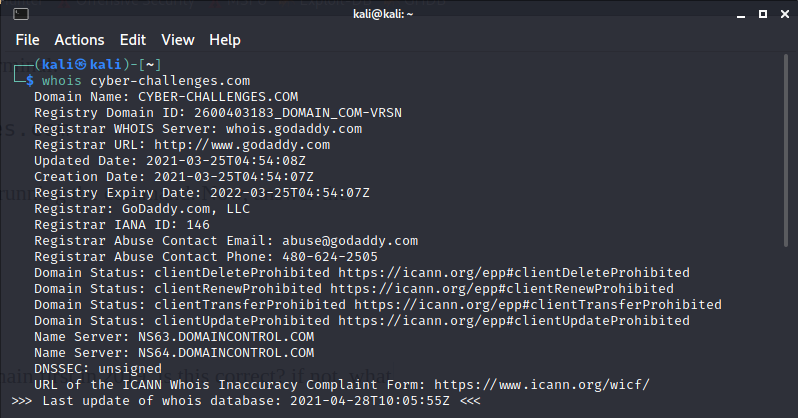
Task 5.1P

Student Name

Institutional Affiliation

**1: Network Reconnaissance**

**Question A:**



Arash claims that he created this domain first in 2019, is this correct? if not, what date was this domain created first?

This is false. As observed, th domain was created on 2021-03-25

When does the registration of the domain expire?

2022-03-25

What is a “Name Server” and what is it used for? (include a reference for your answer)

Nameserver is an internet server specialising in the management of queries about the position of the different services of a domain name. Name servers are a key part of the system of domain names (DNS). Instead of IP addresses they make the use of domains.

What are the Name Servers for this domain? Why there are two Name Servers?

NS63.DOMAINCONTROL.COM

NS64.DOMAINCONTROL.COM

On separate computers, two nameservers support multi-server hosts maintain all of their pages. The other nameserver can handle all requests if one of these nameservers is being rebooted, or offline for maintenance purposes. It is for high redundancy and backup essentially.

What is a registrar? Who is the registrar of this domain?

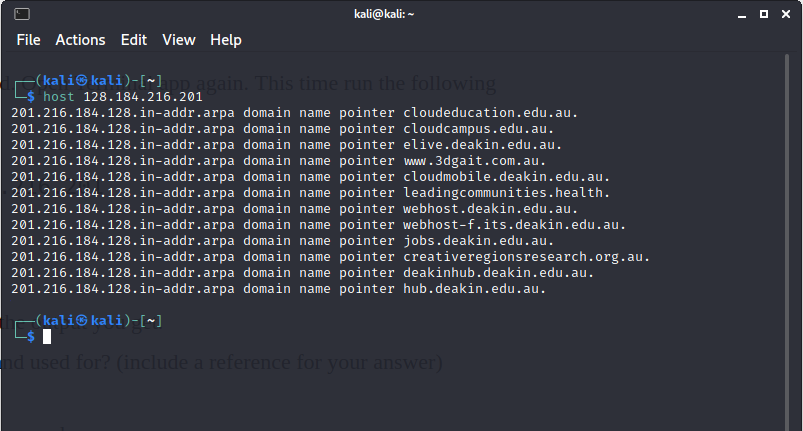
A domain name registrar is a company that allows you to purchase and register domain names

What is “Whois Privacy”? Is this domain using the Whois Privacy service?

Domain privacy is a service provided by a variety of domain name registrars (often known as Whois privacy). A user acquires company privacy which, in turn, replaces WHOIS user information with forwarding service information (for email and sometimes postal mail, it is done by a proxy server).

**Question B:**

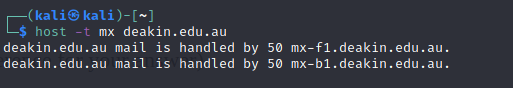
Include a screenshot of the output you get.



What is the host command used for? (include a reference for your answer)

For DNS (Domain Name System) host command is in search operations used for Linux system. This command is used in simple words to find the IP address of a given domain name

3. Include a screenshot of the output you get.

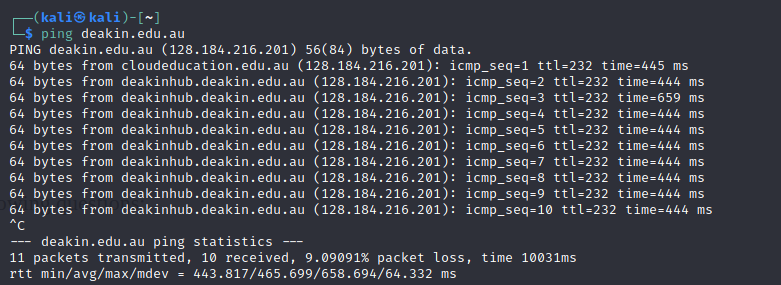


4. What is an MX record in DNS?

The email server responsible for receiving email messages for the sake of a domain name is defined by the mail exchanger record (MX record). Several MX records can be configured which usually point to a server for load balance and redundancy.

**Question C**

1. Include a screenshot of the output you get.



Investigate about ping command and answer the following questions:

2. What is ICMP?

The ICMP is a layer protocol for the diagnostics of network communication problems used by network devices. ICMP is used primarily to decide whether data enter their desired destination in a timely fashion.

3. Fill in the blanks:

A correctly-formed ping packet is typically **56** bytes in size, or **64** bytes when the ICMP header is considered, and **84** including Internet Protocol version 4 header.

4. What does `ttl’ refer to in the ping command output?

TTL (Time-to-Live): The TTL value represents the maximum number of IP routers that the packet can go through before being thrown away.

5. True or False? “A higher `time’ value in ping result indicates a faster connection between your machine and the server” False

**Question D:**

1. Using the “host” you learned about earlier, find the IP address for localhost. What is the IPv4 address for localhost?

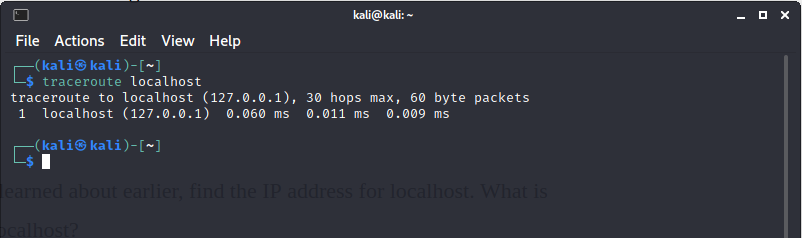
127.0.0.1

2. Do you need Internet access to retrieve the “localhost” domain?

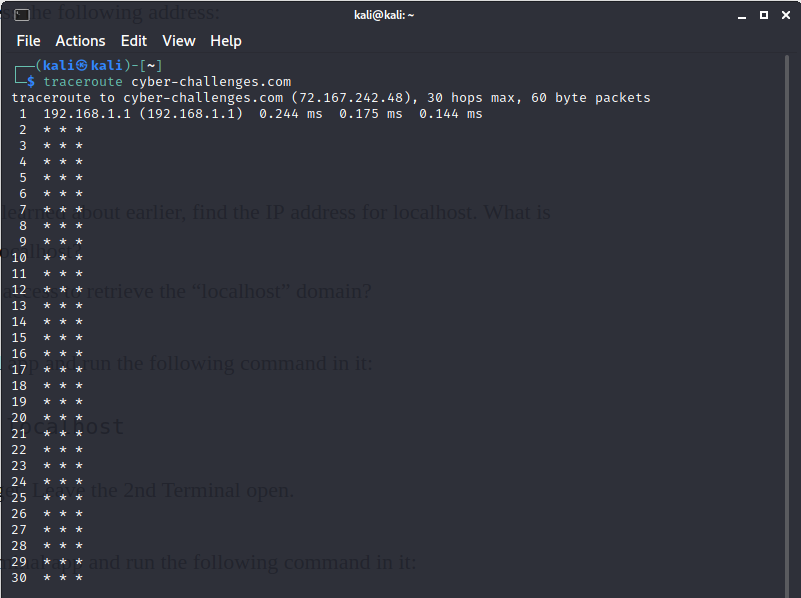
No.

Compare the output between the result you get after running traceroute for localhost and cyber-challenges.com.

traceroute localhost



traceroute cyber-challenges.com



3. What is a `hop’ referring to in the output for the traceroute command?

The journey from one computer to another is known as a hop. The amount of time it takes to make a hop is measured in milliseconds.

4. What happens if one of the servers/routers in the hops is not listening for ICMP echo requests?

The hop number shows no time data and a Request timed out error. This is because the server at the hop is not accepting (ICMP) traffic. As a result, it ignores Traceroutes request for information. However, it still sends the data to the next hop as there are results that follow.

5. How can an attacker use “traceroute” when targeting computer networks? click here to access a suggested reading to find the answer to this question.

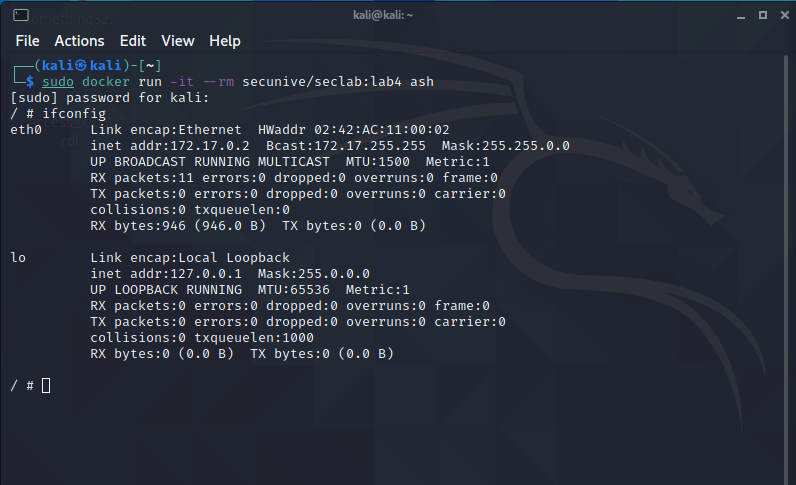
Tracerouting will allow the attacker to build a working topology of systems and routers by listing the systems by which information flows to the target computer. Depending on the type of traceroute carried out, this attack is able to return various results. Traceroute operates by sending packets to a destination while adding time-to-live to the packet header. When the packet passes through each hop, its TTL expires, which generates an ICMP diagnostic message that identifies where the packet has expired.

**2: Packet Inspection**

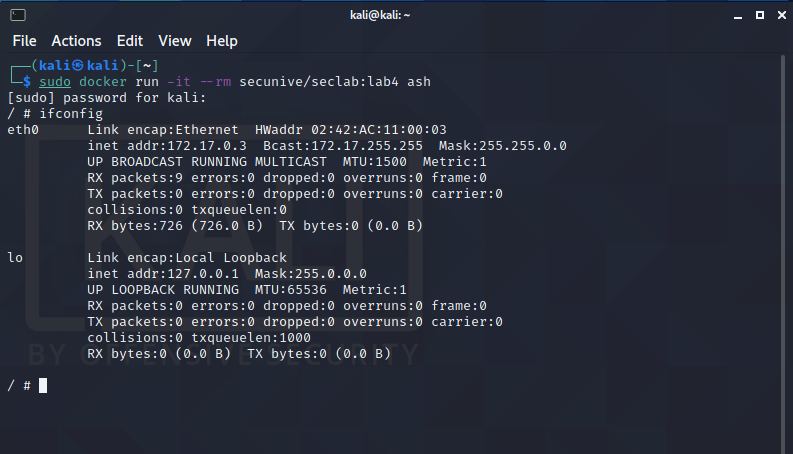
**Question E:**

Include a screenshot of running the “ifconfig” command in each of the terminals. What is the IP address for eth0 in Terminal 1 and what is the IP address for eth0 in Terminal 2?

The IP address in Terminal 1 is 172.17.0.2



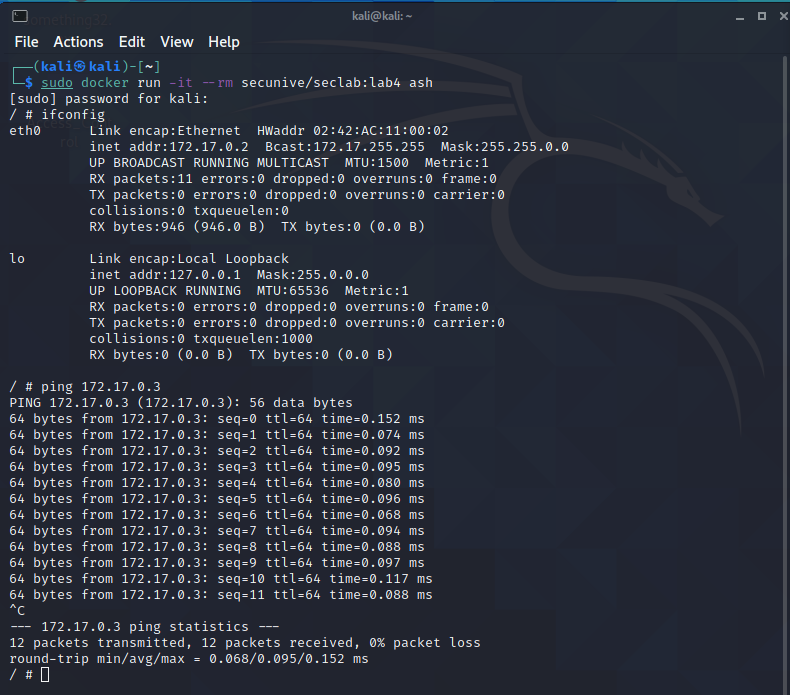
The IP address in Terminal 1 is 172.17.0.3



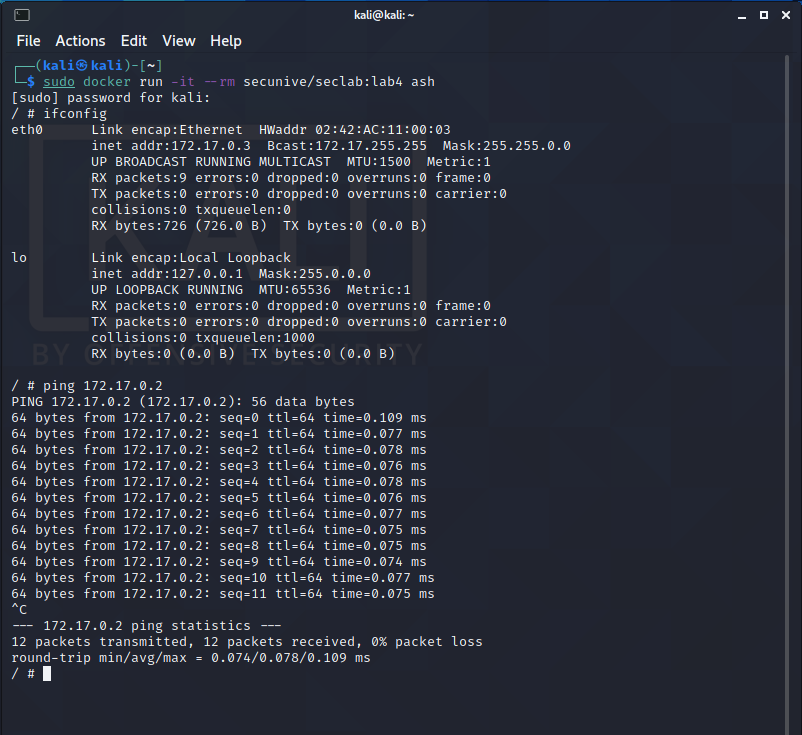
Question F:

Ping host 172.17.0.2 from the second docker instance in the second terminal (that should have the address 172.17.0.3) and vice-versa, to check network connectivity between the two hosts. Include screenshots confirming that you have executed the commands and received ping replies confirming connectivity between the two hosts.

Screenshot from 172.17.0.2



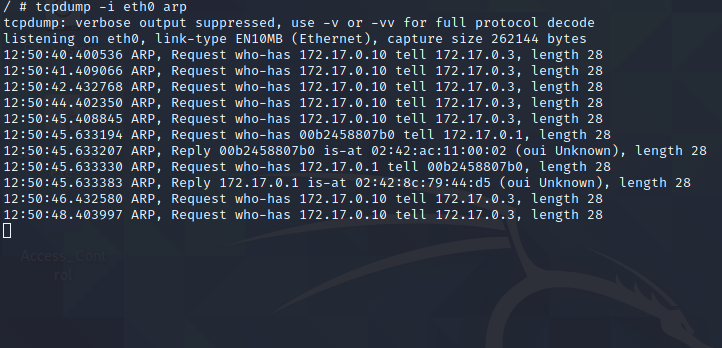
Screenshot from 172.17.0.3



**Question G:**

What is the password to access Challenge 3?

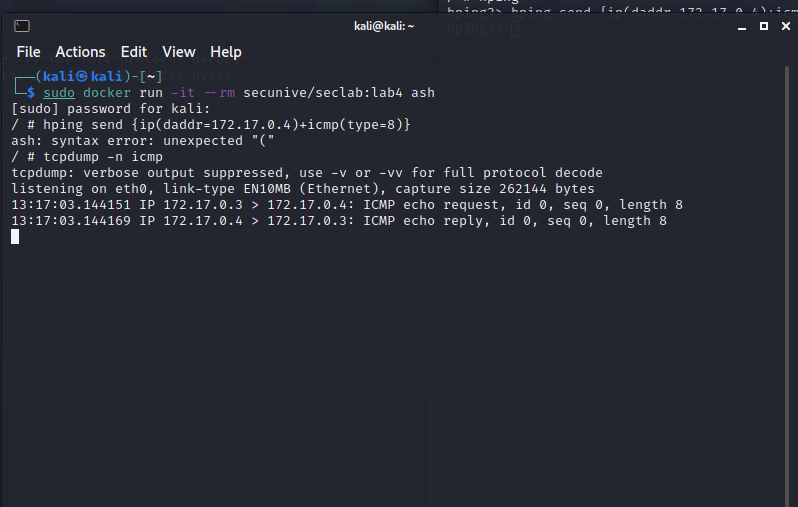
who-has



**3: Source Address Spoofing**

**Question H:**

1. Include a screenshot of the tcpdump output running on the first Terminal (i.e., 172.17.0.2)



2. In your own words, explain what did just happen?

**Question I:**

1. What is the password that you can successfully access Challenge 4 with?

no replies will be shown



2. Why would an attacker spoof his IP when running an attack against a victim?

In IP spoofing, a hacker uses techniques that make the receiving machine believe the packet comes from a trustworthy source like another device on a legit network and to change the source address of the packet header. Due to this, there are no external indicators of tampering on the network stage.

3. Let’s assume a Web Server was running on the host you targetted (i.e., 172.17.0.2). How could they have prevented their system from being targetted by your ICMP flooding attack?

DDoS can be performed by preventing ICMP flood attack by disabling ICMP router, machine or other system features of the targeted router. You can effectively prevent attacks from started outside your network by setting your perimeter firewall to block the pings. This method will not avoid internal attacks, it is necessary to remember.

4. Reflection Point – How did this task complement the theoretical concepts you learned in Week 4 and Week 5? What did you learn that was most exciting for you? Are you finding it easier to use the shell for hands-on activities?

The tasks have helped greatly in operating with docker and also running Kali Linux commands. The most exciting part of the assignment was being able to view packets being sent over the network using ICMP. Performing the DDOS attack was also very informational with helping on knowing how to perform the attacks as well as knowing how to prevent them. The more the tasks continued, the more it became easier to use the Kali Linux shells, especially when the task required multiple shells to be run at once.