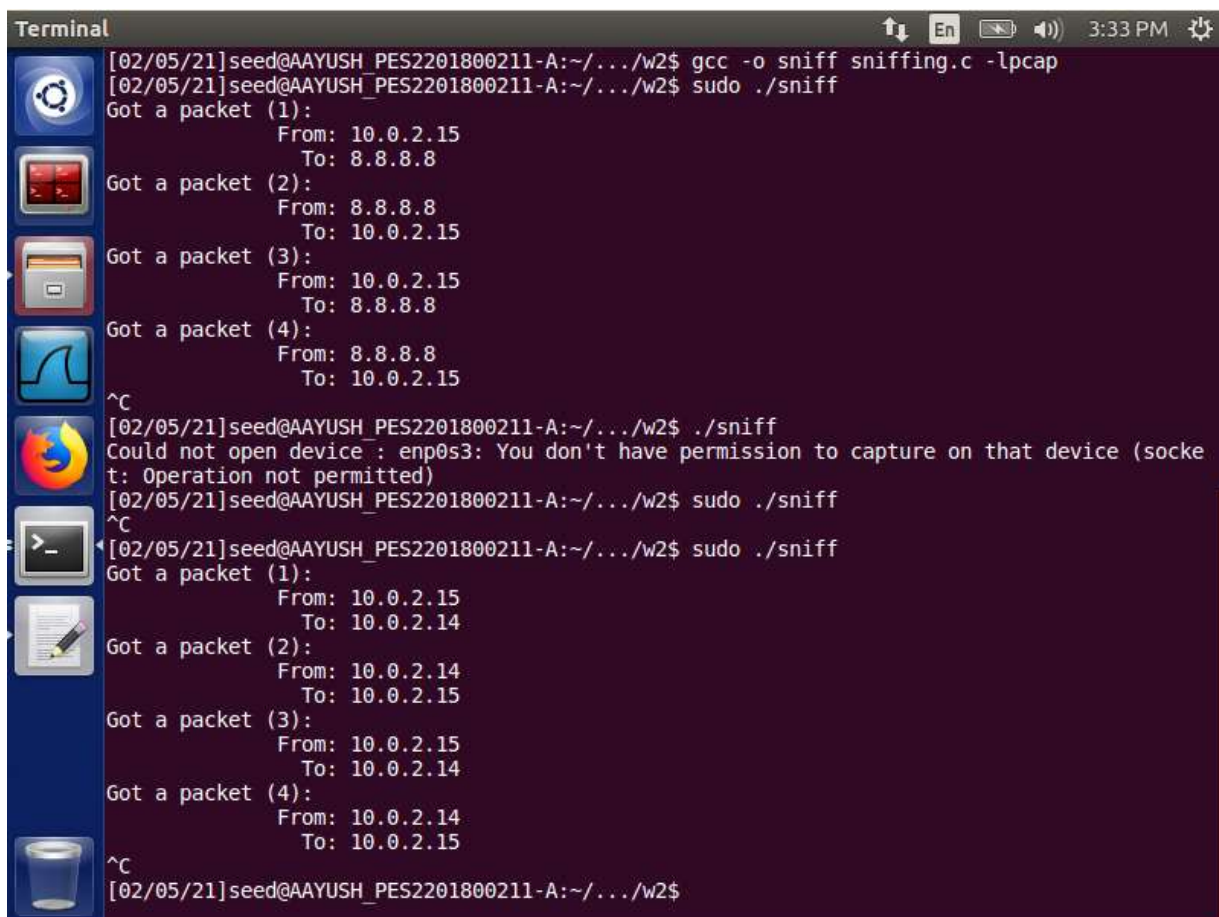


PES UNIVERSITY
COMPUTER SECURITY LAB
WEEK 2
Aayush Kapoor PES2201800211

NOTE : *seed@AAYUSH_PES2201800211-A -> Attacker machine*
seed@AAYUSH_PES2201800211-V -> Victim machine

TASK 1:



```
Terminal
[02/05/21]seed@AAYUSH_PES2201800211-A:~/.../w2$ gcc -o sniff sniffing.c -lpcap
[02/05/21]seed@AAYUSH_PES2201800211-A:~/.../w2$ sudo ./sniff
Got a packet (1):
    From: 10.0.2.15
    To: 8.8.8.8
Got a packet (2):
    From: 8.8.8.8
    To: 10.0.2.15
Got a packet (3):
    From: 10.0.2.15
    To: 8.8.8.8
Got a packet (4):
    From: 8.8.8.8
    To: 10.0.2.15
^C
[02/05/21]seed@AAYUSH_PES2201800211-A:~/.../w2$ ./sniff
Could not open device : enp0s3: You don't have permission to capture on that device (socket: Operation not permitted)
[02/05/21]seed@AAYUSH_PES2201800211-A:~/.../w2$ sudo ./sniff
^C
[02/05/21]seed@AAYUSH_PES2201800211-A:~/.../w2$ sudo ./sniff
Got a packet (1):
    From: 10.0.2.15
    To: 10.0.2.14
Got a packet (2):
    From: 10.0.2.14
    To: 10.0.2.15
Got a packet (3):
    From: 10.0.2.15
    To: 10.0.2.14
Got a packet (4):
    From: 10.0.2.14
    To: 10.0.2.15
^C
[02/05/21]seed@AAYUSH_PES2201800211-A:~/.../w2$
```

```
[02/05/21]seed@AAYUSH_PES2201800211-V:~/.../w2$ ping 8.8.8.8 -c 2
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=119 time=153 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=119 time=171 ms

--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 153.414/162.598/171.782/9.184 ms
[02/05/21]seed@AAYUSH_PES2201800211-V:~/.../w2$
```

1. First we defined the device and the interface from which capturing will begin, this is either defined in the sniffer program or the program looks up for active devices by itself via **pcap_lookupdev**. After the device has been initialized, the sniffer program sends a signal to set up a session for sniffing. Sniffer program requires filtering that helps in sniffing only a certain type of packets from many packets in the network (here we used ICMP filtering).

Now the packets can be sniffed and displayed to the user either by sniffing a packet and analysing it individually or by sniffing n packets and analyzing the entire group of packets and the last step is termination of the sniffer program.

2. Some functions (like pcap_lookupdev) in the sniffer program require root permission as it requires access to the network interface. Sniffer programs need access to raw sockets which is not possible without root permission.

```
[02/05/21]seed@AAYUSH_PES2201800211-A:~/.../w2$ ./sniff
Could not open device: enp0s3: You don't have permission to capture on that device (socket: Operation not permitted)
[02/05/21]seed@AAYUSH_PES2201800211-A:~/.../w2$
```

3. Promiscuous mode is used to allow the network sniffer to pass all the traffic in the network and not just the packets that are to be received by the network controller. This mode can be changed in pcap_open_live function and can vary from 1 -> 0 or vice versa. It will capture the packets only if the victim pings directly to the attacker's IP (Shown below with screenshots of victim's machine).

```
handle = pcap_open_live("enp0s3", SNAP_LEN, 1, 1000, errbuf); -> ON
handle = pcap_open_live("enp0s3", SNAP_LEN, 0, 1000, errbuf); -> OFF
```

```
[02/05/21]seed@AAYUSH_PES2201800211-V:~/.../w2$ ping 8.8.8.8 -c 2
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=119 time=109 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=119 time=58.1 ms

--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 58.136/83.884/109.633/25.750 ms
[02/05/21]seed@AAYUSH_PES2201800211-V:~/.../w2$
```

```
[02/05/21]seed@AAYUSH_PES2201800211-V:~/.../w2$ ping 10.0.2.14 -c 2
PING 10.0.2.14 (10.0.2.14) 56(84) bytes of data.
64 bytes from 10.0.2.14: icmp_seq=1 ttl=64 time=1.03 ms
64 bytes from 10.0.2.14: icmp_seq=2 ttl=64 time=1.33 ms

--- 10.0.2.14 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 1.038/1.185/1.333/0.151 ms
[02/05/21]seed@AAYUSH_PES2201800211-V:~/.../w2$
```

TASK 1.2B:

```

Terminal
[02/05/21]seed@AAYUSH_PES2201800211-A:~/.../w2$ nano sniffing.c
[02/05/21]seed@AAYUSH_PES2201800211-A:~/.../w2$ gcc -o sniffb1 sniffing.c -lpcap
[02/05/21]seed@AAYUSH_PES2201800211-A:~/.../w2$ sudo ./sniffb1
Got a packet (1):
      From: 10.0.2.15
      To: 10.0.2.2
Got a packet (2):
      From: 10.0.2.2
      To: 10.0.2.15
Got a packet (3):
      From: 10.0.2.15
      To: 10.0.2.2
Got a packet (4):
      From: 10.0.2.2
      To: 10.0.2.15
^C
[02/05/21]seed@AAYUSH_PES2201800211-A:~/.../w2$ nano sniffing.c nano sniffing.c
[02/05/21]seed@AAYUSH_PES2201800211-A:~/.../w2$ gcc -o sniffb2 sniffing.c -lpcap
[02/05/21]seed@AAYUSH_PES2201800211-A:~/.../w2$ sudo ./sniffb2
Got a packet (1):
      From: 10.0.2.15
      To: 10.0.2.3
^C
[02/05/21]seed@AAYUSH_PES2201800211-A:~/.../w2$ sudo ./sniffb2
Got a packet (1):
      From: 10.0.2.15
      To: 10.0.2.3
^C
[02/05/21]seed@AAYUSH_PES2201800211-A:~/.../w2$

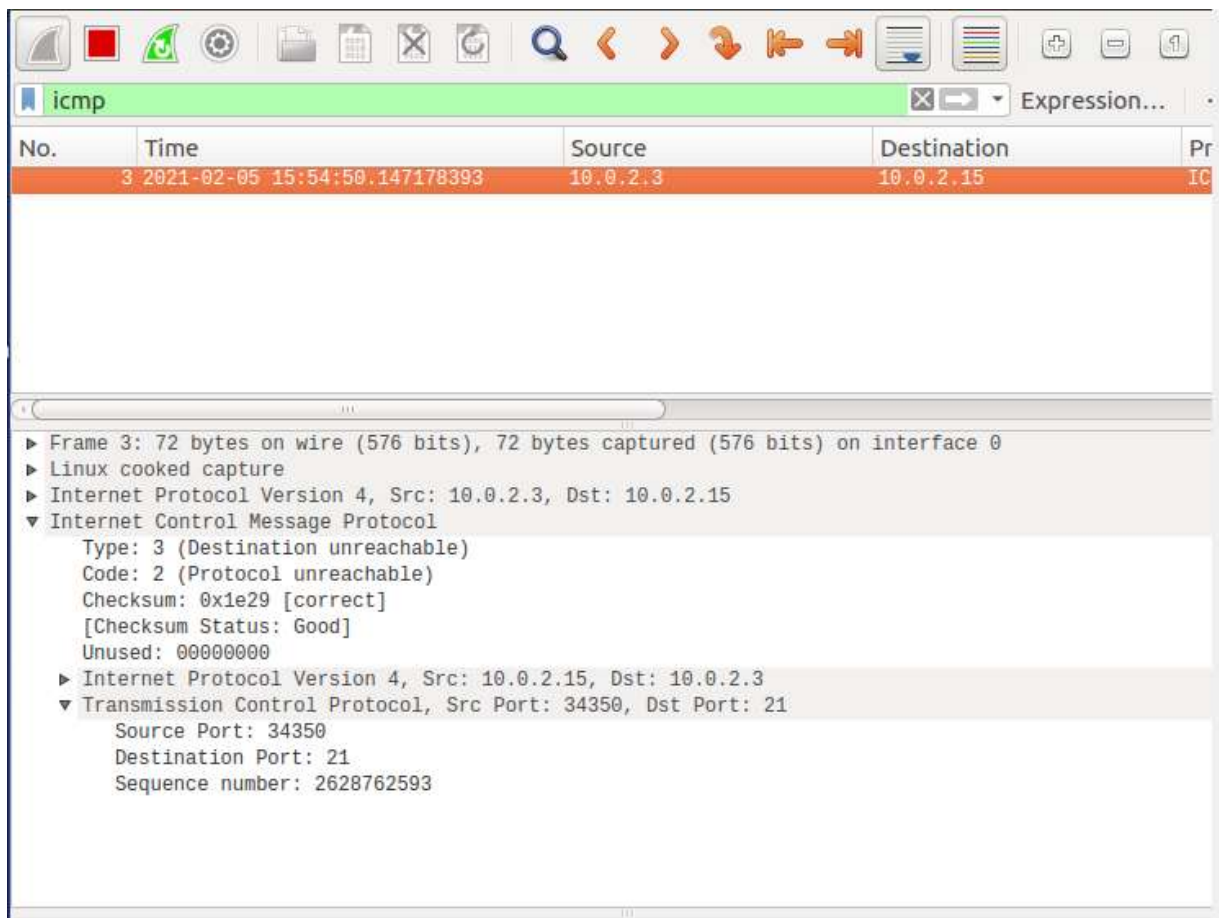
```

```

Terminal
[02/05/21]seed@AAYUSH_PES2201800211-V:~/.../w2$ ping 10.0.2.2 -c 2
PING 10.0.2.2 (10.0.2.2) 56(84) bytes of data:
64 bytes from 10.0.2.2: icmp_seq=1 ttl=128 time=1.08 ms
64 bytes from 10.0.2.2: icmp_seq=2 ttl=128 time=0.686 ms

--- 10.0.2.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.686/0.886/1.087/0.202 ms
[02/05/21]seed@AAYUSH_PES2201800211-V:~/.../w2$ ftp 10.0.2.3
ftp: connect: Protocol not available
ftp> ^C
ftp> ^Z
[2]+  Stopped                  ftp 10.0.2.3
[02/05/21]seed@AAYUSH_PES2201800211-V:~/.../w2$ ftp 10.0.2.3
ftp: connect: Protocol not available
ftp> ^Z
[3]+  Stopped                  ftp 10.0.2.3
[02/05/21]seed@AAYUSH_PES2201800211-V:~/.../w2$

```

Source port - 34350

Destination port - 21

TASK 1.3C:

```
Source Port: 56464
Destination Port: 23
Protocol: TCP
Payload: 1 bytes
00000 64 d
Got a packet (22):
From: 10.0.2.9
To: 10.0.2.15
Source Port: 56464
Destination Port: 23
Protocol: TCP
Payload: 1 bytes
00000 65 e
Got a packet (23):
From: 10.0.2.9
To: 10.0.2.15
Source Port: 56464
Destination Port: 23
Protocol: TCP
Payload: 1 bytes
00000 65 e
Got a packet (24):
From: 10.0.2.9
To: 10.0.2.15
Source Port: 56464
Destination Port: 23
Protocol: TCP
Payload: 1 bytes
00000 73 s
Got a packet (25):
From: 10.0.2.9
To: 10.0.2.15
Source Port: 56464
Destination Port: 23
Protocol: TCP
```

Below is a third machine with **seed@PES2201800211** - where I have executed telnet command to get the remote login of victim's machine whose password is sniffed by the sniffer program.

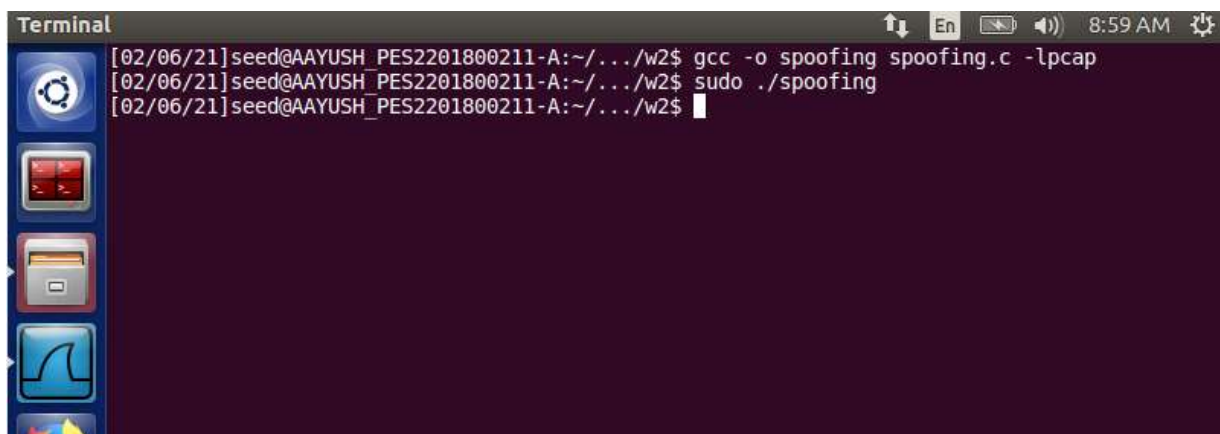
```
[02/06/21]seed@PES2201800211:~$ telnet 10.0.2.15
Trying 10.0.2.15...
Connected to 10.0.2.15.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
AAYUSH PES2201800211-V login: seed
Password:
Last login: Fri Feb  5 18:26:36 EST 2021 from 10.0.2.9 on pts/18
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

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

PS1: command not found
[02/06/21]seed@AAYUSH_PES2201800211-V:~$
```

TASK 2.2:

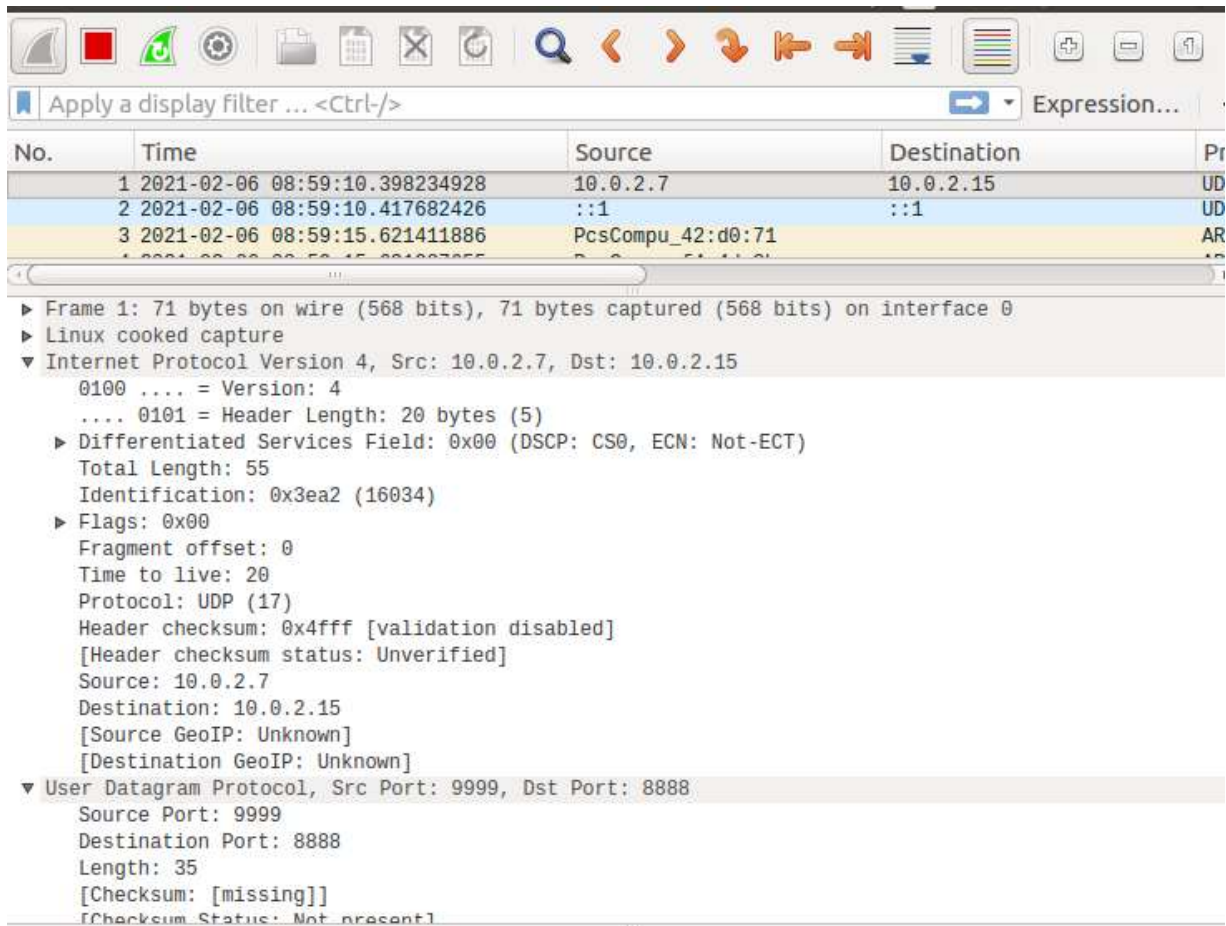
A terminal window titled "Terminal" with a dark background and light text. The window shows three lines of command execution. The first line is a gcc command to compile a file named 'spoofing.c' into 'spoofing' using the 'lpcap' library. The second line is a sudo command to run the compiled 'spoofing' program. The third line shows the prompt after the command has finished. On the left side of the terminal, there is a vertical dock with several application icons. The top status bar of the window shows system icons and the time "8:59 AM".

```
Terminal
[02/06/21]seed@AAYUSH_PES2201800211-A:~/.../w2$ gcc -o spoofing spoofing.c -lpcap
[02/06/21]seed@AAYUSH_PES2201800211-A:~/.../w2$ sudo ./spoofing
[02/06/21]seed@AAYUSH_PES2201800211-A:~/.../w2$
```

Attacker machine executed the spoofing program.

```
[02/06/21]seed@AAYUSH_PES2201800211-V:~/.../w2$ nc -l -p 8888
Listening on [0.0.0.0] (family 0, port 8888)
This is a spoofed packet
```

Victim machine getting spoofed packet response via netcat (utility tool).



Wireshark captured the packet and the source port - 9999 and destination port - 8888.