

CNS (UE20CS326) LAB

Aryansh Bhargavan

PES1UG20CS084

Task 1.1A Sniffing IP Packets using Scapy

Running as superuser

```
seed-attacker:~$ python3 Task1.1A.py
SNIFFING PACKETS...
##### Ethernet #####
dst = ff:ff:ff:ff:ff:ff
src = 02:42:8a:09:00:06
type = ARP
##### ARP #####
hatype = Out
ptype = IPv4
hlen = 6
plen = 4
op = who-has
hwsrc = 02:42:8a:09:00:06
psrc = 10.9.0.6
hwdst = 00:00:00:00:00:00
pdst = 10.9.0.1
##### Ethernet #####
dst = 02:42:8a:09:00:06
src = 02:42:1f:15:03:83
type = ARP
##### ARP #####
hatype = In
ptype = IPv4
hlen = 6
plen = 4
op = is-at
hwsrc = 02:42:1f:15:03:83
psrc = 10.9.0.1
hwdst = 02:42:8a:09:00:06
pdst = 10.9.0.6
##### Ethernet #####
dst = 02:42:1f:15:03:83
src = 02:42:8a:09:00:06
type = IPv4
##### IP #####
version = 4
ihl = 5
tos = 0x0
len = 64
id = 23716
flags = 0
frag = 0
ttl = 64
proto = icmp
checksum = 0xc8ec
src = 10.9.0.6
dst = 10.9.0.1
##### ICMP #####
type = echo-request
code = 0

seed-host:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.9.0.6 netmask 255.255.255.0 broadcast 10.9.0.255
    ether 02:42:8a:09:00:06 txqueuelen 0 (Ethernet)
    RX packets 17 bytes 1422 (1.4 KB)
    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

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    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

seed-host:~$ ping 10.9.0.1
Pinging 10.9.0.1 (10.9.0.1) 56(84) bytes of data:
64 bytes from 10.9.0.1: icmp_seq=1 ttl=64 time=0.138 ms
64 bytes from 10.9.0.1: icmp_seq=2 ttl=64 time=0.111 ms
64 bytes from 10.9.0.1: icmp_seq=3 ttl=64 time=0.148 ms
^C
-- 10.9.0.1 ping statistics --
3 packets transmitted, 3 received, 0% packet loss, time 2070ms
rtt min/avg/max/mdev = 0.111/0.132/0.148/0.015 ms
seed-host:~$
```

We ran this from the attacker's VM since the attacker is the one that is going to be intercepting and sniffing said packets.

Running as non-superuser

```
seed@docker-desktop:/$ python3 Task1.1A.py
SNIFFING PACKETS...
Traceback (most recent call last):
  File "Task1.1A.py", line 6, in <module>
    pkt = sniff(iface = "br-f2cc6eca9a5e",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_socket[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)) # noqa: 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@docker-desktop:/$
```

Above program needs to be ran as superuser since a regular user would not be able to perform the tasks due to lack of privileges.

Task 1.1B Capturing ICMP, TCP packet and Subnet

ICMP

```

aryansh~/mnt/d  x  +
seed-attacker:PE$1U62K5084:AranyashB:/
$python3 Task1.1A.py
SHUFFLING PACKETS...
###[ Ethernet ]###
  dst      = ff:ff:ff:ff:ff:ff
  src      = 02:42:0a:09:00:06
  type     = ARP
###[ ARP ]###
  htype    = 0x1
  ptype    = IPv4
  hlen     = 6
  plen     = 4
  op       = who-has
  hsrc     = 02:42:0a:09:00:06
  psrc     = 10.9.0.0
  hwdest   = 00:0a:00:00:00:00
  pdst     = 10.9.0.1

###[ Ethernet ]###
  dst      = 02:42:0a:09:00:06
  src      = 02:42:1f:15:03:83
  type     = ARP
###[ ARP ]###
  htype    = 0x1
  ptype    = IPv4
  hlen     = 6
  plen     = 4
  op       = is-at
  hsrc     = 02:42:1f:15:03:83
  psrc     = 10.9.0.1
  hwdest   = 02:42:0a:09:00:06
  pdst     = 10.9.0.0

###[ Ethernet ]###
  dst      = 02:42:1f:15:03:83
  src      = 02:42:0a:09:00:06
  type     = IPv4
###[ IP ]###
  version  = 4
  ihl      = 5
  tos      = 0x0
  len      = 64
  id       = 23716
  flags    = 0F
  frag     = 0
  ttl      = 64
  proto    = icmp
  checksum = 0xc9ec
  src      = 10.9.0.0
  dst      = 10.9.0.1
  options  \
###[ ICMP ]###
  type     = echo-request
  code     = 0

aryansh~/mnt/d  x  +
seed-host:PE$1U62K5084:AranyashB:/
$ping 10.9.0.1
PING 10.9.0.1 (10.9.0.1) 56(84) bytes of data:
64 bytes from 10.9.0.1: icmp_seq=1 ttl=64 time=0.106 ms
64 bytes from 10.9.0.1: icmp_seq=2 ttl=64 time=0.164 ms
^C
--- 10.9.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1052ms
rtt min/avg/max/mdev = 0.106/0.135/0.164/0.029 ms
seed-host:PE$1U62K5084:AranyashB:/
$[]

```

We can see that an ICMP Packet has been captured and can see the source and destination as well.

TCP

```

aryansh~/mnt/d  x  +
seed-attacker:PE$1U62K5084:AranyashB:/
$mono Task1.1B-TCP.py
seed-attacker:PE$1U62K5084:AranyashB:/
$python3 Task1.1B-TCP.py
SHUFFLING PACKETS...
###[ Ethernet ]###
  dst      = 02:42:1f:15:03:83
  src      = 02:42:0a:09:00:06
  type     = IPv4
###[ IP ]###
  version  = 4
  ihl      = 5
  tos      = 0x10
  len      = 60
  id       = 46869
  flags    = 0F
  frag     = 0
  ttl      = 64
  proto    = tcp
  checksum = 0xd6ee
  src      = 10.9.0.0
  dst      = 10.9.0.1
  options  \
###[ TCP ]###
  sport    = 36136
  dport    = telnet
  seq      = 3938131664
  ack      = 0
  dataofs  = 30
  reserved = 0
  flags    = S
  window  = 64340
  checksum = 0x1447
  urgptr   = 0
  options  = [('MSS', 1460), ('SackOK', b''), ('Timestamp', (398163929, 0)), ('NOP', None), ('NScale', 7)]

aryansh~/mnt/d  x  +
seed-host:PE$1U62K5084:AranyashB:/
$telnet 10.9.0.1
Trying 10.9.0.1...
telnet: Unable to connect to remote host: Connection refused
seed-host:PE$1U62K5084:AranyashB:/
$[]

```

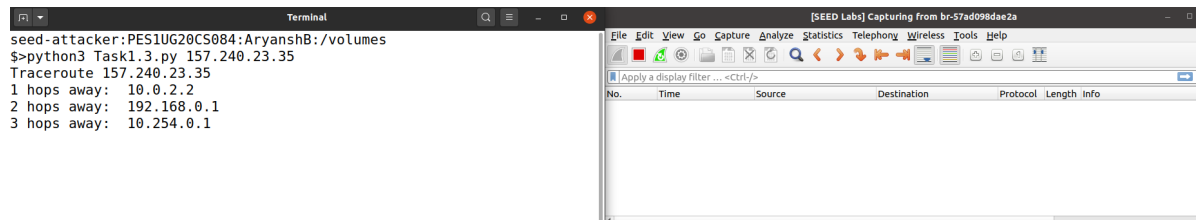
Telnet connection was refused but we received a singular packet

SUBNET

Task 1.3 Traceroute

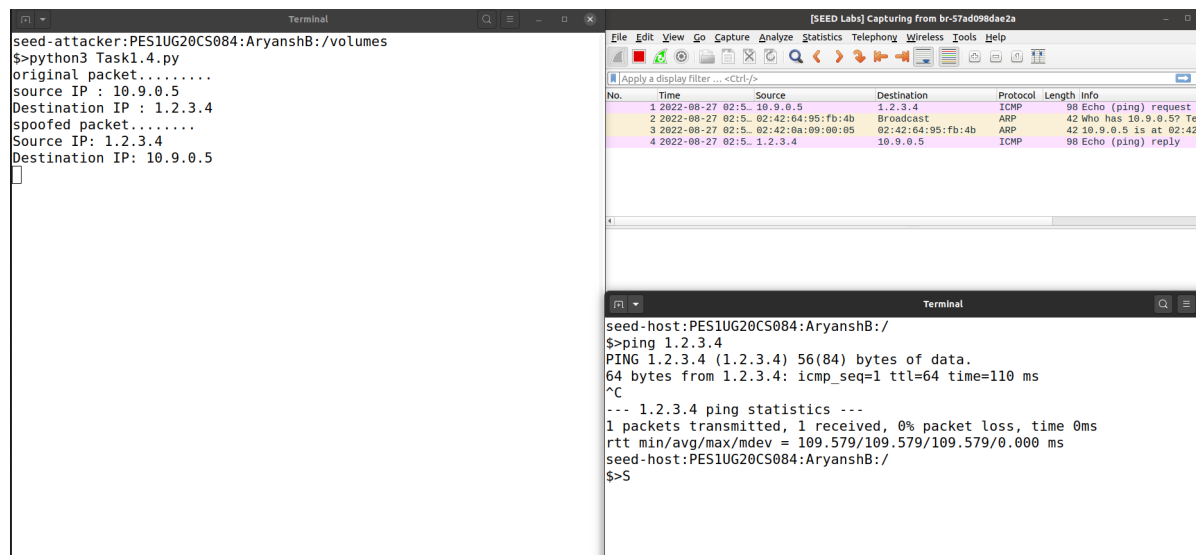
Unfortunately, traceroute was not working properly on college network and could not travel beyond a certain number of hops. I tried the same using my mobile data and home Wi-fi to no avail. Wireshark showed no captures and traceroute could only go travel one hop outside my subnet.

Screenshot for reference:



I tried writing my own traceroute program, which also faced a similar issue.

Task 1.4 Sniffing and then Spoofing



First we sniff a packet meant for IP address 1.2.3.4, then we use this packet and to send spoofed packets.