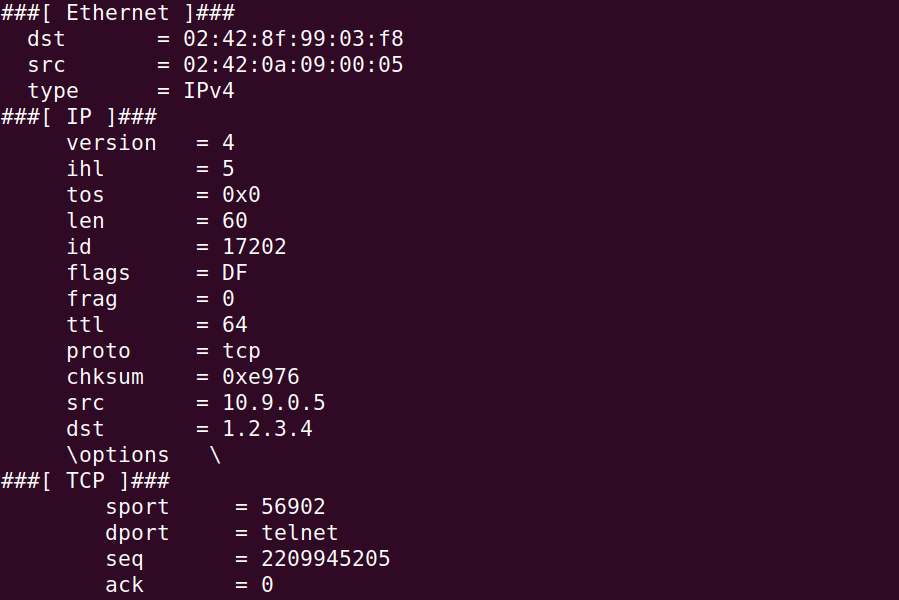
Execution:

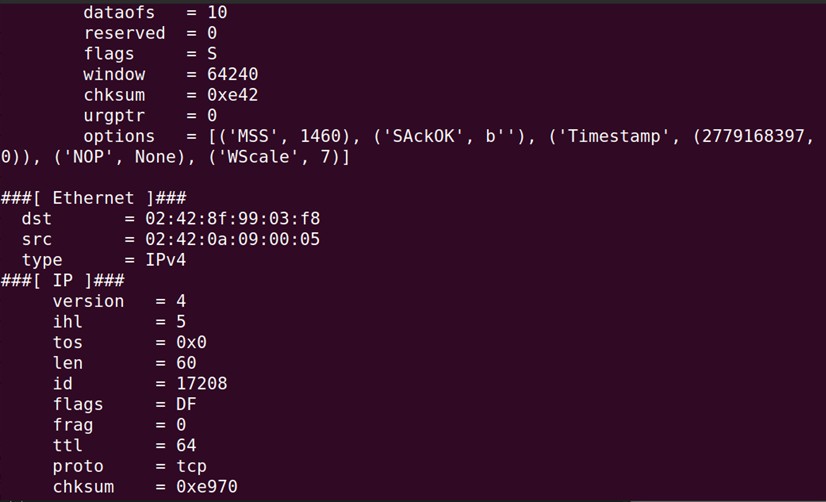
Pinging website from attacker’s terminal.

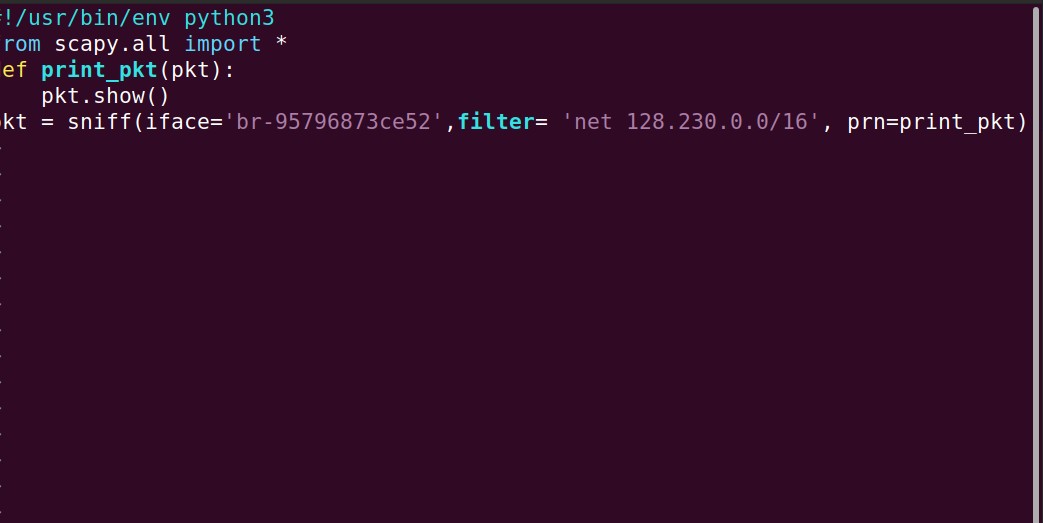
Giving root access

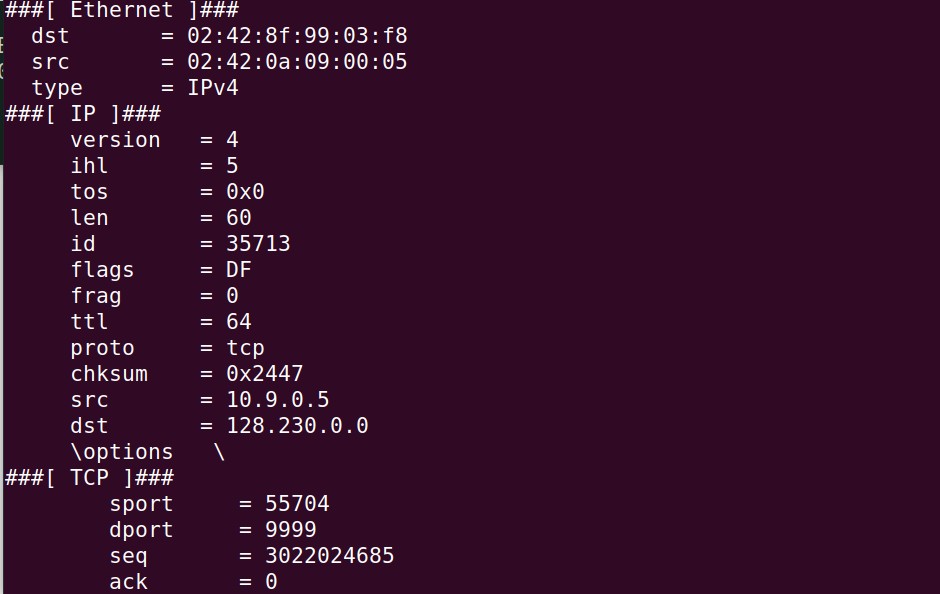
# Text Description automatically generatedB

Giving Source and Destination.

Scapy’s filter use the BPF syntax

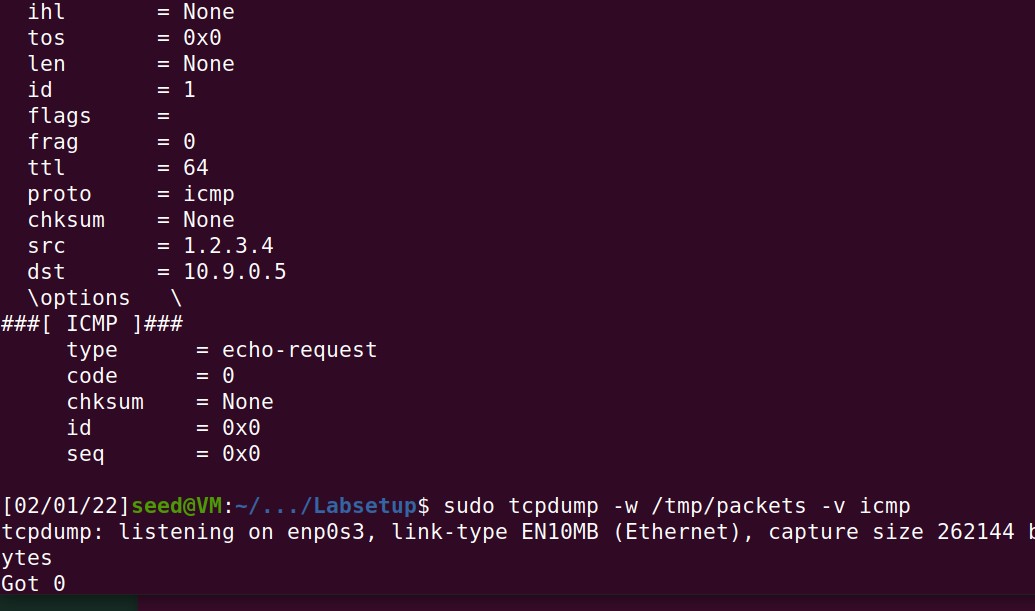


Sending TCP packet

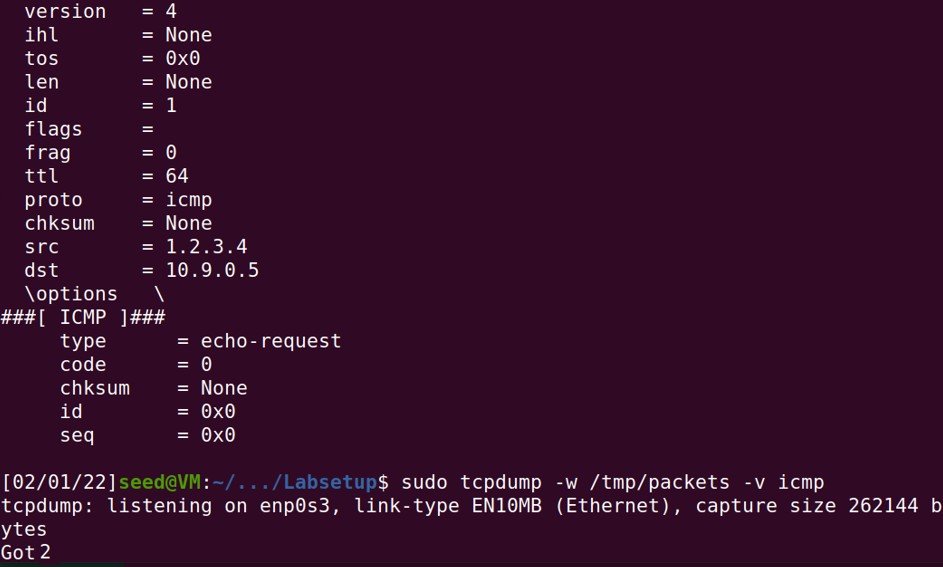
Packet captured.

* 1. Spoofing ICMP packets

As a packet spoofing tool, Scapy allows us to set the fields of IP packets to arbitrary values

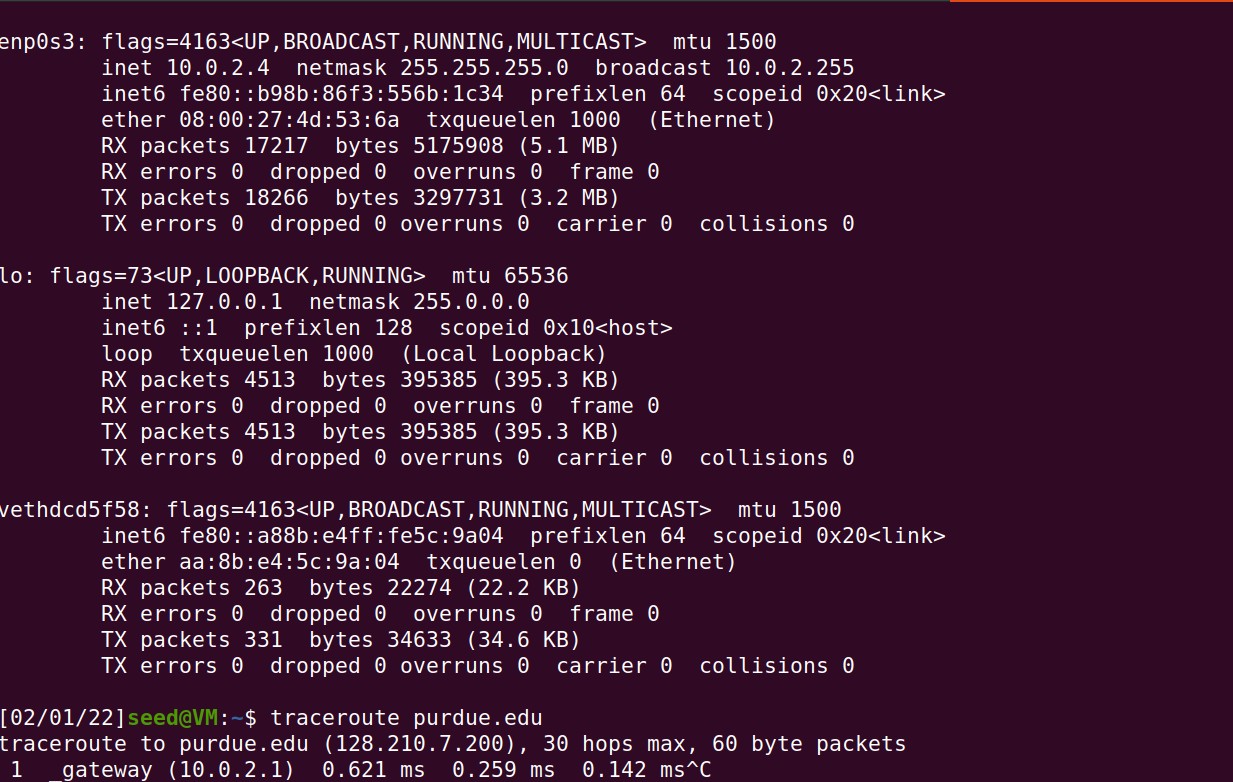


Confirmation

Demonstration of spoofing an ICMP echo request packet with an arbitrary source IP address.

* 1. Traceroute

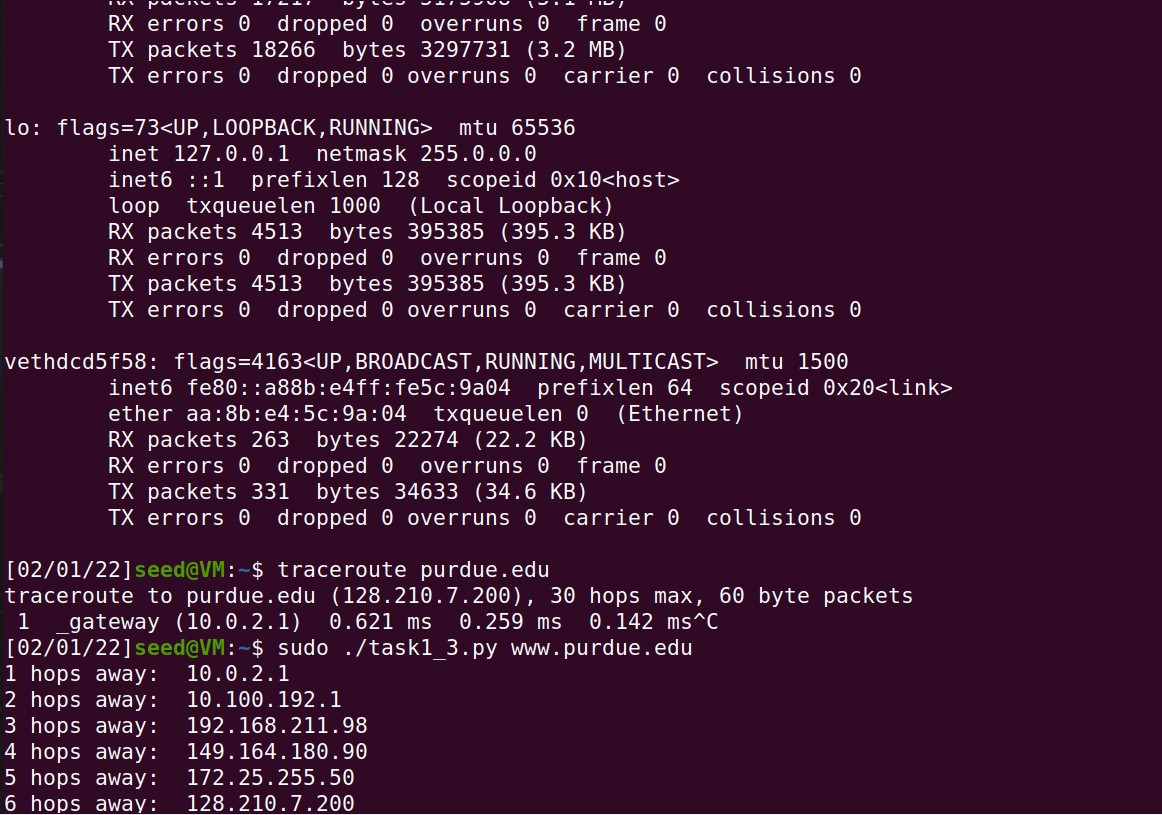
Using Scapy to estimate the distance.

The idea is quite straightforward: just send an packet (any type) to the

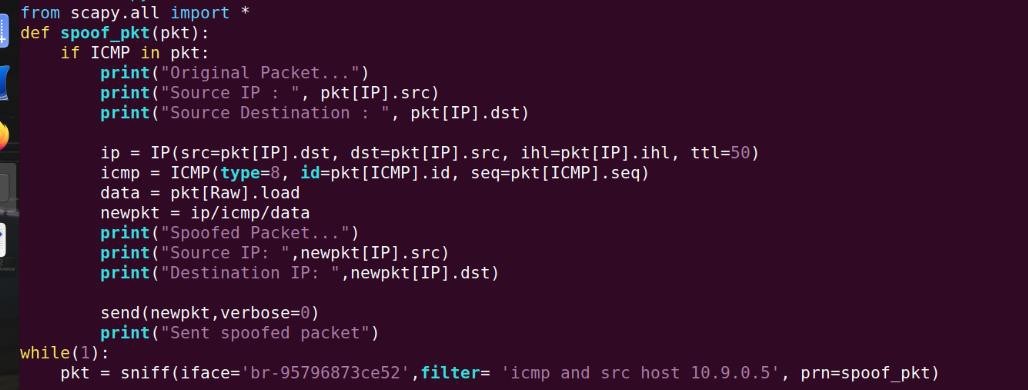
destination, with its Time-To-Live (TTL) field set to 1 first. This packet will be dropped by the first router,

which will send us an ICMP error message, telling us that the time- to-live has exceeded. That is how we get

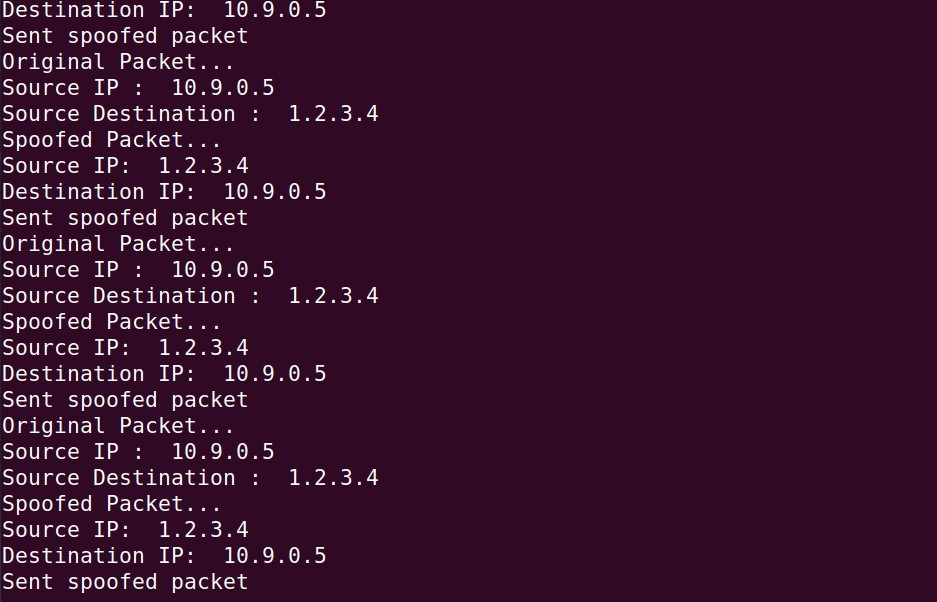
the IP address of the first router**.**

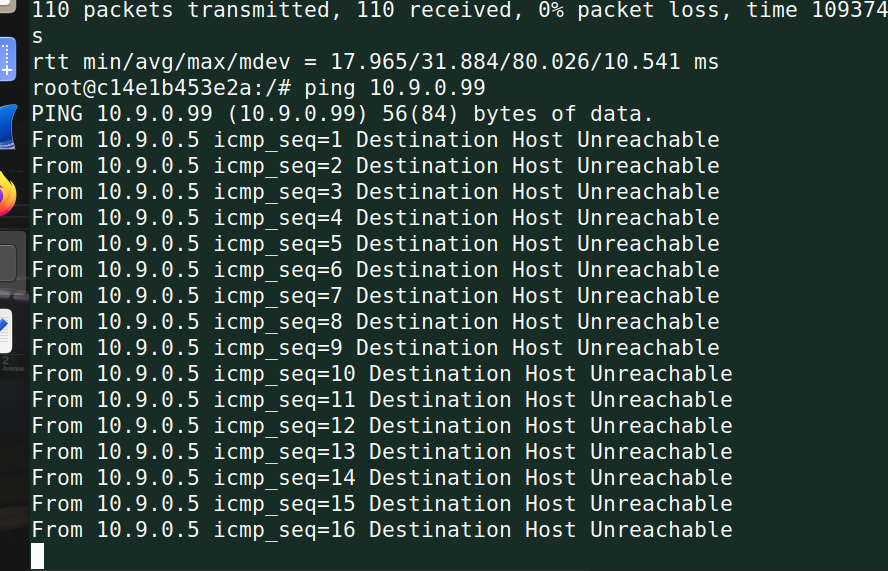
We then increase our TTL field to 2, send out another packet, and get the

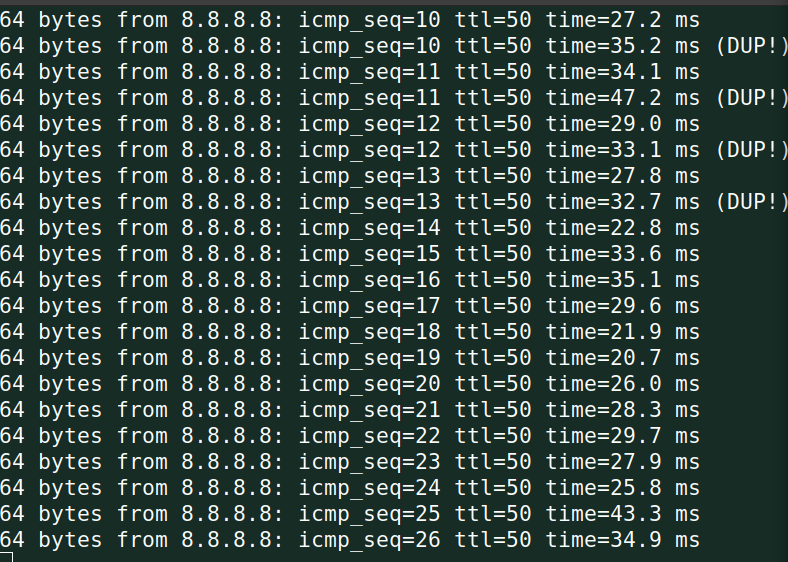
IP address of the second router. We will repeat this procedure until our packet finally reach the destination.

* 1. Sniffing and-then Spoofing

Combining the sniffing and spoofing techniques to implement the following sniff-andthen-spoof program





Regardless of whether machine X is alive or not, the ping program will always receive a reply, indicating that X is alive