**CYBER SECURITY LAB**

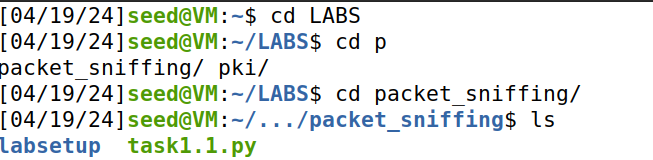
**PACKET SNIFFING SPOOFING**

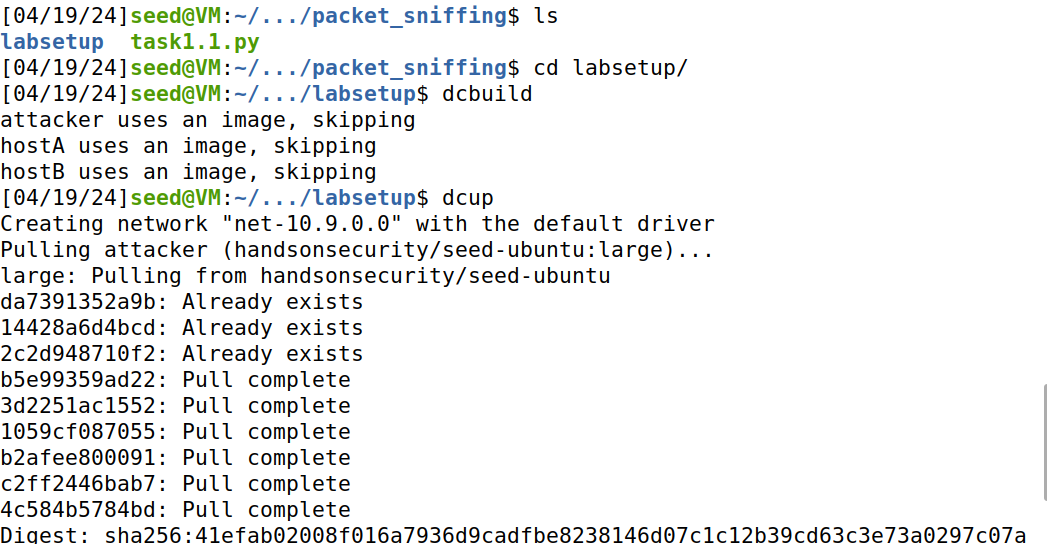
**(CMPG769)**

**ASTHA PATEL**

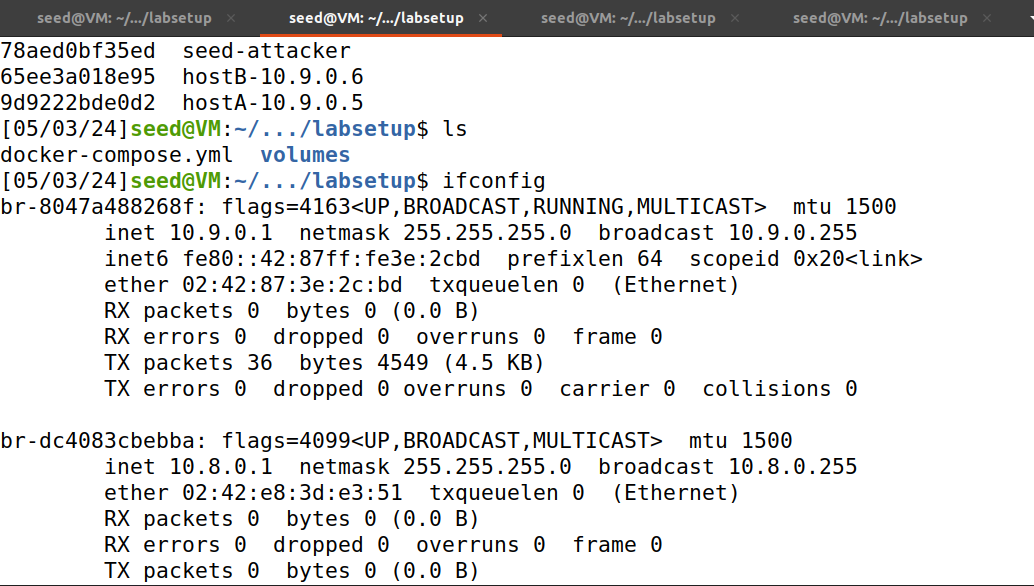
**Environment Setup using Container**

To setup an environment, first we need to copy the Lab set up folder provided in module and then paste it inside our lab folder and then to set up only we need to

****

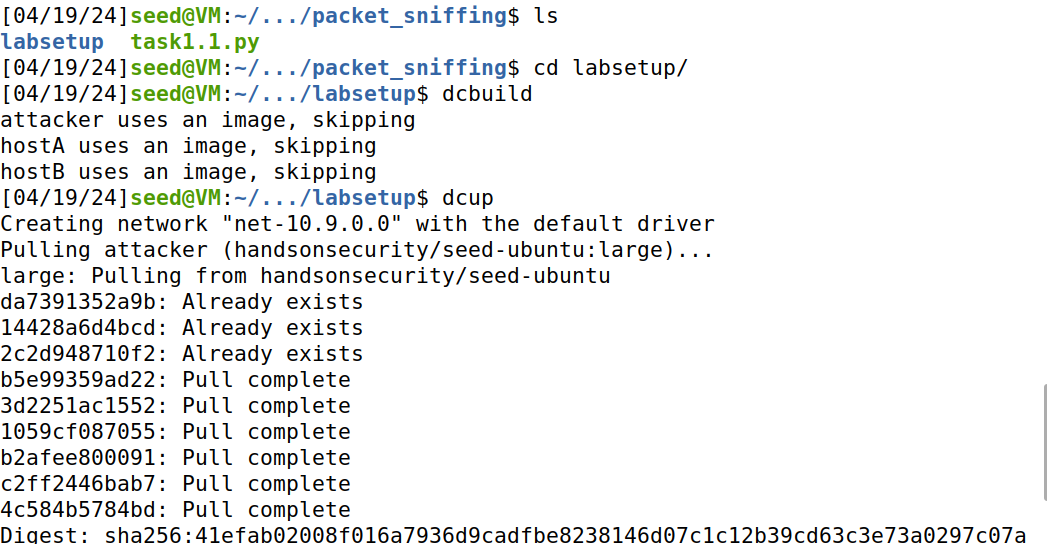
****

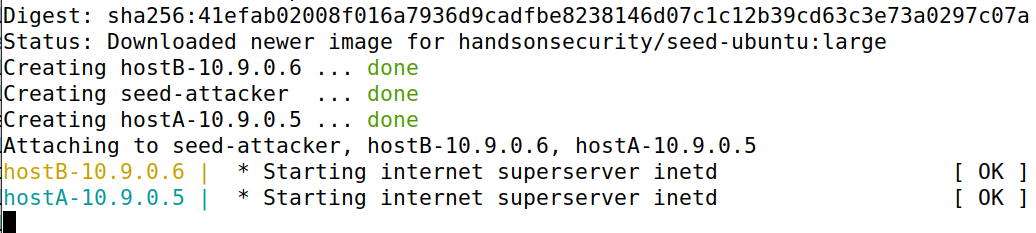
**Two interface numbers:**

****

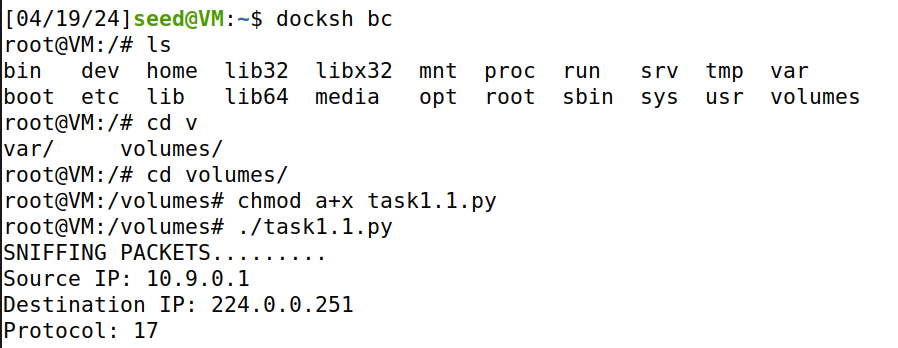
1. br-8047a488268f
2. br-dc4083cbebba

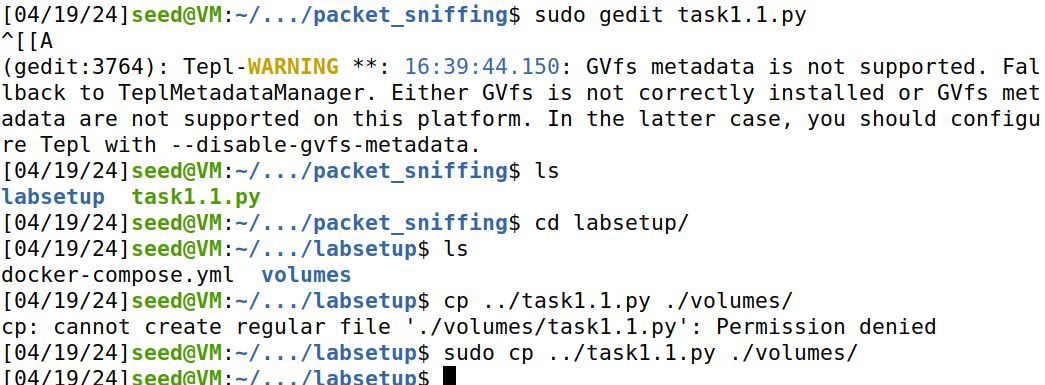
**Lab Task Set 1: Using Scapy to Sniff and Spoof Packets**



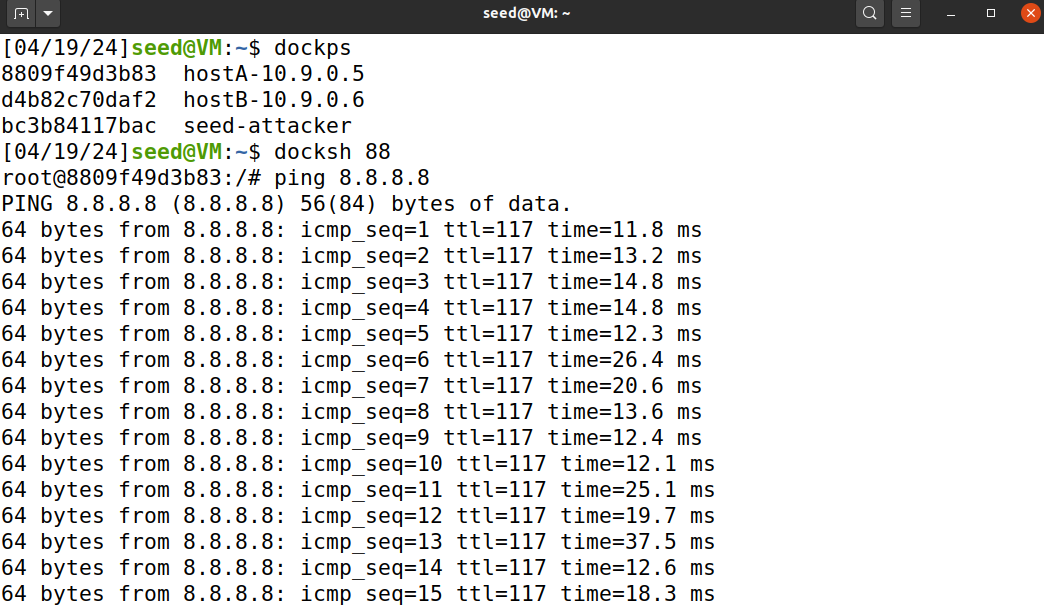


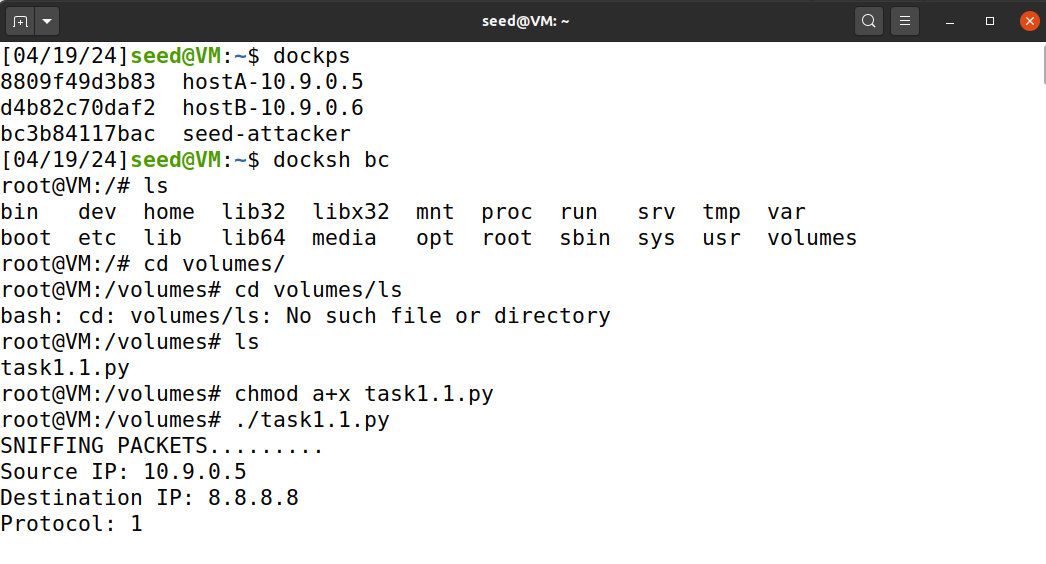
Here we will open hacker side and observe their performance.





To generate traffic we have to run any host. In this case, we will run hostA by docksh 88.

****

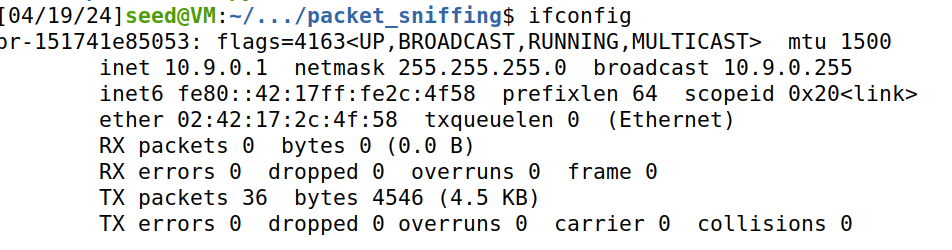
****

****

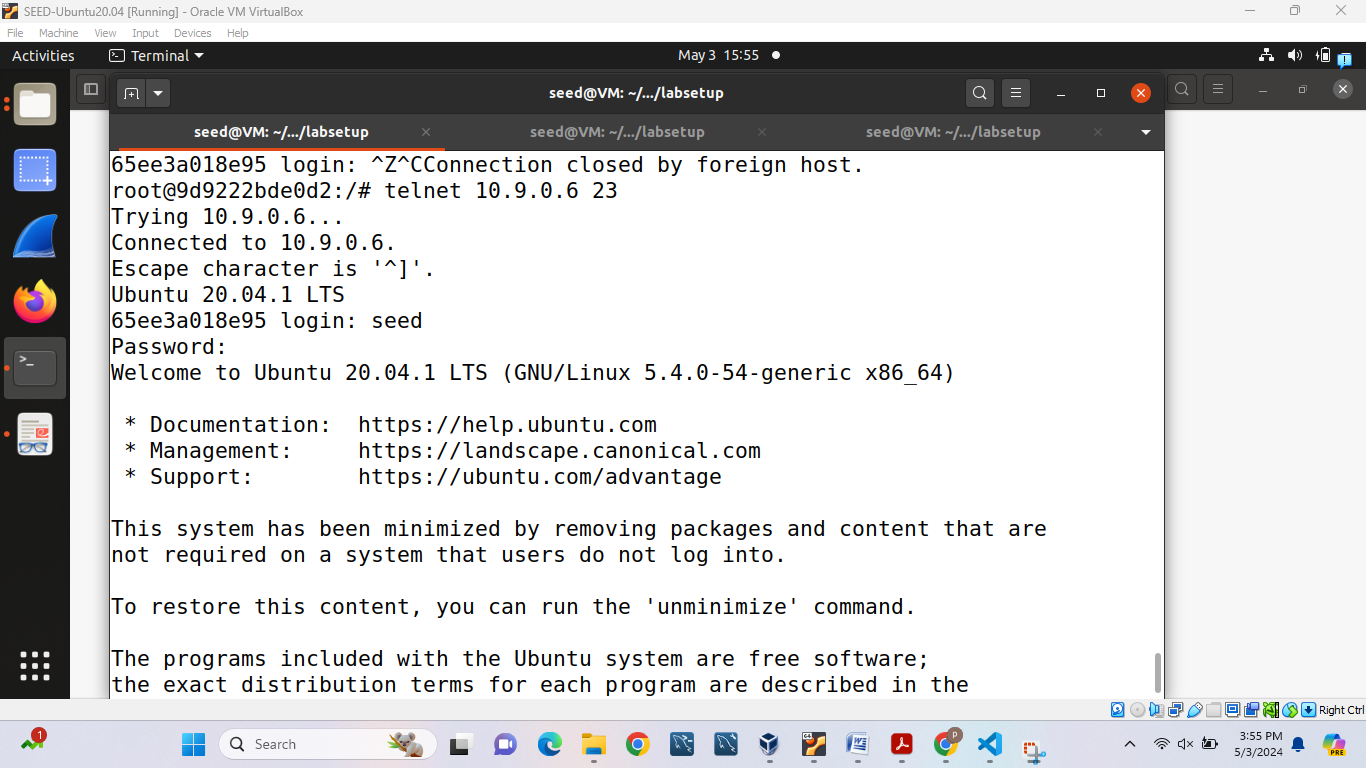
**Task 1.1:** Sniffing Packets

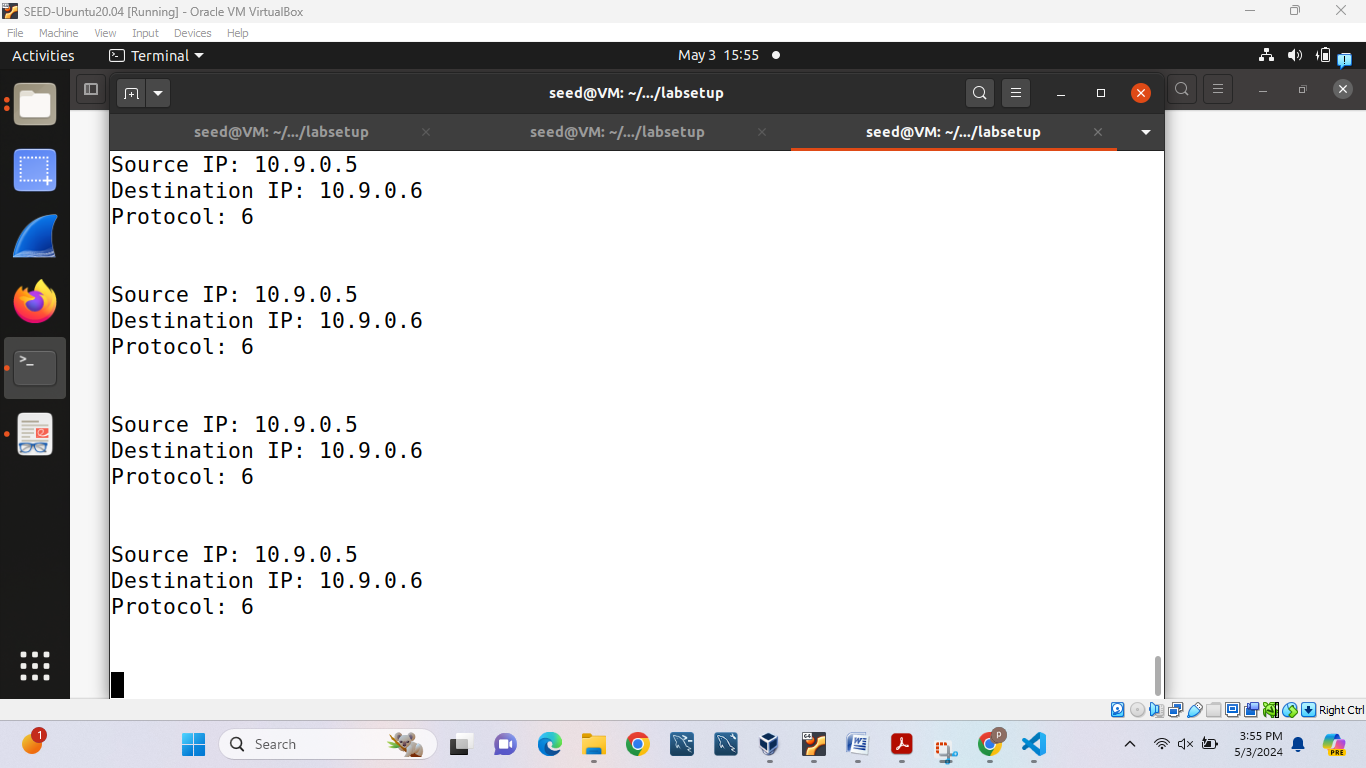
In this task we need to find interface name first. For that we will type command: “ifconfig” and it will return interface name and that we have to copy and paste into our task1 program.

For me interface name is: br – 151741e85053



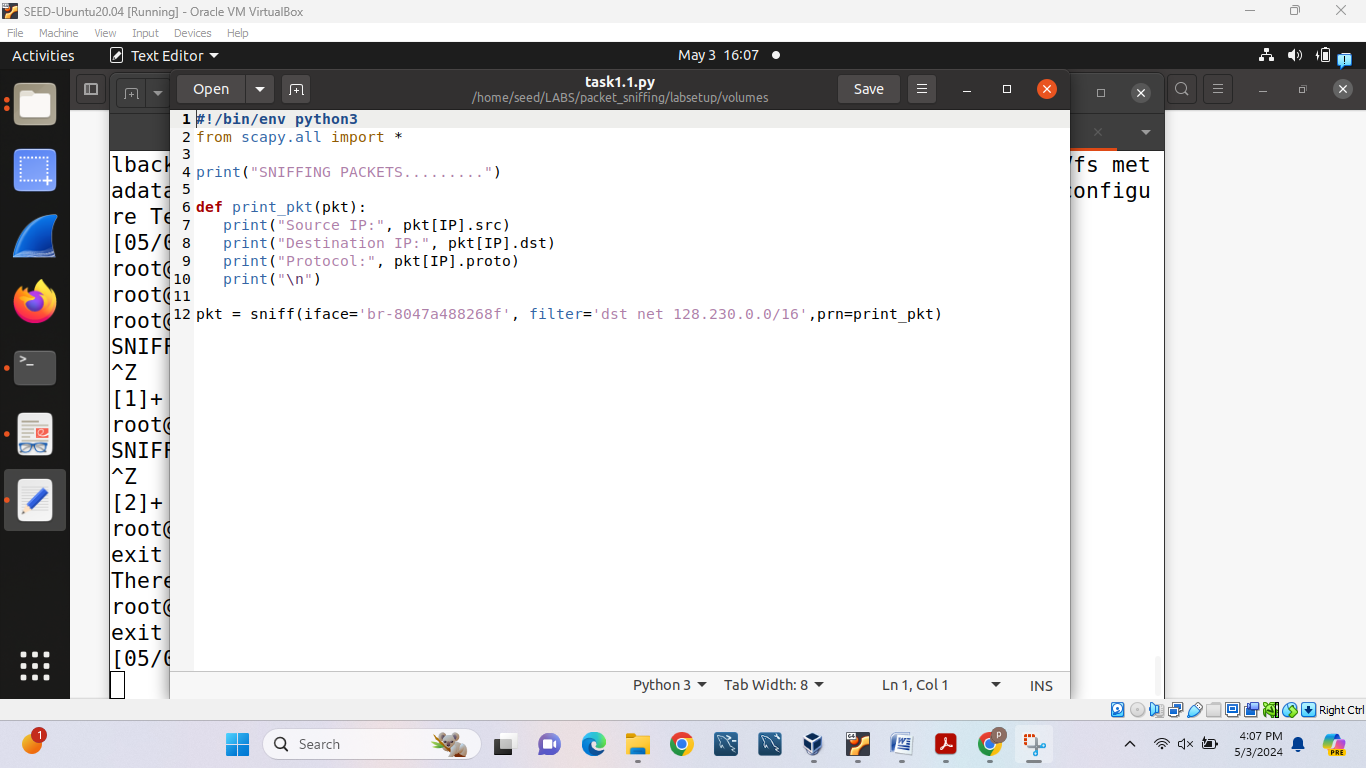
1. Capture any TCP packet that comes from a particular IP and with a destination port number 23.

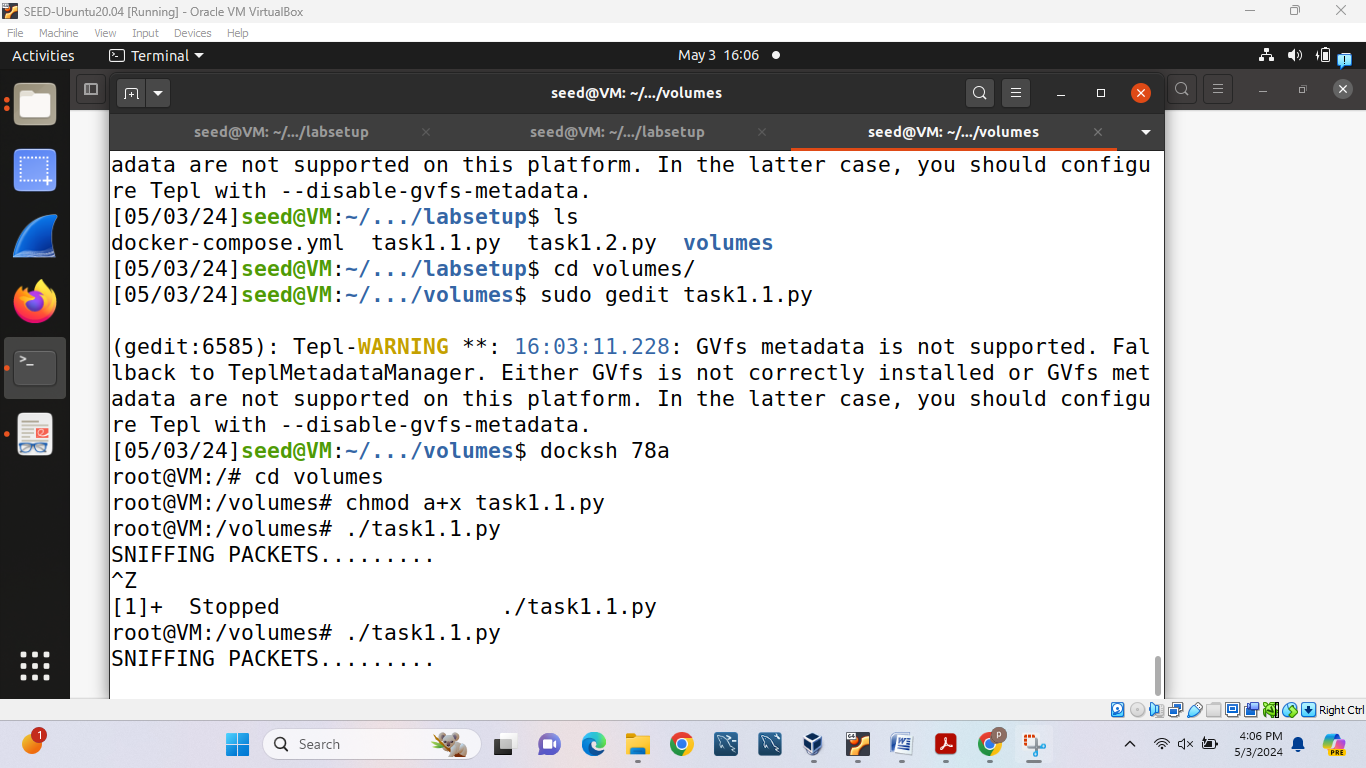




3. Capture packets comes from or to go to a particular subnet. You can pick any subnet, such as

128.230.0.0/16; you should not pick the subnet that your VM is attached to.

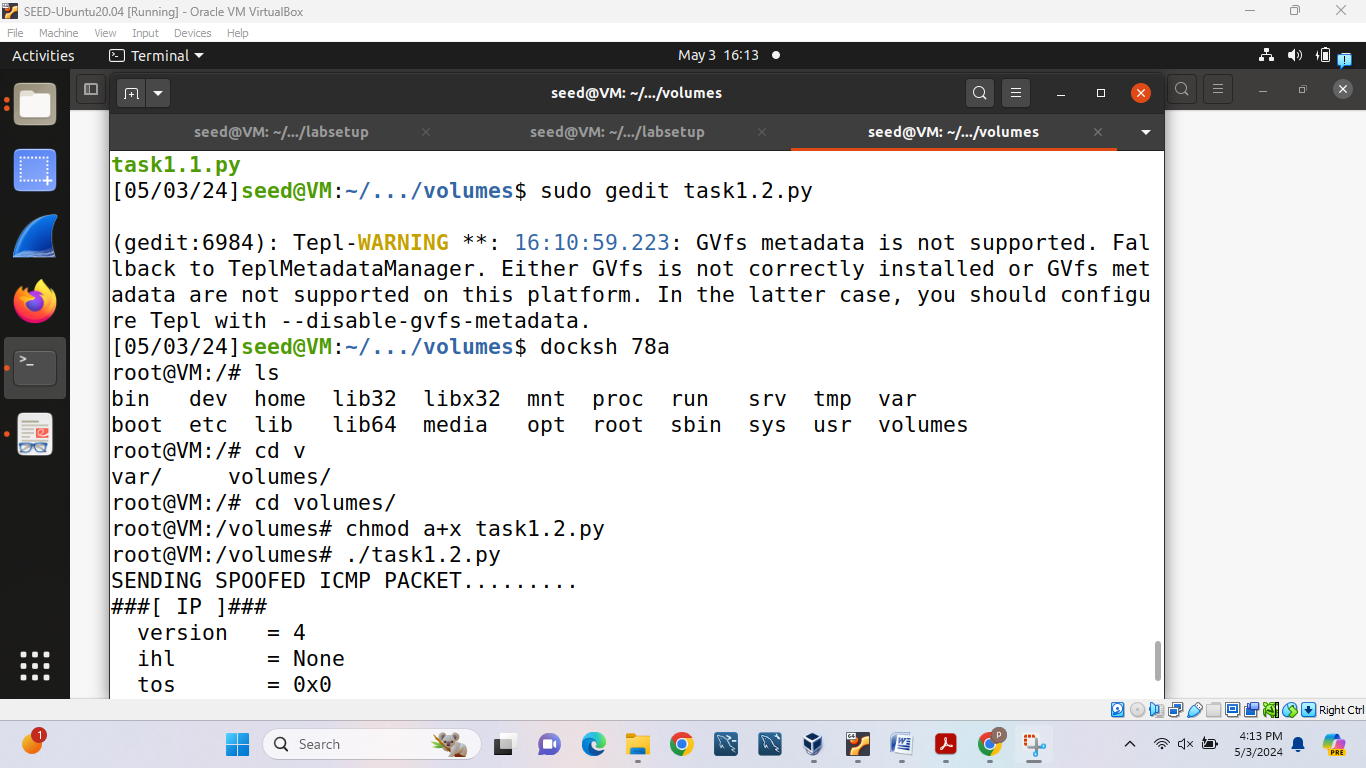




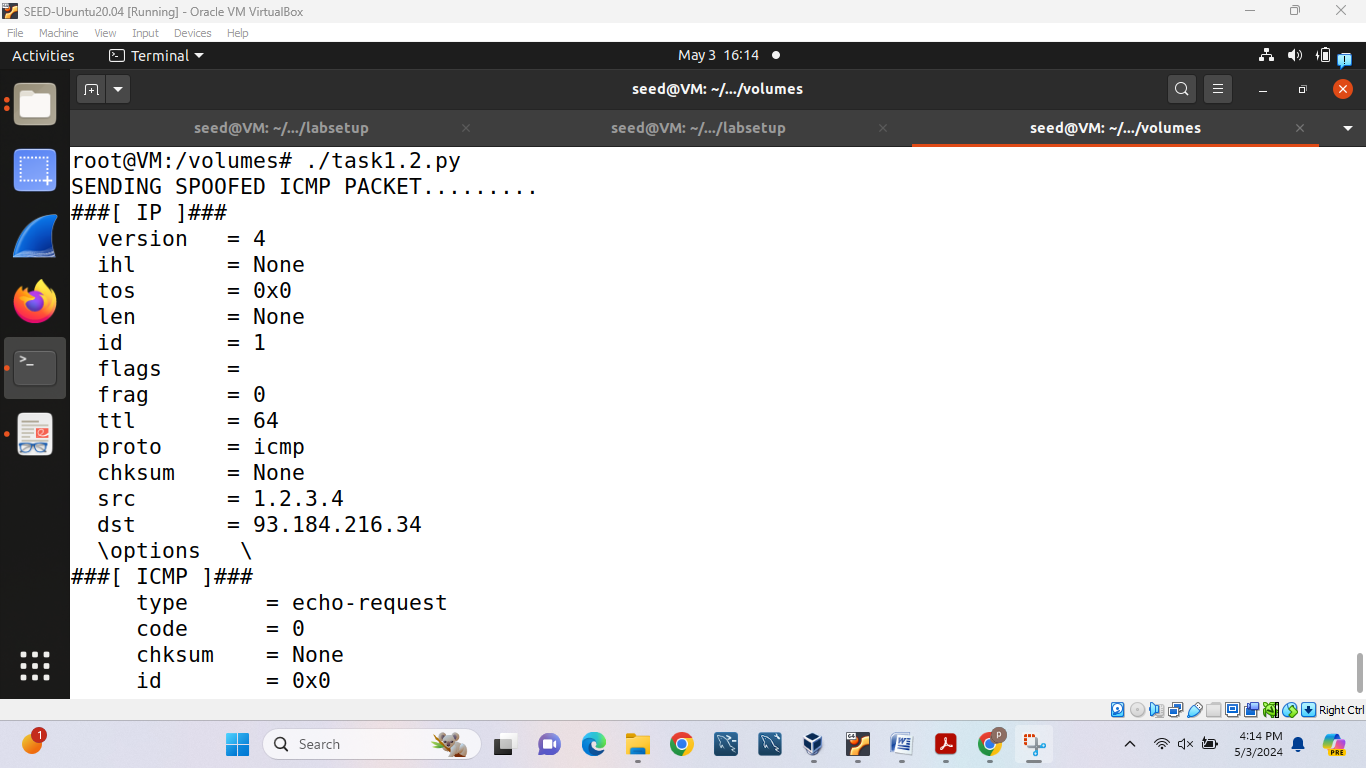
It capture nothing when we change filter = “dst net 128.230.0.0/16” then it will capture nothing in result.

**Task 1.2:** Spoofing ICMP Packets

For this task we first need to copy task1.2.py from moodle and use this code as a reference and start capturing results.

****

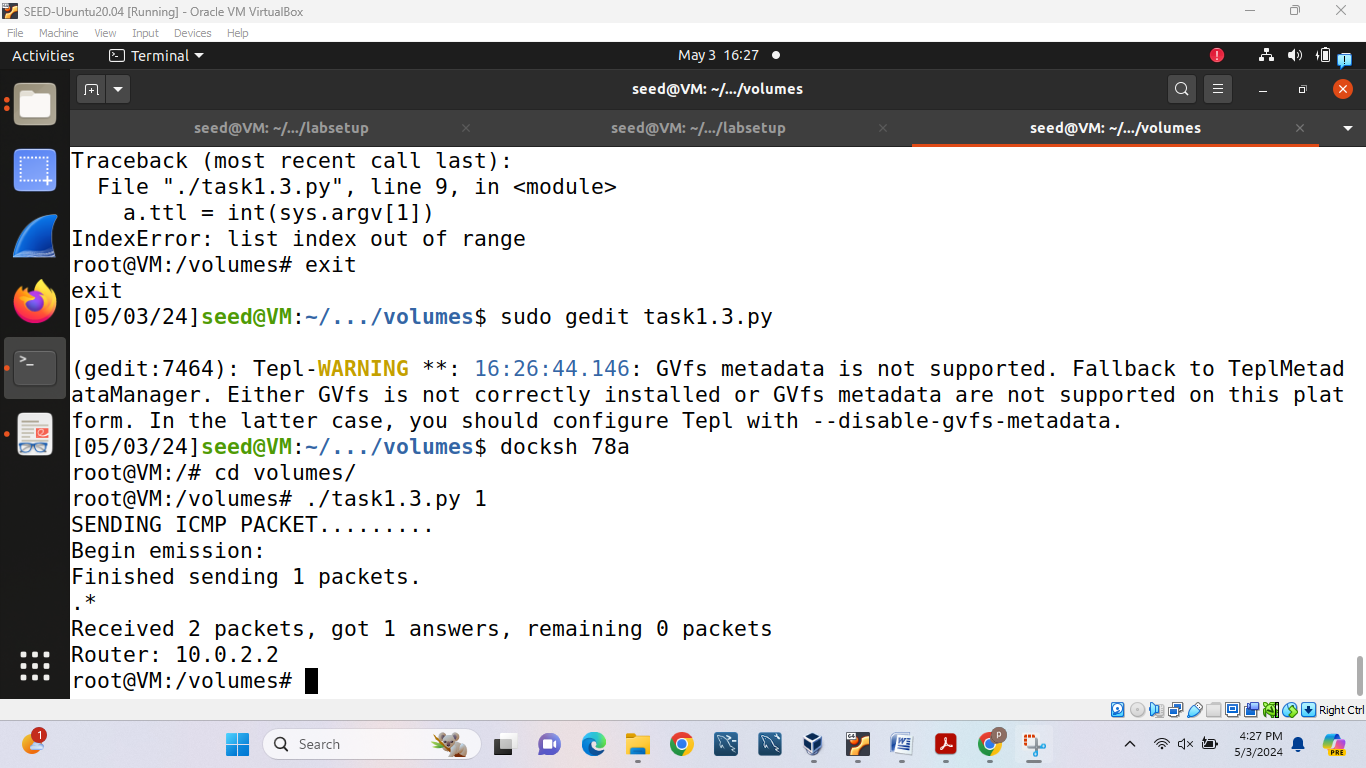
In this task we will get following result after capturing data and here IP address shows: 1.2.3.4 and destination address: 93.184.216.34

****

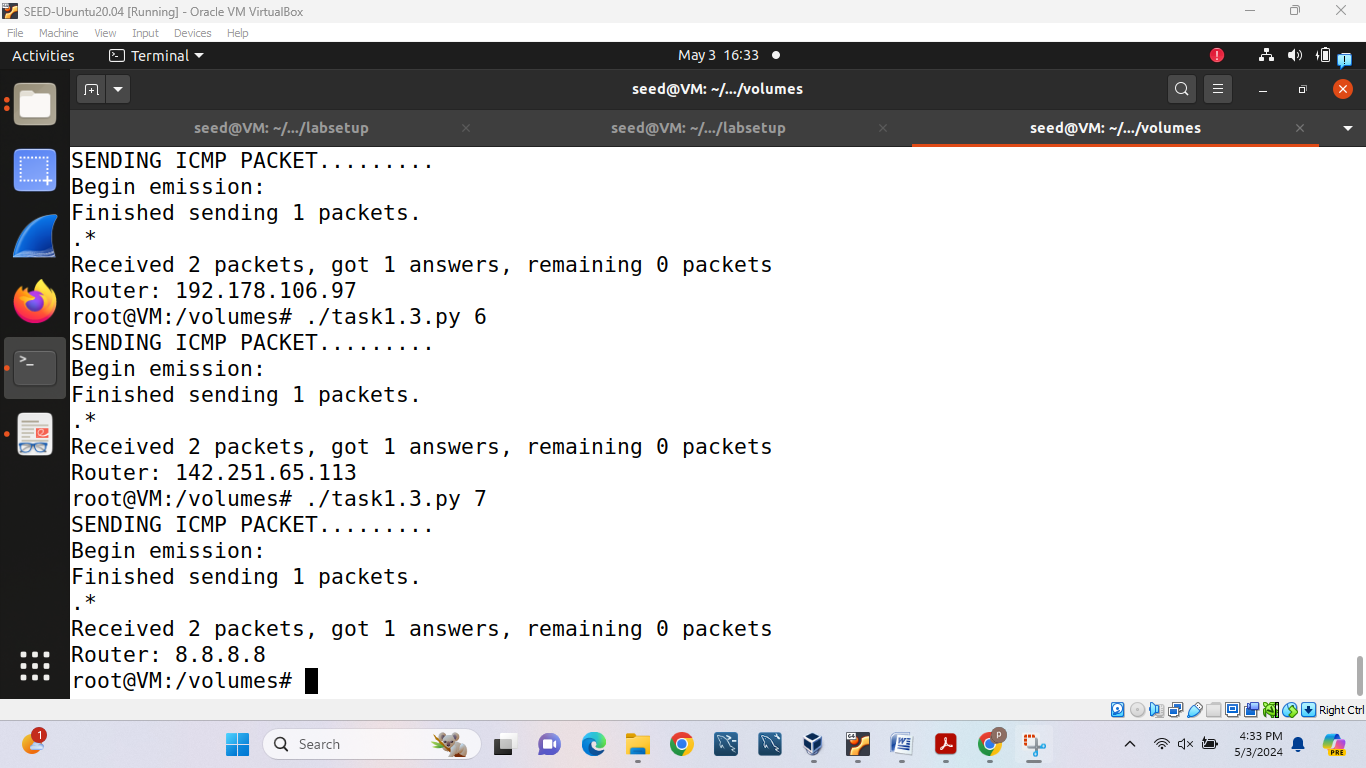
**Task 1.3:** Traceroute

In this task we need to copy task1.3.py code and run it like ./task1.3.py followed by number until we reach final destination 8.8.8.8.

First we will use ./task1.3.py 1 and we will get following result:

****

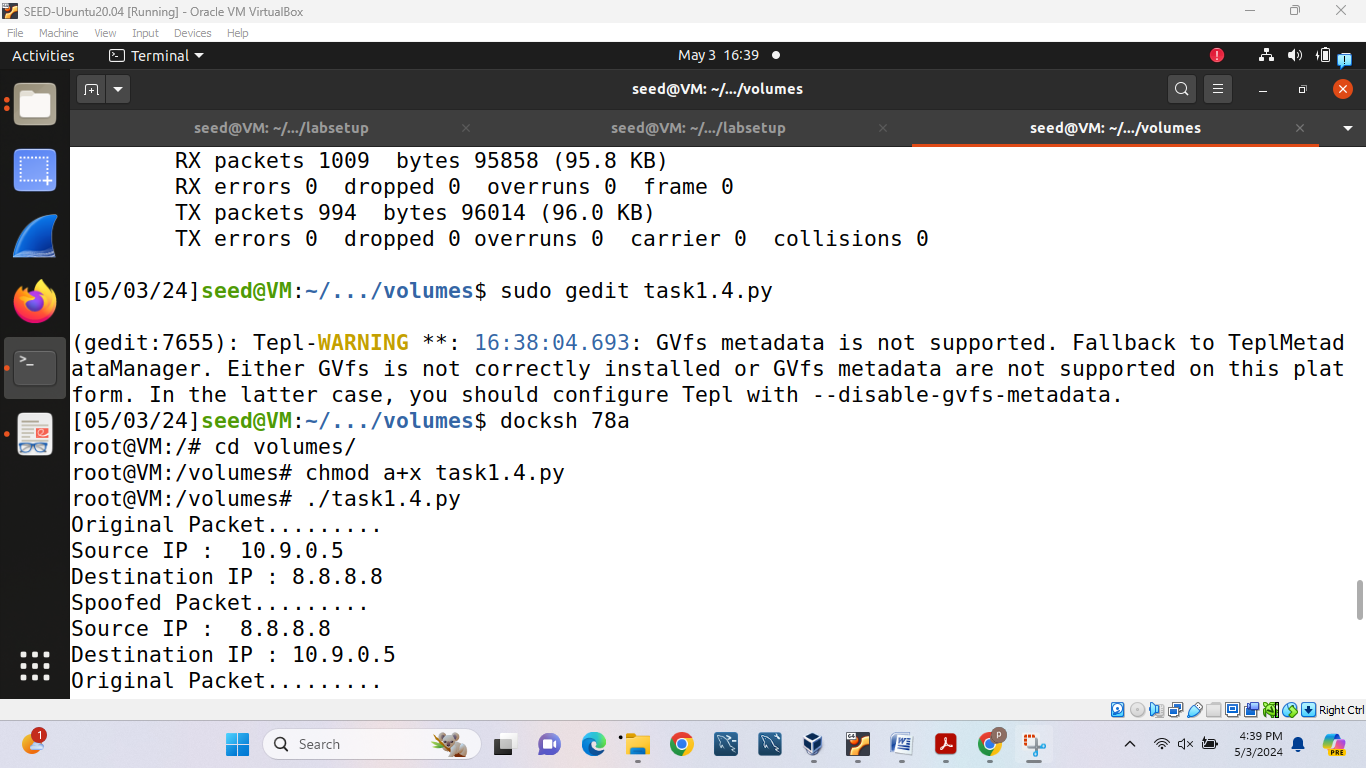
And after 7 iteration I reached to the destination port address which can seen in following screenshot.



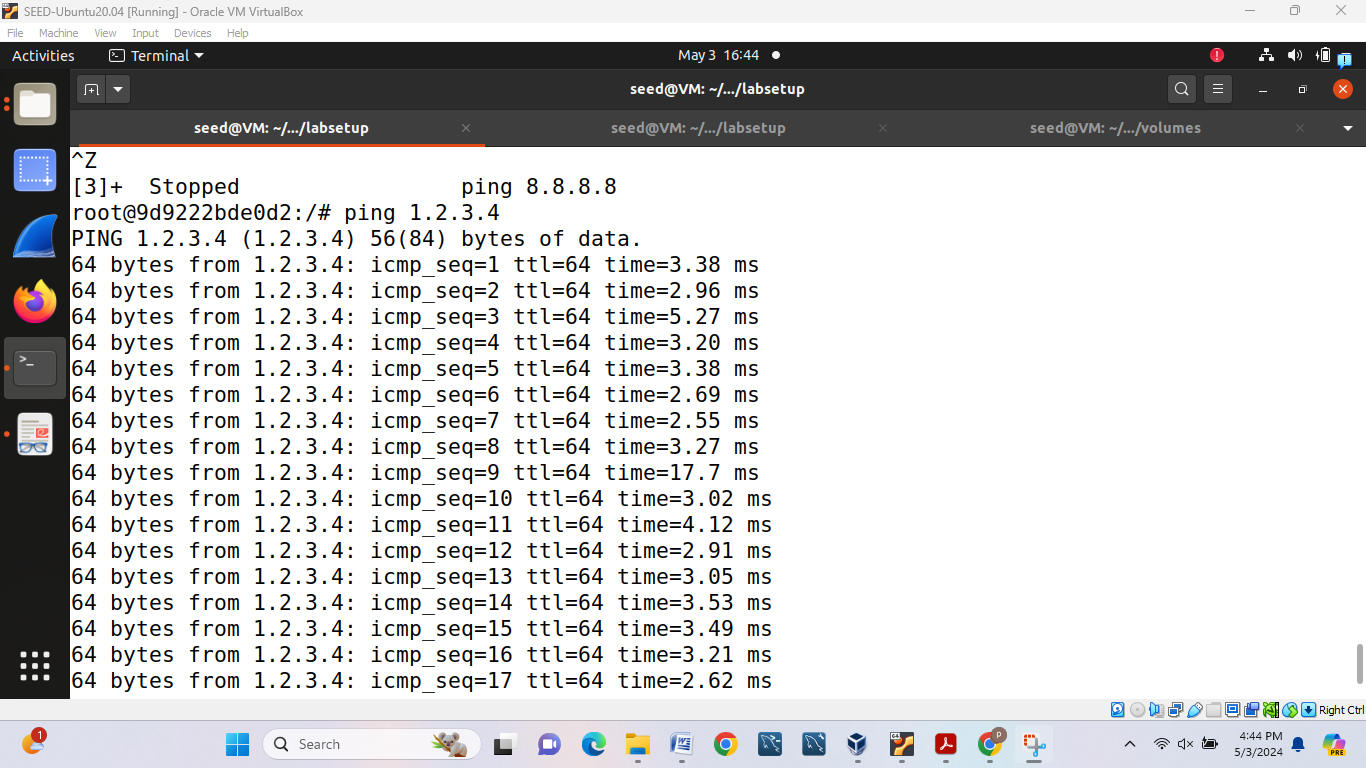
**Task 1.4:** Sniffing and-then Spoofing

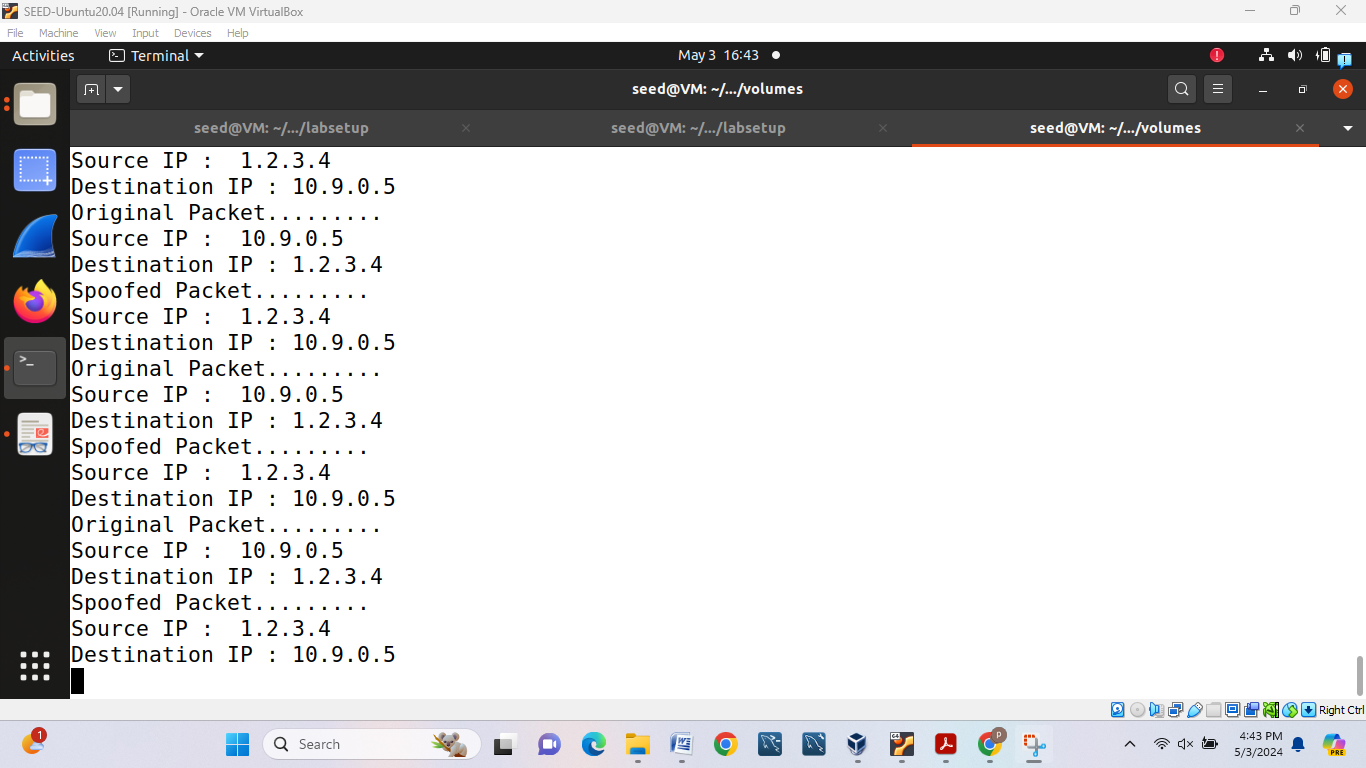
In this task first we will change our iface and start capturing results with different pings:

1. ping 8.8.8.8



1. ping 1.2.3.4:





1. ping 10.9.0.99:

We will not be able to capture anything as destination host is unreachable for this ping number.

