CNS LAB 1

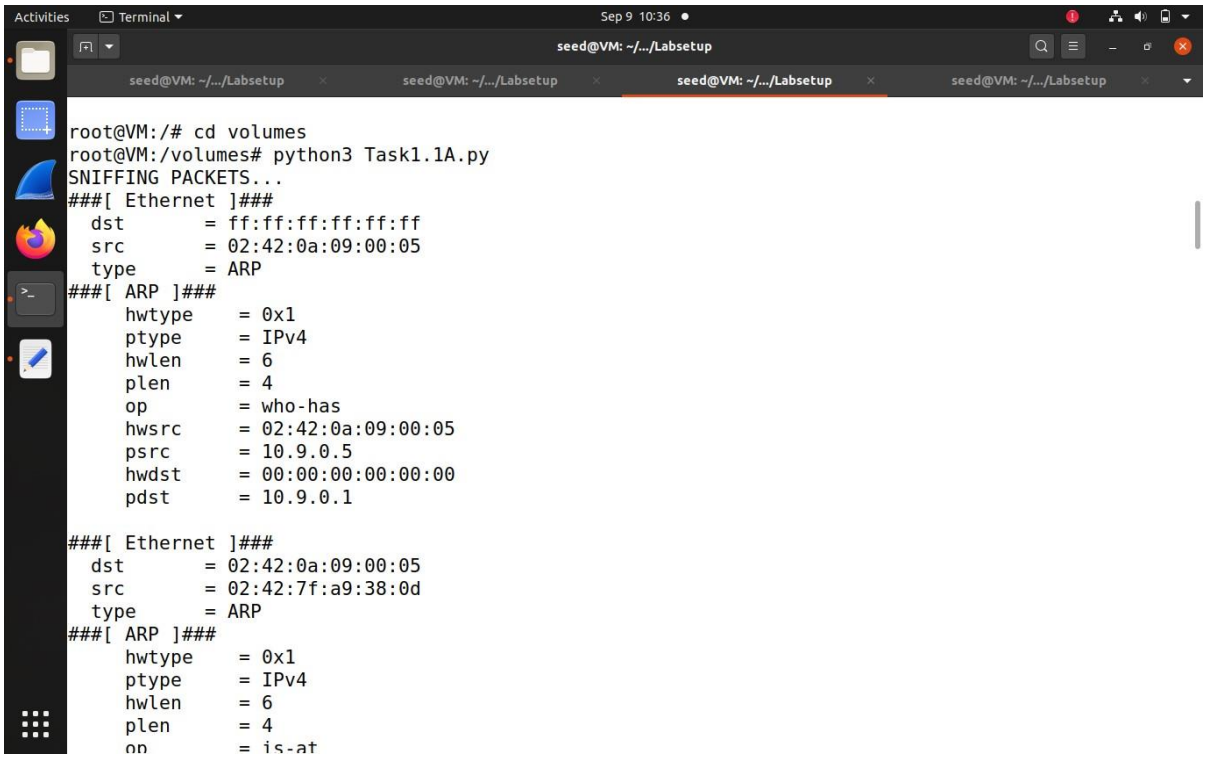
NAME: NAVYA PERAM

SEC: F

SRN: PES1UG21CS924

TASK 1.1 A

The host sent and received packets in this process. The attacker system was able to sniff the packets sent and received by the hostA and was able to extract the information. The show() function printed the layers and fields of the packets sent and received. The packets in the br interface were captured and the print_pkt callback function is called.



```
seed-attacker:PES1UG21CS924:Navya:/volumes
$>python3 Task1.1A.py
SNIFFING PACKETS...
###[ Ethernet ]###
  dst       = ff:ff:ff:ff:ff:ff
  src       = 02:42:0a:09:00:05
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = 6
     plen      = 4
     op        = who-has
     hwsrc     = 02:42:0a:09:00:05
     psrc      = 10.9.0.5
     hwdst     = 00:00:00:00:00:00
     pdst      = 10.9.0.1

###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:9f:11:cd:26
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = 6
     plen      = 4
     op        = is-at
     hwsrc     = 02:42:9f:11:cd:26
     psrc      = 10.9.0.1
     hwdst     = 02:42:0a:09:00:05
     pdst      = 10.9.0.5
```

```
###[ Ethernet ]###
  dst       = 02:42:9f:11:cd:26
  src       = 02:42:0a:09:00:05
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 17604
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = icmp
     chksum    = 0xdbc7
     src       = 10.9.0.5
     dst       = 8.8.8.8
     \options   \
###[ ICMP ]###
        type      = echo-request
        code      = 0
        chksum    = 0xb2bc
        id        = 0x1d
        seq       = 0x1
###[ Raw ]###
           load      = '\xc2\x90\xfcd\x00\x00\x00\x00\xc2\\\x05\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x
1e\x1f !"#$%&\'()*+,-./01234567'

###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:9f:11:cd:26
```

```
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

hostA:PES1UG21CS924:Navya:/
$>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=31.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=27.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=28.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=115 time=27.3 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=115 time=28.3 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=115 time=28.6 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=115 time=27.0 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=115 time=35.7 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=115 time=51.2 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=115 time=28.8 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=115 time=27.5 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=115 time=29.2 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=115 time=35.8 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=115 time=39.7 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=115 time=32.2 ms
^C64 bytes from 8.8.8.8: icmp_seq=16 ttl=115 time=30.2 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=115 time=29.8 ms
^C
--- 8.8.8.8 ping statistics ---
17 packets transmitted, 17 received, 0% packet loss, time 16090ms
rtt min/avg/max/mdev = 26.955/31.696/51.224/5.966 ms
hostA:PES1UG21CS924:Navya:/
$>
```

In this process, the root privileges were removed. Without root privileges the packets cannot be captured due to the privacy and security risks. To be able to prevent unauthorized users from flooding the network with malicious programs or packets, we need use root privileges. Unless we do so, the program won't be able to access a raw socket or put the interface in a promiscuous mode. Hence in the given process, the operation was not permitted.

```
a: E501
  File "/usr/lib/python3.8/socket.py", line 231, in __init__
    _socket.socket.__init__(self, family, type, proto, fileno)
PermissionError: [Errno 1] Operation not permitted
seed@VM:/volumes$ su seed
Password:
seed@VM:/volumes$ python3 Task1.1A.py
SNIFFING PACKETS...
Traceback (most recent call last):
  File "Task1.1A.py", line 6, in <module>
    pkt = sniff(iface = "br-cefa40c1837f",prn=print_pkt)
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py", line 1036, in sniff
    sniffer._run(*args, **kwargs)
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py", line 906, in _run
    sniff_sockets[L2socket(type=ETH_P_ALL, iface=iface,
  File "/usr/local/lib/python3.8/dist-packages/scapy/arch/linux.py", line 398, in __init__
    self.ins = socket.socket(socket.AF_PACKET, socket.SOCK_RAW, socket.htons(type))  # noq
a: E501
  File "/usr/lib/python3.8/socket.py", line 231, in __init__
    _socket.socket.__init__(self, family, type, proto, fileno)
PermissionError: [Errno 1] Operation not permitted
seed@VM:/volumes$
```

TASK 1.1B

ICMP

We applied an ICMP filter in the given process, only the ICMP packets sent and received were captured. It is completely similar to the first process with the attacker sniffing the packets, but only specified to the ICMP ones.

```
###[ ICMP ]###
        type      = echo-reply
        code      = 0
        chksum    = 0x9d19
        id        = 0x1f
        seq       = 0x11
###[ Raw ]###
           load      = '\x84\x92\xfcd\x00\x00\x00\x00"\xec\x00\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1
e\x1f !"#$%&\'()*+,-./01234567'

^Cseed-attacker:PES1UG21CS924:Navya:/volumes
$>python3 Task1.1B-ICMP.py
SNIFFING PACKETS...
###[ Ethernet ]###
  dst       = 02:42:9f:11:cd:26
  src       = 02:42:0a:09:00:05
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 15
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = icmp
     chksum    = 0x207d
     src       = 10.9.0.5
     dst       = 8.8.8.8
     \options   \
###[ ICMP ]###
```

```
^Cseed-attacker:PES1UG21CS924:Navya:/volumes
$>python3 Task1.1B-ICMP.py
SNIFFING PACKETS...
###[ Ethernet ]###
  dst       = 02:42:9f:11:cd:26
  src       = 02:42:0a:09:00:05
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 15
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = icmp
     chksum    = 0x207d
     src       = 10.9.0.5
     dst       = 8.8.8.8
     \options   \
###[ ICMP ]###
        type      = echo-request
```

```
        type      = echo-request
        code      = 0
        chksum    = 0x5e96
        id        = 0x20
        seq       = 0x1
###[ Raw ]###
           load      = '\xe3\x95\xfcd\x00\x00\x00\x00\xf9z\x01\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1
e\x1f !"#$%&\'()*+,-./01234567'

###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:9f:11:cd:26
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x18
     len       = 84
     id        = 24552
     flags     =
     frag      = 0
     ttl       = 115
     proto     = icmp
     chksum    = 0xcd8b
     src       = 8.8.8.8
     dst       = 10.9.0.5
     \options   \
###[ ICMP ]###
        type      = echo-reply
        code      = 0
        chksum    = 0x6696
        id        = 0x20
```

```
64 bytes from 8.8.8.8: icmp_seq=9 ttl=115 time=27.7 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=115 time=93.0 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=115 time=28.4 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=115 time=27.9 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=115 time=27.4 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=115 time=25.9 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=115 time=28.5 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=115 time=30.2 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=115 time=28.9 ms
^C
--- 8.8.8.8 ping statistics ---
17 packets transmitted, 17 received, 0% packet loss, time 16046ms
rtt min/avg/max/mdev = 25.899/32.329/93.047/15.230 ms
hostA:PES1UG21CS924:Navya:/
$>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=26.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=27.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=26.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=115 time=27.3 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=115 time=26.4 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=115 time=43.2 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=115 time=123 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=115 time=59.1 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=115 time=26.6 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=115 time=27.2 ms
^C
--- 8.8.8.8 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9037ms
rtt min/avg/max/mdev = 26.007/41.296/122.609/28.975 ms
hostA:PES1UG21CS924:Navya:/
$>
```

TCP

Here, all the packets going from host A to Telnet(the destination port) on the attackers system are captured. Telnet provides remote access, which allows us to access and extract the username and the password used by the host machine in the above process. This can be seen in the load parameter.

```
        options   = [('NOP', None), ('NOP', None), ('Timestamp', (1268295056, 2856592998))]

^Cseed-attacker:PES1UG21CS924:Navya:/volumes
$>python3 Task1.1B-TCP.py
SNIFFING PACKETS...
###[ Ethernet ]###
  dst       = 02:42:9f:11:cd:26
  src       = 02:42:0a:09:00:05
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x10
     len       = 60
     id        = 15511
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0xe9fd
     src       = 10.9.0.5
     dst       = 10.9.0.1
     \options   \
###[ TCP ]###
        sport     = 55518
        dport     = telnet
        seq       = 3258275258
        ack       = 0
        dataofs   = 10
        reserved  = 0
        flags     = S
        window    = 64240
```

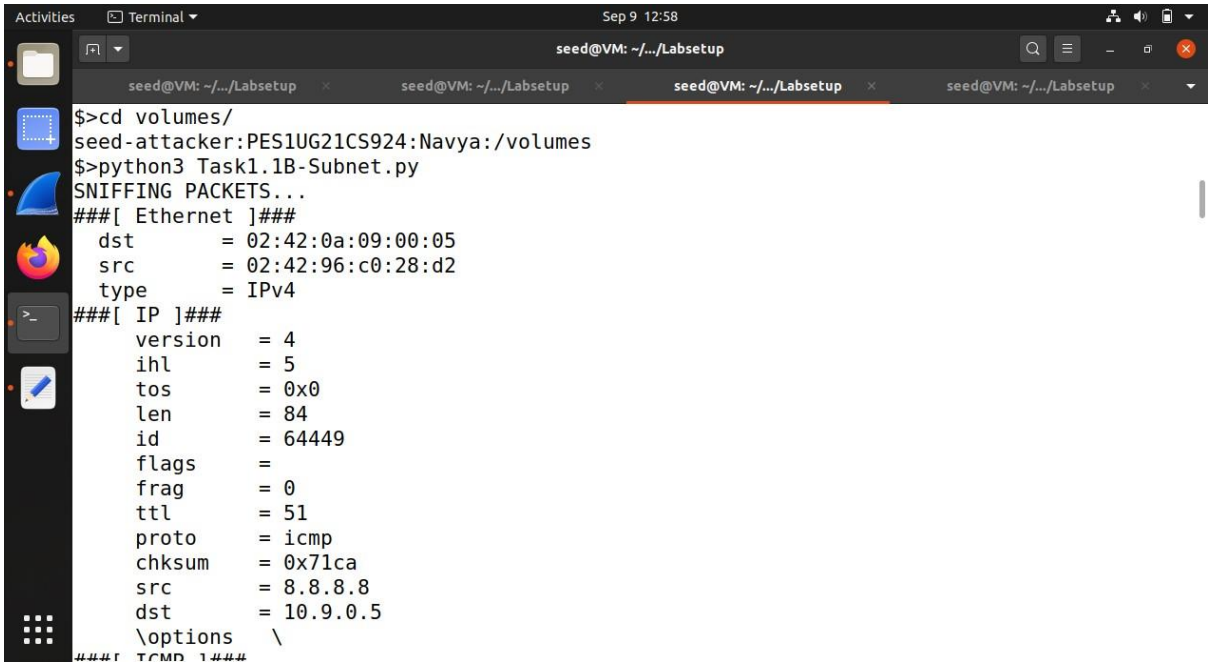
```
        chksum    = 0x1446
        urgptr    = 0
        options   = [('MSS', 1460), ('SAckOK', b''), ('Timestamp', (1268320870, 0)), ('NOP', None), ('WScale', 7)]

###[ Ethernet ]###
  dst       = 02:42:9f:11:cd:26
  src       = 02:42:0a:09:00:05
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x10
     len       = 52
     id        = 15512
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0xea04
     src       = 10.9.0.5
     dst       = 10.9.0.1
     \options   \
###[ TCP ]###
        sport     = 55518
        dport     = telnet
        seq       = 3258275259
        ack       = 1360779263
        dataofs   = 8
        reserved  = 0
        flags     = A
        window    = 502
        chksum    = 0x143e
```

```
        urgptr    = 0
        options   = [('NOP', None), ('NOP', None), ('Timestamp', (1268320870, 2856618812))]

###[ Ethernet ]###
  dst       = 02:42:9f:11:cd:26
  src       = 02:42:0a:09:00:05
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x10
     len       = 76
     id        = 15513
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0xe9eb
     src       = 10.9.0.5
     dst       = 10.9.0.1
     \options   \
###[ TCP ]###
        sport     = 55518
        dport     = telnet
        seq       = 3258275259
        ack       = 1360779263
        dataofs   = 8
        reserved  = 0
        flags     = PA
        window    = 502
        chksum    = 0x1456
        urgptr    = 0
```

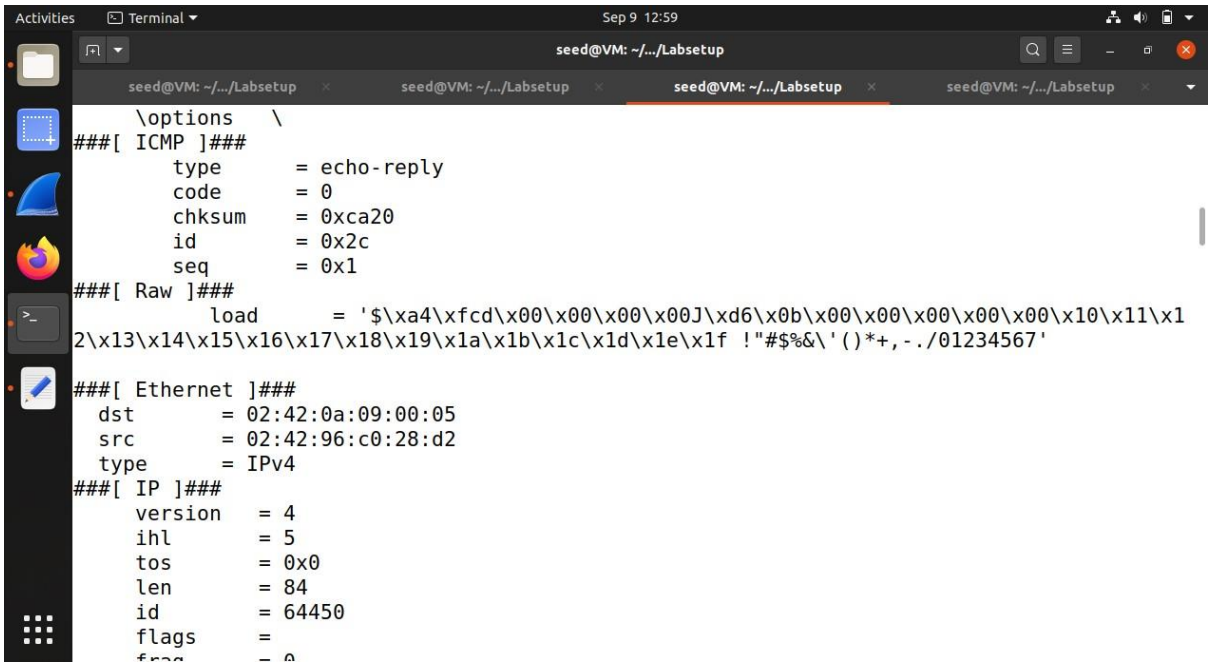
```
64 bytes from 8.8.8.8: icmp_seq=6 ttl=115 time=117 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=115 time=26.6 ms
^C
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6007ms
rtt min/avg/max/mdev = 26.326/54.658/116.513/39.046 ms
hostA:PES1UG21CS924:Navya:/
$>telnet 10.9.0.1
Trying 10.9.0.1...
Connected to 10.9.0.1.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
VM login: dees
Password:
^CConnection closed by foreign host.
hostA:PES1UG21CS924:Navya:/
$>telnet 10.9.0.1
Trying 10.9.0.1...
Connected to 10.9.0.1.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
VM login: SEED
Password:

Login incorrect
VM login: SEED
Password:

Login incorrect
VM login: ^CConnection closed by foreign host.
hostA:PES1UG21CS924:Navya:/
$>
```

Subnet

The packets with the given source subnet are captured. This refers to the fact that only the response packets are captured , unlike the previous methods were both the response and request are captured. Here, the request packages are not captured as Host A is in a different subnet.

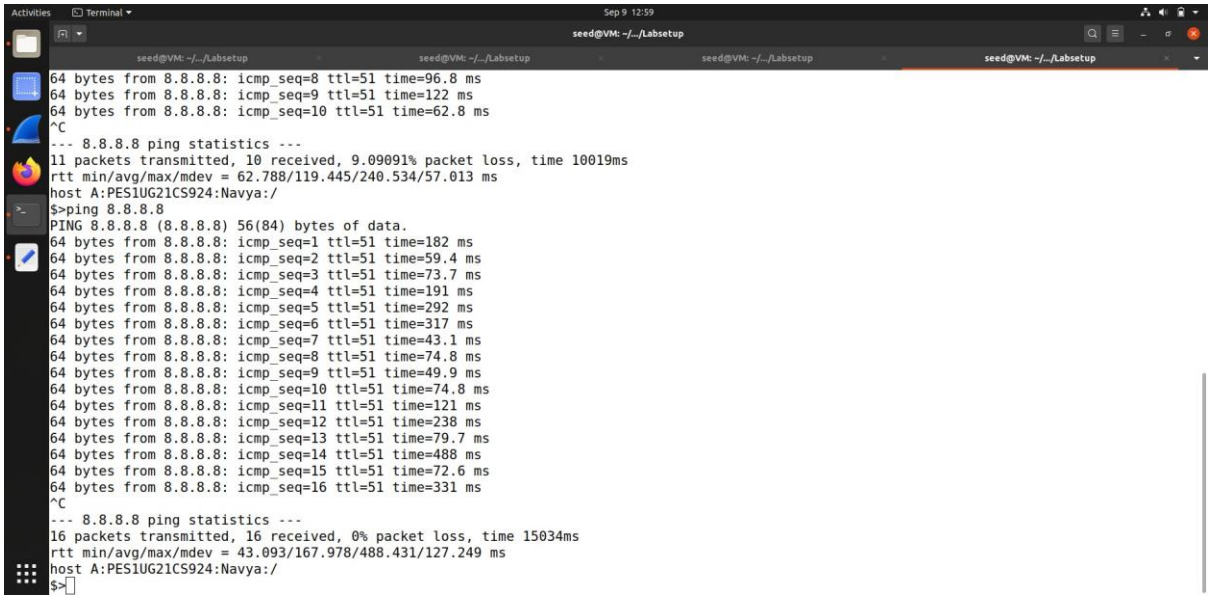


```
$>cd volumes/
seed-attacker:PES1UG21CS924:Navya:/volumes
$>python3 Task1.1B-Subnet.py
SNIFFING PACKETS...
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:96:c0:28:d2
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 64449
     flags     =
     frag      = 0
     ttl       = 51
     proto     = icmp
     chksum    = 0x71ca
     src       = 8.8.8.8
     dst       = 10.9.0.5
     \options   \
```



```
     \options   \
###[ ICMP ]###
        type      = echo-reply
        code      = 0
        chksum    = 0xca20
        id        = 0x2c
        seq       = 0x1
###[ Raw ]###
           load      = '$\xa4\xfcd\x00\x00\x00\x00J\xd6\x0b\x00\x00\x00\x00\x00\x10\x11\x1
2\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#$%&\'()*+,-./01234567'

###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:96:c0:28:d2
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 64450
     flags     =
```

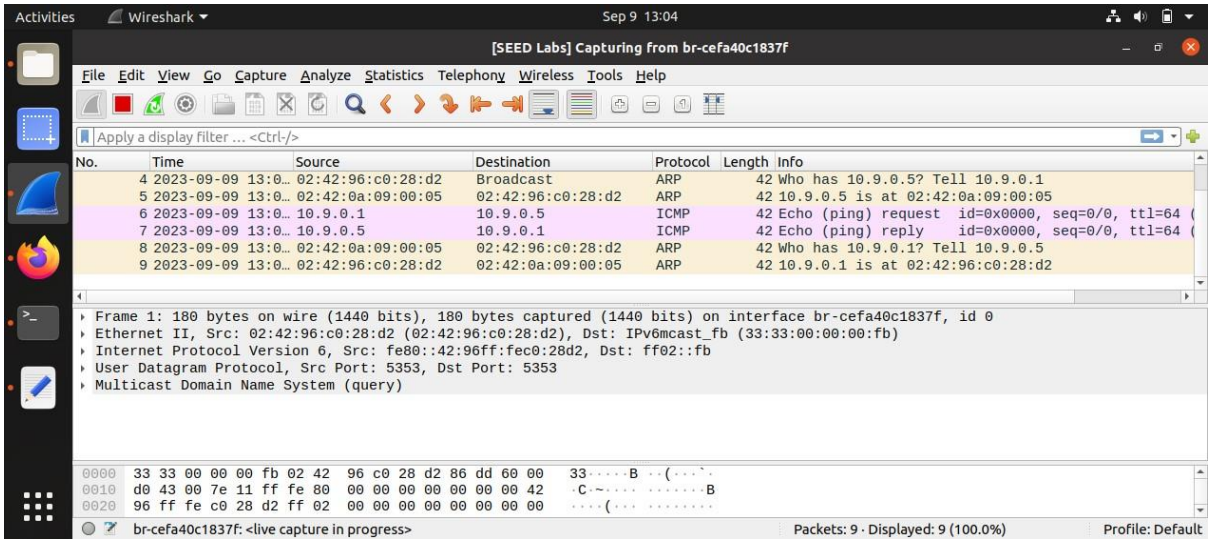
```
Activities  Terminal  Sep 9 12:59
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup   seed@VM: ~/.../Labsetup   seed@VM: ~/.../Labsetup   seed@VM: ~/.../Labsetup
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:96:c0:28:d2
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 64450
     flags     =
     frag      = 0
     ttl       = 51
     proto     = icmp
     chksum    = 0x71c9
     src       = 8.8.8.8
     dst       = 10.9.0.5
     \options   \
###[ ICMP ]###
        type      = echo-reply
        code      = 0
        chksum    = 0x8418
        id        = 0x2c
        seq       = 0x2
###[ Raw ]###
           load      = '%\xa4\xfcd\x00\x00\x00\x00\x8f\xdd\x0b\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1
e\x1f !"#$%&\'()*+,-./01234567'

###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:96:c0:28:d2
```

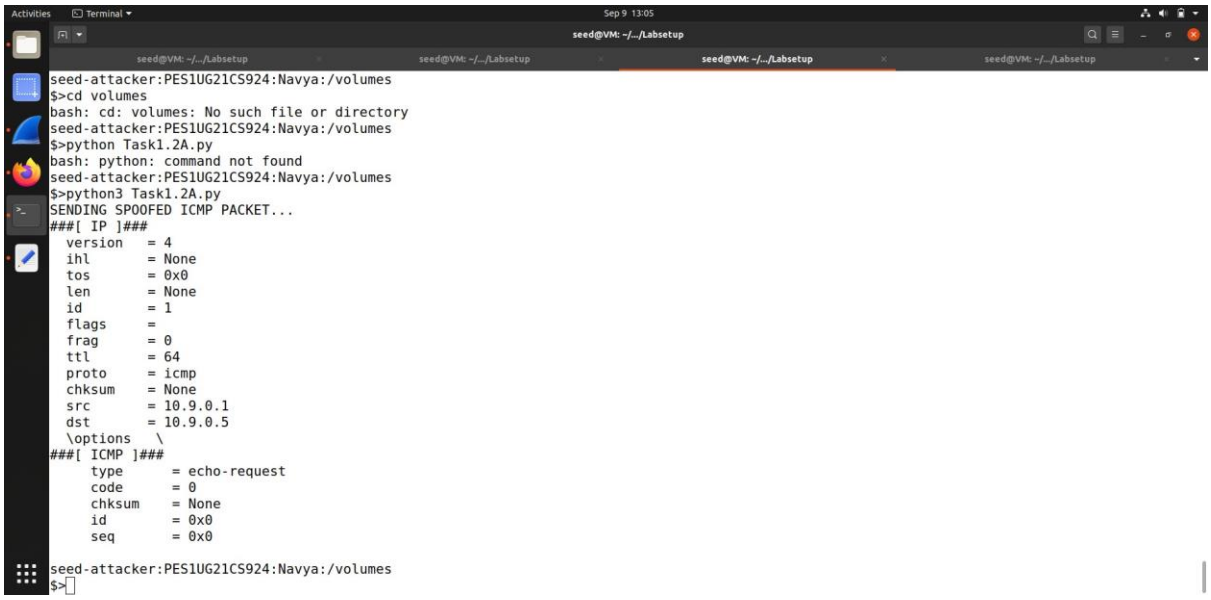


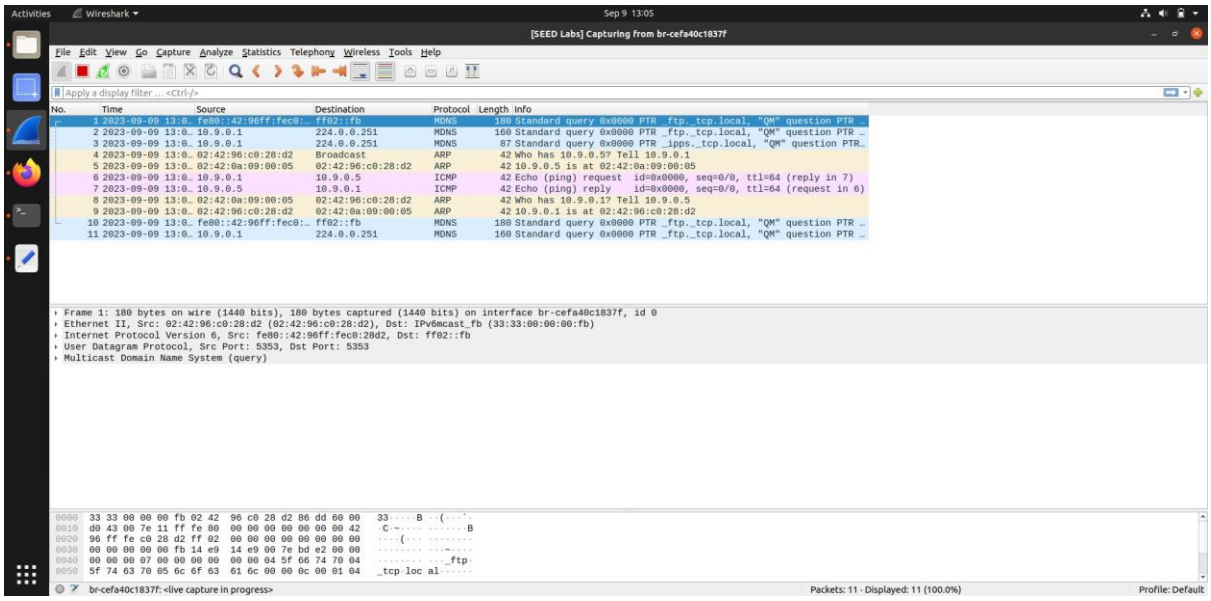
```
Activities  Terminal  Sep 9 12:59
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup   seed@VM: ~/.../Labsetup   seed@VM: ~/.../Labsetup   seed@VM: ~/.../Labsetup
64 bytes from 8.8.8.8: icmp_seq=8 ttl=51 time=96.8 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=51 time=122 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=51 time=62.8 ms
^C
--- 8.8.8.8 ping statistics ---
11 packets transmitted, 10 received, 9.09091% packet loss, time 10019ms
rtt min/avg/max/mdev = 62.788/119.445/240.534/57.013 ms
host A:PES1UG21CS924:Navya:/
$>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=51 time=182 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=51 time=59.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=51 time=73.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=51 time=191 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=51 time=292 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=51 time=317 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=51 time=43.1 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=51 time=74.8 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=51 time=49.9 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=51 time=74.8 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=51 time=121 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=51 time=238 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=51 time=79.7 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=51 time=488 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=51 time=72.6 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=51 time=331 ms
^C
--- 8.8.8.8 ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15034ms
rtt min/avg/max/mdev = 43.093/167.978/488.431/127.249 ms
host A:PES1UG21CS924:Navya:/
$>
```

TASK 1.2

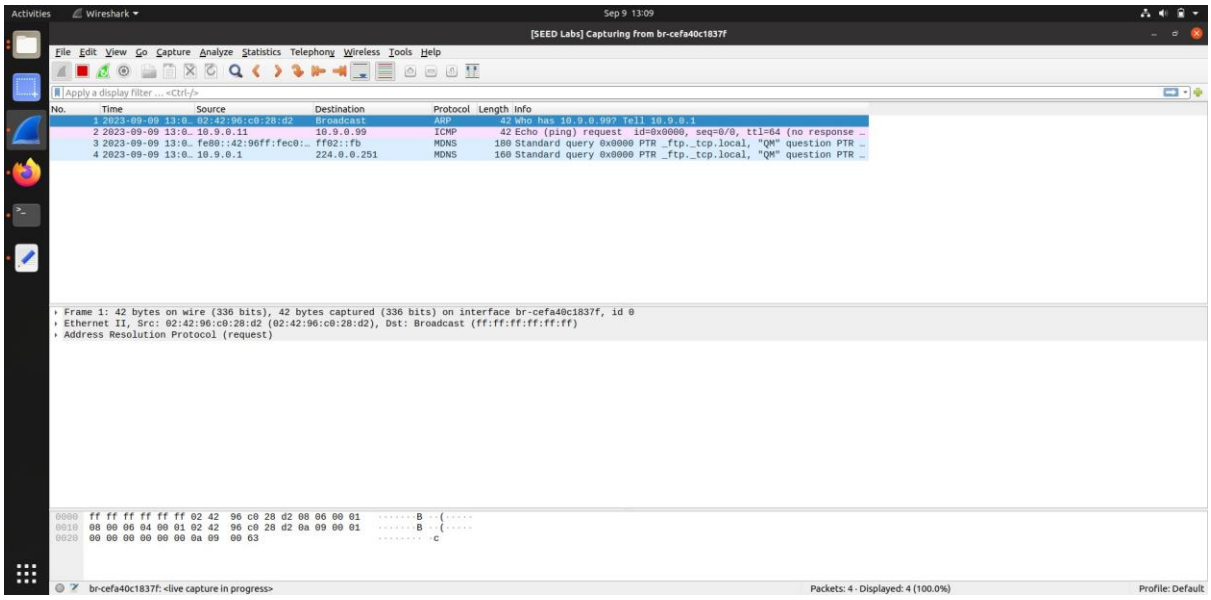
An ICMP request packet is spoofed with a source IP address of 10.9.0.1 ans sent to the Host A machine with the destination IP of 10.9.0.5. The request is then accepted by the host A and a reply is sent to the spoofed IP address.

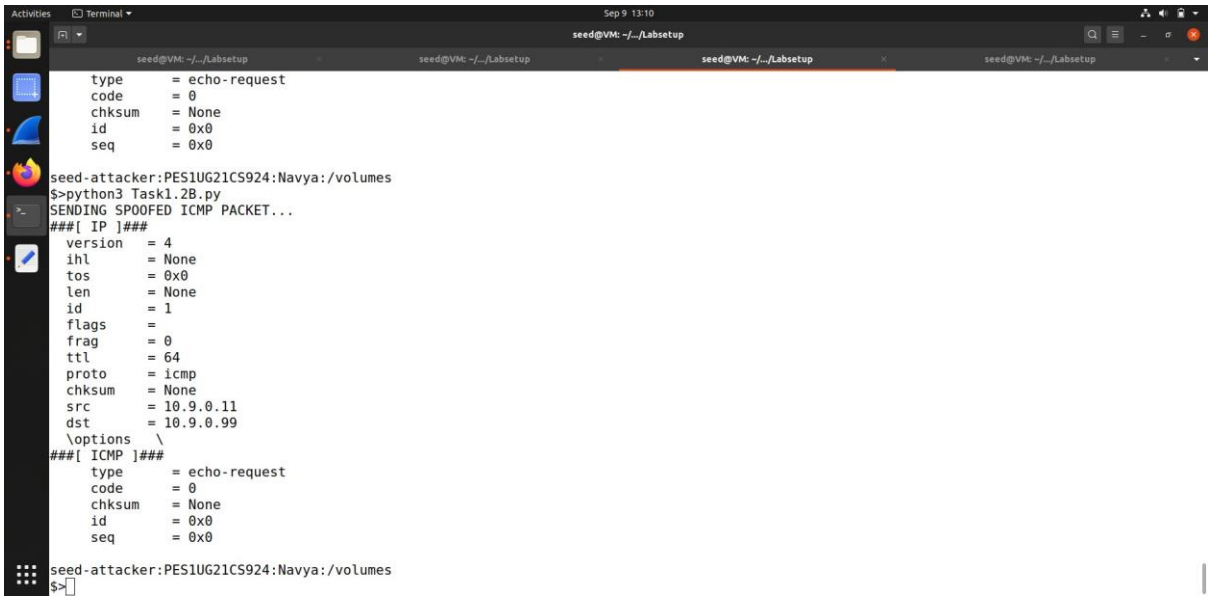

Activities
Wireshark
Sep 9 13:04
[SEED Labs] Capturing from br-cefa40c1837f
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
4 2023-09-09 13:0… 02:42:96:c0:28:d2 Broadcast ARP 42 Who has 10.9.0.5? Tell 10.9.0.1
5 2023-09-09 13:0… 02:42:0a:09:00:05 02:42:96:c0:28:d2 ARP 42 10.9.0.5 is at 02:42:0a:09:00:05
6 2023-09-09 13:0… 10.9.0.1 10.9.0.5 ICMP 42 Echo (ping) request id=0x0000, seq=0/0, ttl=64
7 2023-09-09 13:0… 10.9.0.5 10.9.0.1 ICMP 42 Echo (ping) reply id=0x0000, seq=0/0, ttl=64
8 2023-09-09 13:0… 02:42:0a:09:00:05 02:42:96:c0:28:d2 ARP 42 Who has 10.9.0.1? Tell 10.9.0.5
9 2023-09-09 13:0… 02:42:96:c0:28:d2 02:42:0a:09:00:05 ARP 42 10.9.0.1 is at 02:42:96:c0:28:d2
Frame 1: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface br-cefa40c1837f, id 0
Ethernet II, Src: 02:42:96:c0:28:d2 (02:42:96:c0:28:d2), Dst: IPv6mcast_fb (33:33:00:00:00:fb)
Internet Protocol Version 6, Src: fe80::42:96ff:fec0:28d2, Dst: ff02::fb
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)
0000 33 33 00 00 00 fb 02 42 96 c0 28 d2 86 dd 60 00
0010 d0 43 00 7e 11 ff fe 80 00 00 00 00 00 00 00 42
0020 96 ff fe c0 28 d2 ff 02 00 00 00 00 00 00 00 00
br-cefa40c1837f: <live capture in progress>
Packets: 9 · Displayed: 9 (100.0%)
Profile: Default


Activities
Terminal
Sep 9 13:05
seed@VM: ~/.../Labsetup
seed-attacker:PES1UG21CS924:Navya:/volumes
$>cd volumes
bash: cd: volumes: No such file or directory
seed-attacker:PES1UG21CS924:Navya:/volumes
$>python Task1.2A.py
bash: python: command not found
seed-attacker:PES1UG21CS924:Navya:/volumes
$>python3 Task1.2A.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 = 10.9.0.1
dst = 10.9.0.5
\options \
###[ICMP]###
type = echo-request
code = 0
chksum = None
id = 0x0
seq = 0x0
seed-attacker:PES1UG21CS924:Navya:/volumes
$>


Activities
Wireshark
Sep 9 13:05
[SEED Labs] Capturing from br-cefa40c1837f
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 2023-09-09 13:0… fe80::42:96ff:fec0:… ff02::fb MDNS 180 Standard query 0x0000 PTR _ftp._tcp.local, "QM" question PTR
2 2023-09-09 13:0… 10.9.0.1 224.0.0.251 MDNS 160 Standard query 0x0000 PTR _ftp._tcp.local, "QM" question PTR
3 2023-09-09 13:0… 10.9.0.1 224.0.0.251 MDNS 87 Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR
4 2023-09-09 13:0… 02:42:96:c0:28:d2 Broadcast ARP 42 Who has 10.9.0.5? Tell 10.9.0.1
5 2023-09-09 13:0… 02:42:0a:09:00:05 02:42:96:c0:28:d2 ARP 42 10.9.0.5 is at 02:42:0a:09:00:05
6 2023-09-09 13:0… 10.9.0.1 10.9.0.5 ICMP 42 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 7)
7 2023-09-09 13:0… 10.9.0.5 10.9.0.1 ICMP 42 Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 6)
8 2023-09-09 13:0… 02:42:0a:09:00:05 02:42:96:c0:28:d2 ARP 42 Who has 10.9.0.1? Tell 10.9.0.5
9 2023-09-09 13:0… 02:42:96:c0:28:d2 02:42:0a:09:00:05 ARP 42 10.9.0.1 is at 02:42:96:c0:28:d2
10 2023-09-09 13:0… fe80::42:96ff:fec0:… ff02::fb MDNS 180 Standard query 0x0000 PTR _ftp._tcp.local, "QM" question PTR
11 2023-09-09 13:0… 10.9.0.1 224.0.0.251 MDNS 160 Standard query 0x0000 PTR _ftp._tcp.local, "QM" question PTR
Frame 1: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface br-cefa40c1837f, id 0
Ethernet II, Src: 02:42:96:c0:28:d2 (02:42:96:c0:28:d2), Dst: IPv6mcast_fb (33:33:00:00:00:fb)
Internet Protocol Version 6, Src: fe80::42:96ff:fec0:28d2, Dst: ff02::fb
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)
0000 33 33 00 00 00 fb 02 42 96 c0 28 d2 86 dd 60 00
0010 d0 43 00 7e 11 ff fe 80 00 00 00 00 00 00 00 42
0020 96 ff fe c0 28 d2 ff 02 00 00 00 00 00 00 00 00
0030 00 00 00 00 00 fb 14 e9 14 e9 00 7e bd e2 00 00
0040 00 00 00 07 00 00 00 00 00 00 04 5f 66 74 70 04 _ftp
0050 5f 74 63 70 05 6c 6f 63 61 6c 00 00 0c 00 01 04 _tcp loc al
br-cefa40c1837f: <live capture in progress>
Packets: 11 · Displayed: 11 (100.0%)
Profile: Default

If the destination IP doesn't exist then no reply is sent to the request.





Task 1.3

The given process captures the number of hops that occur between the host machine and the destination IP given by the user, along with source IP of the captured packet. In the given code the time to live is given as 1. The ttl is however exceeded as seen in the wireshark.

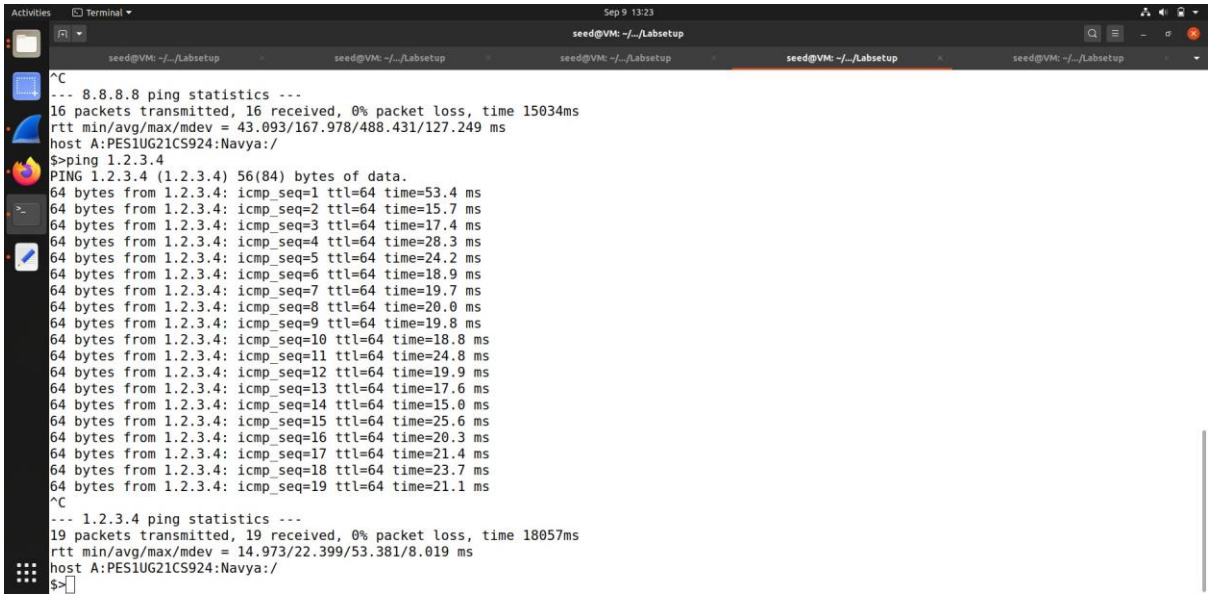
Apply a display filter ... <Ctrl-/>

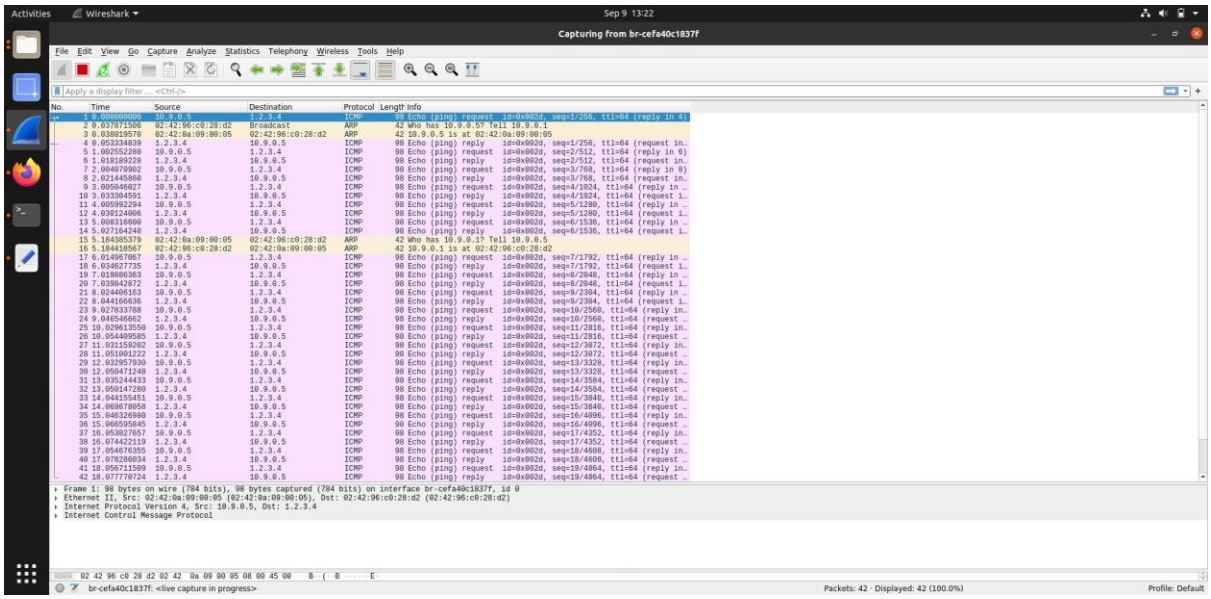
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.4	216.58.196.161	TLSv1.2	95	Application Data
2	0.000869787	10.0.2.4	216.58.196.161	TLSv1.2	80	Application Data
3	0.001091107	10.0.2.4	216.58.196.161	TCP	56	44854 → 443 [FIN, ACK] Seq=64 Ack=1 Win=62780 Len=0
4	0.001700067	216.58.196.161	10.0.2.4	TCP	62	443 → 44854 [ACK] Seq=1 Ack=64 Win=32344 Len=0
5	0.001700449	216.58.196.161	10.0.2.4	TCP	62	443 → 44854 [ACK] Seq=1 Ack=65 Win=32343 Len=0
6	0.043553710	216.58.196.161	10.0.2.4	TCP	62	443 → 44854 [FIN, ACK] Seq=1 Ack=65 Win=32343 Len=0
7	0.043735936	10.0.2.4	216.58.196.161	TCP	56	44854 → 443 [ACK] Seq=65 Ack=2 Win=62780 Len=0
8	1.895021237	10.0.2.4	142.250.183.238	TLSv1.2	95	Application Data
9	1.902265941	142.250.183.238	10.0.2.4	TCP	62	443 → 41210 [ACK] Seq=1 Ack=40 Win=32690 Len=0
10	2.199768202	142.250.183.238	10.0.2.4	TLSv1.2	95	Application Data
11	2.199843920	10.0.2.4	142.250.183.238	TCP	56	41210 → 443 [ACK] Seq=40 Ack=40 Win=63714 Len=0
12	2.896691156	127.0.0.1	127.0.0.53	DNS	77	Standard query 0xfcd8 A ssl.gstatic.com
13	2.896743887	127.0.0.1	127.0.0.53	DNS	77	Standard query 0x3fd7 AAAA ssl.gstatic.com
14	2.899831409	10.0.2.4	8.8.8.8	DNS	88	Standard query 0x6252 A ssl.gstatic.com OPT
15	2.900266696	10.0.2.4	8.8.8.8	DNS	88	Standard query 0x287e AAAA ssl.gstatic.com OPT
16	2.905347042	10.0.2.4	142.250.193.99	TLSv1.2	146	Application Data
17	2.909580726	142.250.193.99	10.0.2.4	TCP	62	443 → 57976 [ACK] Seq=1 Ack=91 Win=31588 Len=0
18	3.153705697	142.250.193.99	10.0.2.4	TLSv1.2	264	Application Data, Application Data, Application Data
19	3.153706252	8.8.8.8	10.0.2.4	DNS	104	Standard query response 0x6252 A ssl.gstatic.com A 142.250.19…
20	3.153706388	8.8.8.8	10.0.2.4	DNS	116	Standard query response 0x287e AAAA ssl.gstatic.com AAAA 2404…
21	3.155110371	10.0.2.4	142.250.193.99	TLSv1.2	95	Application Data
22	3.159812580	127.0.0.53	127.0.0.1	DNS	93	Standard query response 0xfcd8 A ssl.gstatic.com A 142.250.19…
23	3.160164036	127.0.0.53	127.0.0.1	DNS	105	Standard query response 0x3fd7 AAAA ssl.gstatic.com AAAA 2404…
24	3.162110209	142.250.193.99	10.0.2.4	TCP	62	443 → 57976 [ACK] Seq=209 Ack=130 Win=31549 Len=0
25	4.585643876	PcsCompu_ff:ba:5e		ARP	44	Who has 10.0.2.1? Tell 10.0.2.4
26	4.586143403	RealtekU_12:35:00		ARP	62	10.0.2.1 is at 52:54:00:12:35:00
27	4.612521324	10.0.2.4	157.240.23.35	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, ttl=1 (no response f…
28	4.613025972	10.0.2.1	10.0.2.4	ICMP	72	Time-to-live exceeded (Time to live exceeded in transit)
29	4.661895325	10.0.2.4	157.240.23.35	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, ttl=2 (no response f…
30	4.688729348	10.30.200.1	10.0.2.4	ICMP	72	Time-to-live exceeded (Time to live exceeded in transit)
31	4.737477501	10.0.2.4	157.240.23.35	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, ttl=3 (no response f…
32	4.768521728	192.168.4.1	10.0.2.4	ICMP	72	Time-to-live exceeded (Time to live exceeded in transit)
33	4.826583840	10.0.2.4	157.240.23.35	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, ttl=4 (no response f…
34	4.874277165	192.168.254.1	10.0.2.4	ICMP	72	Time-to-live exceeded (Time to live exceeded in transit)
35	4.918148267	10.0.2.4	157.240.23.35	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, ttl=5 (no response f…
36	5.117920308	14.143.35.157	10.0.2.4	ICMP	72	Time-to-live exceeded (Time to live exceeded in transit)
37	5.179185499	10.0.2.4	157.240.23.35	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, ttl=6 (no response f…
38	5.221075183	172.29.251.33	10.0.2.4	ICMP	72	Time-to-live exceeded (Time to live exceeded in transit)
39	5.285823623	10.0.2.4	157.240.23.35	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, ttl=7 (no response f…
40	5.366536398	180.87.36.9	10.0.2.4	ICMP	72	Time-to-live exceeded (Time to live exceeded in transit)
41	5.422433490	10.0.2.4	157.240.23.35	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, ttl=8 (no response f…
42	5.461821292	180.87.36.95	10.0.2.4	ICMP	72	Time-to-live exceeded (Time to live exceeded in transit)
43	5.509134213	10.0.2.4	157.240.23.35	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, ttl=9 (no response f…
44	5.556890119	129.134.34.179	10.0.2.4	ICMP	72	Time-to-live exceeded (Time to live exceeded in transit)
45	5.594523739	10.0.2.4	157.240.23.35	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, ttl=10 (no response …
46	5.621116412	157.240.38.179	10.0.2.4	ICMP	72	Time-to-live exceeded (Time to live exceeded in transit)
47	5.695507177	10.0.2.4	157.240.23.35	ICMP	44	Echo (ping) request id=0x0000, seq=0/0, ttl=11 (reply in 48)
48	5.740327650	157.240.23.35	10.0.2.4	ICMP	62	Echo (ping) reply id=0x0000, seq=0/0, ttl=54 (request in 4…
49	10.001715178	10.0.2.4	142.250.195.78	TLSv1.2	95	Application Data
50	10.002611607	10.0.2.4	142.250.195.78	TLSv1.2	80	Application Data
51	10.002692309	10.0.2.4	142.250.195.78	TCP	56	49146 → 443 [FIN, ACK] Seq=64 Ack=1 Win=63714 Len=0
52	10.003462336	142.250.195.78	10.0.2.4	TCP	62	443 → 49146 [ACK] Seq=1 Ack=64 Win=32588 Len=0
53	10.003462710	142.250.195.78	10.0.2.4	TCP	62	443 → 49146 [ACK] Seq=1 Ack=65 Win=32587 Len=0
54	10.055156575	142.250.195.78	10.0.2.4	TCP	62	443 → 49146 [FIN, ACK] Seq=1 Ack=65 Win=32587 Len=0
55	10.055326226	10.0.2.4	142.250.195.78	TCP	56	49146 → 443 [ACK] Seq=65 Ack=2 Win=63714 Len=0

```
seed-attacker:PES1UG21CS924:Navya:/volumes
$>python3 Task1.3.py 157.240.23.35
Traceroute 157.240.23.35
1 hops away:  10.0.2.1
2 hops away:  172.16.20.1
3 hops away:  119.226.103.130
4 hops away:  100.70.137.135
5 hops away:  100.70.137.119
6 hops away:  172.31.180.57
7 hops away:  180.87.36.9
8 hops away:  180.87.36.95
9 hops away:  129.134.34.175
10 hops away:  173.252.67.19
11 hops away:  157.240.23.35
Done 157.240.23.35
seed-attacker:PES1UG21CS924:Navya:/volumes
$>python3 Task1.3.py 157.240.23.35
Traceroute 157.240.23.35
1 hops away:  10.0.2.1
2 hops away:  172.16.20.1
3 hops away:  119.226.103.130
4 hops away:  100.70.137.135
5 hops away:  100.70.137.119
6 hops away:  172.31.180.57
7 hops away:  180.87.36.9
8 hops away:  180.87.36.95
9 hops away:  129.134.34.175
10 hops away:  173.252.67.19
11 hops away:  157.240.23.35
Done 157.240.23.35
seed-attacker:PES1UG21CS924:Navya:/volumes
$>
```

Task 1.4

In the given process, the Host A pings a non-existent IP address and since the attacker is also present on the same network, it is able to sniff the packets. However, the specifications applied are that only the ICMP packets with the source IP of 10.9.0.5 are to be captured. The reply is then spoofed by the attacker based on the information gathered from the sniffed packets. This in turn makes the host machine assume that the replies were sent by the IP it pinged.





```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

seed-attacker:PES1UG21CS924:Navya:/volumes
$>python3 Task1.4.py
original packet.........
source IP : 10.9.0.5
Destination IP : 1.2.3.4
spoofed packet........
Source IP: 1.2.3.4
Destination IP: 10.9.0.5
original packet.........
source IP : 10.9.0.5
Destination IP : 1.2.3.4
spoofed packet........
Source IP: 1.2.3.4
Destination IP: 10.9.0.5
original packet.........
source IP : 10.9.0.5
Destination IP : 1.2.3.4
spoofed packet........
Source IP: 1.2.3.4
Destination IP: 10.9.0.5
original packet.........
source IP : 10.9.0.5
Destination IP : 1.2.3.4
spoofed packet........
Source IP: 1.2.3.4
Destination IP: 10.9.0.5
original packet.........
source IP : 10.9.0.5
Destination IP : 1.2.3.4
spoofed packet........
```

```
seed-attacker:PES1UG21CS924:Navya:/volumes
$>python3 Task1.3.py 157.240.23.35
Traceroute 157.240.23.35
1 hops away:  10.0.2.1
2 hops away:  172.16.20.1
3 hops away:  119.226.103.130
4 hops away:  100.70.137.135
5 hops away:  100.70.137.119
6 hops away:  172.31.180.57
7 hops away:  180.87.36.9
8 hops away:  180.87.36.95
9 hops away:  129.134.34.175
10 hops away:  173.252.67.19
11 hops away:  157.240.23.35
Done 157.240.23.35
seed-attacker:PES1UG21CS924:Navya:/volumes
$>python3 Task1.3.py 157.240.23.35
Traceroute 157.240.23.35
1 hops away:  10.0.2.1
2 hops away:  172.16.20.1
3 hops away:  119.226.103.130
4 hops away:  100.70.137.135
5 hops away:  100.70.137.119
6 hops away:  172.31.180.57
7 hops away:  180.87.36.9
8 hops away:  180.87.36.95
9 hops away:  129.134.34.175
10 hops away:  173.252.67.19
11 hops away:  157.240.23.35
Done 157.240.23.35
seed-attacker:PES1UG21CS924:Navya:/volumes
$>
```