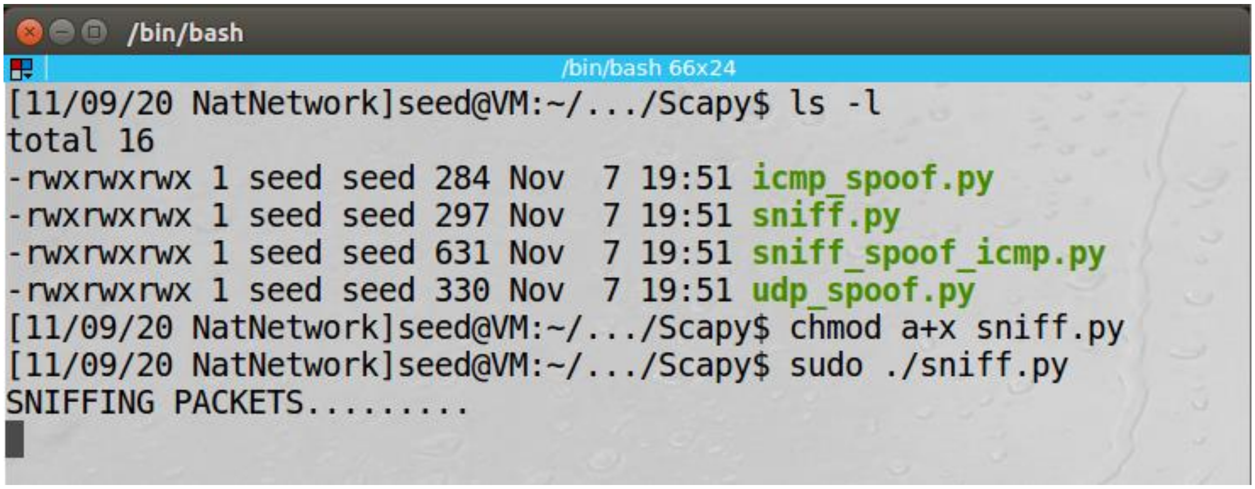
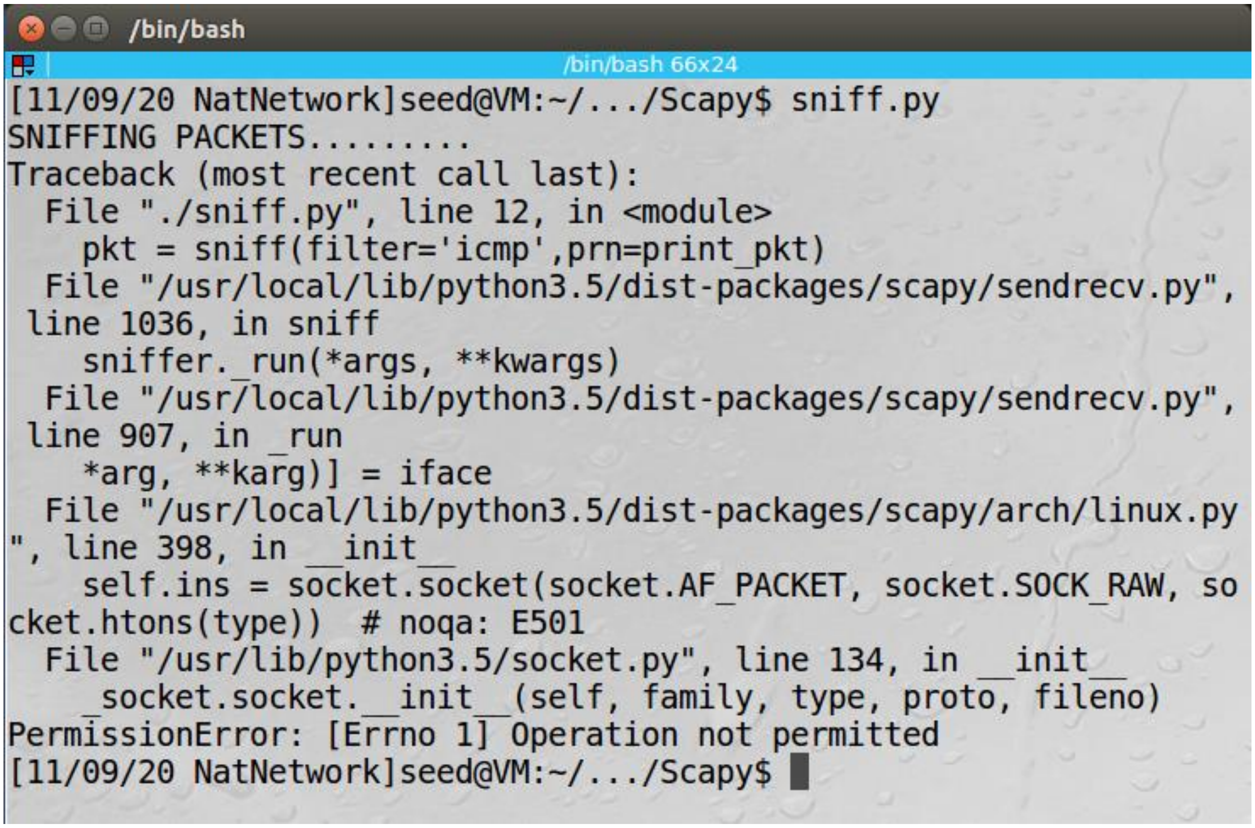
Lab Task Set 1: Using Tools to Sniff and Spoof Packets

- 2.1 Task 1.1: Sniffing Packets
  - Task 1.1A. Run a program that sniffs packet, print out some of information about the packet.
  - We have to run with root privilege.
  - With the root privilege : running.



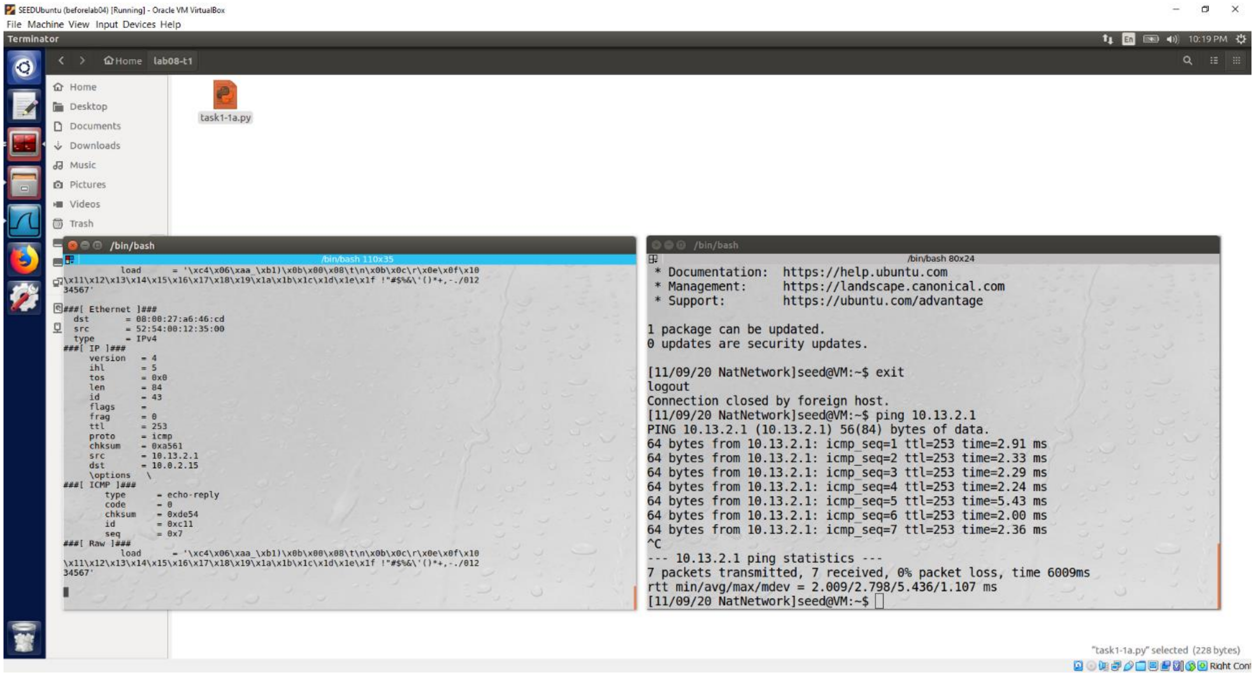
```
[11/09/20 NatNetwork]seed@VM:~/.../Scapy$ ls -l
total 16
-rwxrwxrwx 1 seed seed 284 Nov  7 19:51 icmp_spoof.py
-rwxrwxrwx 1 seed seed 297 Nov  7 19:51 sniff.py
-rwxrwxrwx 1 seed seed 631 Nov  7 19:51 sniff_spoof_icmp.py
-rwxrwxrwx 1 seed seed 330 Nov  7 19:51 udp_spoof.py
[11/09/20 NatNetwork]seed@VM:~/.../Scapy$ chmod a+x sniff.py
[11/09/20 NatNetwork]seed@VM:~/.../Scapy$ sudo ./sniff.py
SNIFFING PACKETS.........
```

  - Without the root privilege : denied.



```
[11/09/20 NatNetwork]seed@VM:~/.../Scapy$ sniff.py
SNIFFING PACKETS.........
Traceback (most recent call last):
  File "./sniff.py", line 12, in <module>
    pkt = sniff(filter='icmp',prn=print_pkt)
  File "/usr/local/lib/python3.5/dist-packages/scapy/sendrecv.py",
 line 1036, in sniff
    sniffer._run(*args, **kwargs)
  File "/usr/local/lib/python3.5/dist-packages/scapy/sendrecv.py",
 line 907, in _run
    *arg, **karg)] = iface
  File "/usr/local/lib/python3.5/dist-packages/scapy/arch/linux.py
", line 398, in __init__
    self.ins = socket.socket(socket.AF_PACKET, socket.SOCK_RAW, so
cket.htons(type))  # noqa: E501
  File "/usr/lib/python3.5/socket.py", line 134, in __init__
    _socket.socket.__init__(self, family, type, proto, fileno)
PermissionError: [Errno 1] Operation not permitted
[11/09/20 NatNetwork]seed@VM:~/.../Scapy$
```

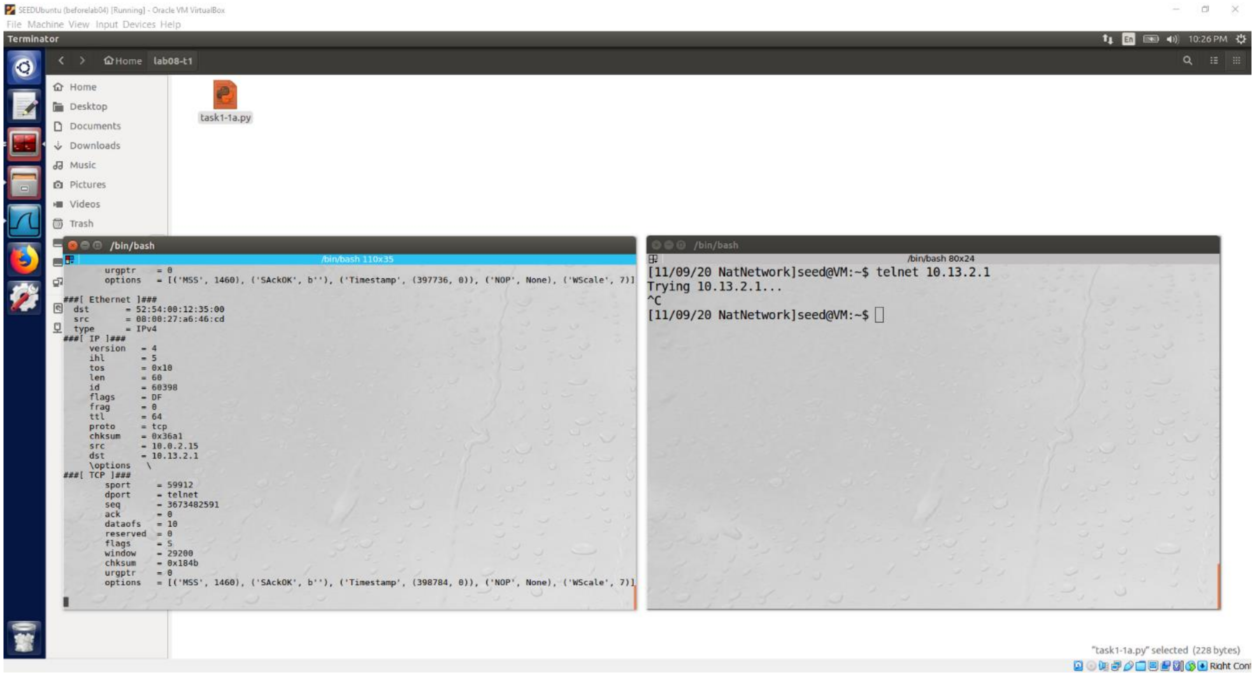
- Task 1.1B.
    - ICMP



```
            load      = '\xc4\x06\xaa_\xb1)\x0b\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 !"#$%&\'()*+,-./012
34567'

###[ Ethernet ]###
  dst       = 08:00:27:a6:46:cd
  src       = 52:54:00:12:35:00
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 43
     flags     =
     frag      = 0
     ttl       = 253
     proto     = icmp
     chksum    = 0xa561
     src       = 10.13.2.1
     dst       = 10.0.2.15
     \options   \
###[ ICMP ]###
        type      = echo-reply
        code      = 0
        chksum    = 0xde54
        id        = 0xc11
        seq       = 0x7
###[ Raw ]###
            load      = '\xc4\x06\xaa_\xb1)\x0b\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 !"#$%&\'()*+,-./012
34567'
```

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

1 package can be updated.
0 updates are security updates.

[11/09/20 NatNetwork]seed@VM:~$ exit
logout
Connection closed by foreign host.
[11/09/20 NatNetwork]seed@VM:~$ ping 10.13.2.1
PING 10.13.2.1 (10.13.2.1) 56(84) bytes of data.
64 bytes from 10.13.2.1: icmp_seq=1 ttl=253 time=2.91 ms
64 bytes from 10.13.2.1: icmp_seq=2 ttl=253 time=2.33 ms
64 bytes from 10.13.2.1: icmp_seq=3 ttl=253 time=2.29 ms
64 bytes from 10.13.2.1: icmp_seq=4 ttl=253 time=2.24 ms
64 bytes from 10.13.2.1: icmp_seq=5 ttl=253 time=5.43 ms
64 bytes from 10.13.2.1: icmp_seq=6 ttl=253 time=2.00 ms
64 bytes from 10.13.2.1: icmp_seq=7 ttl=253 time=2.36 ms
^C
--- 10.13.2.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6009ms
rtt min/avg/max/mdev = 2.009/2.798/5.436/1.107 ms
[11/09/20 NatNetwork]seed@VM:~$
```

    - TCP, port 23
- Proto = tcp, src = 10.0.2.15, dst=10.0.2.7, dport=telnet

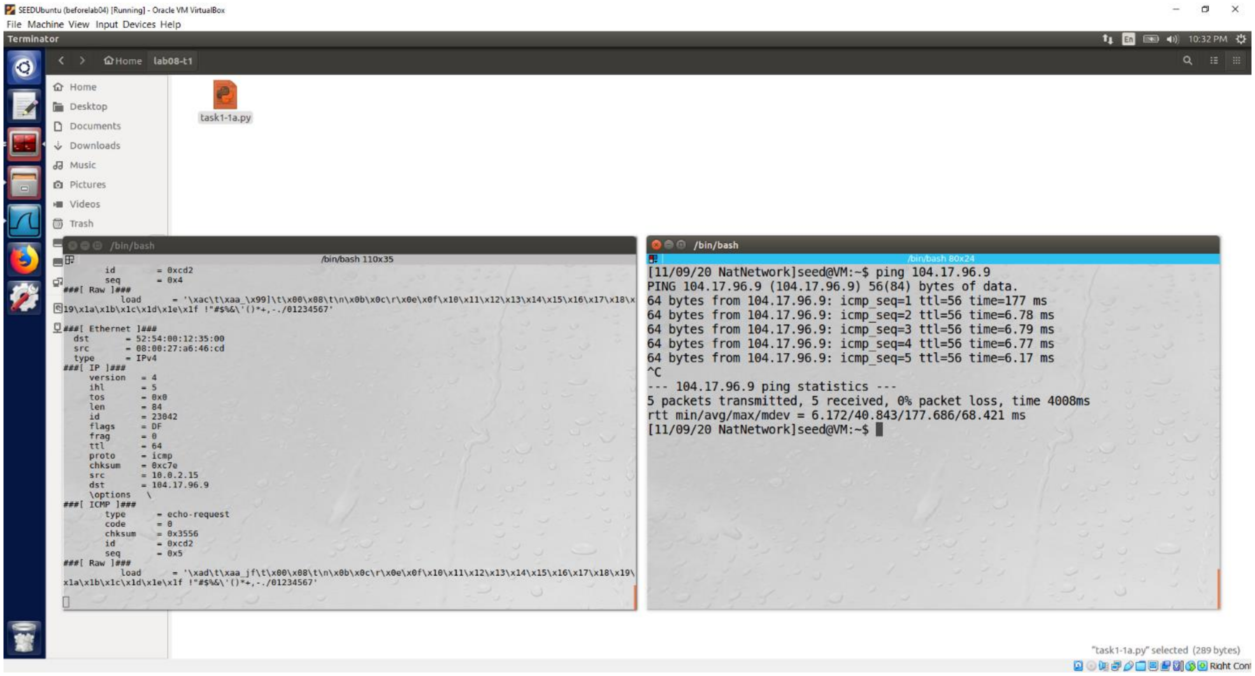


```
        urgptr    = 0
        options   = [('MSS', 1460), ('SAckOK', b''), ('Timestamp', (397736, 0)), ('NOP', None), ('WScale', 7)]

###[ Ethernet ]###
  dst       = 52:54:00:12:35:00
  src       = 08:00:27:a6:46:cd
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x10
     len       = 60
     id        = 60398
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0x36a1
     src       = 10.0.2.15
     dst       = 10.13.2.1
     \options   \
###[ TCP ]###
        sport     = 59912
        dport     = telnet
        seq       = 3673482591
        ack       = 0
        dataofs   = 10
        reserved  = 0
        flags     = S
        window    = 29200
        chksum    = 0x184b
        urgptr    = 0
        options   = [('MSS', 1460), ('SAckOK', b''), ('Timestamp', (398784, 0)), ('NOP', None), ('WScale', 7)]
```

```
[11/09/20 NatNetwork]seed@VM:~$ telnet 10.13.2.1
Trying 10.13.2.1...
^C
[11/09/20 NatNetwork]seed@VM:~$
```

    - Capture packets comes from or to go to a particular subnet.

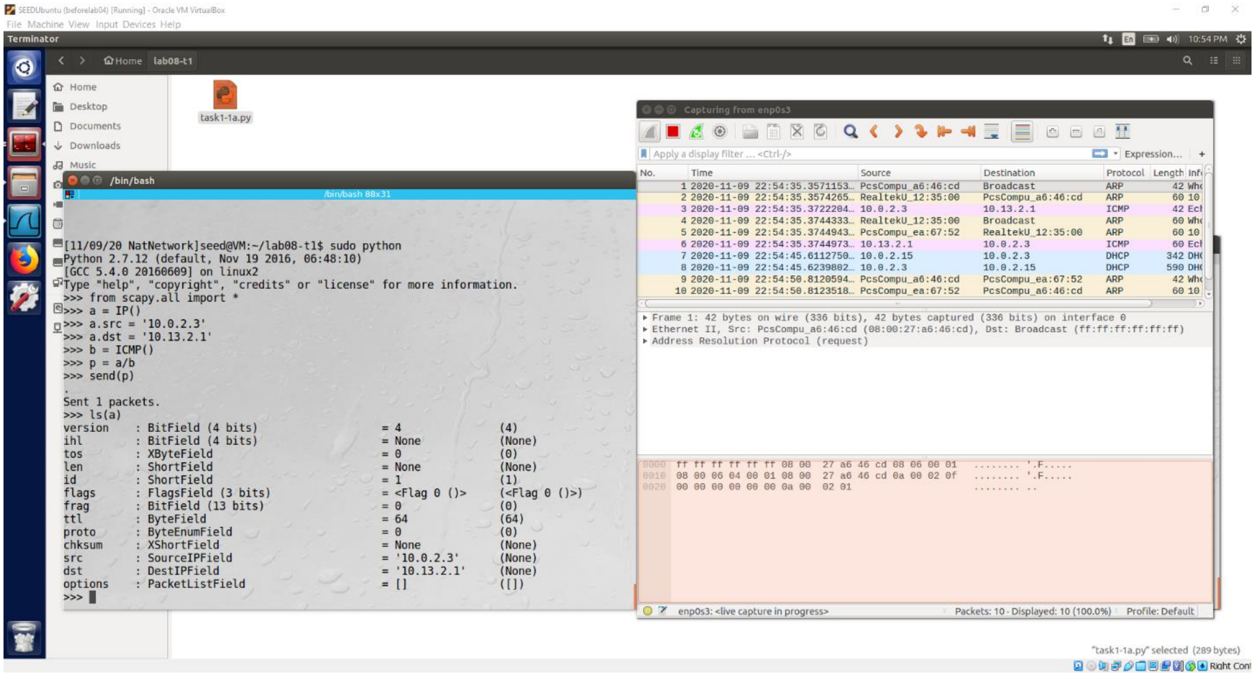
- Set filter to scan from 104.0.0.1 all the way to 104.255.255.254, ping request to subnet 104.17.96.9



```
         id        = 0xcd2
         seq       = 0x4
###[ Raw ]###
            load      = '\xac\t\xaa_\x99]\t\x00\x08\t\n\x0b\x0c\r\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x
19\x1a\x1b\x1c\x1d\x1e\x1f !"#$%&\'()*+,-./01234567'

###[ Ethernet ]###
  dst       = 52:54:00:12:35:00
  src       = 08:00:27:a6:46:cd
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 23042
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = icmp
     chksum    = 0xc7e
     src       = 10.0.2.15
     dst       = 104.17.96.9
     \options   \
###[ ICMP ]###
        type      = echo-request
        code      = 0
        chksum    = 0x3556
        id        = 0xcd2
        seq       = 0x5
###[ Raw ]###
            load      = '\xad\t\xaa_jf\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'
```

```
[11/09/20 NatNetwork]seed@VM:~$ ping 104.17.96.9
PING 104.17.96.9 (104.17.96.9) 56(84) bytes of data.
64 bytes from 104.17.96.9: icmp_seq=1 ttl=56 time=177 ms
64 bytes from 104.17.96.9: icmp_seq=2 ttl=56 time=6.78 ms
64 bytes from 104.17.96.9: icmp_seq=3 ttl=56 time=6.79 ms
64 bytes from 104.17.96.9: icmp_seq=4 ttl=56 time=6.77 ms
64 bytes from 104.17.96.9: icmp_seq=5 ttl=56 time=6.17 ms
^C
--- 104.17.96.9 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 6.172/40.843/177.686/68.421 ms
[11/09/20 NatNetwork]seed@VM:~$ 
```

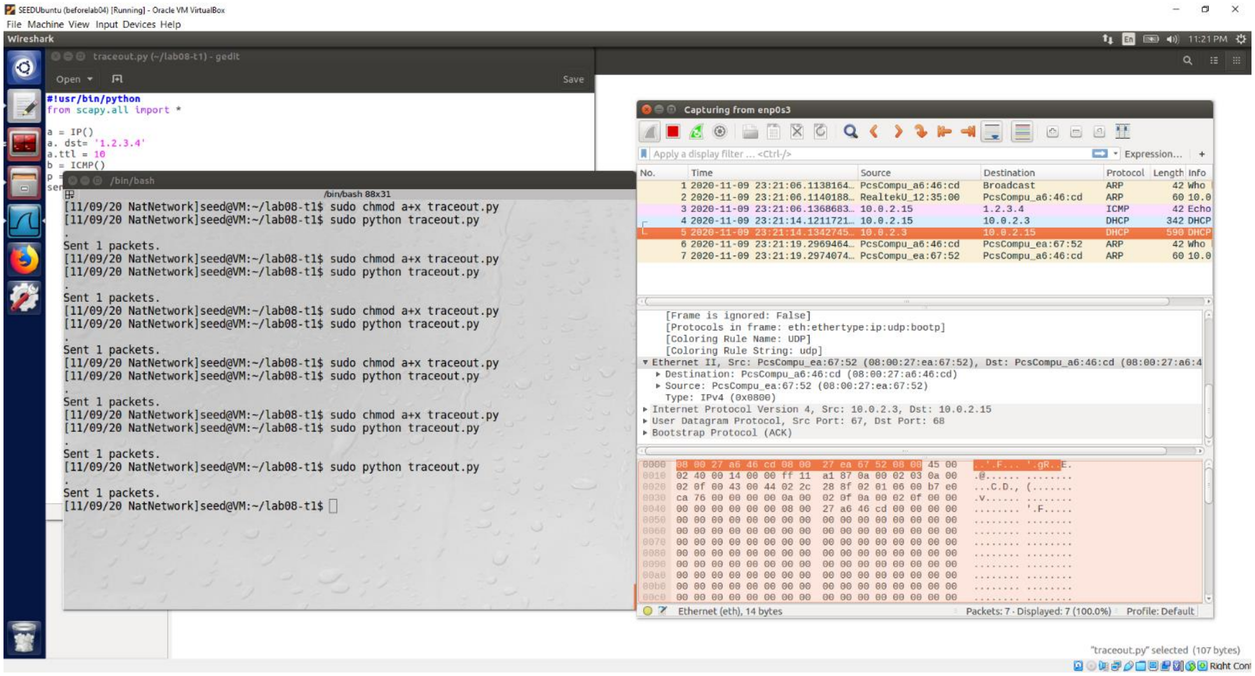
- 2.2 Task 1.2: Spoofing ICMP Packets
  - Spoof IP packets with an arbitrary source IP address – spoof ICMP echo request packets, and send them to another VM on the same network.
  - Process and observation:
    - Spoof the source IP address to an arbitrary IP address, whatever we want it to be.
    - The spoofed IP address, 10.0.2.3, sent to the real IP, 10.13.2.1
    - Checked on the Wireshark, or through ls(a), that 10.13.2.1 replied to it.


SEEDUbuntu (beforelab04) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
10:54 PM
Home
lab08-t1
Home
Desktop
Documents
Downloads
Music
task1-1a.py
/bin/bash
/bin/bash 88x31
Capturing from enp0s3
Apply a display filter ... <Ctrl-/>
Expression...
enp0s3: <live capture in progress>
Packets: 10 · Displayed: 10 (100.0%)
Profile: Default
"task1-1a.py" selected (289 bytes)
Right Ctrl

```
[11/09/20 NatNetwork]seed@VM:~/lab08-t1$ sudo python
Python 2.7.12 (default, Nov 19 2016, 06:48:10)
[GCC 5.4.0 20160609] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> from scapy.all import *
>>> a = IP()
>>> a.src = '10.0.2.3'
>>> a.dst = '10.13.2.1'
>>> b = ICMP()
>>> p = a/b
>>> send(p)
.
Sent 1 packets.
>>> ls(a)
version    : BitField (4 bits)                      = 4              (4)
ihl        : BitField (4 bits)                      = None           (None)
tos        : XByteField                             = 0              (0)
len        : ShortField                             = None           (None)
id         : ShortField                             = 1              (1)
flags      : FlagsField (3 bits)                    = <Flag 0 ()>    (<Flag 0 ()>)
frag       : BitField (13 bits)                     = 0              (0)
ttl        : ByteField                              = 64             (64)
proto      : ByteEnumField                          = 0              (0)
chksum     : XShortField                            = None           (None)
src        : SourceIPField                          = '10.0.2.3'     (None)
dst        : DestIPField                            = '10.13.2.1'    (None)
options    : PacketListField                        = []             ([])
>>> 
```

```
No. Time                           Source              Destination         Protocol Length Inf
  1 2020-11-09 22:54:35.3571153…   PcsCompu_a6:46:cd   Broadcast           ARP        42 Whc
  2 2020-11-09 22:54:35.3574265…   RealtekU_12:35:00   PcsCompu_a6:46:cd   ARP        60 10
  3 2020-11-09 22:54:35.3722204…   10.0.2.3            10.13.2.1           ICMP       42 Ech
  4 2020-11-09 22:54:35.3744333…   RealtekU_12:35:00   Broadcast           ARP        60 Whc
  5 2020-11-09 22:54:35.3744943…   PcsCompu_ea:67:52   RealtekU_12:35:00   ARP        60 10
  6 2020-11-09 22:54:35.3744973…   10.13.2.1           10.0.2.3            ICMP       60 Ech
  7 2020-11-09 22:54:45.6112750…   10.0.2.15           10.0.2.3            DHCP      342 DHC
  8 2020-11-09 22:54:45.6239802…   10.0.2.3            10.0.2.15           DHCP      590 DHC
  9 2020-11-09 22:54:50.8120594…   PcsCompu_a6:46:cd   PcsCompu_ea:67:52   ARP        42 Whc
 10 2020-11-09 22:54:50.8123518…   PcsCompu_ea:67:52   PcsCompu_a6:46:cd   ARP        60 10

▸ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_a6:46:cd (08:00:27:a6:46:cd), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 08 00  27 a6 46 cd 08 06 00 01   ........ '.F.....
0010  08 00 06 04 00 01 08 00  27 a6 46 cd 0a 00 02 0f   ........ '.F.....
0020  00 00 00 00 00 00 0a 00  02 01                     ........ ..
```

- 2.3 Task 1.3: Traceroute
  - Use Scapy to estimate the distance between my VM and a selected destination(1.2.3.4)
  - Increased ttl by 1 until it reaches the destination (get reply from it)
  - Program name has been changed to “task1-3.py”

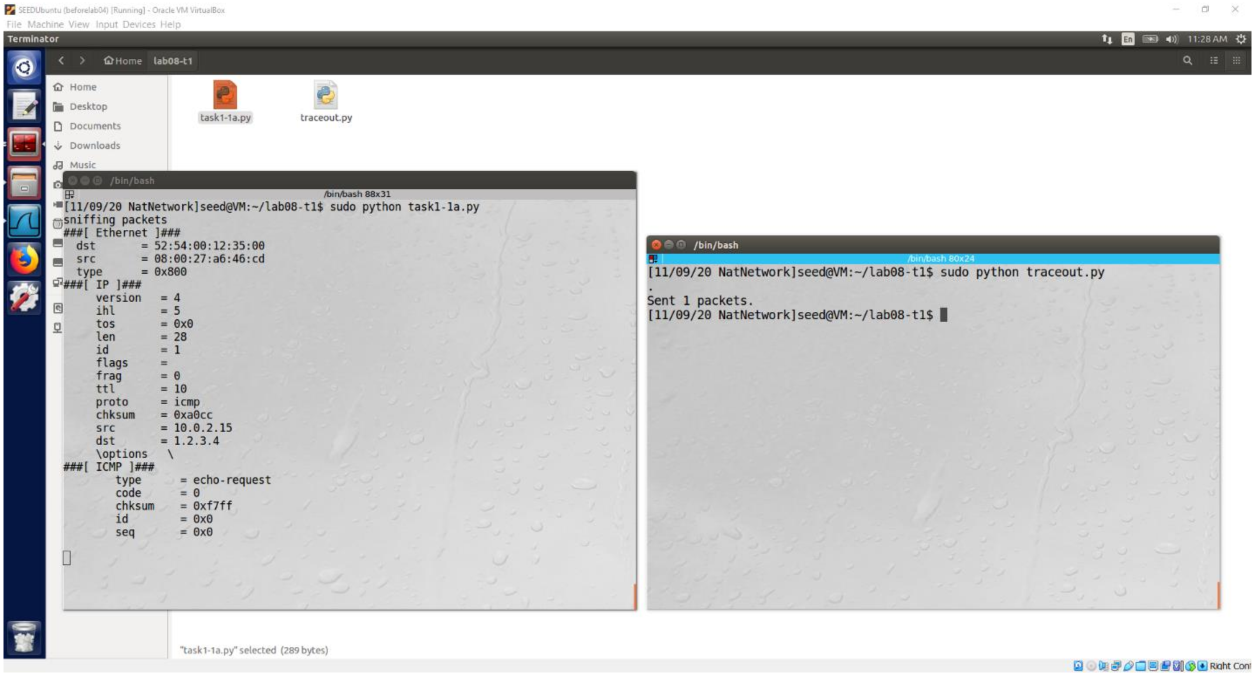

SEEDUbuntu (beforelab04) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wireshark
11:21 PM
traceout.py (~/lab08-t1) - gedit
Open
Save
/bin/bash
/bin/bash 88x31
Capturing from enp0s3
Apply a display filter ... <Ctrl-/>
Expression...
Ethernet (eth), 14 bytes
Packets: 7 · Displayed: 7 (100.0%)
Profile: Default
"traceout.py" selected (107 bytes)
Right Ctrl

```
#!usr/bin/python
from scapy.all import *

a = IP()
a. dst= '1.2.3.4'
a.ttl = 10
b = ICMP()
p =
sen
```

```
[11/09/20 NatNetwork]seed@VM:~/lab08-t1$ sudo chmod a+x traceout.py
[11/09/20 NatNetwork]seed@VM:~/lab08-t1$ sudo python traceout.py
.
Sent 1 packets.
[11/09/20 NatNetwork]seed@VM:~/lab08-t1$ sudo chmod a+x traceout.py
[11/09/20 NatNetwork]seed@VM:~/lab08-t1$ sudo python traceout.py
.
Sent 1 packets.
[11/09/20 NatNetwork]seed@VM:~/lab08-t1$ sudo chmod a+x traceout.py
[11/09/20 NatNetwork]seed@VM:~/lab08-t1$ sudo python traceout.py
.
Sent 1 packets.
[11/09/20 NatNetwork]seed@VM:~/lab08-t1$ sudo chmod a+x traceout.py
[11/09/20 NatNetwork]seed@VM:~/lab08-t1$ sudo python traceout.py
.
Sent 1 packets.
[11/09/20 NatNetwork]seed@VM:~/lab08-t1$ sudo chmod a+x traceout.py
[11/09/20 NatNetwork]seed@VM:~/lab08-t1$ sudo python traceout.py
.
Sent 1 packets.
[11/09/20 NatNetwork]seed@VM:~/lab08-t1$ sudo python traceout.py
.
Sent 1 packets.
[11/09/20 NatNetwork]seed@VM:~/lab08-t1$ 
```

```
No. Time                           Source              Destination         Protocol Length Info
  1 2020-11-09 23:21:06.1138164…   PcsCompu_a6:46:cd   Broadcast           ARP        42 Who
  2 2020-11-09 23:21:06.1140188…   RealtekU_12:35:00   PcsCompu_a6:46:cd   ARP        60 10.0
  3 2020-11-09 23:21:06.1368683…   10.0.2.15           1.2.3.4             ICMP       42 Echo
  4 2020-11-09 23:21:14.1211721…   10.0.2.15           10.0.2.3            DHCP      342 DHCP
  5 2020-11-09 23:21:14.1342745…   10.0.2.3            10.0.2.15           DHCP      590 DHCP
  6 2020-11-09 23:21:19.2969464…   PcsCompu_a6:46:cd   PcsCompu_ea:67:52   ARP        42 Who
  7 2020-11-09 23:21:19.2974074…   PcsCompu_ea:67:52   PcsCompu_a6:46:cd   ARP        60 10.0

    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:bootp]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
▾ Ethernet II, Src: PcsCompu_ea:67:52 (08:00:27:ea:67:52), Dst: PcsCompu_a6:46:cd (08:00:27:a6:4
  ▸ Destination: PcsCompu_a6:46:cd (08:00:27:a6:46:cd)
  ▸ Source: PcsCompu_ea:67:52 (08:00:27:ea:67:52)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.0.2.3, Dst: 10.0.2.15
▸ User Datagram Protocol, Src Port: 67, Dst Port: 68
▸ Bootstrap Protocol (ACK)

0000  08 00 27 a6 46 cd 08 00  27 ea 67 52 08 00 45 00   ..'.F... '.gR..E.
0010  02 40 00 14 00 00 ff 11  a1 87 0a 00 02 03 0a 00   .@...... ........
0020  02 0f 00 43 00 44 02 2c  28 8f 02 01 06 00 b7 e0   ...C.D., (.......
0030  ca 76 00 00 00 00 0a 00  02 0f 0a 00 02 0f 00 00   .v...... ........
0040  00 00 00 00 00 00 08 00  27 a6 46 cd 00 00 00 00   ........ '.F.....
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

- 2.4 Task 1.4: Sniffing and-then Spoofing
  - Combine the sniffing and spoofing technigues.
  - Checked “echo-request”



```
[11/09/20 NatNetwork]seed@VM:~/lab08-t1$ sudo python task1-1a.py
sniffing packets
###[ Ethernet ]###
  dst       = 52:54:00:12:35:00
  src       = 08:00:27:a6:46:cd
  type      = 0x800
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 28
     id        = 1
     flags     =
     frag      = 0
     ttl       = 10
     proto     = icmp
     chksum    = 0xa0cc
     src       = 10.0.2.15
     dst       = 1.2.3.4
     \options   \
###[ ICMP ]###
        type      = echo-request
        code      = 0
        chksum    = 0xf7ff
        id        = 0x0
        seq       = 0x0
```

```
[11/09/20 NatNetwork]seed@VM:~/lab08-t1$ sudo python traceout.py
.
Sent 1 packets.
[11/09/20 NatNetwork]seed@VM:~/lab08-t1$
```