COMPUTER NETWORK LAB WEEK-1
PES1UG20CS821
NIKHIL TM

1. Linux Interface Configuration

1.1 ifconfig

```
student@PESSAT-191:~$ ifconfig
enp2s0    Link encap:Ethernet  HWaddr b8:ae:ed:35:c2:46
          inet addr:10.2.20.203  Bcast:10.2.20.255  Mask:255.255.255.0
          inet6 addr: fe80::5139:b04:ef10:2bb5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10666 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8372 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13921608 (13.9 MB)  TX bytes:707433 (707.4 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:3271 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3271 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:237221 (237.2 KB)  TX bytes:237221 (237.2 KB)

student@PESSAT-191:~$
```

IP Address Table:

Interface name	IP address (IPv4 / IPv6)	MAC address
Enp2s0	10.2.20.203	B8:ae:ed:35:c2:46
Lo	127.0.0.1	00.00.00.00.00.00

1.2 Assigning IP Address

sudo ifconfig enp2s0 10.0.8.21 netmask 255.255.255.0

```
student@PESSAT-191:~$ sudo ifconfig enp2s0 10.0.8.21 netmask 255.255.255.0
student@PESSAT-191:~$
```

1.3 Interface Off

sudo ifconfig enp2s0 down

```
student@PESSAT-191:~$ sudo ifconfig enp2s0 down
student@PESSAT-191:~$ ifconfig
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:4651 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4651 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:353697 (353.6 KB)  TX bytes:353697 (353.6 KB)

student@PESSAT-191:~$
```

1.4 Interface On

sudo ifconfig enp2s0 up

```
student@PESSAT-191:~$ sudo ifconfig enp2s0 up
student@PESSAT-191:~$ ifconfig
enp2s0    Link encap:Ethernet  HWaddr b8:ae:ed:35:c2:46
          inet addr:10.2.20.203  Bcast:10.2.20.255  Mask:255.255.255.0
          inet6 addr: fe80::5139:b04:ef10:2bb5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:18089 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14818 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21287111 (21.2 MB)  TX bytes:2140232 (2.1 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:4889 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4889 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:373416 (373.4 KB)  TX bytes:373416 (373.4 KB)

student@PESSAT-191:~$
```

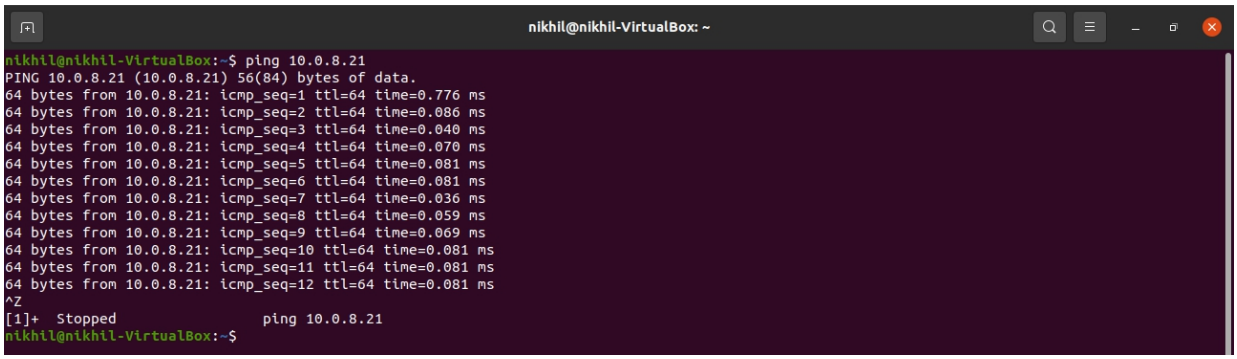
1.5 Neighbor Port

ip neigh

```
student@PESSAT-191:~$ ip neigh
10.2.20.1 dev enp2s0 lladdr 14:58:d0:d4:86:00 REACHABLE
student@PESSAT-191:~$
```

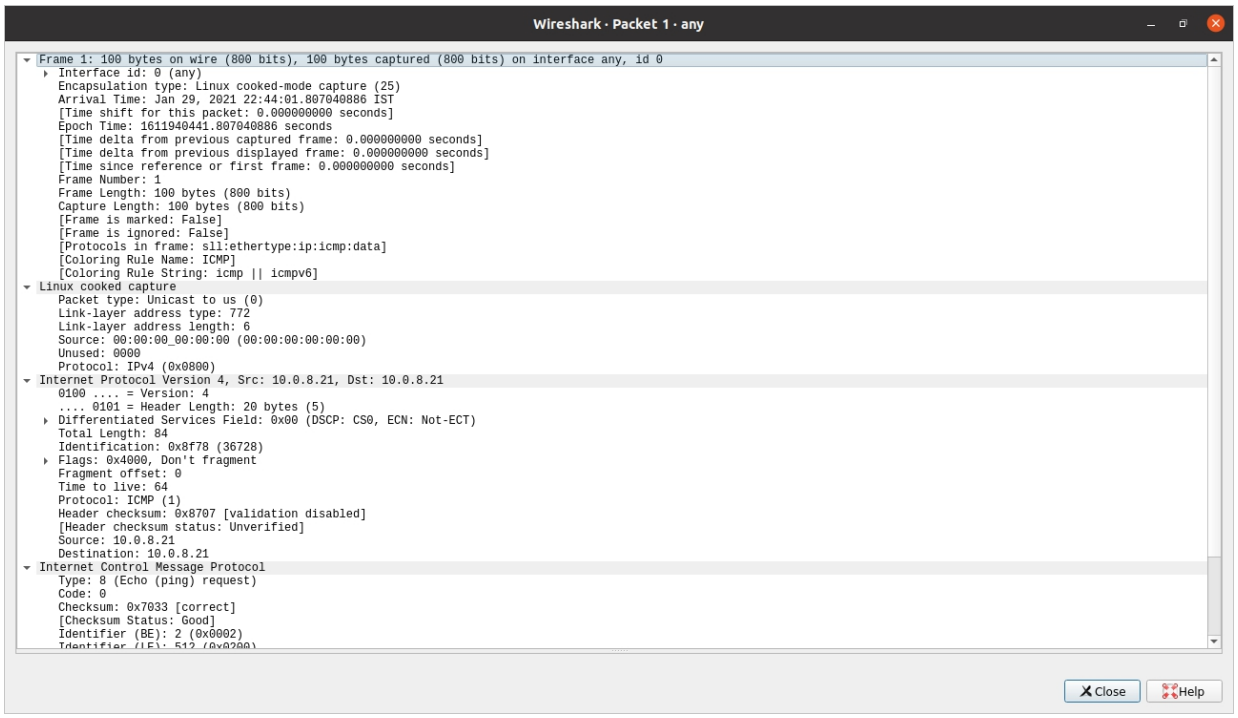
2.PDU (Packet Data Units or Packets) Capture

Ping 10.0.8.21

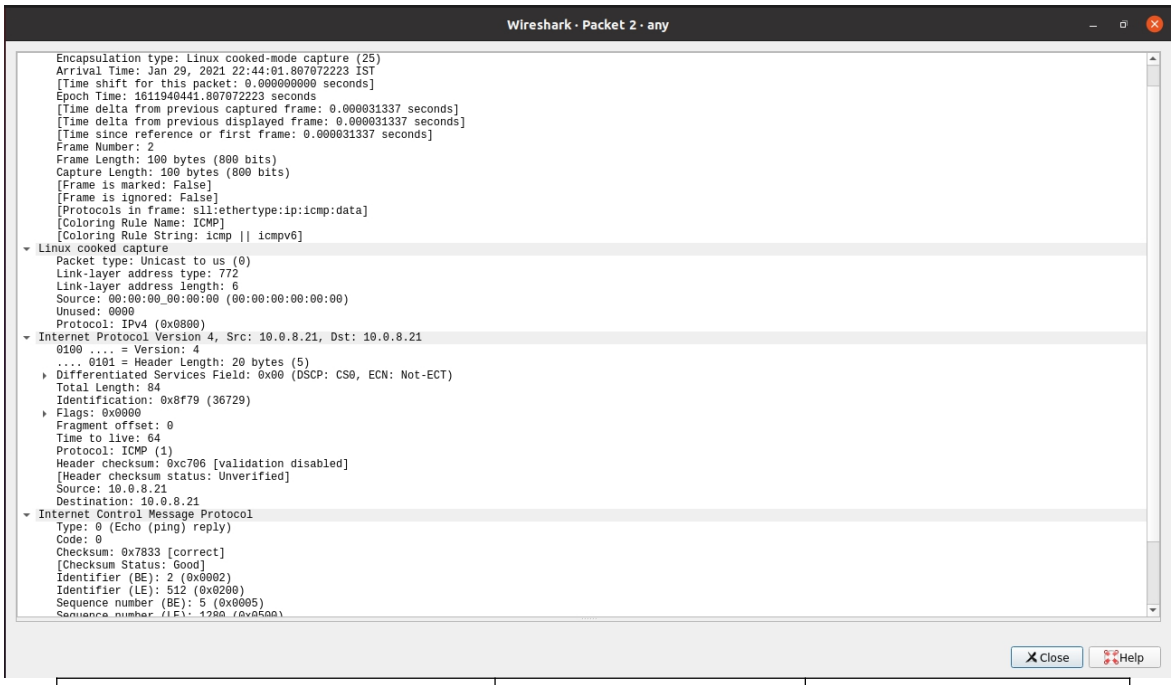


TTL	64
Protocol used by ping	ICMP
Time	Order of 10^{-2} ms

Request



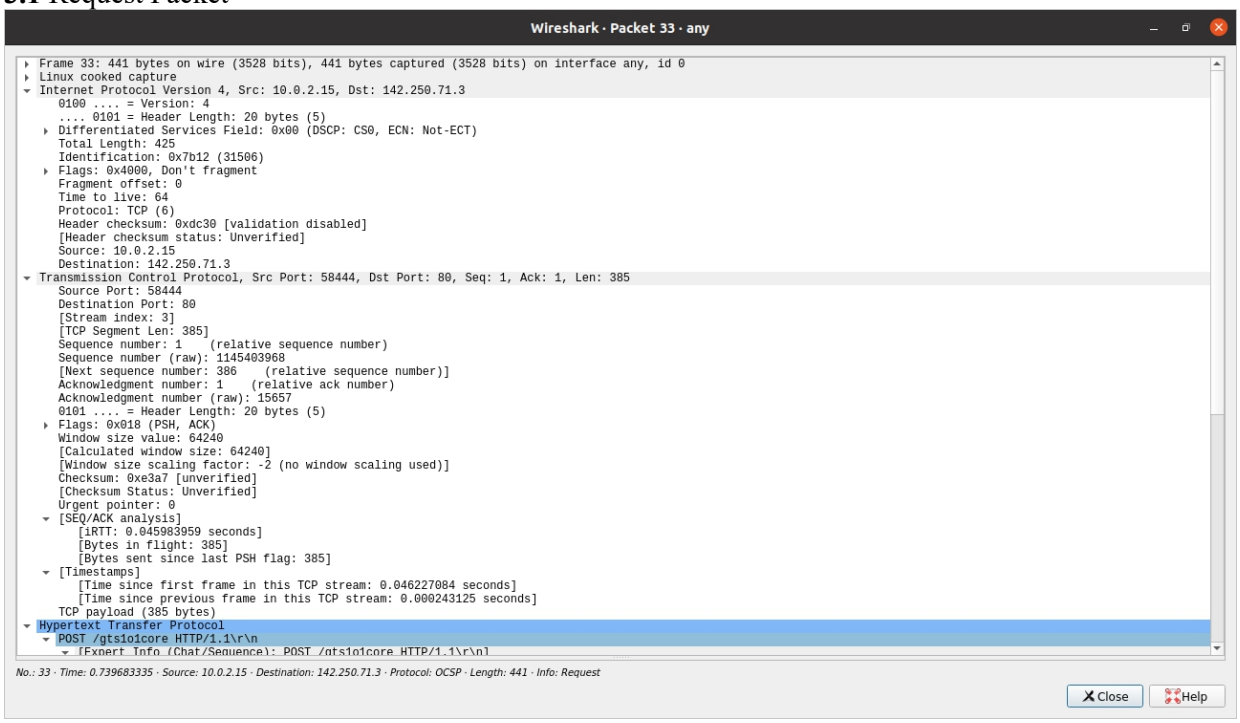
Response



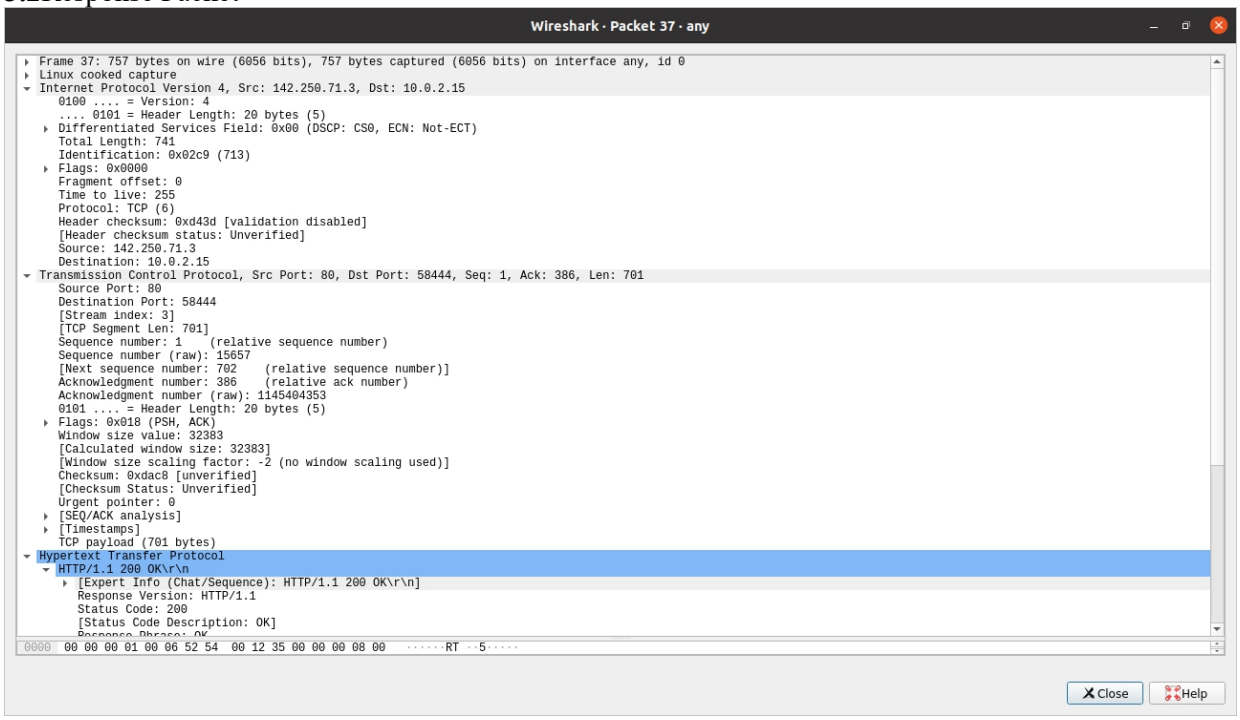
Details	First Echo Request	First Echo Reply
Frame Number	1	2
Source IP address	10.0.8.21	10.0.8.21
Destination IP address	10.0.8.21	10.0.8.21
ICMP Type Value	8	0
ICMP Code Value	0	0
Source Ethernet Address	00.00.00.00.00.00	00.00.00.00.00.00
Destination Ethernet Address	00.00.00.00.00.00	00.00.00.00.00.00
Internet Protocol Version	IPv4	IPv4
Time To Live (TTL) Value	64	64

3.HTTP PDU Capture

3.1 Request Packet



3.2 Response Packet



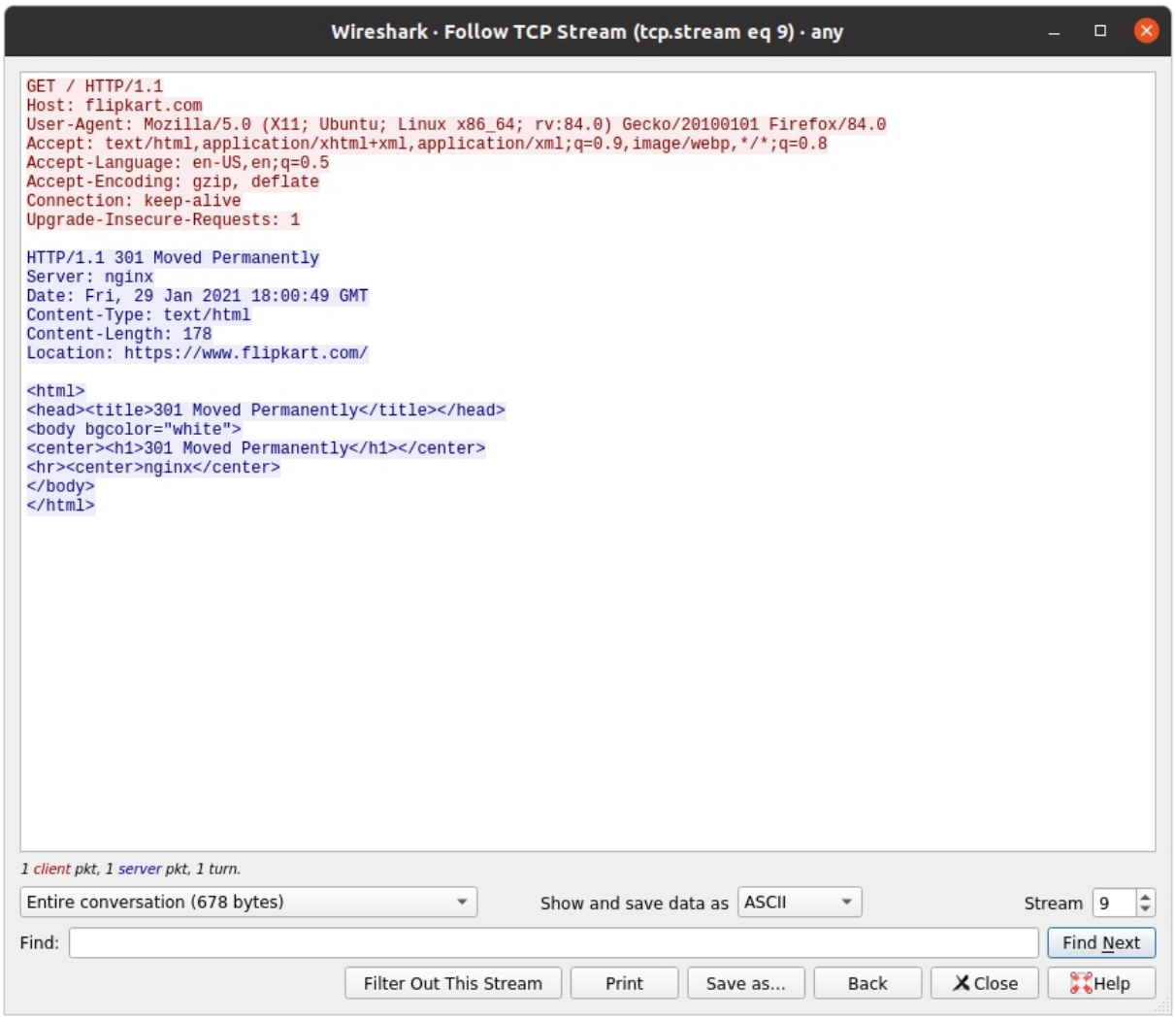
3.3 First and Second Frame Analysis

Details	First Echo Request	First Echo Reply
Frame Number	33	37
Source IP address	10.0.2.15	142.250.71.3
Destination IP address	142.250.71.3	10.0.2.15
ICMP Type Value	8	0
ICMP Code Value	0	0
Source Ethernet Address	B8:ae:ed:35:c2:46	08:00:27:b2:96:5f
Destination Ethernet Address	08:00:27:b2:96:5f	B8:ae:ed:35:c2:46
Internet Protocol Version	IPv4	IPv4
Time To Live (TTL) Value	64	255

3.4 HTTP request and response

HTTP Request		HTTP Response	
Get	GET /HTTP/1.1\r\n	Server	ocsp_responder\r\n
Host	www.flipkart.com\r\n	Content-Type	application/ocsp-response\r\n
User-Agent	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0\r\n	Date	29 Jan 2021 18:00:44 GMT\r\n
Accept-Language	en-US,en;q=0.5\r\n	Location	
Accept-Encoding	gzip, deflate\r\n	Content-Length	471\r\n
Connection	keep-alive\r\n	Connection	keep-alive\r\n

3.5 TCP Stream



4.Capturing packets with tcpdump

4.1 Available Interfaces
sudo tcpdump –
D

```
student@PESSAT-191:~$ sudo tcpdump -D
1.enp2s0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.nflog (Linux netfilter log (NFLOG) interface)
5.nfqueue (Linux netfilter queue (NFQUEUE) interface)
6.usbmon1 (USB bus number 1)
7.usbmon2 (USB bus number 2)
8.usbmon3 (USB bus number 3)
9.usbmon4 (USB bus number 4)
student@PESSAT-191:~$
```

4.2 Packets Capturing
sudo tcpdump -i any

```
student@PESSAT-191:~$ 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), capture size 262144 bytes
11:42:59.542987 ARP, Request who-has 192.168.3.5 tell 10.0.8.30, length 46
11:42:59.543016 ARP, Request who-has 202.148.200.3 tell 10.0.8.30, length 46
11:42:59.543020 ARP, Request who-has 202.148.202.4 tell 10.0.8.30, length 46
11:42:59.543023 ARP, Request who-has 4.2.2.2 tell 10.0.8.30, length 46
11:42:59.544157 IP localhost.59890 > PESSAT-191.domain: 17103+ PTR? 5.3.168.192.in-addr.arpa. (42)
11:42:59.544316 ARP, Request who-has 192.168.3.5 tell 10.0.8.21, length 28
11:43:49.591953 IP 10.2.20.34.netbios-dgm > 10.2.20.255.netbios-dgm: UDP, length 193
11:43:49.592114 IP localhost.43597 > PESSAT-191.domain: 50581+ PTR? 21.8.0.10.in-addr.arpa. (40)
11:43:59.600040 IP localhost.59652 > PESSAT-191.domain: 37939+ PTR? 255.20.2.10.in-addr.arpa. (42)
11:43:59.600203 ARP, Request who-has 192.168.3.5 tell 10.0.8.21, length 28
11:43:59.600225 ARP, Request who-has 202.148.200.3 tell 10.0.8.21, length 28
11:44:19.671938 IP localhost.55069 > PESSAT-191.domain: 15692+ A? incoming.telemetry.mozilla.org. (48)
11:44:19.671959 IP localhost.55069 > PESSAT-191.domain: 55069+ AAAA? incoming.telemetry.mozilla.org. (48)
11:44:19.672048 ARP, Request who-has 192.168.3.5 tell 10.0.8.21, length 28
11:44:19.672076 ARP, Request who-has 202.148.200.3 tell 10.0.8.21, length 28
11:44:19.672087 ARP, Request who-has 202.148.202.4 tell 10.0.8.21, length 28
11:44:19.672098 ARP, Request who-has 4.2.2.2 tell 10.0.8.21, length 28
11:44:20.454251 IP6 fe80::d491:17d:7f51:833a.mdns > ff02::fb.mdns: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
11:44:20.454573 IP localhost.53334 > PESSAT-191.domain: 39586+ PTR? b.f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa. (9
0)
11:44:20.675864 ARP, Request who-has 4.2.2.2 tell 10.0.8.21, length 28
11:44:20.675883 ARP, Request who-has 202.148.202.4 tell 10.0.8.21, length 28
11:44:20.675891 ARP, Request who-has 202.148.200.3 tell 10.0.8.21, length 28
11:44:20.675900 ARP, Request who-has 192.168.3.5 tell 10.0.8.21, length 28
11:44:47.652725 IP 10.2.20.198.netbios-dgm > 10.2.20.255.netbios-dgm: UDP, length 234
11:44:47.652969 IP localhost.52192 > PESSAT-191.domain: 42048+ PTR? 198.20.2.10.in-addr.arpa. (42)
11:44:47.652999 IP 10.2.20.39.netbios-ns > 10.2.20.255.netbios-ns: UDP, length 50
11:44:47.653132 ARP, Request who-has 192.168.3.5 tell 10.0.8.21, length 28
11:44:47.653150 ARP, Request who-has 202.148.200.3 tell 10.0.8.21, length 28
11:44:47.653160 ARP, Request who-has 202.148.202.4 tell 10.0.8.21, length 28
11:44:57.663486 IP localhost.52761 > PESSAT-191.domain: 58029+ PTR? 39.20.2.10.in-addr.arpa. (41)
11:44:57.663625 ARP, Request who-has 192.168.3.5 tell 10.0.8.21, length 28
11:45:08.440285 ARP, Reply 192.168.14.30 is-at 4c:11:bf:9c:69:d5 (oui Unknown), length 46
11:45:08.440570 IP localhost.41635 > PESSAT-191.domain: 27471+ PTR? 30.14.168.192.in-addr.arpa. (44)
11:45:08.440739 ARP, Request who-has 192.168.3.5 tell 10.0.8.21, length 28
11:45:08.440759 ARP, Request who-has 202.148.200.3 tell 10.0.8.21, length 28
11:45:08.440769 ARP, Request who-has 202.148.202.4 tell 10.0.8.21, length 28
11:45:08.440779 ARP, Request who-has 4.2.2.2 tell 10.0.8.21, length 28
^Z
[4]+  Stopped                 sudo tcpdump -i any
```

4.3 Filtering Packets
sudo tcpdump -i any -c5 icmp

```
student@PESSAT-191:~$ 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), capture size 262144 bytes
11:46:17.731806 IP 10.0.8.21 > 10.0.8.21: ICMP host 4.2.2.2 unreachable, length 69
11:46:17.731815 IP 10.0.8.21 > 10.0.8.21: ICMP host 4.2.2.2 unreachable, length 69
11:46:17.731819 IP 10.0.8.21 > 10.0.8.21: ICMP host 4.2.2.2 unreachable, length 70
11:46:17.731823 IP 10.0.8.21 > 10.0.8.21: ICMP host 4.2.2.2 unreachable, length 70
11:46:17.731828 IP 10.0.8.21 > 10.0.8.21: ICMP host 4.2.2.2 unreachable, length 71
5 packets captured
328 packets received by filter
314 packets dropped by kernel
student@PESSAT-191:~$
```

4.4 Packet Content

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

```
student@PESSAT-191:~$ 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), capture size 262144 bytes
12:00:18.731365 IP 10.2.20.203.41370 > 34.107.221.82.80: Flags [S], seq 1587657851, win 64240, options [mss 1460,sackOK,TS val 2403887374 ecr 0,
nop,wscale 7], length 0
E..<..@.@.v[
..."k.R...P^..{........y&.........
.Hi.........
12:00:18.731545 IP 34.107.221.82.80 > 10.2.20.203.41370: Flags [S.], seq 122566985, ack 1587657852, win 29200, options [mss 1412,nop,nop,sackOK]
, length 0
E..0..@.>..>"k.R
....P...N9I^..|p.r.............
12:00:18.731594 IP 10.2.20.203.41370 > 34.107.221.82.80: Flags [.], ack 1, win 64240, length 0
E..(..@.@.vn
..."k.R...P^..|.N9JP.......
12:00:18.731960 IP 10.2.20.203.41370 > 34.107.221.82.80: Flags [P.], seq 1:297, ack 1, win 64240, length 296: HTTP: GET /success.txt HTTP/1.1
E..P..@.@.uE
..."k.R...P^..|.N9JP...y...GET /success.txt HTTP/1.1
Host: detectportal.firefox.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
Cache-Control: no-cache
Pragma: no-cache
Connection: keep-alive


12:00:18.732113 IP 34.107.221.82.80 > 10.2.20.203.41370: Flags [.], ack 297, win 30016, length 0
E..(.n@.>..."k.R
....P...N9J^...P.u@.A........
12:00:18.732420 IP 34.107.221.82.80 > 10.2.20.203.41370: Flags [P.], seq 1:824, ack 297, win 30016, length 823: HTTP: HTTP/1.1 200 OK
E..._.o@.>..."k.R
....P...N9J^...P.u@....HTTP/1.1 200 OK
Date: Thu, 21 Jan 2021 06:30:18 GMT
Cache-Control: no-cache
Pragma: no-cache
Content-Type: text/html; charset="UTF-8"
Content-Length: 603
Via: HTTP/1.1 forward.http.proxy:3128
Connection: close

<HTML><HEAD>
```

```
12:00:18.732113 IP 34.107.221.82.80 > 10.2.20.203.41370: Flags [.], ack 297, win 30016, length 0
E..(.n@.>..."k.R
....P...N9J^...P.u@.A........
12:00:18.732420 IP 34.107.221.82.80 > 10.2.20.203.41370: Flags [P.], seq 1:824, ack 297, win 30016, length 823: HTTP: HTTP/1.1 200 OK
E..._.o@.>..."k.R
....P...N9J^...P.u@....HTTP/1.1 200 OK
Date: Thu, 21 Jan 2021 06:30:18 GMT
Cache-Control: no-cache
Pragma: no-cache
Content-Type: text/html; charset="UTF-8"
Content-Length: 603
Via: HTTP/1.1 forward.http.proxy:3128
Connection: close

<HTML><HEAD>
<meta http-equiv=pragma content=nocache>
<META HTTP-EQUIV=Expires CONTENT=-1>
<SCRIPT>
var url = new DOMParser().parseFromString('<a>?u=http://detectportal.firefox.com/success.txt</a>', 'text/xml').documentElement.textContent;
        location.href='http://192.168.254.1:8090/httpclient.html' + url;


</SCRIPT>
</HEAD><BODY>
</BODY>
</HTML>

12:00:18.732458 IP 10.2.20.203.41370 > 34.107.221.82.80: Flags [.], ack 824, win 63417, length 0
E..(..@.@.vl
..."k.R...P^....N<.P.......
12:00:18.732476 IP 34.107.221.82.80 > 10.2.20.203.41370: Flags [F.], seq 824, ack 297, win 30016, length 0
E..(.p@.>..."k.R
....P...N<.^...P.u@.    ........
12:00:18.732929 IP 10.2.20.203.41370 > 34.107.221.82.80: Flags [F.], seq 297, ack 825, win 63417, length 0
E..(..@.@.vk
..."k.R...P^....N<.P.......
12:00:18.733031 IP 34.107.221.82.80 > 10.2.20.203.41370: Flags [.], ack 298, win 30016, length 0
E..(.q@.>..."k.R
....P...N<.^...P.u@..........
10 packets captured
10 packets received by filter
0 packets dropped by kernel
student@PESSAT-191:~$
```

4.5 Saving Packet

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

```
student@PESSAT-191:~$ sudo tcpdump -i any -c10 -nn -w webserver.pcap port 80
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
10 packets captured
10 packets received by filter
0 packets dropped by kernel
student@PESSAT-191:~$
```

5. Perform Traceroute checks

5.1 Running Traceroute
sudo traceroute www.google.com

```
student@PESSAT-191:~$ sudo traceroute www.google.com
traceroute to www.google.com (142.250.67.228), 30 hops max, 60 byte packets
 1  10.2.20.1 (10.2.20.1)  1.098 ms  1.091 ms  1.084 ms
 2  192.168.4.1 (192.168.4.1)  0.873 ms  0.866 ms  0.858 ms
 3  192.168.254.1 (192.168.254.1)  0.130 ms  0.143 ms  0.148 ms
 4  1.6.180.188 (1.6.180.188)  79.231 ms 14.143.35.157.static-bangalore.vsnl.net.in (14.143.35.157)  1.529 ms 1.6.180.188 (1.6.180.188)  79.248
ms
 5  * 172.31.167.54 (172.31.167.54)  6.183 ms *
 6  100.66.8.23 (100.66.8.23)  97.084 ms 14.140.100.6.static-vsnl.net.in (14.140.100.6)  5.855 ms 100.67.56.103 (100.67.56.103)  96.267 ms
 7  72.14.210.200 (72.14.210.200)  100.906 ms 115.112.71.65.stdill-chennai.vsnl.net.in (115.112.71.65)  6.153 ms 72.14.210.200 (72.14.210.200)
100.263 ms
 8  108.170.248.193 (108.170.248.193)  97.671 ms 121.240.1.50 (121.240.1.50)  6.120 ms 108.170.248.209 (108.170.248.209)  101.362 ms
^Z
[8]+  Stopped                 sudo traceroute www.google.com
student@PESSAT-191:~$
```

5.2 Disabling the mapping
sudo traceroute -n www.google.com

```
student@PESSAT-191:~$ sudo traceroute -n www.google.com
traceroute to www.google.com (172.217.160.164), 30 hops max, 60 byte packets
 1  10.2.20.1  1.188 ms  1.190 ms  1.181 ms
 2  192.168.4.1  0.810 ms  0.802 ms  0.795 ms
 3  192.168.254.1  0.121 ms  0.133 ms  0.154 ms
 4  1.6.180.188  2.018 ms  2.051 ms 14.143.35.157  1.607 ms
 5  100.66.0.23  8.871 ms  9.029 ms *
 6  100.66.0.23  8.632 ms  8.362 ms 121.240.1.46  6.120 ms
 7  72.14.219.169  8.423 ms  8.592 ms 74.125.242.155  7.248 ms
 8  74.125.242.139  9.683 ms 74.125.242.130  9.982 ms 142.250.212.6  24.469 ms
 9  142.250.212.2  25.650 ms  25.223 ms 108.170.248.161  30.156 ms
10  108.170.248.177  25.869 ms 108.170.248.161  25.582 ms 216.239.62.237  22.972 ms
11  108.170.248.161  26.058 ms 216.239.62.237  22.778 ms 172.217.160.164  24.082 ms
student@PESSAT-191:~$
```

5.3 Using ICMP
sudo traceroute -I www.google.com

```
student@PESSAT-191:~$ sudo traceroute -I www.google.com
traceroute to www.google.com (172.217.160.164), 30 hops max, 60 byte packets
 1  10.2.20.1 (10.2.20.1)  1.235 ms  1.234 ms  1.526 ms
 2  192.168.4.1 (192.168.4.1)  0.885 ms  0.902 ms  0.906 ms
 3  192.168.254.1 (192.168.254.1)  0.146 ms  0.157 ms  0.156 ms
 4  1.6.180.188 (1.6.180.188)  1.959 ms * *
 5  * * 100.66.0.23 (100.66.0.23)  11.352 ms
 6  100.66.0.23 (100.66.0.23)  10.831 ms  10.879 ms  11.039 ms
 7  72.14.219.169 (72.14.219.169)  10.636 ms  10.466 ms  10.585 ms
 8  108.170.253.122 (108.170.253.122)  11.453 ms  10.753 ms  10.866 ms
 9  142.250.212.2 (142.250.212.2)  71.483 ms  70.718 ms  70.700 ms
10  216.239.54.93 (216.239.54.93)  33.323 ms  33.349 ms  33.342 ms
11  108.170.248.177 (108.170.248.177)  34.186 ms  34.267 ms  34.267 ms
12  74.125.251.133 (74.125.251.133)  33.326 ms  33.322 ms  33.418 ms
13  bom05s12-in-f4.1e100.net (172.217.160.164)  28.352 ms  28.374 ms  28.373 ms
student@PESSAT-191:~$
```

5.4 Testing TCP
sudo traceroute -T www.google.com

```
student@PESSAT-191:~$ sudo traceroute -T www.google.com
traceroute to www.google.com (142.250.67.228), 30 hops max, 60 byte packets
 1  10.2.20.1 (10.2.20.1)  1.287 ms  1.288 ms  1.281 ms
 2  192.168.4.1 (192.168.4.1)  0.739 ms  0.734 ms *
 3  192.168.254.1 (192.168.254.1)  0.140 ms  0.143 ms  0.147 ms
 4  14.143.35.157.static-bangalore.vsnl.net.in (14.143.35.157)  1.930 ms 1.6.180.188 (1.6.180.188)  2.164 ms  2.285 ms
 5  172.31.167.54 (172.31.167.54)  6.140 ms * *
 6  14.140.100.6.static-vsnl.net.in (14.140.100.6)  6.228 ms 100.67.56.103 (100.67.56.103)  15.597 ms 100.70.66.174 (100.70.66.174)  15.596 ms
 7  115.112.71.65.stdill-chennai.vsnl.net.in (115.112.71.65)  6.152 ms 72.14.210.200 (72.14.210.200)  16.230 ms  15.930 ms
 8  108.170.248.209 (108.170.248.209)  17.041 ms  17.023 ms 121.240.1.50 (121.240.1.50)  7.940 ms
 9  216.239.58.19 (216.239.58.19)  20.201 ms 142.250.228.47 (142.250.228.47)  20.185 ms 108.170.253.122 (108.170.253.122)  8.117 ms
10  bom07s24-in-f4.1e100.net (142.250.67.228)  15.885 ms  15.788 ms 142.250.212.6 (142.250.212.6)  22.931 ms
student@PESSAT-191:~$
```

6.Explore an entire network for information

6.1 Scanning With Host Name
nmap www.pes.edu

```
student@PESSAT-191:~$ nmap www.pes.edu

Starting Nmap 7.01 ( https://nmap.org ) at 2021-01-21 12:15 IST
Nmap scan report for www.pes.edu (13.71.123.138)
Host is up (0.013s 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 4.83 seconds
student@PESSAT-191:~$
```

6.2 Scanning With IP Address
nmap 163.53.78.128

```
student@PESSAT-191:~$ nmap 163.53.78.128

Starting Nmap 7.01 ( https://nmap.org ) at 2021-01-21 12:15 IST
Nmap scan report for 163.53.78.128
Host is up (0.020s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE
21/tcp   open   ftp
80/tcp   open   http
443/tcp  open   https
6346/tcp closed gnutella

Nmap done: 1 IP address (1 host up) scanned in 5.60 seconds
student@PESSAT-191:~$
```

6.3 Scanning Multiple IP Address
nmap 192.168.1.1 192.168.1.2 192.168.1.3

```
student@PESSAT-191:~$ nmap 192.168.1.1 192.168.1.2 192.168.1.3

Starting Nmap 7.01 ( https://nmap.org ) at 2021-01-21 12:17 IST
Nmap done: 3 IP addresses (0 hosts up) scanned in 1.13 seconds
student@PESSAT-191:~$
```

7. Netcat as Chat tool

7a. Intra System Communication

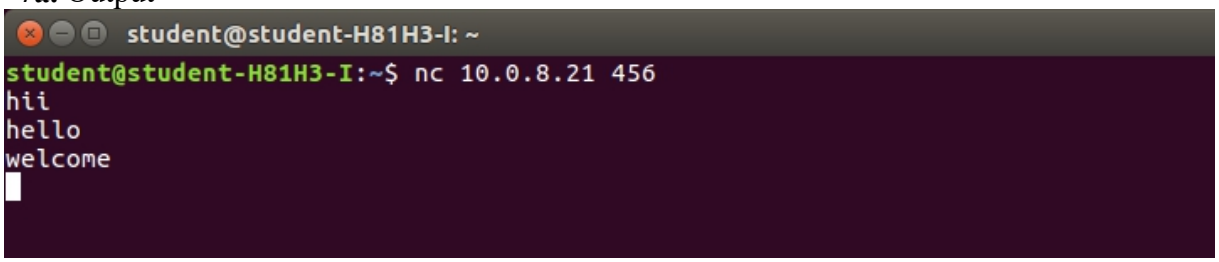
7a.1 listening terminal
nc -l 456

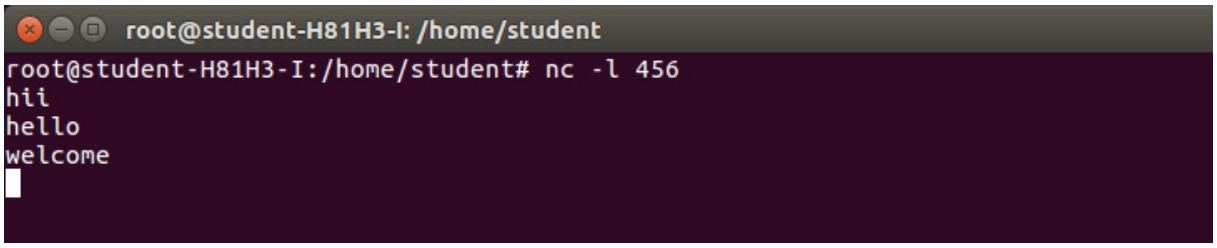
```
root@student-H81H3-I: /home/student
root@student-H81H3-I:/home/student# nc -l 456
```

nc 10.0.8.21 456

```
student@student-H81H3-I: ~
student@student-H81H3-I:~$ nc 10.0.8.21 456
```

7a. Output





7ab.Inter system communication

nc -l 456

nc 10.0.8.15 456

Client Screen

Server Screen

Task 7b.Use Netcat to Transfer Files

sudo nc -l 789 > test.txt

sudo nc 10.0.8.15 789 < testfile.txt

cat test.txt

```
student@CSELAB:~$ sudo nc 10.0.8.15 789 < testfile.txt
student@CSELAB:~$ cat testfile.txt
hello,this is nikhil and meghana

student@CSELAB:~$
```

Task 7c. Other Commands

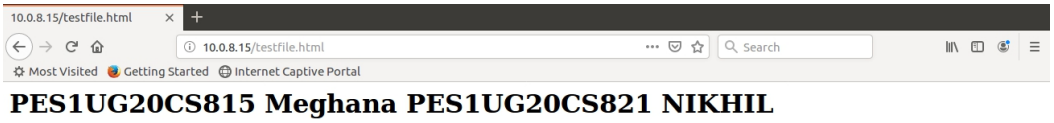
nc -vn 10.0.8.21 80
while true; do sudo nc -lp 80 < testfile.html; done

```
student@CSELAB:/var/www/html$ ls
index.html  info.php
student@CSELAB:/var/www/html$ cat>testfile.html
bash: testfile.html: Permission denied
student@CSELAB:/var/www/html$ sudo su
root@CSELAB:/var/www/html# student
student: command not found
root@CSELAB:/var/www/html# cat>testfile.html
<html>
<h1>
PES1UG20CS815 Meghana
PES1UG20CS821 NIKHIL
</h1>
</html>
^C
root@CSELAB:/var/www/html# cat testfile.html
<html>
<h1>
PES1UG20CS815 Meghana
PES1UG20CS821 NIKHIL
</h1>
</html>
root@CSELAB:/var/www/html# nc -vn 10.0.8.21 80
Connection to 10.0.8.21 80 port [tcp/*] succeeded!
while true; do sudo nc -lp 80 < testfile.html; done
HTTP/1.1 400 Bad Request
Date: Fri, 29 Jan 2021 07:38:00 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 301
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.18 (Ubuntu) Server at 127.0.1.1 Port 80</address>
</body></html>
root@CSELAB:/var/www/html#
```

7.c Output

http://10.0.2.8/test.html

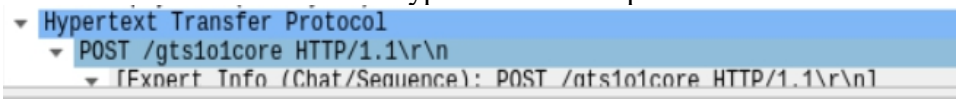


Questions

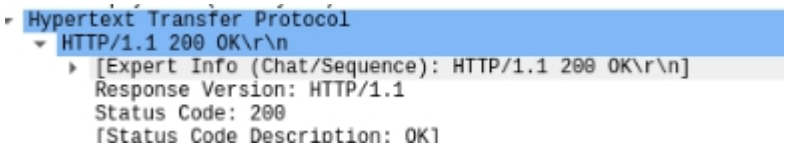
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server?

Answer: The browser is running in HTTP version 1.1.Even the web server is also running in HTTP version 1.1.it can it viewed in the hypertext transfer protocol section.

Request



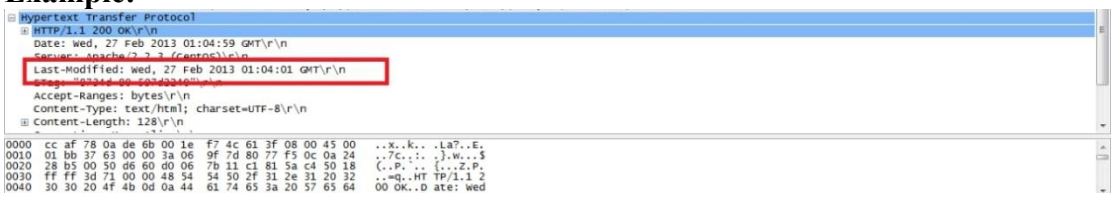
Response



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

Answer: We can find the last modified time in the Hypertext Transfer protocol section Which contains the modified date and time present next to server section.

Example:



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

Answer: This can be done with the use of 'c' in the command followed by the number of packets.

Example ping -c 5 www.pes.edu

It will contentiously sents the packets untill it receives an interrupt signal.

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

Answer: We can identify remote host apps and OS by Fingerprinting and OS detection.

We can use nmap to find open ports & closed ports, services running on specific ports and also OS detection.

Example: Nmap scan to find open ports, services running and OS detection

Nmap -sV -O -p- 10.0.2.15