

## CNS LAB 2

### PACKET SNIFFING AND SPOOFING USING PCAP

**NAME: NAVYA PERAM**

**SRN: PES1UG21CS924**

**SEC: F**

#### Task 2.1 A

In this task, we are using a sniffer program with a pcap library to analyze and print the source and destination of each packet. The icmp packets sent and received are captured and various information, such as their header and IP protocol info are stored. Here, the ipheader and the ethheader are used to store information about the ip protocols and the ethernet header. The got\_packet() function, then extracts information about the packet into the two structures and then displays various info about the packet such as the protocol, source and destination ip addresses.



```
Activities Terminal Sep 16 13:07
seed@VM: ~/Labsetup2 seed@VM: - seed@VM: -/Labsetup1 seed@VM: -/Labsetup2

[09/16/23]seed@VM:~/Labsetup2$ docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED             STATUS              PORTS
1c026b86baac        handsonsecurity/seed-ubuntu:large "/bin/sh -c /bin/bash" 4 hours ago         Up 9 seconds
seed-attacker       26e9353073ff        handsonsecurity/seed-ubuntu:large "bash -c ' /etc/init_" 4 hours ago         Up 9 seconds
hostB-10.9.0.6      5a4baa401a91        handsonsecurity/seed-ubuntu:large "bash -c ' /etc/init_" 4 hours ago         Up 9 seconds
hostA-10.9.0.5

[09/16/23]seed@VM:~/Labsetup2$ docker cp Task2.1A.c 1c:/volumes
lstat /home/seed/Labsetup2/Task2.1A.c: no such file or directory
[09/16/23]seed@VM:~/Labsetup2$ docker cp Task2.1A.c 1c:/volumes
lstat /home/seed/Labsetup2/Task2.1A.c: no such file or directory
[09/16/23]seed@VM:~/Labsetup2$ docker cp Task2.1A.c 1c:/volumes
lstat /home/seed/Labsetup2/Task2.1A.c: no such file or directory
[09/16/23]seed@VM:~/Labsetup2$ cd Home
bash: cd: Home: No such file or directory
[09/16/23]seed@VM:~/Labsetup2$ cd..
cd..: command not found
[09/16/23]seed@VM:~/Labsetup2$ cd
[09/16/23]seed@VM:~$ docker cp Task2.1A.c 1c:/volumes
[09/16/23]seed@VM:~$ gcc -o sniff Task2.1A.c -lpcap
[09/16/23]seed@VM:~$ docker cp sniff 1c026b86baac:/volumes
[09/16/23]seed@VM:~$
```

```

[09/16/23] seed@VM: ~/Labsetup2$ docker ps
CONTAINER ID        IMAGE                                     COMMAND                  CREATED            STATUS            PORTS
1c026b86baac       handsonsecurity/seed-ubuntu:large       "/bin/sh -c /bin/bash"  4 hours ago       Up 9 seconds
seed-attacker      26e9353073ff       handsonsecurity/seed-ubuntu:large       "bash -c ' /etc/init_"  4 hours ago       Up 9 seconds
hostB-10.9.0.6     5a4baa401a91       handsonsecurity/seed-ubuntu:large       "bash -c ' /etc/init_"  4 hours ago       Up 9 seconds
hostA-10.9.0.5

[09/16/23] seed@VM: ~/Labsetup2$ docker cp Task2.1A.c 1c:/volumes
lsstat /home/seed/Labsetup2/Task2.1A.c: no such file or directory
[09/16/23] seed@VM: ~/Labsetup2$ docker cp Task2.1A.c 1c:/volumes
lsstat /home/seed/Labsetup2/Task2.1A.c: no such file or directory
[09/16/23] seed@VM: ~/Labsetup2$ docker cp Task2.1A.c 1c:/volumes
lsstat /home/seed/Labsetup2/Task2.1A.c: no such file or directory
[09/16/23] seed@VM: ~/Labsetup2$ cd Home
bash: cd: Home: No such file or directory
[09/16/23] seed@VM: ~/Labsetup2$ cd..
cd..: command not found
[09/16/23] seed@VM: ~/Labsetup2$ cd
[09/16/23] seed@VM: ~$ docker cp Task2.1A.c 1c:/volumes
[09/16/23] seed@VM: ~$ gcc -o sniff Task2.1A.c -lpcap
[09/16/23] seed@VM: ~$ docker cp sniff 1c026b86baac:/volumes
[09/16/23] seed@VM: ~$

```

```

root@5a4baa401a91:/# export PS1="hostA:PE51UG21CS924:Navya:\w\n\${}"
hostA:PE51UG21CS924:Navya:/
$>ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.9.0.5 netmask 255.255.255.0 broadcast 10.9.0.255
    ether 02:42:0a:09:00:05 txqueuelen 0 (Ethernet)
    RX packets 64 bytes 7866 (7.8 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

hostA:PE51UG21CS924:Navya:/
$>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=0.100 ms
64 bytes from 10.9.0.1: icmp_seq=2 ttl=64 time=0.097 ms
64 bytes from 10.9.0.1: icmp_seq=3 ttl=64 time=0.103 ms
64 bytes from 10.9.0.1: icmp_seq=4 ttl=64 time=0.099 ms
^C
--- 10.9.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3236ms
rtt min/avg/max/mdev = 0.097/0.099/0.103/0.002 ms
hostA:PE51UG21CS924:Navya:/
$>

```

# 1. The various functions are:

Pcap\_open\_live() - this is used to initiate the packet capture on the given interfaces.

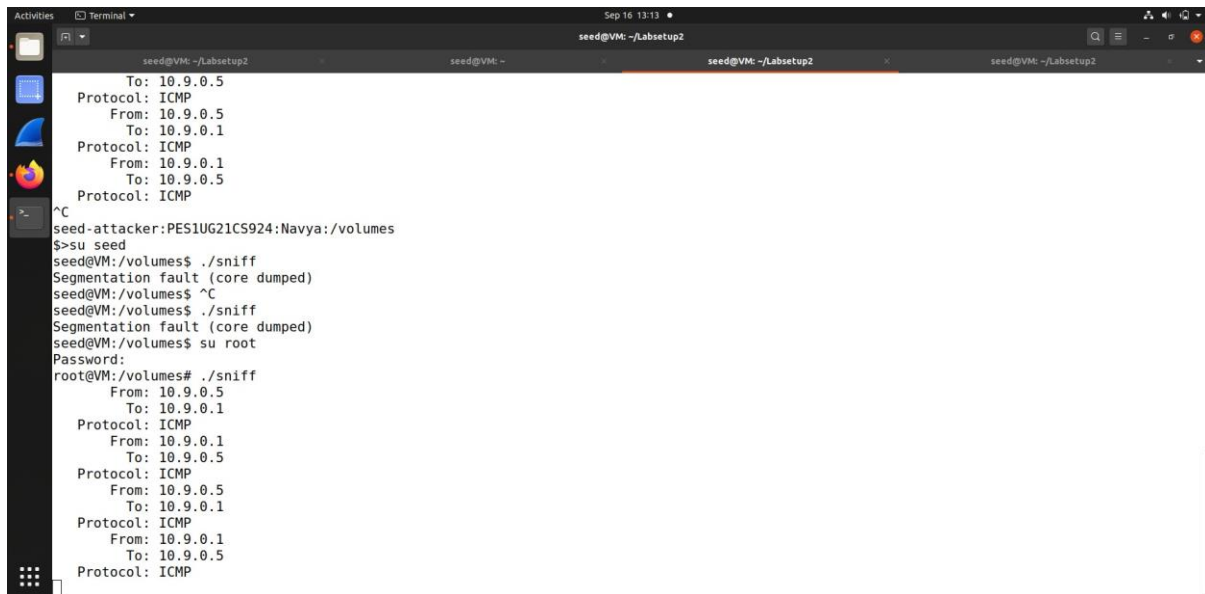
Pcap\_perror() – it is used to print error messages while debugging

Pcap\_compile - this reads the filter expression and then applies it to the packet capture

Pcap\_loop() – this is used repeatedly throughout the code whenever we need to capture packets and process them

Pcap\_close() – this function is used at the end, to stop packet capturing

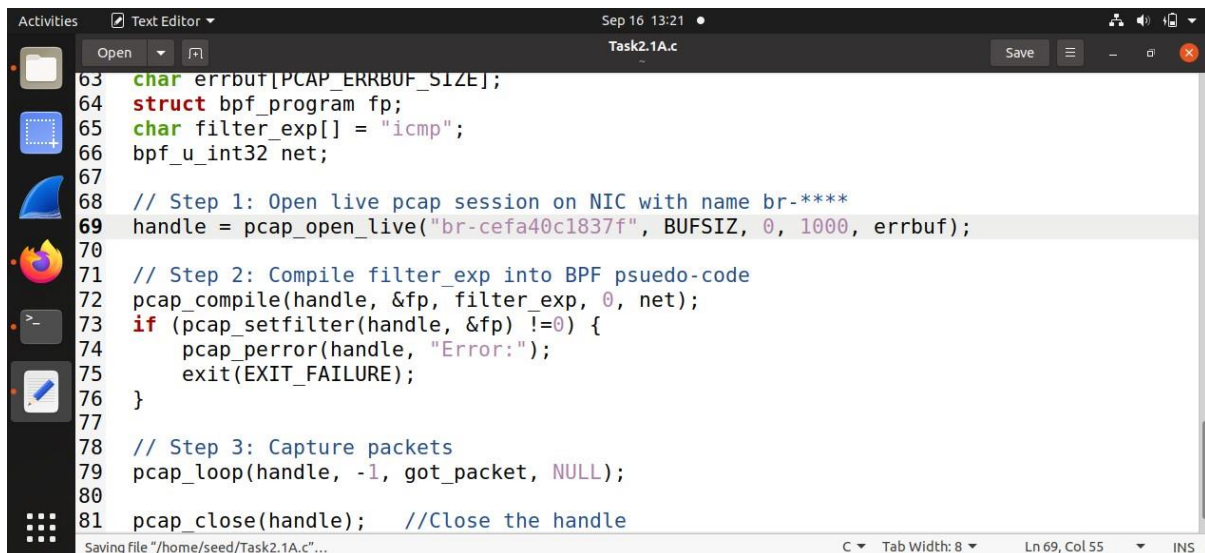
## 2. Without root



```
Activities Sep 16 13:13 seed@VM: ~/Labsetup2
To: 10.9.0.5
Protocol: ICMP
From: 10.9.0.5
To: 10.9.0.1
Protocol: ICMP
From: 10.9.0.1
To: 10.9.0.5
Protocol: ICMP
^C
seed-attacker: PES1UG21CS924:Navya:/volumes
$>su seed
seed@VM:/volumes$ ./sniff
Segmentation fault (core dumped)
seed@VM:/volumes$ ^C
seed@VM:/volumes$ ./sniff
Segmentation fault (core dumped)
seed@VM:/volumes$ su root
Password:
root@VM:/volumes# ./sniff
From: 10.9.0.5
To: 10.9.0.1
Protocol: ICMP
From: 10.9.0.1
To: 10.9.0.5
Protocol: ICMP
From: 10.9.0.5
To: 10.9.0.1
Protocol: ICMP
From: 10.9.0.1
To: 10.9.0.5
Protocol: ICMP
From: 10.9.0.5
To: 10.9.0.1
Protocol: ICMP
```

We cannot capture the packets in the absence of root privileges due to privacy and security concerns. There are no checks in this mode, which may allow unauthorized users from flooding the network with malicious or unnecessary packets. The program will not be able to access a raw socket.

## PROMISCUOUS MODE



```
Activities Sep 16 13:21 Task2.1A.c
63 char errbuf[PCAP_ERRBUF_SIZE];
64 struct bpf_program fp;
65 char filter_exp[] = "icmp";
66 bpf_u_int32 net;
67
68 // Step 1: Open live pcap session on NIC with name br-****
69 handle = pcap_open_live("br-cefa40c1837f", BUFSIZ, 0, 1000, errbuf);
70
71 // Step 2: Compile filter_exp into BPF psuedo-code
72 pcap_compile(handle, &fp, filter_exp, 0, net);
73 if (pcap_setfilter(handle, &fp) != 0) {
74     pcap_perror(handle, "Error:");
75     exit(EXIT_FAILURE);
76 }
77
78 // Step 3: Capture packets
79 pcap_loop(handle, -1, got_packet, NULL);
80
81 pcap_close(handle); //Close the handle
Saving file "/home/seed/Task2.1A.c"...
```

```

seed-attacker: PES1UG21CS924: Navya: /volumes
$> su seed
seed@VM: /volumes$ ./sniff
Segmentation fault (core dumped)
seed@VM: /volumes$ ^C
seed@VM: /volumes$ ./sniff
Segmentation fault (core dumped)
seed@VM: /volumes$ su root
Password:
root@VM: /volumes# ./sniff
  From: 10.9.0.5
  To: 10.9.0.1
  Protocol: ICMP
  From: 10.9.0.1
  To: 10.9.0.5
  Protocol: ICMP
  From: 10.9.0.5
  To: 10.9.0.1
  Protocol: ICMP
  From: 10.9.0.1
  To: 10.9.0.5
  Protocol: ICMP
^C
root@VM: /volumes# ./sniff

```

```

Activities Terminal Sep 16 13:24
seed@VM: ~/Labsetup2
seed@VM: ~/Labsetup2 x seed@VM: ~ x seed@VM: ~/Labsetup2 x seed@VM: ~/Labsetup2 x
64 bytes from 10.9.0.1: icmp_seq=1 ttl=64 time=0.071 ms
64 bytes from 10.9.0.1: icmp_seq=2 ttl=64 time=0.088 ms
^C
--- 10.9.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1027ms
rtt min/avg/max/mdev = 0.071/0.079/0.088/0.008 ms
hostA: PES1UG21CS924: Navya: /
$> ping 10.9.0.6
PING 10.9.0.6 (10.9.0.6) 56(84) bytes of data.
64 bytes from 10.9.0.6: icmp_seq=1 ttl=64 time=0.524 ms
64 bytes from 10.9.0.6: icmp_seq=2 ttl=64 time=0.108 ms
64 bytes from 10.9.0.6: icmp_seq=3 ttl=64 time=0.128 ms
^C
--- 10.9.0.6 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2055ms
rtt min/avg/max/mdev = 0.108/0.253/0.524/0.191 ms
hostA: PES1UG21CS924: Navya: /
$>

```

3. In the case of promiscuous mode, when it is turned on, all the packets sent in that particular network are captured. However, on turning it off, the packets which are sent between the host machine and the other machine are only captured.

## Task 2.1 B

### ICMP

This process is similar to the previous process, where the packets sent and received are captured. However, here only the packets sent and received between the hosts A and B are captured and the rest are ignored.





TCP

This process is also similar to the previous process, however, only the TCP packets sent between ports 10 and 100, between the given two machines are captured.

```
Activities terminal Sep 16 13:30 seed@VM: - seed@VM: - seed@VM: - seed@VM: -  
seed@VM: ~/Labsetup2  
[09/16/23]seed@VM:~/Labsetup2$ docker ps  
CONTAINER ID        IMAGE                                     COMMAND                  CREATED            STATUS             PORTS  
1c026b86baac       handsonsecurity/seed-ubuntu:large      "/bin/sh -c '/bin/bash'" 4 hours ago       Up 9 seconds  
seed-attacker      26e9353073ff                           "bash -c ' /etc/init..." 4 hours ago       Up 9 seconds  
hostB-10.9.0.6     5a4baa401a91                           "bash -c ' /etc/init..." 4 hours ago       Up 9 seconds  
hostA-10.9.0.5  
[09/16/23]seed@VM:~/Labsetup2$ docker cp Task2.1A.c 1c:/volumes  
lsstat /home/seed/Labsetup2/Task2.1A.c: no such file or directory  
[09/16/23]seed@VM:~/Labsetup2$ docker cp Task2.1A.c 1c:/volumes  
lsstat /home/seed/Labsetup2/Task2.1A.c: no such file or directory  
[09/16/23]seed@VM:~/Labsetup2$ docker cp Task2.1A.c 1c:/volumes  
lsstat /home/seed/Labsetup2/Task2.1A.c: no such file or directory  
[09/16/23]seed@VM:~/Labsetup2$ cd Home  
bash: cd: Home: No such file or directory  
[09/16/23]seed@VM:~/Labsetup2$ cd..  
cd.: command not found  
[09/16/23]seed@VM:~/Labsetup2$ cd  
[09/16/23]seed@VM:~$ docker cp Task2.1A.c 1c:/volumes  
[09/16/23]seed@VM:~$ gcc -o sniff Task2.1A.c -lpcap  
[09/16/23]seed@VM:~$ docker cp sniff 1c026b86baac:/volumes  
[09/16/23]seed@VM:~$ gcc -o sniff Task2.1A.c -lpcap  
[09/16/23]seed@VM:~$ docker cp sniff 1c026b86baac:/volumes  
[09/16/23]seed@VM:~$ gcc -o sniff Task2.1B-ICMP.c -lpcap  
[09/16/23]seed@VM:~$ docker cp sniff 1c026b86baac:/volumes  
[09/16/23]seed@VM:~$ gcc -o sniff Task2.1B-TCP.c -lpcap  
[09/16/23]seed@VM:~$ docker cp sniff 1c026b86baac:/volumes  
[09/16/23]seed@VM:~$
```

[illegible]

```
Activities Terminal Sep 16 13:38
seed@VM: ~/Labsetup2
26e9353073ff login: dees
Password:
^CConnection closed by foreign host.
hostA:PES1UG21CS924:Navya:/
$>telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
26e9353073ff login: SEED
Password:

Login incorrect
26e9353073ff login: ^CConnection closed by foreign host.
hostA:PES1UG21CS924:Navya:/
$>
```

## Task 2.1C :SNIFFING PASSWORDS

In the given process, the BPF filter is set to the telnet port, which is 23. Hence, only the telnet packets are captured and displayed. Since, telnet also has the ability of remote monitoring, we can view all the information on the Host A's screen along with the password given there, as shown in the photos.

```
Activities Terminal Sep 16 14:10
seed@VM: ~/Labsetup2
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 303 bytes 28510 (28.5 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

seed-attacker:PES1UG21CS924:Navya:/
$>cd volumes\
> ^C
seed-attacker:PES1UG21CS924:Navya:/
$>cd volumes/
seed-attacker:PES1UG21CS924:Navya:/volumes
$>./sniff
00000000 00:00:00 000000 00:00 000000!00*0000#0000 0000 00000000 00000000Ubuntu 20.04.1 LTS
00026e9353073ff login: sseeeedd
Password: dees
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sat Sep 16 17:44:30 UTC 2023 from hostA-10.9.0.5.net-10.9.0.0 on pts/1
unminimize
0seed@26e9353073ff:~$ unnnmiinniimmiizzee

0CThis system has been minimized by removing packages and content that are
not required on a system that users do not log into.0

This script restores content and packages that are found on a default
```

```
Activities Terminal Sep 16 14:10
seed@VM: ~/Labsetup2 seed@VM: seed@VM: seed@VM: seed@VM:
26e9353073ff login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sat Sep 16 18:04:14 UTC 2023 from 26e9353073ff on pts/4
seed@26e9353073ff:~$ telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^'.
Ubuntu 20.04.1 LTS
26e9353073ff login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sat Sep 16 18:05:00 UTC 2023 from 26e9353073ff on pts/5
seed@26e9353073ff:~$
```

## Task 2.2: SPOOFING

```
Activities Terminal Sep 16 14:24
seed@VM: ~/Labsetup2 seed@VM: seed@VM: seed@VM: seed@VM:
seed-attacker
26e9353073ff handsonsecurity/seed-ubuntu:large "bash -c ' /etc/init..." 4 hours ago Up 9 seconds
hostB-10.9.0.6
5a4baa401a91 handsonsecurity/seed-ubuntu:large "bash -c ' /etc/init..." 4 hours ago Up 9 seconds
hostA-10.9.0.5
[09/16/23]seed@VM:~/Labsetup2$ docker cp Task2.1A.c 1c:/volumes
lsstat /home/seed/Labsetup2/Task2.1A.c: no such file or directory
[09/16/23]seed@VM:~/Labsetup2$ docker cp Task2.1A.c 1c:/volumes
lsstat /home/seed/Labsetup2/Task2.1A.c: no such file or directory
[09/16/23]seed@VM:~/Labsetup2$ docker cp Task2.1A.c 1c:/volumes
lsstat /home/seed/Labsetup2/Task2.1A.c: no such file or directory
[09/16/23]seed@VM:~/Labsetup2$ cd Home
bash: cd: Home: No such file or directory
[09/16/23]seed@VM:~/Labsetup2$ cd..
cd..: command not found
[09/16/23]seed@VM:~/Labsetup2$ cd
[09/16/23]seed@VM:~$ docker cp Task2.1A.c 1c:/volumes
[09/16/23]seed@VM:~$ gcc -o sniff Task2.1A.c -lpcap
[09/16/23]seed@VM:~$ docker cp sniff 1c026b86baac:/volumes
[09/16/23]seed@VM:~$ gcc -o sniff Task2.1A.c -lpcap
[09/16/23]seed@VM:~$ docker cp sniff 1c026b86baac:/volumes
[09/16/23]seed@VM:~$ gcc -o sniff Task2.1B-ICMP.c -lpcap
[09/16/23]seed@VM:~$ docker cp sniff 1c026b86baac:/volumes
[09/16/23]seed@VM:~$ gcc -o sniff Task2.1B-TCP.c -lpcap
[09/16/23]seed@VM:~$ docker cp sniff 1c026b86baac:/volumes
[09/16/23]seed@VM:~$ gcc -o sniff Task2.1C.c -lpcap
[09/16/23]seed@VM:~$ docker cp sniff 1c026b86baac:/volumes
[09/16/23]seed@VM:~$ gcc -o spooficmp Task2.2.c -lpcap
[09/16/23]seed@VM:~$ docker cp sniff 1c026b86baac:/volumes
[09/16/23]seed@VM:~$ gcc -o spooficmp Task2.2.c -lpcap
[09/16/23]seed@VM:~$ docker cp spooficmp 1c026b86baac:/volumes
[09/16/23]seed@VM:~$
```



```

seed@VM: ~$ cat /dev/net/tun
TX packets 31965 bytes 17997124 (17.9 MB)
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
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 9947 bytes 760090 (760.0 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 9947 bytes 760090 (760.0 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

veth253bcc5: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet6 fe80::344a:b6ff:fe69:48da prefixlen 64 scopeid 0x20<link>
ether 36:4a:b6:69:48:da txqueuelen 0 (Ethernet)
RX packets 630 bytes 42516 (42.5 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 607 bytes 54796 (54.7 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

veth4713a9c: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet6 fe80::d8c5:c9ff:fee9:658e prefixlen 64 scopeid 0x20<link>
ether da:c5:c9:e9:65:8e txqueuelen 0 (Ethernet)
RX packets 465 bytes 36863 (36.8 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 752 bytes 58869 (58.8 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

seed-attacker: PES1UG21CS924:Navya:/volumes
$> ./spooficmp
seed-attacker: PES1UG21CS924:Navya:/volumes
$>

```

```

Activities Wireshark Sep 16 14:25 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 0.000000000 02:42:f3:49:6b:9d Broadcast ARP 42 Who has 10.9.0.6? Tell 10.9.0.1
2 0.000054421 02:42:0a:09:00:06 02:42:f3:49:6b:9d ARP 42 10.9.0.6 is at 02:42:0a:09:00:06
3 0.000067166 1.2.3.4 10.9.0.6 ICMP 42 Echo (ping) request id=0x0000, seq=0/0, ttl=20 (reply in 4)
4 0.000093287 10.9.0.6 1.2.3.4 ICMP 42 Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 3)
5 5.181716068 02:42:0a:09:00:06 02:42:f3:49:6b:9d ARP 42 Who has 10.9.0.1? Tell 10.9.0.6
6 5.182025249 02:42:f3:49:6b:9d 02:42:0a:09:00:06 ARP 42 10.9.0.1 is at 02:42:f3:49:6b:9d

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface br-cefa40c1837f, id 0
Ethernet II, Src: 02:42:f3:49:6b:9d (02:42:f3:49:6b:9d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

0000 ff ff ff ff ff ff 02 42 f3 49 6b 9d 08 06 00 01 .....B..Ik....
0010 08 00 06 04 00 01 02 42 f3 49 6b 9d 0a 09 00 01 .....B..Ik....
0020 00 00 00 00 00 00 0a 09 00 06 .....

```

In the above process, icmp packets are spoofed and are sent. We use the `in_chksm()` function in the code, to calculate the checksum values of the icmp protocol. The packet we spoofed is shown to have a source IP address of 1.2.3.4 and is shown to be sent to the destination 10.9.0.6, which is our host B.

4. No, we don't need to calculate the checksum for the IP headers as this is already done by the system. In case, there is an occurrence of an incorrect value, then the system would calculate and correct it and then replace it with the right value.

5. We need the root privilege to run the programs in promiscuous mode and to implement raw sockets. When we run a program in the absence of the root privilege, then it will fail at the socket setup stage .

## Task 2.3: SNIFF AND SPOOF

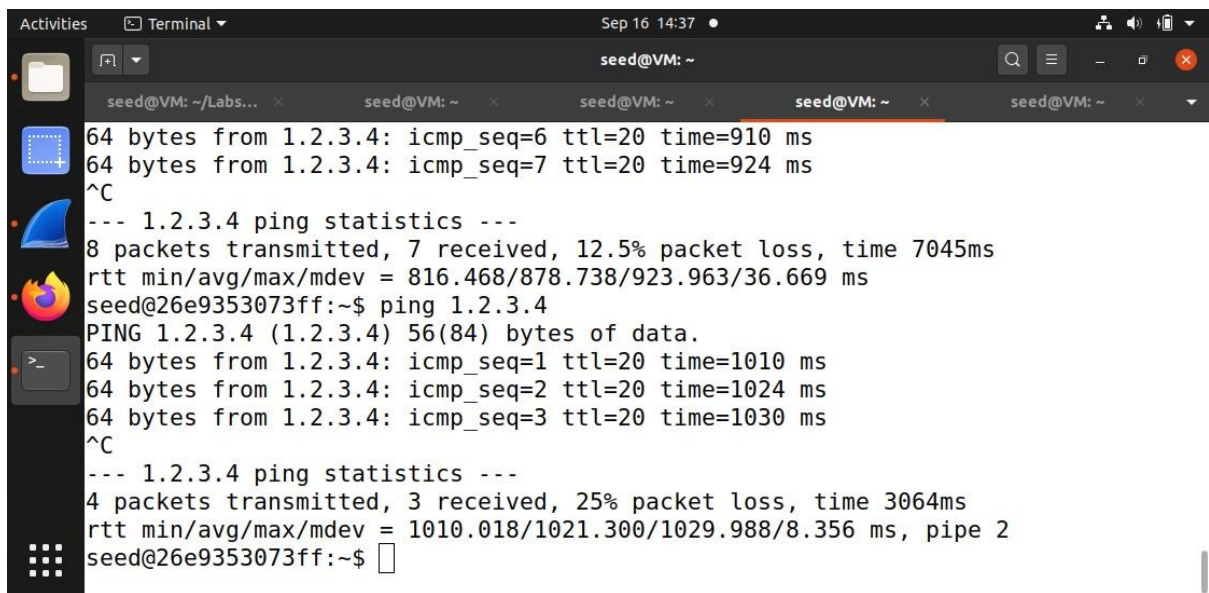
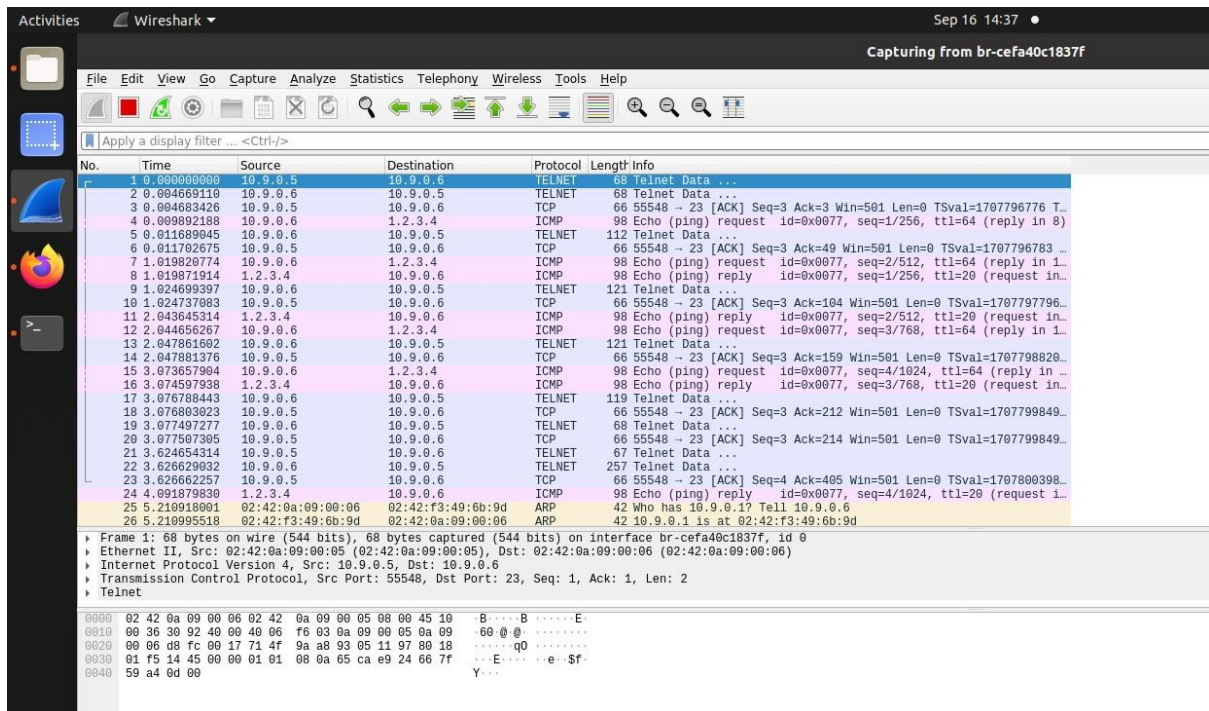
In the given process, all the icmp packets which are sent and received are captured. We use various structures such as ipheader, ethheader and the icmpheader to store information about their respective protocols – ip, ethernet and icmp. Similar to the codes in the above processes, the `in_chksum()` calculates the checksum for both the ip and icmp protocols and the `got_packet()` function once on receiving the packet, it extracts the information and displays the source and destination ip addresses along with the packet protocol. We also use the `send_raw_ip_packet()`, to spoof a packet by creating a raw socket and then sending the spoofed packet through it. Since, we have both the attacker and the hosts on the same network, an attacker can easily sniff any packet and spoof a reply immediately, which can be confused by the host as of an actual reply sent by the ip address it has pinged.

The image shows a Wireshark network traffic capture. The top bar indicates the capture is from interface `br-cefa40c1837f`. The main pane displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Length. The packet list shows various ICMP ping requests and replies, Telnet data, and ARP requests. The packet details pane for packet 1 shows the frame structure and the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.009892188	10.9.0.6	1.2.3.4	ICMP	98	Echo (ping) request id=0x0077, seq=1/256, ttl=64 (reply in 8)
5	0.011889045	10.9.0.6	10.9.0.5	Telnet	112	Telnet Data ...
6	0.011702675	10.9.0.5	10.9.0.6	TCP	66	55548 → 23 [ACK] Seq=3 Ack=49 Win=501 Len=0 TSval=1707796783 ...
7	1.019820774	10.9.0.6	1.2.3.4	ICMP	98	Echo (ping) request id=0x0077, seq=2/512, ttl=64 (reply in 1..
8	1.019871914	1.2.3.4	10.9.0.6	ICMP	98	Echo (ping) reply id=0x0077, seq=1/256, ttl=20 (request in..
9	1.024699397	10.9.0.6	10.9.0.5	Telnet	121	Telnet Data ...
10	1.024737083	10.9.0.5	10.9.0.6	TCP	66	55548 → 23 [ACK] Seq=3 Ack=104 Win=501 Len=0 TSval=1707797796..
11	2.043645314	1.2.3.4	10.9.0.6	ICMP	98	Echo (ping) request id=0x0077, seq=2/512, ttl=20 (request in..
12	2.044656267	10.9.0.6	1.2.3.4	ICMP	98	Echo (ping) request id=0x0077, seq=3/768, ttl=64 (reply in 1..
13	2.047861602	10.9.0.6	10.9.0.5	Telnet	121	Telnet Data ...
14	2.047881376	10.9.0.5	10.9.0.6	TCP	66	55548 → 23 [ACK] Seq=3 Ack=159 Win=501 Len=0 TSval=1707798820..
15	3.073657904	10.9.0.6	1.2.3.4	ICMP	98	Echo (ping) request id=0x0077, seq=4/1024, ttl=64 (reply in ..
16	3.074597938	1.2.3.4	10.9.0.6	ICMP	98	Echo (ping) reply id=0x0077, seq=3/768, ttl=20 (request in..
17	3.076788443	10.9.0.6	10.9.0.5	Telnet	119	Telnet Data ...
18	3.076803023	10.9.0.5	10.9.0.6	TCP	66	55548 → 23 [ACK] Seq=3 Ack=212 Win=501 Len=0 TSval=1707799849..
19	3.077497277	10.9.0.6	10.9.0.5	Telnet	68	Telnet Data ...
20	3.077507305	10.9.0.5	10.9.0.6	TCP	66	55548 → 23 [ACK] Seq=3 Ack=214 Win=501 Len=0 TSval=1707799849..
21	3.624654314	10.9.0.5	10.9.0.6	Telnet	67	Telnet Data ...
22	3.626629032	10.9.0.6	10.9.0.5	Telnet	257	Telnet Data ...
23	3.626662257	10.9.0.5	10.9.0.6	TCP	66	55548 → 23 [ACK] Seq=4 Ack=405 Win=501 Len=0 TSval=1707800398..
24	4.091879830	1.2.3.4	10.9.0.6	ICMP	98	Echo (ping) reply id=0x0077, seq=4/1024, ttl=20 (request i..
25	5.210918001	02:42:0a:09:00:06	02:42:f3:49:6b:9d	ARP	42	Who has 10.9.0.1? Tell 10.9.0.6
26	5.210995518	02:42:f3:49:6b:9d	02:42:0a:09:00:06	ARP	42	10.9.0.1 is at 02:42:f3:49:6b:9d
27	6.238900717	02:42:f3:49:6b:9d	02:42:0a:09:00:06	ARP	42	Who has 10.9.0.6? Tell 10.9.0.1
28	6.239038687	02:42:0a:09:00:06	02:42:f3:49:6b:9d	ARP	42	10.9.0.6 is at 02:42:0a:09:00:06

Frame 1: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface br-cefa40c1837f, id 0  
Ethernet II, Src: 02:42:0a:09:00:05 (02:42:0a:09:00:05), Dst: 02:42:0a:09:00:06 (02:42:0a:09:00:06)  
Internet Protocol Version 4, Src: 10.9.0.5, Dst: 10.9.0.6  
Transmission Control Protocol, Src Port: 55548, Dst Port: 23, Seq: 1, Ack: 1, Len: 2  
Telnet

```
0000 02 42 0a 09 00 06 02 42 0a 09 00 05 08 00 45 10  B...B...E
0010 00 36 30 92 40 00 40 06 f6 03 0a 09 00 05 0a 09  60 @ @...
0020 00 06 d8 fc 00 17 71 4f 9a a8 93 05 11 97 80 18  ....q0....
0030 01 f5 14 45 00 00 01 01 08 0a 65 ca e9 24 66 7f  ..E...e:$f
0040 59 a4 0d 00                                     Y...
```



```
Activities Terminal Sep 16 14:37
seed@VM: ~/Labsetup2 seed@VM: - seed@VM: - seed@VM: - seed@VM: -
Protocol: ICMP
From: 1.2.3.4
To: 10.9.0.6
Protocol: ICMP
^C
seed-attacker: PES1UG21CS924: Navya: /volumes
$> ./sniffspoofer
From: 10.9.0.6
To: 1.2.3.4
Protocol: ICMP
From: 10.9.0.6
To: 1.2.3.4
Protocol: ICMP
From: 1.2.3.4
To: 10.9.0.6
Protocol: ICMP
From: 1.2.3.4
To: 10.9.0.6
Protocol: ICMP
From: 10.9.0.6
To: 1.2.3.4
Protocol: ICMP
From: 10.9.0.6
To: 1.2.3.4
Protocol: ICMP
From: 1.2.3.4
To: 10.9.0.6
Protocol: ICMP
From: 1.2.3.4
To: 10.9.0.6
Protocol: ICMP
From: 1.2.3.4
To: 10.9.0.6
Protocol: ICMP
```