

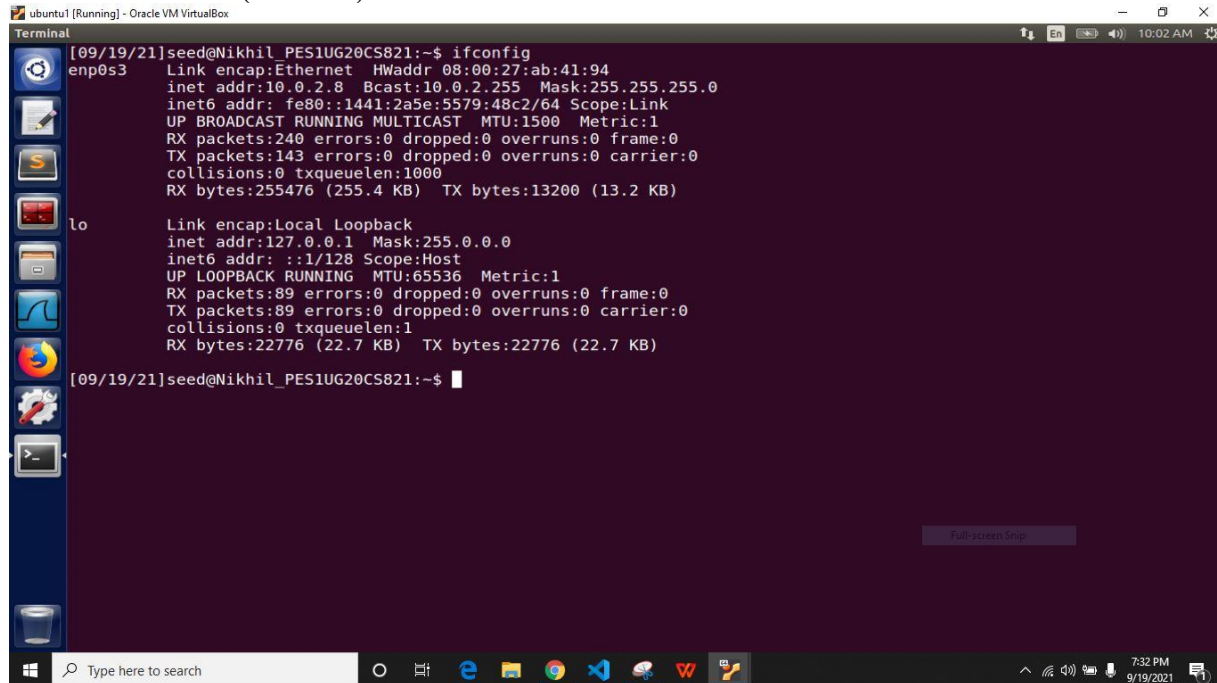
Week 1 Packet Sniffing and Spoofing

Name: Nikhil T M

SRN: PES1UG20CS821

Subject: Computer Network Security

Attacker Machine(ubuntu1): 10.0.2.8

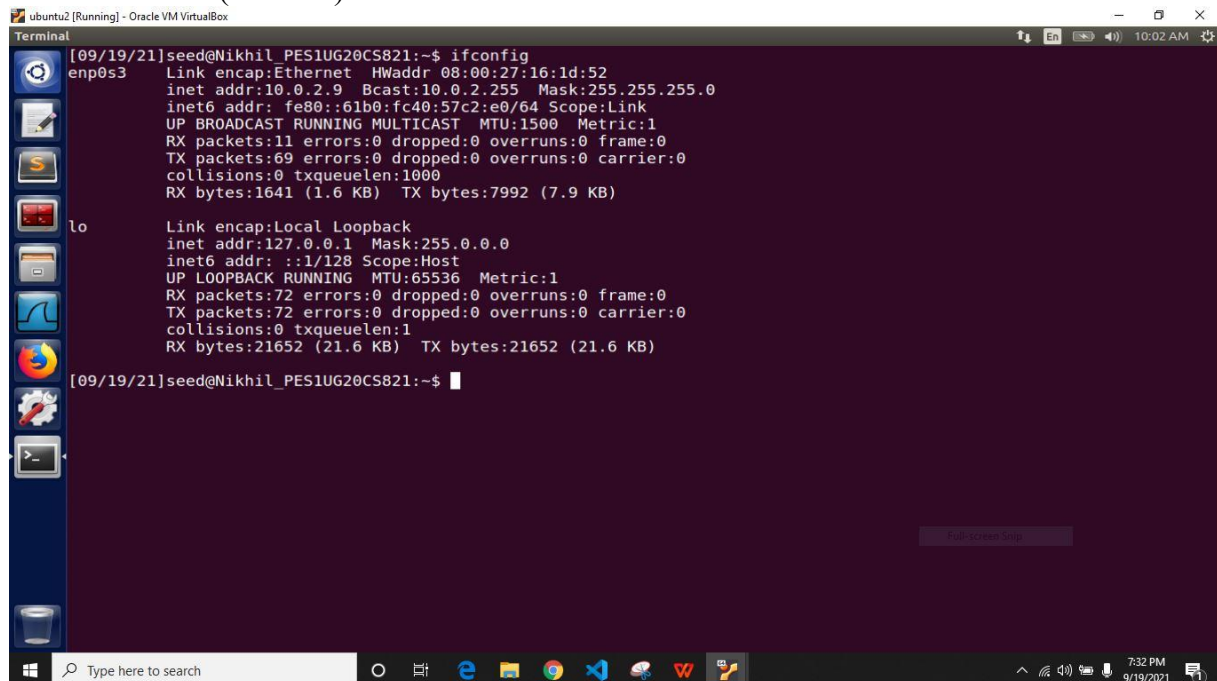


```
Terminal
[09/19/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:ab:41:94
        inet addr:10.0.2.8  Bcast:10.0.2.255  Mask:255.255.255.0
        inet6 addr: fe80::1441:2a5e:5579:48c2/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:240 errors:0 dropped:0 overruns:0 frame:0
        TX packets:143 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:255476 (255.4 KB)  TX bytes:13200 (13.2 KB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:89 errors:0 dropped:0 overruns:0 frame:0
        TX packets:89 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:22776 (22.7 KB)  TX bytes:22776 (22.7 KB)

[09/19/21]seed@Nikhil_PES1UG20CS821:~$
```

Victim Machine(ubuntu2): 10.0.2.9



```
Terminal
[09/19/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:16:1d:52
        inet addr:10.0.2.9  Bcast:10.0.2.255  Mask:255.255.255.0
        inet6 addr: fe80::61b0:fc40:57c2:e0/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:11 errors:0 dropped:0 overruns:0 frame:0
        TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:1641 (1.6 KB)  TX bytes:7992 (7.9 KB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:72 errors:0 dropped:0 overruns:0 frame:0
        TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:21652 (21.6 KB)  TX bytes:21652 (21.6 KB)

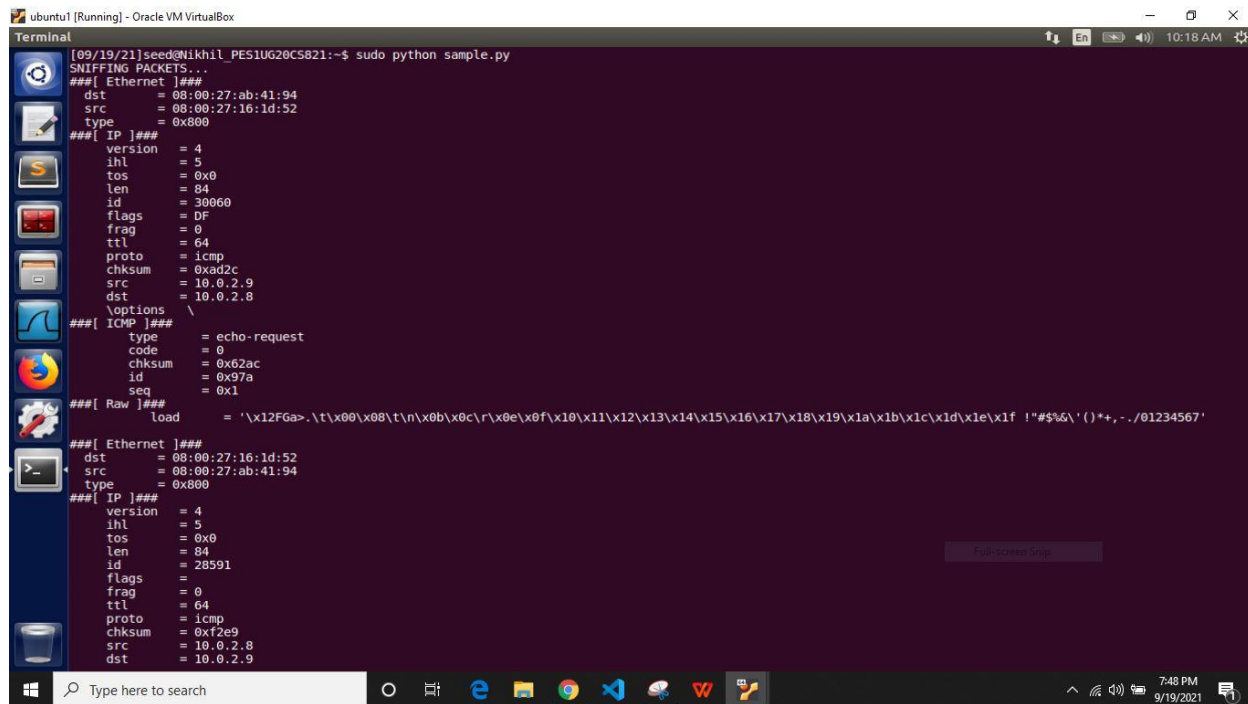
[09/19/21]seed@Nikhil_PES1UG20CS821:~$
```

Task 1: Sniffing Packet

Task 1.1 Sniff IP packets using Scapy

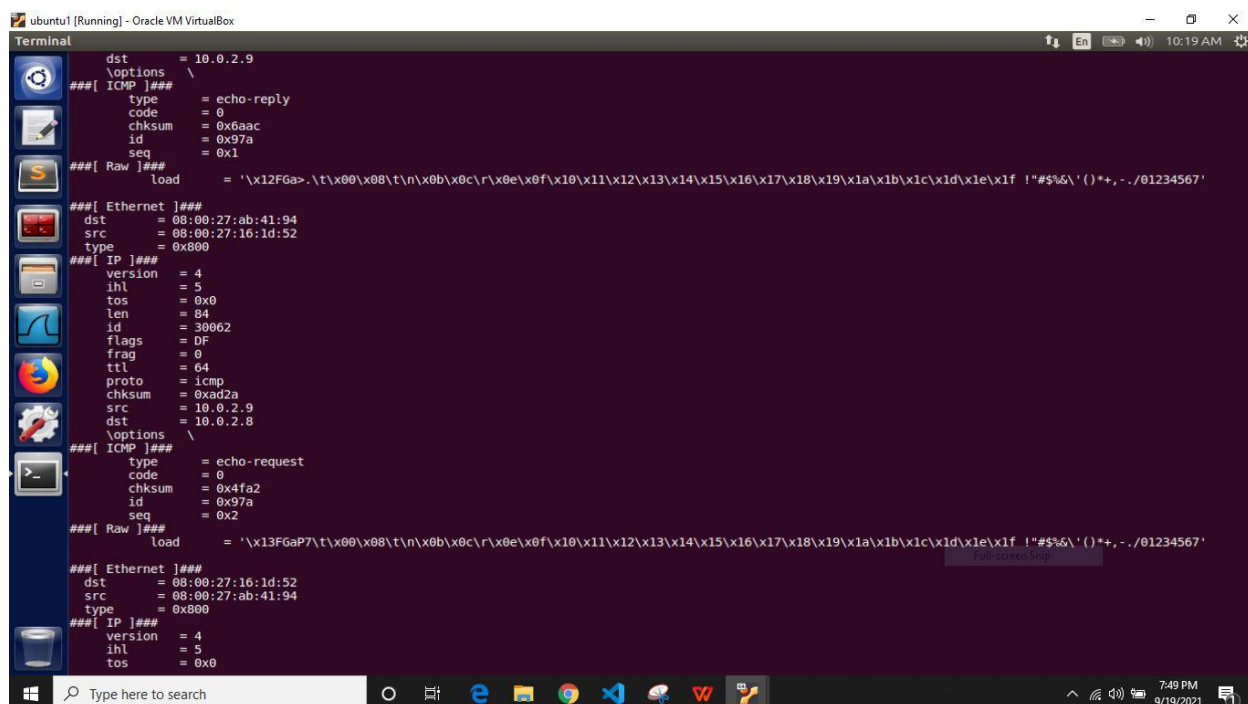
We run the command `sudo python sample.py` on the attacker machine (ubuntu1) of IP address 10.0.2.8. because attacker is the one who want to sniff the packets.

Observation On attacker machine: we run the code on the attacker machine using `sudo python sample.py` and capture the packets.



```
[09/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo python sample.py
SNIFFING PACKETS...
#### Ethernet ####
  dst      = 08:00:27:ab:41:94
  src      = 08:00:27:16:1d:52
  type     = 0x800
#### IP ####
  version  = 4
  ihl      = 5
  tos      = 0x0
  len      = 84
  id       = 30860
  flags    = DF
  frag     = 0
  ttl      = 64
  proto    = icmp
  chksum   = 0xad2c
  src      = 10.0.2.9
  dst      = 10.0.2.8
  \options
#### ICMP ####
  type     = echo-request
  code     = 0
  chksum   = 0x62ac
  id       = 0x97a
  seq      = 0x1
#### Raw ####
  Load     = '\x12FGa>.\t\x00\x08\t\n\x0b\x0c\r\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#%&'()*+,-./01234567'

#### Ethernet ####
  dst      = 08:00:27:16:1d:52
  src      = 08:00:27:ab:41:94
  type     = 0x800
#### IP ####
  version  = 4
  ihl      = 5
  tos      = 0x0
  len      = 84
  id       = 28591
  flags    =
  frag     = 0
  ttl      = 64
  proto    = icmp
  chksum   = 0xf2e9
  src      = 10.0.2.8
  dst      = 10.0.2.9
```

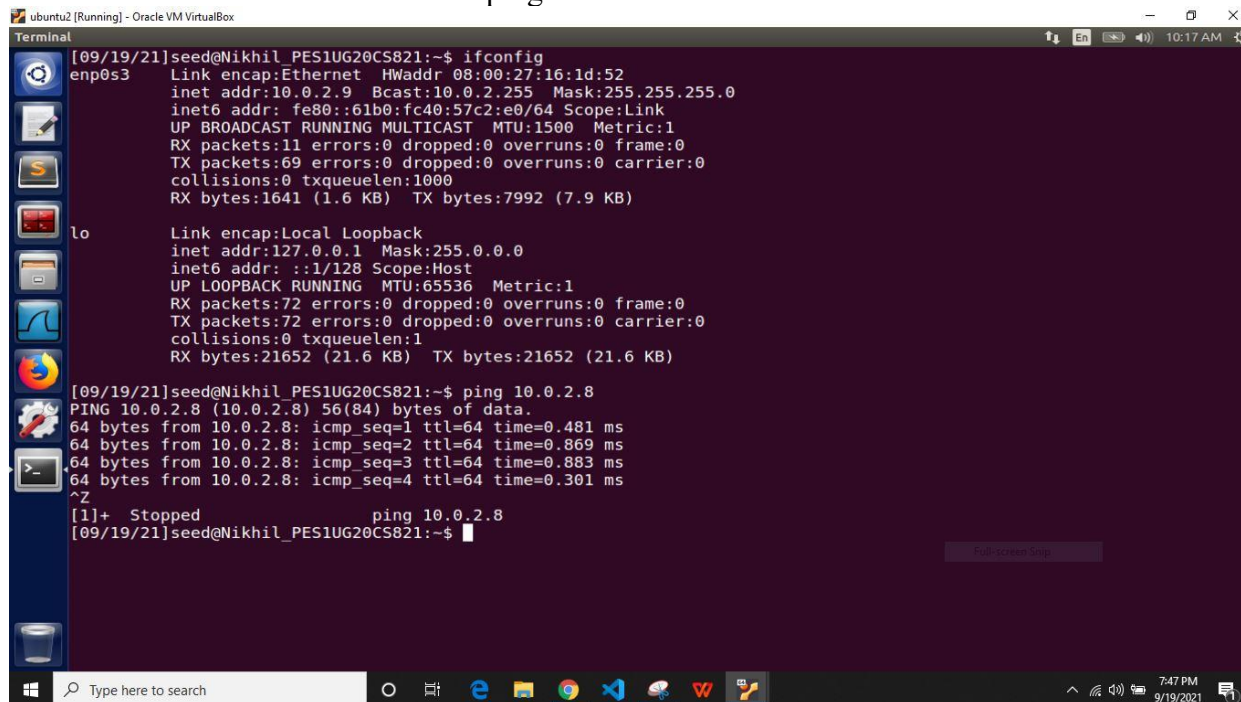


```
dst      = 10.0.2.9
\options
#### ICMP ####
  type     = echo-reply
  code     = 0
  chksum   = 0x6aac
  id       = 0x97a
  seq      = 0x1
#### Raw ####
  Load     = '\x12FGa>.\t\x00\x08\t\n\x0b\x0c\r\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#%&'()*+,-./01234567'

#### Ethernet ####
  dst      = 08:00:27:ab:41:94
  src      = 08:00:27:16:1d:52
  type     = 0x800
#### IP ####
  version  = 4
  ihl      = 5
  tos      = 0x0
  len      = 84
  id       = 30862
  flags    = DF
  frag     = 0
  ttl      = 64
  proto    = icmp
  chksum   = 0xad2a
  src      = 10.0.2.9
  dst      = 10.0.2.8
  \options
#### ICMP ####
  type     = echo-request
  code     = 0
  chksum   = 0x4fa2
  id       = 0x97a
  seq      = 0x2
#### Raw ####
  Load     = '\x13FGaP7.\t\x00\x08\t\n\x0b\x0c\r\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#%&'()*+,-./01234567'

#### Ethernet ####
  dst      = 08:00:27:16:1d:52
  src      = 08:00:27:ab:41:94
  type     = 0x800
#### IP ####
  version  = 4
  ihl      = 5
  tos      = 0x0
```

Observations On victim machine:we ping the attacker



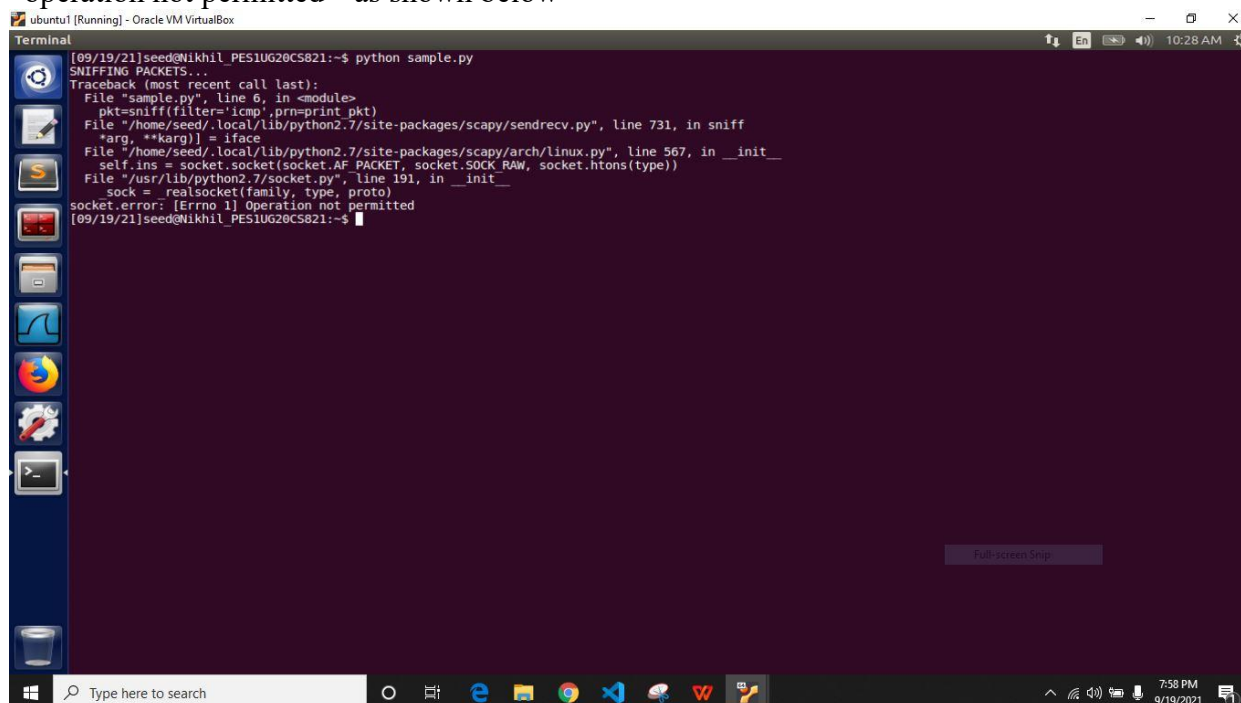
```
Terminal
[09/19/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:16:1d:52
          inet addr:10.0.2.9  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::61b0:fc40:57c2:e0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1641 (1.6 KB)  TX bytes:7992 (7.9 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:72 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:21652 (21.6 KB)  TX bytes:21652 (21.6 KB)

[09/19/21]seed@Nikhil_PES1UG20CS821:~$ ping 10.0.2.8
PING 10.0.2.8 (10.0.2.8) 56(84) bytes of data:
64 bytes from 10.0.2.8: icmp_seq=1 ttl=64 time=0.481 ms
64 bytes from 10.0.2.8: icmp_seq=2 ttl=64 time=0.869 ms
64 bytes from 10.0.2.8: icmp_seq=3 ttl=64 time=0.883 ms
64 bytes from 10.0.2.8: icmp_seq=4 ttl=64 time=0.301 ms
^Z
[1]+  Stopped                  ping 10.0.2.8
[09/19/21]seed@Nikhil_PES1UG20CS821:~$
```

We get to know that we can sniff the packets and gather information such such as packets source and destination IP address and mac address along with the port number ,length of the packet,ICMP type etc.

When we run the same program without root (sudo) privileges we end up with an error “operation not permitted “ as shown below

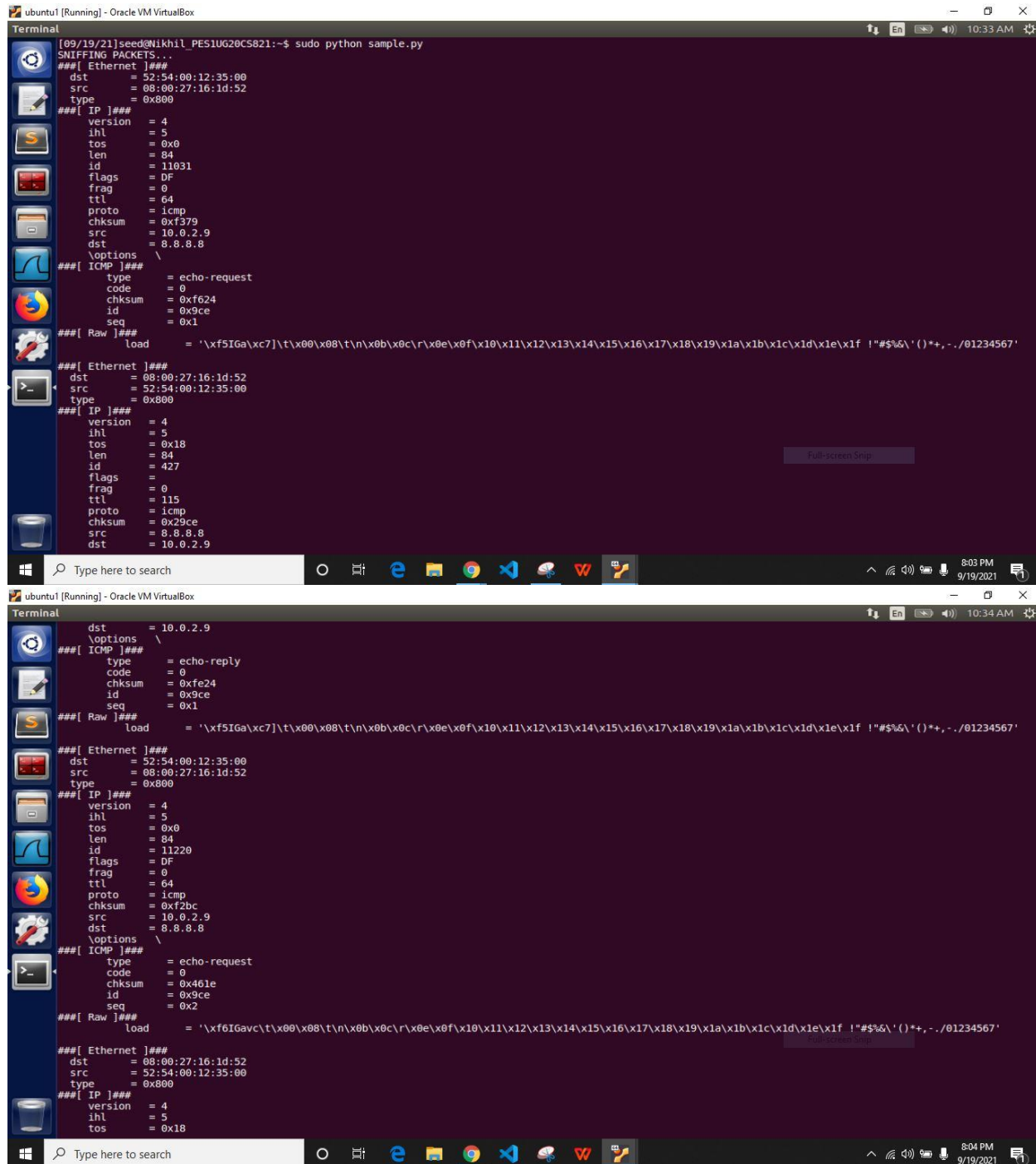


```
Terminal
[09/19/21]seed@Nikhil_PES1UG20CS821:~$ python sample.py
SNIFFING PACKETS...
Traceback (most recent call last):
  File "sample.py", line 6, in <module>
    pkt=sniff(filters='icmp',prn=print pkt)
  File "/home/seed/.local/lib/python2.7/site-packages/scapy/sendrecv.py", line 731, in sniff
    *arg, **karg)) = iface
  File "/home/seed/.local/lib/python2.7/site-packages/scapy/arch/linux.py", line 567, in __init__
    self.ins = socket.socket(socket.AF_PACKET, socket.SOCK_RAW, socket.htons(type))
  File "/usr/lib/python2.7/socket.py", line 191, in __init__
    sock = _realsocket(family, type, proto)
socket.error: [Errno 1] Operation not permitted
[09/19/21]seed@Nikhil_PES1UG20CS821:~$
```

Task 1.2 Capturing ICMP, TCP packet and Subnet

Task 1.2.1 Capture only the ICMP packet

Observation on attacker machine



```
[09/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo python sample.py
SNIFFING PACKETS...
###[ Ethernet ]###
  dst      = 52:54:00:12:35:00
  src      = 08:00:27:16:1d:52
  type     = 0x800
###[ IP ]###
  version  = 4
  ihl      = 5
  tos      = 0x0
  len      = 84
  id       = 11031
  flags    = DF
  frag     = 0
  ttl      = 64
  proto    = icmp
  chksum   = 0xf379
  src      = 10.0.2.9
  dst      = 8.8.8.8
  \options \
###[ ICMP ]###
  type     = echo-request
  code     = 0
  chksum   = 0xf624
  id       = 0x9ce
  seq      = 0x1
###[ Raw ]###
  Load    = '\xf5IGa\xc7\t\x00\x08\t\n\x0b\x0c\r\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"%&'()*+,-./01234567'
###[ Ethernet ]###
  dst      = 08:00:27:16:1d:52
  src      = 52:54:00:12:35:00
  type     = 0x800
###[ IP ]###
  version  = 4
  ihl      = 5
  tos      = 0x18
  len      = 84
  id       = 427
  flags    =
  frag     = 0
  ttl      = 115
  proto    = icmp
  chksum   = 0x29ce
  src      = 8.8.8.8
  dst      = 10.0.2.9
  \options \
###[ ICMP ]###
  type     = echo-reply
  code     = 0
  chksum   = 0xfe24
  id       = 0x9ce
  seq      = 0x1
###[ Raw ]###
  Load    = '\xf5IGa\xc7\t\x00\x08\t\n\x0b\x0c\r\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"%&'()*+,-./01234567'
###[ Ethernet ]###
  dst      = 52:54:00:12:35:00
  src      = 08:00:27:16:1d:52
  type     = 0x800
###[ IP ]###
  version  = 4
  ihl      = 5
  tos      = 0x0
  len      = 84
  id       = 11220
  flags    = DF
  frag     = 0
  ttl      = 64
  proto    = icmp
  chksum   = 0xf2bc
  src      = 10.0.2.9
  dst      = 8.8.8.8
  \options \
###[ ICMP ]###
  type     = echo-request
  code     = 0
  chksum   = 0x461e
  id       = 0x9ce
  seq      = 0x2
###[ Raw ]###
  Load    = '\xf6IGavc\t\x00\x08\t\n\x0b\x0c\r\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"%&'()*+,-./01234567'
###[ Ethernet ]###
  dst      = 08:00:27:16:1d:52
  src      = 52:54:00:12:35:00
  type     = 0x800
###[ IP ]###
  version  = 4
  ihl      = 5
  tos      = 0x18
```


Observation on victim machine while ping 8.8.8.8

```
Terminal
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:16:1d:52
        inet addr:10.0.2.9  Bcast:10.0.2.255  Mask:255.255.255.0
        inet6 addr: fe80::61b0:fc40:57c2:e0/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:11 errors:0 dropped:0 overruns:0 frame:0
        TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:1641 (1.6 KB)  TX bytes:7992 (7.9 KB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:72 errors:0 dropped:0 overruns:0 frame:0
        TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:21652 (21.6 KB)  TX bytes:21652 (21.6 KB)

[09/19/21]seed@Nikhil_PES1UG20CS821:~$ ping 10.0.2.8
PING 10.0.2.8 (10.0.2.8) 56(84) bytes of data.
 64 bytes from 10.0.2.8: icmp_seq=1 ttl=64 time=0.481 ms
 64 bytes from 10.0.2.8: icmp_seq=2 ttl=64 time=0.869 ms
 64 bytes from 10.0.2.8: icmp_seq=3 ttl=64 time=0.883 ms
 64 bytes from 10.0.2.8: icmp_seq=4 ttl=64 time=0.301 ms
^Z
[1]+  Stopped                  ping 10.0.2.8
[09/19/21]seed@Nikhil_PES1UG20CS821:~$ 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=115 time=9.10 ms
 64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=9.02 ms
 64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=10.0 ms
 64 bytes from 8.8.8.8: icmp_seq=4 ttl=115 time=8.95 ms
^Z
[2]+  Stopped                  ping 8.8.8.8
[09/19/21]seed@Nikhil_PES1UG20CS821:~$
```

While running the same program on the attacker machine along with pinging 8.8.8.8 on the same virtual machine in another terminal, we can identify those two with the help of source IP address and Mac address.

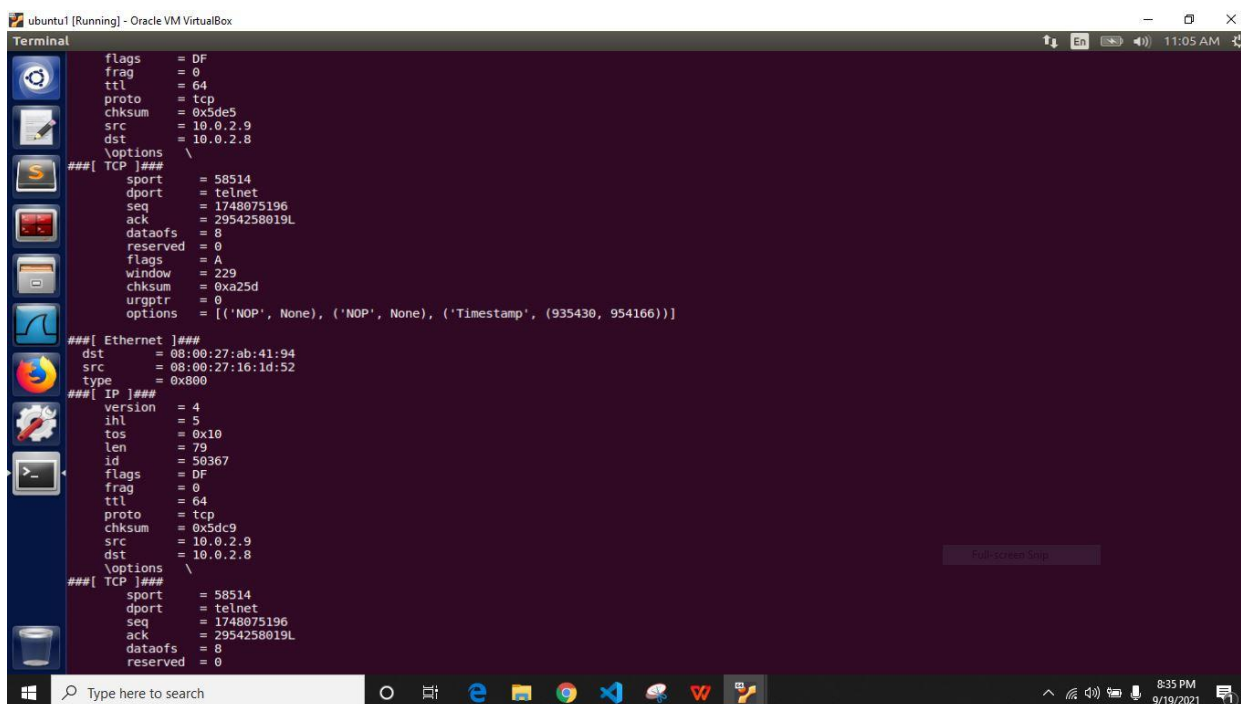
```
Terminal
[09/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo python sample.py
SNIFFING PACKETS...
###[ Ethernet ]###
  dst      = 52:54:00:12:35:00
  src      = 08:00:27:ab:41:94
  type     = 0x800
###[ IP ]###
  version  = 4
  ihl      = 5
  tos      = 0x0
  len      = 84
  id       = 31197
  flags    = DF
  frag     = 0
  ttl      = 64
  proto    = icmp
  checksum = 0xa4b4
  src      = 10.0.2.8
  dst      = 8.8.8.8
  \options \
###[ ICMP ]###
  type     = echo-request
  code     = 0
  checksum = 0x4d49
  id       = 0xd7b
  seq      = 0x1
###[ Raw ]###
  Load    = '\x0a\x00\x0b\x01\x00\x08\t\n\x0b\x0c\r\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#%&\'()*+,-./01234567'
###[ Ethernet ]###
  dst      = 08:00:27:ab:41:94
  src      = 52:54:00:12:35:00
  type     = 0x800
###[ IP ]###
  version  = 4
  ihl      = 5
  tos      = 0x18
  len      = 84
  id       = 431
  flags    =
  frag     = 0
  ttl      = 115
  proto    = icmp
  checksum = 0x29cb
  src      = 8.8.8.8
  dst      = 10.0.2.8
```

```
ubuntu1 [Running] - Oracle VM VirtualBox
Terminal
dst = 10.0.2.8
\options
###[ ICMP ]###
type = echo-reply
code = 0
chksum = 0x5549
id = 0xd7b
seq = 0x1
###[ Raw ]###
Load = 'iKGa\x00\x8b\x01\x00\x08\t\n\x0b\x0c\r\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#%&\'()*+,-./01234567'
###[ Ethernet ]###
dst = 52:54:00:12:35:00
src = 08:00:27:ab:41:94
type = 0x800
###[ IP ]###
version = 4
ihl = 5
tos = 0x0
len = 84
id = 31304
flags = DF
frag = 0
ttl = 64
proto = icmp
chksum = 0xa449
src = 10.0.2.8
dst = 8.8.8.8
\options
###[ ICMP ]###
type = echo-request
code = 0
chksum = 0xae40
id = 0xd7b
seq = 0x2
###[ Raw ]###
Load = 'jKGa\x9e\x92\x01\x00\x08\t\n\x0b\x0c\r\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#%&\'()*+,-./01234567'
###[ Ethernet ]###
dst = 08:00:27:ab:41:94
src = 52:54:00:12:35:00
type = 0x800
###[ IP ]###
version = 4
ihl = 5
tos = 0x18
```

Task 1.2.2 Capture any TCP packet that comes from a particular IP and with a destination port number 23.

Observation on attacker machine

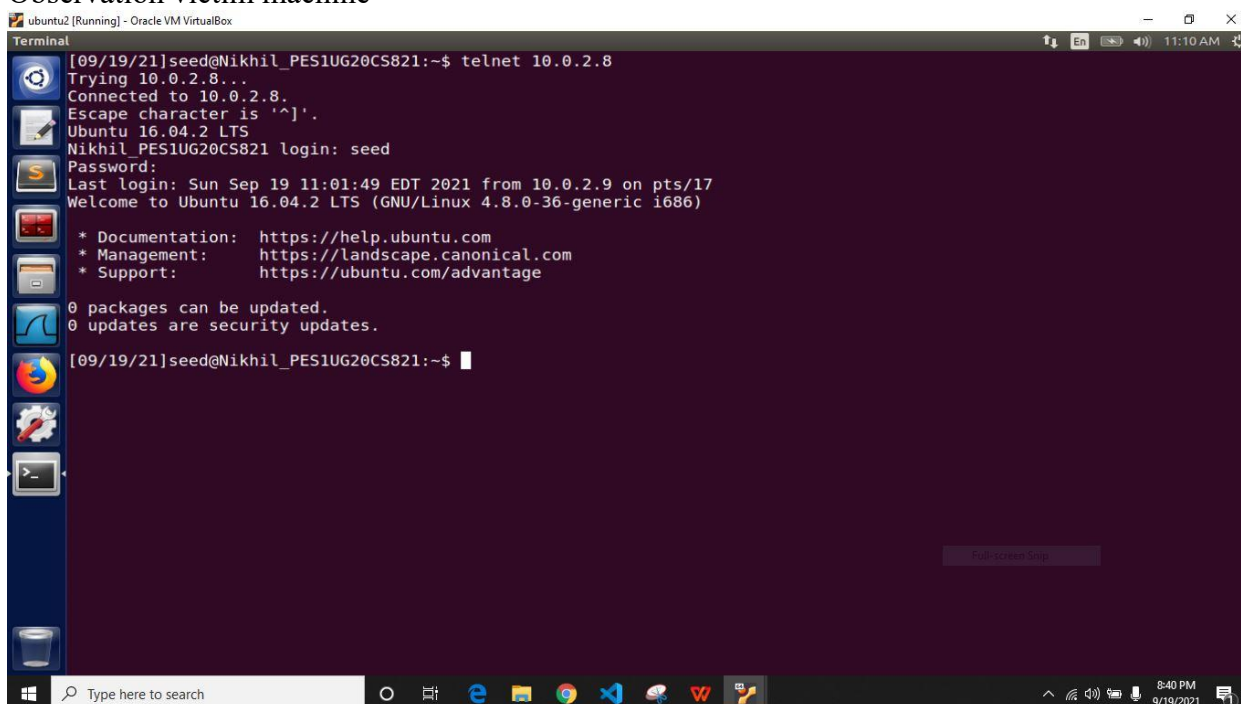
```
ubuntu1 [Running] - Oracle VM VirtualBox
Terminal
[09/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo python sniff.py
SNIFFING PACKETS...
###[ Ethernet ]###
dst = 08:00:27:ab:41:94
src = 08:00:27:16:1d:52
type = 0x800
###[ IP ]###
version = 4
ihl = 5
tos = 0x10
len = 60
id = 50365
flags = DF
frag = 0
ttl = 64
proto = tcp
chksum = 0x5dde
src = 10.0.2.9
dst = 10.0.2.8
\options
###[ TCP ]###
sport = 58514
dport = telnet
seq = 1748075195
ack = 0
dataofs = 10
reserved = 0
flags = S
window = 29200
chksum = 0xa834
urgptr = 0
options = [('MSS', 1460), ('SACKOK', ''), ('Timestamp', (935430, 0)), ('NOP', None), ('WScale', 7)]
###[ Ethernet ]###
dst = 08:00:27:ab:41:94
src = 08:00:27:16:1d:52
type = 0x800
###[ IP ]###
version = 4
ihl = 5
tos = 0x10
len = 52
id = 50366
flags = DF
frag = 0
ttl = 64
```



```
ubuntu1 [Running] - Oracle VM VirtualBox
Terminal
flags      = DF
frag       = 0
ttl        = 64
proto      = tcp
chksum     = 0x5de5
src        = 10.0.2.9
dst        = 10.0.2.8
\options
###[ TCP ]###
sport      = 58514
dport      = telnet
seq        = 1748075196
ack        = 2954258019L
dataoffs   = 8
reserved   = 0
flags      = A
window     = 229
chksum     = 0xa25d
urgptr     = 0
options    = [('NOP', None), ('NOP', None), ('Timestamp', (935430, 954166))]
```

```
###[ Ethernet ]###
dst        = 08:00:27:ab:41:94
src        = 08:00:27:10:1d:52
type       = 0x800
###[ IP ]###
version    = 4
ihl        = 5
tos        = 0x10
len        = 79
id         = 50367
flags      = DF
frag       = 0
ttl        = 64
proto      = tcp
chksum     = 0x5dc9
src        = 10.0.2.9
dst        = 10.0.2.8
\options
###[ TCP ]###
sport      = 58514
dport      = telnet
seq        = 1748075196
ack        = 2954258019L
dataoffs   = 8
reserved   = 0
```

Observation victim machine



```
ubuntu2 [Running] - Oracle VM VirtualBox
Terminal
[09/19/21]seed@Nikhil_PES1UG20CS821:~$ telnet 10.0.2.8
Trying 10.0.2.8...
Connected to 10.0.2.8.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
Nikhil_PES1UG20CS821 login: seed
Password:
Last login: Sun Sep 19 11:01:49 EDT 2021 from 10.0.2.9 on pts/17
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

[09/19/21]seed@Nikhil_PES1UG20CS821:~$
```

We run the telnet on the victim machine because Telnet is a computer protocol that provides two-way interactive communication compatibility for computers on the internet and local area networks. here we achieve this by using telnet on victim machine to get connect with the attacker machine.

Task 1.2.3 Capture packets comes from or to go to a particular subnet

Observation on attacker machine

```
Terminal
[09/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo python sniff1.py
SNIFFING PACKETS...
###[ Ethernet ]###
  dst      = 08:00:27:16:1d:52
  src      = 52:54:00:12:35:00
  type     = 0x800
###[ IP ]###
  version  = 4
  ihl      = 5
  tos      = 0x0
  len      = 84
  id       = 12
  flags    =
  frag     = 0
  ttl      = 61
  proto    = icmp
  chksum   = 0xb2ea
  src      = 192.168.254.1
  dst      = 10.0.2.9
  \options \
###[ ICMP ]###
  type     = echo-reply
  code     = 0
  chksum   = 0xe2cb
  id       = 0x947
  seq      = 0x1
###[ Raw ]###
  load     = 'i\xfcGak\x8b\x0c\x00\x08\t\n\x0b\x0c\r\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#%&'()*+,-./01234567'
###[ Ethernet ]###
  dst      = 08:00:27:16:1d:52
  src      = 52:54:00:12:35:00
  type     = 0x800
###[ IP ]###
```

```
Terminal
###[ IP ]###
  version  = 4
  ihl      = 5
  tos      = 0x0
  len      = 84
  id       = 13
  flags    =
  frag     = 0
  ttl      = 61
  proto    = icmp
  chksum   = 0xb2e9
  src      = 192.168.254.1
  dst      = 10.0.2.9
  \options \
###[ ICMP ]###
  type     = echo-reply
  code     = 0
  chksum   = 0xaabf
  id       = 0x947
  seq      = 0x2
###[ Raw ]###
  load     = 'j\xfcGa\xa2\x96\x0c\x00\x08\t\n\x0b\x0c\r\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#%&'()*+,-./01234567'
###[ Ethernet ]###
  dst      = 08:00:27:16:1d:52
  src      = 52:54:00:12:35:00
  type     = 0x800
###[ IP ]###
  version  = 4
  ihl      = 5
  tos      = 0x0
  len      = 84
  id       = 14
  flags    =
```



```
ubuntu1 [Running] - Oracle VM VirtualBox
Terminal
###[ Raw ]###
load = 'j\xfcGa\xa2\x96\x0c\x08\t\n\x0b\x0c\r\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#%&\'()*+,-./01234567'
###[ Ethernet ]###
dst = 08:00:27:16:1d:52
src = 52:54:00:12:35:00
type = 0x800
###[ IP ]###
version = 4
ihl = 5
tos = 0x0
len = 84
id = 14
flags =
frag = 0
ttl = 61
proto = icmp
chksum = 0xb2e8
src = 192.168.254.1
dst = 10.0.2.9
\options \
###[ ICMP ]###
type = echo-reply
code = 0
chksum = 0x2db7
id = 0x947
seq = 0x3
###[ Raw ]###
load = 'k\xfcGa\x1e\x9e\x0c\x08\t\n\x0b\x0c\r\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#%&\'()*+,-./01234567'
^Z
[1]+  Stopped                  sudo python sniff1.py
[09/19/21]seed@Nikhil_PES1UG20CS821:~$
```

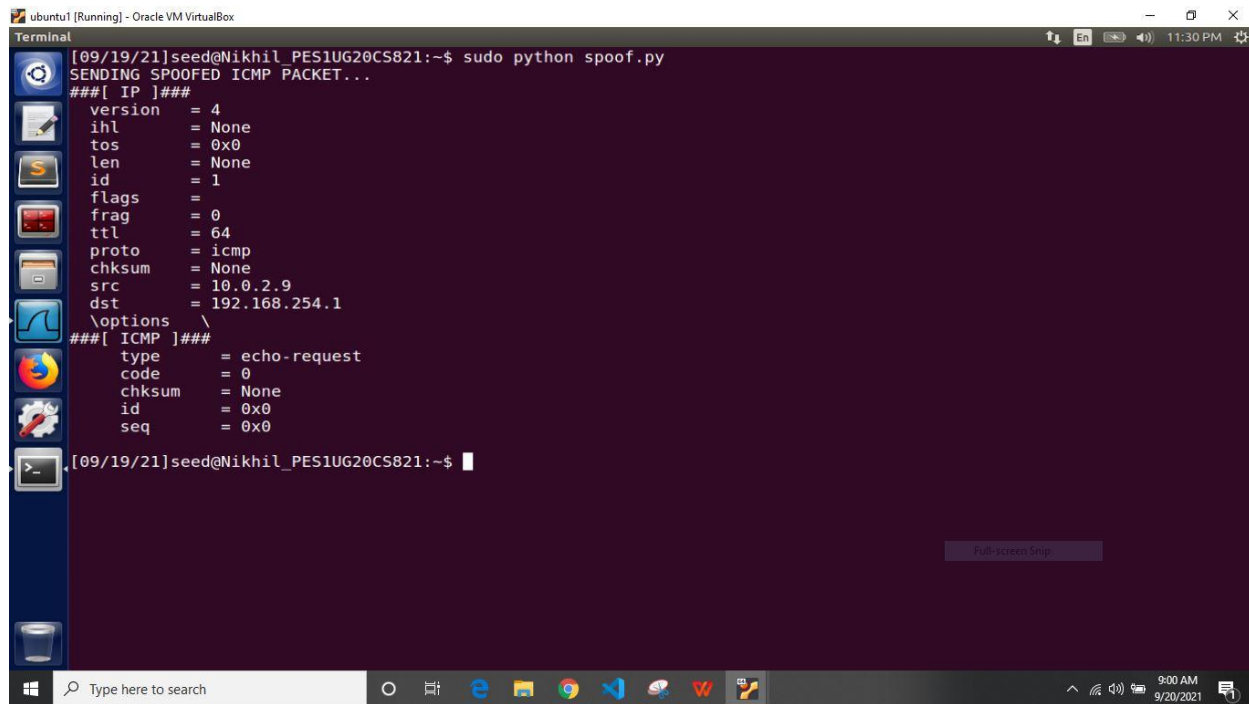
Observation on victim machine

```
ubuntu2 [Running] - Oracle VM VirtualBox
Terminal
[09/19/21]seed@Nikhil_PES1UG20CS821:~$ ping 192.168.254.1
PING 192.168.254.1 (192.168.254.1) 56(84) bytes of data:
64 bytes from 192.168.254.1: icmp_seq=1 ttl=61 time=2.50 ms
64 bytes from 192.168.254.1: icmp_seq=2 ttl=61 time=3.92 ms
64 bytes from 192.168.254.1: icmp_seq=3 ttl=61 time=29.6 ms
^Z
[2]+  Stopped                  ping 192.168.254.1
[09/19/21]seed@Nikhil_PES1UG20CS821:~$
```

In this task the packets are sniffed from the particular subnet 192.168.254.0/24. Whenever the victim try to access the IP address from 192.168.254.0 to 192.168.254.24 those packets are sniffed from the attacker.

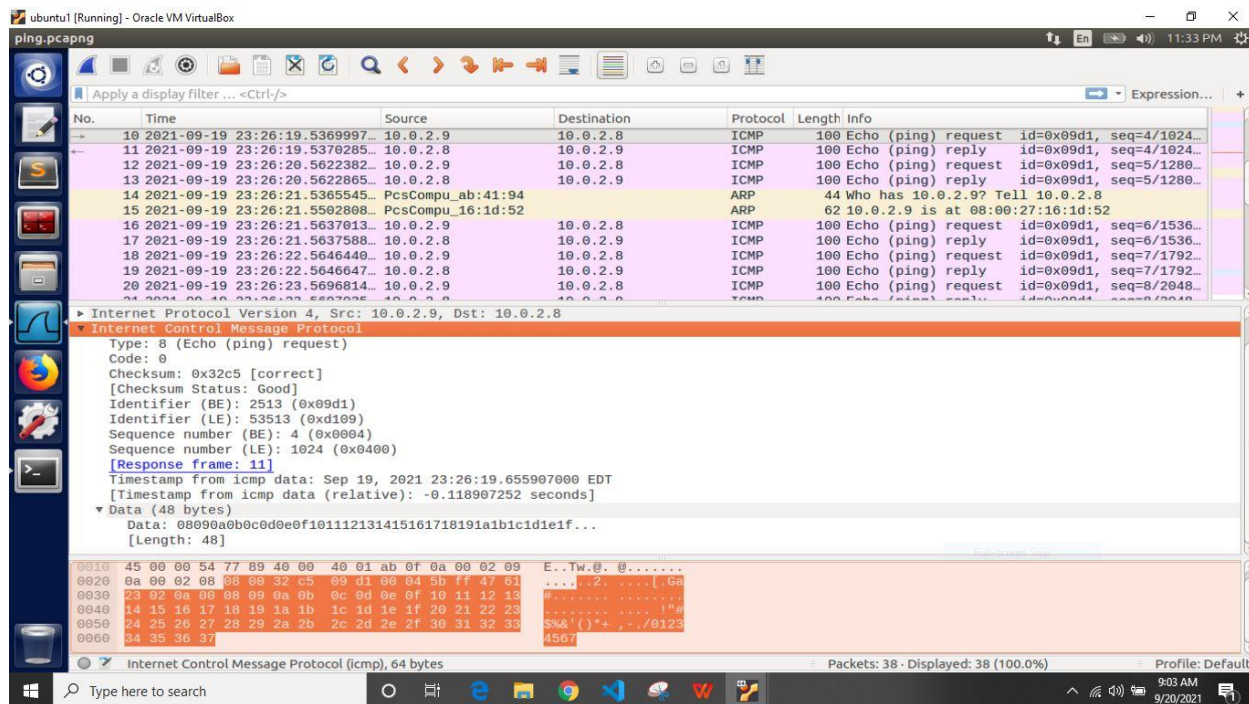
Task 2: Spoofing

Observation on attacker machine



```
ubuntu1 [Running] - Oracle VM VirtualBox
Terminal
[09/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo python spoof.py
SENDING SPOOFED ICMP PACKET...
###[ IP ]###
version      = 4
ihl          = None
tos          = 0x0
len          = None
id           = 1
flags        =
frag         = 0
ttl          = 64
proto        = icmp
chksum       = None
src          = 10.0.2.9
dst          = 192.168.254.1
\options     \
###[ ICMP ]###
type         = echo-request
code         = 0
chksum       = None
id           = 0x0
seq          = 0x0
[09/19/21]seed@Nikhil_PES1UG20CS821:~$
```

Observation on wireshark



ping.pcapng

No.	Time	Source	Destination	Protocol	Length	Info
10	2021-09-19 23:26:19.5369997	10.0.2.9	10.0.2.8	ICMP	100	Echo (ping) request id=0x09d1, seq=4/1024...
11	2021-09-19 23:26:19.5370285	10.0.2.8	10.0.2.9	ICMP	100	Echo (ping) reply id=0x09d1, seq=4/1024...
12	2021-09-19 23:26:20.5622382	10.0.2.9	10.0.2.8	ICMP	100	Echo (ping) request id=0x09d1, seq=5/1280...
13	2021-09-19 23:26:20.5622865	10.0.2.8	10.0.2.9	ICMP	100	Echo (ping) reply id=0x09d1, seq=5/1280...
14	2021-09-19 23:26:21.5365545	PcsCompu_ab:41:94		ARP	44	Who has 10.0.2.9? Tell 10.0.2.8
15	2021-09-19 23:26:21.5502808	PcsCompu_16:1d:52		ARP	62	10.0.2.9 is at 08:00:27:16:1d:52
16	2021-09-19 23:26:21.5637013	10.0.2.9	10.0.2.8	ICMP	100	Echo (ping) request id=0x09d1, seq=6/1536...
17	2021-09-19 23:26:21.5637588	10.0.2.8	10.0.2.9	ICMP	100	Echo (ping) reply id=0x09d1, seq=6/1536...
18	2021-09-19 23:26:22.5646440	10.0.2.9	10.0.2.8	ICMP	100	Echo (ping) request id=0x09d1, seq=7/1792...
19	2021-09-19 23:26:22.5646647	10.0.2.8	10.0.2.9	ICMP	100	Echo (ping) reply id=0x09d1, seq=7/1792...
20	2021-09-19 23:26:23.5696814	10.0.2.9	10.0.2.8	ICMP	100	Echo (ping) request id=0x09d1, seq=8/2048...

Internet Protocol Version 4, Src: 10.0.2.9, Dst: 10.0.2.8

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x32c5 [correct]

[Checksum Status: Good]

Identifier (BE): 2513 (0x09d1)

Identifier (LE): 53513 (0xd109)

Sequence number (BE): 4 (0x0004)

Sequence number (LE): 1024 (0x0400)

[Response frame: 11]

Timestamp from icmp data: Sep 19, 2021 23:26:19.655907000 EDT

[Timestamp from icmp data (relative): -0.118907252 seconds]

Data (48 bytes)

Data: 00090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f...

[Length: 48]

0010 45 00 00 54 77 89 40 00 40 01 ab 0f 0a 00 02 09 E..Tw.0. @.....

0020 0a 00 02 08 38 00 32 c5 09 d1 09 04 5b ff 47 012.[Ga

0030 23 02 0a 00 08 09 0a 0b 0e 0d 0e 0f 10 11 12 13

0040 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23

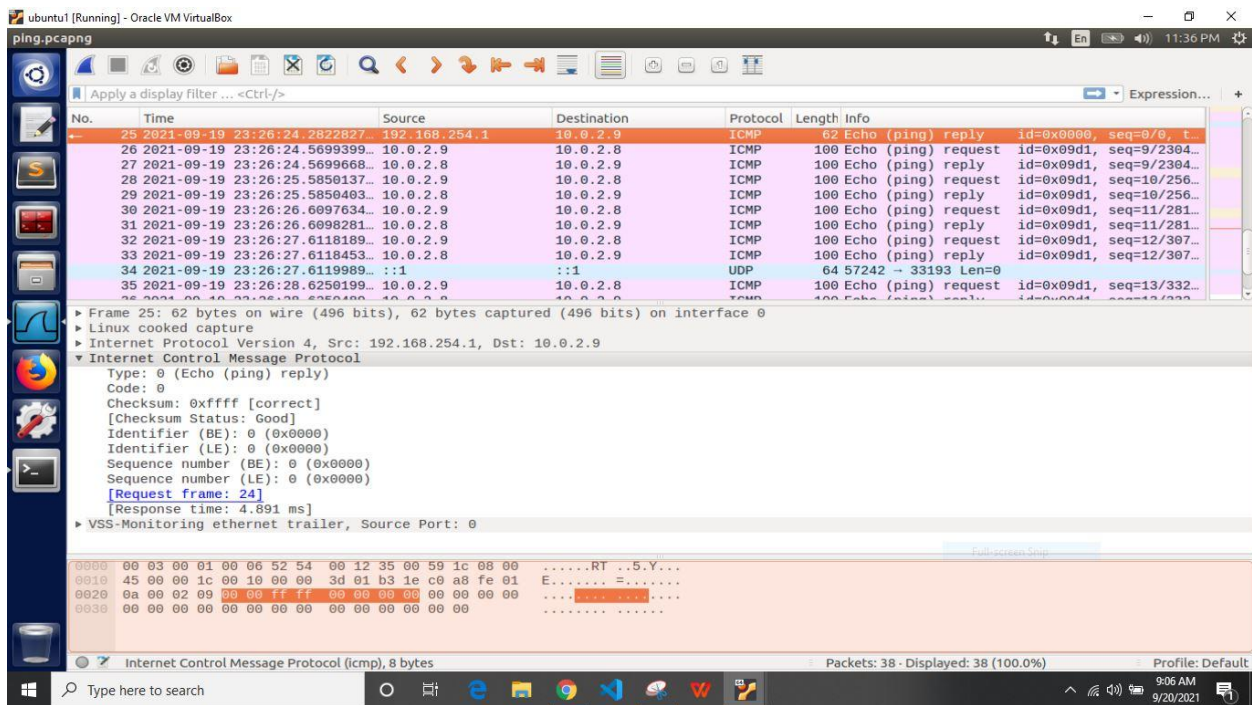
0050 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 \$%&'()*+,.../0123

0060 34 35 36 37 4567

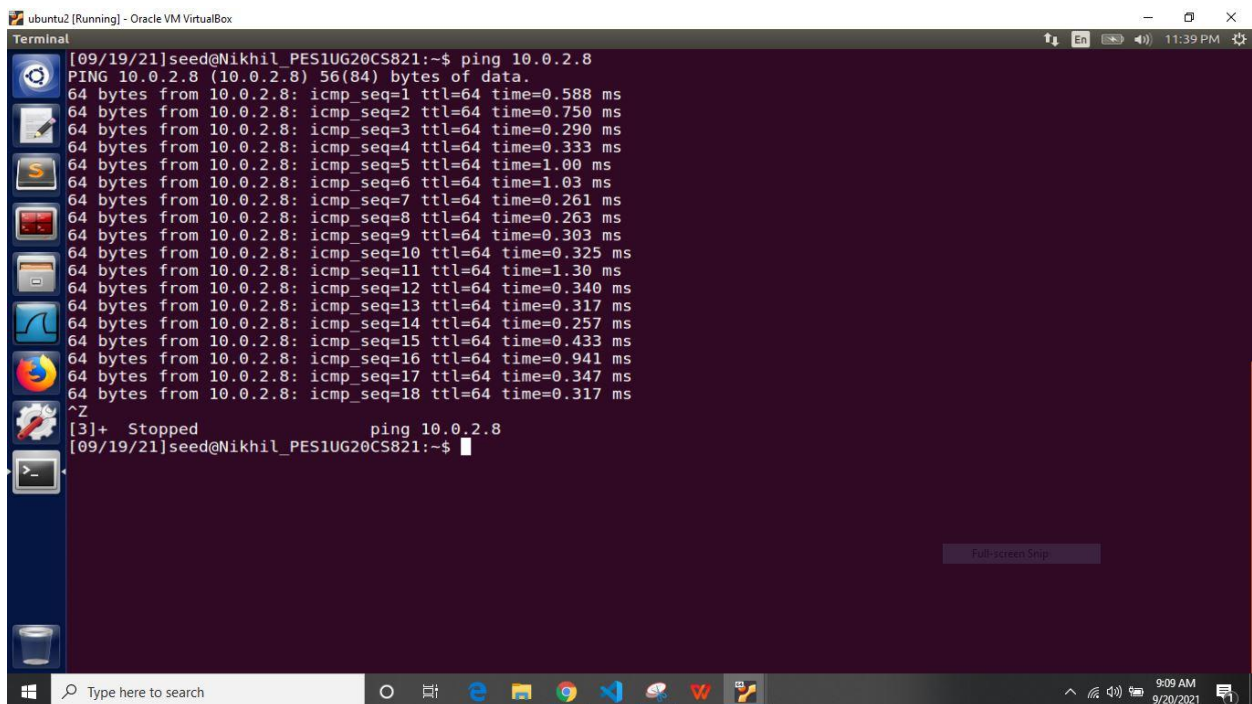
Internet Control Message Protocol (icmp), 64 bytes

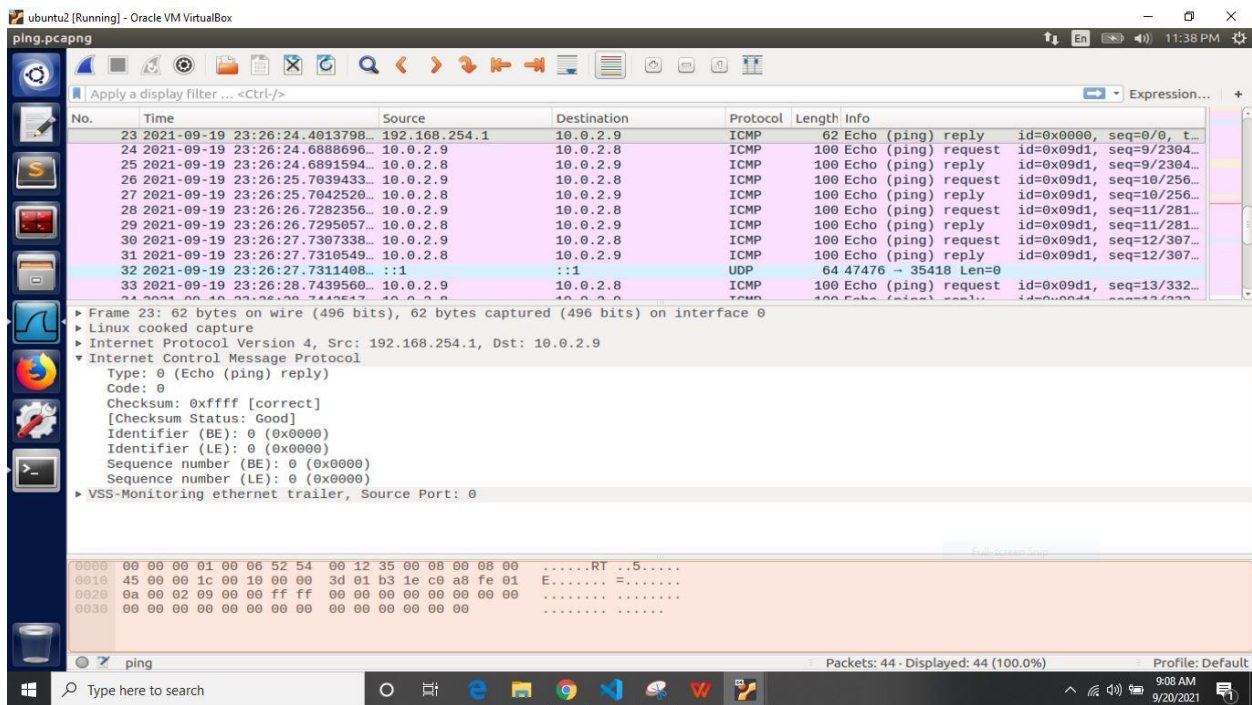
Packets: 38 · Displayed: 38 (100.0%)

Profile: Default



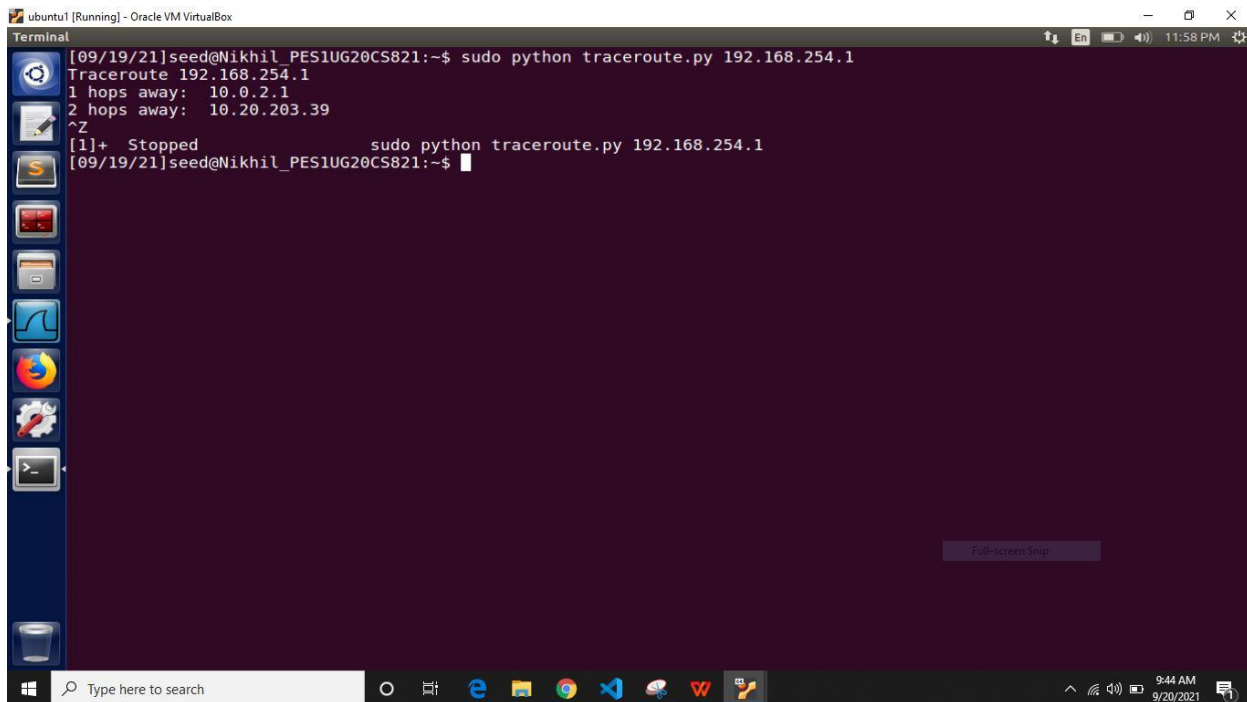
Observation on victim machine





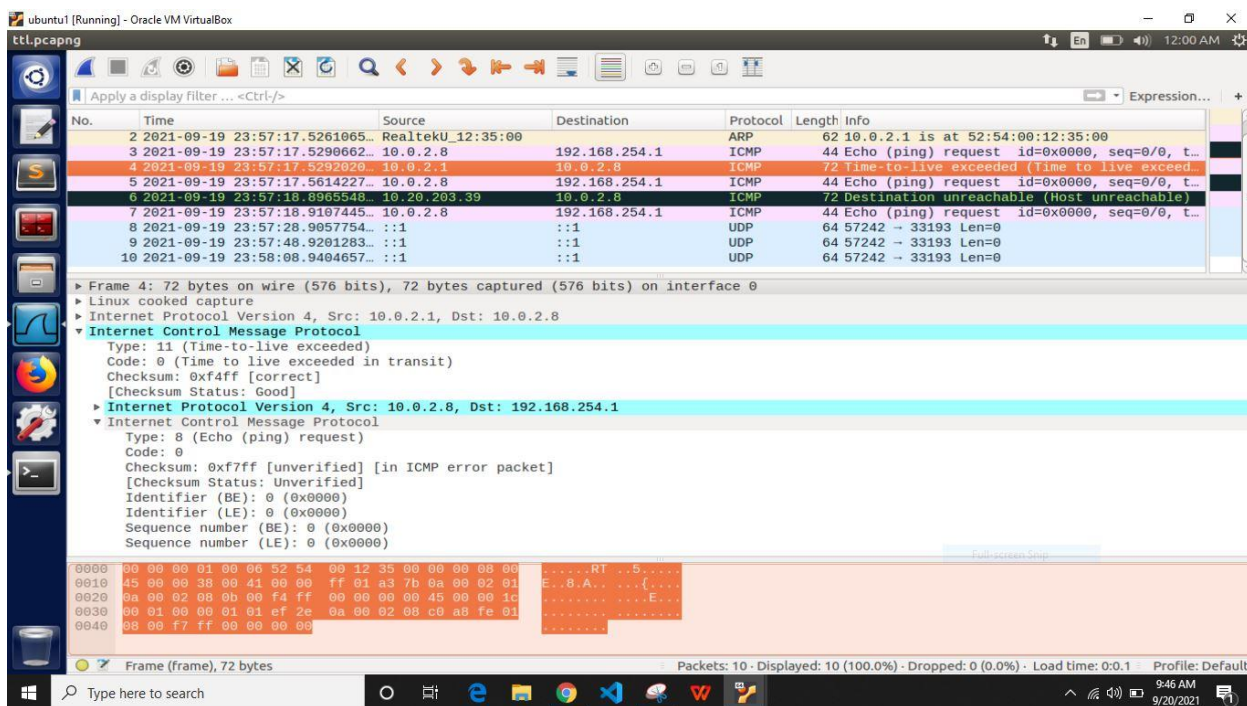
In this task the user is going to ping the attacker machine (10.0.2.8) then the user spoofs the packets and sends the packets to the IP address 192.168.254.1 with the victim IP address then the victim gets the reply from the IP address 192.168.254.1 even though he pinged 10.0.2.8.

Task 3: Traceroute



The terminal window shows the execution of the traceroute command. The user runs `sudo python traceroute.py 192.168.254.1`. The output shows the path taken by the packet, including the source IP and the destination IP. The command is then stopped using `Ctrl+C`.

```
[09/19/21]seed@Nikhil_PES1UG20CS821:~$ sudo python traceroute.py 192.168.254.1
Traceroute 192.168.254.1
1 hops away: 10.0.2.1
2 hops away: 10.20.203.39
^Z
[1]+  Stopped                  sudo python traceroute.py 192.168.254.1
[09/19/21]seed@Nikhil_PES1UG20CS821:~$
```



The Wireshark packet capture shows the traceroute results. The table below summarizes the captured packets, highlighting the ICMP error messages received from the destination.

No.	Time	Source	Destination	Protocol	Length	Info
2	2021-09-19 23:57:17.5261065	RealtekU_12:35:00	10.0.2.8	ARP	62	10.0.2.1 is at 52:54:00:12:35:00
3	2021-09-19 23:57:17.5290662	10.0.2.8	192.168.254.1	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, t...
4	2021-09-19 23:57:17.5292020	10.0.2.1	10.0.2.8	ICMP	72	Time-to-live exceeded (Time to live exceed...
5	2021-09-19 23:57:17.5614227	10.0.2.8	192.168.254.1	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, t...
6	2021-09-19 23:57:18.8965548	10.20.203.39	10.0.2.8	ICMP	72	Destination unreachable (Host unreachable)
7	2021-09-19 23:57:18.9107445	10.0.2.8	192.168.254.1	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, t...
8	2021-09-19 23:57:28.9057754	:::1	:::1	UDP	64	57242 → 33193 Len=0
9	2021-09-19 23:57:48.9201283	:::1	:::1	UDP	64	57242 → 33193 Len=0
10	2021-09-19 23:58:08.9404657	:::1	:::1	UDP	64	57242 → 33193 Len=0

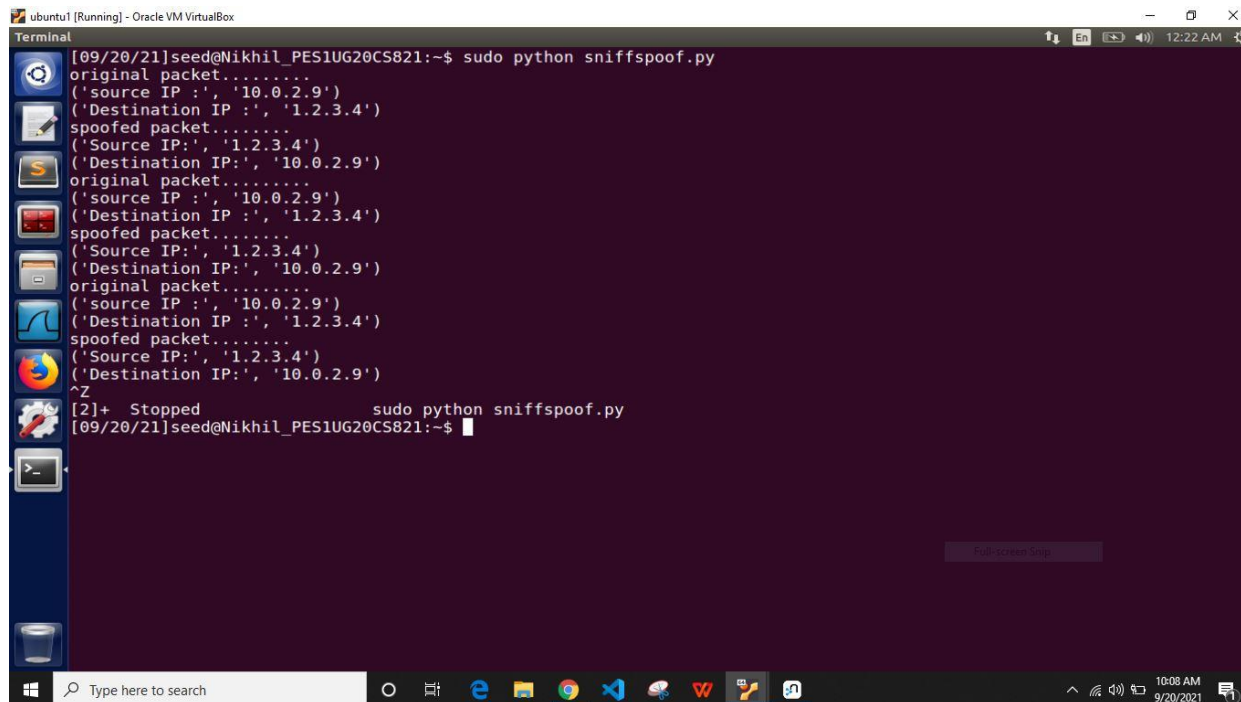
The detailed view of the selected packet (Frame 4) shows the ICMP error message details:

- Internet Protocol Version 4, Src: 10.0.2.1, Dst: 10.0.2.8
- Internet Control Message Protocol
 - Type: 11 (Time-to-live exceeded)
 - Code: 0 (Time to live exceeded in transit)
 - Checksum: 0xf4ff [correct]
 - Checksum Status: Good
- Internet Protocol Version 4, Src: 10.0.2.8, Dst: 192.168.254.1
- Internet Control Message Protocol
 - Type: 8 (Echo (ping) request)
 - Code: 0
 - Checksum: 0xf7ff [unverified] [in ICMP error packet]
 - Checksum Status: Unverified
 - Identifier (BE): 0 (0x0000)
 - Identifier (LE): 0 (0x0000)
 - Sequence number (BE): 0 (0x0000)
 - Sequence number (LE): 0 (0x0000)

in this task we will do traceroute which is used to find the hops that the packet goes through in the network. We increase the ttl (time to live) value of the packets at last the error response form the router is obtained which shows Time to live exceed.

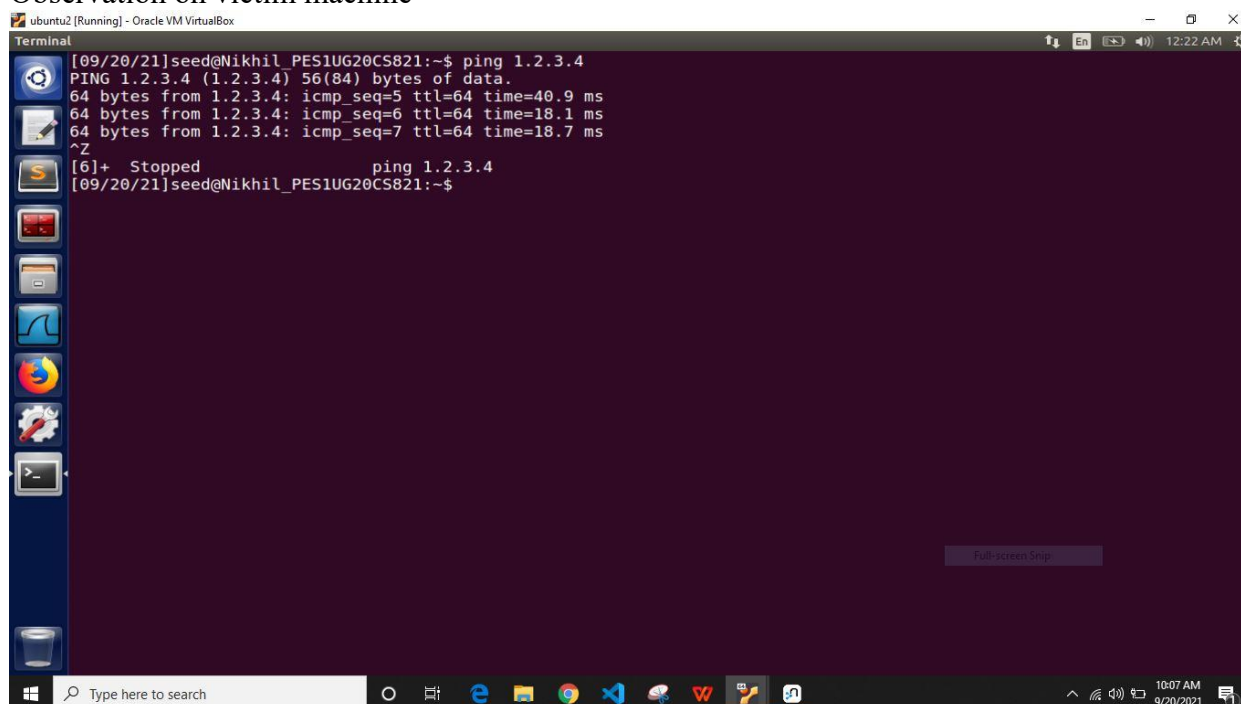
Task 4: Sniffing and-then Spoofing

Observation on attacker machine



```
Terminal
[09/20/21]seed@Nikhil_PES1UG20CS821:~$ sudo python sniffspoof.py
original packet.....
('source IP :', '10.0.2.9')
('Destination IP :', '1.2.3.4')
spoofed packet.....
('Source IP:', '1.2.3.4')
('Destination IP:', '10.0.2.9')
original packet.....
('source IP :', '10.0.2.9')
('Destination IP :', '1.2.3.4')
spoofed packet.....
('Source IP:', '1.2.3.4')
('Destination IP:', '10.0.2.9')
original packet.....
('source IP :', '10.0.2.9')
('Destination IP :', '1.2.3.4')
spoofed packet.....
('Source IP:', '1.2.3.4')
('Destination IP:', '10.0.2.9')
^Z
[2]+  Stopped                  sudo python sniffspoof.py
[09/20/21]seed@Nikhil_PES1UG20CS821:~$
```

Observation on victim machine



```
Terminal
[09/20/21]seed@Nikhil_PES1UG20CS821:~$ ping 1.2.3.4
PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
64 bytes from 1.2.3.4: icmp_seq=5 ttl=64 time=40.9 ms
64 bytes from 1.2.3.4: icmp_seq=6 ttl=64 time=18.1 ms
64 bytes from 1.2.3.4: icmp_seq=7 ttl=64 time=18.7 ms
^Z
[6]+  Stopped                  ping 1.2.3.4
[09/20/21]seed@Nikhil_PES1UG20CS821:~$
```

In this task both sniffing and spoofing are done by the attacker. The victim is going to ping the non existing IP address 1.2.3.4 but the victim will get the response this is done by the attacker. The attacker will sniff the packets and spoof it but the victim doesn't get to know that he is getting response from the attacker instead of machine having IP address 1.2.3.4. when the same IP address is pinged from the same machine it results in no response.