COMPUTER NETWORKS LAB

COURSE CODE:UE19CS255

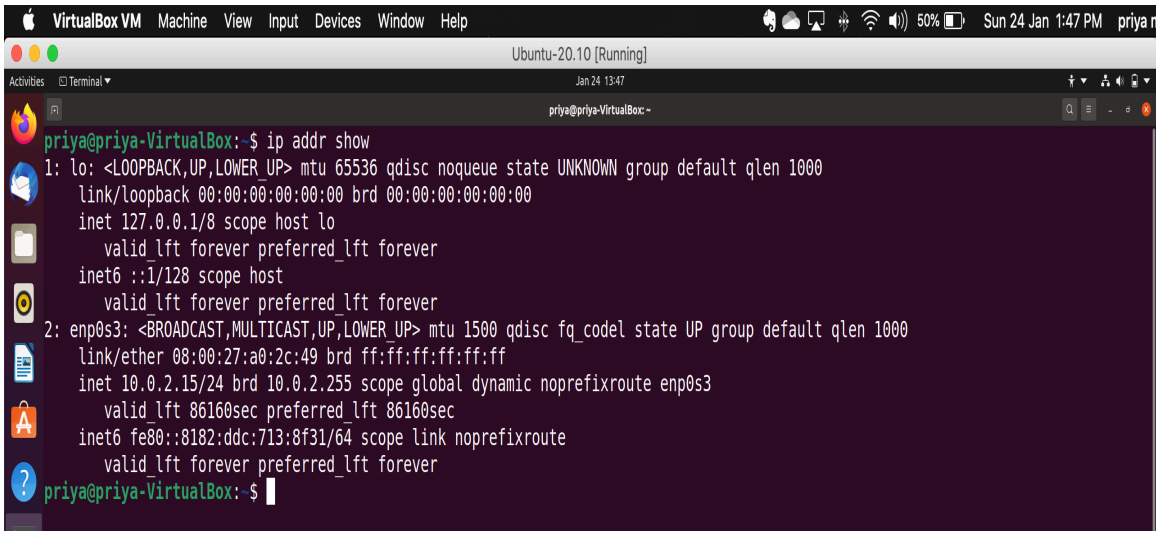
NAME : PRIYA MOHATA
SRN : PES2UG19CS301
SECTION:E
DATE : 24/01/2021

TASK 1:Linux Interface Configuration(ifconfig/IP command)

a) Display status of network interfaces

Command Used : ip addr show

SCREENSHOT



a.Two interfaces are seen in the screenshot

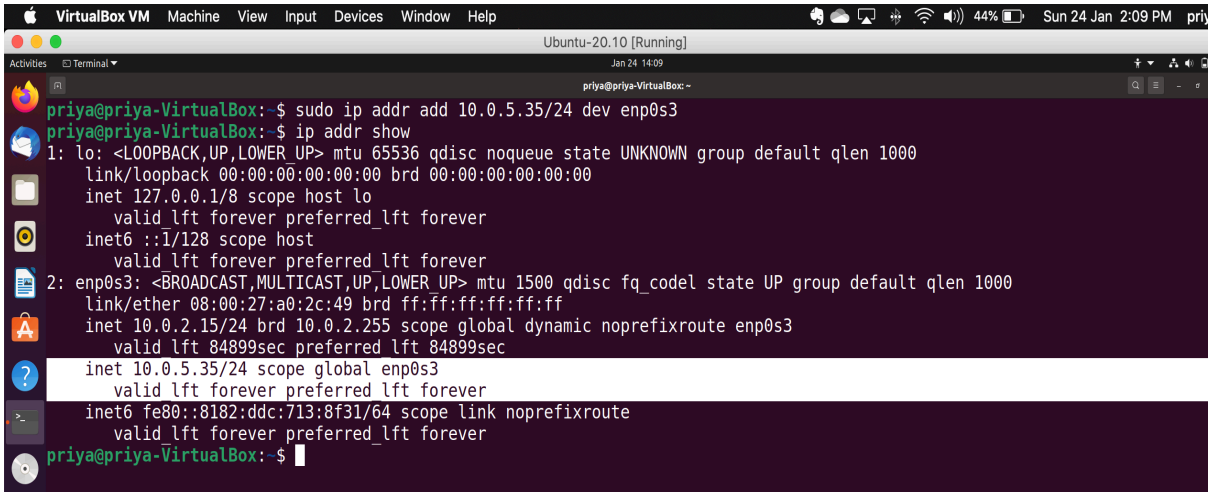
TABLE

Interface Name	IP address (IPv4 / IPv6)	MAC address
lo	IPv4 - 127.0.0.1/8 IPv6 - ::1/128	00:00:00:00:00:00
enp0s3	IPv4- 10.0.2.15/24 IPv6- fe80::8182:ddc:713:8f31/64	08:00:27:a0:2c:49

b) Assigning the IP

Command used : sudo ip addr add 10.0.5.35/24 dev enp0s3

SCREENSHOT

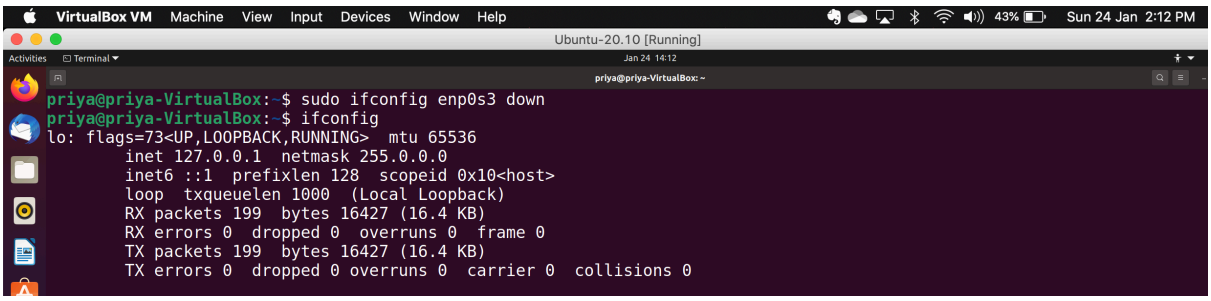


inet 10.0.5.35/24 scope global enp0s3

c)Activating & Deactivating Network Interfaces

Command used to deactivate: sudo ifconfig enp0s3 down

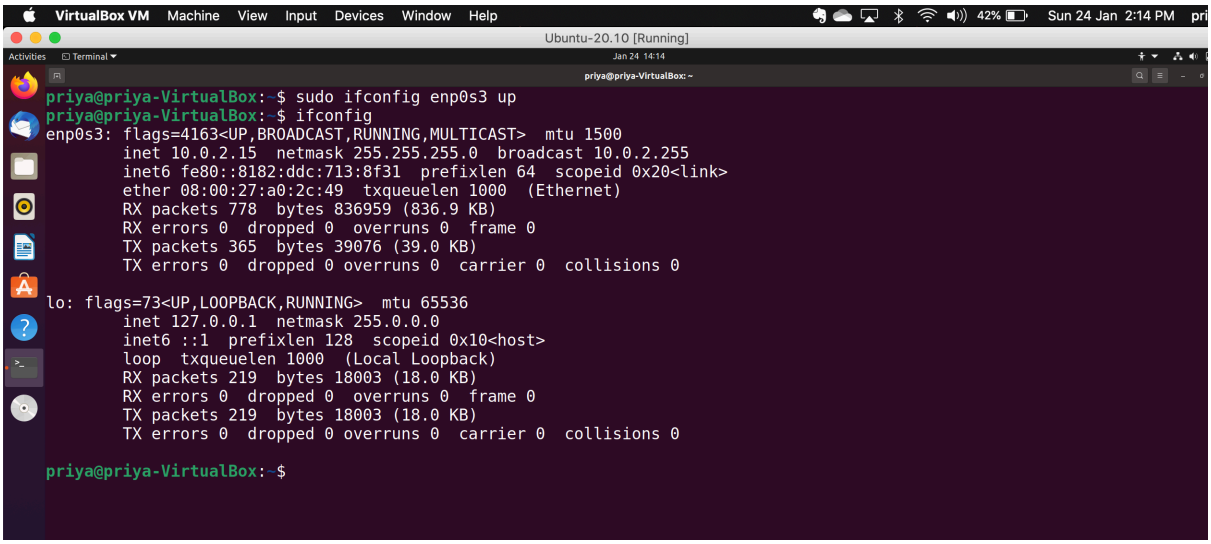
SCREENSHOT



enp0s3 is not seen

Command used to activate: sudo ifconfig enp0s3 up

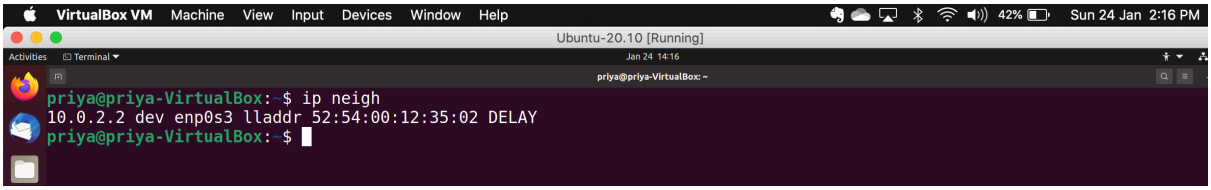
SCREENSHOT



enp0s3 is seen

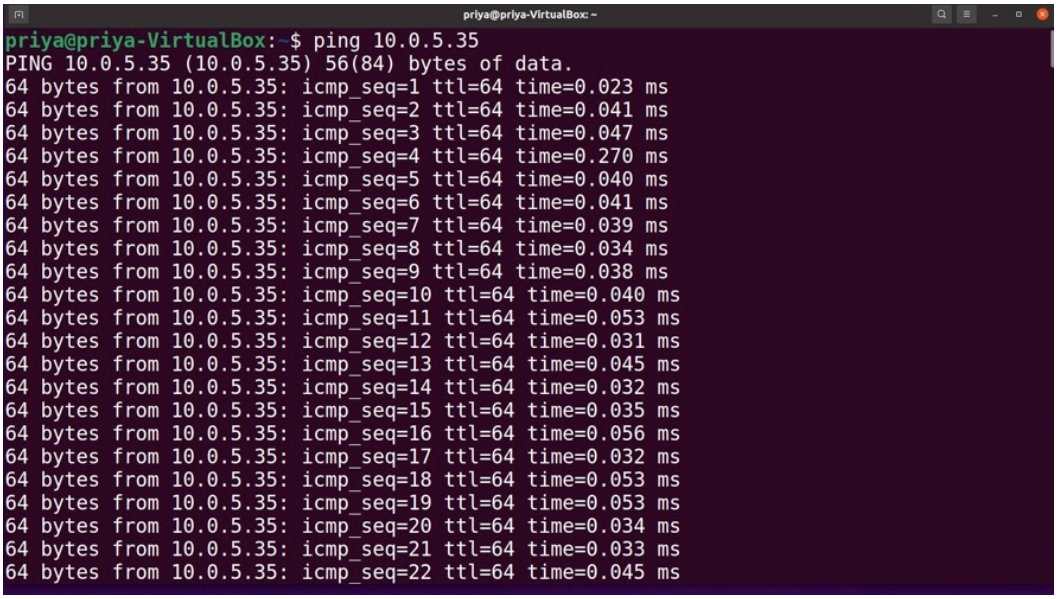
d)Command Used :ip neigh

SCREENSHOT



TASK 2: Ping PDU (Packet Data Units or Packets) Capture

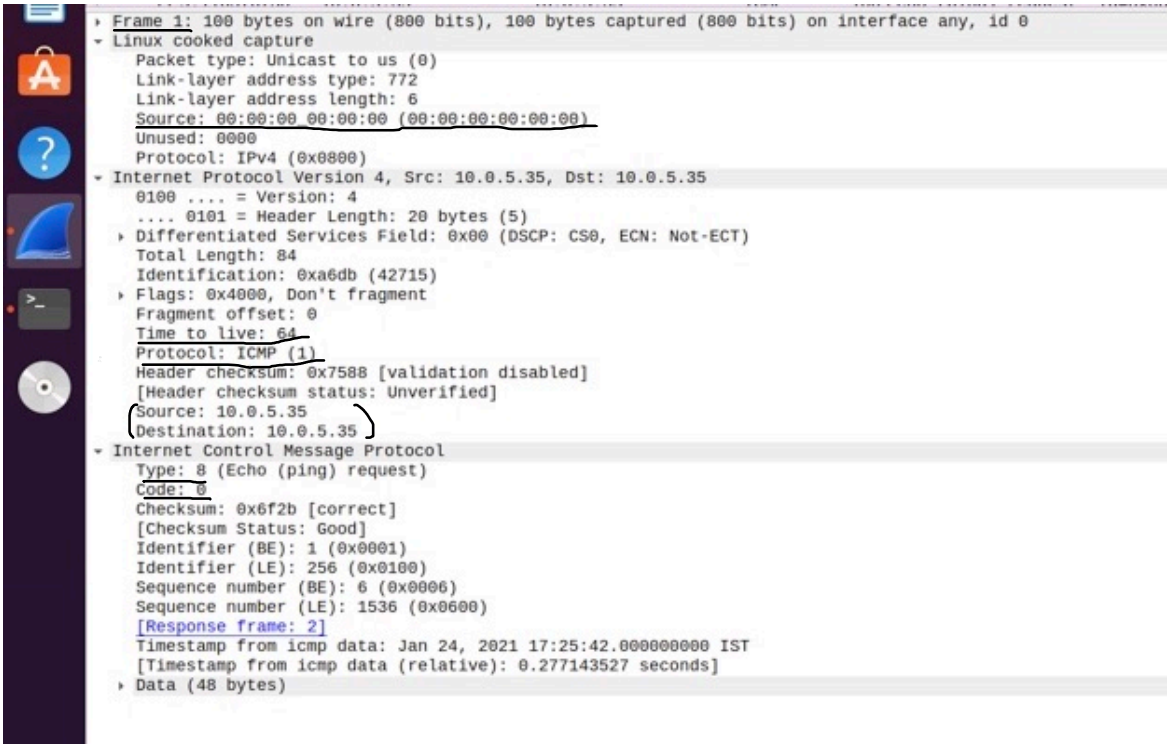
Command Used : ping 10.0.5.35



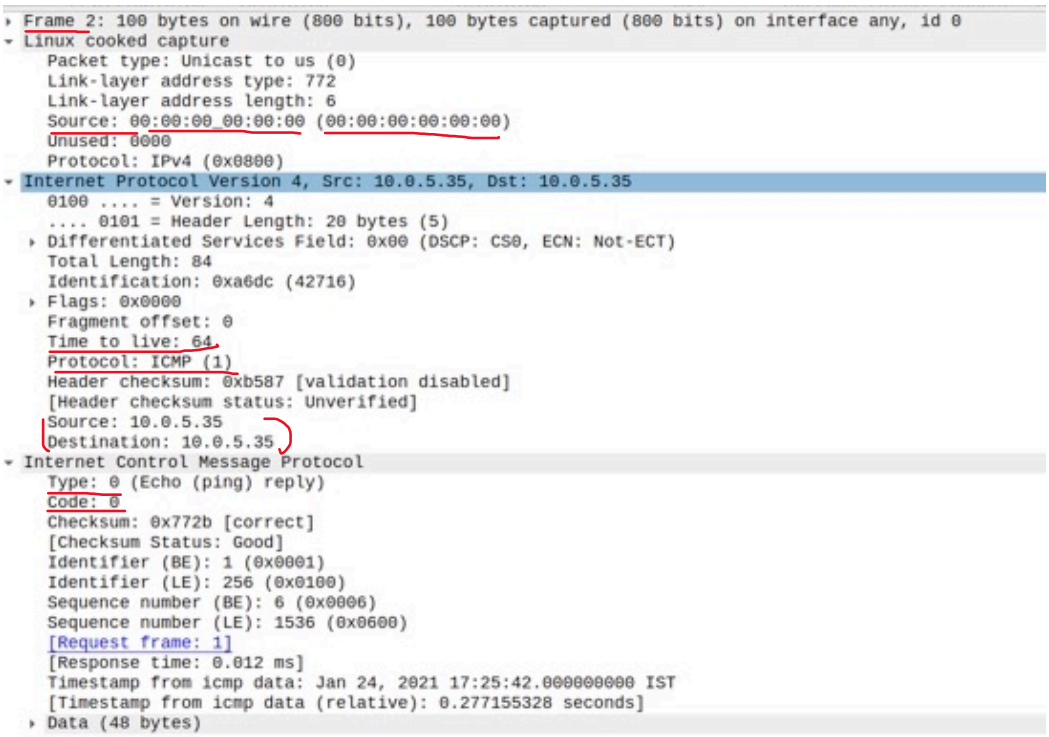
OBSERVATIONS MADE

TTL	64
PROTOCOL USED BY PING	ICMP
TIME	ORDER OF (1/100) milliseconds Since I haven't pressed Ctrl+C Total time wasn't shown so I have written the order

REQUEST PACKET



Response Packet

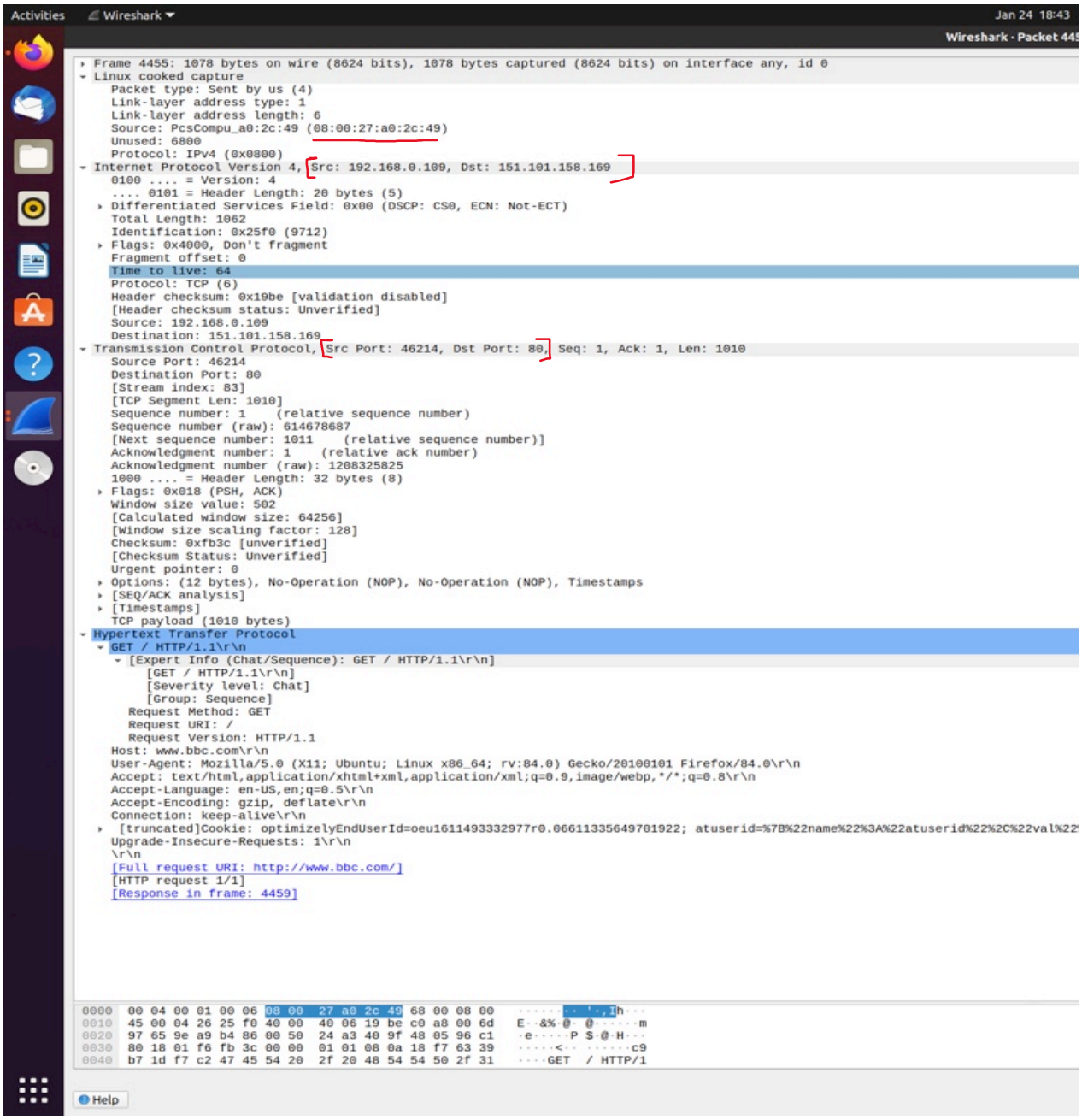


OBSERVATIONS MADE

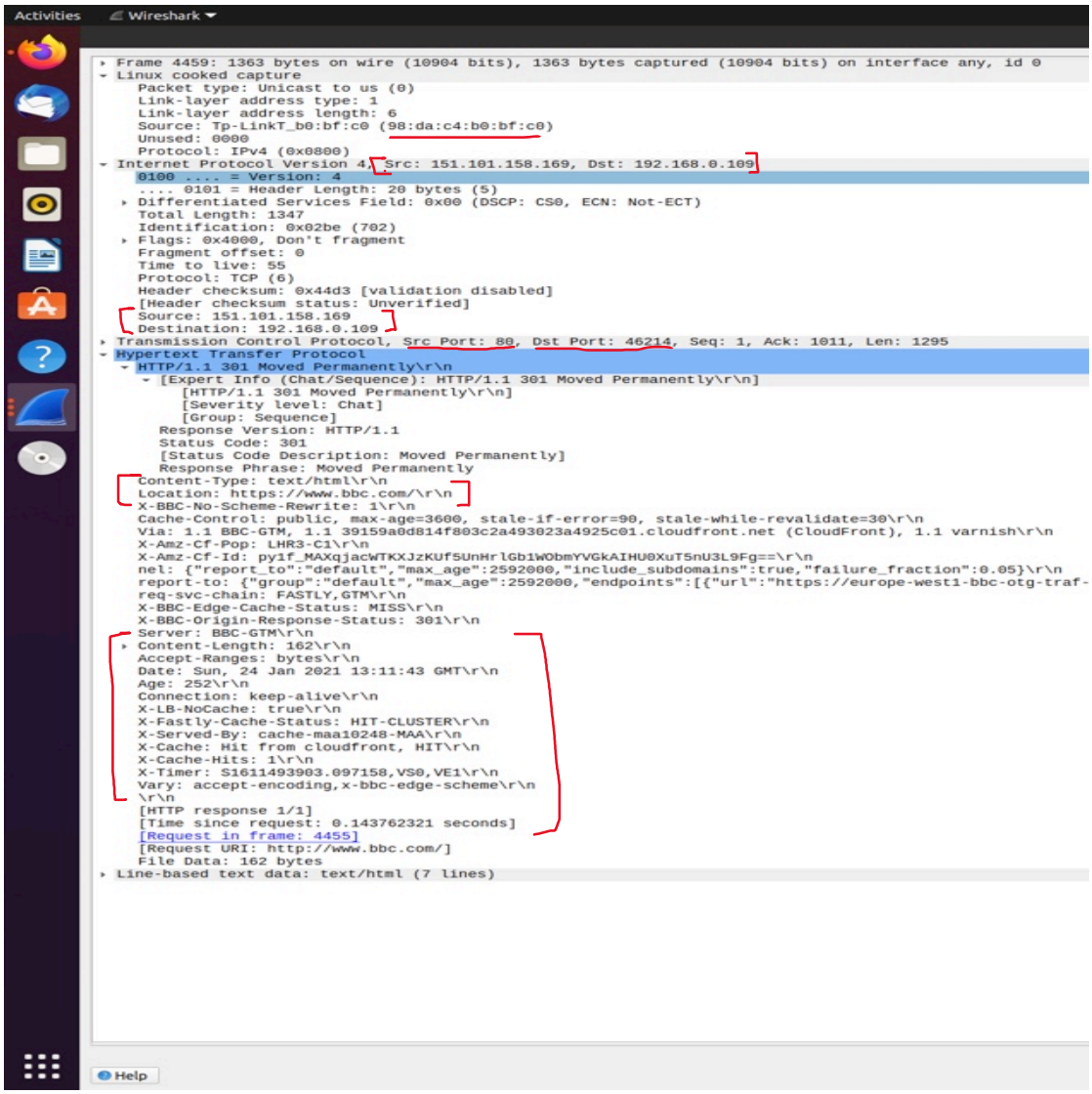
DETAILS	FIRST ECHO REQUEST	FIRST ECHO REPLY
Frame Number	1	2
Source IP address	10.0.5.35	10.0.5.35
Destination IP address	10.0.5.35	10.0.5.35
ICMP Type Value	8	0
ICMP Code Value	0	0
Source Ethernet Address	00:00:00:00:00:00	00:00:00:00:00:00
Destination Ethernet Address	00:00:00:00:00:00	00:00:00:00:00:00
Internet Protocol Version	ICMP- Version 4	ICMP- Version 4
Time To Live (TTL) Value	64	64

TASK 3: HTTP PDU Capture

Request packet (request to bbc.com)



Response packet



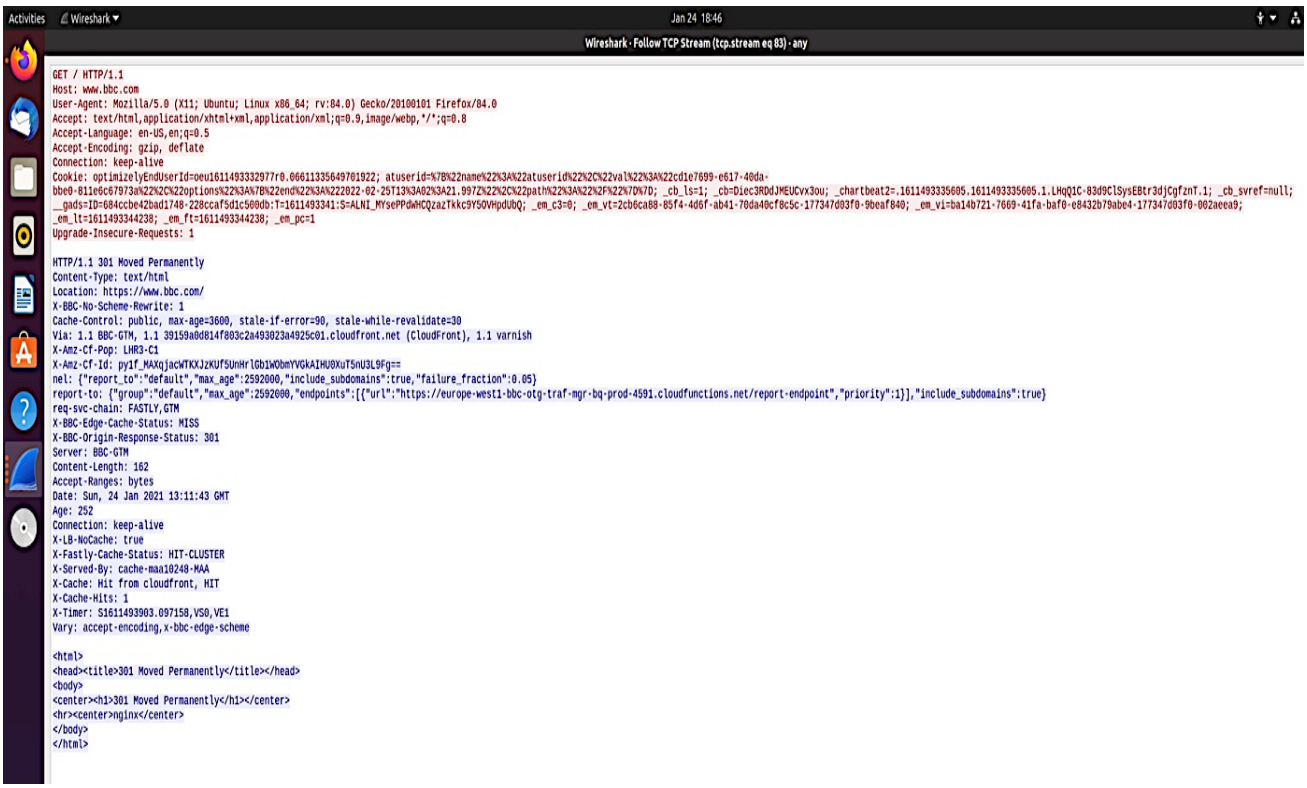
CONNECTION DETAILS

DETAILS	FIRST ECHO REQUEST	FIRST ECHO REPLY
Frame Number	4455	4459
Source Port	46214	80
Destination Port	80	46214
Source IP address	192.168.0.109	151.101.158.169
Destination IP address	151.101.158.169	192.168.0.109
Source Ethernet Address	08:00:27:a0:2c:49	98:da:c4:b0:bf:c0
Destination Ethernet Address	98:da:c4:b0:bf:c0	08:00:27:a0:2c:49

HTTP REQUEST AND RESPONSE

HTTP Request		HTTP Response	
Get	GET / HTTP/1.1\r\n	Server	BBC-GTM
Host	www.bbc.com	Content-Type	text/html
User-Agent	Mozilla/5.0	Date	Sun,24 Jan 2021 13:11:43 GMT
Accept-Language	en-US	Location	https://www.bbc.com
Accept-Encoding	gzip,deflate	Content-Length	162
Connection	keep-alive	Connection	keep-alive

TCP STREAM

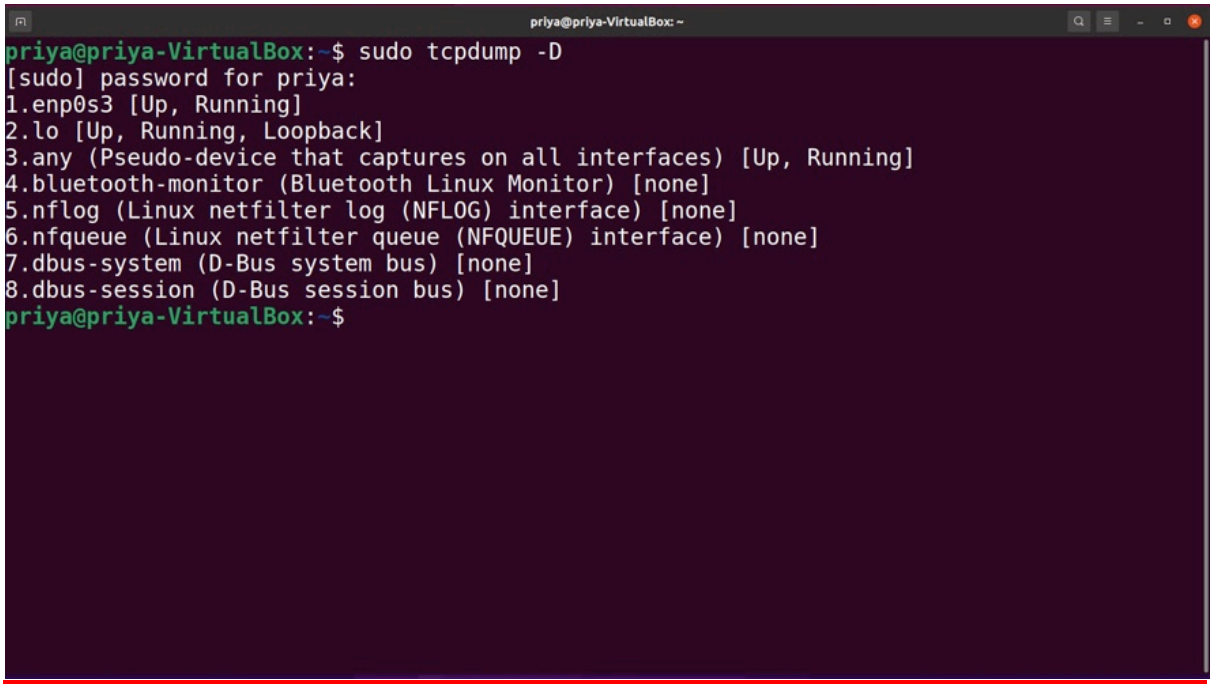


Task 4: Capturing packets with tcpdump

a)Viewing Interfaces available for packet capture

Command Used : sudo tcpdump -D

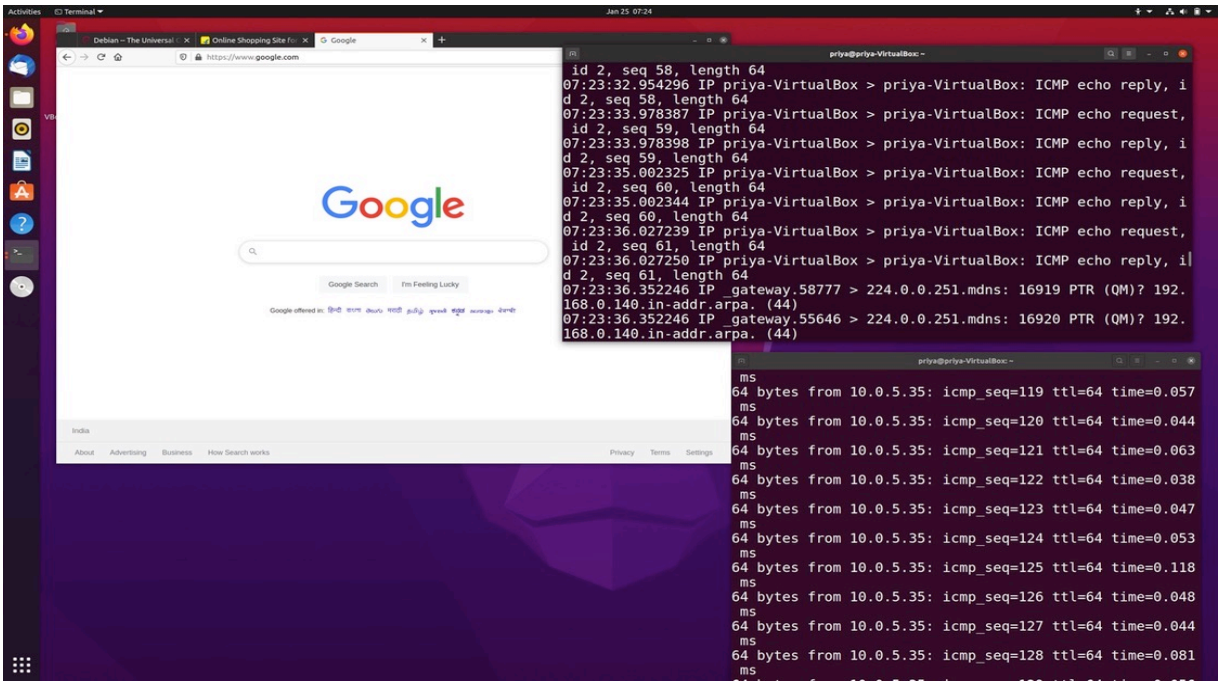
SCREENSHOT



b) Capturing packets in ‘any’ interface

Command Used : sudo tcpdump -i any

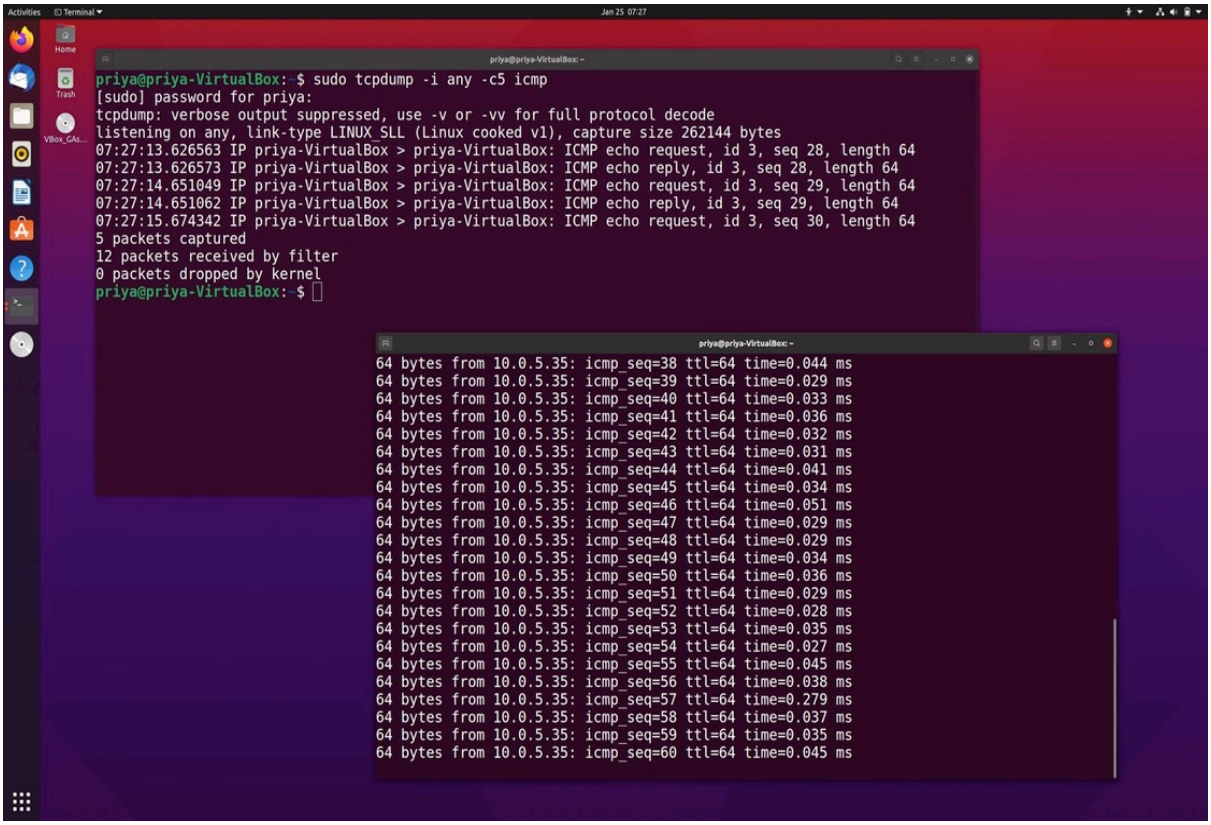
SCREENSHOT **shows the browser with www.google.com the terminal with ping 10.0.5.35 and another terminal with sudo tcpdump -i any**



c) Filtering packets based on the protocol (here its ICMP)

Command Used : sudo tcpdump -i any -c5 icmp

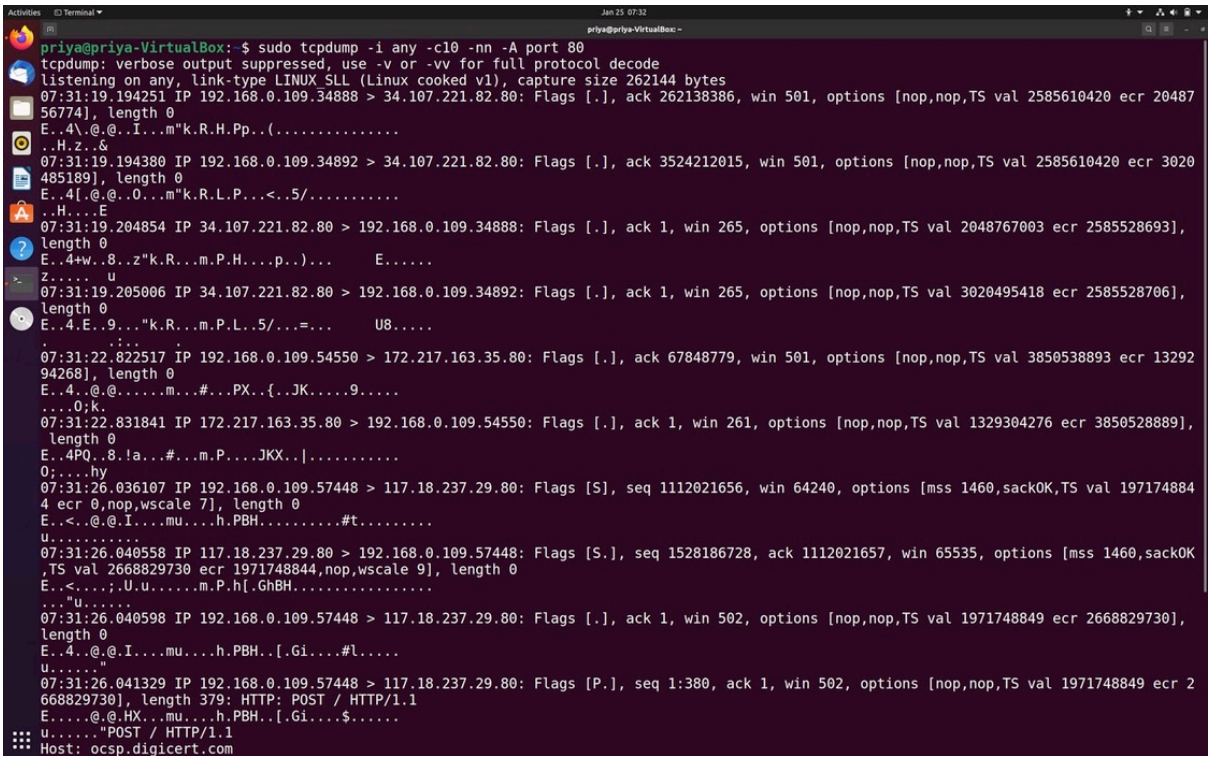
SCREENSHOT

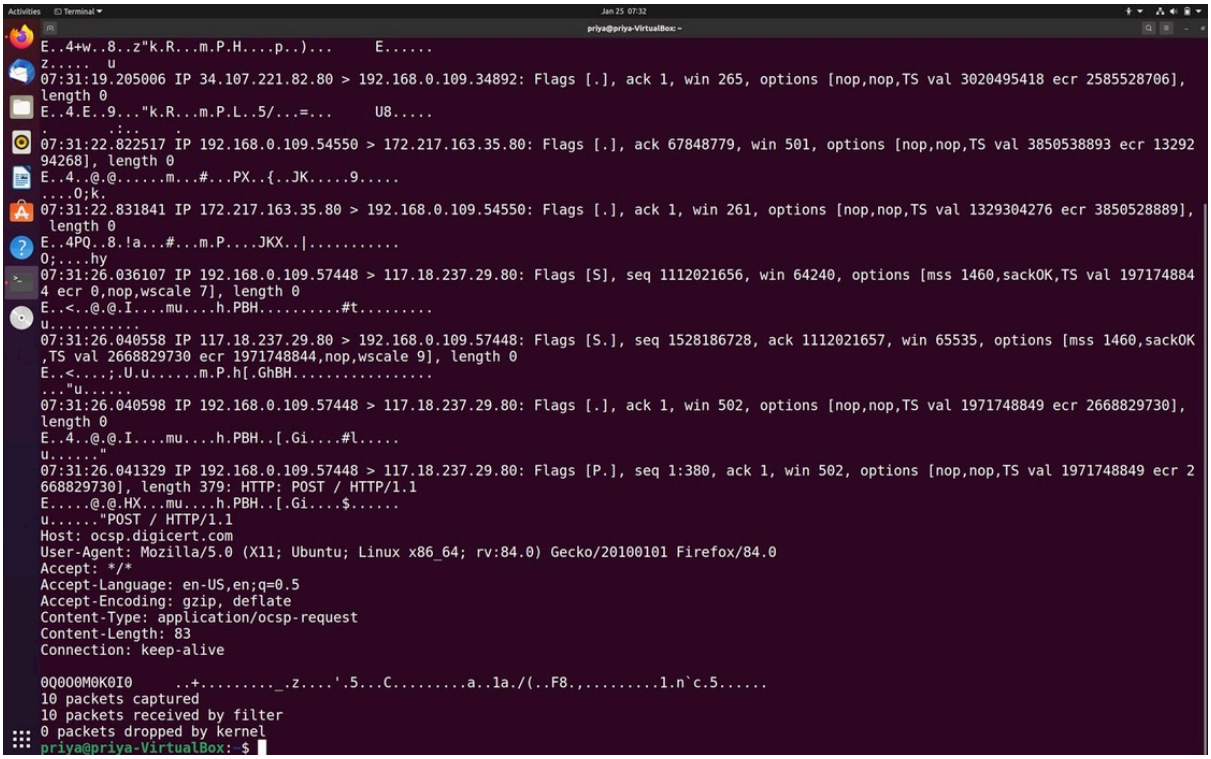


d)Checking packet content

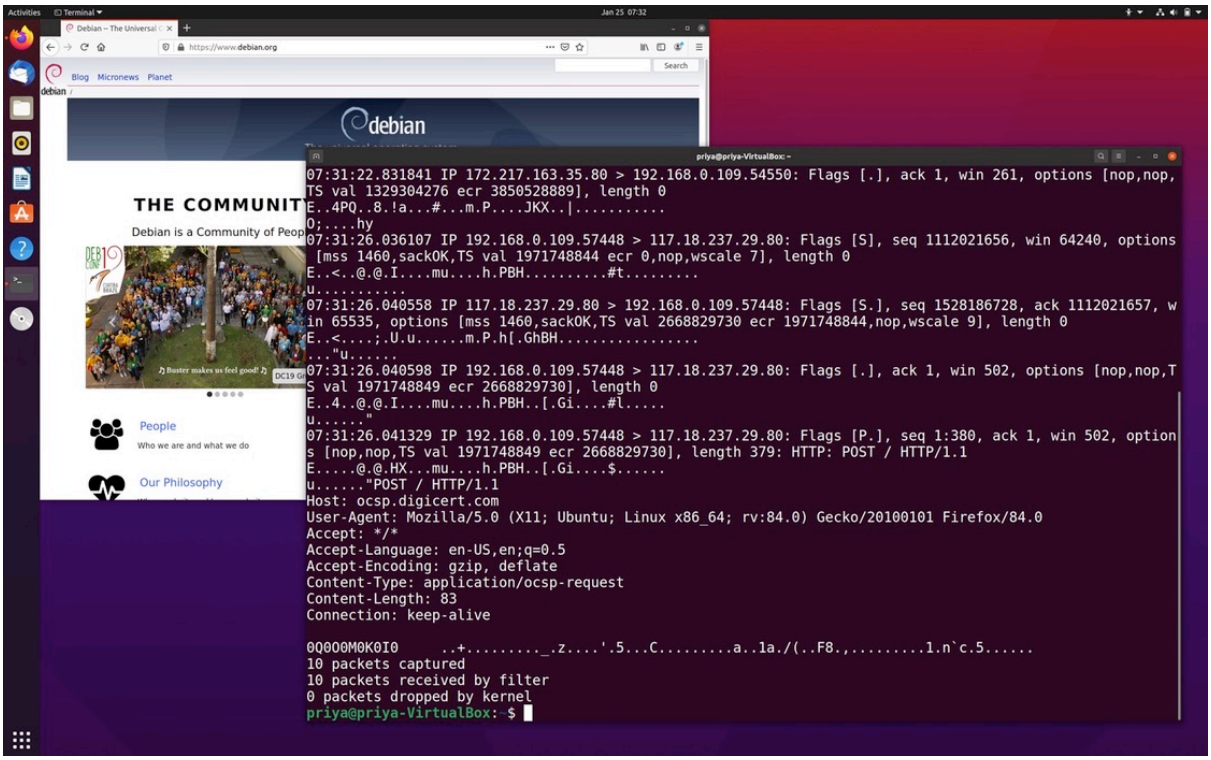
Command Used : sudo tcpdump -i any -c10 -nn -A port 80

SCREENSHOTs show the HTTP content of a web request to www.debian.org


priya@priya-VirtualBox:~$ sudo tcpdump -i any -c10 -nn -A port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
07:31:19.194251 IP 192.168.0.109.34888 > 34.107.221.82.80: Flags [.], ack 262138386, win 501, options [nop,nop,TS val 2585610420 ecr 20487
56774], length 0
E..4\.@.@..I...m"k.R.H.Pp..(.....
..H.z..&
07:31:19.194380 IP 192.168.0.109.34892 > 34.107.221.82.80: Flags [.], ack 3524212015, win 501, options [nop,nop,TS val 2585610420 ecr 3020
485189], length 0
E..4[.@.@..O...m"k.R.L.P...<..5/.....
..H....E
07:31:19.204854 IP 34.107.221.82.80 > 192.168.0.109.34888: Flags [.], ack 1, win 265, options [nop,nop,TS val 2048767003 ecr 2585528693],
length 0
E..4+w..8..z"k.R...m.P.H....p..)...   E.....
z..... u
07:31:19.205006 IP 34.107.221.82.80 > 192.168.0.109.34892: Flags [.], ack 1, win 265, options [nop,nop,TS val 3020495418 ecr 2585528706],
length 0
E..4.E..9..."k.R...m.P.L..5/...=...   U8.....
.   .:.. .
07:31:22.822517 IP 192.168.0.109.54550 > 172.217.163.35.80: Flags [.], ack 67848779, win 501, options [nop,nop,TS val 3850538893 ecr 13292
94268], length 0
E..4..@.@......m...#...PX..{..JK.....9.....
....O;k.
07:31:22.831841 IP 172.217.163.35.80 > 192.168.0.109.54550: Flags [.], ack 1, win 261, options [nop,nop,TS val 1329304276 ecr 3850528889],
 length 0
E..4PQ..8.!a...#...m.P....JKX..|..........
O;....hy
07:31:26.036107 IP 192.168.0.109.57448 > 117.18.237.29.80: Flags [S], seq 1112021656, win 64240, options [mss 1460,sackOK,TS val 197174884
4 ecr 0,nop,wscale 7], length 0
E..<..@.@.I....mu....h.PBH.........#t.........
u...........
07:31:26.040558 IP 117.18.237.29.80 > 192.168.0.109.57448: Flags [S.], seq 1528186728, ack 1112021657, win 65535, options [mss 1460,sackOK
,TS val 2668829730 ecr 1971748844,nop,wscale 9], length 0
E..<....;.U.u......m.P.h[.GhBH.................
..."u.....
07:31:26.040598 IP 192.168.0.109.57448 > 117.18.237.29.80: Flags [.], ack 1, win 502, options [nop,nop,TS val 1971748849 ecr 2668829730],
length 0
E..4..@.@.I....mu....h.PBH..[.Gi....#l.....
u......"
07:31:26.041329 IP 192.168.0.109.57448 > 117.18.237.29.80: Flags [P.], seq 1:380, ack 1, win 502, options [nop,nop,TS val 1971748849 ecr 2
668829730], length 379: HTTP: POST / HTTP/1.1
E.....@.@.HX...mu....h.PBH..[.Gi....$.....
u......"POST / HTTP/1.1
Host: ocsp.digicert.com


E..4+w..8..z"k.R...m.P.H....p..)...   E.....
z..... u
07:31:19.205006 IP 34.107.221.82.80 > 192.168.0.109.34892: Flags [.], ack 1, win 265, options [nop,nop,TS val 3020495418 ecr 2585528706],
length 0
E..4.E..9..."k.R...m.P.L..5/...=...   U8.....
.   .:.. .
07:31:22.822517 IP 192.168.0.109.54550 > 172.217.163.35.80: Flags [.], ack 67848779, win 501, options [nop,nop,TS val 3850538893 ecr 13292
94268], length 0
E..4..@.@......m...#...PX..{..JK.....9.....
....O;k.
07:31:22.831841 IP 172.217.163.35.80 > 192.168.0.109.54550: Flags [.], ack 1, win 261, options [nop,nop,TS val 1329304276 ecr 3850528889],
 length 0
E..4PQ..8.!a...#...m.P....JKX..|..........
O;....hy
07:31:26.036107 IP 192.168.0.109.57448 > 117.18.237.29.80: Flags [S], seq 1112021656, win 64240, options [mss 1460,sackOK,TS val 197174884
4 ecr 0,nop,wscale 7], length 0
E..<..@.@.I....mu....h.PBH.........#t.........
u...........
07:31:26.040558 IP 117.18.237.29.80 > 192.168.0.109.57448: Flags [S.], seq 1528186728, ack 1112021657, win 65535, options [mss 1460,sackOK
,TS val 2668829730 ecr 1971748844,nop,wscale 9], length 0
E..<....;.U.u......m.P.h[.GhBH.................
..."u.....
07:31:26.040598 IP 192.168.0.109.57448 > 117.18.237.29.80: Flags [.], ack 1, win 502, options [nop,nop,TS val 1971748849 ecr 2668829730],
length 0
E..4..@.@.I....mu....h.PBH..[.Gi....#l.....
u......"
07:31:26.041329 IP 192.168.0.109.57448 > 117.18.237.29.80: Flags [P.], seq 1:380, ack 1, win 502, options [nop,nop,TS val 1971748849 ecr 2
668829730], length 379: HTTP: POST / HTTP/1.1
E.....@.@.HX...mu....h.PBH..[.Gi....$.....
u......"POST / HTTP/1.1
Host: ocsp.digicert.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/ocsp-request
Content-Length: 83
Connection: keep-alive

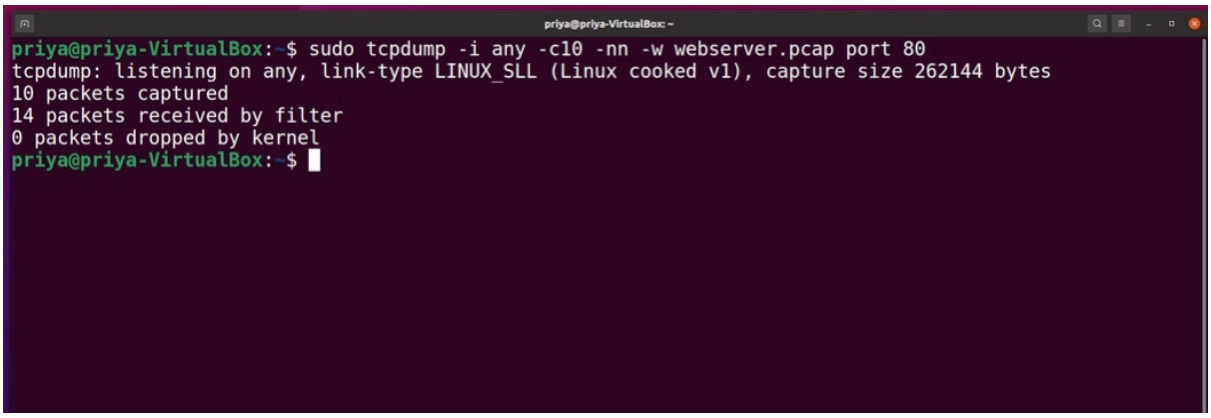
0Q0O0M0K0I0   ..+......._.z....'.5...C.........a..1a./(..F8.,.........1.n`c.5.....
10 packets captured
10 packets received by filter
0 packets dropped by kernel
priya@priya-VirtualBox:~$



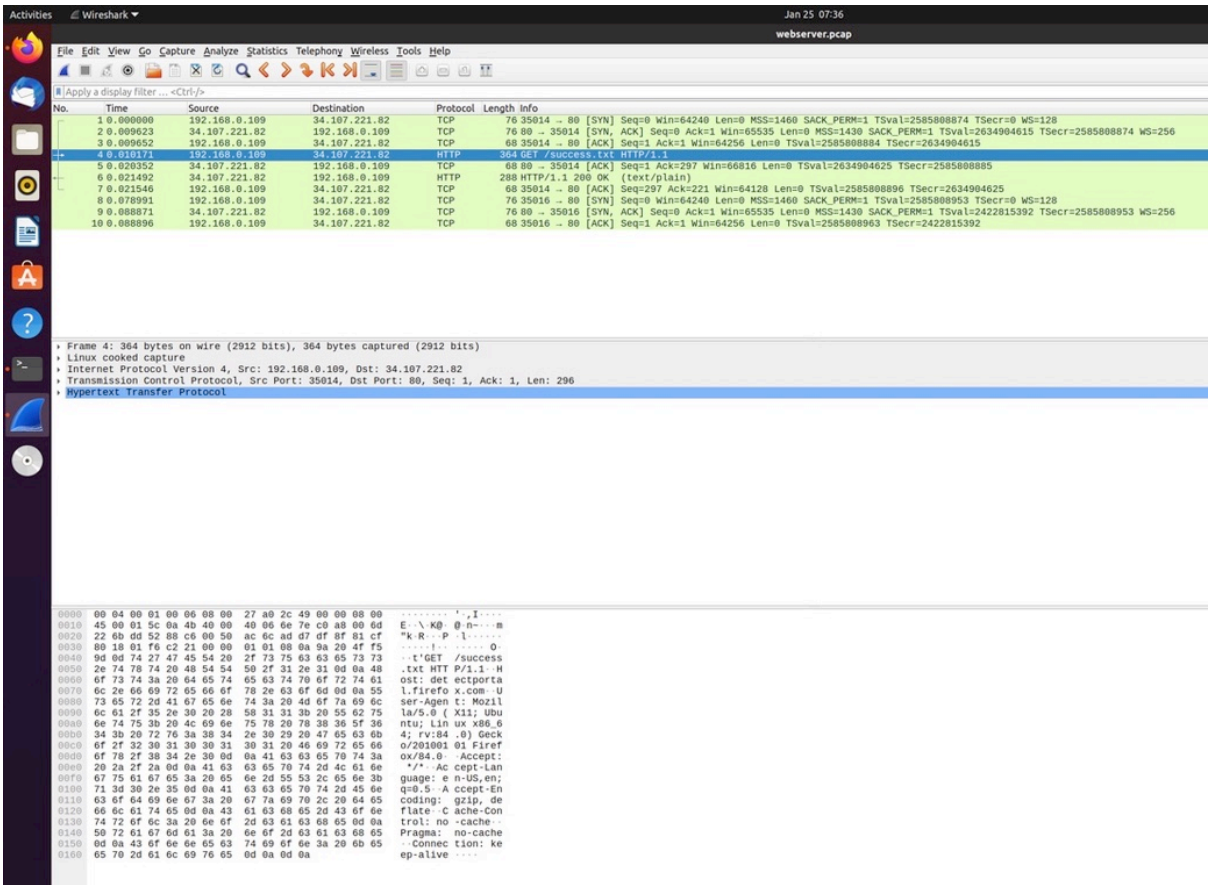
e)Saving the packet content in a file

Command Used : sudo tcpdump -i any -c10 -nn -w webserver.pcap port 80

SCREENSHOT



THE FILE WEBSERVER.PCAP



Task 5: Perform Traceroute checks

a)Traceroute to www.google.com

Command Used : sudo traceroute www.google.com

SCREENSHOT

Destination address is : 142.250.71.36

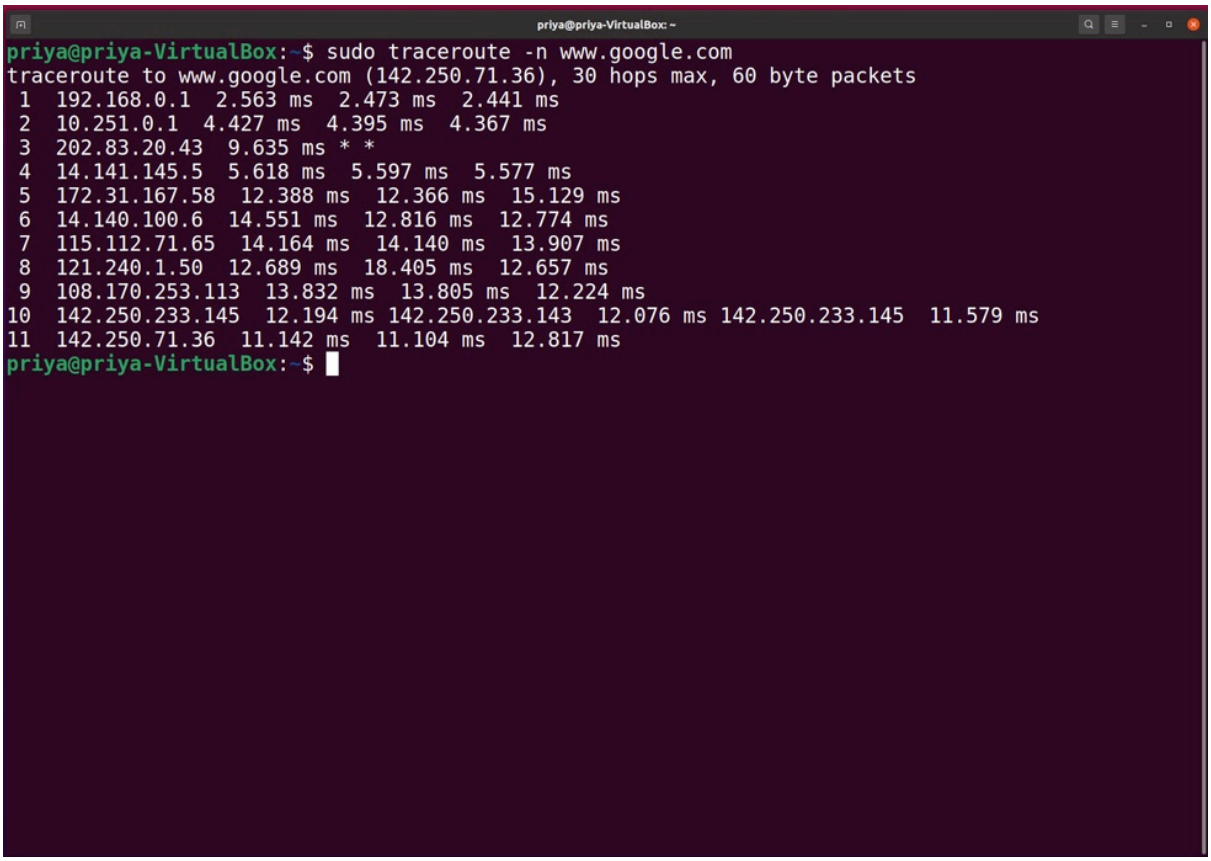
Number of Hops is :11

Maximum number of hops : 30

c) Disable the mapping of IP addresses with hostnames

Command Used : sudo traceroute -n www.google.com

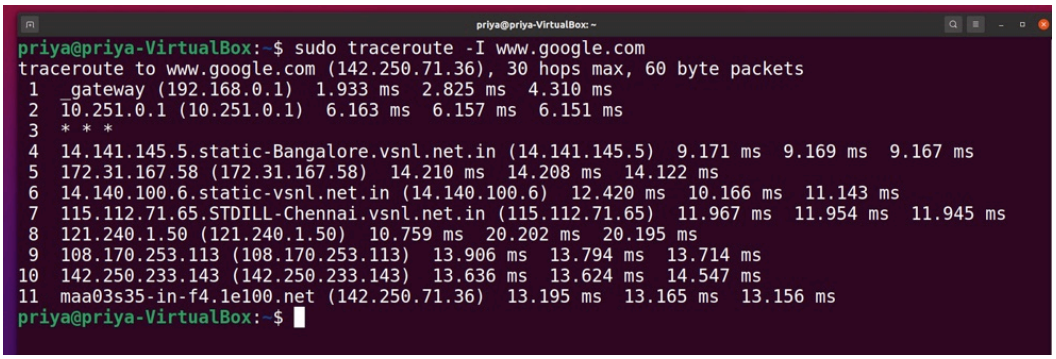
SCREENSHOT



d) Traceroute uses ICMP Protocol

Command Used : sudo traceroute -I www.google.com

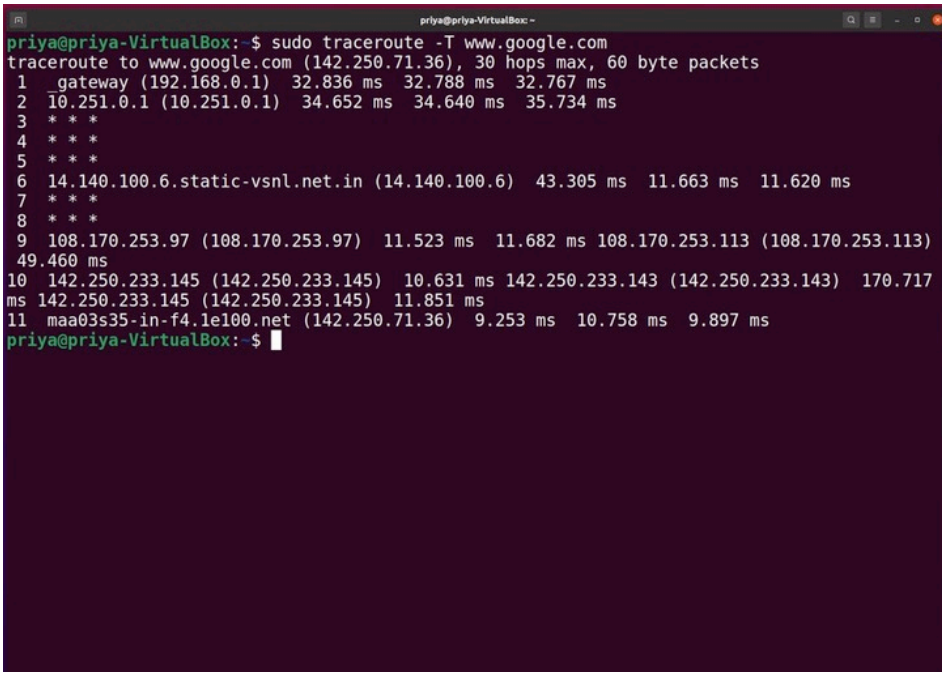
SCREENSHOT



e) Testing TCP Connection with traceroute

Command Used : sudo traceroute -I www.google.com

SCREENSHOT

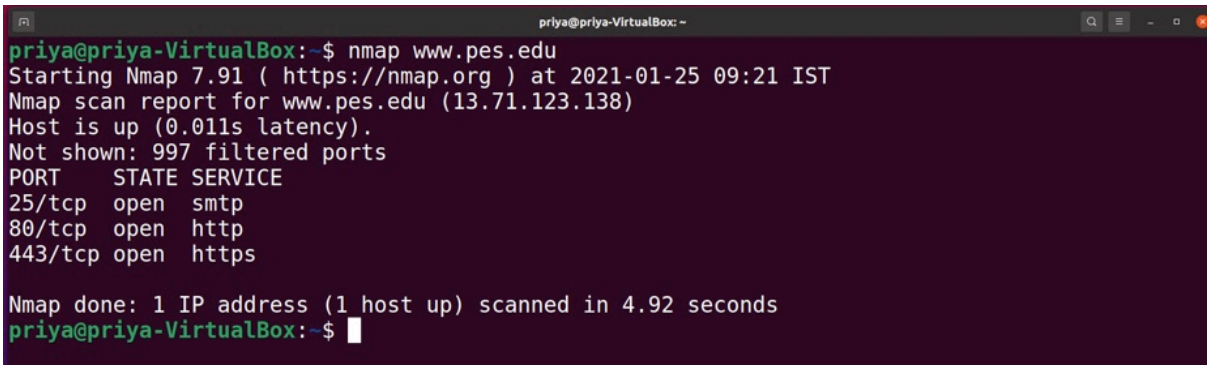


Task 6: Explore an entire network for information (Nmap)

a) scan a host using its host name

Command Used : nmap www.pes.edu

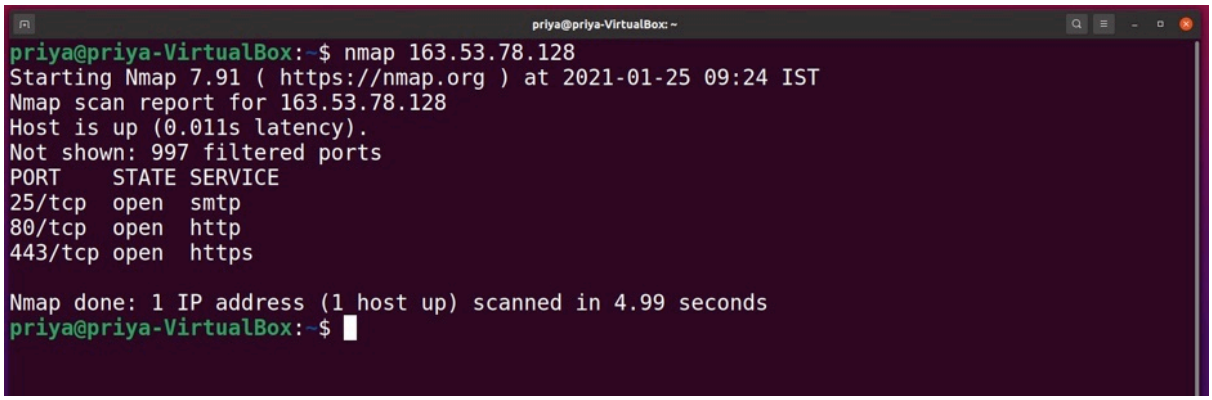
SCREENSHOT



b) Scan a host using IP Address

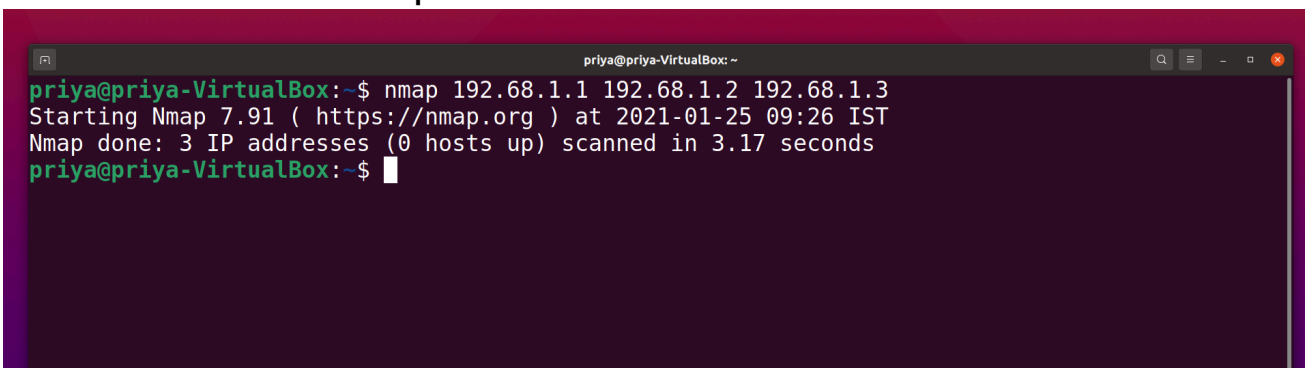
Command Used : nmap 163.53.78.128

SCREENSHOT



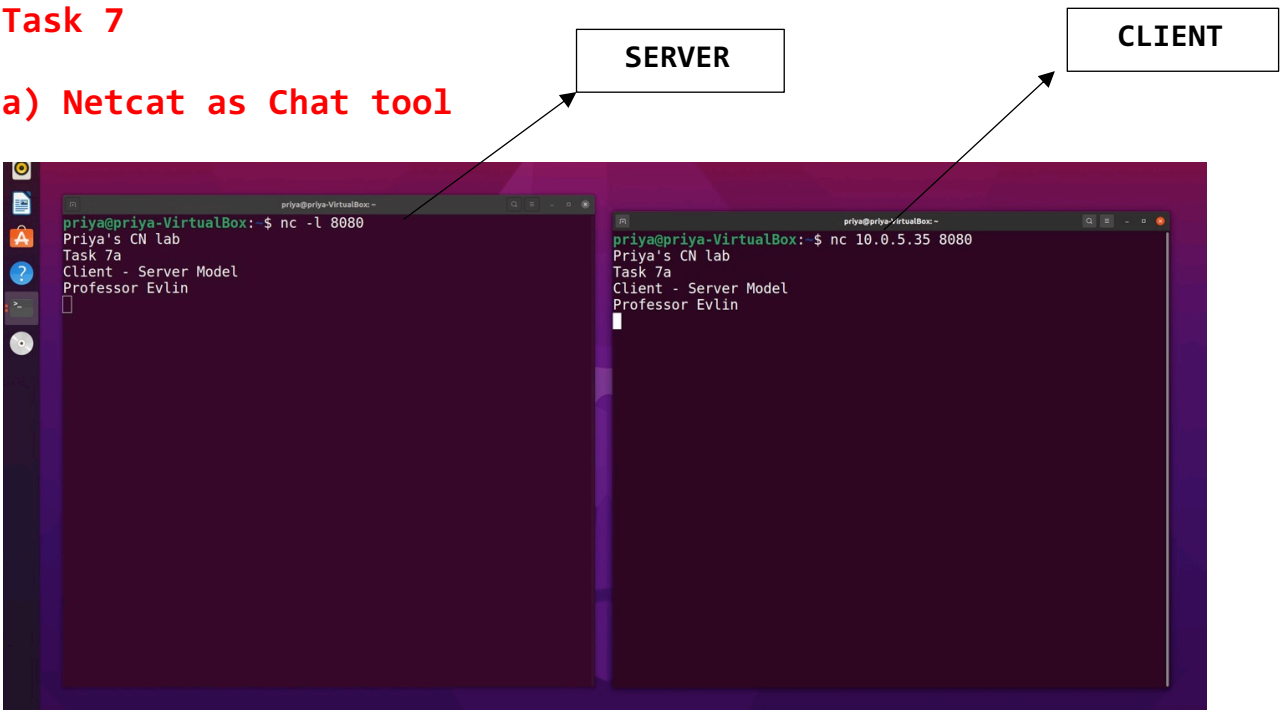
c) Scan multiple IP Addresses

Command Used : nmap 192.168.1.1 192.168.1.2 192.168.1.3



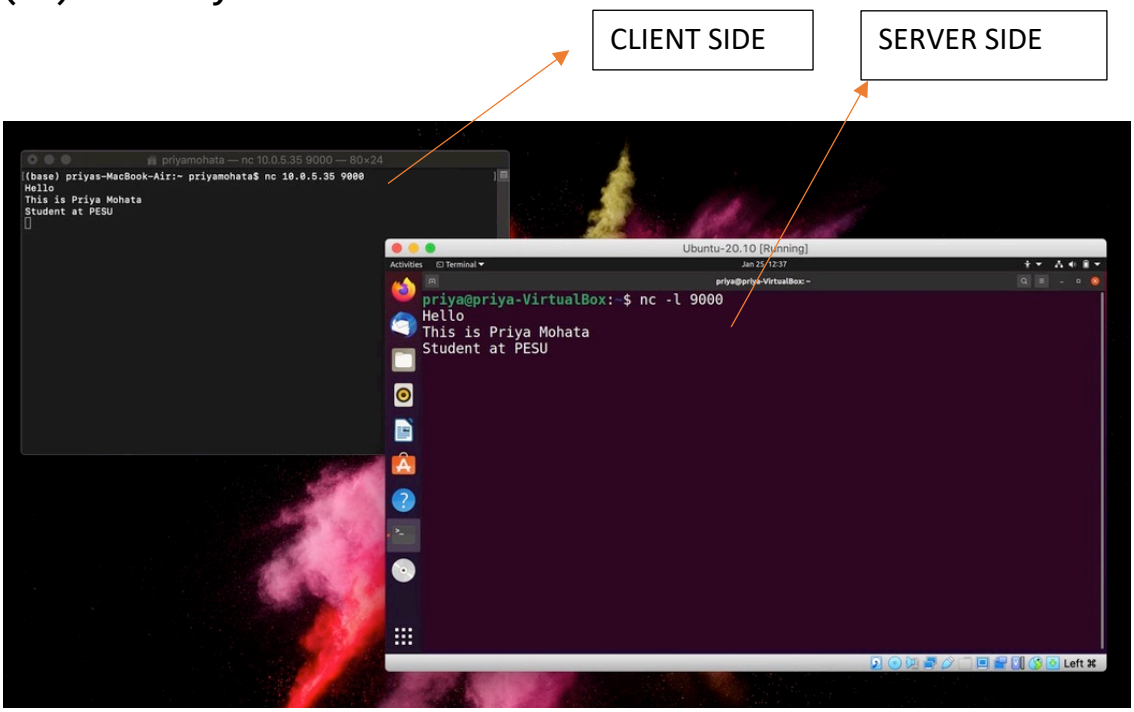
Task 7

a) Netcat as Chat tool



(i)Intra System Communication

(ii) Inter system communication

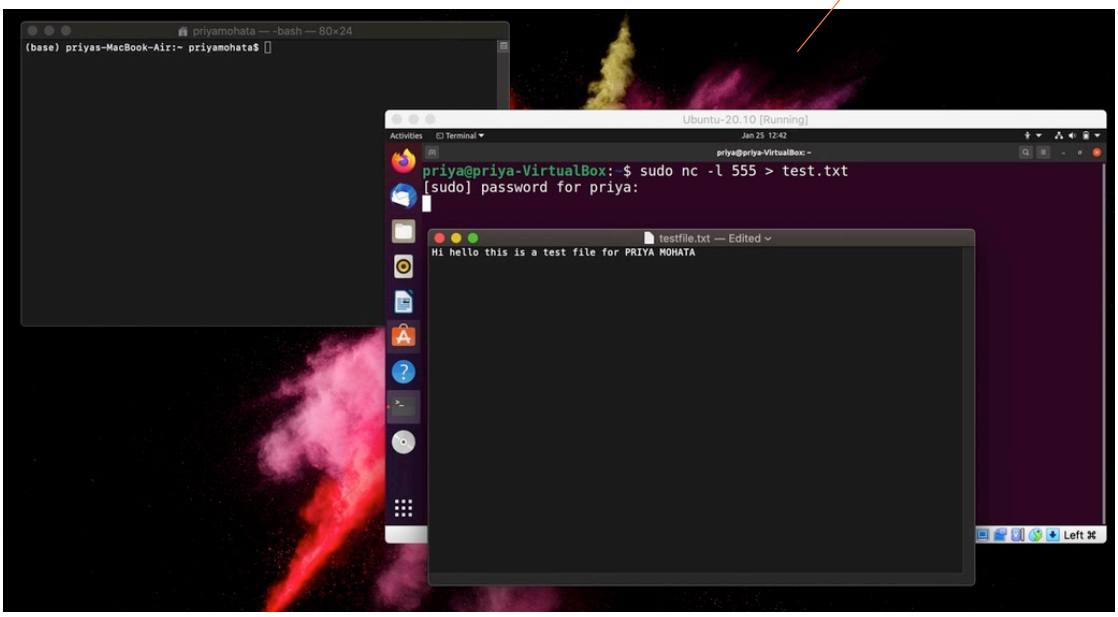


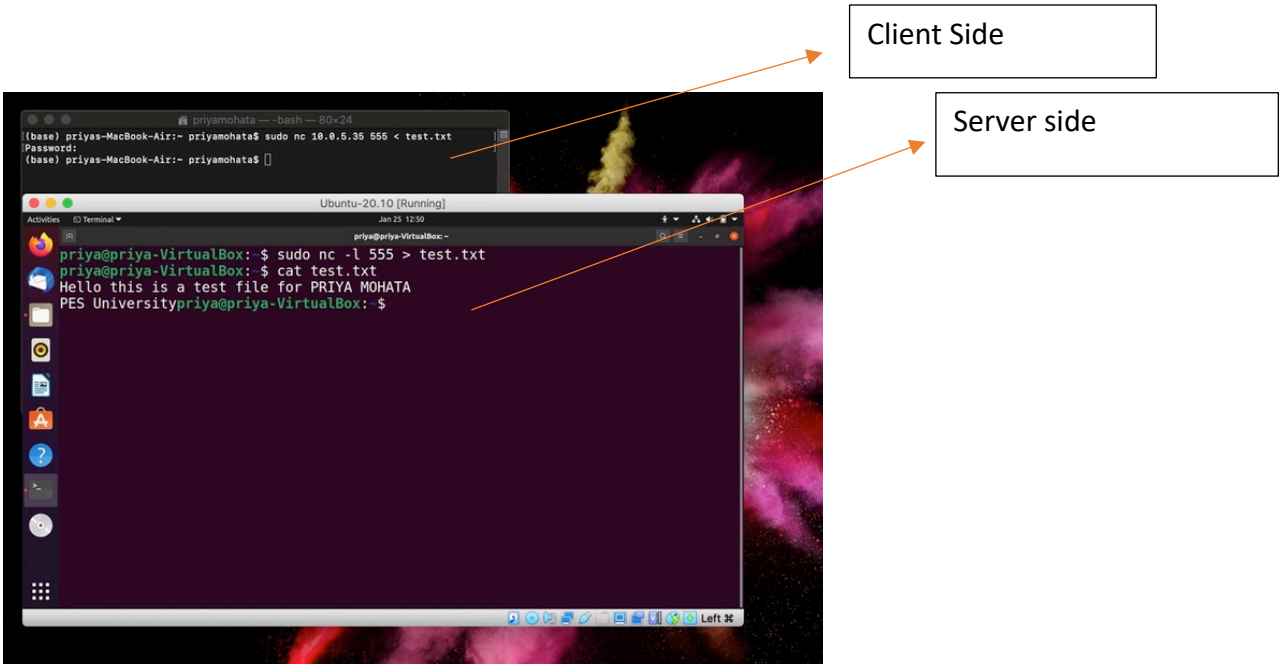
b) Use Netcat to Transfer Files

Command Used : **sudo nc -l 555 > test.txt // Server Side**

sudo nc 10.0.5.35 555 < test.txt //Client side

cat test.txt

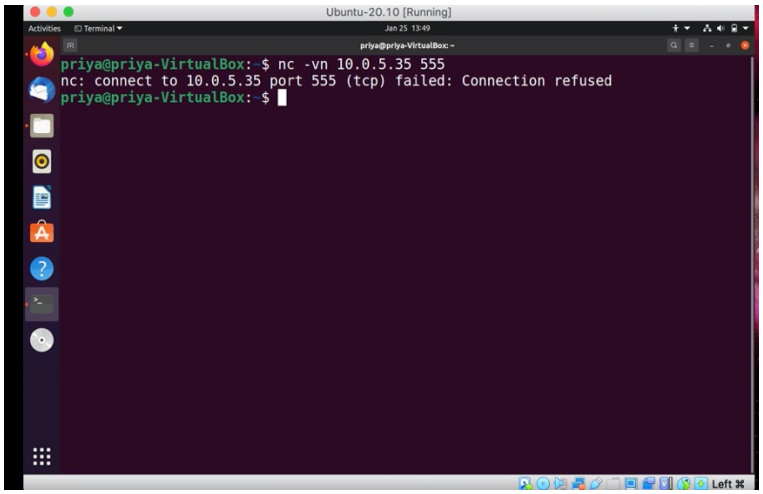




Task 7 c): Other Commands

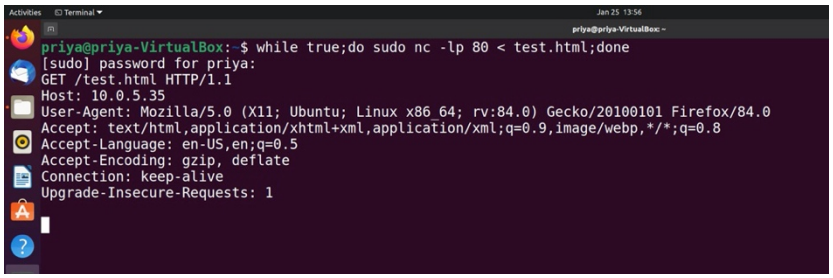
(i) To test if a particular TCP port of a remote host is open.

Command Used : nc -vn 10.0.5.35 555



(ii) Run a web server with a static web page.

Command Used : **while true; do sudo nc -lp 80 < test.html; done**



QUESTION & ANSWER

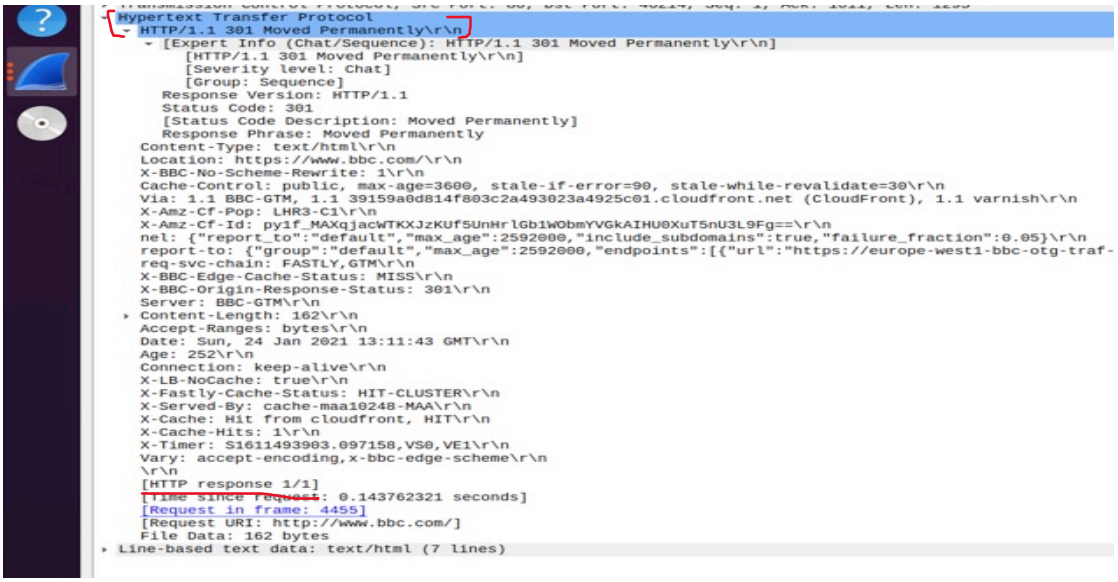
1) **Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server?**

ANSWER : The Mozilla Firefox is running on the HTTP Version 1.1.

We can observe this in the screenshot below :

GET /HTTP/1.1\r\n

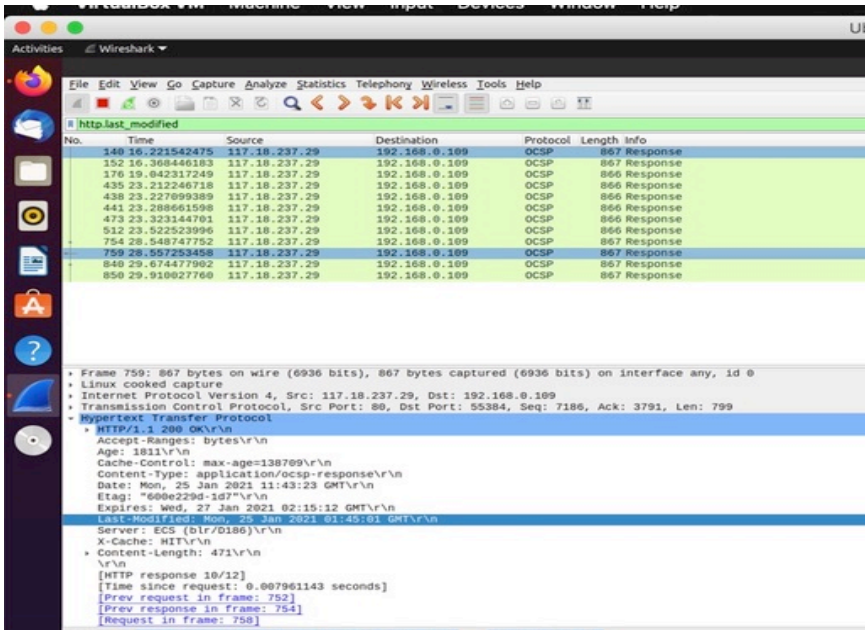
The web server also is running on the HTTP Version 1.1



2) **When was the HTML file that you are retrieving last modified at the server?**

ANSWER :In the filter tab of wireshark type ‘http.last_modified’

Example : In the example below last modified is Mon,25 Jan 2021 , 01:45:01 GMT

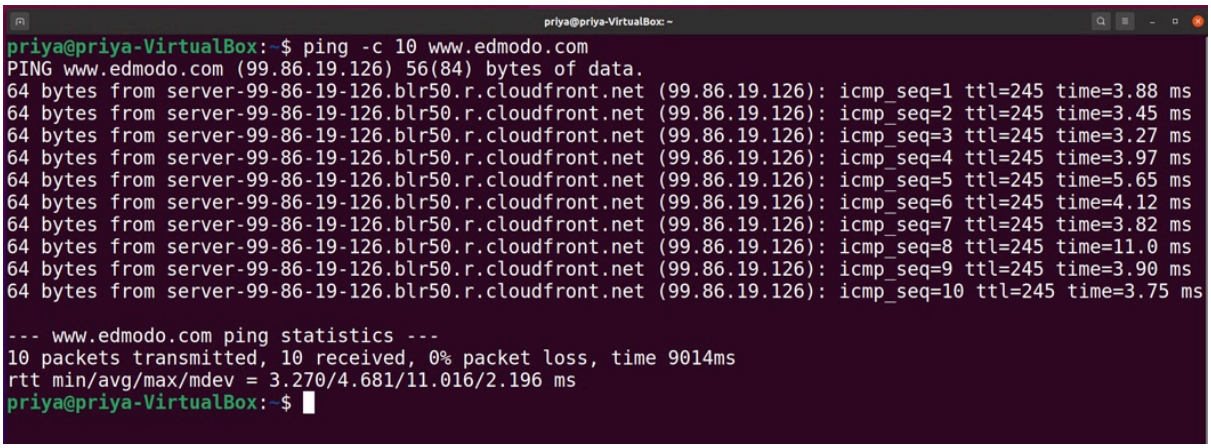


3) **How to tell ping to exit after a specified number of ECHO_REQUEST packets?**

ANSWER : Ping continuously sends the ICMP packets until it receives an interrupt signal.To specify the number of packets we use the -c flag followed by the number of packets

Command Used in the example : ping -c 10 www.edmodo.com

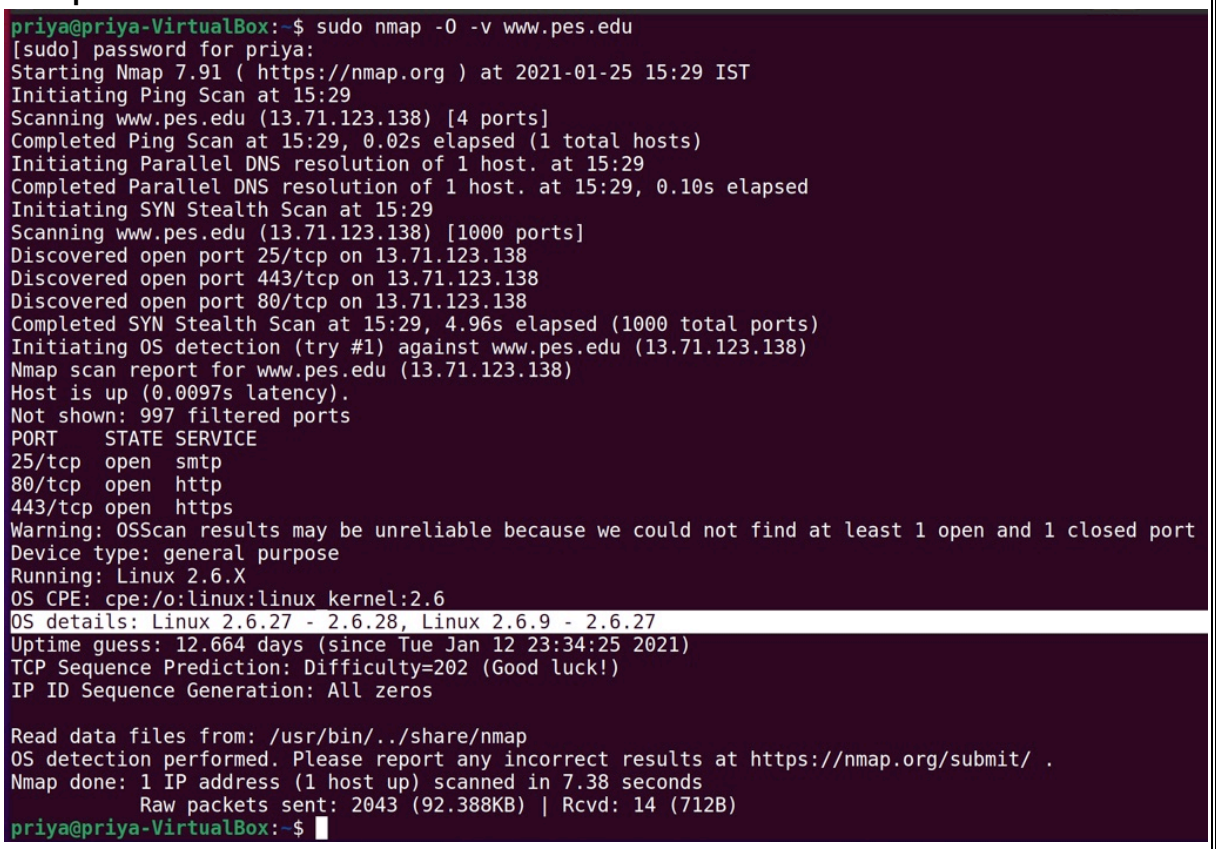
Example :



4) **How will you identify remote host apps and OS?**

ANSWER : We can use nmap -O -v {domain name}

Example :


priya@priya-VirtualBox:~$ sudo nmap -O -v www.pes.edu
[sudo] password for priya:
Starting Nmap 7.91 (https://nmap.org) at 2021-01-25 15:29 IST
Initiating Ping Scan at 15:29
Scanning www.pes.edu (13.71.123.138) [4 ports]
Completed Ping Scan at 15:29, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:29
Completed Parallel DNS resolution of 1 host. at 15:29, 0.10s elapsed
Initiating SYN Stealth Scan at 15:29
Scanning www.pes.edu (13.71.123.138) [1000 ports]
Discovered open port 25/tcp on 13.71.123.138
Discovered open port 443/tcp on 13.71.123.138
Discovered open port 80/tcp on 13.71.123.138
Completed SYN Stealth Scan at 15:29, 4.96s elapsed (1000 total ports)
Initiating OS detection (try #1) against www.pes.edu (13.71.123.138)
Nmap scan report for www.pes.edu (13.71.123.138)
Host is up (0.0097s latency).
Not shown: 997 filtered ports
PORT STATE SERVICE
25/tcp open smtp
80/tcp open http
443/tcp open https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux kernel:2.6
OS details: Linux 2.6.27 - 2.6.28, Linux 2.6.9 - 2.6.27
Uptime guess: 12.664 days (since Tue Jan 12 23:34:25 2021)
TCP Sequence Prediction: Difficulty=202 (Good luck!)
IP ID Sequence Generation: All zeros
Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.38 seconds
Raw packets sent: 2043 (92.388KB) | Rcvd: 14 (712B)
priya@priya-VirtualBox:~$