**Advanced Computer Networking and Security**

**Name: Kranthi Kumar Puttapaka**

**700#: 700753999**

1.done with folder setup

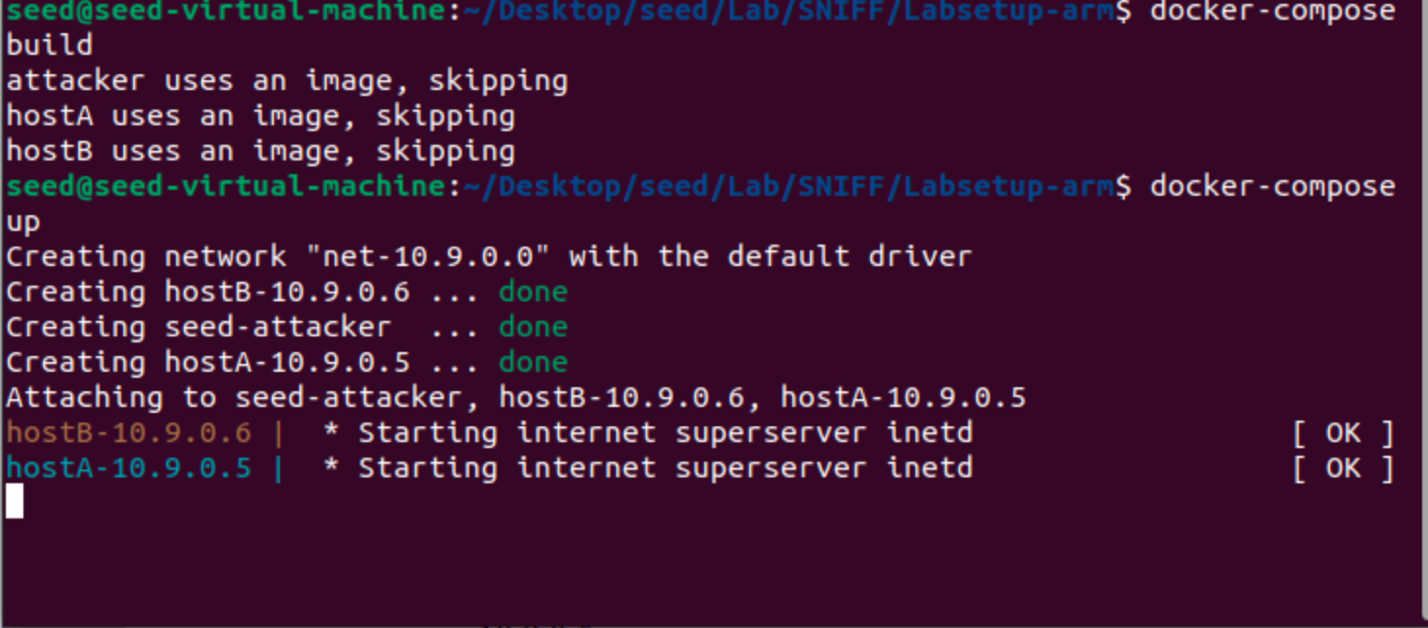
2.installed lab zip file

3.docker setup is up and running

4.using our own VM as attacker instead of seed-attacker docker machine

5.Host A and Host B are other two machines

6.Created shared folder Volumes to access across the containers



**Task1.1:**

Sniffing the packets

A screenshot of a computer

Description automatically generated

The IP() method generates and returns a new, default, and empty IP packet. When the show() command is executed, it displays the packet's contents. I used 'sudo' to gain root privileges, as they are necessary for packet manipulation

**Task1.1.A:**

Run sniffing using root privileges and without root privileges. Observe the difference

A computer screen shot of a program

Description automatically generated

If we run sniffing command without root privileges it throws an error, because raw access to network interface needed root privileges.

**Task1.1.B:**

Sniffing the specific packets using BPF (Berkeley Packet Filtering)

->Capture only ICMP packets

Screenshot of a computer screen

Description automatically generated

->Capture any TCP packets that comes from a particular IP address and with a destination port 23.

A screenshot of a computer

Description automatically generated

->Capture packets come from or to go to a particular subnet. Pick any update like 128.230.0.0/16 and should not pick the subnet attached to the VM.

**A screenshot of a computer

Description automatically generated**

**A computer screen shot of a computer screen

Description automatically generated**

**Task1.2:**

Creating ICMP packets and spoofing to destination IP address

**A screenshot of a computer program

Description automatically generated**

Validate ICMP packets through Wireshark

**A screenshot of a computer

Description automatically generated**

**Task1.3:**

The task here is to find the distance between VM and the selected destination in terms of number of routers in between them using scapy.

A computer screen shot of a computer

Description automatically generated

**Task1.4:**

**Sniff-and-then-spoofing**

To Implement this we need two machines on the same LAN.

1.VM 2. Docker container

Run sniffing program from VM

Try to ping IP address from docker container

Ping a non-exisitng host on the internet 4.3.2.1

A screenshot of a computer screen

Description automatically generated

Ping 10.9.0.99 #a non-existing host on the LAN

A screenshot of a computer

Description automatically generated

Ping 8.8.8.8 #existing host on the internet

A screenshot of a computer screen

Description automatically generated

**IP Route Command to understand the ARP protocol**

**A screenshot of a computer code

Description automatically generated**

**Extra Task 1: Network Sweeper Task**

**A computer screen shot of a computer program

Description automatically generated**

**Extra Task 2: Multi-Port Scanner**

**A computer screen shot of a computer program

Description automatically generated**