**COMPUTER NETWORK SECURITY**

**LAB-3**

**ICMP ATTACK**

**LAB**

NAME: VISHWAS M

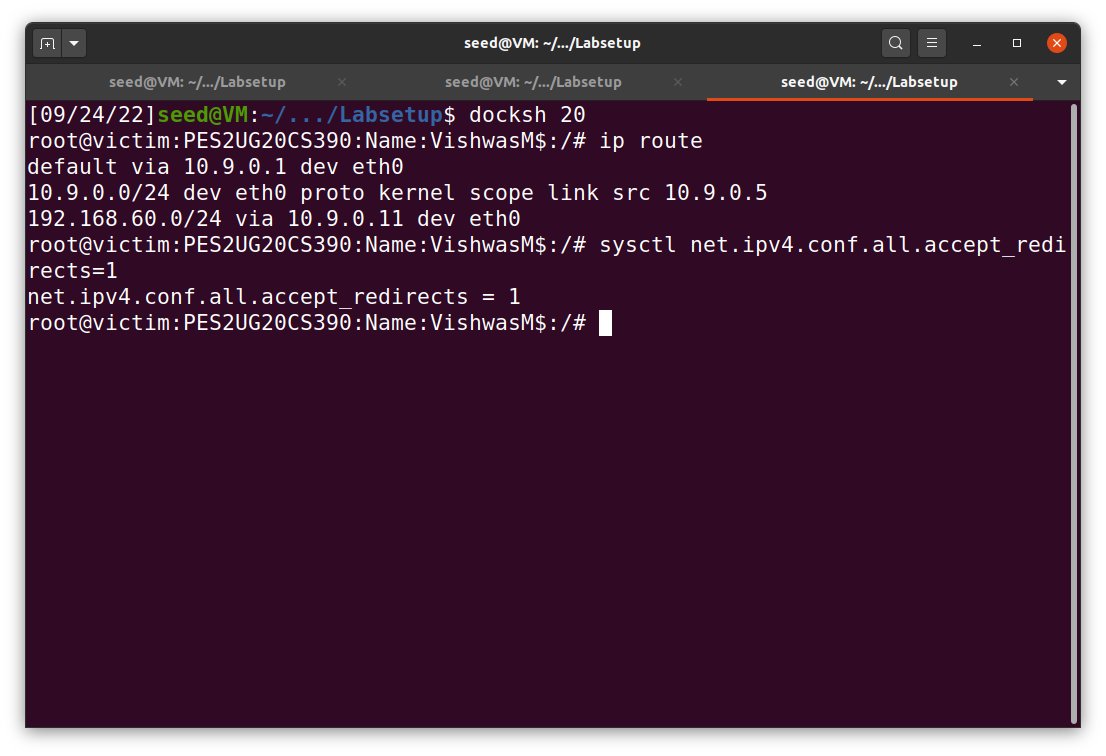
SRN: PES2UG20CS390

SEC: F

DATE:24/09/2022

Task 1: Launching ICMP Redirect Attack

Run the following command on the Victim Machine to remove the countermeasure

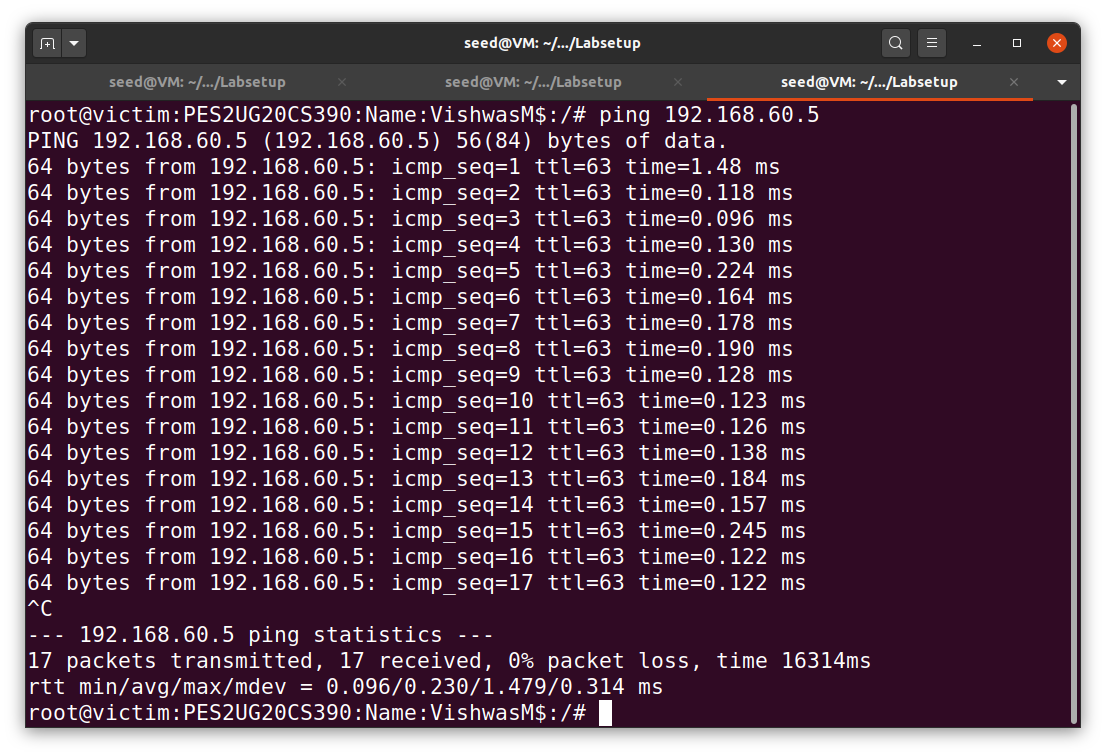


Task 1A:

In order to perform the attack i.e., make the Victim Machine route its packets through the Malicious router.

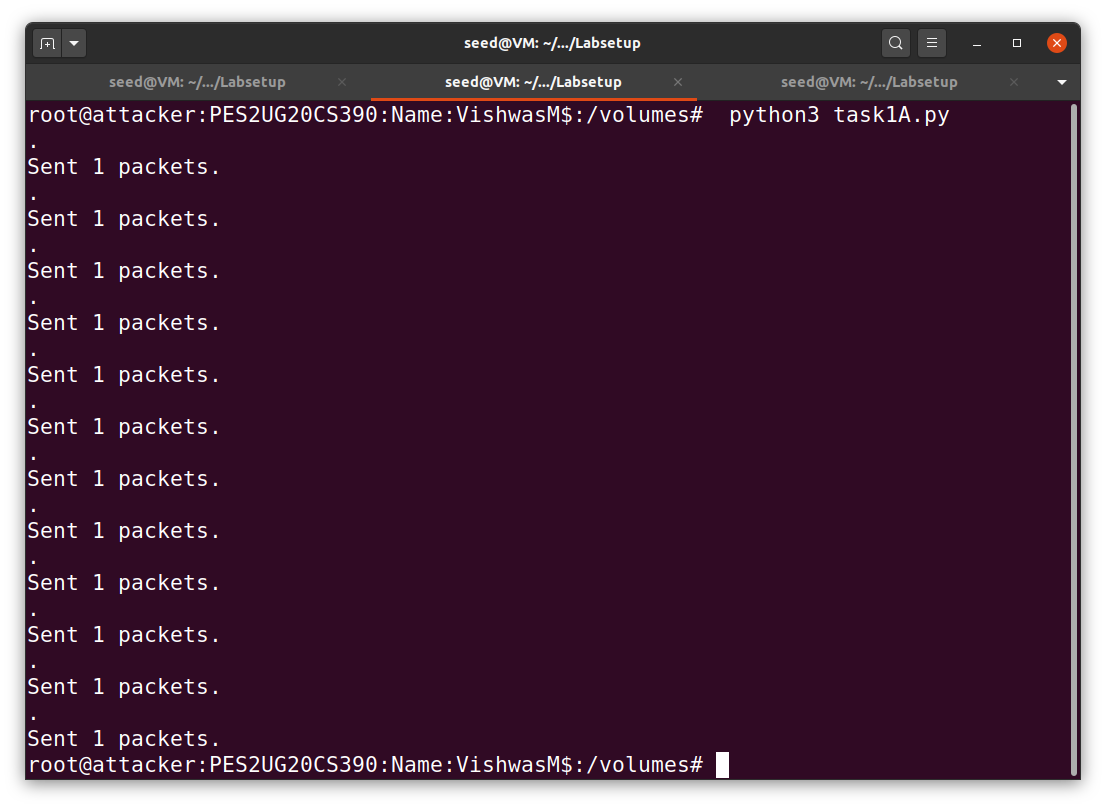
Step1:

First, we ping the Host -192.168.60.5 from the Victim Machine.



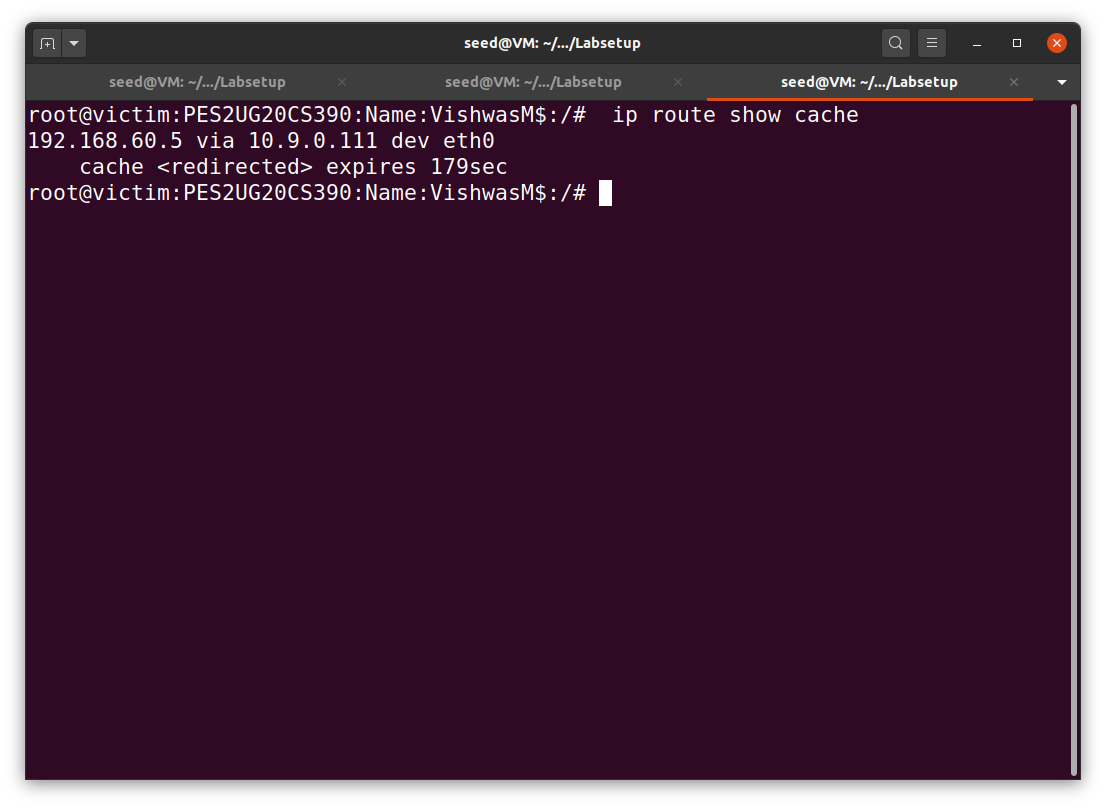
Step2:

Then we run the following code on the Attacker Machine.



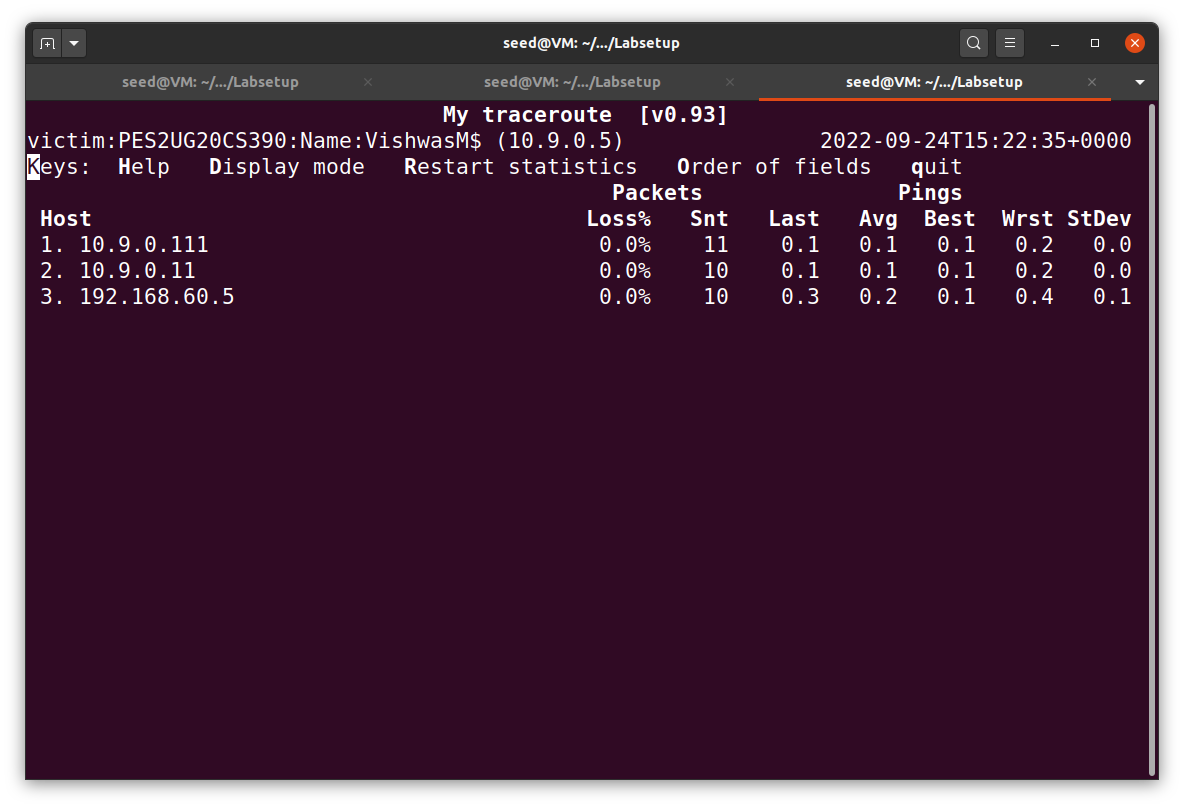
Step3:

ICMP redirect messages will not affect the routing table; instead, it affects the routing cache. Entries in the routing cache overwrite those in the routing table, until the entries expire. To check if we have successfully executed the attack, check the routing cache on the Victim Machine.

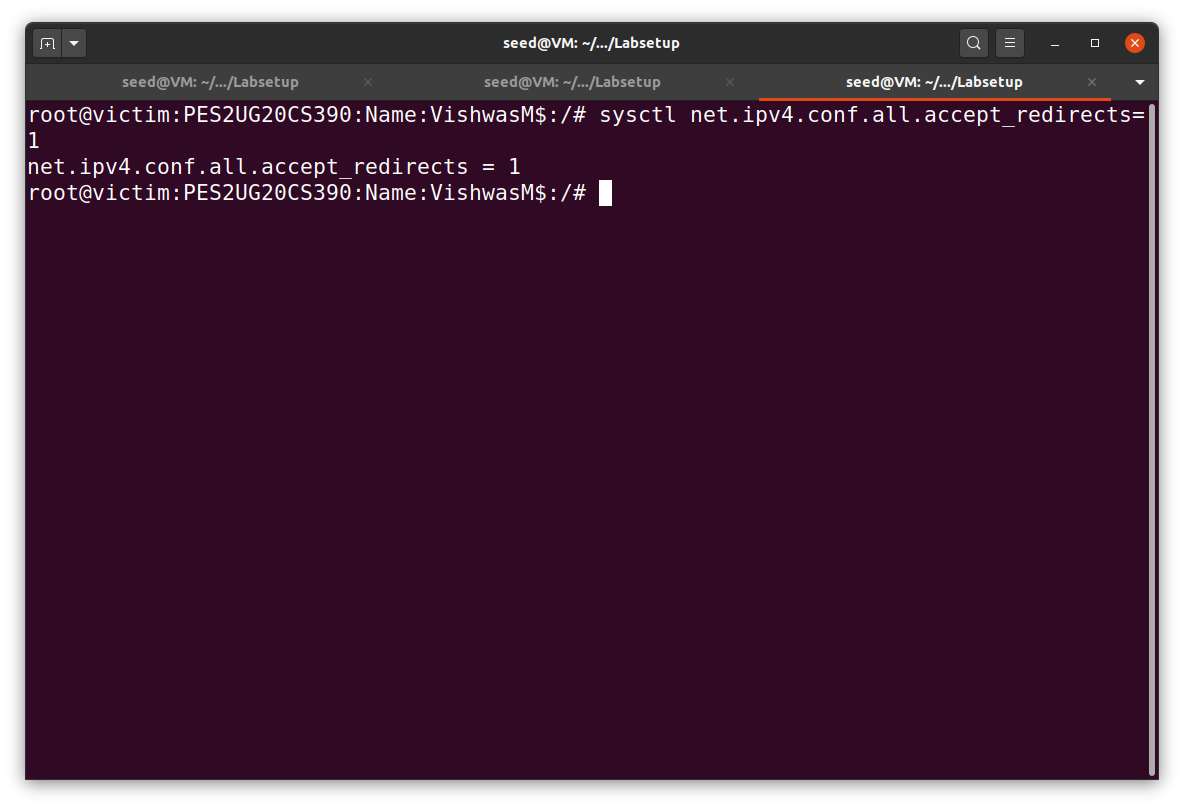


Step4:

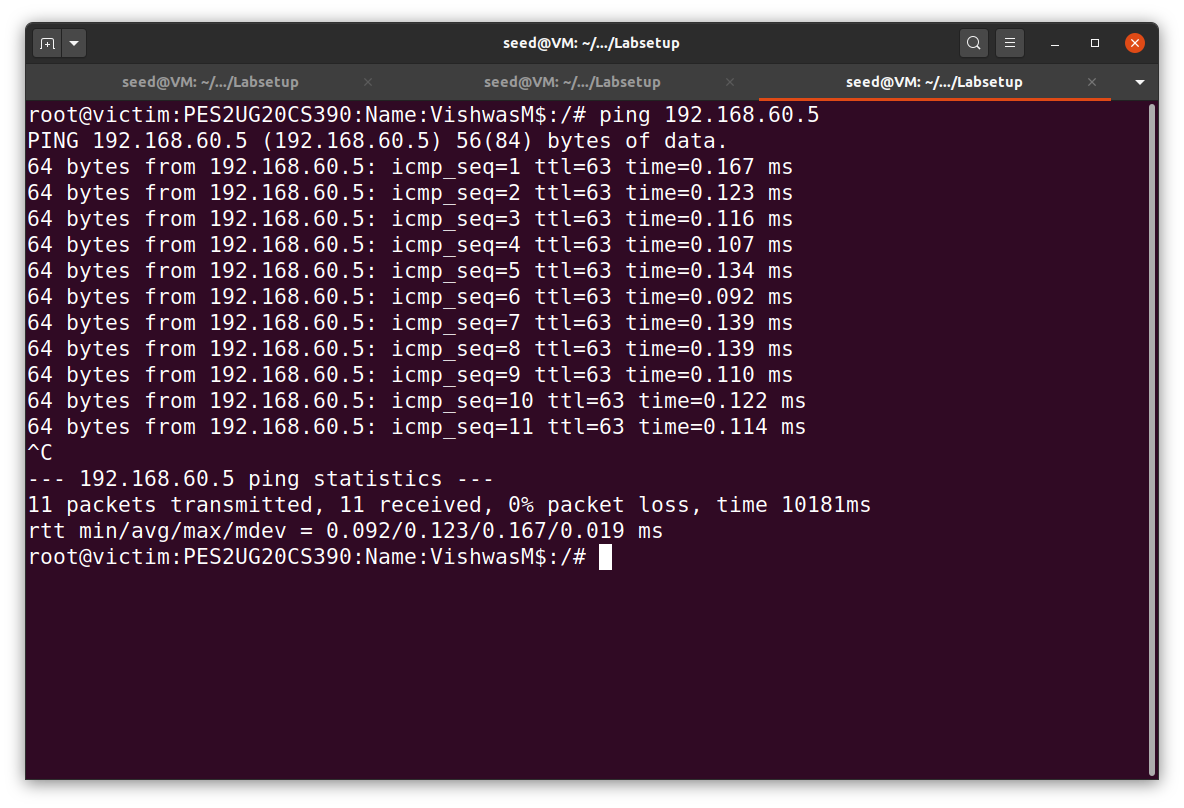
Now run a traceroute on the victim machine, and see whether the packet is rerouted or not.



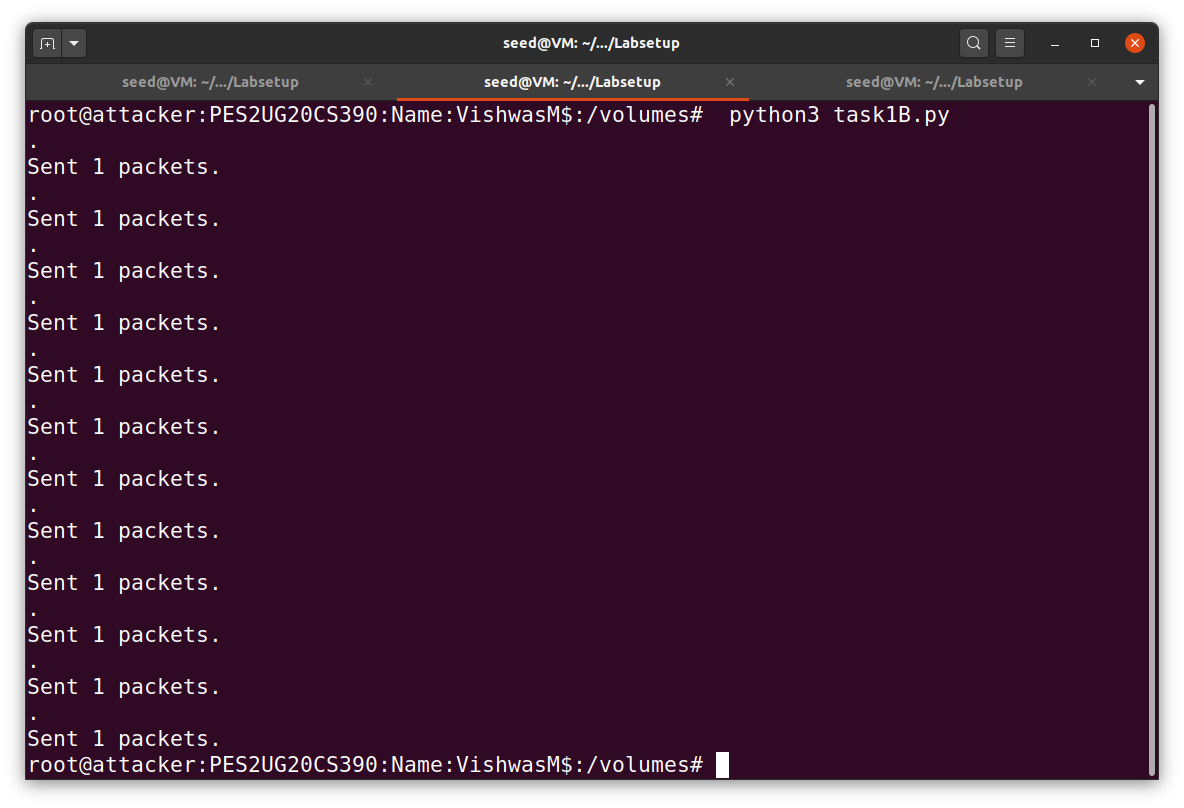
**ICMP redirect attacks to redirect to a remote machine**



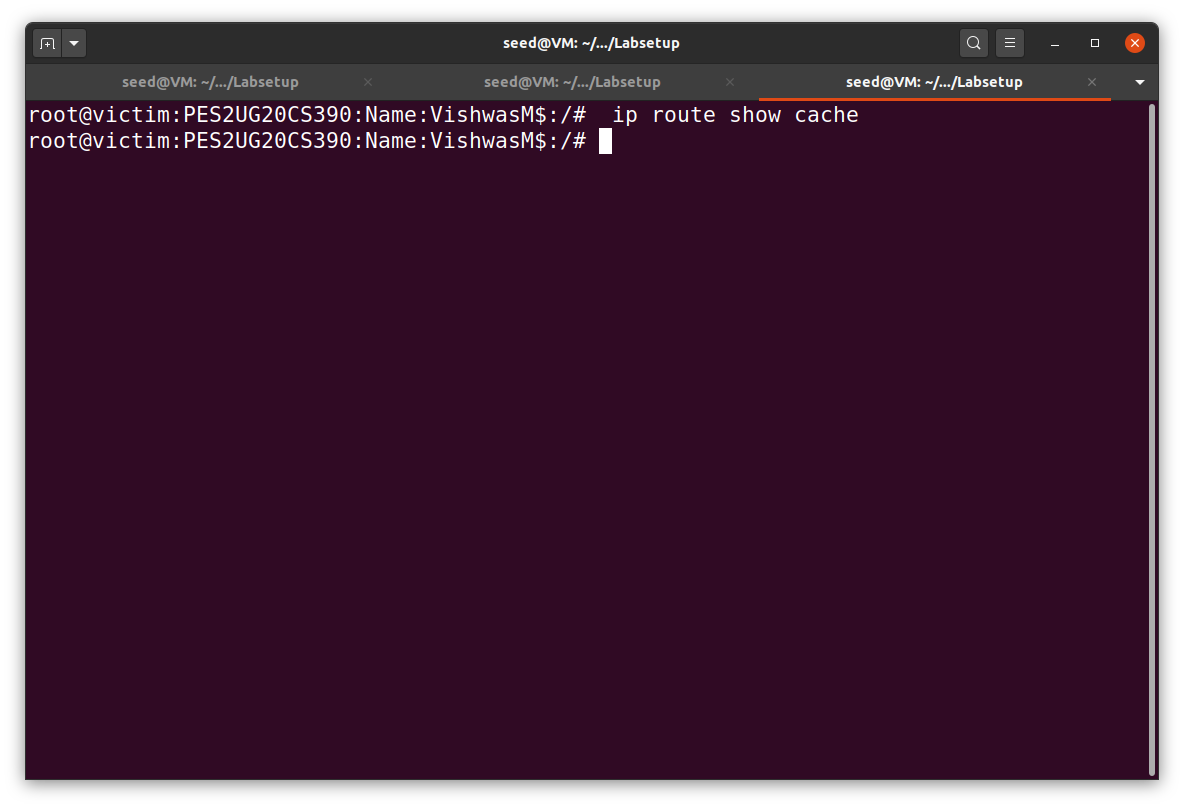
Step1:



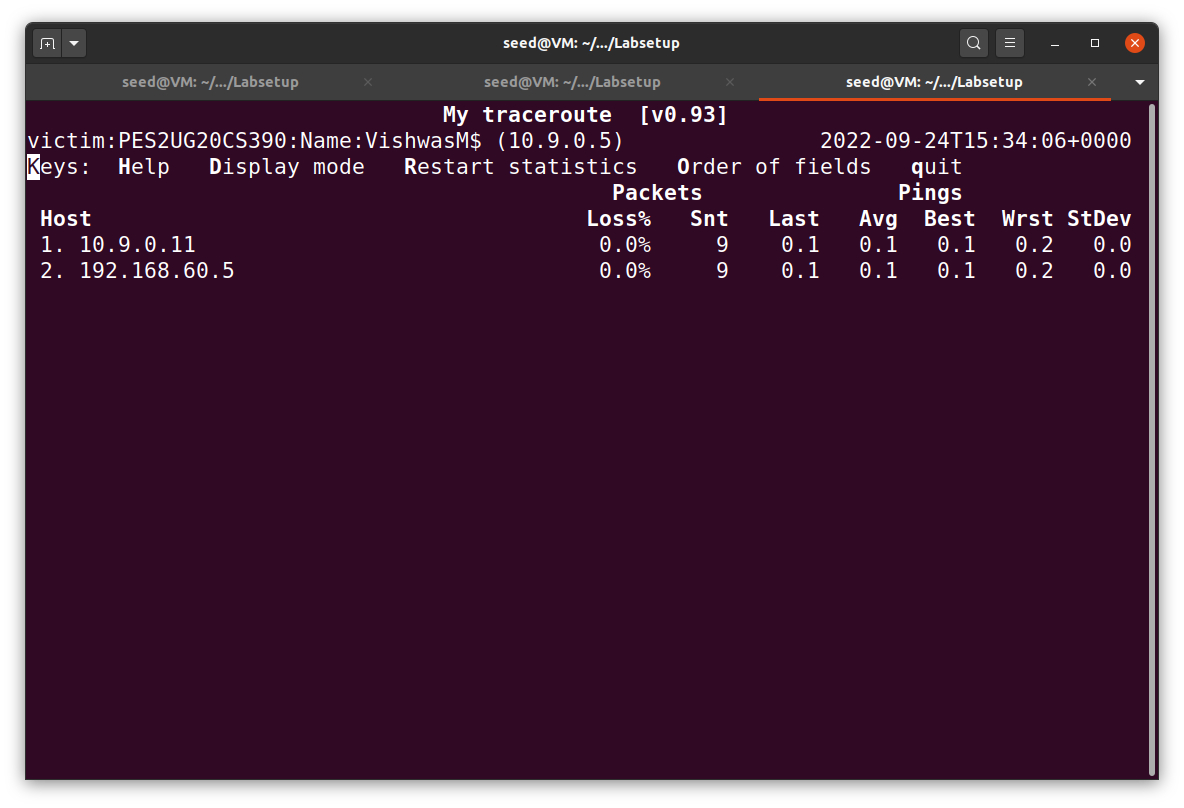
Step2:



Step3:



Step4:

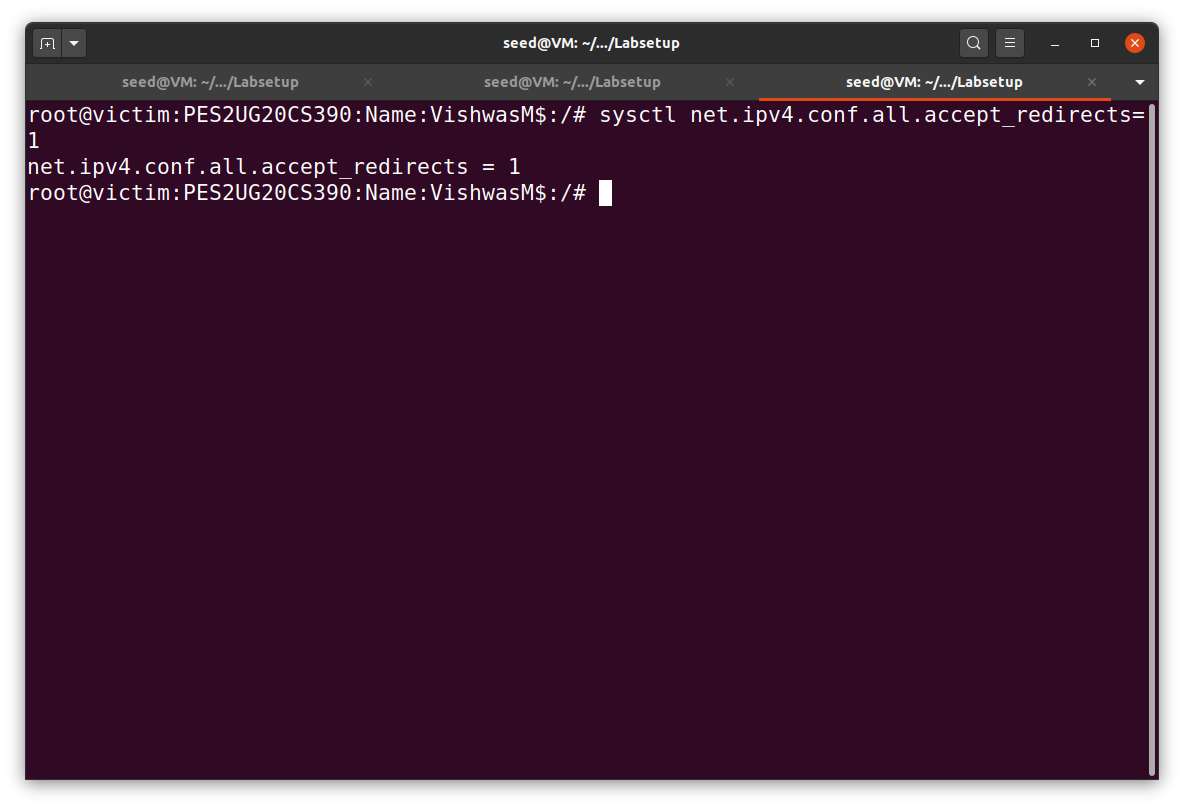


Question 1: Can you use ICMP redirect attacks to redirect to a remote machine? Namely, the IP address assigned to icmp.gwis a computer not on the local LAN. Please show your experiment result, and explain your observation.

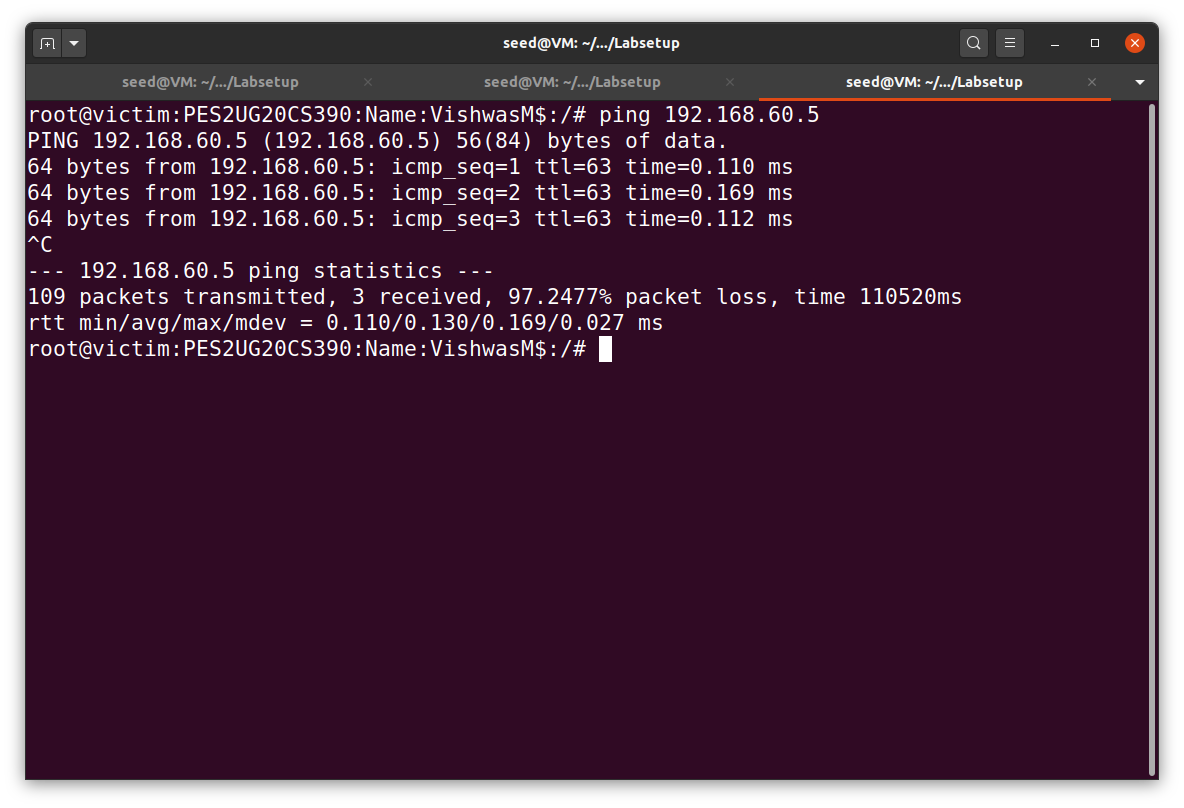
Ans:

Question 2: Can you use ICMP redirect attacks to redirect to a non-existing machine on the same network? Namely, the IP address assigned to icmp.gw is a local computer that is either offline or non-existing. Please show your experiment result, and explain your observation

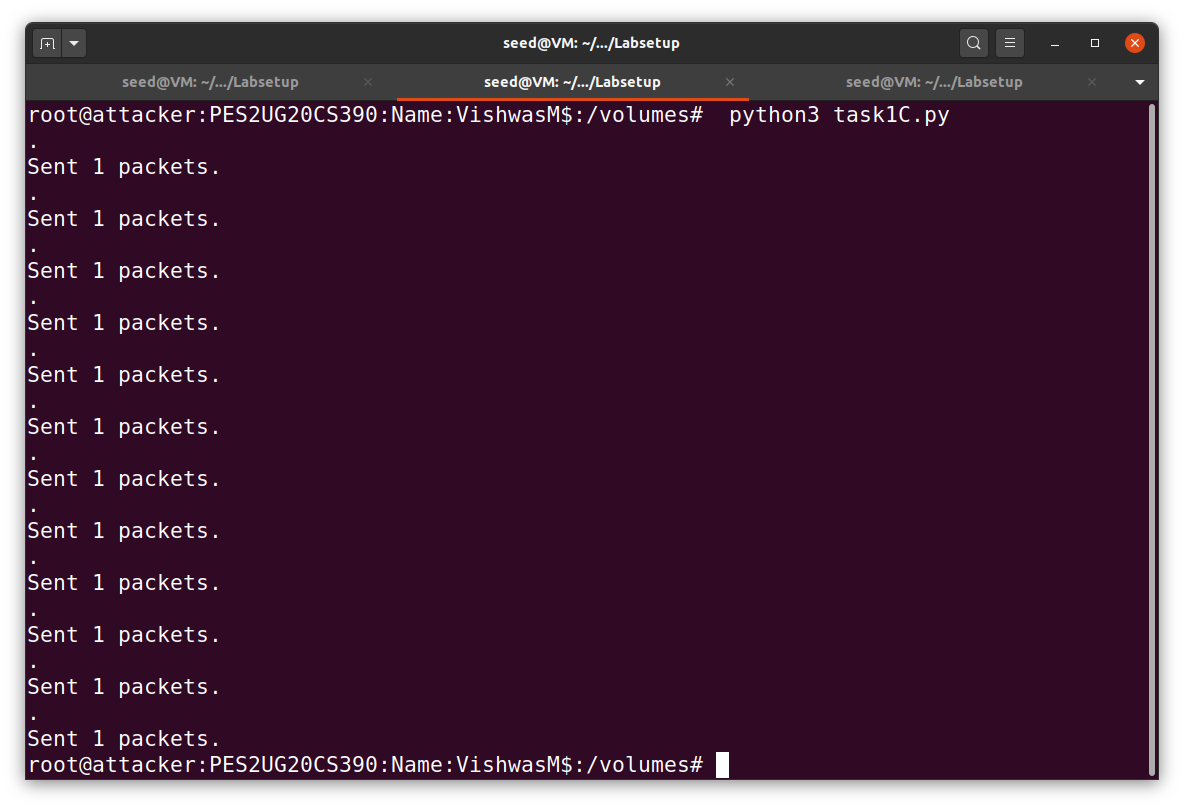
Ans:



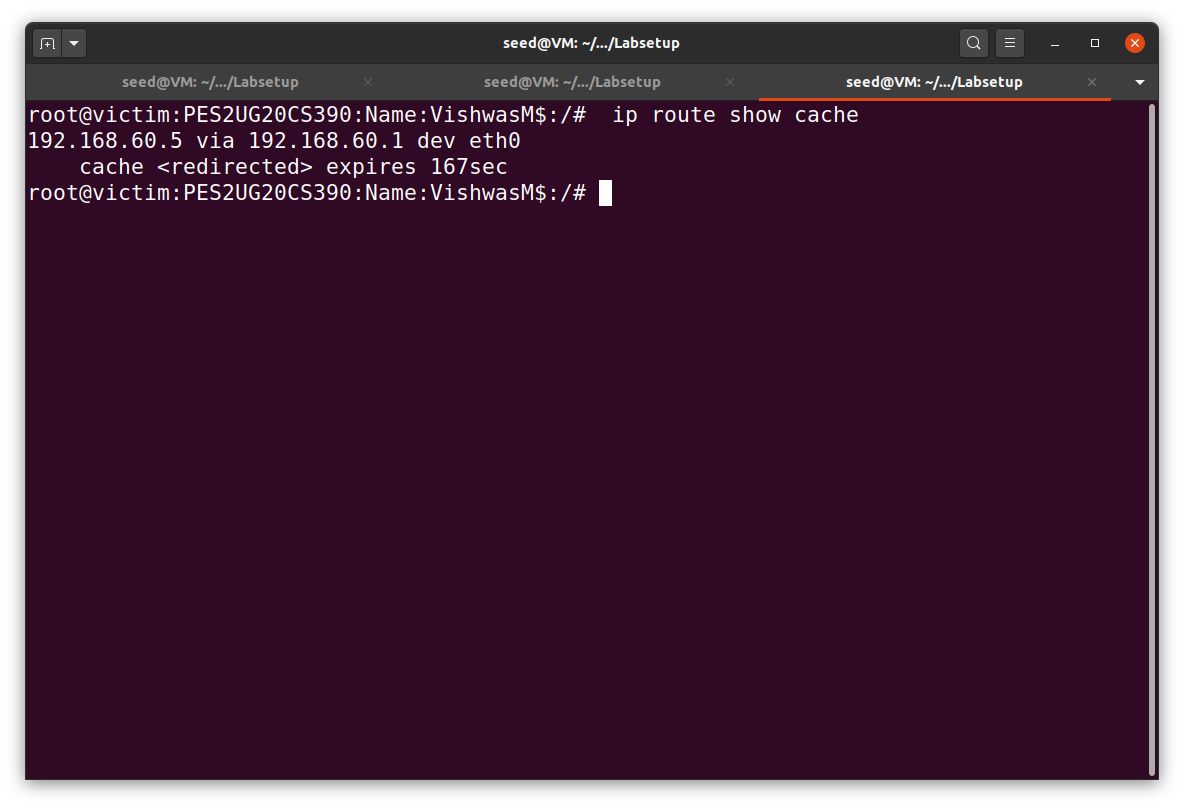
Step1:



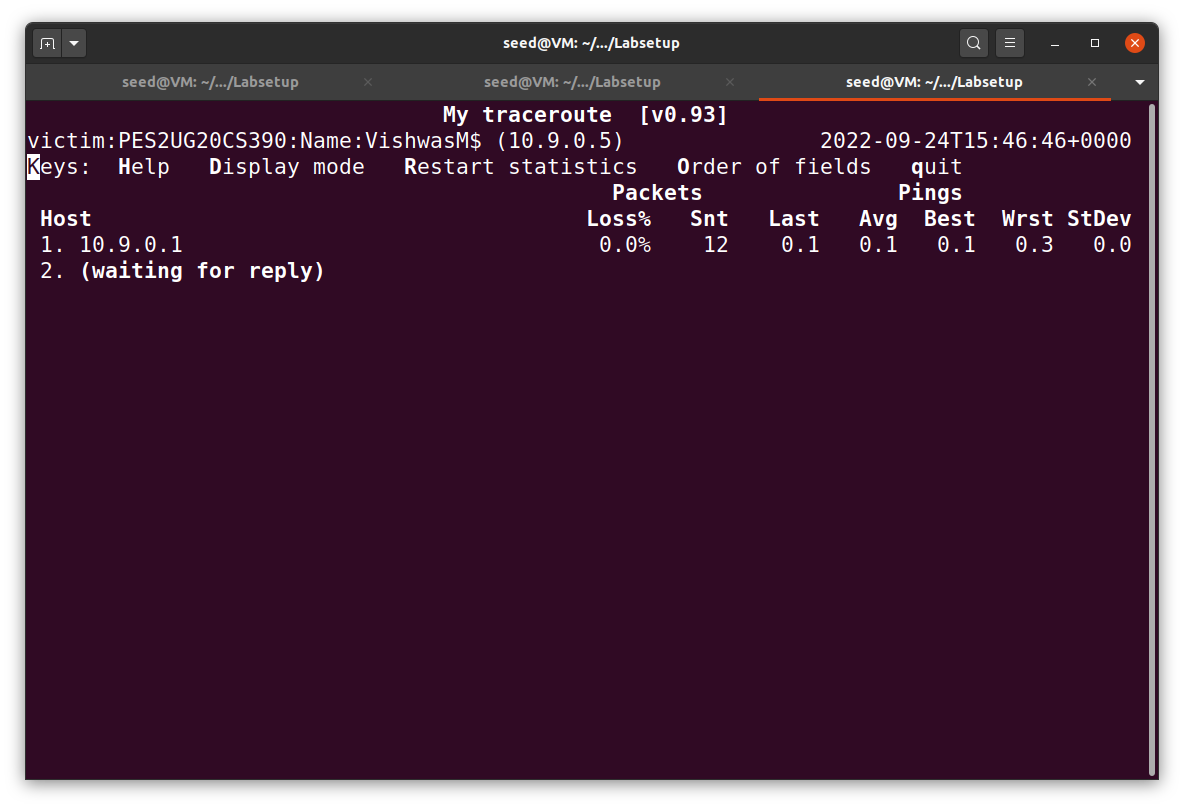
Step2:



Step3:

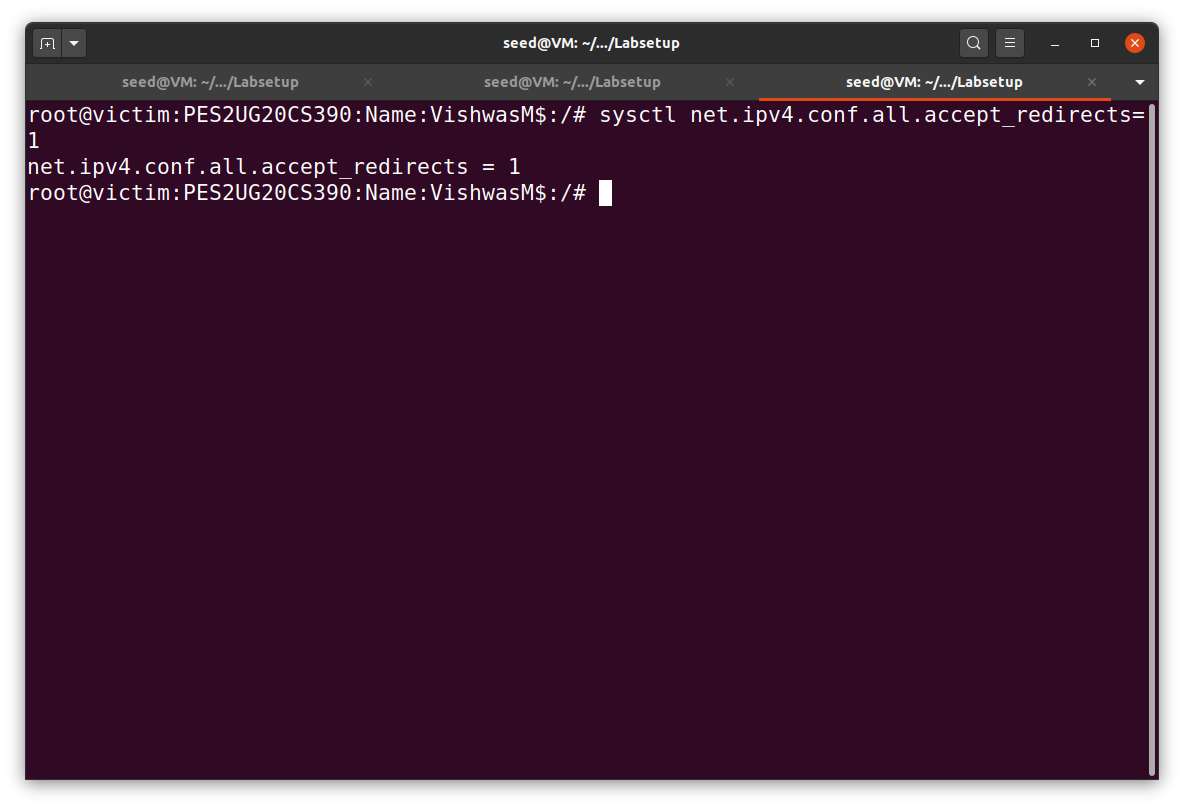


Step4:

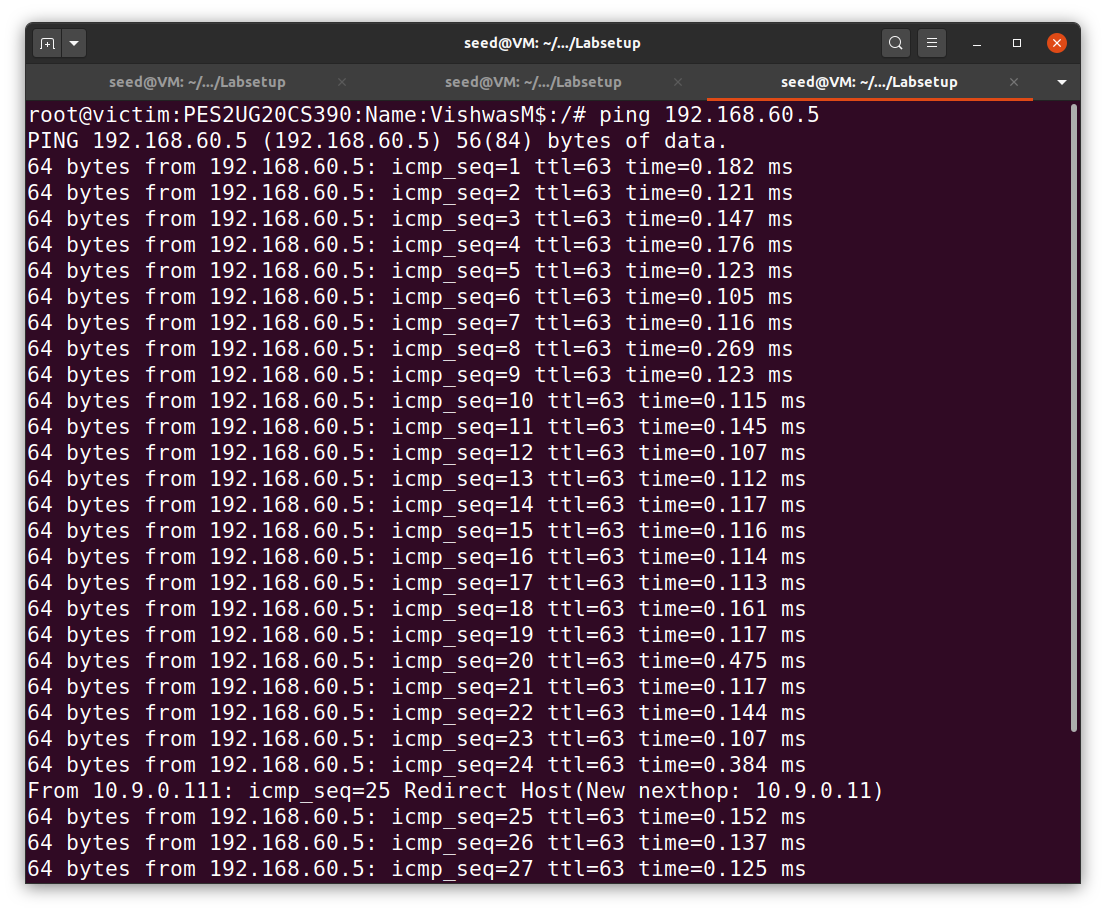


Question 3: If you look at the docker-compose.yml file, you will find the following entries for the malicious router container. What are the purposes of these entries? Please change their value to 1, and launch the attack again. Please describe and explain your observation.

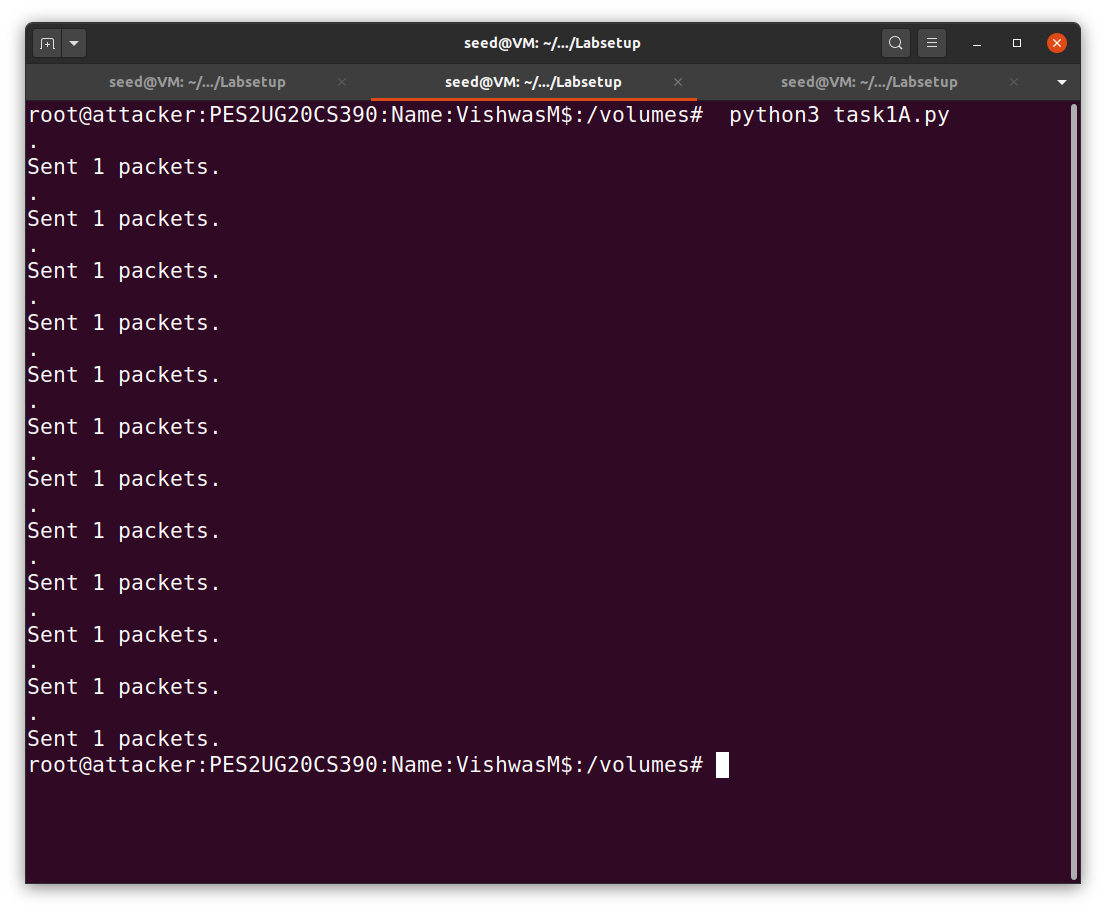
Ans:



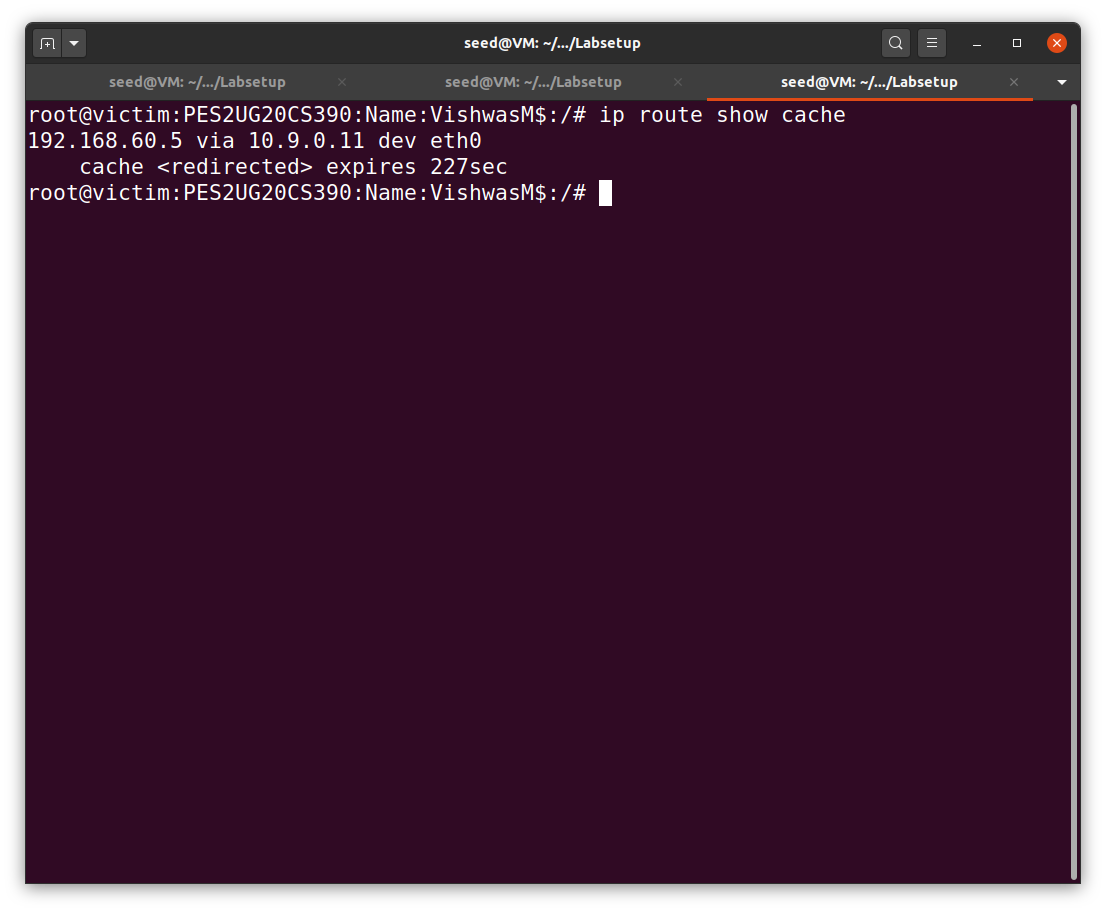
Step1:



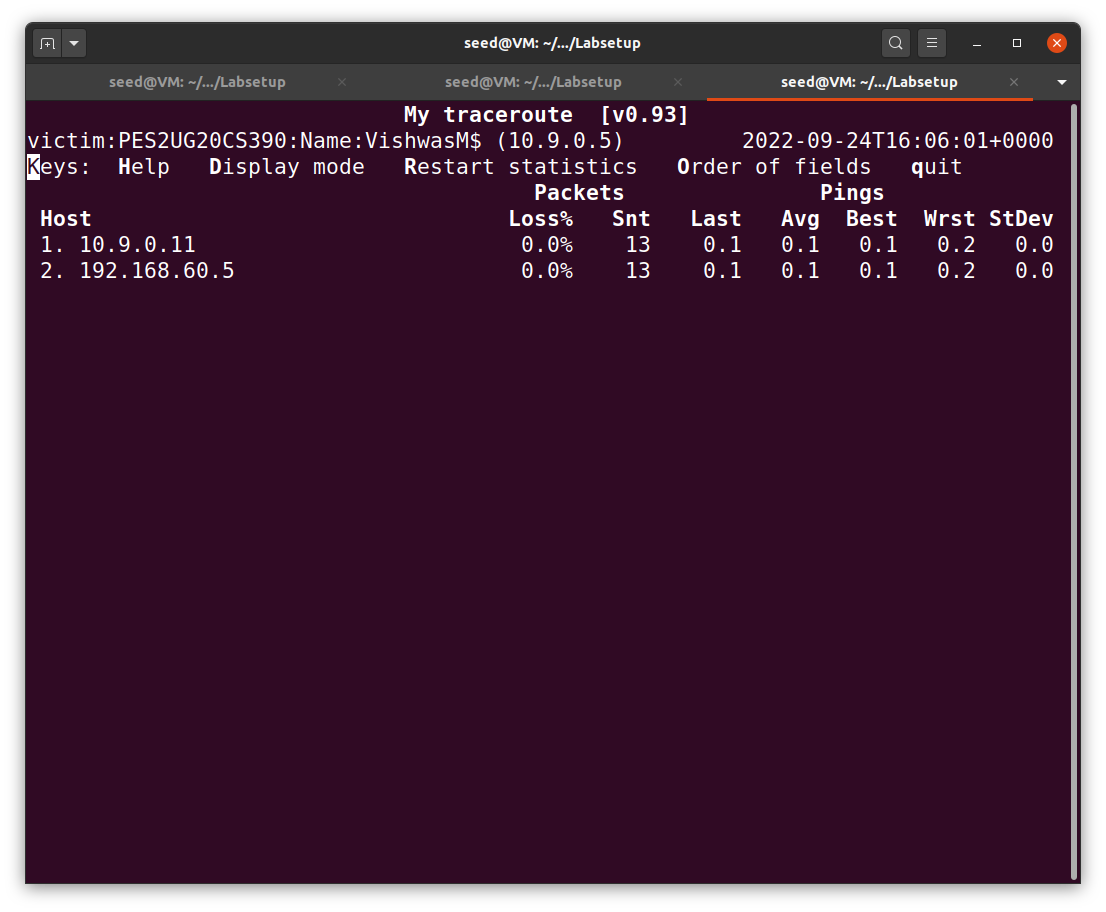
Step2:



Step3:



Step4:



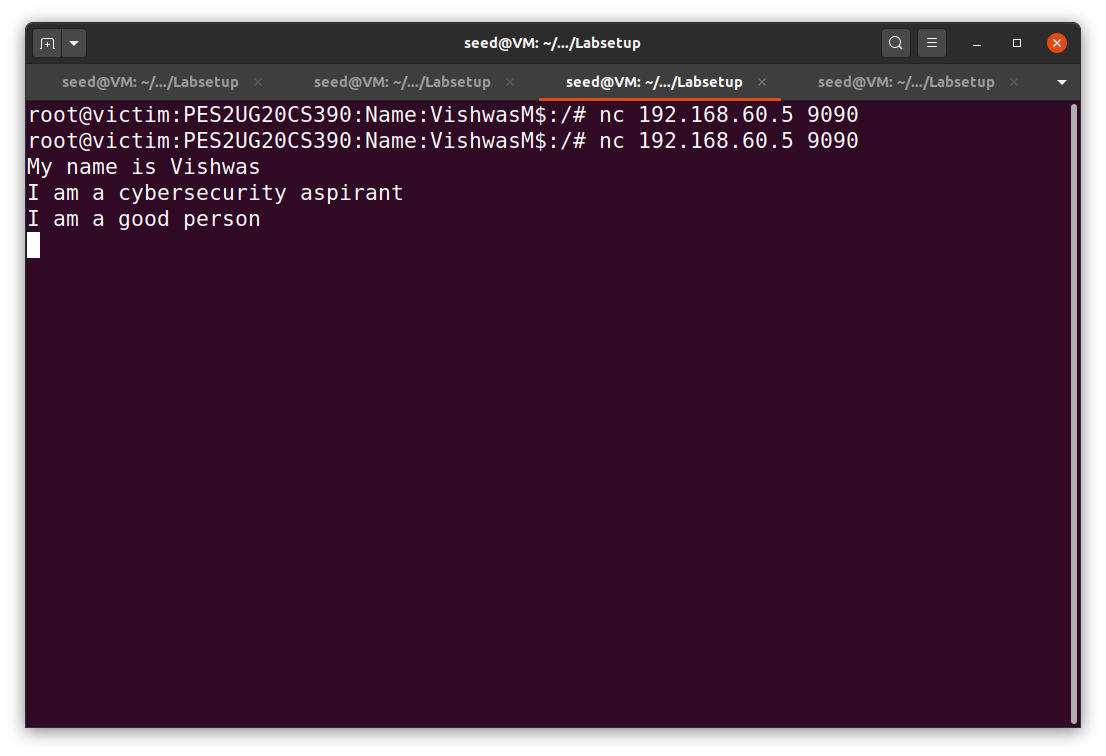
Task 2: Launching the MITM Attack

We should reset the changes that we did in the docker-compose.yml file in the earlier task. Then we have to execute all the steps in Task1 again. Then we have to continue with task2.

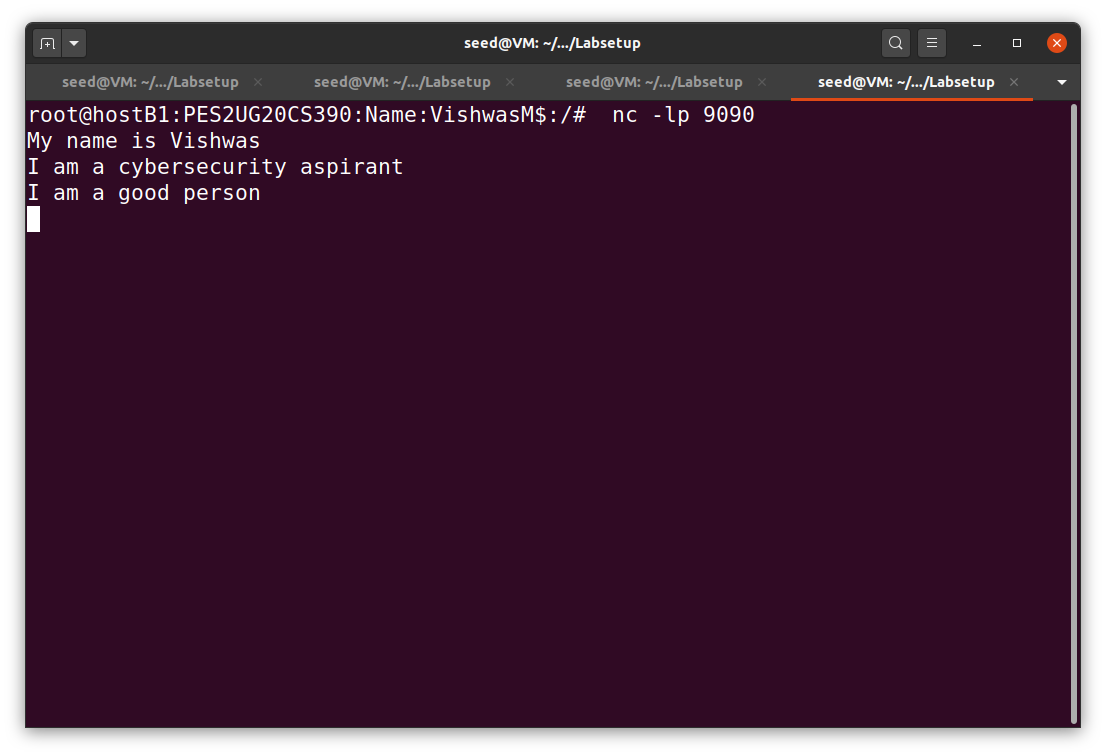
Task 2A -Netcat Connection:

Before launching the MITM attack, we start a TCP client and server program using netcat. On the destination container 192.168.60.5, start the netcat server:

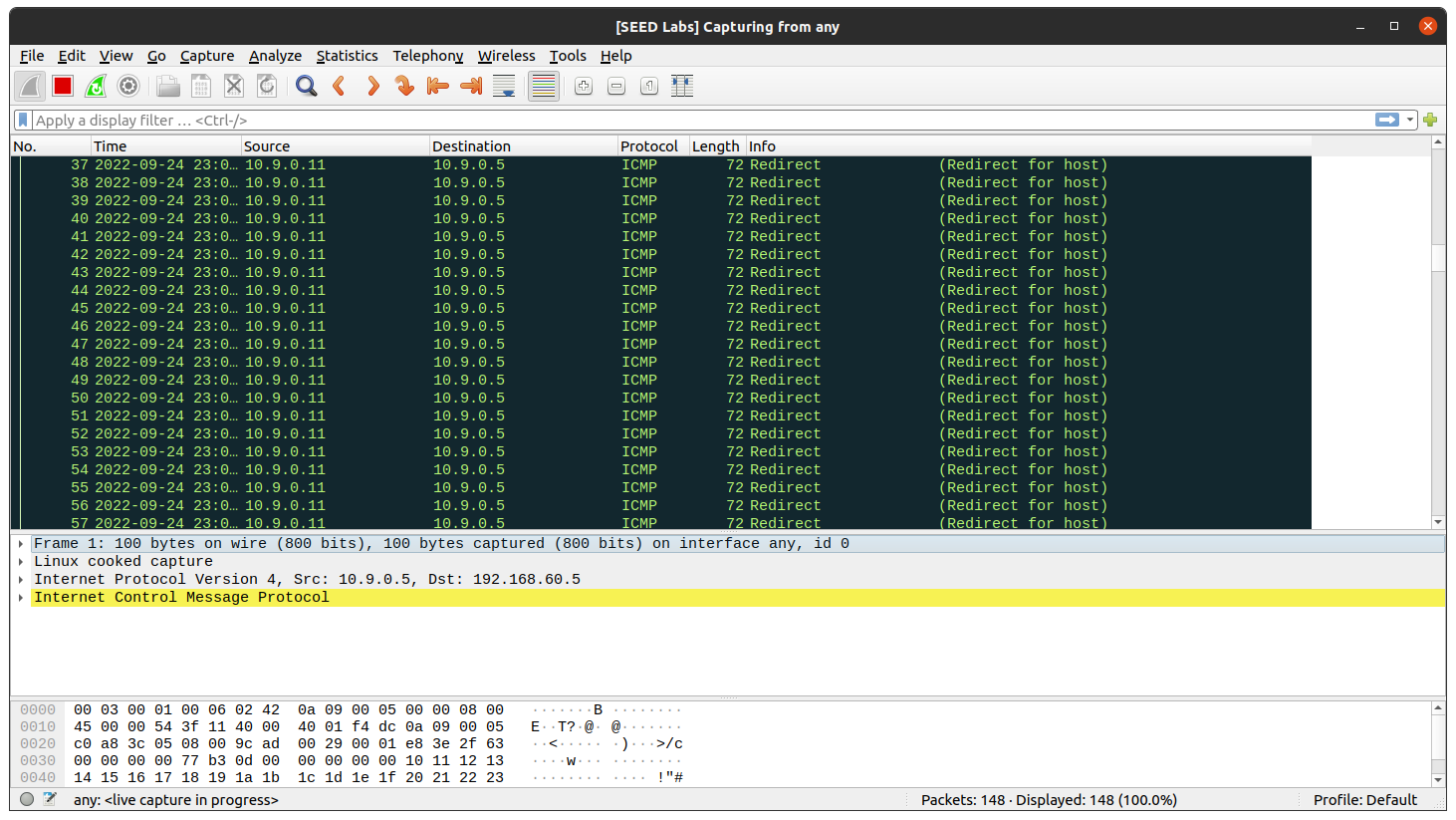
On the victim container, connect to the server:



On the victim container, connect to the server:

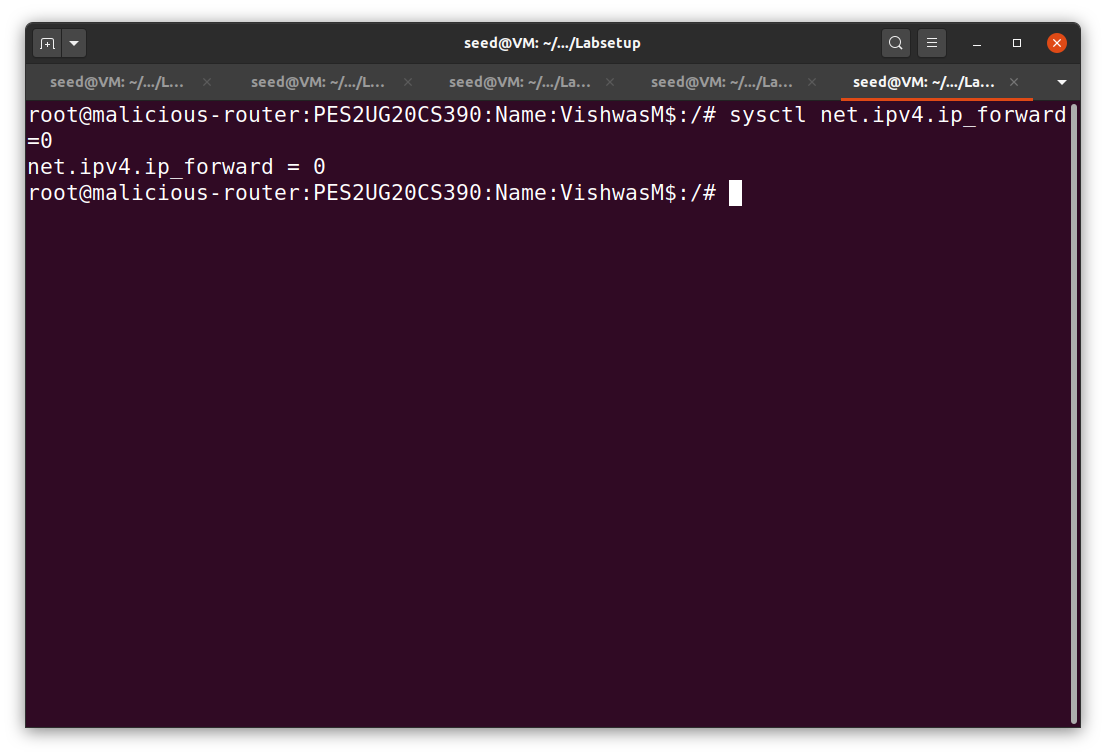


Wireshark image:

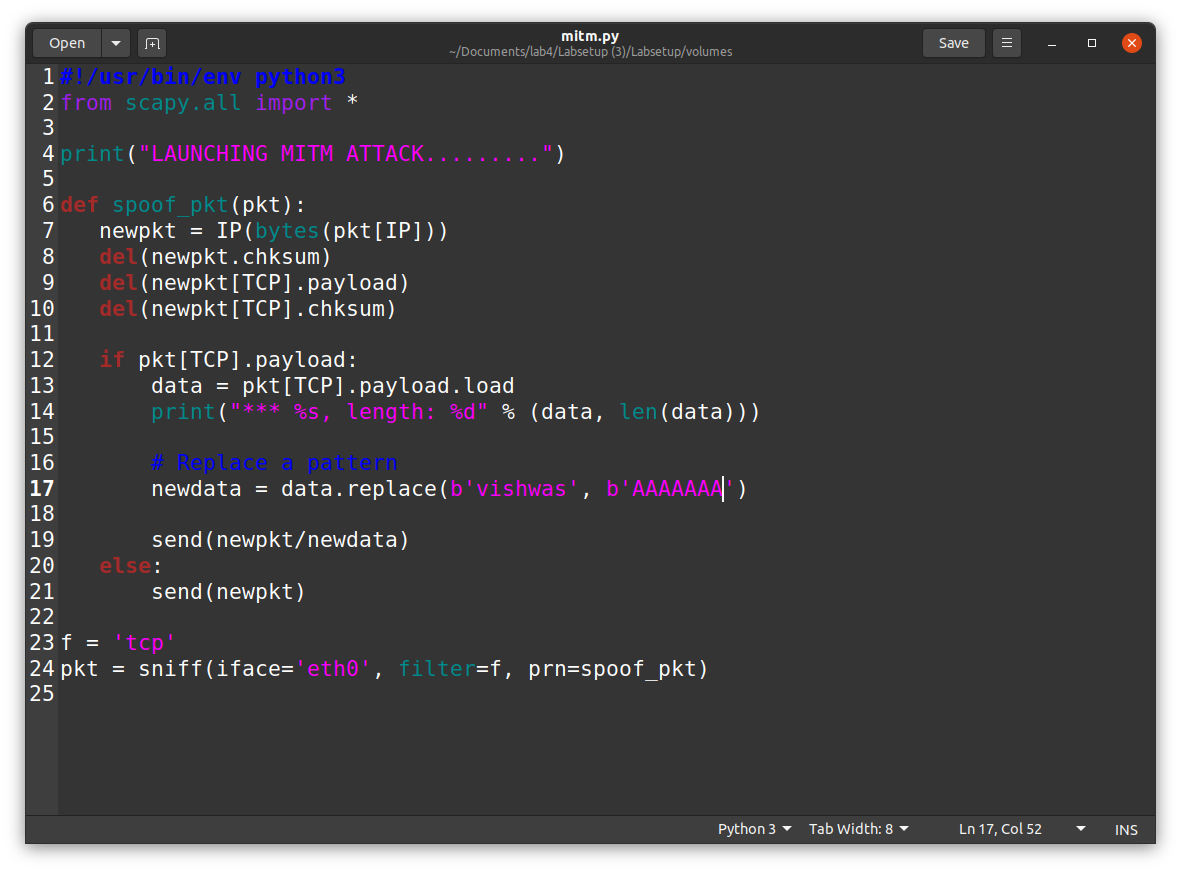


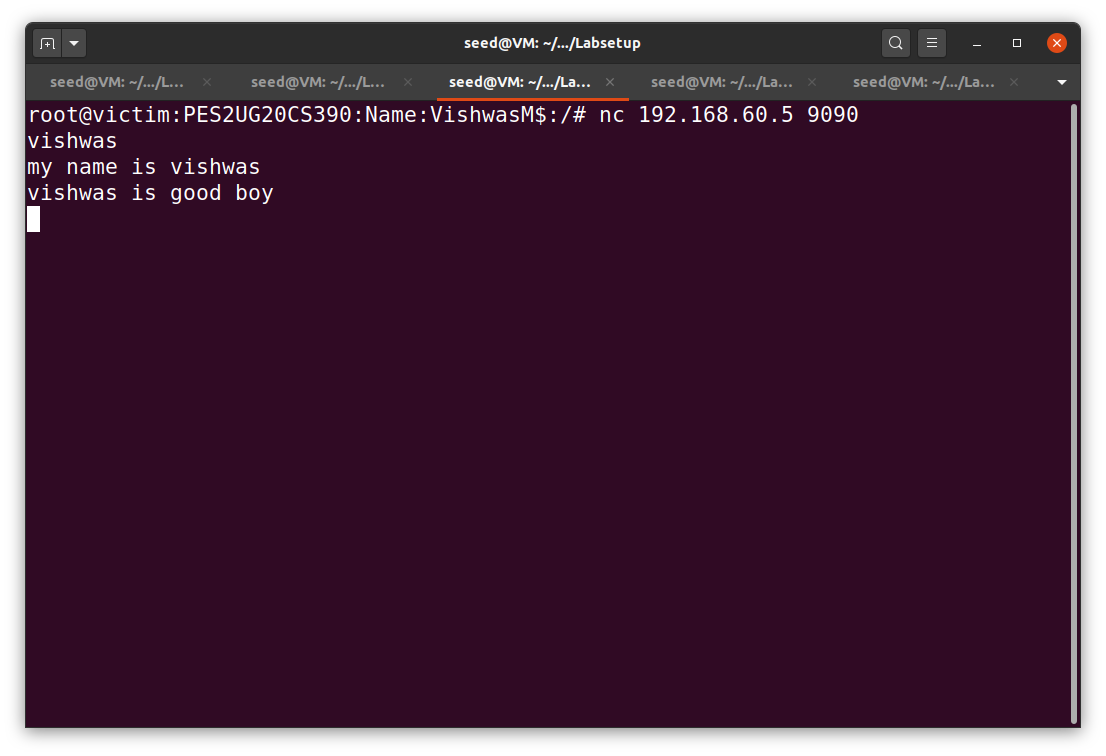
Task 2B -To launch the MITM Attack:

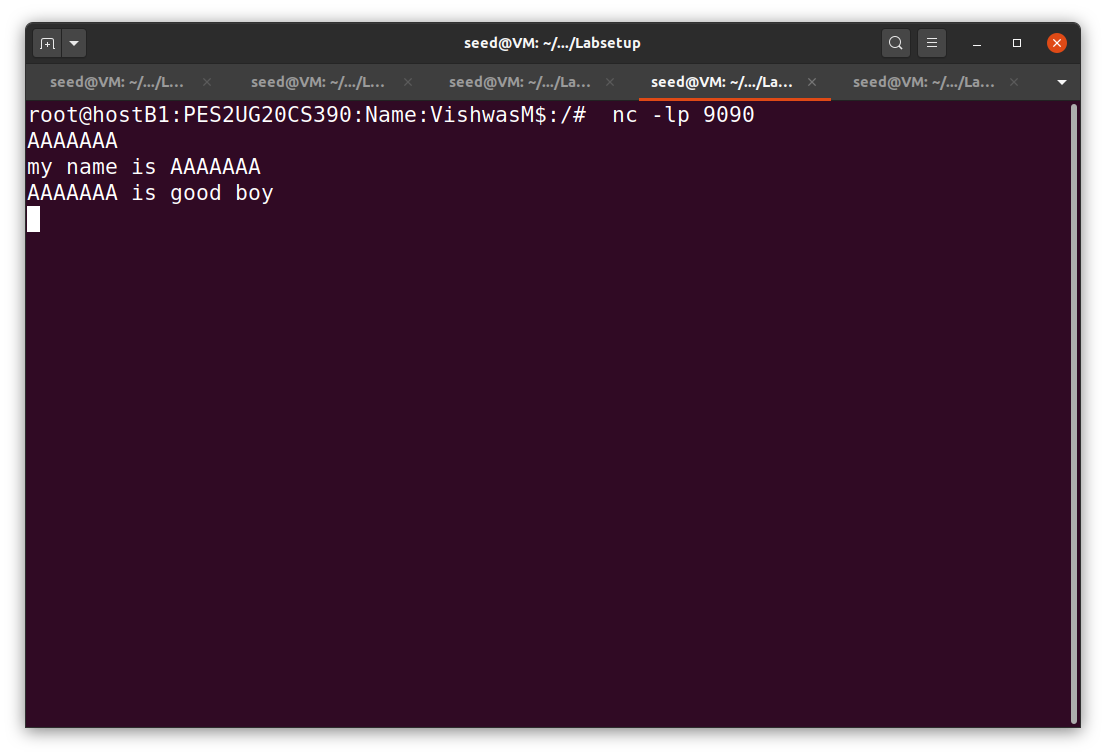
We should now have to replace every occurrence of your first name in the message with a sequence of A’s. The length of the sequence should be the same as that of your first name, or you will mess up the TCP sequence number, and hence the entire TCP connection. You need to use your real first name, so we know the work is done by you.



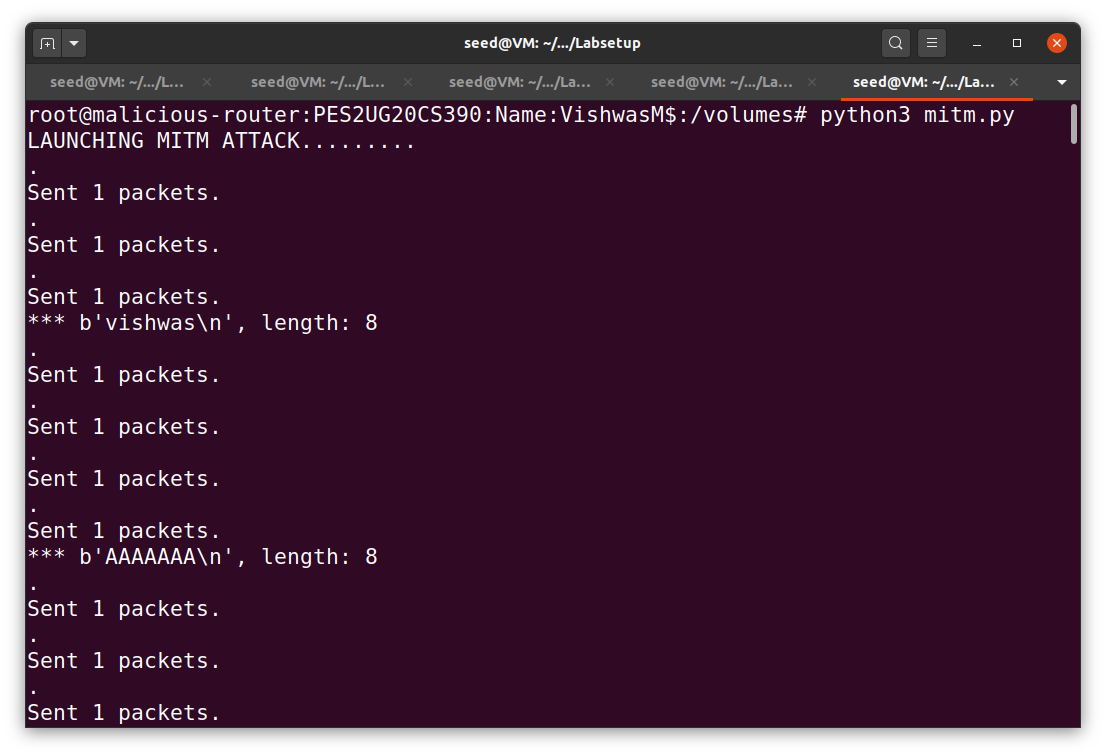
Code snippet:







On the malicious router terminal run the mitm attack.



Question 4: In your MITM program, you only need to capture the traffic in one direction. Please indicate which direction, and explain why.

Ans: We have to capture packets travelling only from source to destination because attacker can play role as either destination or source.

Question 5:

In the MITM program, when you capture the nc traffic from A (10.9.0.5), you can use A’s IP address or MAC address in the filter. One of the choices is not good and is going to create issues, even though both choices may work. Please try both, and use your experiment results to show which choice is the correct one, and please explain your conclusion

1. For using A’s IP address as a filter, change the variable ‘f’ (mitm.py) value to -‘tcp and src host 10.9.0.5’

Ans: Error will not occur in dis case as the packets are travelling properly from source to destination.

1. For using A’s MAC address as a filter, change the variable ‘f’ (mitm.py) value to -‘tcp and ether host 02:42:0a:09:00:05’

Ans: Error occurs here