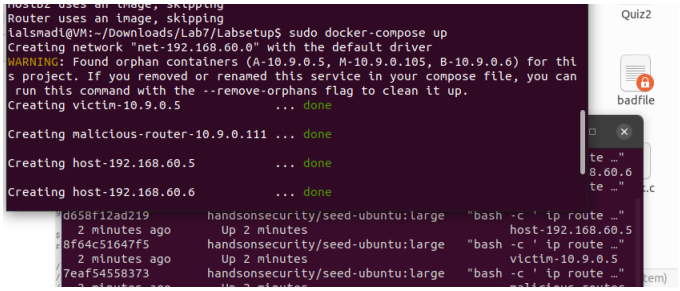
**Lab7_ICMP Redirect Attack**

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.

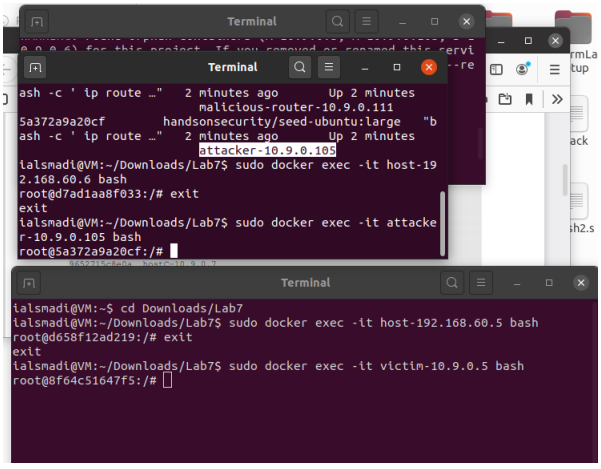
The objective of this task is to launch an ICMP redirect attack on the victim, such that when the victim sends packets to 192.168.60.5, it will use the malicious router container (10.9.0.111) as its router. Since the malicious router is controlled by the attacker, the attacker can intercept the packets, make changes, and then send the modified packets out.

(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.)

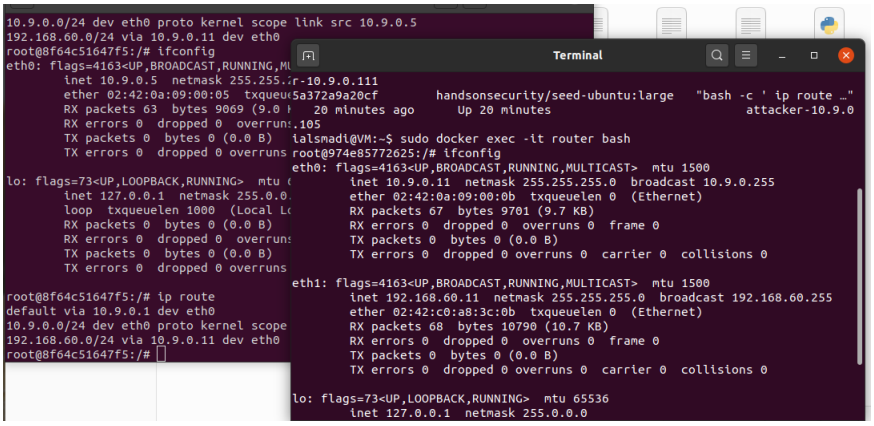
- Start the simulation network



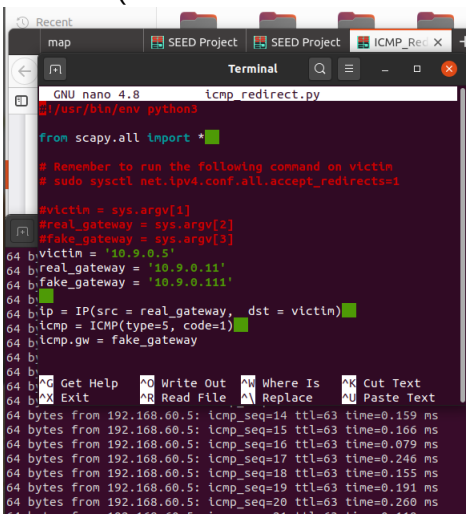

- For this task, we will attack the victim container from the attacker container. In the current setup, the victim will use the router container (192.168.60.11) as the router to get to the 192.168.60.0/24 network. If we run ip route on the victim container, we will see the following
- Login to the attacker and victim machines



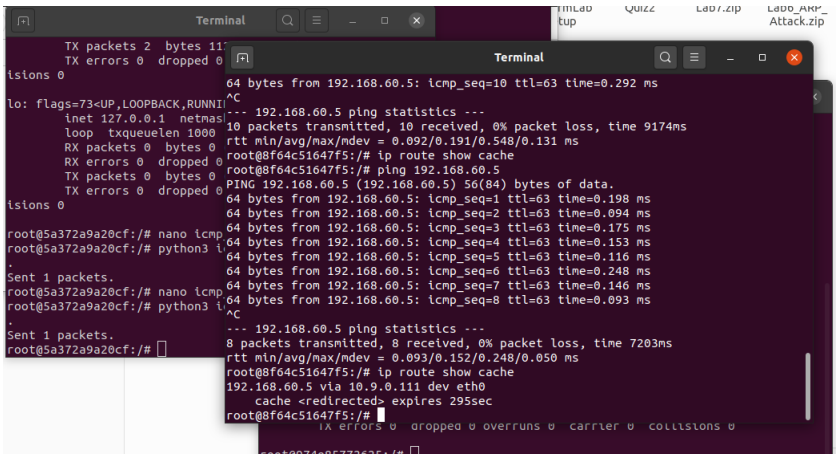
- In the current setup, the victim will use the router container (192.168.60.11) as the router to get to the 192.168.60.0/24 network. If we run ip route on the victim container, we will see the following




- We need to send out packets on the victim machine, or the ICMP redirect will not work. Start pinging on the victim machine, then create the icmp_redirect.py code on the attacker machine (run the attacker code while pining is running




- If attack is successful you should see the text below when you type (ip route show cache): in the victim machine



- From the route cache, we can see that the route to `192.168.60.5` on the victim container has changed to `10.9.0.111`, which is our malicious router. If you don't get this result, run `icmp_redirect.py` multiple times while the ping command is still running. (Also make sure all 4 machines are running, victim, original router, malicious router and attacker)
- We can further check the actual route by running the `mtr` traceroute command. From the result, we can see that packets do go through our malcious router.

- Continue to the rest of the lab