COMPUTER NETWORKS LAB

WEEK 1

ABHISHEK ADITYA BS

PES1UG19CS019

SECTION A

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

1.1 : To display status of all active network interfaces.

ip addr show

```
abhishek@abhishek-VirtualBox:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:22:91:ab brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 86397sec preferred_lft 86397sec
    inet6 fe80::7c83:14bb:df8b:54b3/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
abhishek@abhishek-VirtualBox:~$
```

Interface Name	IPv4/IPv6	MAC Address
lo	127.0.0.1/::1	00:00:00:00:00:00
enp0s3	10.0.2.15/fe80::7c83:14bb:df8b:54b3	08:00:27:22:91:ab

1.2) Assigning IP Address

sudo ip addr add 10.0.1.18/24 dev enp0s3

Now, we add an IP address to the Interface **enp0s3**.The IP Address being added is 10.0.1.18

```
abhishek@abhishek-VirtualBox: ~
abhishek@abhishek-VirtualBox:~$ sudo ip addr add 10.0.1.18/24 dev enp0s3
[sudo] password for abhishek:
abhishek@abhishek-VirtualBox:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:22:91:ab brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 86240sec preferred_lft 86240sec
    inet 10.0.1.18/24 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::7c83:14bb:df8b:54b3/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
abhishek@abhishek-VirtualBox:~$
```

We observe that the IP Address is added to the Interface enp0s3.

1.3 : To activate/deactivate a network interface

Deactivating enp0s3

sudo ifconfig enp0s3 down

```
abhishek@abhishek-VirtualBox:~$ sudo ifconfig enp0s3 down
abhishek@abhishek-VirtualBox:~$ ifconfig
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 3352  bytes 325563 (325.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3352  bytes 325563 (325.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

abhishek@abhishek-VirtualBox:~$
```

Activating enp0s3

sudo ifconfig enp0s3 up

```
abhishek@abhishek-VirtualBox:~$ sudo ifconfig enp0s3 up
abhishek@abhishek-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::7c83:14bb:df8b:54b3  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:22:91:ab  txqueuelen 1000  (Ethernet)
        RX packets 285043  bytes 350192845 (350.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 77585  bytes 9766366 (9.7 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 3404  bytes 329515 (329.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3404  bytes 329515 (329.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

abhishek@abhishek-VirtualBox:~$
```

1.4 : To show the current neighbour table in kernel

ip neigh

```
abhishek@abhishek-VirtualBox:~$ ip neigh
10.0.2.2 dev enp0s3 lladdr 52:54:00:12:35:02 REACHABLE
abhishek@abhishek-VirtualBox:~$
```

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

```
abhishek@abhishek-VirtualBox:~$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.021 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.064 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.065 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.055 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.067 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.042 ms
64 bytes from 10.0.2.15: icmp_seq=7 ttl=64 time=0.064 ms
64 bytes from 10.0.2.15: icmp_seq=8 ttl=64 time=0.066 ms
64 bytes from 10.0.2.15: icmp_seq=9 ttl=64 time=0.052 ms
64 bytes from 10.0.2.15: icmp_seq=10 ttl=64 time=0.043 ms
64 bytes from 10.0.2.15: icmp_seq=11 ttl=64 time=0.060 ms
64 bytes from 10.0.2.15: icmp_seq=12 ttl=64 time=0.060 ms
64 bytes from 10.0.2.15: icmp_seq=13 ttl=64 time=0.065 ms
64 bytes from 10.0.2.15: icmp_seq=14 ttl=64 time=0.068 ms
64 bytes from 10.0.2.15: icmp_seq=15 ttl=64 time=0.069 ms
64 bytes from 10.0.2.15: icmp_seq=16 ttl=64 time=0.062 ms
64 bytes from 10.0.2.15: icmp_seq=17 ttl=64 time=0.065 ms
64 bytes from 10.0.2.15: icmp_seq=18 ttl=64 time=0.065 ms
64 bytes from 10.0.2.15: icmp_seq=19 ttl=64 time=0.065 ms
^C
--- 10.0.2.15 ping statistics ---
19 packets transmitted, 19 received, 0% packet loss, time 18438ms
rtt min/avg/max/mdev = 0.021/0.058/0.069/0.011 ms
abhishek@abhishek-VirtualBox:~$
```

ping 10.0.2.15

TTL	64
Protocol used by ping	ICMP
Time	Order of 10^{-2} ms

```
▸ Frame 1: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
▾ Linux cooked capture
    Packet type: Unicast to us (0)
    Link-layer address type: 772
    Link-layer address length: 6
    Source: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Unused: 0000
    Protocol: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.15
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xf377 (62327)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x2f14 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.15
    Destination: 10.0.2.15
▾ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x45aa [correct]
    [Checksum Status: Good]
    Identifier (BE): 10 (0x000a)
    Identifier (LE): 2560 (0x0a00)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Response frame: 2]
    Timestamp from icmp data: Jan 23, 2021 00:57:08.000000000 IST
    [Timestamp from icmp data (relative): 0.323813531 seconds]
  ▸ Data (48 bytes)
```

Request Packet

```
▸ Frame 2: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
▾ Linux cooked capture
    Packet type: Unicast to us (0)
    Link-layer address type: 772
    Link-layer address length: 6
    Source: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Unused: 0000
    Protocol: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.15
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xf378 (62328)
  ▸ Flags: 0x0000
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x6f13 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.15
    Destination: 10.0.2.15
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x4daa [correct]
    [Checksum Status: Good]
    Identifier (BE): 10 (0x000a)
    Identifier (LE): 2560 (0x0a00)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Request frame: 1]
    [Response time: 0.007 ms]
    Timestamp from icmp data: Jan 23, 2021 00:57:08.000000000 IST
    [Timestamp from icmp data (relative): 0.323820454 seconds]
  ▸ Data (48 bytes)
```

Response Packet

Details	First Echo Request	First Echo Reply
Frame Number	1	2
Source IP address	10.0.2.15	10.0.2.15
Destination IP address	10.0.2.15	10.0.2.15
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	IPv4	IPv4
Time to Live (TTL)	64	64

Task 3 : HTTP PDU Capture

Echo Request and Reply

```
▸ Frame 38: 862 bytes on wire (6896 bits), 862 bytes captured (6896 bits) on interface any, id 0
▾ Linux cooked capture
    Packet type: Sent by us (4)
    Link-layer address type: 1
    Link-layer address length: 6
    Source: PcsCompu_22:91:ab (08:00:27:22:91:ab)
    Unused: 0000
    Protocol: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 163.53.78.110
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 846
    Identification: 0x5f6a (24426)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xda8d [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.15
    Destination: 163.53.78.110
▸ Transmission Control Protocol, Src Port: 37002, Dst Port: 80, Seq: 1, Ack: 1, Len: 806
▾ Hypertext Transfer Protocol
  ▸ GET / HTTP/1.1\r\n
    Host: www.flipkart.com\r\n
    Connection: keep-alive\r\n
    DNT: 1\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.96 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
  ▸ [truncated]Cookie: SN=VI994B16C8869043298B2A5020B473C388.TOKF1C151D6616C4643885A4CA85DEB9E39.1611318822.LO; AMCV_17EB401053DAF4840A490D4C%40AdobeOrg=
    \r\n
    [Full request URI: http://www.flipkart.com/]
    [HTTP request 1/1]
    [Response in frame: 50]
```

Request Packet

```
▸ Frame 50: 403 bytes on wire (3224 bits), 403 bytes captured (3224 bits) on interface any, id 0
▾ Linux cooked capture
      Packet type: Unicast to us (0)
      Link-layer address type: 1
      Link-layer address length: 6
      Source: RealtekU_12:35:02 (52:54:00:12:35:02)
      Unused: 0000
      Protocol: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 163.53.78.110, Dst: 10.0.2.15
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 387
      Identification: 0x8408 (33800)
    ▸ Flags: 0x0000
      Fragment offset: 0
      Time to live: 64
      Protocol: TCP (6)
      Header checksum: 0xf7ba [validation disabled]
      [Header checksum status: Unverified]
      Source: 163.53.78.110
      Destination: 10.0.2.15
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 37002, Seq: 1, Ack: 807, Len: 347
▾ Hypertext Transfer Protocol
    ▸ HTTP/1.1 301 Moved Permanently\r\n
      Server: nginx\r\n
      Date: Fri, 22 Jan 2021 20:10:15 GMT\r\n
      Content-Type: text/html\r\n
    ▸ Content-Length: 178\r\n
      Location: https://www.flipkart.com/\r\n
      \r\n
      [HTTP response 1/1]
      [Time since request: 0.050968952 seconds]
      [Request in frame: 38]
      [Request URI: http://www.flipkart.com/]
      File Data: 178 bytes
▸ Line-based text data: text/html (7 lines)
```

Response Packet

Details	First Echo Request	First Echo Reply
Frame Number	38	50
Source Port	37002	80
Destination Port	80	37002
Source IP Address	10.0.2.15	163.53.78.110
Destination IP Address	163.53.78.110	10.0.2.15
Source Ethernet Address	08:00:27:22:91:ab	52:54:00:12:35:02
Destination Ethernet Address	52:54:00:12:35:02	08:00:27:22:91:ab

Connection details

HTTP Request Response

HTTP Request		HTTP Response	
Get	GET / HTTP/1.1\r\n	Server	nginx
Host	www.flipkart.com	Content-Type	text/html
User-Agent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.96 /Safari/537.36	Date	Fri, 22 Jan 2021 20:10:15 GMT
Accept-Language	en-GB, en-US;q=0.9,en;q=0.8	Location	https://www.flipkart.com
Accept-Encoding	gzip , deflate	Content-Length	178
Connection	Keep-alive	Connection	Keep-alive

Following TCP Stream

Wireshark · Follow TCP Stream (tcp.stream eq 12) · any

```
GET / HTTP/1.1
Host: www.flipkart.com
Connection: keep-alive
DNT: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.96 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: SN=VI994B16C8869043298B2A5020B473C308.TOKF1C151D6616C4643885A4CA85DEB9E39.1611318822.LO;
AMCV_17EB401053DAF4840A490D4C%40AdobeOrg=-227196251%7CMCIDTS%7C18650%7CMCMID%7C23996836177534371110325534852811858690%7CMCAAMLH-1611923624%7C12%7CMCAAMB-1611923624%7C6G1ynYcLPuiQxYZrsz_pkqfLG9yMXBpb2zX
5dvJdYQJzPXImdj0y%7CMCOPTOUT-1611326025s%7CNONE%7CMCAID%7CNONE

HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Fri, 22 Jan 2021 20:10:15 GMT
Content-Type: text/html
Content-Length: 178
Location: https://www.flipkart.com/

<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

Task 4 : Capturing packets with tcpdump

4.1 : Viewing Interfaces available for Capture

sudo tcpdump -D

```
abhishek@abhishek-VirtualBox:~$ sudo tcpdump -D
1.enp0s3 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.bluetooth-monitor (Bluetooth Linux Monitor) [none]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
abhishek@abhishek-VirtualBox:~$
```

4.2 : Capturing all Packets in any Interface

sudo tcpdump -i any

```
abhishek@abhishek-VirtualBox:~$ sudo tcpdump -i any
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
20:32:09.385229 IP abhishek-VirtualBox > broadband.actcorp.in: ICMP echo request, id 11, seq 4, length 64
20:32:09.386580 IP localhost.53520 > localhost.domain: 34879+ [1au] PTR? 192.145.51.106.in-addr.arpa. (56)
20:32:09.387009 IP localhost.domain > localhost.53520: 34879 1/0/1 PTR broadband.actcorp.in. (90)
20:32:09.387226 IP localhost.55286 > localhost.domain: 4990+ [1au] PTR? 15.2.0.10.in-addr.arpa. (51)
20:32:09.387480 IP abhishek-VirtualBox.45698 > 192.168.0.1.domain: 62136+ [1au] PTR? 15.2.0.10.in-addr.arpa. (51)
20:32:09.411572 IP localhost.35145 > localhost.domain: 36925+ [1au] PTR? 53.0.0.127.in-addr.arpa. (52)
20:32:09.412411 IP localhost.43187 > localhost.domain: 40490+ [1au] PTR? 1.0.168.192.in-addr.arpa. (53)
20:32:09.412693 IP abhishek-VirtualBox.57240 > 192.168.0.1.domain: 12361+ [1au] PTR? 1.0.168.192.in-addr.arpa. (53)
20:32:09.420931 IP 192.168.0.1.domain > abhishek-VirtualBox.57240: 12361 NXDomain 0/1/1 (130)
20:32:09.421261 IP abhishek-VirtualBox.57240 > 192.168.0.1.domain: 12361+ PTR? 1.0.168.192.in-addr.arpa. (42)
20:32:10.386307 IP abhishek-VirtualBox > broadband.actcorp.in: ICMP echo request, id 11, seq 5, length 64
20:32:10.389953 IP broadband.actcorp.in > abhishek-VirtualBox: ICMP echo reply, id 11, seq 5, length 64
20:32:11.388455 IP abhishek-VirtualBox > broadband.actcorp.in: ICMP echo request, id 11, seq 6, length 64
20:32:11.397177 IP broadband.actcorp.in > abhishek-VirtualBox: ICMP echo reply, id 11, seq 6, length 64
20:32:12.391242 IP abhishek-VirtualBox > broadband.actcorp.in: ICMP echo request, id 11, seq 7, length 64
20:32:12.410473 IP broadband.actcorp.in > abhishek-VirtualBox: ICMP echo reply, id 11, seq 7, length 64
20:32:13.392966 IP abhishek-VirtualBox > broadband.actcorp.in: ICMP echo request, id 11, seq 8, length 64
20:32:13.397202 IP broadband.actcorp.in > abhishek-VirtualBox: ICMP echo reply, id 11, seq 8, length 64
20:32:14.395026 IP abhishek-VirtualBox > broadband.actcorp.in: ICMP echo request, id 11, seq 9, length 64
20:32:14.399714 IP broadband.actcorp.in > abhishek-VirtualBox: ICMP echo reply, id 11, seq 9, length 64
20:32:15.395231 IP abhishek-VirtualBox > broadband.actcorp.in: ICMP echo request, id 11, seq 10, length 64
20:32:15.413097 IP broadband.actcorp.in > abhishek-VirtualBox: ICMP echo reply, id 11, seq 10, length 64
20:32:16.397184 IP abhishek-VirtualBox > broadband.actcorp.in: ICMP echo request, id 11, seq 11, length 64
20:32:16.401620 IP broadband.actcorp.in > abhishek-VirtualBox: ICMP echo reply, id 11, seq 11, length 64
20:32:17.398942 IP abhishek-VirtualBox > broadband.actcorp.in: ICMP echo request, id 11, seq 12, length 64
20:32:17.404616 IP broadband.actcorp.in > abhishek-VirtualBox: ICMP echo reply, id 11, seq 12, length 64
20:32:17.517064 ARP, Request who-has _gateway tell abhishek-VirtualBox, length 28
20:32:17.517656 ARP, Reply _gateway is-at 52:54:00:12:35:02 (oui Unknown), length 46
20:32:17.517810 IP localhost.50849 > localhost.domain: 45266+ [1au] PTR? 2.2.0.10.in-addr.arpa. (50)
```

4.3 : Filtering Packets based on Protocol

sudo tcpdump -i any -c5 icmp

```
abhishek@abhishek-VirtualBox:~$ sudo tcpdump -i any -c5 icmp
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
20:36:05.996074 IP abhishek-VirtualBox > broadband.actcorp.in: ICMP echo request, id 11, seq 240, length 64
20:36:05.999490 IP broadband.actcorp.in > abhishek-VirtualBox: ICMP echo reply, id 11, seq 240, length 64
20:36:06.998044 IP abhishek-VirtualBox > broadband.actcorp.in: ICMP echo request, id 11, seq 241, length 64
20:36:07.002011 IP broadband.actcorp.in > abhishek-VirtualBox: ICMP echo reply, id 11, seq 241, length 64
20:36:07.999156 IP abhishek-VirtualBox > broadband.actcorp.in: ICMP echo request, id 11, seq 242, length 64
5 packets captured
5 packets received by filter
0 packets dropped by kernel
abhishek@abhishek-VirtualBox:~$
```

4.5 : Checking Packet Content

sudo tcpdump -i any -c10 -nn -A port 80

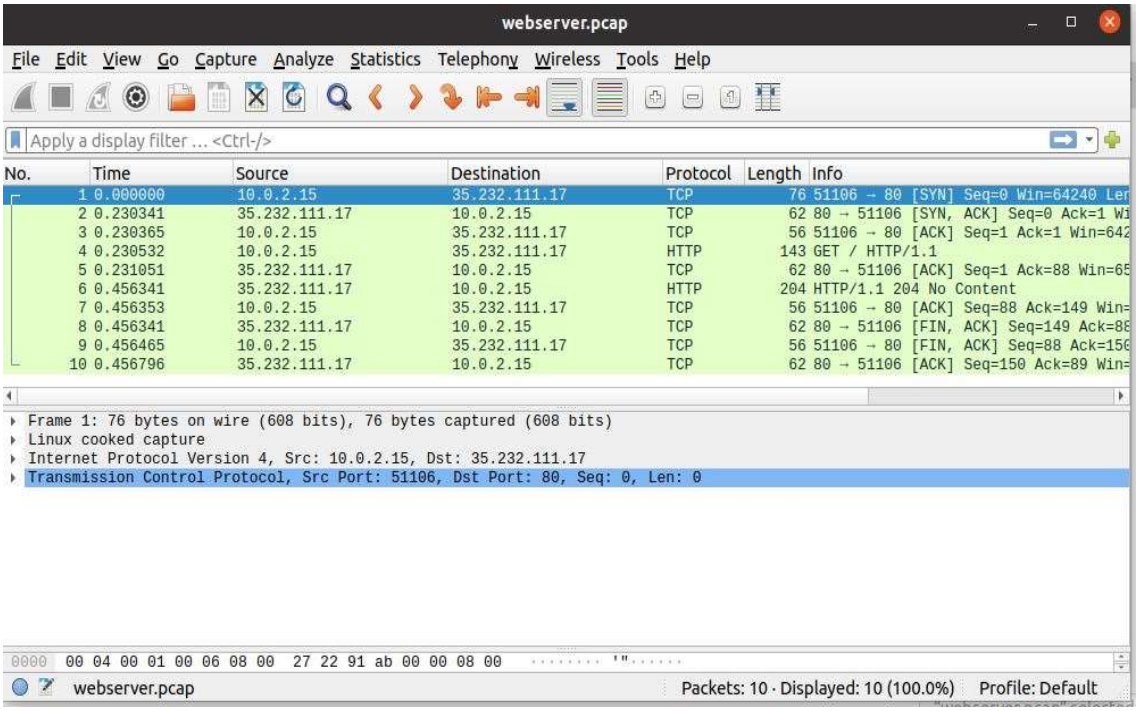
```
abhishek@abhishek-VirtualBox:~$ sudo tcpdump -i any -c10 -nn -A port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
20:38:20.704368 IP 10.0.2.15.48520 > 35.224.170.84.80: Flags [S], seq 588900009, win 64240, options [mss 1460,sackOK,TS val 1658635371 ecr 0,n
op,wscale 7], length 0
E..<R.@.@...
...#..T...P#...........q.........
p..k........
20:38:20.937641 IP 35.224.170.84.80 > 10.0.2.15.48520: Flags [S.], seq 456512001, ack 588900010, win 65535, options [mss 1460], length 0
E..,....@...#..T
....P...5..#...`...     .........
20:38:20.937711 IP 10.0.2.15.48520 > 35.224.170.84.80: Flags [.], ack 1, win 64240, length 0
E..(R.@.@...
...#..T...P#....5..P....]..
20:38:20.938371 IP 10.0.2.15.48520 > 35.224.170.84.80: Flags [P.], seq 1:88, ack 1, win 64240, length 87: HTTP: GET / HTTP/1.1
E...R.@.@..N
...#..T...P#....5..P.......GET / HTTP/1.1
Host: connectivity-check.ubuntu.com
Accept: */*
Connection: close


20:38:20.939431 IP 35.224.170.84.80 > 10.0.2.15.48520: Flags [.], ack 88, win 65535, length 0
E..(....@...#..T
....P...5..#...P... f........
20:38:21.165814 IP 35.224.170.84.80 > 10.0.2.15.48520: Flags [P.], seq 1:149, ack 88, win 65535, length 148: HTTP: HTTP/1.1 204 No Content
E.......@...#..T
....P...5..#...P.......HTTP/1.1 204 No Content
Date: Sun, 24 Jan 2021 15:08:21 GMT
Server: Apache/2.4.18 (Ubuntu)
X-NetworkManager-Status: online
Connection: close
```

```
20:38:21.165831 IP 10.0.2.15.48520 > 35.224.170.84.80: Flags [.], ack 149, win 64092, length 0
E..(R.@.@...
...#..T...P#....5..P..\.]..
20:38:21.165814 IP 35.224.170.84.80 > 10.0.2.15.48520: Flags [F.], seq 149, ack 88, win 65535, length 0
E..(....@...#..T
....P...5..#...P.............
20:38:21.166030 IP 10.0.2.15.48520 > 35.224.170.84.80: Flags [F.], seq 88, ack 150, win 64091, length 0
E..(R.@.@...
...#..T...P#....5..P..[.]..
20:38:21.166283 IP 35.224.170.84.80 > 10.0.2.15.48520: Flags [.], ack 89, win 65535, length 0
E..(....@...#..T
....P...5..#...P.............
10 packets captured
10 packets received by filter
0 packets dropped by kernel
abhishek@abhishek-VirtualBox:~$
```

4.6 : Saving Packets to a File

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

```
abhishek@abhishek-VirtualBox:~$ sudo tcpdump -i any -c10 -nn -w webserver.pcap port 80
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
10 packets captured
10 packets received by filter
0 packets dropped by kernel
abhishek@abhishek-VirtualBox:~$
```



webserver.pcap

Task 5 : Perform Traceroute checks

5.1: Running traceroute

sudo traceroute www.google.com

```
abhishek@abhishek-VirtualBox:~$ sudo traceroute www.google.com
traceroute to www.google.com (142.250.71.36), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.247 ms  0.235 ms  0.229 ms
 2  * * *
 3  * * *
```

```
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
abhishek@abhishek-VirtualBox:~$
```

5.2 : Disabling mapping of IP addresses with hostnames

sudo traceroute -n www.google.com

```
abhishek@abhishek-VirtualBox:~$ sudo traceroute -n www.google.com
traceroute to www.google.com (142.250.71.36), 30 hops max, 60 byte packets
 1  10.0.2.2  0.281 ms  0.251 ms  0.239 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
```

5.3 : traceroute with ICMP protocol

sudo traceroute -I www.google.com

```
abhishek@abhishek-VirtualBox:~$ sudo traceroute -I www.google.com
traceroute to www.google.com (142.250.71.36), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.209 ms  0.188 ms  0.182 ms
 2  192.168.0.1 (192.168.0.1)  2.707 ms  3.397 ms  4.390 ms
 3  10.240.0.1 (10.240.0.1)  6.484 ms  16.076 ms  16.234 ms
 4  14.142.183.201.static-Bangalore.vsnl.net.in (14.142.183.201)  16.229 ms  20.522 ms  22.483 ms
 5  172.31.167.54 (172.31.167.54)  61.322 ms  63.800 ms  69.467 ms
 6  14.140.100.6.static-vsnl.net.in (14.140.100.6)  16.149 ms  11.329 ms  12.354 ms
 7  115.112.71.65.STDILL-Chennai.vsnl.net.in (115.112.71.65)  111.477 ms  87.017 ms  98.801 ms
 8  121.240.1.50 (121.240.1.50)  17.951 ms  18.111 ms  18.451 ms
 9  108.170.253.113 (108.170.253.113)  17.320 ms  17.532 ms  17.313 ms
10  142.250.233.143 (142.250.233.143)  11.479 ms  10.611 ms  12.218 ms
11  maa03s35-in-f4.1e100.net (142.250.71.36)  20.484 ms  17.141 ms  14.704 ms
abhishek@abhishek-VirtualBox:~$
```

5.4 : Testing TCP connection with traceroute

sudo traceroute -T www.google.com

```
abhishek@abhishek-VirtualBox:~$ sudo traceroute -T www.google.com
traceroute to www.google.com (142.250.71.36), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.198 ms  0.166 ms  0.133 ms
 2  maa03s35-in-f4.1e100.net (142.250.71.36)  27.379 ms  27.323 ms  15.753 ms
abhishek@abhishek-VirtualBox:~$
```

Task 6 : Exploring a Network with nmap

6.1 : Scanning Host with Hostname

nmap www.pes.edu

```
abhishek@abhishek-VirtualBox:~$ nmap www.pes.edu
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-24 21:16 IST
Nmap scan report for www.pes.edu (13.71.123.138)
Host is up (0.018s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https

Nmap done: 1 IP address (1 host up) scanned in 5.37 seconds
abhishek@abhishek-VirtualBox:~$
```

6.2 : Scanning Host with IP Address

nmap 163.53.78.128

```
abhishek@abhishek-VirtualBox:~$ nmap 163.53.78.128
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-24 21:17 IST
Nmap scan report for 163.53.78.128
Host is up (0.020s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 4.20 seconds
```

6.3 : Scanning Multiple IP Address or Subnet(IPv4)

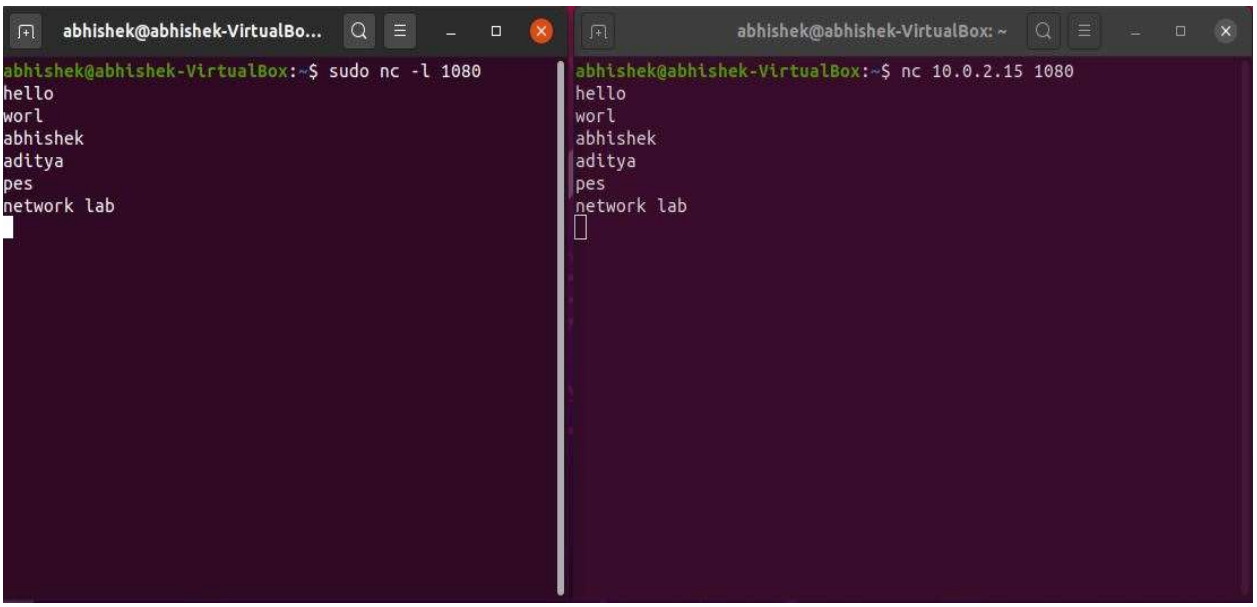
nmap 192.168.1.1 192.168.1.2 192.168.1.3

```
abhishek@abhishek-VirtualBox:~$ nmap 192.168.1.1 192.168.1.2 192.168.1.3
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-24 21:18 IST
Nmap done: 3 IP addresses (0 hosts up) scanned in 3.04 seconds
abhishek@abhishek-VirtualBox:~$
```

Task 7 : NETCAT

A) Netcat as Chat tool

a) Intra system communication using two terminals on the same system.



Server in listening mode

sudo nc -l 1080

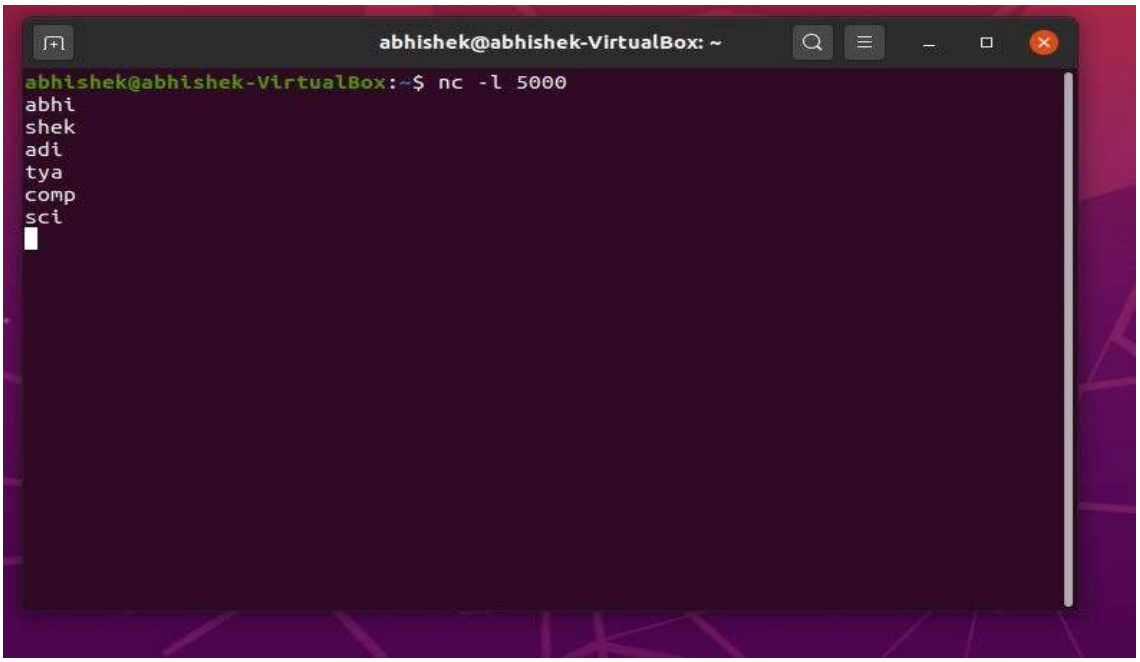
Client

sudo 10.0.2.15 1080

b) Inter system communication

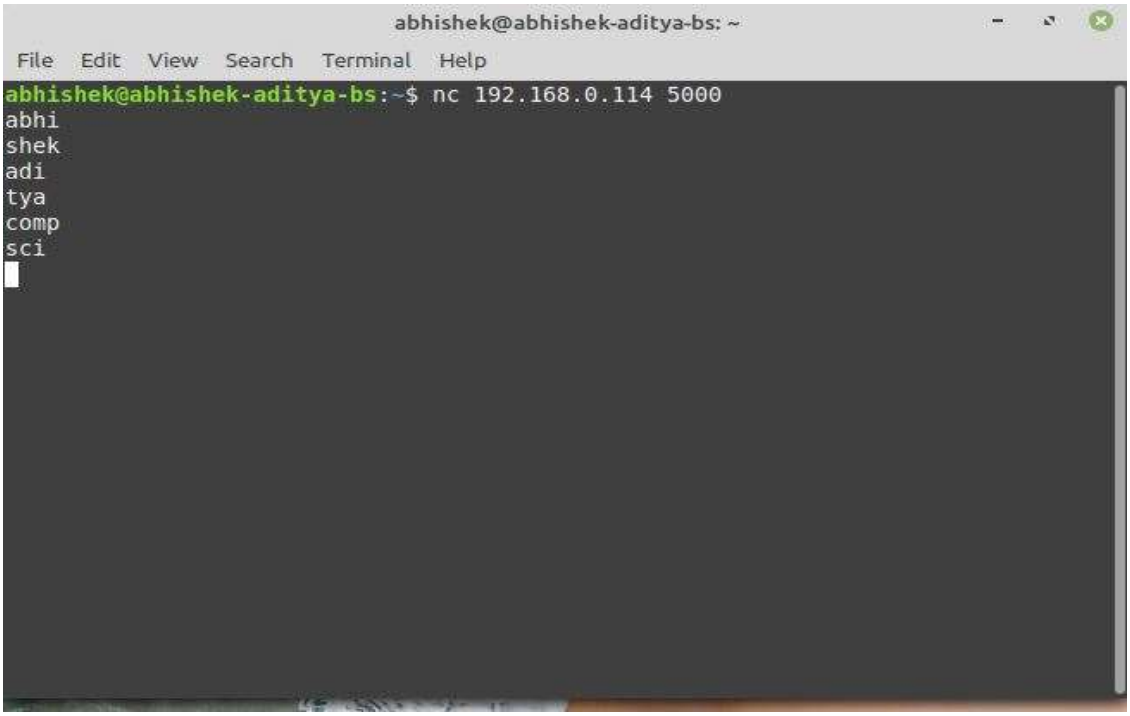
Server (Machine 1)

nc -l 5000



Client (Machine 2)

nc 192.168.0.114 5000



B) Using Netcat to Transfer Files

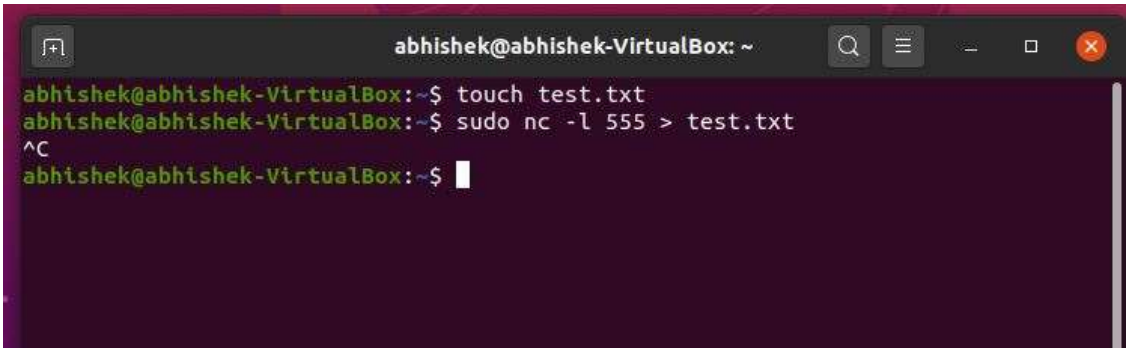
Server (Machine 1)

At the server side, create an empty file named ‘test.txt’

touch test.txt

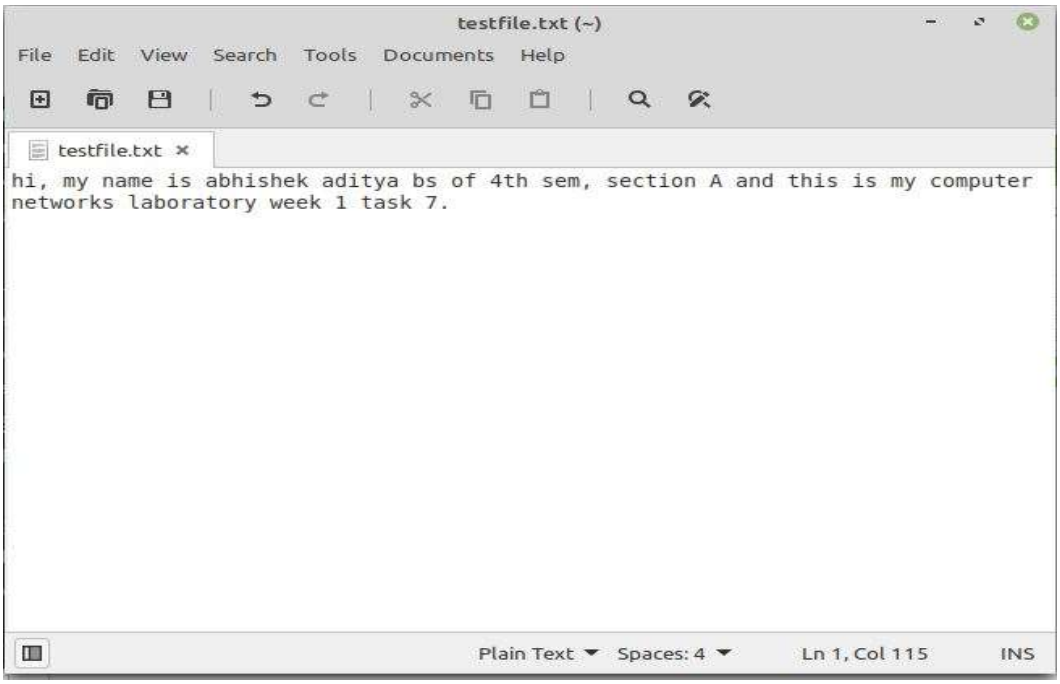
To make the Server go into listening mode

sudo nc -l 555 > test.txt



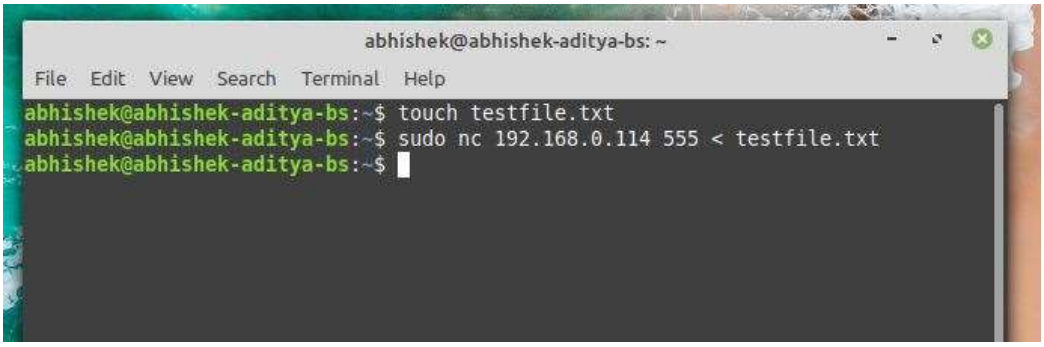
Client (Machine 2)

At the client side, we have a file ‘testfile.txt’. Add some contents to it. touch testfile.txt

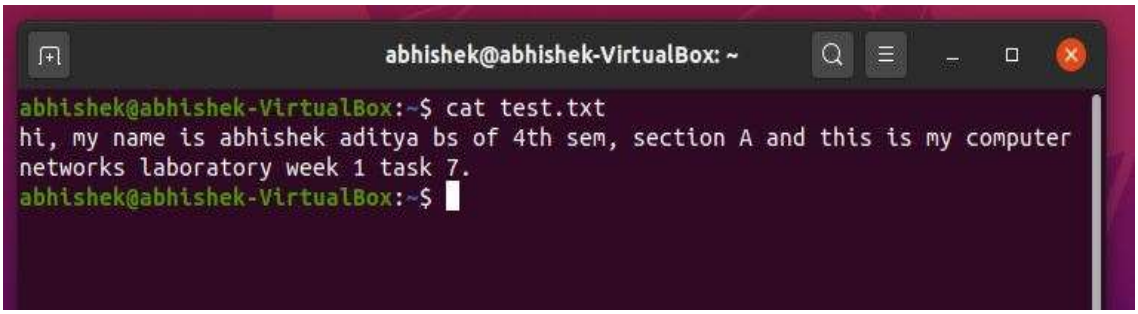


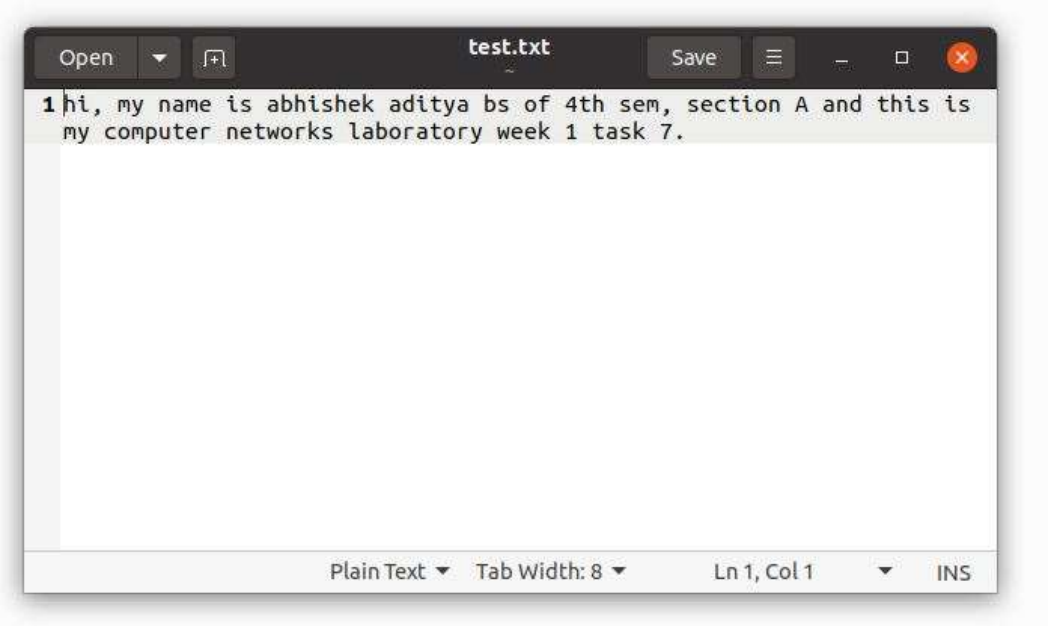
Running the client as :

sudo nc 192.168.0.114 555 < testfile.txt



At server side, verify the file transfer using the command cat test.txt

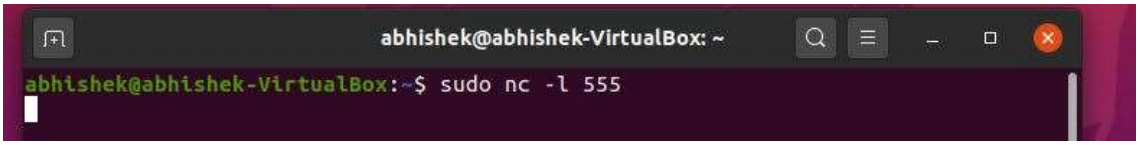




C) Other Commands

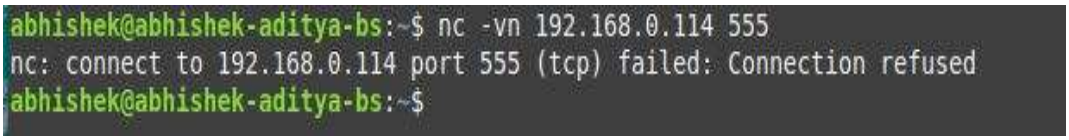
1) To test if a particular TCP port of a remote host is open.

When Server (Host) is in listening mode on port 555



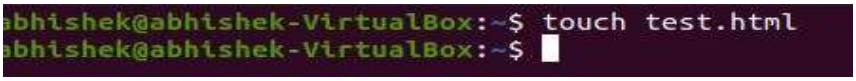
On Client Terminal type nc -vn 192.168.0.114 555 to test if TCP port (555) of remote host is open.

When Server is not in listening mode port 555 is closed, therefore connection is refused.

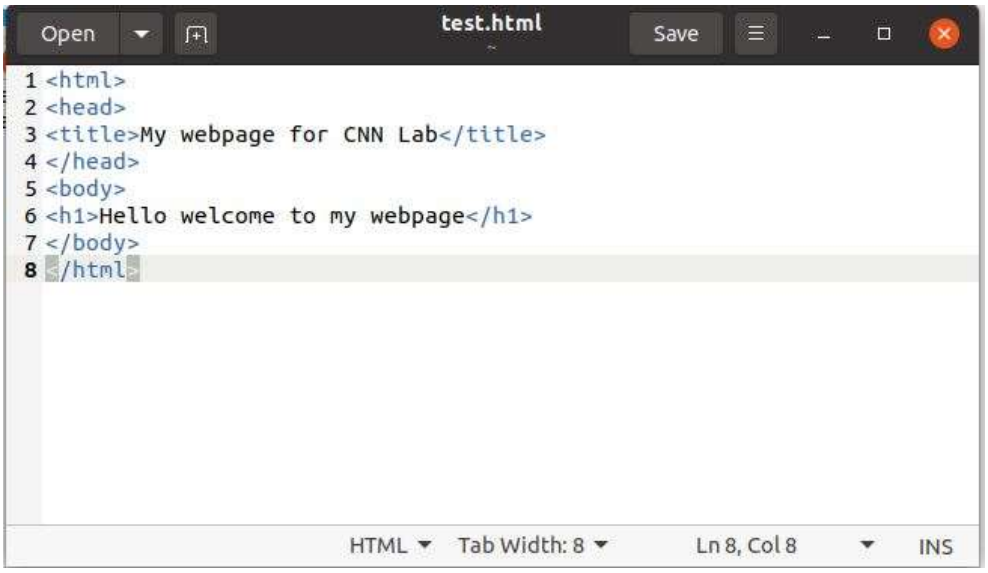


2) Run a web server with a static page.

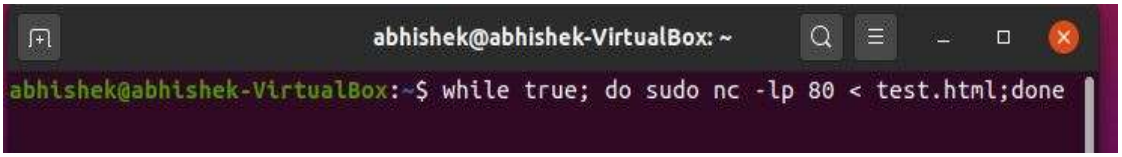
Create a html file in Server (Host 1) using touch test.html



Add some HTML content in test.html



Run the command while true; do sudo nc -lp 80 < test.html; done on local host (host 1) to start a web server that serves test.html on port 80.



open http://192.168.0.114/test.html from another host (host 2) to access it.

On the Terminal in the Server (Host 1)

```
abhishek@abhishek-VirtualBox: ~
abhishek@abhishek-VirtualBox:~$ while true; do sudo nc -lp 80 < test.html;done
GET /test.html HTTP/1.1
Host: 192.168.0.114
Connection: keep-alive
DNT: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gec
ko) Chrome/88.0.4324.96 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
```

Questions on above observations:

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

Answer – The browser used is running HTTP v1.1, and this can be seen in the request header which contains the method (GET) followed by the HTTP version. Similarly, the HTTP version of the web server is also v1.1 and can be seen in the header of the HTTP response sent back to the browser.

```
▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    Host: www.flipkart.com\r\n
    Connection: keep-alive\r\n
```

Request

```
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 301 Moved Permanently\r\n
    Server: nginx\r\n
    Date: Fri, 22 Jan 2021 20:10:15 GMT\r\n
    Content-Type: text/html\r\n
  ▸ Content-Length: 178\r\n
    Location: https://www.flipkart.com/\r\n
```

Response

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

Answer – We can find the last modified time of the HTML file at server by observing the **Last-Modified** field of the HTTP response object. The Last-Modified field contains a timestamp indicating when the file was modified last.

```
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Mon, 25 Jan 2021 18:15:03 GMT\r\n
    Server: Apache/2.4.41 (Ubuntu)\r\n
    Last-Modified: Mon, 25 Jan 2021 18:14:12 GMT\r\n
    ETag: "2aa6-5b9bd81490783-gzip"\r\n
    Accept-Ranges: bytes\r\n
```

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

Answer – Ping keeps sending ICMP packages until it receives an interrupt signal. To specify the number of ECHO_REQUEST packets after which ping should exit, we use the -c option followed by the number of packets.

ping -c 10 www.pes.edu

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

Answer – Method 1 : Using HTTP Response Object

We can obtain the remote host apps and OS of the server by observing the server files of the HTTP Response object using Wireshark. The server field stores the remote host apps or server on which it is hosted as well as the OS.

```
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Mon, 25 Jan 2021 18:15:03 GMT\r\n
    Server: Apache/2.4.41 (Ubuntu)\r\n
    Last-Modified: Mon, 25 Jan 2021 18:14:12 GMT\r\n
    ETag: "2aa6-5b9bd81490783-gzip"\r\n
    Accept-Ranges: bytes\r\n
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n
  ▸ Content-Length: 3138\r\n
```

Method 2 : Using nmap

We can scan the network using **nmap** to find information about the remote host apps and the OS.

Command Used : sudo nmap -O -v www.flipkart.com

```
abhishek@abhishek-VirtualBox: ~
Nmap scan report for www.flipkart.com (163.53.78.110)
Host is up (0.0087s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
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|switch|game console|VoIP adapter|bridge
Running (JUST GUESSING): Linux 1.0.X (88%), Cisco embedded (88%), Ouya embedded
 (86%), Oracle Virtualbox (85%)
OS CPE: cpe:/o:linux:linux_kernel:1.0.9 cpe:/h:cisco:catalyst_1900 cpe:/h:cisco
:ata_188_voip_gateway cpe:/o:oracle:virtualbox
Aggressive OS guesses: Linux 1.0.9 (88%), Cisco Catalyst 1900 switch (88%), OUY
A game console (86%), Cisco ATA 188 VoIP adapter (85%), Oracle Virtualbox (85%)
No exact OS matches for host (test conditions non-ideal).

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 29.92 seconds
           Raw packets sent: 3115 (140.972KB) | Rcvd: 36 (1.956KB)
abhishek@abhishek-VirtualBox:~$
```