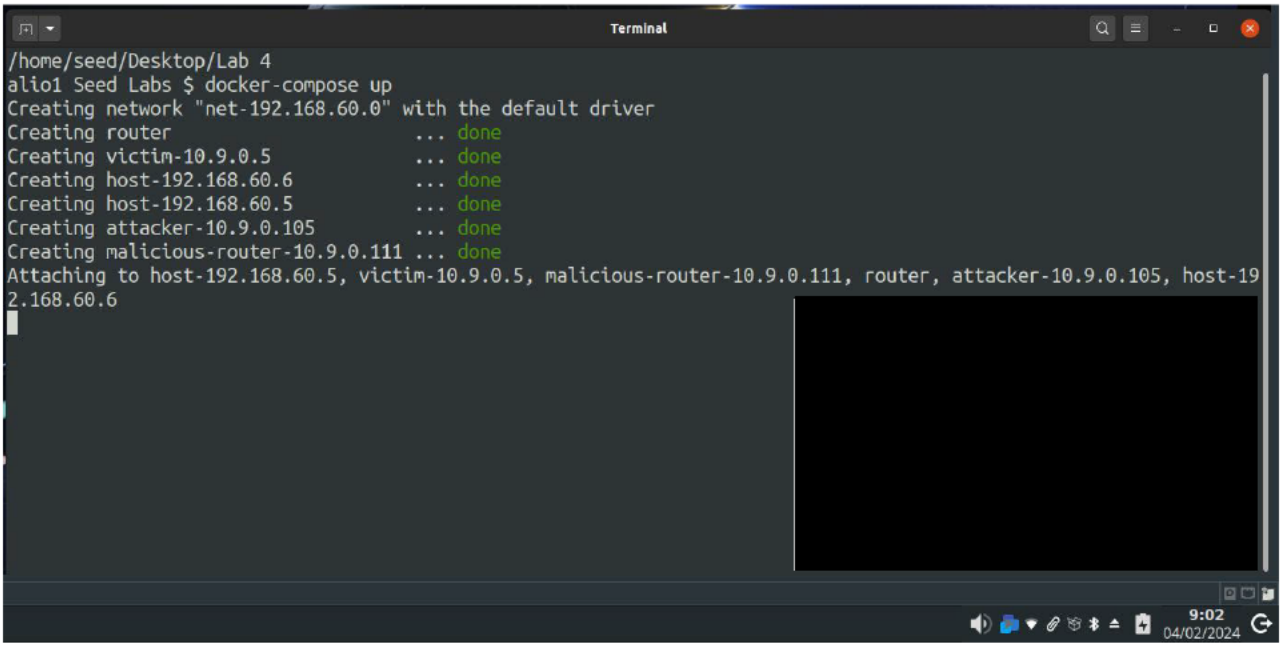
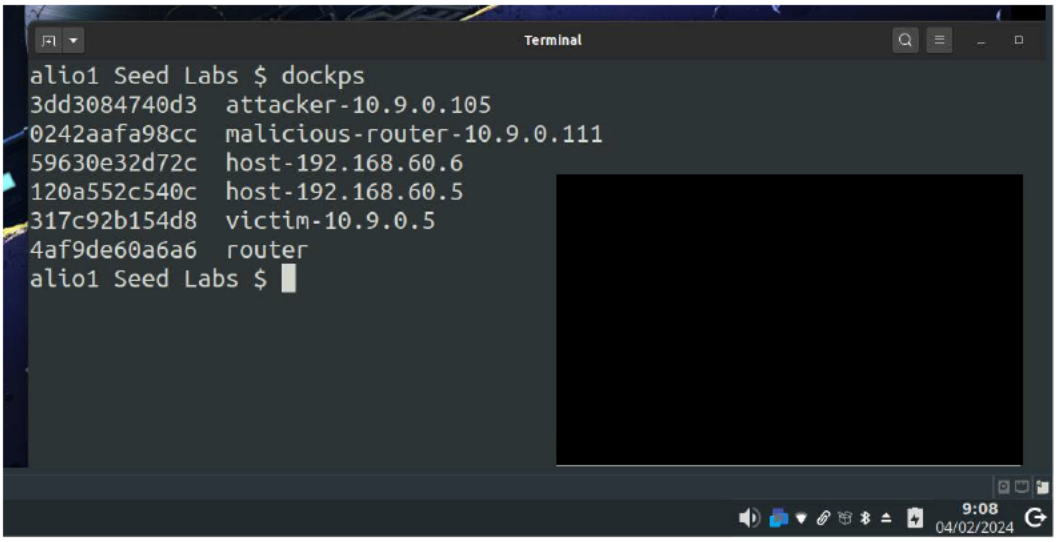
Table of Contents

Task 0 – Creating the Environment

The lab environment was created by downloading the appropriate Labsetup.zip from the SEED website, the using *cd Desktop/Lab\ 4* to enter the folder (that I renamed to keep the labsetup folders organized) and run *docker-compose up* (for subsequent uses, I utilize *docker-compose start* as the containers are already built). The subsequent screenshot shows the output of the aforementioned commands.

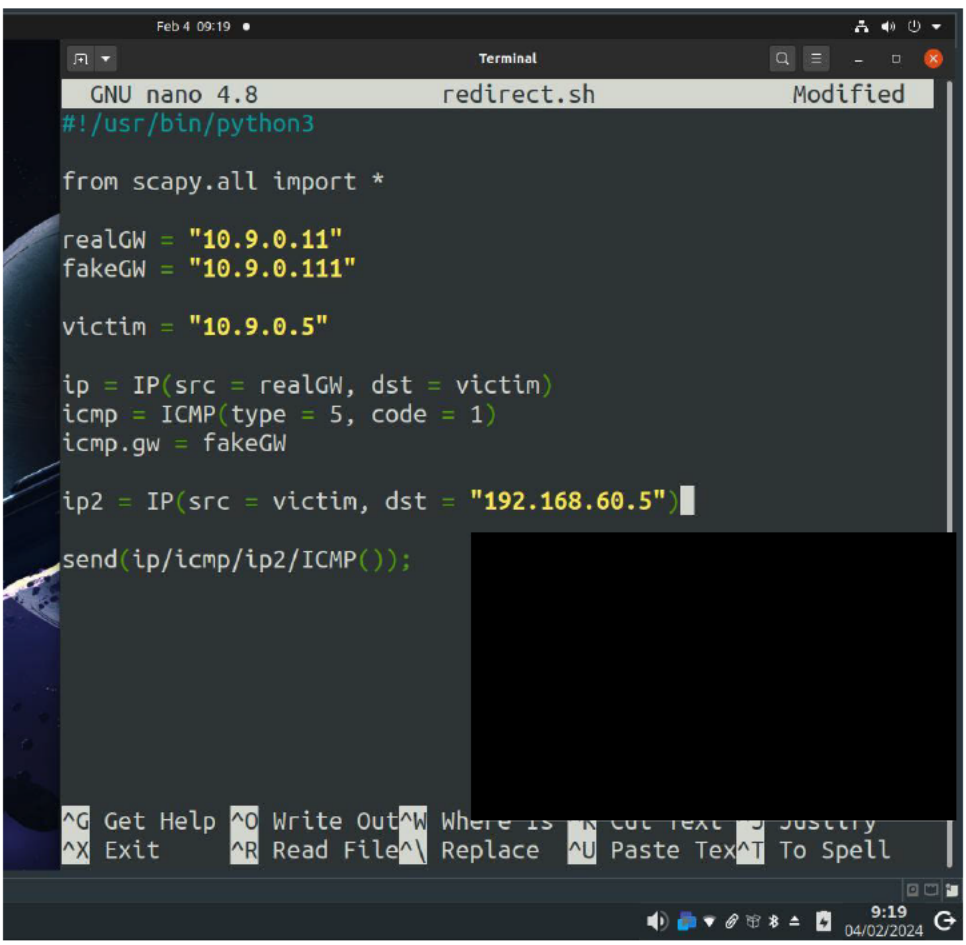


We can verify the docker containers are running by using *dockps* to list all active containers.

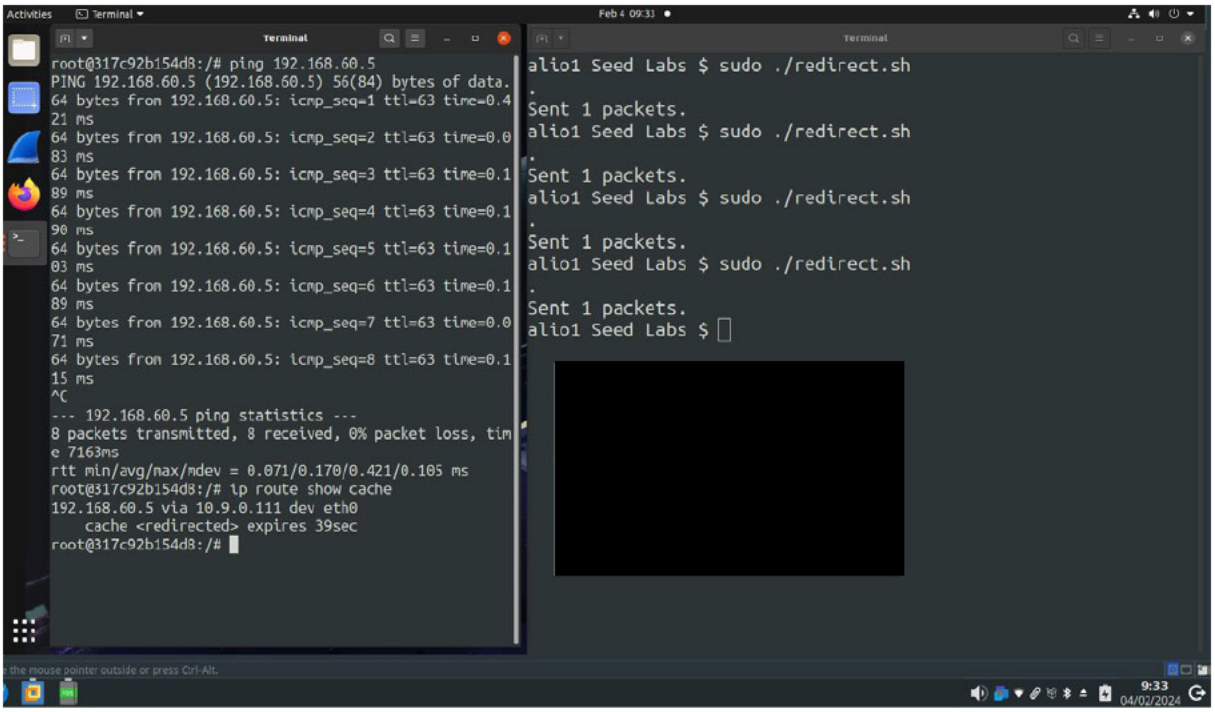


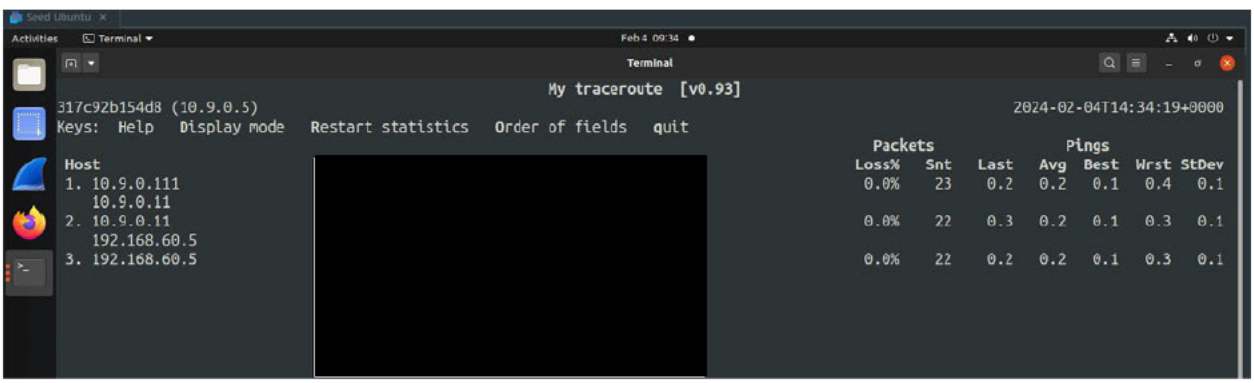
Task 1 – Launching ICMP Redirect Attack

The first task of this lab, scapy is utilized from the attacker container to create a redirect using the router container (192.168.60.11) to get to the 192.168.60.0/24 network on the victim container. Below is a screenshot displaying my Python code.



This code working can be verified by displaying the routing cache (as a redirect does not show in the routing table) and can be further verified by using traceroute in the victim container. Both are shown in the screenshot below.





Due to Docker constraints, this must have been run using the VM to issue the script. Because of this, I made a modification to the Python script where I specified the interface of the Docker network. I created a variable called *int = "br-935f87722f66"* to ensure this packet was sent on the correct network

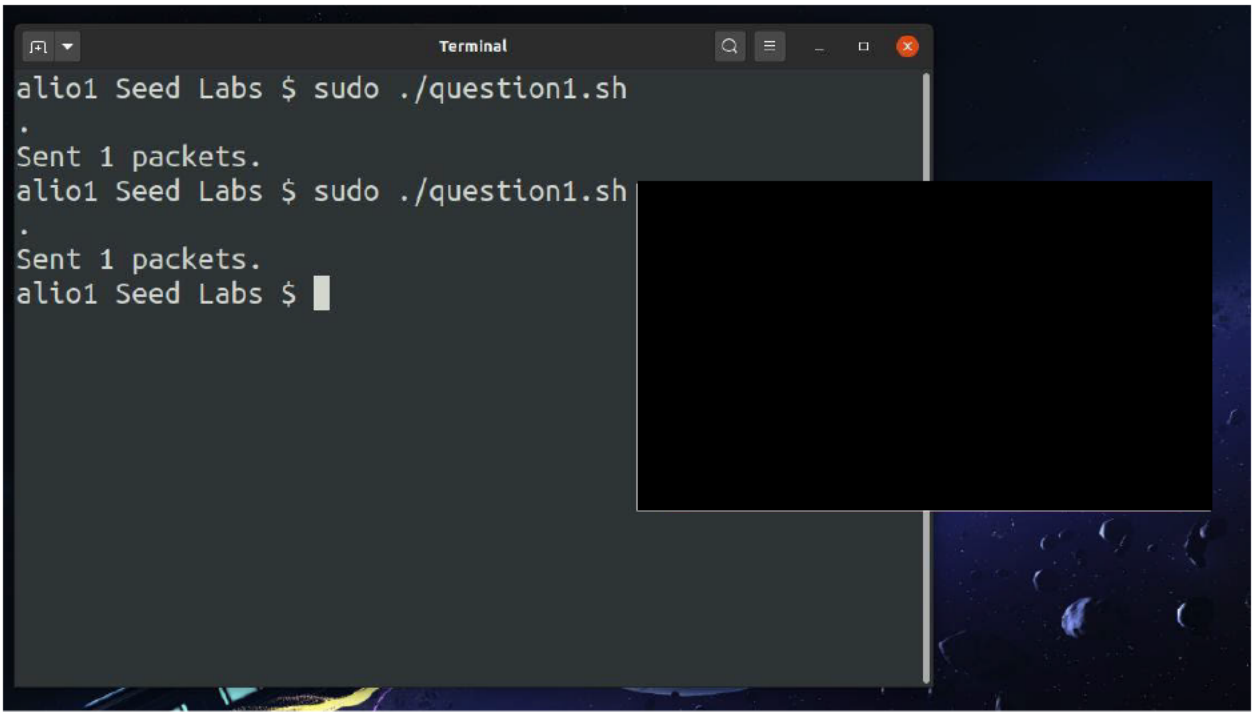
```
victim = "10.9.0.5"
int = "br-935f87722f66"


ip = IP(src = realGW, dst = victim)
icmp = ICMP(type = 5, code = 1)
icmp.gw = fakeGW

ip2 = IP(src = victim, dst = "192.168.60.5")

send(ip/icmp/ip2/ICMP(), iface=int);
alio1 Seed Labs $
```

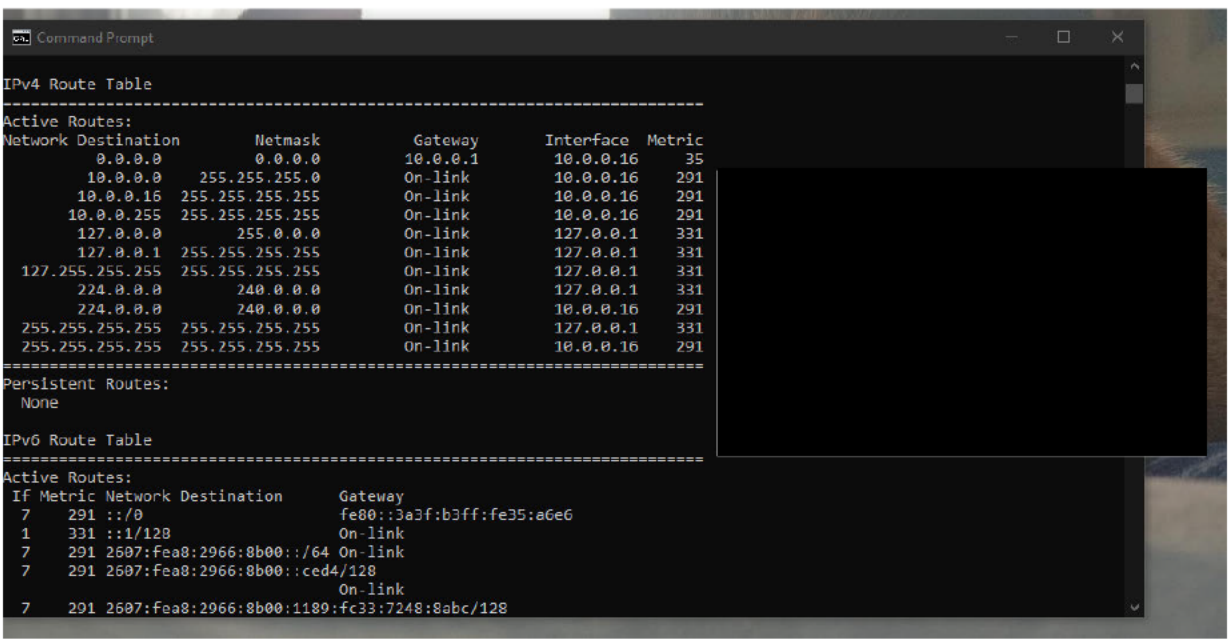
Questions

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 results and explain your observation.
    a. Due to the nature of ICMP redirect messages this attack will not work, as the packet will be dropped as ICMP redirect in effect, are meant to inform devices within one's LAN of a different route. There should be no mechanisms in place for a remote device to listen to a foreign device for routing.

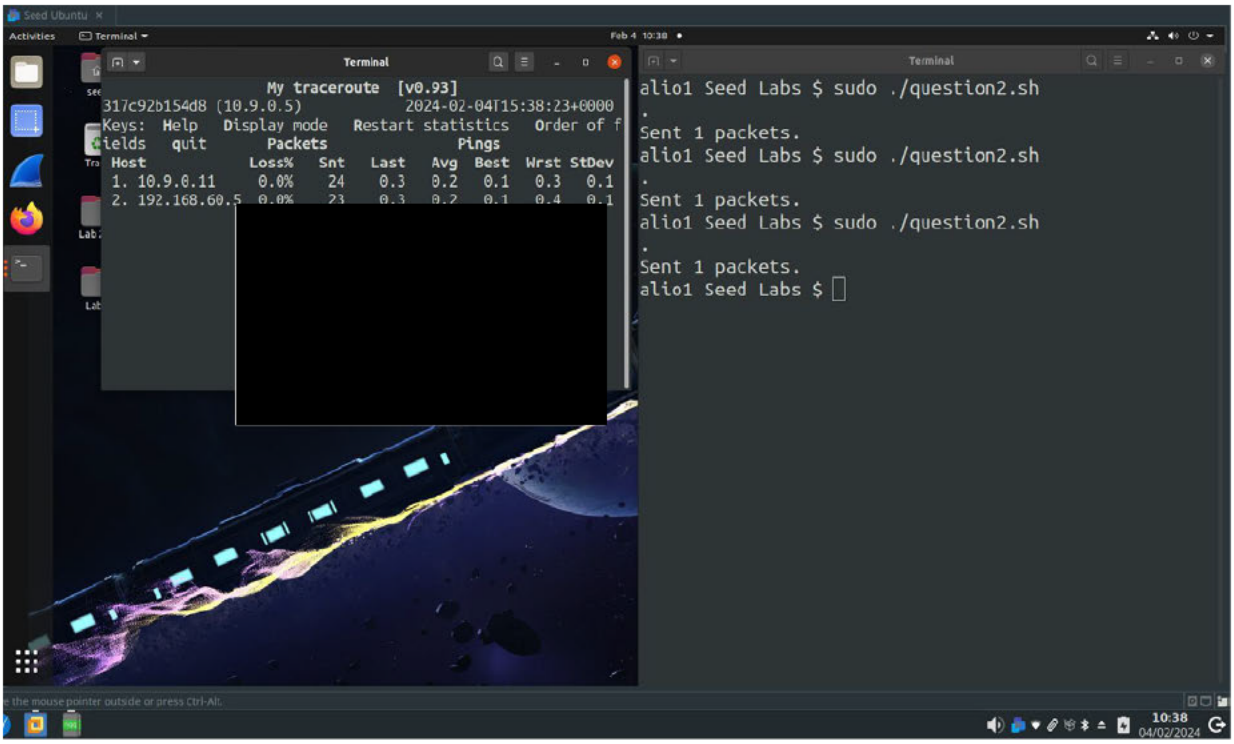
```
from scapy.all import *

realGW = "10.0.0.1"
fakeGW = "10.9.0.111"

victim = "10.0.0.16"
int = "ens33"


ip = IP(src = realGW, dst = victim)
icmp = ICMP(type = 5, code = 1)
icmp.gw = fakeGW

ip2 = IP(src = victim, dst = "10.0.0.1")

send(ip/icmp/ip2/ICMP(), iface=int);
alio1 Seed Labs $
```

I modified the attack used previously to attempt to redirect to my other computer. The outcome is demonstrated below.



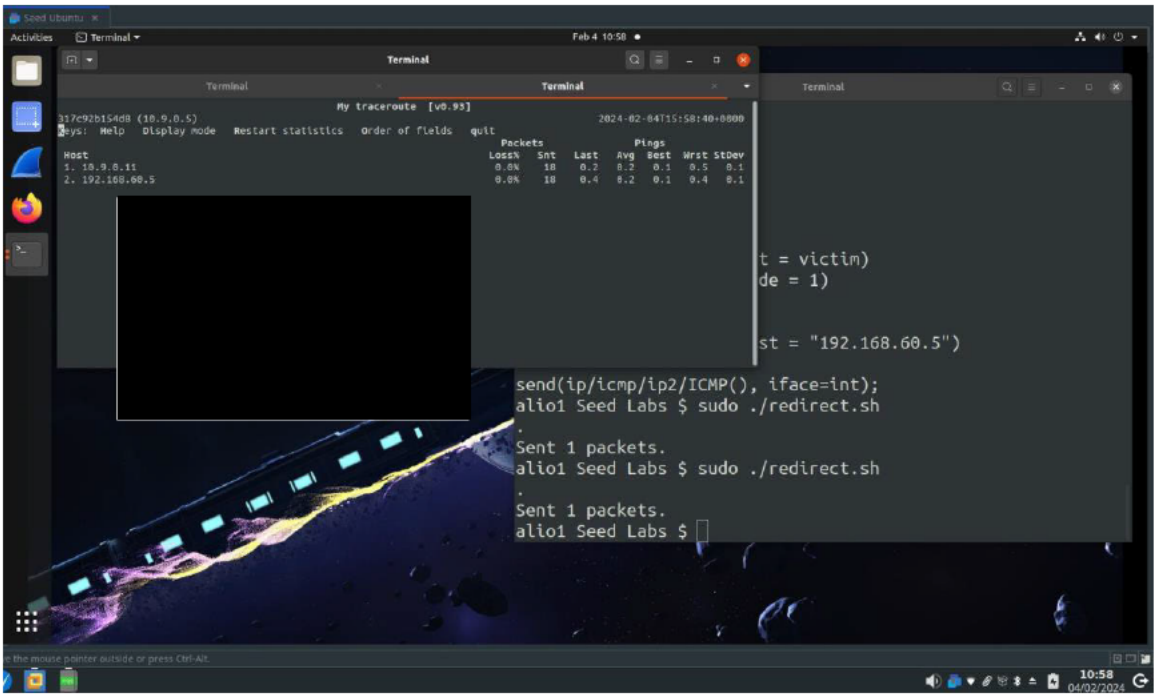


2. Can you use ICMP redirect attacks to redirect to a non-existing machine on the same network? Namely, the IP address assigned to icmp.gw is a local computer that is either offline or non-existent. Please show your experiment results and explain your observation.
    a. This modification took the form of changing the fakeGW variable to an IP that didn't exist, however, this did not work, however. After sending the packet checking *ip route show cache* yielded nothing. Moreover, the output of mtr –n 192.168.60.5 showed the following



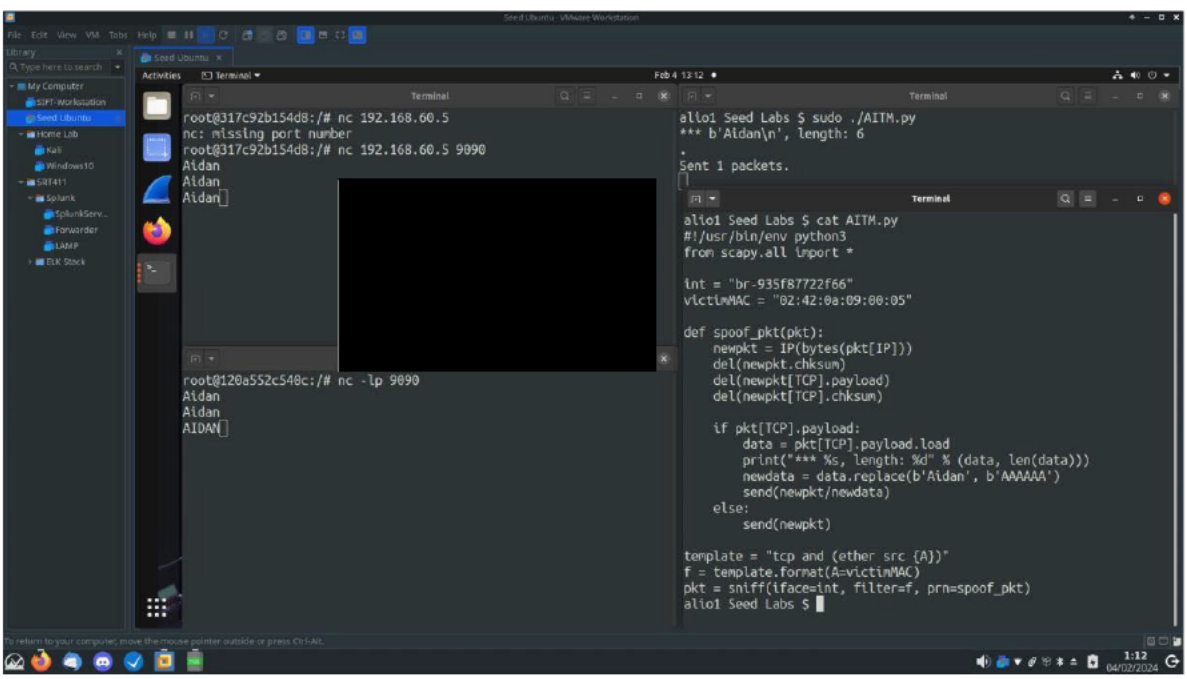
3. If you look at the *docker-compose.yml* file, you will find the following entries for the malicious router container. What are the purposes of these entries? Please change their value to 1 and attempt the attack again. Describe and explain your observations.
    a. net.ipv4.conf.all.send_redirects=0
    b. net.ipv4.conf.default.send_redirects=0
    c. net.ipv4.conf.eth0.send_redirects=0

Together, these values ensure that the malicious router does not send an ICMP redirect message. The book specifies that these are turned to 0 as if they were set to 1, eventually the routers would communicate and determine the quickest proper route, thus defeating the attack. The below screenshot shows the output after changing the values to 1 and using the redirect attack again. The output of *ip show route cache* yielded nothing.



Task 2 – Launching the AITM Attack

This task asks to create a netcat server and facilitate an AITM attack where every instance of Aidan is replaced with the same length of A's, therefore AAAAA. The code below is what was utilized to facilitate this as well as the successful AITM attack.



Questions

1. In the AITM program, traffic only needs to be captured in one direction. Please indicate which direction and explain why.

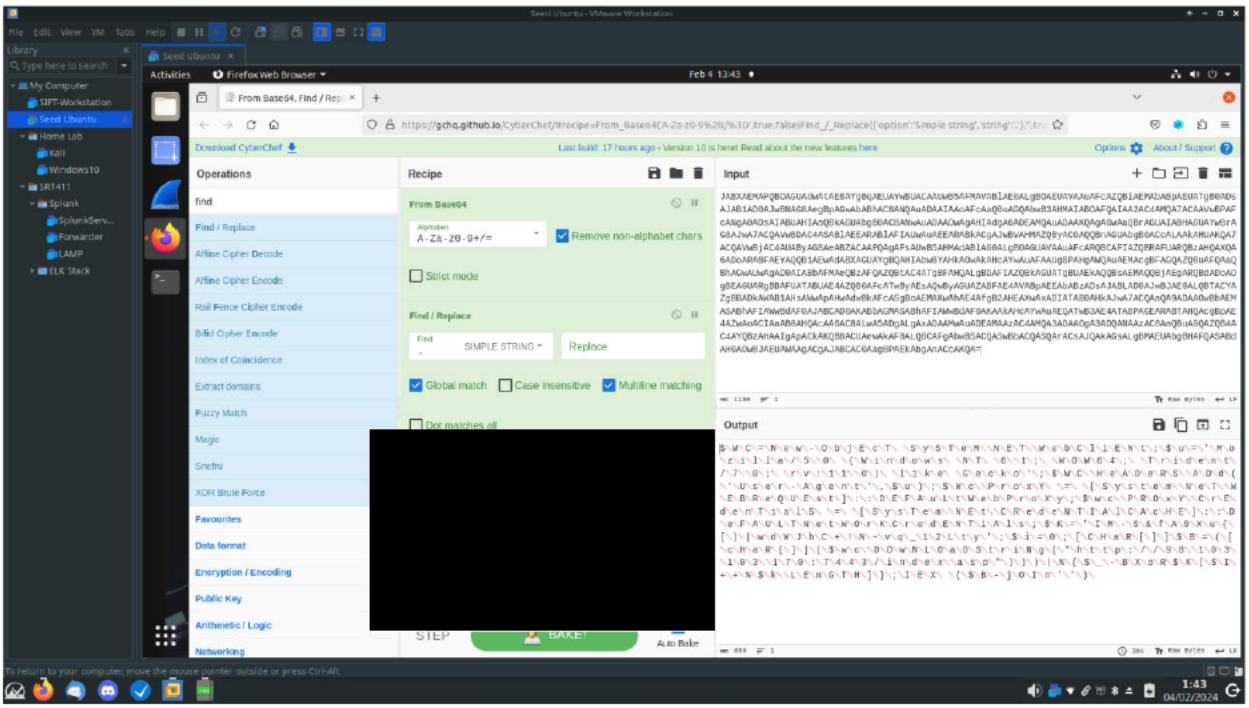
a. We only need to capture traffic from victim to destination as there is no purpose in capturing the traffic from the other entity.

2. When the nc traffic is captured from A, A's IP address or MAC address can be used in the filer. Even though both choices work, one will create issues. Try both and use the experiment results to show which choice is correct. Explain your conclusion.
   a. As referenced in last week's lab, the more appropriate choice is to utilize the MAC address. If we do not specify an address, the sniffer will capture traffic from our malicious machine. If we specify just the IP address, this will create a loop that will slow down the program and eventually stop it. By using the MAC address we know that we are only capturing the outbound packets from the victim.

Task 3 – Cyber Chefs

Exercise 1

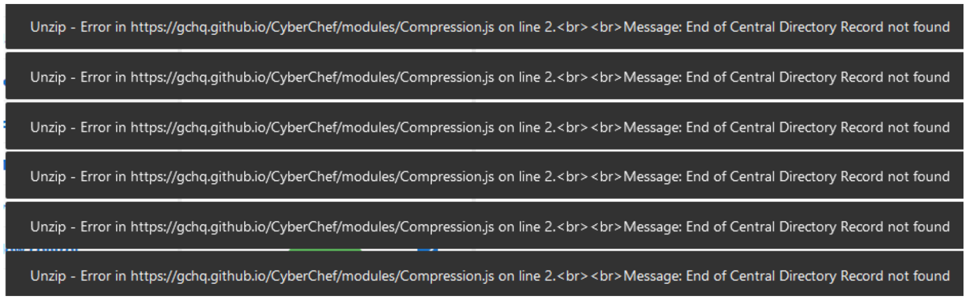
- Following the instructions on the website, I was able to decode example one to the output of the screenshot below. I was not able to figure out a way to remove the extra character.



- What does the following say when decoded":4oCcSGUgd2FzIGFwcGFsbGVkIGJ5IHRoZSBleGFtaW5hdGlvbiBzeXN0ZW0sIHdoZW4gaXQgd2FzIGV4cGxhaW5l
- It says: "He was appalled by the examination system, when it was explained"

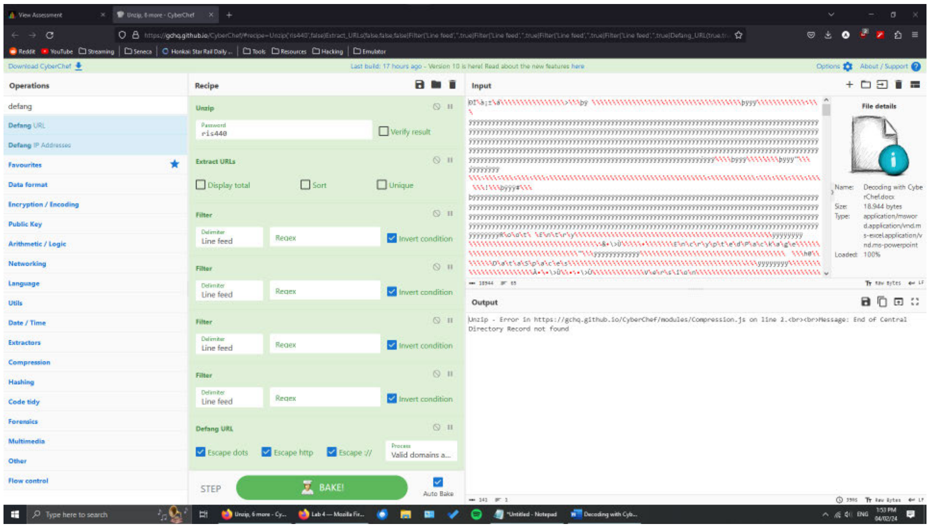
Exercise 2

- For this, even though I followed the steps, I kept receiving the error of:



```
Unzip - Error in https://gchq.github.io/CyberChef/modules/Compression.js on line 2.<br><br>Message: End of Central Directory Record not found
Unzip - Error in https://gchq.github.io/CyberChef/modules/Compression.js on line 2.<br><br>Message: End of Central Directory Record not found
Unzip - Error in https://gchq.github.io/CyberChef/modules/Compression.js on line 2.<br><br>Message: End of Central Directory Record not found
Unzip - Error in https://gchq.github.io/CyberChef/modules/Compression.js on line 2.<br><br>Message: End of Central Directory Record not found
Unzip - Error in https://gchq.github.io/CyberChef/modules/Compression.js on line 2.<br><br>Message: End of Central Directory Record not found
Unzip - Error in https://gchq.github.io/CyberChef/modules/Compression.js on line 2.<br><br>Message: End of Central Directory Record not found
```

- As shown in the screenshot below I followed the steps



Recipe

Unzip
Password: ris440
☐ Verify result

Extract URLs
☐ Display total ☐ Sort ☐ Unique

Filter
Delimiter: Line feed
Regex
☑ Invert condition

Filter
Delimiter: Line feed
Regex
☑ Invert condition

Filter
Delimiter: Line feed
Regex
☑ Invert condition

Filter
Delimiter: Line feed
Regex
☑ Invert condition

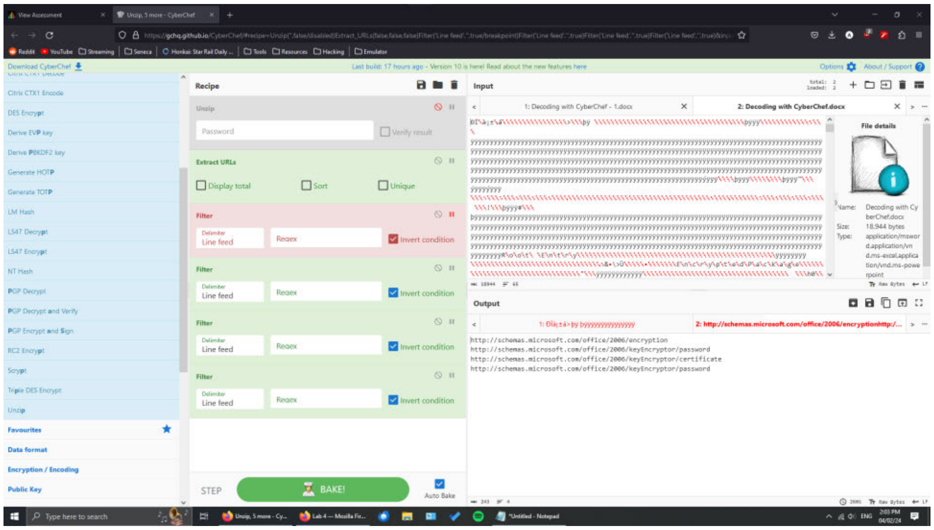
Defang URL
☑ Escape dots ☑ Escape http ☑ Escape ://
Process: Valid domains a...

File details
Name: Decoding with CyberChef.docx
Size: 18,944 bytes
Type: application/msword.application/vnd.ms-excel.application/vnd.ms-powerpoint
Loaded: 100%

Output

```
Unzip - Error in https://gchq.github.io/CyberChef/modules/Compression.js on line 2.<br><br>Message: End of Central
Directory Record not found
```

- Which I thought indicated that the password was wrong, however, I was able to open the Word Document. When I removed the Unzip function it mostly worked, except the URLs displayed were encrypted Microsoft URLs (I believe), as shown below.



Recipe

Unzip
Password
☐ Verify result

Extract URLs
☐ Display total ☐ Sort ☐ Unique

Filter
Delimiter: Line feed
Regex
☑ Invert condition

Filter
Delimiter: Line feed
Regex
☑ Invert condition

Filter
Delimiter: Line feed
Regex
☑ Invert condition

Filter
Delimiter: Line feed
Regex
☑ Invert condition

Input: 1: Decoding with CyberChef - 1.docx | 2: Decoding with CyberChef.docx

File details
Name: Decoding with CyberChef.docx
Size: 18,944 bytes
Type: application/msword.application/vnd.ms-excel.application/vnd.ms-powerpoint

Output

```
http://schemas.microsoft.com/office/2006/encryption
http://schemas.microsoft.com/office/2006/keyEncryptor/password
http://schemas.microsoft.com/office/2006/keyEncryptor/certificate
http://schemas.microsoft.com/office/2006/keyEncryptor/password
```