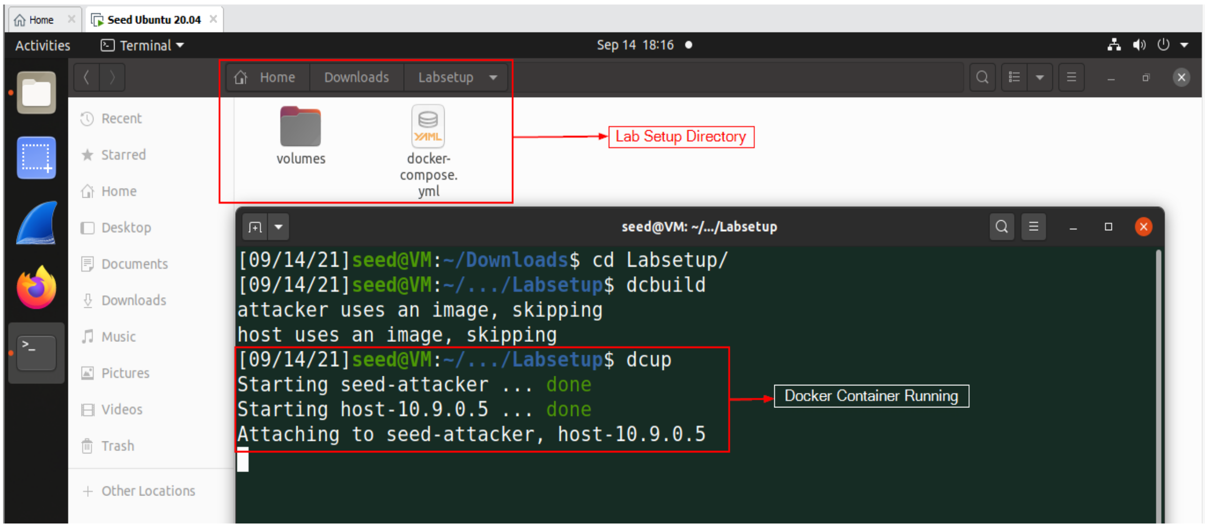
Lab 2 Report- Packet Sniffing and Spoofing Lab

Name: Shrikant Kale - #700727822

1. Task 1.1A: Lab Environment Setup

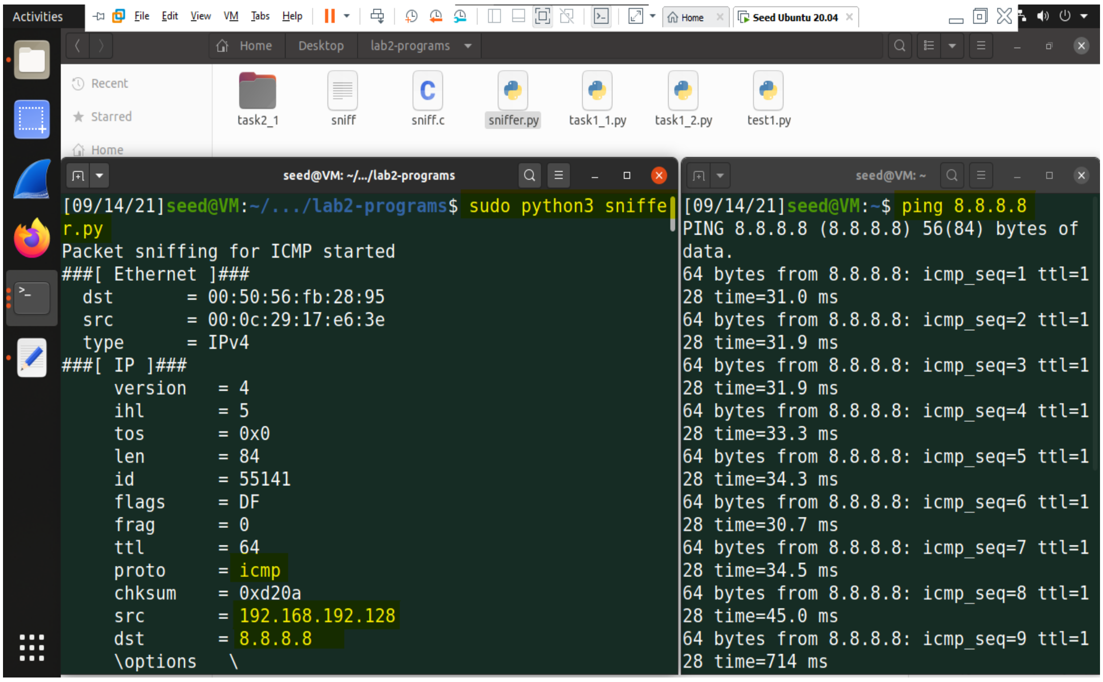
- Created Lab environment using docker containers.
- To execute docker container, I have used docker-compose commands.
  - dcbuild (docker-compose build) – to build the docker container image
  - dcup (docker-compose up) – to run the docker container
  - dcdown (docker-compose down) – to shut down the container



```
[09/14/21]seed@VM:~/Downloads$ cd Labsetup/
[09/14/21]seed@VM:~/.../Labsetup$ dcbuild
attacker uses an image, skipping
host uses an image, skipping
[09/14/21]seed@VM:~/.../Labsetup$ dcup
Starting seed-attacker ... done
Starting host-10.9.0.5 ... done
Attaching to seed-attacker, host-10.9.0.5
```

2. Task 1.1B:

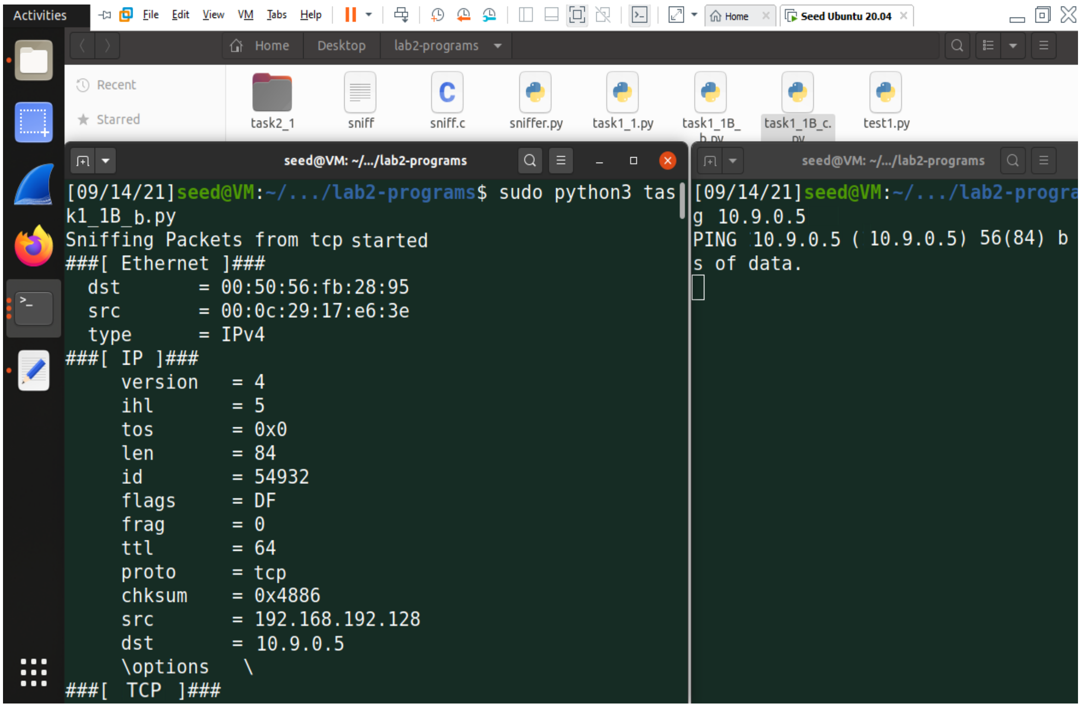
- Capture only the ICMP packet – after setting the filter on your sniff program, try to ping 8.8.8.8
  - Set filter to capture/sniff ICMP packets using python program



```
[09/14/21]seed@VM:~/.../lab2-programs$ sudo python3 sniffer.py
Packet sniffing for ICMP started
###[ Ethernet ]###
  dst       = 00:50:56:fb:28:95
  src       = 00:0c:29:17:e6:3e
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 55141
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = icmp
     chksum    = 0xd20a
     src       = 192.168.192.128
     dst       = 8.8.8.8
     \options   \
```

```
[09/14/21]seed@VM:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=31.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=31.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=31.9 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=33.3 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=128 time=34.3 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=128 time=30.7 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=128 time=34.5 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=128 time=45.0 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=128 time=714 ms
```

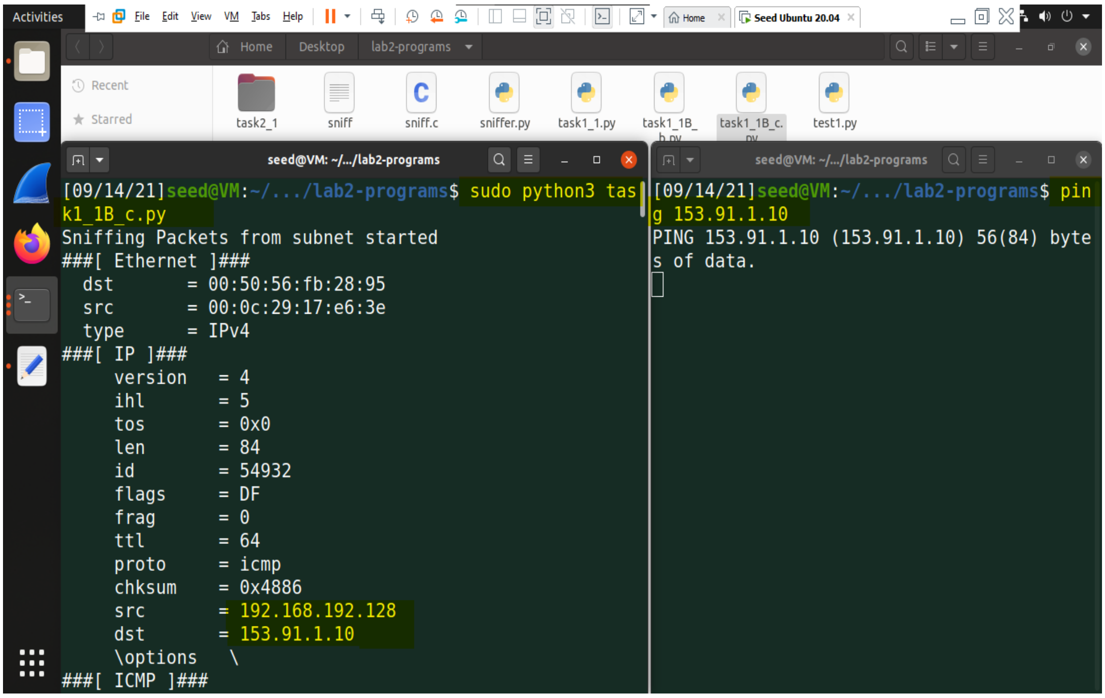
- Capture any TCP packet that comes from a particular IP and with a destination port number 23 – after setting the filter on your sniff program, try to telnet from your host VM to the victim at 10.9.0.5.
    - Captured TCP packets



```
[09/14/21]seed@VM:~/.../lab2-programs$ sudo python3 tas
k1_1B_b.py
Sniffing Packets from tcp started
###[ Ethernet ]###
  dst       = 00:50:56:fb:28:95
  src       = 00:0c:29:17:e6:3e
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 54932
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0x4886
     src       = 192.168.192.128
     dst       = 10.9.0.5
     \options   \
###[ TCP ]###
```

```
[09/14/21]seed@VM:~/.../lab2-progra
g 10.9.0.5
PING 10.9.0.5 ( 10.9.0.5) 56(84) b
s of data.
```

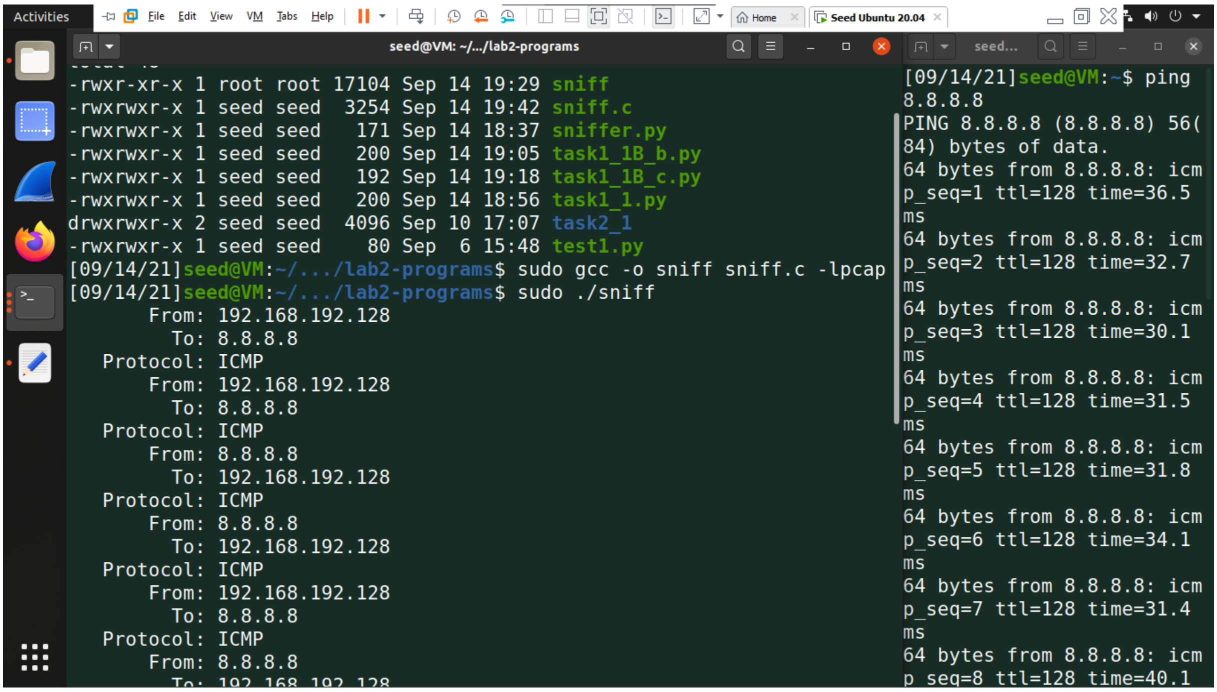
- Capture packets comes from or to go to a particular subnet. You can pick any subnet, such as 128.230.0.0/16; you should not pick the subnet that your VM is attached to – you can use 153.91.1.0/24 - the subnet belongs to UCM and ping UCM's web server at 153.91.1.10 after setting the filter on your sniff program
    - Op



```
[09/14/21]seed@VM:~/.../lab2-programs$ sudo python3 tas
k1_1B_c.py
Sniffing Packets from subnet started
###[ Ethernet ]###
  dst       = 00:50:56:fb:28:95
  src       = 00:0c:29:17:e6:3e
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 54932
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = icmp
     chksum    = 0x4886
     src       = 192.168.192.128
     dst       = 153.91.1.10
     \options   \
###[ ICMP ]###
```

```
[09/14/21]seed@VM:~/.../lab2-programs$ pin
g 153.91.1.10
PING 153.91.1.10 (153.91.1.10) 56(84) byte
s of data.
```

3. **Task 2.1A**: On the Host VM (attacker), open Firefox and surf to the Blackboard. Download sniff.c. You only need to modify one line of code based on your VM's NIC. Compile and run the sniff program using super user privilege. Open another terminal on the Attacker VM and ping 8.8.8.8. You should see the source IP, destination IP and protocol information printed by the sniff program.
   - Done sniffing with c programs and printed source and destination.



```
-rwxr-xr-x 1 root root 17104 Sep 14 19:29 sniff
-rwxrwxr-x 1 seed seed  3254 Sep 14 19:42 sniff.c
-rwxrwxr-x 1 seed seed   171 Sep 14 18:37 sniffer.py
-rwxrwxr-x 1 seed seed   200 Sep 14 19:05 task1_1B_b.py
-rwxrwxr-x 1 seed seed   192 Sep 14 19:18 task1_1B_c.py
-rwxrwxr-x 1 seed seed   200 Sep 14 18:56 task1_1.py
drwxrwxr-x 2 seed seed  4096 Sep 10 17:07 task2_1
-rwxrwxr-x 1 seed seed    80 Sep  6 15:48 test1.py
[09/14/21]seed@VM:~/.../lab2-programs$ sudo gcc -o sniff sniff.c -lpcap
[09/14/21]seed@VM:~/.../lab2-programs$ sudo ./sniff
       From: 192.168.192.128
         To: 8.8.8.8
   Protocol: ICMP
       From: 192.168.192.128
         To: 8.8.8.8
   Protocol: ICMP
       From: 8.8.8.8
         To: 192.168.192.128
   Protocol: ICMP
       From: 8.8.8.8
         To: 192.168.192.128
   Protocol: ICMP
       From: 192.168.192.128
         To: 8.8.8.8
   Protocol: ICMP
       From: 8.8.8.8
         To: 192.168.192.128
```

```
[09/14/21]seed@VM:~$ ping
8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(
84) bytes of data.
64 bytes from 8.8.8.8: icm
p_seq=1 ttl=128 time=36.5
ms
64 bytes from 8.8.8.8: icm
p_seq=2 ttl=128 time=32.7
ms
64 bytes from 8.8.8.8: icm
p_seq=3 ttl=128 time=30.1
ms
64 bytes from 8.8.8.8: icm
p_seq=4 ttl=128 time=31.5
ms
64 bytes from 8.8.8.8: icm
p_seq=5 ttl=128 time=31.8
ms
64 bytes from 8.8.8.8: icm
p_seq=6 ttl=128 time=34.1
ms
64 bytes from 8.8.8.8: icm
p_seq=7 ttl=128 time=31.4
ms
64 bytes from 8.8.8.8: icm
p_seq=8 ttl=128 time=40.1
```