# Sniffing and Spoofing using PCAP Library

## CNS Lab2

### Aryansh Bhargavan

### PES1UG20CS084

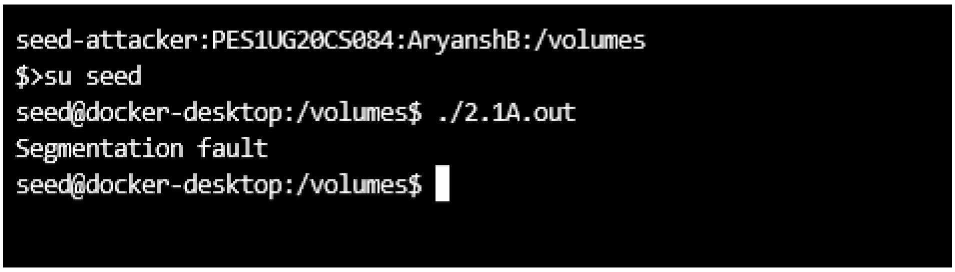
---

- ### Task 2.1 A : Understanding how a Sniffer Works

  - `Question 1: Please use your own words to describe the sequence of the library calls that are essential for sniffer programs. This is meant to be a summary, not detailed explanation like the one in the tutorial`

    - First we open a live pcap session with a specific interface name `pcap_open_live()`
    - We then set traffic filter as `` `icmp `` and convert to Berkley Packet Filter pseudo code `pcap_compile()`
    - Then we begin capturing packets and execute the sniff `lol`

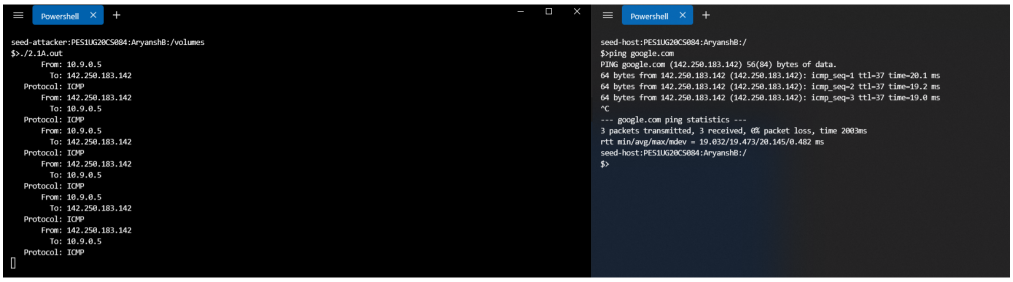
  - `Question 2: Why do you need the root privilege to run sniffex? Where does the program fail if executed without the root privilege?`

    - Since a Network Interface is being accessed, root privileges are required.
    - 

```
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>su seed
seed@docker-desktop:/volumes$ ./2.1A.out
Segmentation fault
seed@docker-desktop:/volumes$
```

  - `Question 3: Please turn on and turn off the promiscuous mode in your sniffer program. The value 1 of the third parameter in the pcap_open_live() function turns on the promiscuous mode (use 0 to turn it off). Can you demonstrate the difference when this mode is on and off? Change the code given in line 69 of Task2.1A.c file to the following : handle = pcap_open_live("br-****", BUFSIZ, 0, 1000, errbuf);`

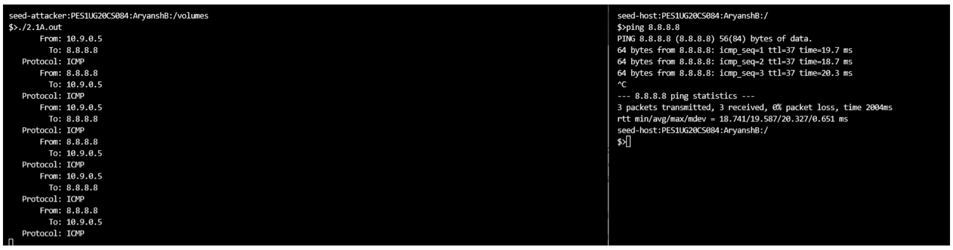
    - Promiscous mode turned off:



```
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>./2.1A.out
       From: 10.9.0.5
         To: 142.250.183.142
   Protocol: ICMP
       From: 142.250.183.142
         To: 10.9.0.5
   Protocol: ICMP
       From: 10.9.0.5
         To: 142.250.183.142
   Protocol: ICMP
       From: 142.250.183.142
         To: 10.9.0.5
   Protocol: ICMP
       From: 10.9.0.5
         To: 142.250.183.142
   Protocol: ICMP
       From: 142.250.183.142
         To: 10.9.0.5
   Protocol: ICMP
```

```
seed-host:PES1UG20CS084:AryanshB:/
$>ping google.com
PING google.com (142.250.183.142) 56(84) bytes of data.
64 bytes from 142.250.183.142 (142.250.183.142): icmp_seq=1 ttl=37 time=20.1 ms
64 bytes from 142.250.183.142 (142.250.183.142): icmp_seq=2 ttl=37 time=19.2 ms
64 bytes from 142.250.183.142 (142.250.183.142): icmp_seq=3 ttl=37 time=19.0 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 19.032/19.473/20.145/0.482 ms
seed-host:PES1UG20CS084:AryanshB:/
$>
```

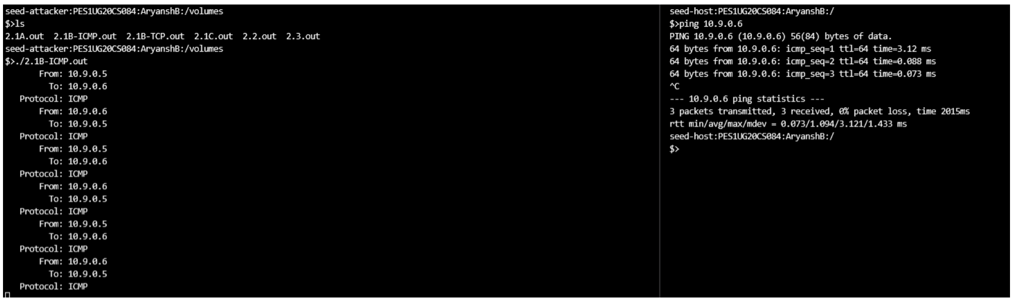
    - Promiscous mode turned on:

- I get the same output with both promiscous mode turned on or off since no other activity is happening in my host machine (Since I am not using a VM, and running the docker containers on windows). If I used this on my VM, then host traffic would also be captured, along with the ping request I made on `seed-host`
- 

```
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>./2.1A.out
       From: 10.9.0.5
         To: 8.8.8.8
   Protocol: ICMP
       From: 8.8.8.8
         To: 10.9.0.5
   Protocol: ICMP
       From: 10.9.0.5
         To: 8.8.8.8
   Protocol: ICMP
       From: 8.8.8.8
         To: 10.9.0.5
   Protocol: ICMP
       From: 10.9.0.5
         To: 8.8.8.8
   Protocol: ICMP
       From: 8.8.8.8
         To: 10.9.0.5
   Protocol: ICMP
```

```
seed-host:PES1UG20CS084:AryanshB:/
$>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=37 time=19.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=37 time=18.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=37 time=20.3 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 18.741/19.587/20.327/0.651 ms
seed-host:PES1UG20CS084:AryanshB:/
$>
```

## Task 2.1 B : Writing Filters

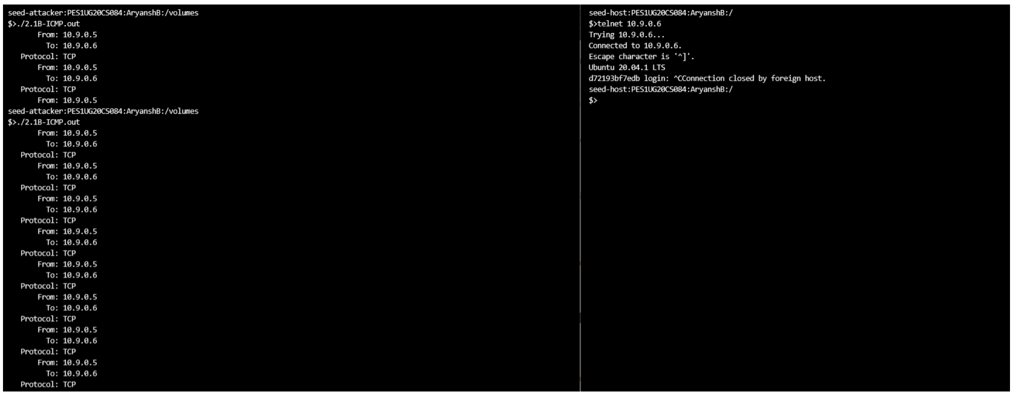
- `Question: Capture the ICMP packets between two specific hosts`
  - 

```
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>ls
2.1A.out  2.1B-ICMP.out  2.1B-TCP.out  2.1C.out  2.2.out  2.3.out
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>./2.1B-ICMP.out
       From: 10.9.0.5
         To: 10.9.0.6
   Protocol: ICMP
       From: 10.9.0.6
         To: 10.9.0.5
   Protocol: ICMP
       From: 10.9.0.5
         To: 10.9.0.6
   Protocol: ICMP
       From: 10.9.0.6
         To: 10.9.0.5
   Protocol: ICMP
       From: 10.9.0.5
         To: 10.9.0.6
   Protocol: ICMP
       From: 10.9.0.6
         To: 10.9.0.5
   Protocol: ICMP
```

```
seed-host:PES1UG20CS084:AryanshB:/
$>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=3.12 ms
64 bytes from 10.9.0.6: icmp_seq=2 ttl=64 time=0.088 ms
64 bytes from 10.9.0.6: icmp_seq=3 ttl=64 time=0.073 ms
^C
--- 10.9.0.6 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2015ms
rtt min/avg/max/mdev = 0.073/1.094/3.121/1.433 ms
seed-host:PES1UG20CS084:AryanshB:/
$>
```

  - traffic between `10.9.0.5` and `10.9.0.6` has been captured using the filter

    `proto ICMP and (host 10.9.0.5 and 10.9.0.6)`

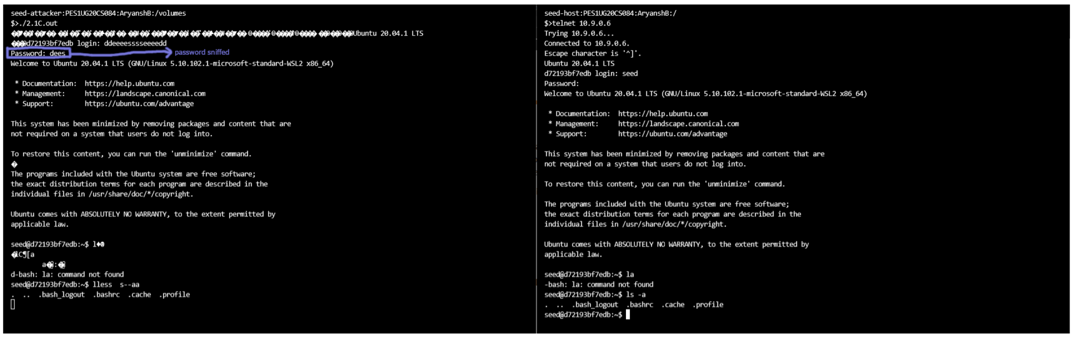
- `Question: Capture the TCP packets that have a destination port range from to sort 10 - 100`
  - 

```
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>./2.1B-ICMP.out
       From: 10.9.0.5
         To: 10.9.0.6
   Protocol: TCP
       From: 10.9.0.5
         To: 10.9.0.6
   Protocol: TCP
       From: 10.9.0.5
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>./2.1B-ICMP.out
       From: 10.9.0.5
         To: 10.9.0.6
   Protocol: TCP
       From: 10.9.0.5
         To: 10.9.0.6
   Protocol: TCP
       From: 10.9.0.5
         To: 10.9.0.6
   Protocol: TCP
       From: 10.9.0.5
         To: 10.9.0.6
   Protocol: TCP
       From: 10.9.0.5
         To: 10.9.0.6
   Protocol: TCP
       From: 10.9.0.5
         To: 10.9.0.6
   Protocol: TCP
       From: 10.9.0.5
         To: 10.9.0.6
   Protocol: TCP
       From: 10.9.0.5
         To: 10.9.0.6
   Protocol: TCP
```

```
seed-host:PES1UG20CS084:AryanshB:/
$>telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
d72193bf7edb login: ^CConnection closed by foreign host.
seed-host:PES1UG20CS084:AryanshB:/
$>
```

  - traffic from ports `10-100` have been captured using the filter `tcp dst portrange 10-100`

## Task 2.1 C : Sniffing Passwords

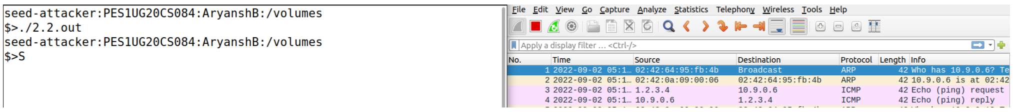


```
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>./2.1C.out
�������� ���� ������ ������ ���������� ������ ����������ￅ����ￅ����ￅ���� ����������Ubuntu 20.04.1 LTS
���d72193bf7edb login: ddeeeesssseeeedd
Password: dees
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.10.102.1-microsoft-standard-WSL2 x86_64)

 * 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.
�
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@d72193bf7edb:~$ l��
�lC¶[a
        a��:��
d-bash: la: command not found
seed@d72193bf7edb:~$ lless  s--aa
.  ..  .bash_logout  .bashrc  .cache  .profile
▯
```

```
seed-host:PES1UG20CS084:AryanshB:/
$>telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
d72193bf7edb login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.10.102.1-microsoft-standard-WSL2 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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@d72193bf7edb:~$ la
-bash: la: command not found
seed@d72193bf7edb:~$ ls -a
.  ..  .bash_logout  .bashrc  .cache  .profile
seed@d72193bf7edb:~$ █
```

- TCP Packets have been sniffed on port 23 and

## Task 2.2 : Spoofing

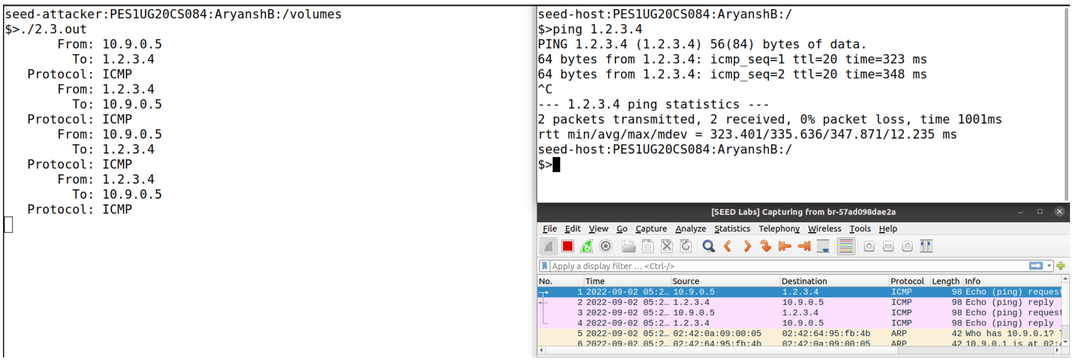
- `Question: Spoof an ICMP Request`
  - 

```
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>./2.2.out
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>S
```

```
No.  Time                Source             Destination        Protocol Length Info
   1 2022-09-02 05:1…   02:42:64:95:fb:4b  Broadcast          ARP          42 Who has 10.9.0.6? Te
   2 2022-09-02 05:1…   02:42:0a:09:00:06  02:42:64:95:fb:4b  ARP          42 10.9.0.6 is at 02:42
   3 2022-09-02 05:1…   1.2.3.4            10.9.0.6           ICMP         42 Echo (ping) request
   4 2022-09-02 05:1…   10.9.0.6           1.2.3.4            ICMP         42 Echo (ping) reply
```

- `Question :  Using the raw socket programming, do you have to calculate the checksum for the IP header?`
  - Yes, In this case, we are calculating checksum in the `in_chksum()` function

## Task 2.3 : Sniffing and Spoofing



```
seed-attacker:PES1UG20CS084:AryanshB:/volumes
$>./2.3.out
       From: 10.9.0.5
         To: 1.2.3.4
   Protocol: ICMP
       From: 1.2.3.4
         To: 10.9.0.5
   Protocol: ICMP
       From: 10.9.0.5
         To: 1.2.3.4
   Protocol: ICMP
       From: 1.2.3.4
         To: 10.9.0.5
   Protocol: ICMP
▯
```

```
seed-host:PES1UG20CS084:AryanshB:/
$>ping 1.2.3.4
PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
64 bytes from 1.2.3.4: icmp_seq=1 ttl=20 time=323 ms
64 bytes from 1.2.3.4: icmp_seq=2 ttl=20 time=348 ms
^C
--- 1.2.3.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 323.401/335.636/347.871/12.235 ms
seed-host:PES1UG20CS084:AryanshB:/
$>█
```

[SEED Labs] Capturing from br-57ad098dae2a
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>

```
No.  Time                Source             Destination        Protocol Length Info
   1 2022-09-02 05:2…   10.9.0.5           1.2.3.4            ICMP         98 Echo (ping) request
   2 2022-09-02 05:2…   1.2.3.4            10.9.0.5           ICMP         98 Echo (ping) reply
   3 2022-09-02 05:2…   10.9.0.5           1.2.3.4            ICMP         98 Echo (ping) request
   4 2022-09-02 05:2…   1.2.3.4            10.9.0.5           ICMP         98 Echo (ping) reply
   5 2022-09-02 05:2…   02:42:0a:09:00:05  02:42:64:95:fb:4b  ARP          42 Who has 10.9.0.1? T
   6 2022-09-02 05:2…   02:42:64:95:fb:4b  02:42:0a:09:00:05  ARP          42 10.9.0.1 is at 02:4
```

- A raw socket (IP) is set up
- We observe that a reply from 1.2.3.4 is being received even though it does not exist, this shows that the sniffing and consequent spoofing was successful.