An ICMP redirect is an error message sent by a router to the sender of an IP packet. Redirects are used when a router believes a packet is being routed incorrectly, and it would like to inform the sender that it should use a different router for the subsequent packets sent to that same destination. ICMP redirect can be used by attackers to change a victim's routing

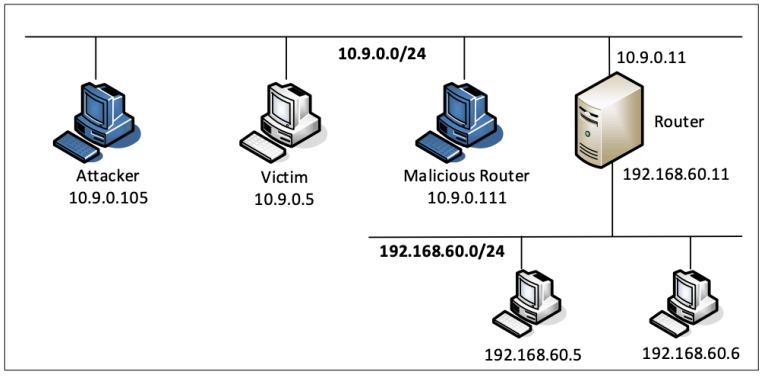


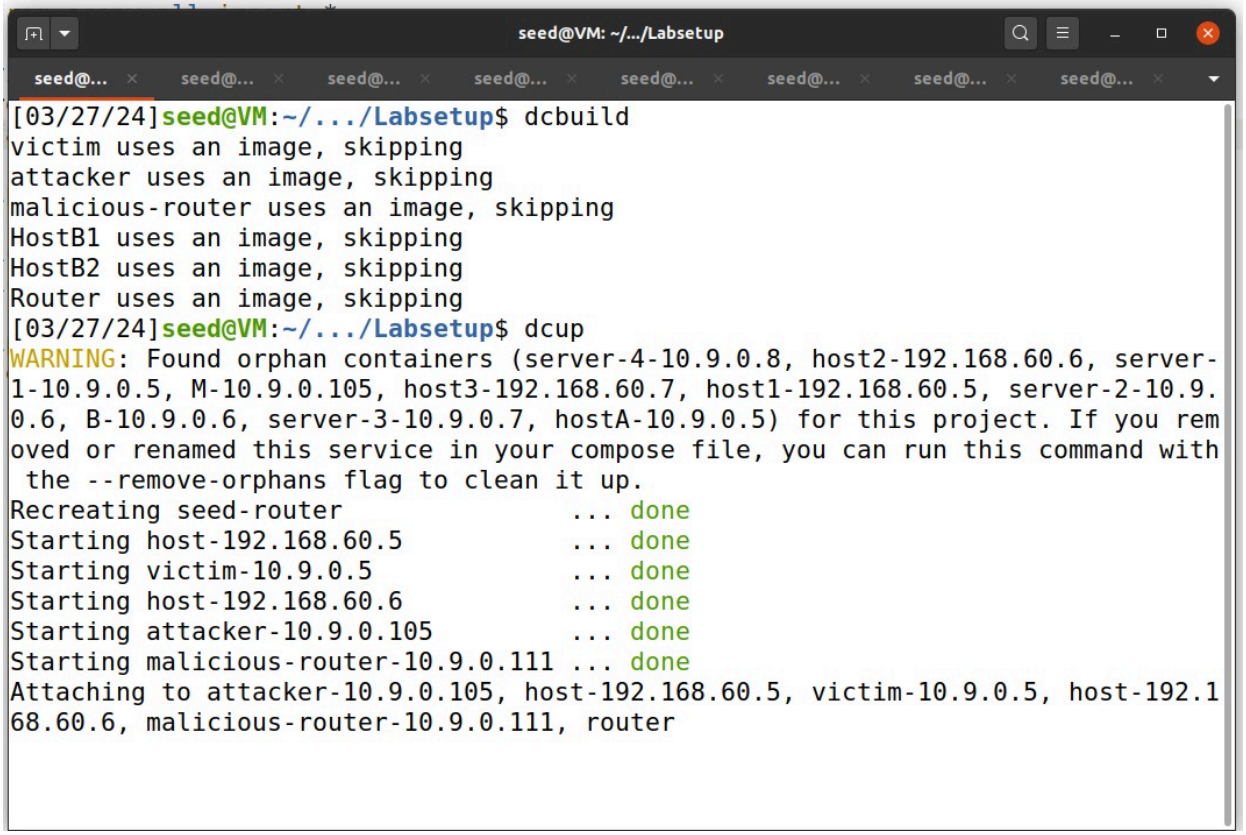
Figure 1: Lab environment setup

```
$ docker-compose build  # Build the container images
$ docker-compose up     # Start the containers
$ docker-compose down   # Shut down the containers

// Aliases for the Compose commands above
$ dcbuild       # Alias for: docker-compose build
$ dcup          # Alias for: docker-compose up
$ dcdown        # Alias for: docker-compose down
```

In this case, we intend to launch an ICMP redirect attack to alter the victim's routing behaviour. Essentially, we want to mislead the victim's system into thinking that our malicious router (IP address 10.9.0.111) is the proper gateway for reaching the destination IP 192.168.60.5.

This allows us to act as a "man-in-the-middle," intercepting and changing the victim's traffic before passing it to its intended destination. This type of attack uses ICMP protocol flaws to reroute the victim's traffic to our controlled router.

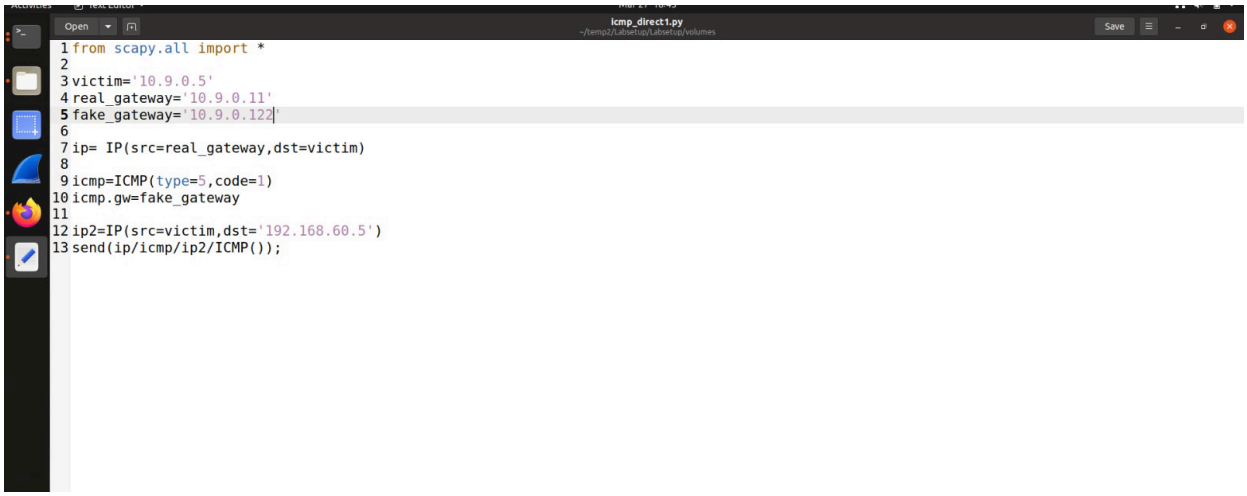
By successfully carrying out this assault, we obtain the power to eavesdrop on or manipulate the victim's conversations, potentially compromising critical information or launching more attacks. It poses a serious security risk, emphasizing the significance of protecting against ICMP-based exploits and implementing strong network security measures.



3 Task 1: Launching ICMP Redirect Attack

In the Ubuntu operating system, there is a countermeasure against the ICMP redirect attack. In the Compose file, we have already turned off the countermeasure by configuring the victim container to accept ICMP redirect messages.

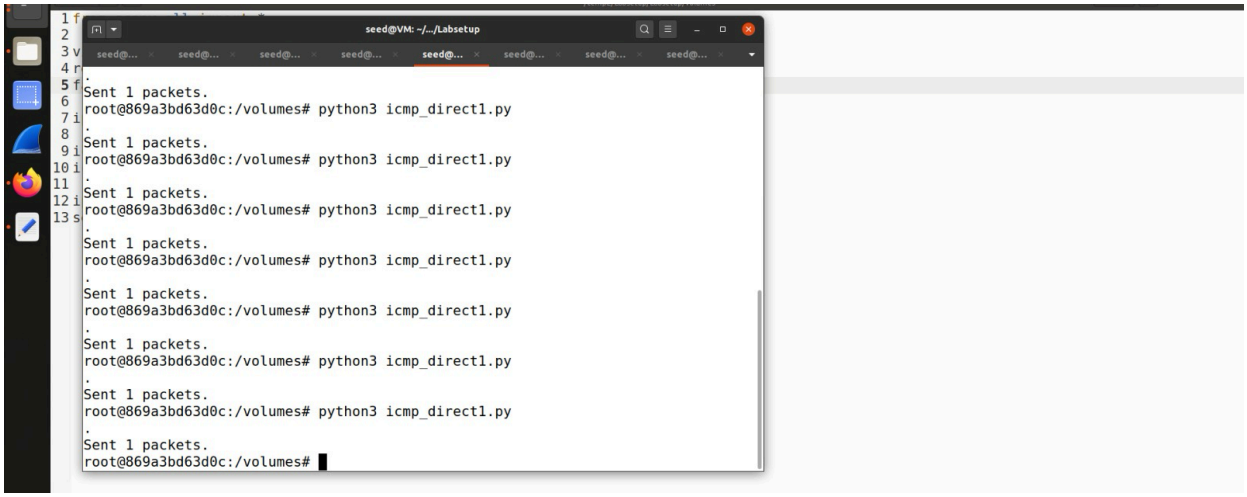
```
// In docker-compose.yml
sysctls:
      - net.ipv4.conf.all.accept_redirects=1

// To turn the protection on, set its value to 0
# sysctl net.ipv4.conf.all.accept_redirects=0
```



Using ping command on 192.168.60.5

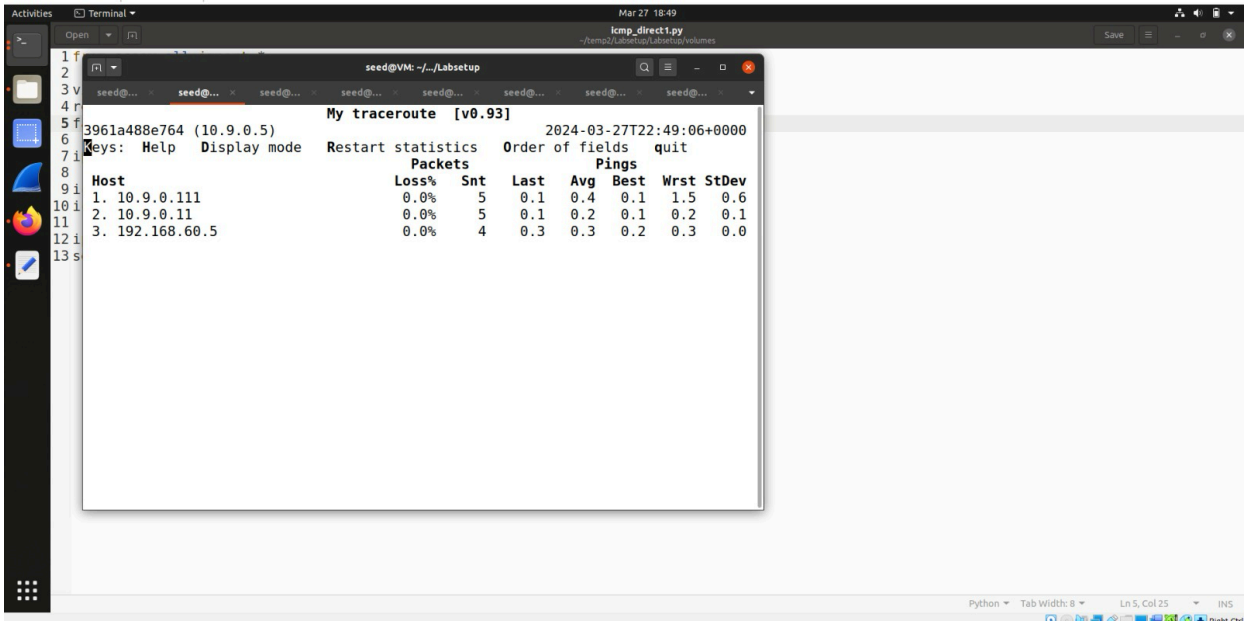
```
--- 192.168.60.5 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11272ms
rtt min/avg/max/mdev = 0.068/0.172/0.681/0.158 ms
root@3961a488e764:/# ip route show cache
root@3961a488e764:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=63 time=0.570 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.194 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.087 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.129 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.250 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.214 ms
```

After running the attack script on the attacker server, we observed a cache that was valid for a few seconds.



Now we do a traceroute on the victim machine using mtr -n 192.168.60.5 to see whether the packet is rerouted or not.

We can see the trace out here



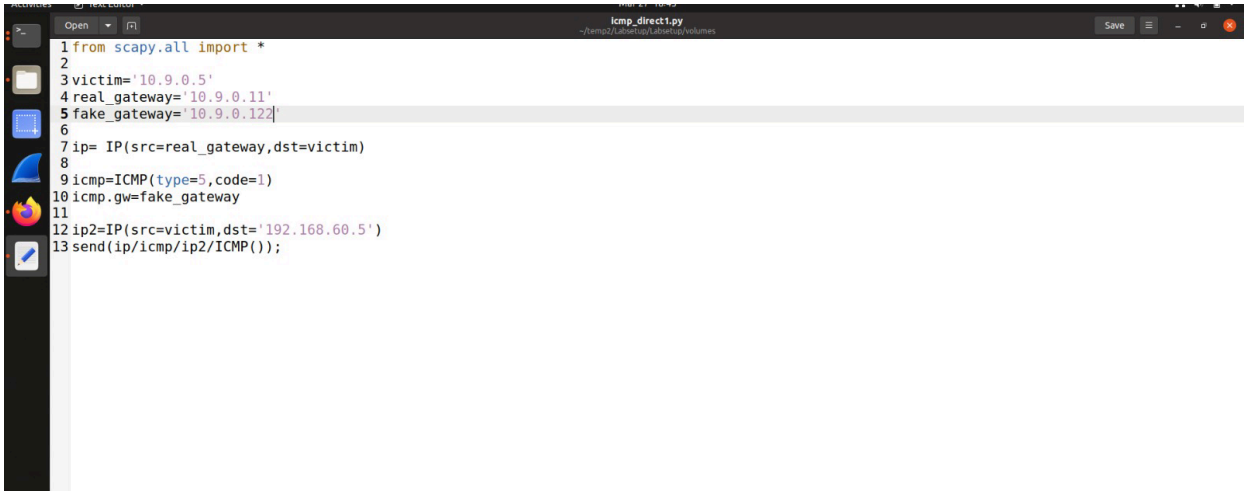
Question1 :
Can you use ICMP redirect attacks to redirect to a remote machine? Namely, the IP address assigned to icmp.gw is a computer not on the local LAN. Please show your experiment result, and explain your observation.

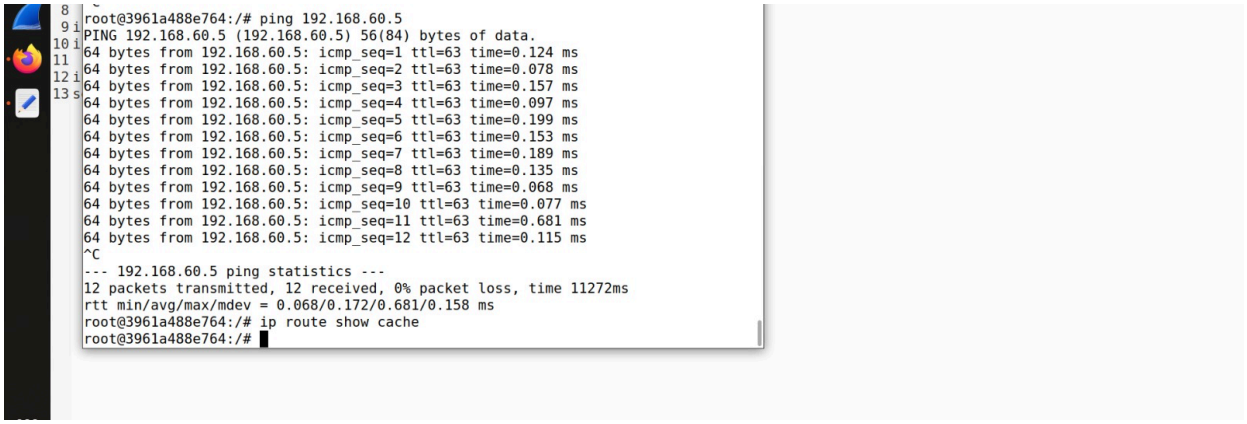
We try to do that by changing our python script and we see that .

The answer is given below.

```
--- 192.168.60.5 ping statistics ---
8 packets transmitted, 6 received, 25% packet loss, time 7086ms
rtt min/avg/max/mdev = 0.087/0.240/0.570/0.156 ms
root@3961a488e764:/# ip route show cache
192.168.60.5 via 10.9.0.111 dev eth0
    cache <redirected> expires 295sec
root@3961a488e764:/#
```

Question 2:
To answer this question we try to change the gateway the fake one to some value such as 10.9.0.122
And try to run the attack and below is the screen shot



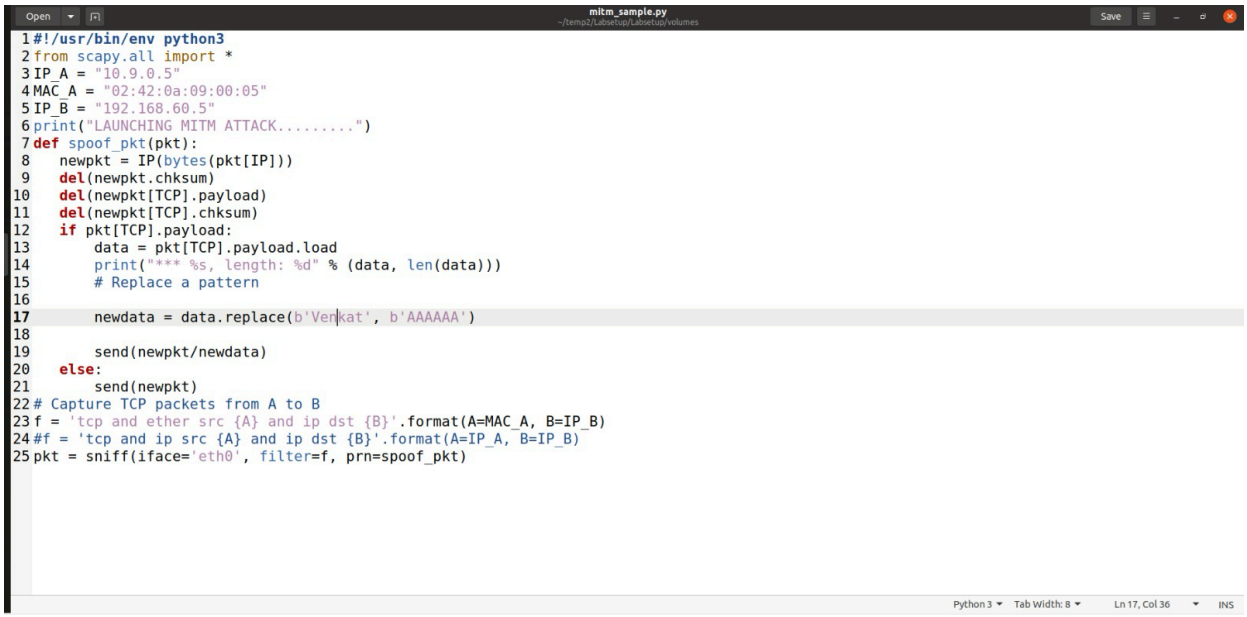


.
We observe there is no output as we are trying to redirect the icmp attack to nonexistence in the network.

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: we see that we fail to the attack as the redirect does not exist to the fake gateway. Again we try to make it zero and launch the attack we have successfully got the cache for.

4. TASK 2

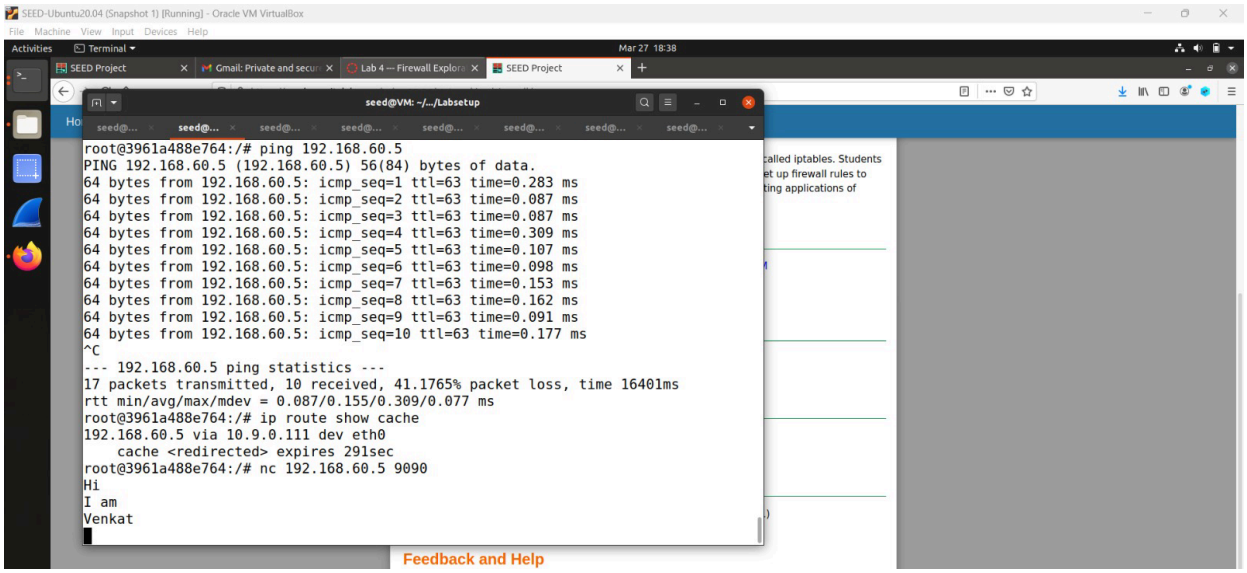


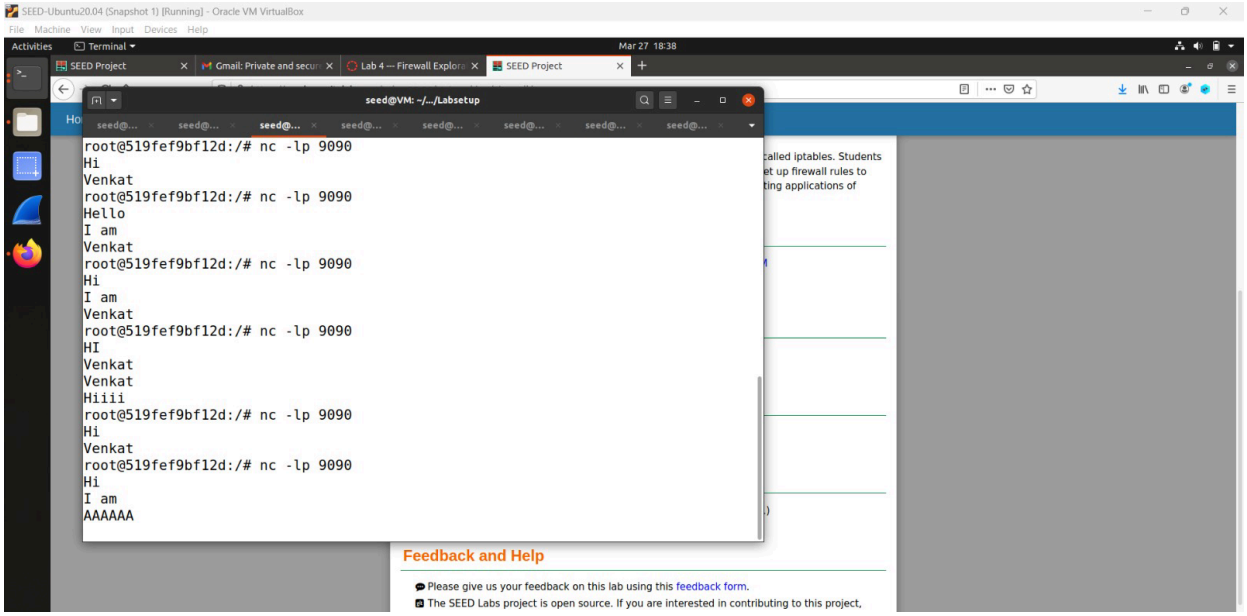
In this scenario, after deactivating IP forwarding on the victim's PC, our application must step in and take over the task of forwarding packets from the victim to the target. However, since the kernel's ICMP mechanism will not transfer packets intended for the target to us, we must take an alternative strategy.

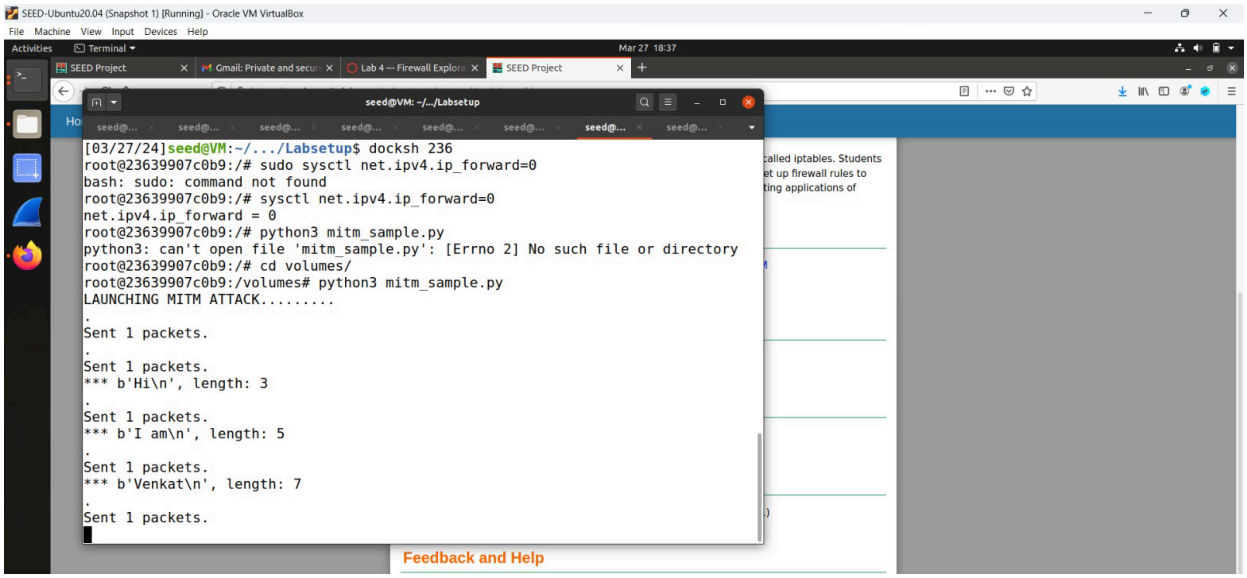
The MITM attack will be carried out using the sniff-and-spoof method. This means that our programme will function as a sniffer, intercepting packets from the victim and modifying them before sending them to their intended destination. Essentially, we are listening in on the victim's communication, making changes as needed, and then sending them along.

For example, suppose we are eavesdropping TCP traffic. Our programme takes these packets, modifies them as necessary, and then sends them out. This allows us to alter the communication between the victim and the target without their knowledge.

By effectively applying this sniff-and-spoof technique, we obtain control of the communication flow and have the opportunity to intercept sensitive information or launch additional network attacks. It emphasizes the need of having comprehensive security measures to guard against such assaults and the need for vigilance in securing networks.







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

Ans: A man-in-the-middle attack occurs when an unauthorized entity intercepts a data transmission or a live communication. The attackers insert themselves into the conversation and seem to be actual participants. This allows them to distribute malicious links or content to real participants without being detected until it is too late. The intermediary, unobserved by the other parties, gradually modifies the discourse to either obtain sensitive information or cause harm. This form of attack is initiated by the victim and targets the host or server.

Question 5:
In the MITM program, when you capture the nc traffics 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
ICMP ATTACK
choices may work. Please try both, and use your experiment results to show which choice is the correct
one, and please explain your conclusion.

Ans: I conducted tests using two entities, referred to as A (with IP address 10.9.0.5) and B (with its own IP). Initially, I adjusted the filter to capture traffic from A by specifying its IP address,

while unselecting the filter that targets A. However, I later modified the filter to reject packets based on IP addresses, substituting "AAAAAA" for Venkat.

Despite these adjustments, the rogue router continued to transmit packets. However, when I incorporated MAC and IP addresses into the filter, an MITM attack was successfully executed. Using the MAC address as a filter made the captured packets more comprehensible and easier to analyze compared to filtering solely by IP address.

Thus, based on the intended objective, employing the MAC address as a filter instead of the IP address is preferable.

Done by VENKATESH