CNS-SNIFF AND SPOOF USING PCAP(C PROGRAM)

Name : Ankith J Rai
SRN : PES1UG19CS069
SEC : B

Task 1: Writing Packet Sniffing Program

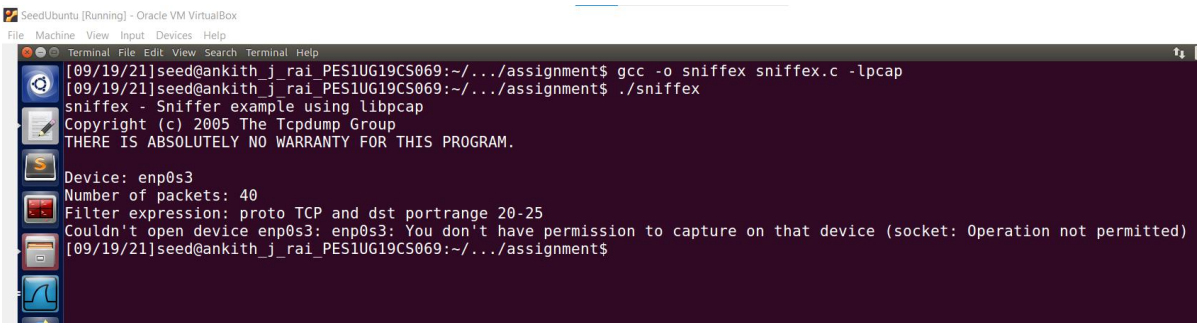
Understanding how a Sniffer Works

Problem 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 a detailed explanation like the one in the tutorial.**

Ans)We use string.h library to get the name of the ethernet card and we use pcap library to set up the environment for getting the packets.

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

Ans) The sniffex program has to be run with root privileges because of security reason and pcap_lookupdev() needs root permission to access the NIC.If we run the program without the root privilege then:



Problem 3: Please turn on and turn off the promiscuous mode in the sniffer program. Can you demonstrate the difference when this mode is on and off? Please describe how you demonstrate this

Ans) From the screenshots below we can see the difference when the promiscuous mode is turned on and turned off.

For the network adapter to monitor all the packets in the network the Promiscuous Mode must be **ON**.

Promiscuous Mode On:

SeedUbuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```
[09/15/21]seed@ankith_j_rai_PES1UG19CS069:~/.../assignment$ gcc -o sniffex sniffex.c -lpcap
[09/15/21]seed@ankith_j_rai_PES1UG19CS069:~/.../assignment$ sudo ./sniffex
sniffex - Sniffer example using libpcap
Copyright (c) 2005 The Tcpdump Group
THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.

Device: enp0s3
Number of packets: 40
Filter expression: proto ICMP and (host 10.0.2.7 and 10.0.2.8)
```

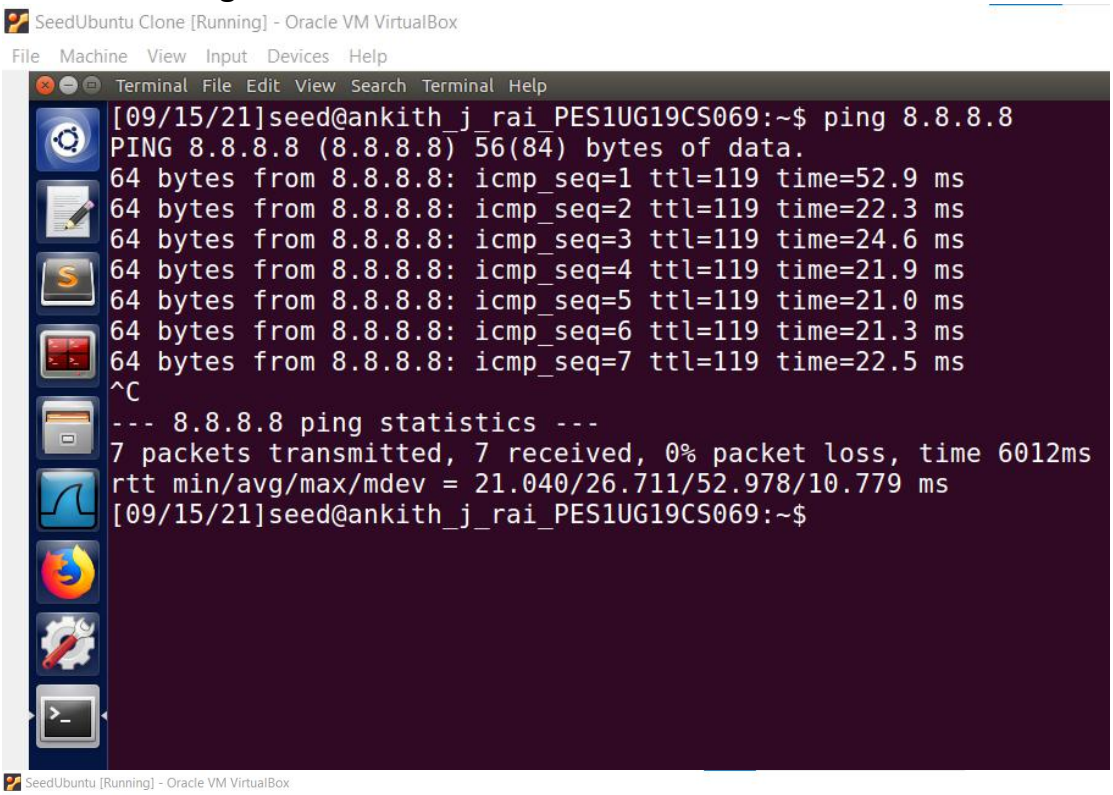
SeedUbuntu [Running] - Oracle VM VirtualBox

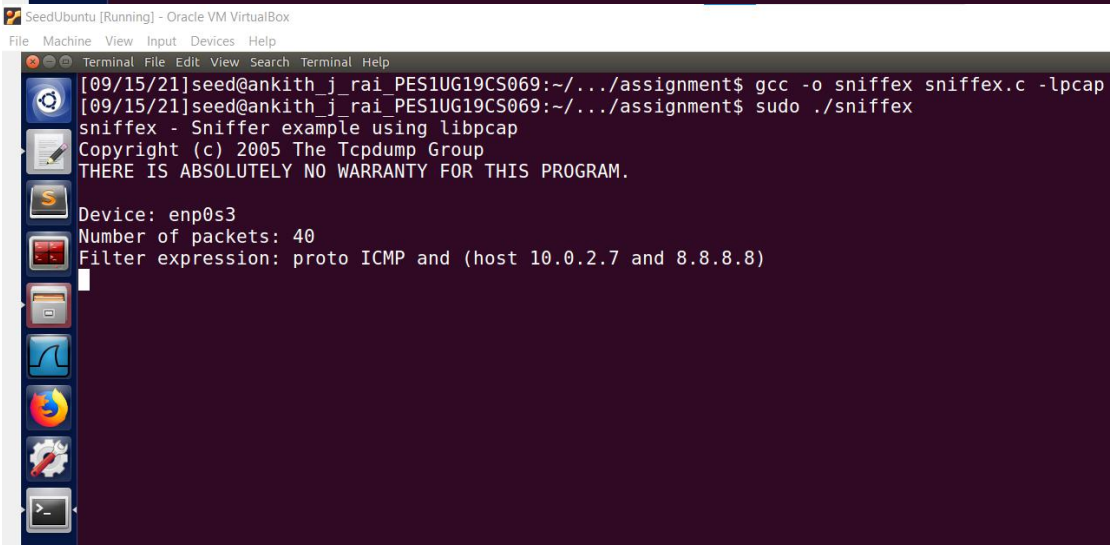
File Machine View Input Devices Help

```
[09/15/21]seed@ankith_j_rai_PES1UG19CS069:~/.../assignment$ gcc -o sniffex sniffex.c -lpcap
[09/15/21]seed@ankith_j_rai_PES1UG19CS069:~/.../assignment$ sudo ./sniffex
sniffex - Sniffer example using libpcap
Copyright (c) 2005 The Tcpdump Group
THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.

Device: enp0s3
Number of packets: 40
Filter expression: proto ICMP and (host 10.0.2.7 and 1.2.3.4)

Packet number 1:
       From: 10.0.2.7
         To: 1.2.3.4
   Protocol: ICMP

Packet number 2:
       From: 10.0.2.7
         To: 1.2.3.4
   Protocol: ICMP

Packet number 3:
       From: 10.0.2.7
         To: 1.2.3.4
   Protocol: ICMP

Packet number 4:
       From: 10.0.2.7
         To: 1.2.3.4
   Protocol: ICMP

Packet number 5:
       From: 10.0.2.7
         To: 1.2.3.4
   Protocol: ICMP
```

Promiscuous Mode Off:

Now let us Ping 8.8.8.8 from 10.0.2.7





From the above screenshot we can see that when the promiscuous mode is off, the sniffex program does not sniff packets going from the victim machine to another random machine as adapter is not able to switch to monitor mode.

Now pinging the attacker machine itself

SeedUbuntu Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```
[09/15/21]seed@ankith_j_rai_PES1UG19CS069:~$ ping 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_seq=1 ttl=64 time=0.815 ms
64 bytes from 10.0.2.5: icmp_seq=2 ttl=64 time=0.520 ms
64 bytes from 10.0.2.5: icmp_seq=3 ttl=64 time=1.08 ms
64 bytes from 10.0.2.5: icmp_seq=4 ttl=64 time=0.249 ms
64 bytes from 10.0.2.5: icmp_seq=5 ttl=64 time=0.359 ms
64 bytes from 10.0.2.5: icmp_seq=6 ttl=64 time=1.01 ms
64 bytes from 10.0.2.5: icmp_seq=7 ttl=64 time=0.330 ms
^C
--- 10.0.2.5 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6087ms
rtt min/avg/max/mdev = 0.249/0.624/1.084/0.320 ms
[09/15/21]seed@ankith_j_rai_PES1UG19CS069:~$
```

SeedUbuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

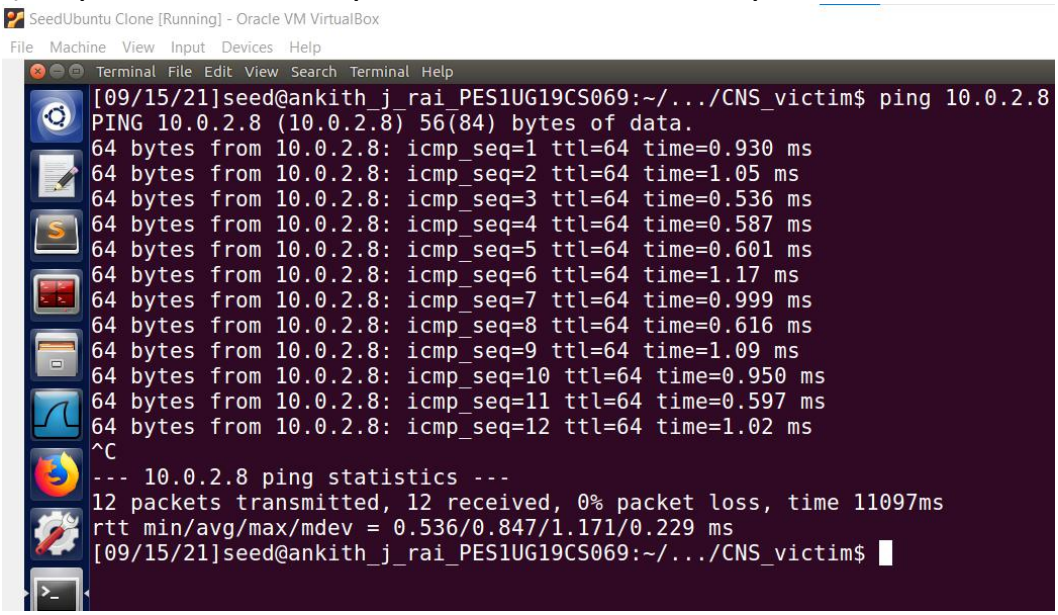
Terminal File Edit View Search Terminal Help

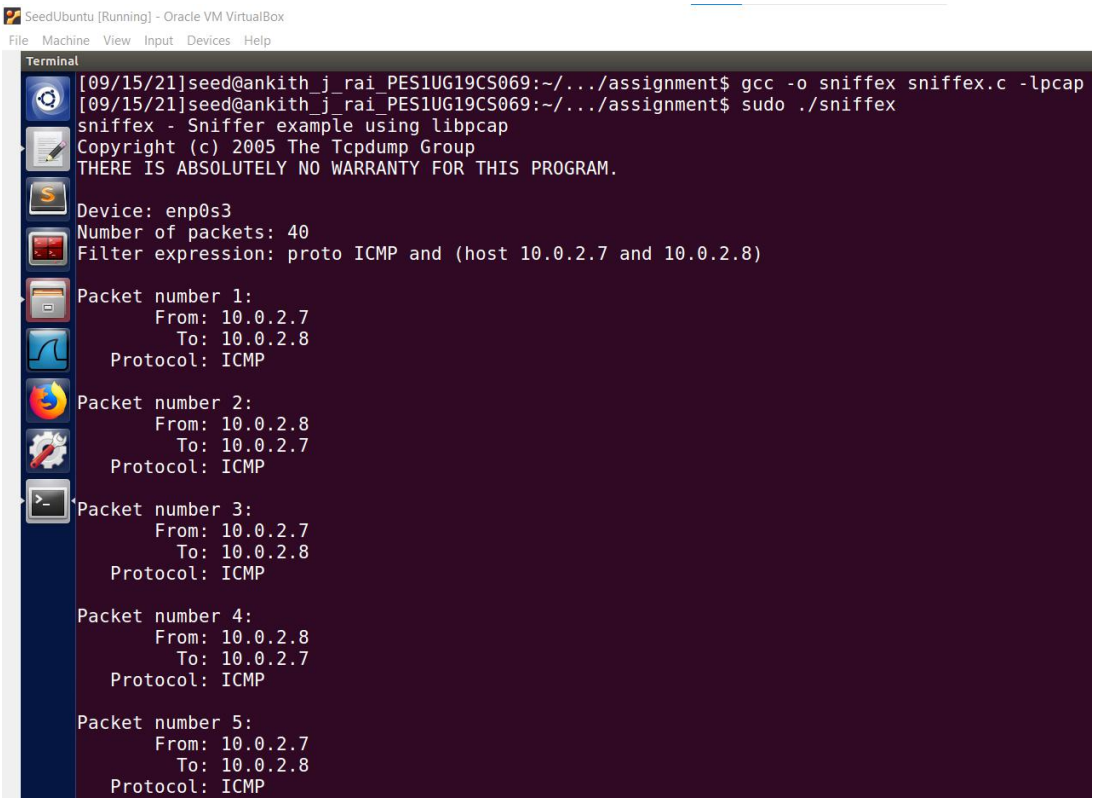
```
[09/15/21]seed@ankith_j_rai_PES1UG19CS069:~/.../assignment$ gcc -o sniffex sniffex.c -lpcap
[09/15/21]seed@ankith_j_rai_PES1UG19CS069:~/.../assignment$ sudo ./sniffex
sniffex - Sniffer example using libpcap
Copyright (c) 2005 The Tcpdump Group
THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.

Device: enp0s3
Number of packets: 40
Filter expression: proto ICMP and (host 10.0.2.7 and 10.0.2.5)

Packet number 1:
       From: 10.0.2.7
         To: 10.0.2.5
   Protocol: ICMP

Packet number 2:
       From: 10.0.2.5
         To: 10.0.2.7
   Protocol: ICMP

Packet number 3:
       From: 10.0.2.7
         To: 10.0.2.5
   Protocol: ICMP

Packet number 4:
       From: 10.0.2.5
         To: 10.0.2.7
   Protocol: ICMP

Packet number 5:
       From: 10.0.2.7
         To: 10.0.2.5
   Protocol: ICMP
```

From the screenshot we can see that when the promiscuous mode is off the sniffex program sniffs packets if and only if the packets are coming to the machine which is running the sniffex program.

Task 1.2: Writing Filters

i) Capture the ICMP packets between two specific hosts





From the above screenshot we can see that only the ICMP packets are sniffed by the sniffex program.

ii) Capture the TCP packets that have a destination port range from to sort 10 - 100

SeedUbuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```
[09/15/21]seed@ankith_j_rai_PES1UG19CS069:~$ ftp 10.0.2.8
Connected to 10.0.2.8.
220 (vsFTPd 3.0.3)
Name (10.0.2.8:seed): seed
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxr-x    2 1000     1000         4096 Jan 14  2018 Customization
drwxr-xr-x    2 1000     1000         4096 Sep 06 13:30 Desktop
drwxr-xr-x    2 1000     1000         4096 Jul 25  2017 Documents
drwxr-xr-x    2 1000     1000         4096 May 09  2018 Downloads
drwxr-xr-x    2 1000     1000         4096 Jul 25  2017 Music
drwxr-xr-x    3 1000     1000         4096 Jan 14  2018 Pictures
drwxr-xr-x    2 1000     1000         4096 Jul 25  2017 Public
drwxr-xr-x    2 1000     1000         4096 Jul 25  2017 Templates
drwxr-xr-x    2 1000     1000         4096 Jul 25  2017 Videos
drwxrwxr-x    4 1000     1000         4096 May 01  2018 android
drwxrwxr-x    2 1000     1000         4096 Jan 14  2018 bin
-rw-r--r--    1 1000     1000         8980 Jul 25  2017 examples.desktop
-rw-rw-r--    1 1000     1000      1661676 Jan 02  2019 get-pip.py
drwxrwxr-x    3 1000     1000         4096 May 09  2018 lib
drwxrwxr-x    4 1000     1000         4096 May 09  2018 source
226 Directory send OK.
ftp>
```

SeedUbuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal File Edit View Search Terminal Help

```
[09/15/21]seed@ankith_j_rai_PES1UG19CS069:~/.../assignment$ sudo ./sniffex
sniffex - Sniffer example using libpcap
Copyright (c) 2005 The Tcpdump Group
THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.

Device: enp0s3
Number of packets: 40
Filter expression: proto TCP and dst portrange 10-100

Packet number 1:
       From: 10.0.2.5
         To: 10.0.2.8
   Protocol: TCP
   Src port: 52954
   Dst port: 21

Packet number 2:
       From: 10.0.2.5
         To: 10.0.2.8
   Protocol: TCP
   Src port: 52954
   Dst port: 21

Packet number 3:
       From: 10.0.2.5
         To: 10.0.2.8
   Protocol: TCP
   Src port: 52954
   Dst port: 21

Packet number 4:
       From: 10.0.2.5
         To: 10.0.2.8
   Protocol: TCP
   Src port: 52954
   Dst port: 21
   Payload (11 bytes):
```

SeedUbuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```
Packet number 10:
       From: 10.0.2.5
         To: 10.0.2.8
   Protocol: TCP
   Src port: 52954
   Dst port: 21
   Payload (22 bytes):
00000   50 4f 52 54 20 31 30 2c  30 2c 32 2c 35 2c 31 33    PORT 10,0,2,5,13
00016   38 2c 38 39 0d 0a                                   8,89..

Packet number 11:
       From: 10.0.2.5
         To: 10.0.2.8
   Protocol: TCP
   Src port: 52954
   Dst port: 21

Packet number 12:
       From: 10.0.2.5
         To: 10.0.2.8
   Protocol: TCP
   Src port: 52954
   Dst port: 21
   Payload (6 bytes):
00000   4c 49 53 54 0d 0a                                   LIST..

Packet number 13:
       From: 10.0.2.5
         To: 10.0.2.8
   Protocol: TCP
   Src port: 35417
   Dst port: 20

Packet number 14:
       From: 10.0.2.5
         To: 10.0.2.8
   Protocol: TCP
```

SeedUbuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
2	2021-09-15 21:29:13.7965756…	10.0.2.5	10.0.2.8	TCP	76	52954 → 21 [SYN] Seq=1017349183 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=606622 TSecr=0 WS=128
3	2021-09-15 21:29:13.7968986…	10.0.2.8	10.0.2.5	TCP	76	21 → 52954 [SYN, ACK] Seq=139075018 Ack=1017349184 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=609537 …
4	2021-09-15 21:29:13.7969114…	10.0.2.5	10.0.2.8	TCP	68	52954 → 21 [ACK] Seq=1017349184 Ack=139075019 Win=29312 Len=0 TSval=606623 TSecr=609537
5	2021-09-15 21:29:13.7985383…	10.0.2.8	10.0.2.5	FTP	88	Response: 220 (vsFTPd 3.0.3)
6	2021-09-15 21:29:13.7985582…	10.0.2.5	10.0.2.8	TCP	68	52954 → 21 [ACK] Seq=1017349184 Ack=139075039 Win=29312 Len=0 TSval=606623 TSecr=609537
7	2021-09-15 21:29:16.7753930…	10.0.2.5	10.0.2.8	FTP	79	Request: USER seed
8	2021-09-15 21:29:16.7759002…	10.0.2.8	10.0.2.5	TCP	68	21 → 52954 [ACK] Seq=139075039 Ack=1017349195 Win=29056 Len=0 TSval=610282 TSecr=607367
9	2021-09-15 21:29:16.7761118…	10.0.2.8	10.0.2.5	FTP	102	Response: 331 Please specify the password.
10	2021-09-15 21:29:16.7761451…	10.0.2.5	10.0.2.8	TCP	68	52954 → 21 [ACK] Seq=1017349195 Ack=139075073 Win=29312 Len=0 TSval=607367 TSecr=610282
11	2021-09-15 21:29:18.7555782…	10.0.2.5	10.0.2.8	FTP	79	Request: PASS dees
12	2021-09-15 21:29:18.7846338…	10.0.2.8	10.0.2.5	FTP	91	Response: 230 Login successful.
13	2021-09-15 21:29:18.7846906…	10.0.2.5	10.0.2.8	TCP	68	52954 → 21 [ACK] Seq=1017349206 Ack=139075096 Win=29312 Len=0 TSval=607869 TSecr=610784
14	2021-09-15 21:29:18.7847361…	10.0.2.5	10.0.2.8	FTP	74	Request: SYST
15	2021-09-15 21:29:18.7852031…	10.0.2.8	10.0.2.5	FTP	87	Response: 215 UNIX Type: L8
16	2021-09-15 21:29:18.8294553…	10.0.2.5	10.0.2.8	TCP	68	52954 → 21 [ACK] Seq=1017349212 Ack=139075115 Win=29312 Len=0 TSval=607881 TSecr=610784
22	2021-09-15 21:30:52.0326435…	10.0.2.5	10.0.2.8	FTP	90	Request: PORT 10,0,2,5,138,89
23	2021-09-15 21:30:52.0332239…	10.0.2.8	10.0.2.5	FTP	119	Response: 200 PORT command successful. Consider using PASV.
24	2021-09-15 21:30:52.0332560…	10.0.2.5	10.0.2.8	TCP	68	52954 → 21 [ACK] Seq=1017349234 Ack=139075166 Win=29312 Len=0 TSval=631182 TSecr=634108
25	2021-09-15 21:30:52.0332951…	10.0.2.5	10.0.2.8	FTP	74	Request: LIST
26	2021-09-15 21:30:52.0337660…	10.0.2.8	10.0.2.5	TCP	76	20 → 35417 [SYN] Seq=588382533 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=634108 TSecr=0 WS=128
27	2021-09-15 21:30:52.0337774…	10.0.2.5	10.0.2.8	TCP	76	35417 → 20 [SYN, ACK] Seq=68943511 Ack=588382534 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=631182 TS…
28	2021-09-15 21:30:52.0341837…	10.0.2.8	10.0.2.5	TCP	68	20 → 35417 [ACK] Seq=588382534 Ack=68943512 Win=29312 Len=0 TSval=634108 TSecr=631182
29	2021-09-15 21:30:52.0341954…	10.0.2.8	10.0.2.5	FTP	107	Response: 150 Here comes the directory listing.
30	2021-09-15 21:30:52.0344572…	10.0.2.8	10.0.2.5	FTP-DA…	1055	FTP Data: 987 bytes
31	2021-09-15 21:30:52.0344617…	10.0.2.8	10.0.2.5	TCP	68	20 → 35417 [FIN, ACK] Seq=588383521 Ack=68943512 Win=29312 Len=0 TSval=634108 TSecr=631182
32	2021-09-15 21:30:52.0344755…	10.0.2.5	10.0.2.8	TCP	68	35417 → 20 [ACK] Seq=68943512 Ack=588383521 Win=30976 Len=0 TSval=631182 TSecr=634108
33	2021-09-15 21:30:52.0345180…	10.0.2.5	10.0.2.8	TCP	68	35417 → 20 [FIN, ACK] Seq=68943512 Ack=588383522 Win=30976 Len=0 TSval=631182 TSecr=634108
34	2021-09-15 21:30:52.0348172…	10.0.2.8	10.0.2.5	TCP	68	20 → 35417 [ACK] Seq=588383522 Ack=68943513 Win=29312 Len=0 TSval=634108 TSecr=631182
35	2021-09-15 21:30:52.0348233…	10.0.2.8	10.0.2.5	FTP	92	Response: 226 Directory send OK.
36	2021-09-15 21:30:52.0348352…	10.0.2.5	10.0.2.8	TCP	68	52954 → 21 [ACK] Seq=1017349240 Ack=139075229 Win=29312 Len=0 TSval=631182 TSecr=634108

SeedUbuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wireshark · Packet 2 · wireshark_any_20210915212906_oQ5qsn

```
▸ Frame 2: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.0.2.5, Dst: 10.0.2.8
▾ Transmission Control Protocol, Src Port: 52954, Dst Port: 21, Seq: 1017349183, Len: 0
    Source Port: 52954
    Destination Port: 21
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 1017349183
    Acknowledgment number: 0
    Header Length: 40 bytes
  ▾ Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    ▸ .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ··********S·]
    Window size value: 29200
    [Calculated window size: 29200]
    Checksum: 0x183b [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▸ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
```

From the above screenshots we can see that the **source port number is 52954 and destination port number is 21**.

Task 1.3: Sniffing Passwords

SeedUbuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

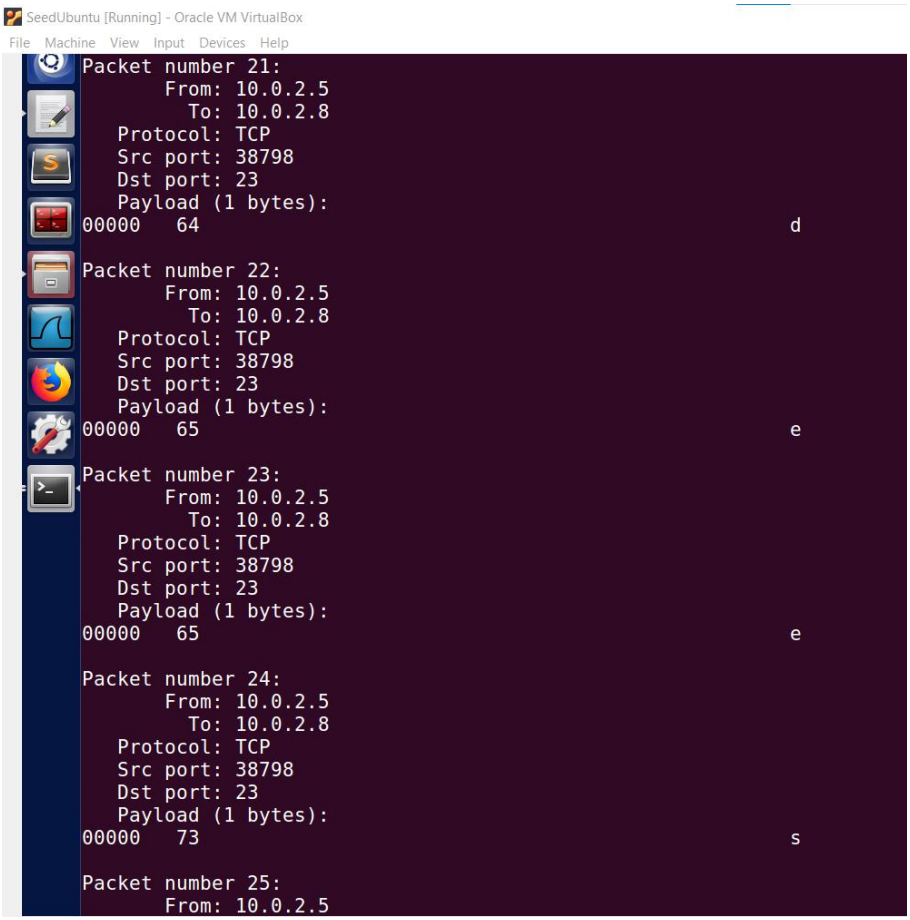
```
[09/15/21]seed@ankith_j_rai_PES1UG19CS069:~$ telnet 10.0.2.8
Trying 10.0.2.8...
Connected to 10.0.2.8.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
ankith_j_rai_PES1UG19CS069 login: seed
Password:
Last login: Mon Sep  6 06:57:09 EDT 2021 from 10.0.2.5 on pts/22
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

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

0 packages can be updated.
0 updates are security updates.

[09/15/21]seed@ankith_j_rai_PES1UG19CS069:~$
```

SeedUbuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal File Edit View Search Terminal Help

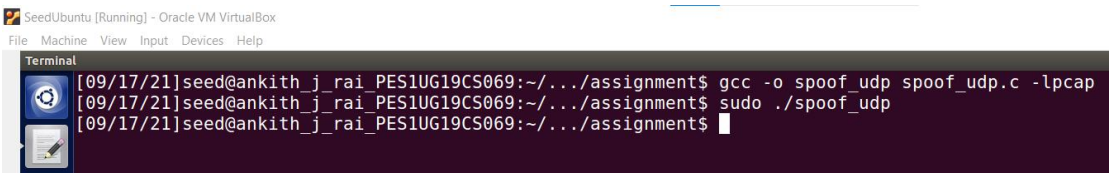
```
[09/15/21]seed@ankith_j_rai_PES1UG19CS069:~/.../assignment$ gcc -o sniffex sniffex.c -lpcap
[09/15/21]seed@ankith_j_rai_PES1UG19CS069:~/.../assignment$ sudo ./sniffex
sniffex - Sniffer example using libpcap
Copyright (c) 2005 The Tcpdump Group
THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.

Device: enp0s3
Number of packets: 40
Filter expression: proto TCP and dst portrange 20-25

Packet number 1:
       From: 10.0.2.5
         To: 10.0.2.8
   Protocol: TCP
   Src port: 38798
   Dst port: 23

Packet number 2:
       From: 10.0.2.5
         To: 10.0.2.8
   Protocol: TCP
   Src port: 38798
   Dst port: 23

Packet number 3:
       From: 10.0.2.5
         To: 10.0.2.8
   Protocol: TCP
   Src port: 38798
   Dst port: 23
   Payload (27 bytes):
00000   ff fd 03 ff fb 18 ff fb  1f ff fb 20 ff fb 21 ff    ........... ..!.
00016   fb 22 ff fb 27 ff fd 05  ff fb 23                   ."..'.....#
```

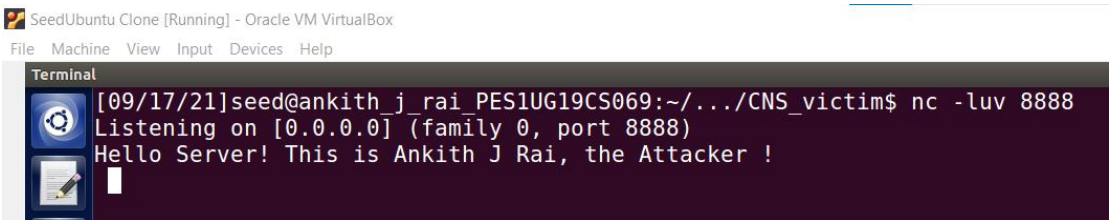


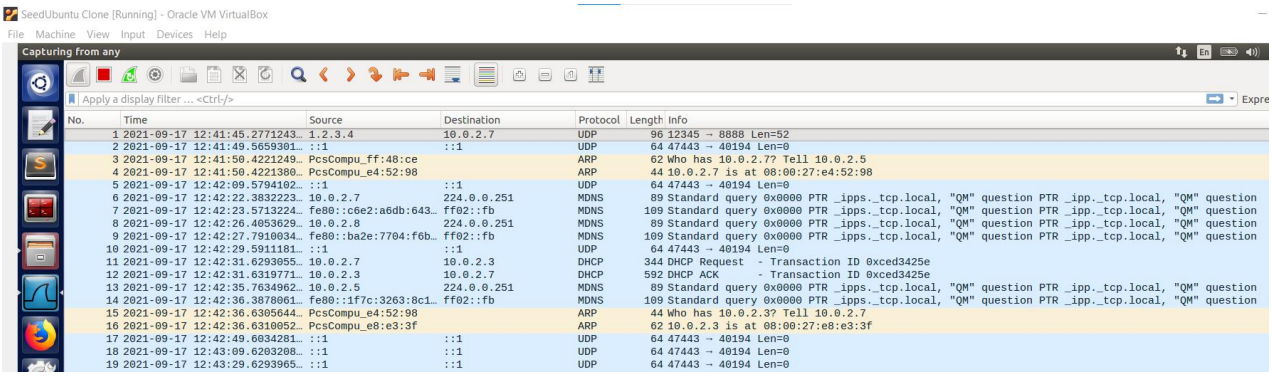
In the above screenshot we can see that the sniffex program has sniffed the password(i.e dees).

Task 2: Spoofing

Task 2.1 - A Writing a spoofing program:





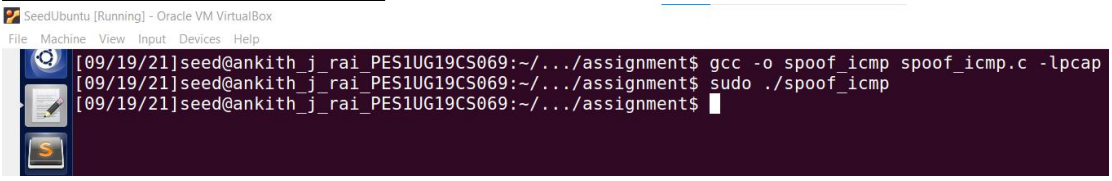


No.	Time	Source	Destination	Protocol	Length	Info
1	2021-09-17 12:41:45.2771243…	1.2.3.4	10.0.2.7	UDP	96	12345 → 8888 Len=52
2	2021-09-17 12:41:49.5659301…	::1	::1	UDP	64	47443 → 40194 Len=0
3	2021-09-17 12:41:50.4221249…	PcsCompu_ff:48:ce		ARP	62	Who has 10.0.2.7? Tell 10.0.2.5
4	2021-09-17 12:41:50.4221380…	PcsCompu_e4:52:98		ARP	44	10.0.2.7 is at 08:00:27:e4:52:98
5	2021-09-17 12:42:09.5794102…	::1	::1	UDP	64	47443 → 40194 Len=0
6	2021-09-17 12:42:22.3832223…	10.0.2.7	224.0.0.251	MDNS	89	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
7	2021-09-17 12:42:23.5713224…	fe80::c6e2:a6db:643…	ff02::fb	MDNS	109	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
8	2021-09-17 12:42:26.4053629…	10.0.2.8	224.0.0.251	MDNS	89	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
9	2021-09-17 12:42:27.7910034…	fe80::ba2e:7704:f6b…	ff02::fb	MDNS	109	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
10	2021-09-17 12:42:29.5911181…	::1	::1	UDP	64	47443 → 40194 Len=0
11	2021-09-17 12:42:31.6293055…	10.0.2.7	10.0.2.3	DHCP	344	DHCP Request - Transaction ID 0xced3425e
12	2021-09-17 12:42:31.6319771…	10.0.2.3	10.0.2.7	DHCP	592	DHCP ACK - Transaction ID 0xced3425e
13	2021-09-17 12:42:35.7634962…	10.0.2.5	224.0.0.251	MDNS	89	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
14	2021-09-17 12:42:36.3878061…	fe80::1f7c:3263:8c1…	ff02::fb	MDNS	109	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
15	2021-09-17 12:42:36.6305644…	PcsCompu_e4:52:98		ARP	44	Who has 10.0.2.3? Tell 10.0.2.7
16	2021-09-17 12:42:36.6310052…	PcsCompu_e8:e3:3f		ARP	62	10.0.2.3 is at 08:00:27:e8:e3:3f
17	2021-09-17 12:42:49.6034281…	::1	::1	UDP	64	47443 → 40194 Len=0
18	2021-09-17 12:43:09.6203208…	::1	::1	UDP	64	47443 → 40194 Len=0
19	2021-09-17 12:43:29.6293965…	::1	::1	UDP	64	47443 → 40194 Len=0

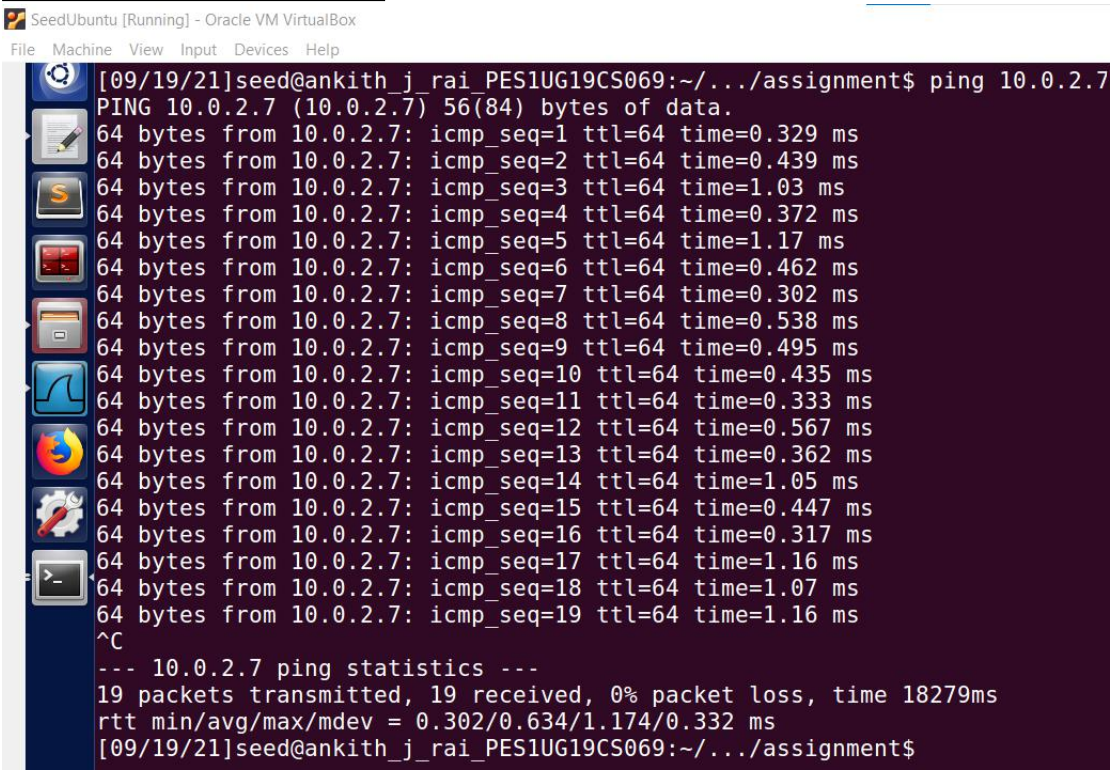
Task 2.2 – Spoof an ICMP Echo Request

In order to observe this we shall ping the victim machine from attacker machine(which is runs the spoof_icmp file lets say in termianl 1) from termianl 2.

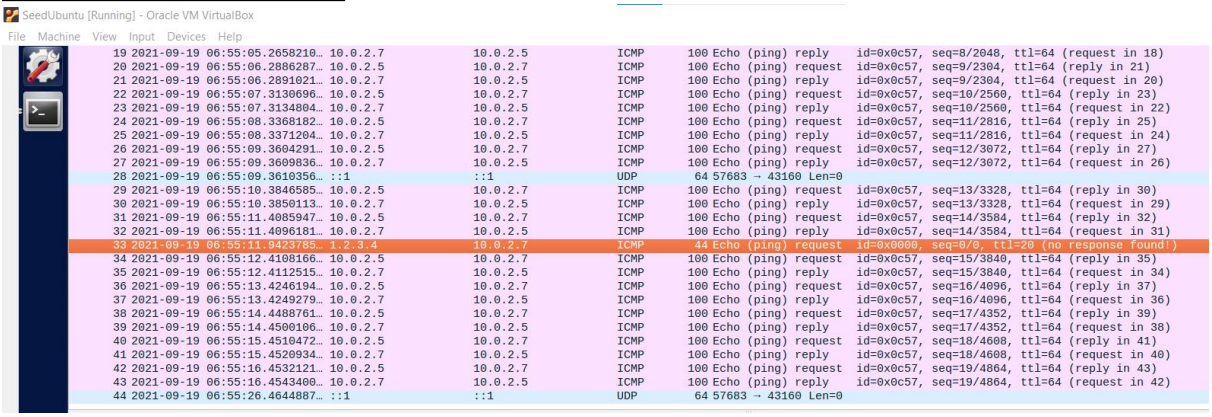
Screenshot of terminal 1:

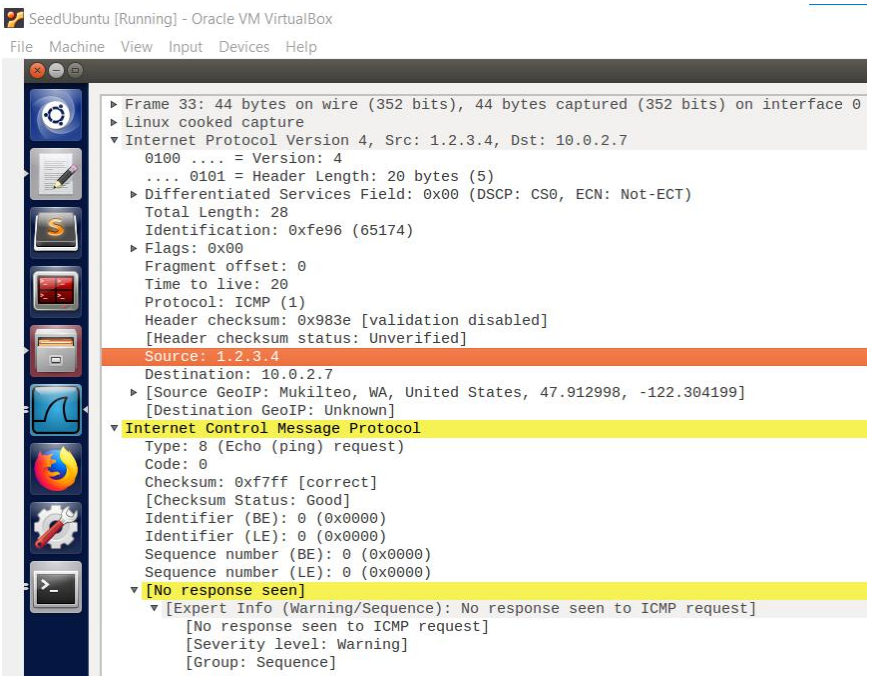


Screenshot of terminal 2:



Wireshark Screenshot:





From the above screenshot we can see that an icmp request packet is sent from 1.2.3.4(i.e the ip address spoofed by attacker machine) to victim machine(10.0.2.7) .

Task 2.3 – Sniff and then Spoof

SeedUbuntu Clone [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```
[09/17/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$ ping 1.2.3.4
PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
8 bytes from 1.2.3.4: icmp_seq=1 ttl=50 (truncated)
8 bytes from 1.2.3.4: icmp_seq=2 ttl=50 (truncated)
8 bytes from 1.2.3.4: icmp_seq=3 ttl=50 (truncated)
8 bytes from 1.2.3.4: icmp_seq=4 ttl=50 (truncated)
8 bytes from 1.2.3.4: icmp_seq=5 ttl=50 (truncated)
8 bytes from 1.2.3.4: icmp_seq=6 ttl=50 (truncated)
8 bytes from 1.2.3.4: icmp_seq=7 ttl=50 (truncated)
8 bytes from 1.2.3.4: icmp_seq=8 ttl=50 (truncated)
8 bytes from 1.2.3.4: icmp_seq=9 ttl=50 (truncated)
8 bytes from 1.2.3.4: icmp_seq=10 ttl=50 (truncated)
8 bytes from 1.2.3.4: icmp_seq=11 ttl=50 (truncated)
8 bytes from 1.2.3.4: icmp_seq=12 ttl=50 (truncated)
8 bytes from 1.2.3.4: icmp_seq=13 ttl=50 (truncated)
8 bytes from 1.2.3.4: icmp_seq=14 ttl=50 (truncated)
^C
--- 1.2.3.4 ping statistics ---
15 packets transmitted, 14 received, 6% packet loss, time 14002ms
rtt min/avg/max/mdev = 2147483.647/0.000/0.000/0.000 ms
[09/17/21]seed@ankith_j_rai_PES1UG19CS069:~/.../CNS_victim$
```

SeedUbuntu [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal File Edit View Search Terminal Help

```
[09/17/21]seed@ankith_j_rai_PES1UG19CS069:~/.../assignment$ sudo ./sniffspoof
Packet Sent from Attacker to host:10.0.2.7
Packet Sent from Attacker to host:10.0.2.7
Packet Sent from Attacker to host:10.0.2.7
Packet Sent from Attacker to host:10.0.2.7
Packet Sent from Attacker to host:10.0.2.7
Packet Sent from Attacker to host:10.0.2.7
Packet Sent from Attacker to host:10.0.2.7
Packet Sent from Attacker to host:10.0.2.7
Packet Sent from Attacker to host:10.0.2.7
Packet Sent from Attacker to host:10.0.2.7
Packet Sent from Attacker to host:10.0.2.7
Packet Sent from Attacker to host:10.0.2.7
Packet Sent from Attacker to host:10.0.2.7
Packet Sent from Attacker to host:10.0.2.7
Packet Sent from Attacker to host:10.0.2.7
^C
[09/17/21]seed@ankith_j_rai_PES1UG19CS069:~/.../assignment$
```

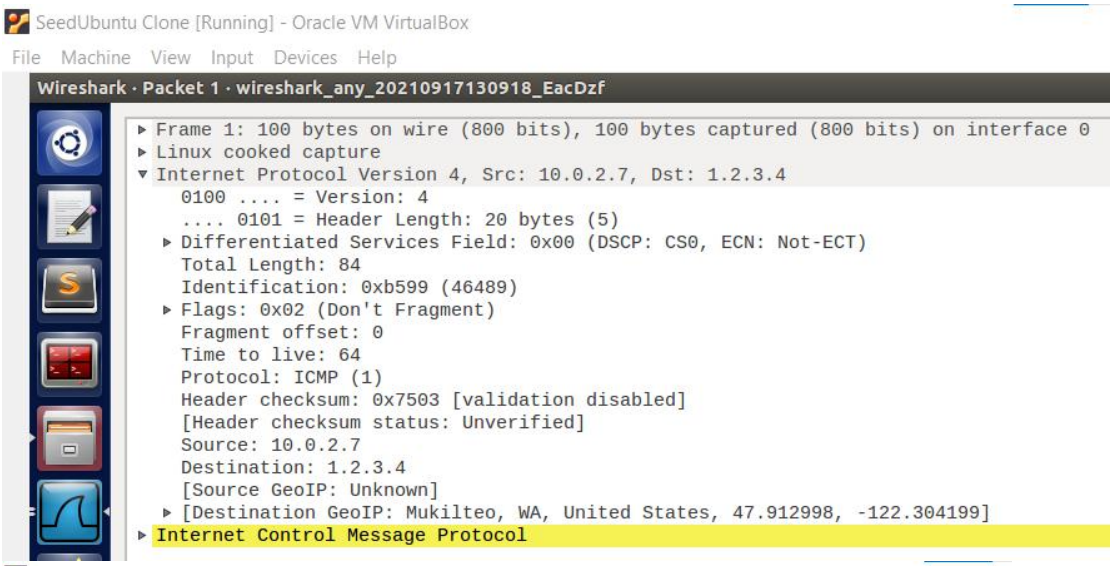
SeedUbuntu Clone [Running] - Oracle VM VirtualBox

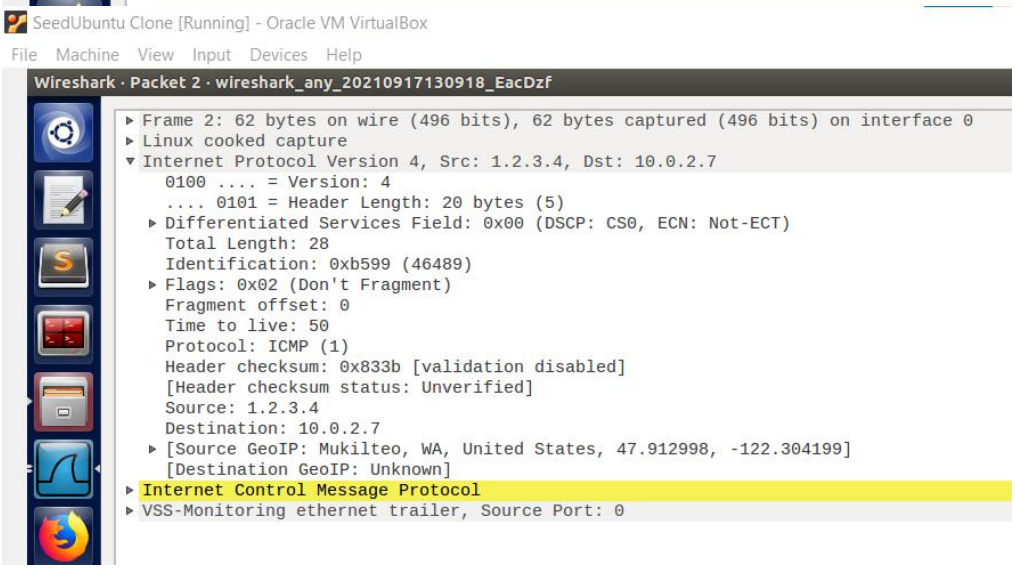
File Machine View Input Devices Help

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	2021-09-17 13:09:20.5875817…	10.0.2.7	1.2.3.4	ICMP	100	Echo (ping) request id=0x0e7c, seq=1/256, ttl=64 (no response found!)
2	2021-09-17 13:09:21.1751069…	1.2.3.4	10.0.2.7	ICMP	62	Echo (ping) reply id=0x0e7c, seq=1/256, ttl=50
3	2021-09-17 13:09:21.1752721…	::1	::1	UDP	64	47443 → 40194 Len=0
4	2021-09-17 13:09:21.5875984…	10.0.2.7	1.2.3.4	ICMP	100	Echo (ping) request id=0x0e7c, seq=2/512, ttl=64 (no response found!)
5	2021-09-17 13:09:22.1986998…	1.2.3.4	10.0.2.7	ICMP	62	Echo (ping) reply id=0x0e7c, seq=2/512, ttl=50
6	2021-09-17 13:09:22.5869659…	10.0.2.7	1.2.3.4	ICMP	100	Echo (ping) request id=0x0e7c, seq=3/768, ttl=64 (no response found!)
7	2021-09-17 13:09:23.2228649…	1.2.3.4	10.0.2.7	ICMP	62	Echo (ping) reply id=0x0e7c, seq=3/768, ttl=50
8	2021-09-17 13:09:23.5875687…	10.0.2.7	1.2.3.4	ICMP	100	Echo (ping) request id=0x0e7c, seq=4/1024, ttl=64 (no response found!)
9	2021-09-17 13:09:24.2465471…	1.2.3.4	10.0.2.7	ICMP	62	Echo (ping) reply id=0x0e7c, seq=4/1024, ttl=50
10	2021-09-17 13:09:24.5871136…	10.0.2.7	1.2.3.4	ICMP	100	Echo (ping) request id=0x0e7c, seq=5/1280, ttl=64 (no response found!)
11	2021-09-17 13:09:25.2707967…	1.2.3.4	10.0.2.7	ICMP	62	Echo (ping) reply id=0x0e7c, seq=5/1280, ttl=50
12	2021-09-17 13:09:25.5876156…	10.0.2.7	1.2.3.4	ICMP	100	Echo (ping) request id=0x0e7c, seq=6/1536, ttl=64 (no response found!)
13	2021-09-17 13:09:26.2319912…	PcsCompu_ff:48:ce		ARP	62	Who has 10.0.2.7? Tell 10.0.2.5
14	2021-09-17 13:09:26.2320152…	PcsCompu_e4:52:98		ARP	44	10.0.2.7 is at 08:00:27:e4:52:98
15	2021-09-17 13:09:26.2958095…	1.2.3.4	10.0.2.7	ICMP	62	Echo (ping) reply id=0x0e7c, seq=6/1536, ttl=50
16	2021-09-17 13:09:26.5875529…	10.0.2.7	1.2.3.4	ICMP	100	Echo (ping) request id=0x0e7c, seq=7/1792, ttl=64 (no response found!)
17	2021-09-17 13:09:27.3192853…	1.2.3.4	10.0.2.7	ICMP	62	Echo (ping) reply id=0x0e7c, seq=7/1792, ttl=50
18	2021-09-17 13:09:27.5878615…	10.0.2.7	1.2.3.4	ICMP	100	Echo (ping) request id=0x0e7c, seq=8/2048, ttl=64 (no response found!)
19	2021-09-17 13:09:28.3427002…	1.2.3.4	10.0.2.7	ICMP	62	Echo (ping) reply id=0x0e7c, seq=8/2048, ttl=50
20	2021-09-17 13:09:28.5881871…	10.0.2.7	1.2.3.4	ICMP	100	Echo (ping) request id=0x0e7c, seq=9/2304, ttl=64 (no response found!)
21	2021-09-17 13:09:29.3667595…	1.2.3.4	10.0.2.7	ICMP	62	Echo (ping) reply id=0x0e7c, seq=9/2304, ttl=50
22	2021-09-17 13:09:29.5892286…	10.0.2.7	1.2.3.4	ICMP	100	Echo (ping) request id=0x0e7c, seq=10/2560, ttl=64 (no response found!)
23	2021-09-17 13:09:30.3912917…	1.2.3.4	10.0.2.7	ICMP	62	Echo (ping) reply id=0x0e7c, seq=10/2560, ttl=50
24	2021-09-17 13:09:30.5892858…	10.0.2.7	1.2.3.4	ICMP	100	Echo (ping) request id=0x0e7c, seq=11/2816, ttl=64 (no response found!)
25	2021-09-17 13:09:31.4154643…	1.2.3.4	10.0.2.7	ICMP	62	Echo (ping) reply id=0x0e7c, seq=11/2816, ttl=50
26	2021-09-17 13:09:31.5899600…	10.0.2.7	1.2.3.4	ICMP	100	Echo (ping) request id=0x0e7c, seq=12/3072, ttl=64 (no response found!)
27	2021-09-17 13:09:32.4393498…	1.2.3.4	10.0.2.7	ICMP	62	Echo (ping) reply id=0x0e7c, seq=12/3072, ttl=50
28	2021-09-17 13:09:32.4396610…	::1	::1	UDP	64	47443 → 40194 Len=0
29	2021-09-17 13:09:32.5904655…	10.0.2.7	1.2.3.4	ICMP	100	Echo (ping) request id=0x0e7c, seq=13/3328, ttl=64 (no response found!)
30	2021-09-17 13:09:33.4627922…	1.2.3.4	10.0.2.7	ICMP	62	Echo (ping) reply id=0x0e7c, seq=13/3328, ttl=50
31	2021-09-17 13:09:33.5901760…	10.0.2.7	1.2.3.4	ICMP	100	Echo (ping) request id=0x0e7c, seq=14/3584, ttl=64 (no response found!)





We can see here that the victim machine which is pinging ip address 1.2.3.4(non existing) is receiving reply from attacker machine which has spoofed the machine with ip address 1.2.3.4 .