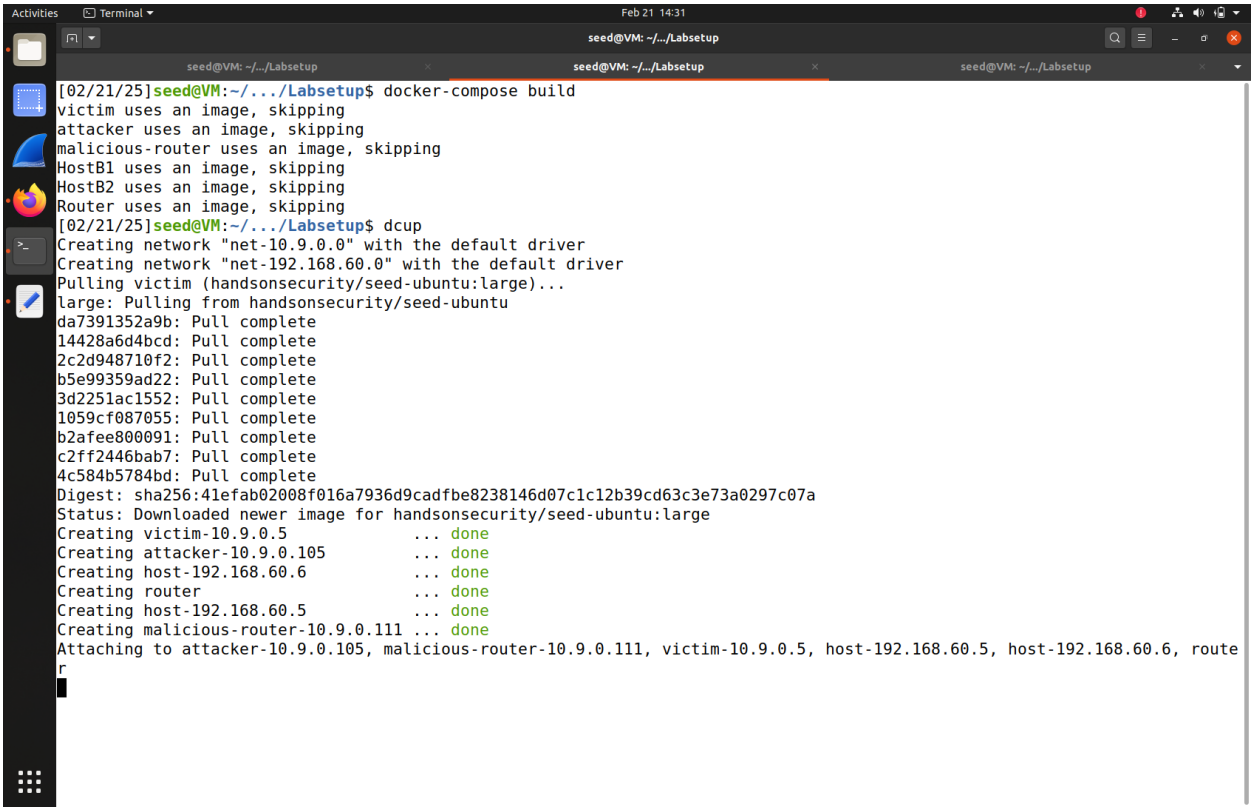
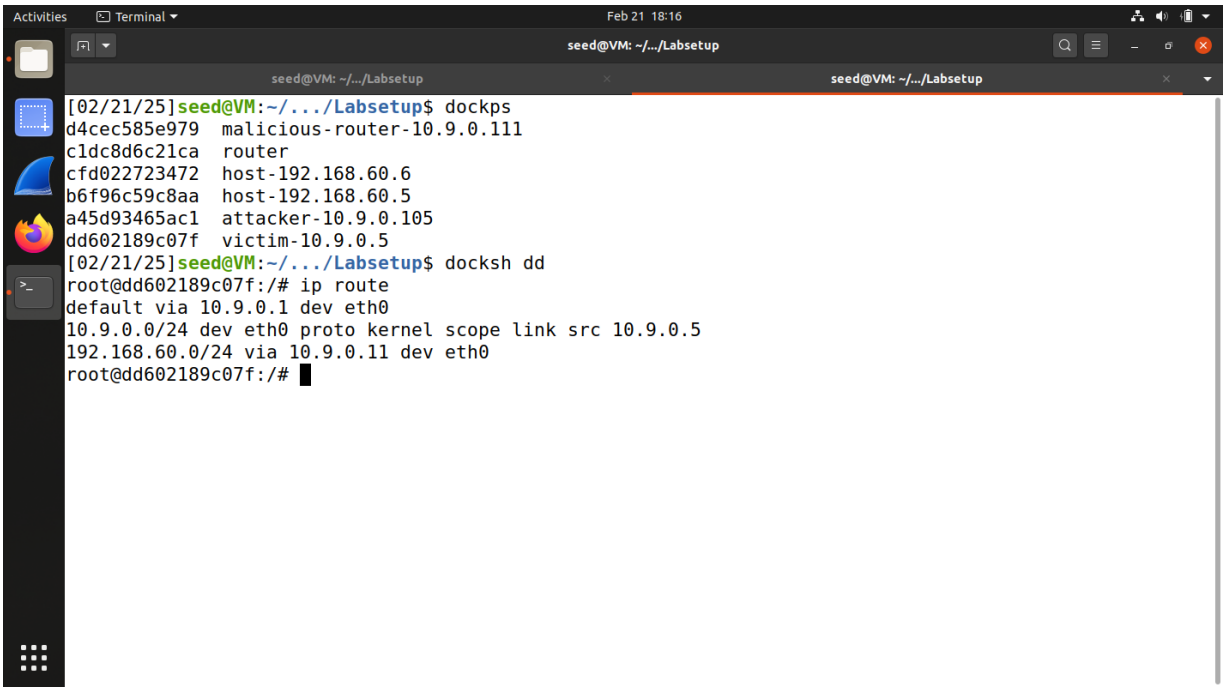
Lab 3 Report

Alexandria Deleon

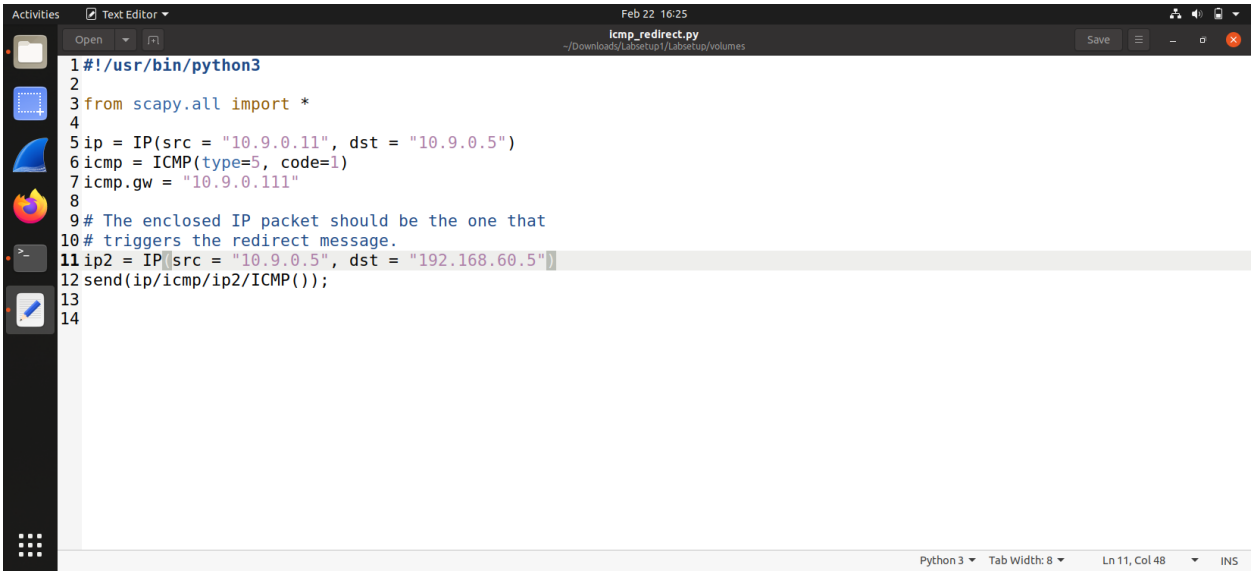


This is showing the setting up of the lab environment.

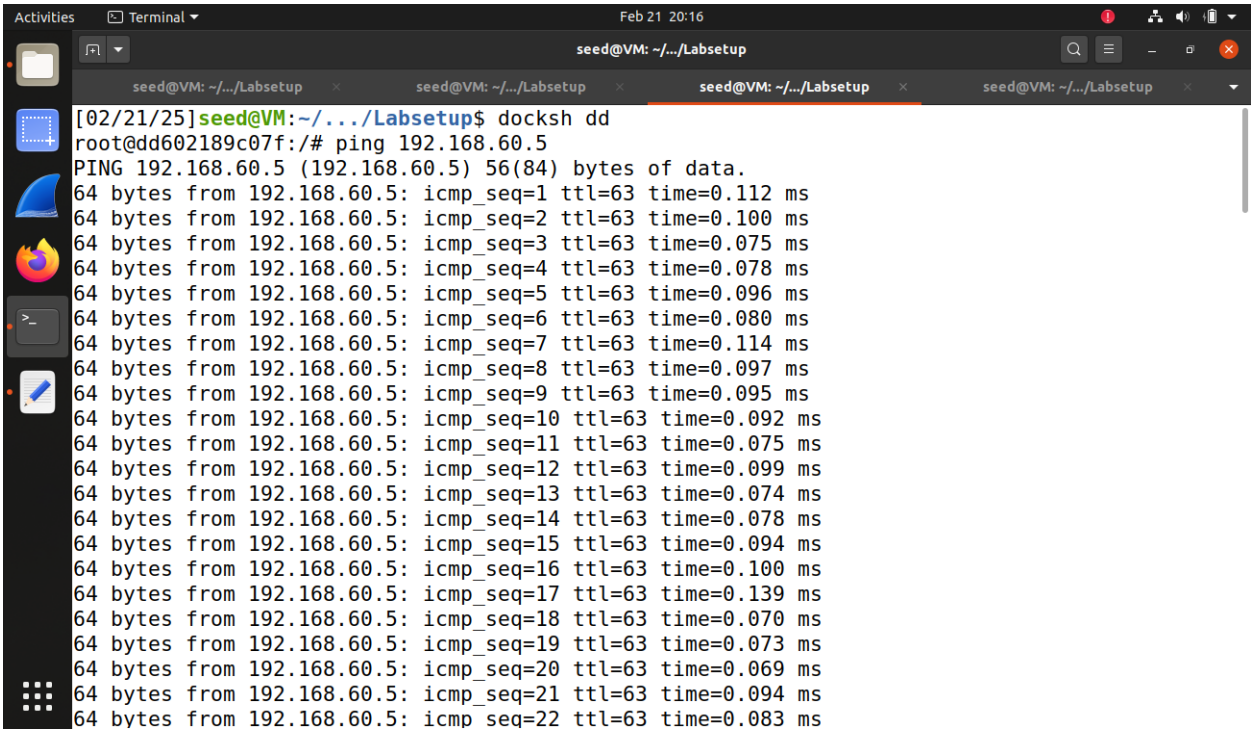
Task 1:



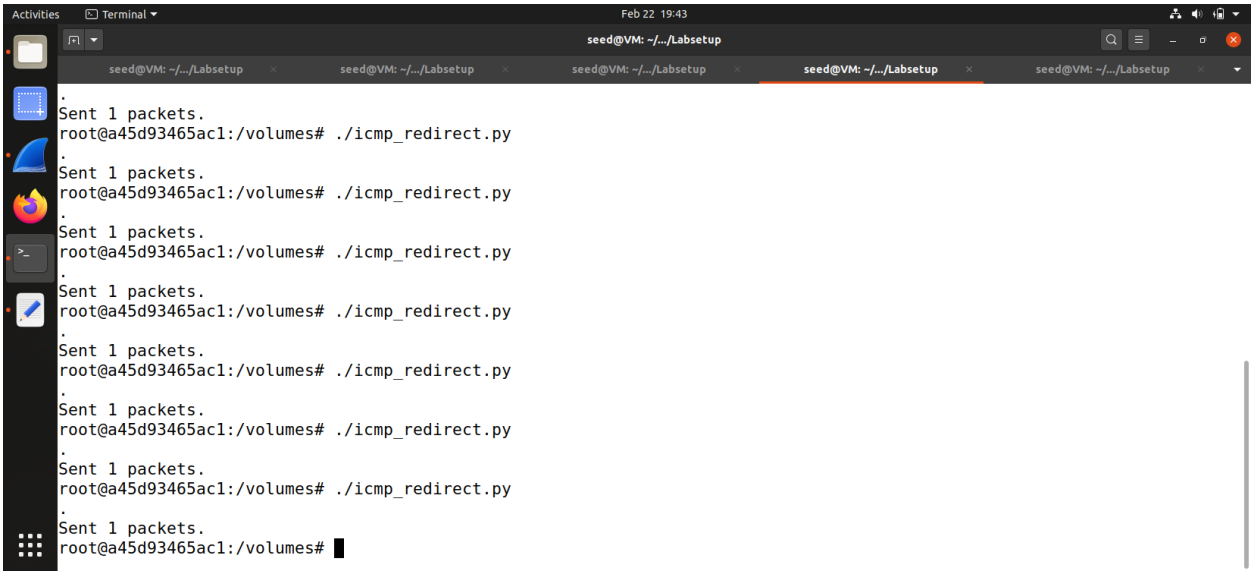
This is showing the current setup for the victim container.



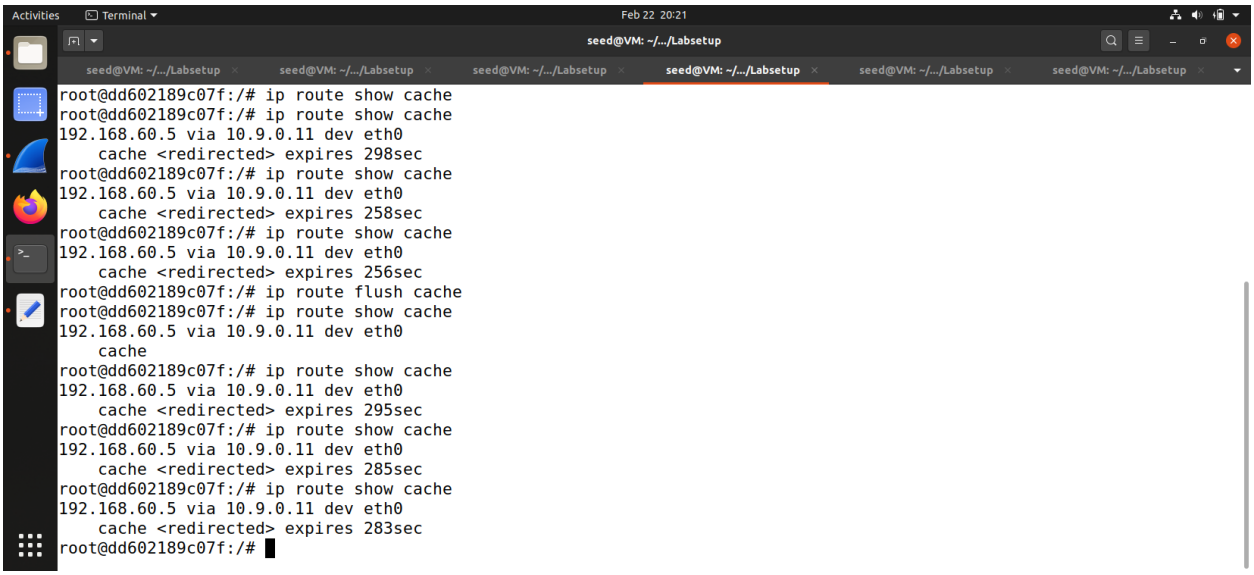
This is showing the created python file to redirect the packets.



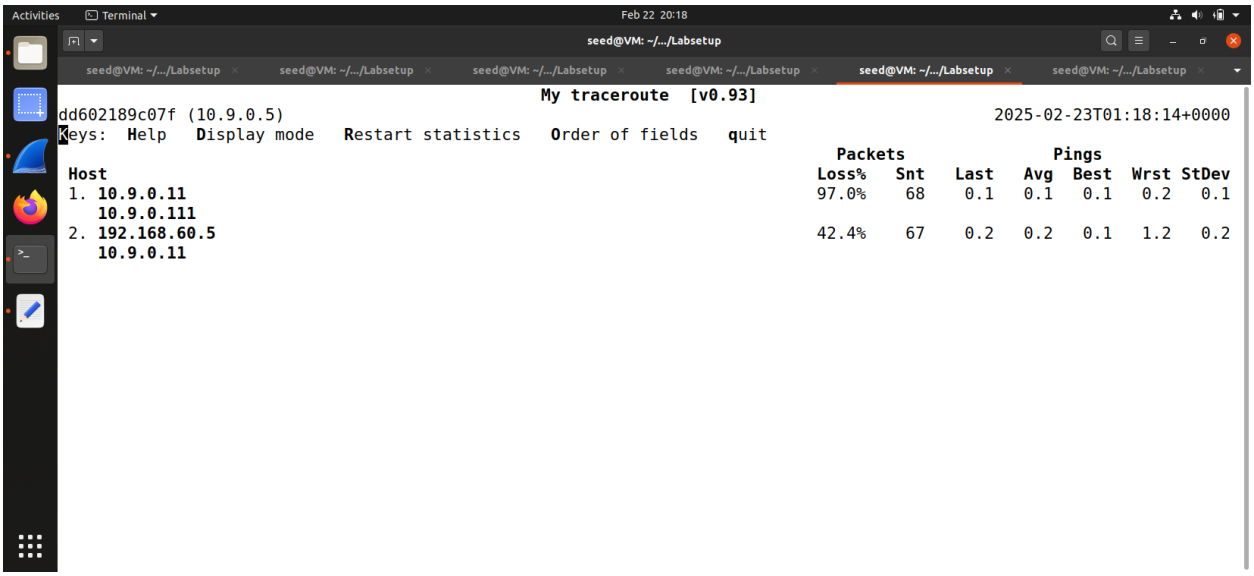
Performing a ping from victim container to host.



This shows me redirecting the packets using the created python file.



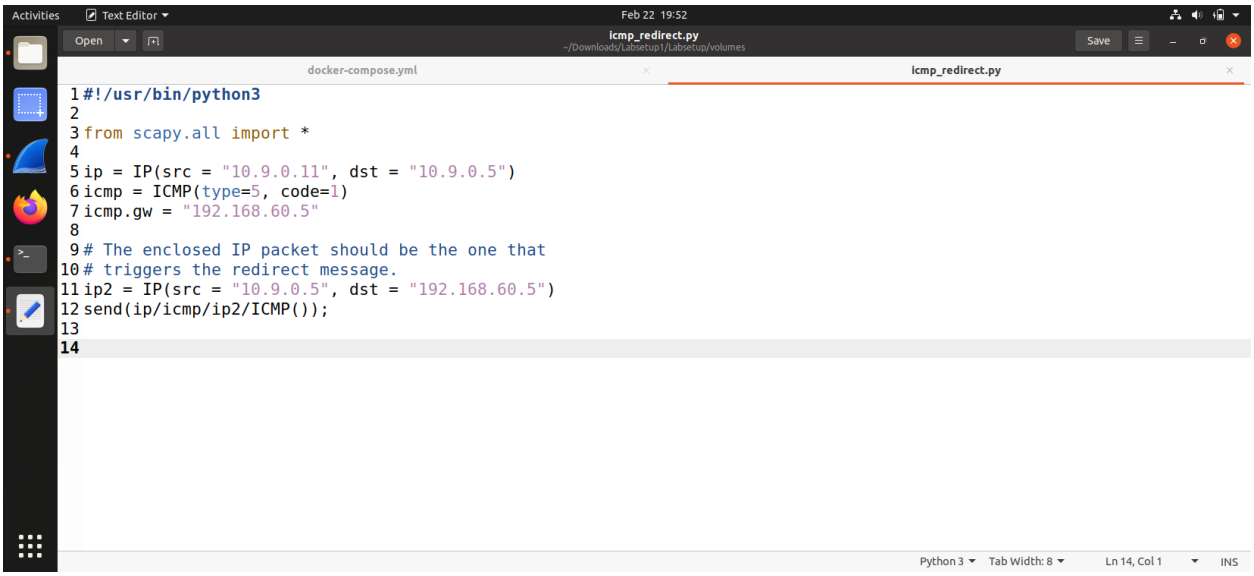
This shows how I was trying to show the cache. The result shows I was successful in the attack.

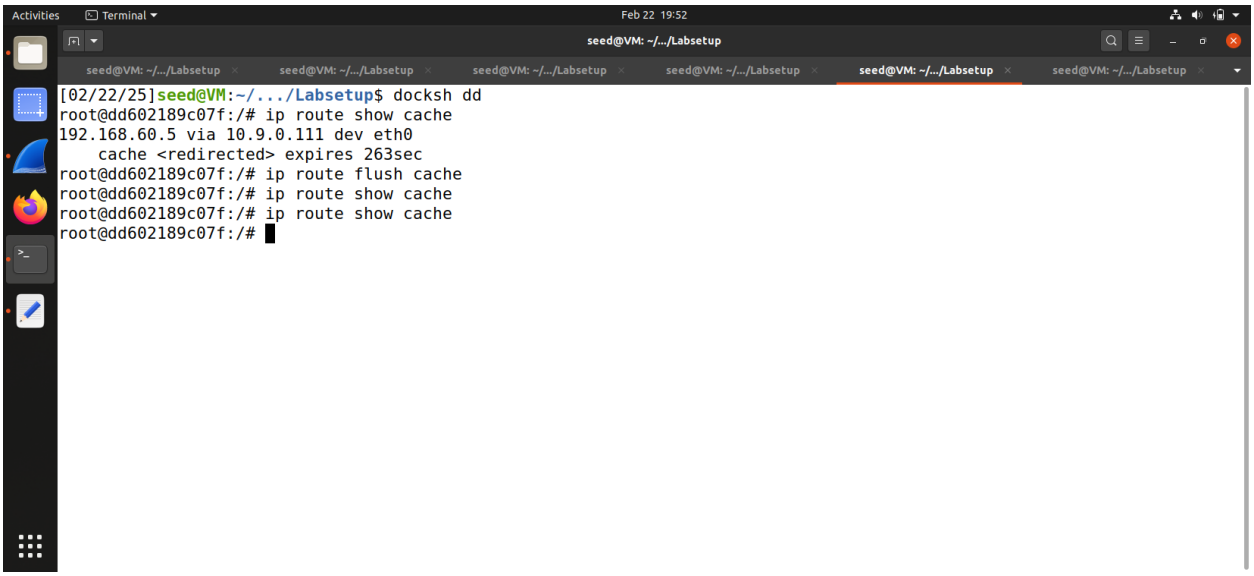


This shows the traceroute of the victim machine. The packets were successfully redirected.

Question 1: 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.

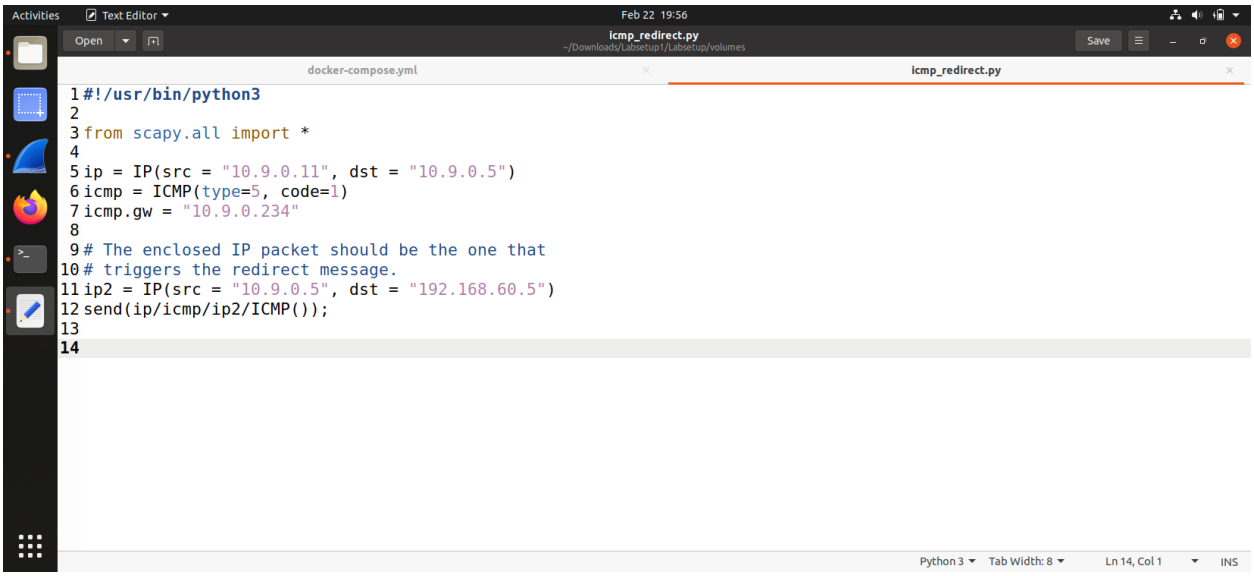
- To try to accomplish this I changed the icmp.gw to 192.168.60.5, but from what I observed, this does not result in a successful attack as nothing happened when I tried to show the cache.

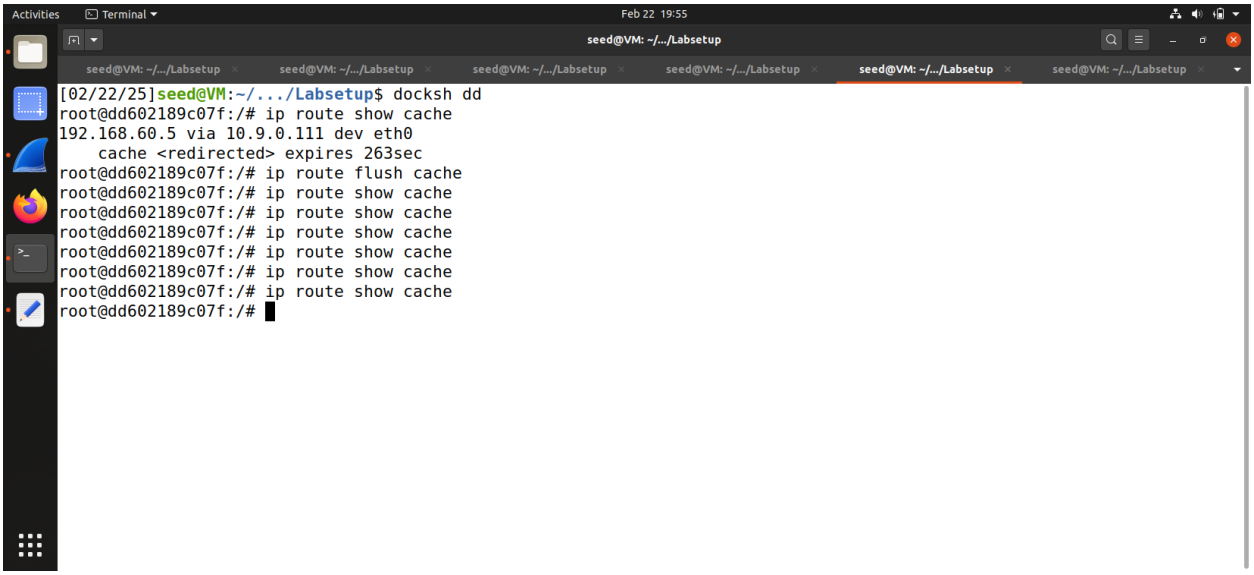




Question 2: Can you use ICMP redirect attacks to redirect to a non-existing machine on the same network? Namely, the IP address assigned to icmp.gw is a local computer that is either offline or non-existing. Please show your experiment result, and explain your observation.

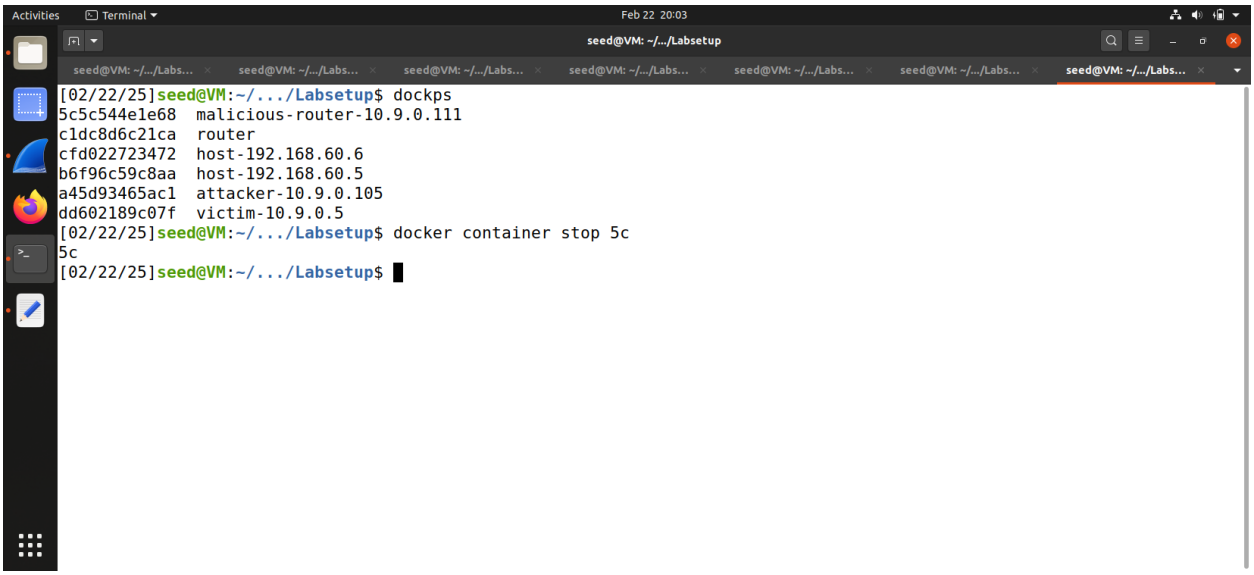
- To redirect the attacks to a non-existing machine I changed the icmp.gw to 10.9.0.234. This did not result in a successful attack as the machine does not exist and wouldn't be able to do anything.

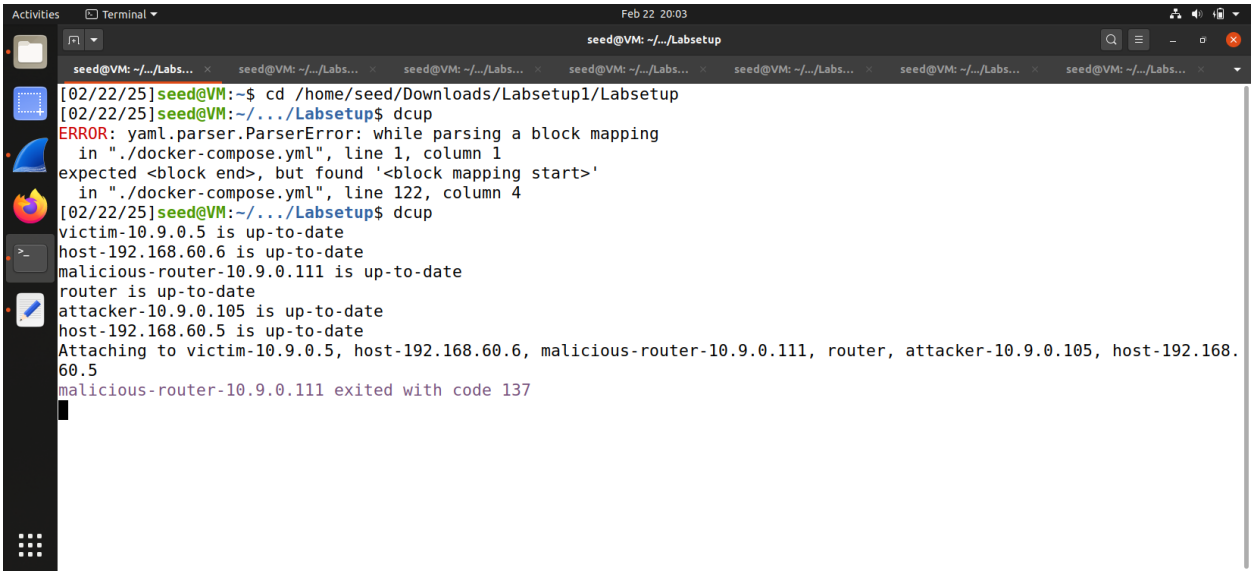


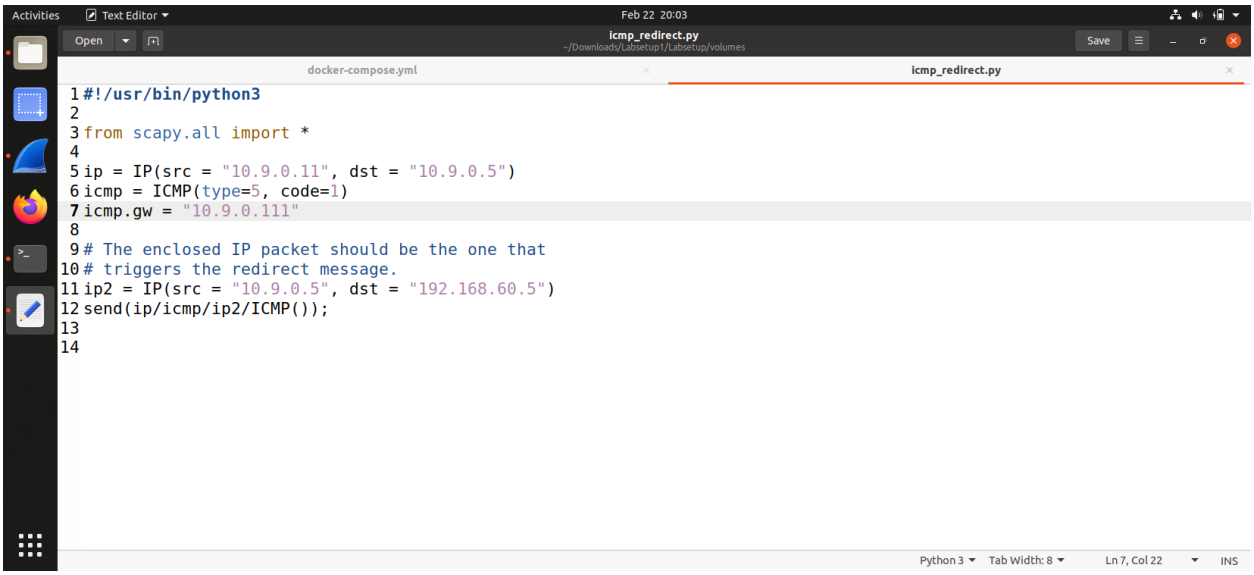


This shows that the attack was not successful as no cache was shown.

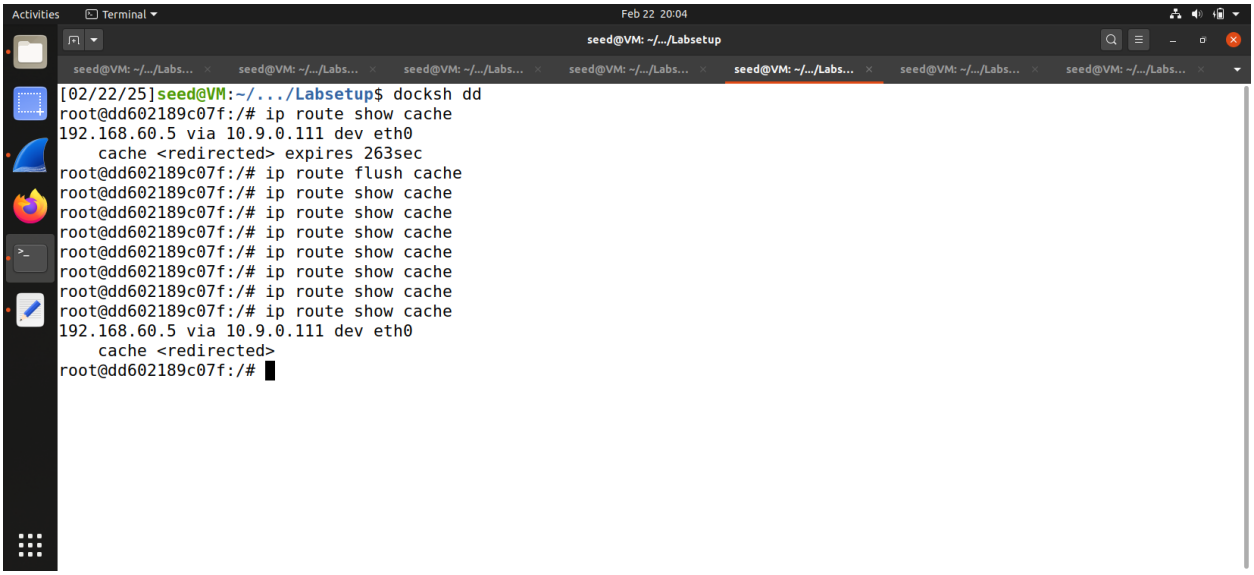
Next, I attempted to redirect attacks to a machine that was offline. I did this by turning off the malicious router and replacing the icpm.gw to its ip address.


Activities
Terminal
Feb 22 20:03
seed@VM: ~/.../Labsetup
[02/22/25]seed@VM:~/.../Labsetup$ dockps
5c5c544e1e68 malicious-router-10.9.0.111
c1dc8d6c21ca router
cfd022723472 host-192.168.60.6
b6f96c59c8aa host-192.168.60.5
a45d93465ac1 attacker-10.9.0.105
dd602189c07f victim-10.9.0.5
[02/22/25]seed@VM:~/.../Labsetup$ docker container stop 5c
5c
[02/22/25]seed@VM:~/.../Labsetup$


Activities
Terminal
Feb 22 20:03
seed@VM: ~/.../Labsetup
[02/22/25]seed@VM:~$ cd /home/seed/Downloads/Labsetup1/Labsetup
[02/22/25]seed@VM:~/.../Labsetup$ dcup
ERROR: yaml.parser.ParserError: while parsing a block mapping
in "./docker-compose.yml", line 1, column 1
expected <block end>, but found '<block mapping start>'
in "./docker-compose.yml", line 122, column 4
[02/22/25]seed@VM:~/.../Labsetup$ dcup
victim-10.9.0.5 is up-to-date
host-192.168.60.6 is up-to-date
malicious-router-10.9.0.111 is up-to-date
router is up-to-date
attacker-10.9.0.105 is up-to-date
host-192.168.60.5 is up-to-date
Attaching to victim-10.9.0.5, host-192.168.60.6, malicious-router-10.9.0.111, router, attacker-10.9.0.105, host-192.168.60.5
malicious-router-10.9.0.111 exited with code 137

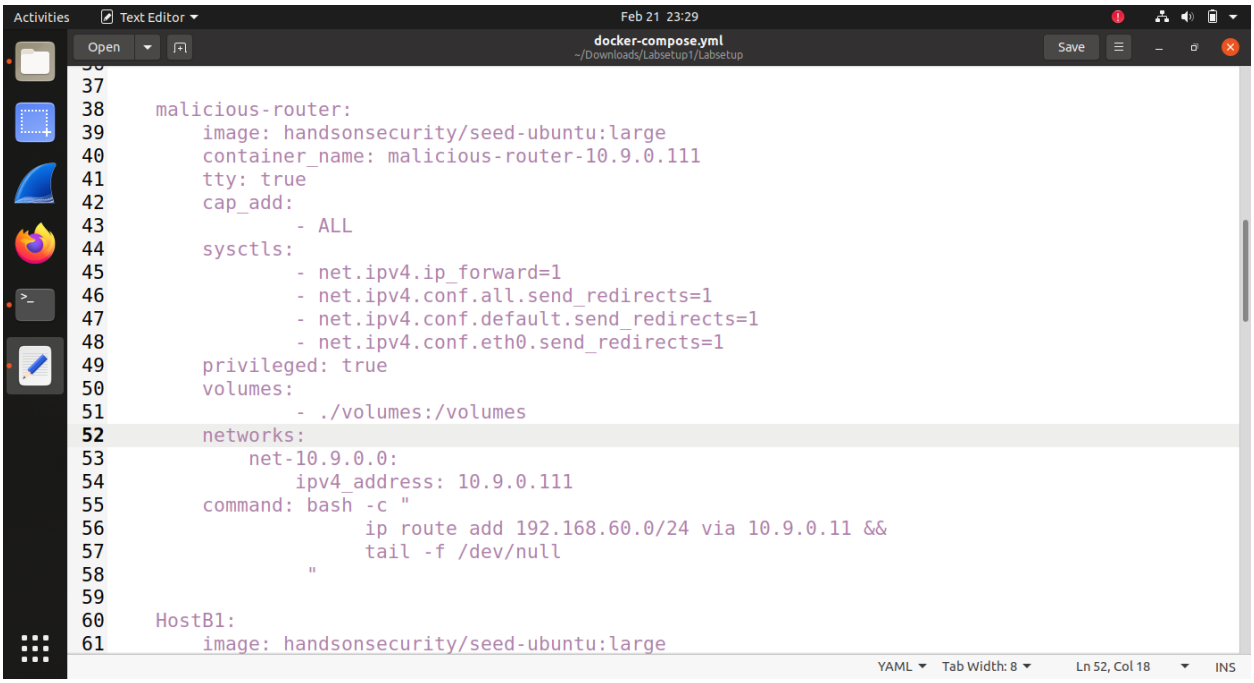


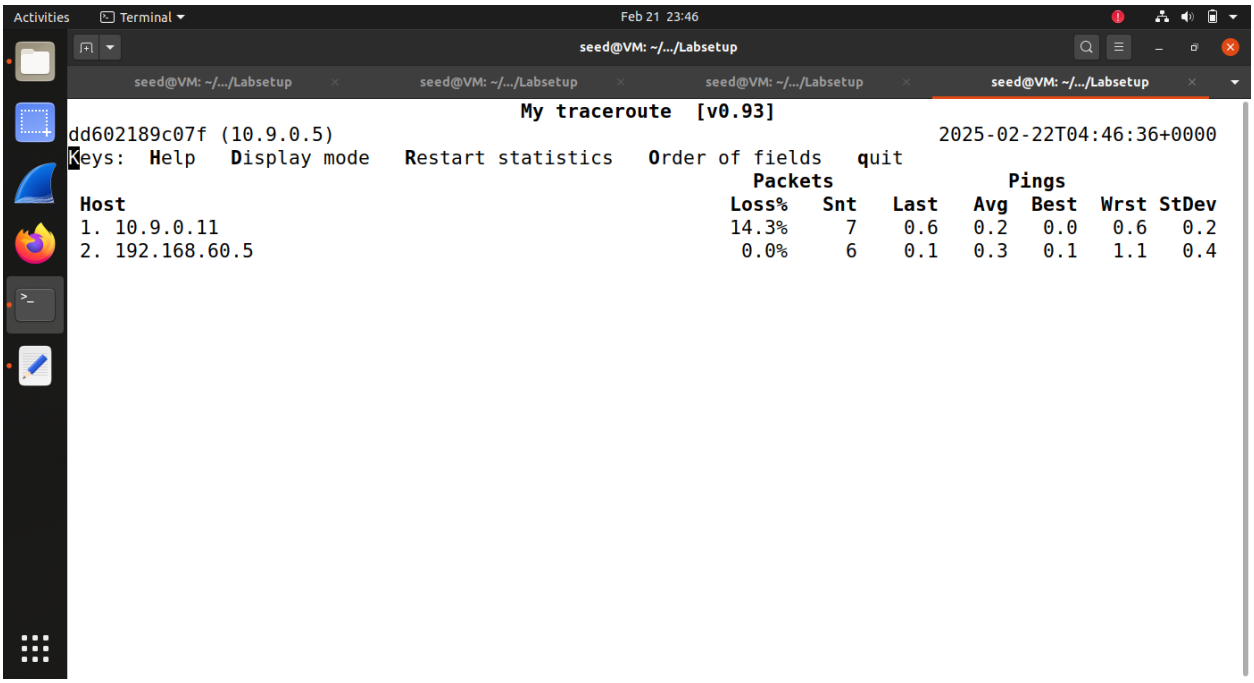
When I attempted to show the cache, it shows that the attack worked. The attack probably worked because the machine still exists even with it being turned off.



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

- The purpose of these entries is so the malicious router can redirect packets from the victim container to the 192.168.60.0/24 network to the original router. The picture below shows that I changed the values to 1.

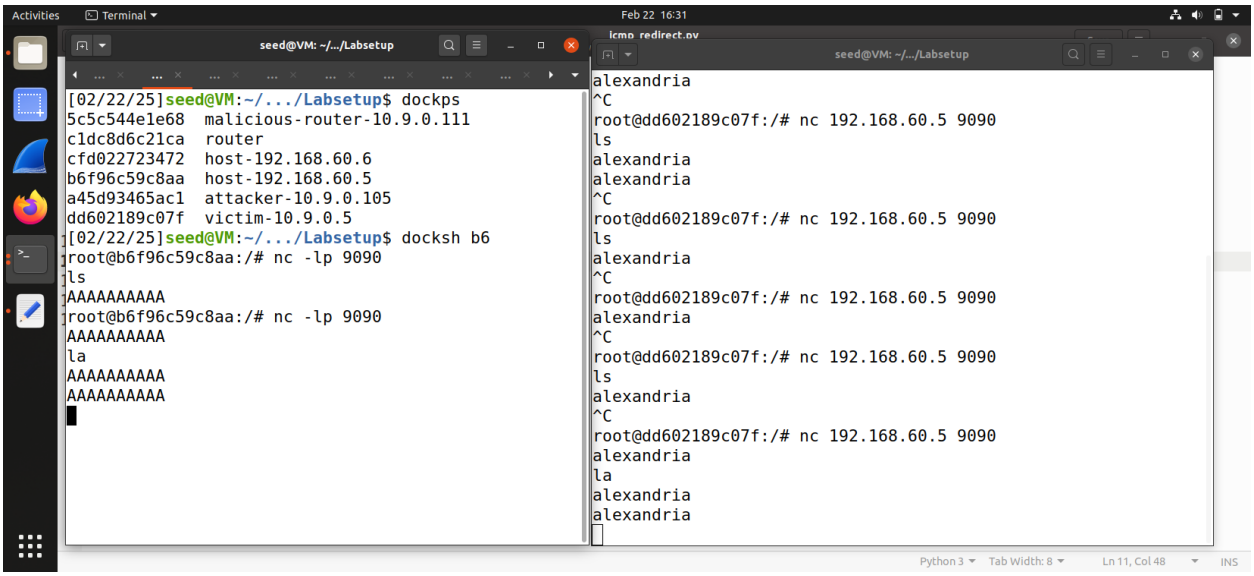




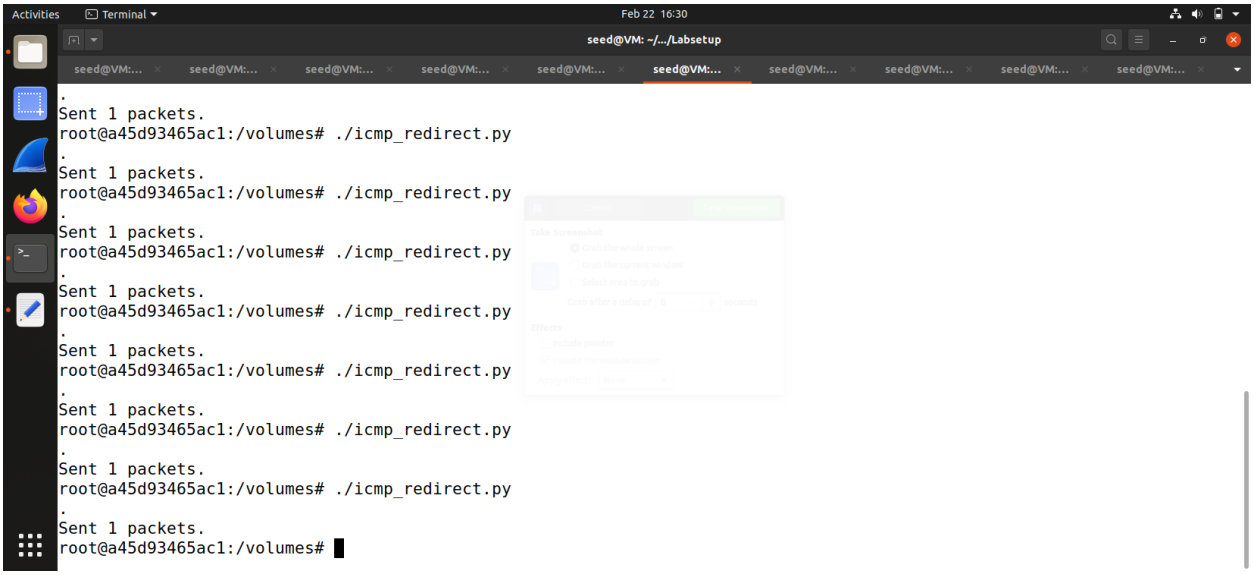
With the configurations turned on the attack failed as it did not redirect the packets.

Task 2:

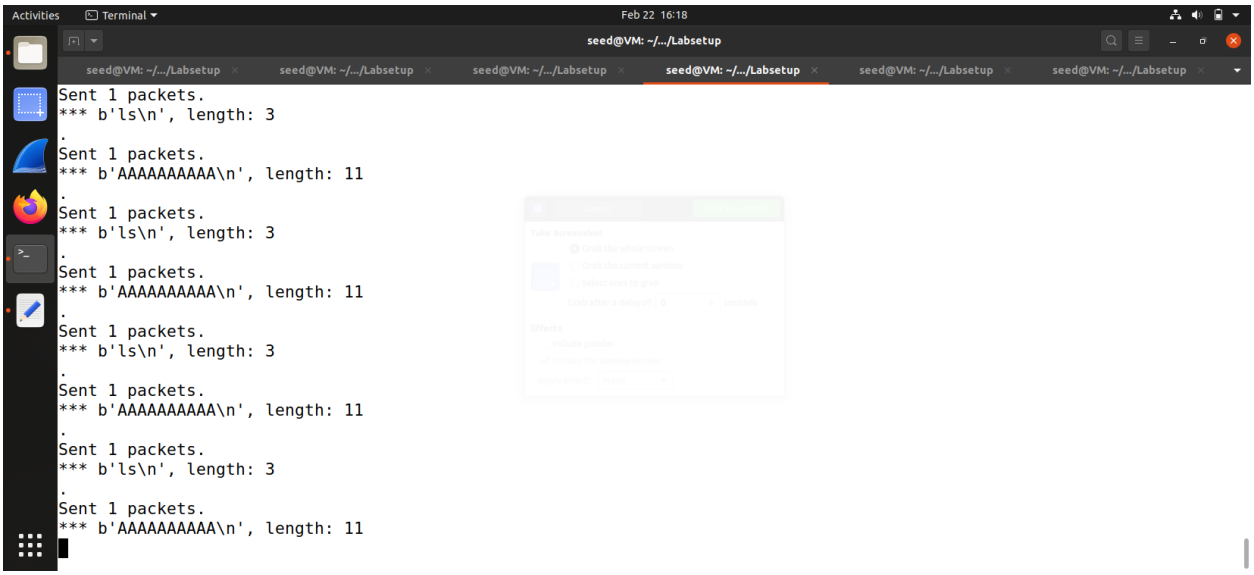
The following images show the process of me launching the MITM attack and all that was happening at the same time.



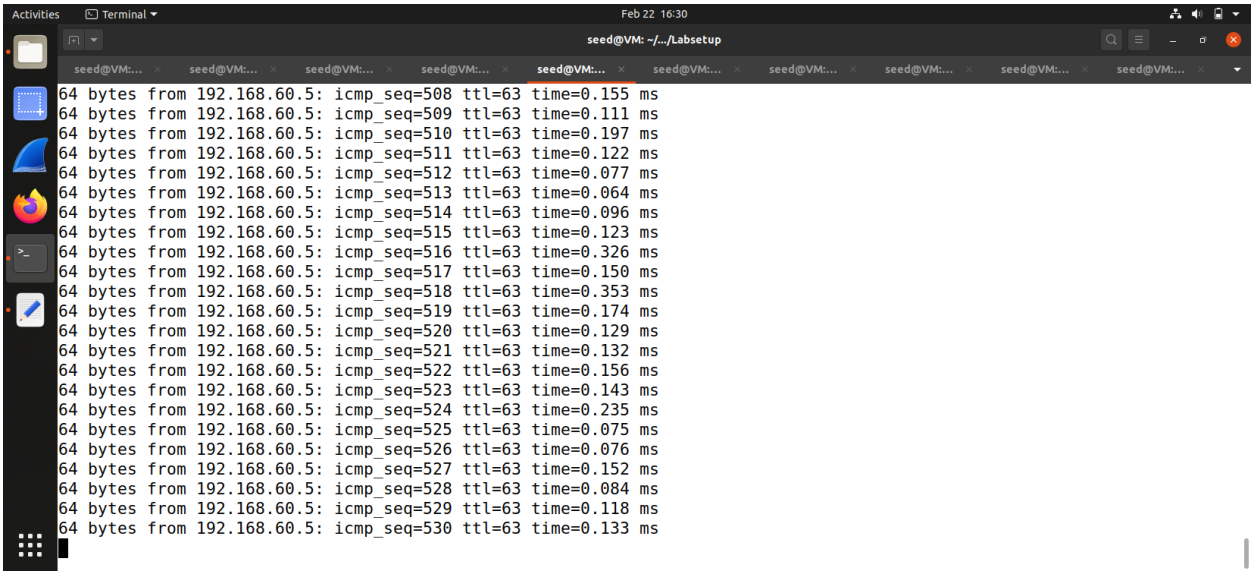
This is showing how I started a TCP client and server program and how I was successful in replacing my name with the series of A's.



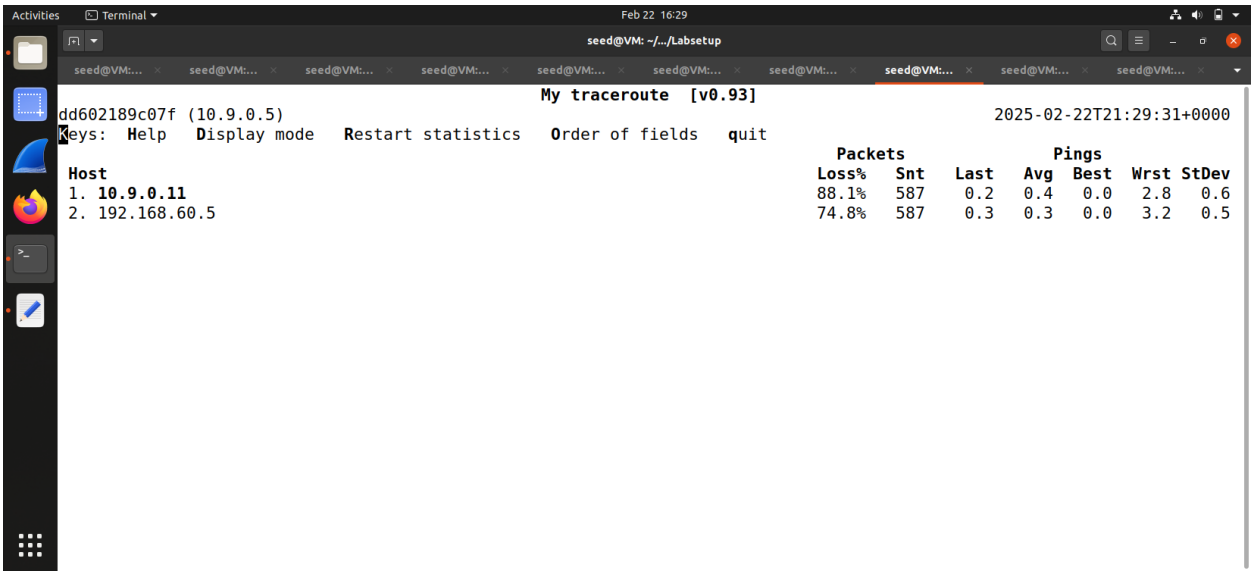
This is showing how I redirected the packets.



This was a stream of the packets being sent.



This is showing the ping's stream of traffic.



This is showing the traceroute of the victim container. I do not know why the malicious router's ip wasn't shown.

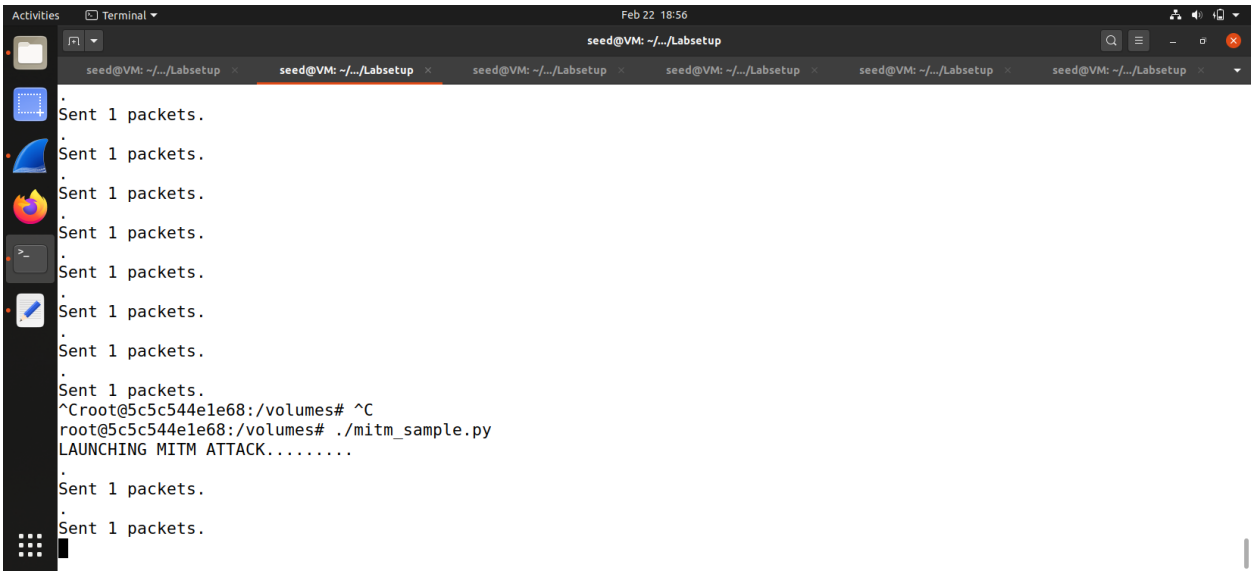
Question 4: In your MITM program, you only need to capture the traffics in one direction. Please indicate which direction, and explain why.

- You need to capture the traffics so that only the victim will send messages to the malicious router and not vice versa, because we only induce the victim host to send messages, and we do not induce the target host. It is not necessary to do it in the opposite direction.

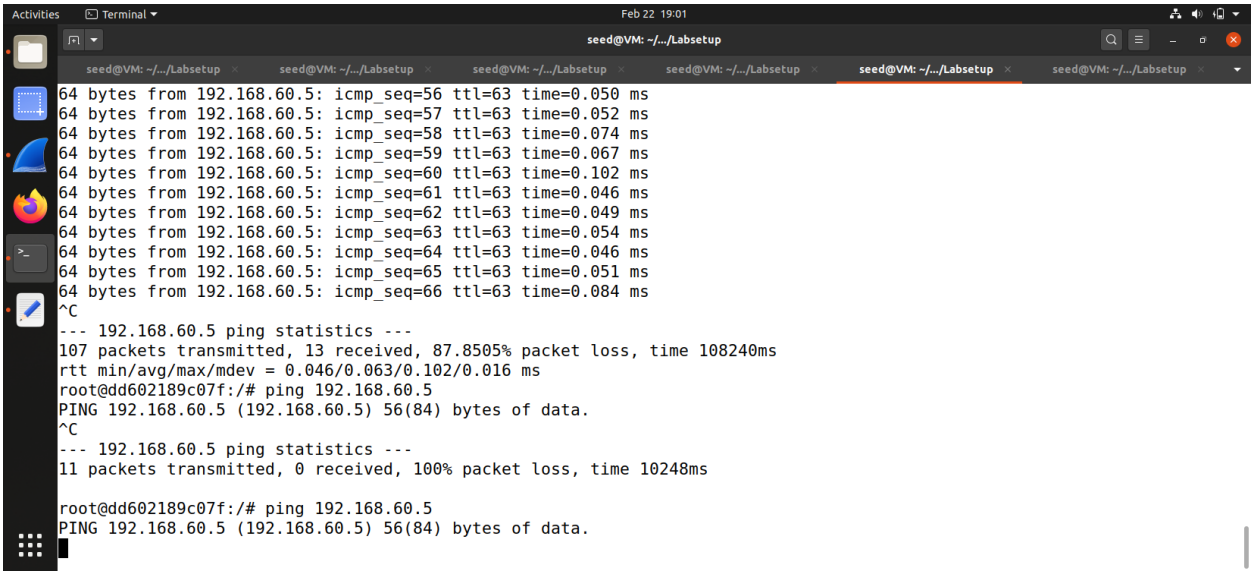
Question 5: In the MITM program, when you capture the nc traffics from A (10.9.0.5), you can use A's IP address or MAC address in the filter. One of the choices is not good and is going to create issues, even though both choices may work. Please try both, and use your experiment results to show which choice is the correct one, and please explain your conclusion.

This is showing me using A's ip address by adding it to the mitm file. I followed the same procedures for the MITM attacked and noting seemed to be different.

Next, I used the MAC address by inserting it into the mitm file and followed the same procedures for the attack. I noticed some differences.



I noticed that the attack was slower, sending less packets.



I also noticed that the ping was slower.

Since using the MAC address caused more issues I would say that using the ip address is the correct choice.