

LAB 1

Summary

This lab discusses basic and essential networking commands and their use cases in linux. For a lot of these, we require super user permissions, so we use su and change user to '489labuser'. Overall this lab provides a base for all the other labs.

Switch User

```
489labuser@co2061-20
File Edit View Search Terminal Help
bash-4.4$ hostname
co2061-20.ece.iastate.edu
bash-4.4$ su 489labuser
Password:
[489labuser@co2061-20 nzaheer]$
```

```
[489labuser@co2061-20 ~]$ ping -c 4 www.google.com
PING www.google.com (142.250.191.228) 56(84) bytes of data.
64 bytes from ord38s32-in-f4.1e100.net (142.250.191.228): icmp_seq=1 ttl=52 time=18.4 ms
64 bytes from ord38s32-in-f4.1e100.net (142.250.191.228): icmp_seq=2 ttl=52 time=18.4 ms
64 bytes from ord38s32-in-f4.1e100.net (142.250.191.228): icmp_seq=3 ttl=52 time=18.5 ms
64 bytes from ord38s32-in-f4.1e100.net (142.250.191.228): icmp_seq=4 ttl=52 time=18.5 ms

--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 18.424/18.469/18.525/0.171 ms
[489labuser@co2061-20 ~]$ ping -c 4 www.cam.ac.uk
PING www.cam.ac.uk (128.232.132.8) 56(84) bytes of data.
64 bytes from tm-128-232-132-8.tm.uis.cam.ac.uk (128.232.132.8): icmp_seq=1 ttl=38 time=119 ms
64 bytes from tm-128-232-132-8.tm.uis.cam.ac.uk (128.232.132.8): icmp_seq=2 ttl=38 time=119 ms
64 bytes from tm-128-232-132-8.tm.uis.cam.ac.uk (128.232.132.8): icmp_seq=3 ttl=38 time=119 ms
64 bytes from tm-128-232-132-8.tm.uis.cam.ac.uk (128.232.132.8): icmp_seq=4 ttl=38 time=119 ms

--- www.cam.ac.uk ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 118.766/118.889/118.972/0.084 ms
[489labuser@co2061-20 ~]$ ping -c 4 www.iastate.edu
PING www.iastate.edu (20.221.234.34) 56(84) bytes of data.
64 bytes from 20.221.234.34 (20.221.234.34): icmp_seq=1 ttl=108 time=25.6 ms
64 bytes from 20.221.234.34 (20.221.234.34): icmp_seq=2 ttl=108 time=25.8 ms
64 bytes from 20.221.234.34 (20.221.234.34): icmp_seq=3 ttl=108 time=25.6 ms
64 bytes from 20.221.234.34 (20.221.234.34): icmp_seq=4 ttl=108 time=25.5 ms

--- www.iastate.edu ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 25.530/25.639/25.813/0.108 ms
[489labuser@co2061-20 ~]$
```

PING

1) Average time:

Google – 18.5ms

cam.ac – 119ms

iastate - 25.6

2)

```
[489labuser@co2061-20 ~]$ ping -c 4 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.051 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.043 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.067 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.071 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3111ms
rtt min/avg/max/mdev = 0.043/0.058/0.071/0.011 ms
[489labuser@co2061-20 ~]$
```

Average RTT: 0.065 ms

This is much lesser than the rest of it. The reason is pinging the localhost will return ICMP packages almost immediately since it is local to the system as compared to the other hosts which have to be accessed from a server somewhere on the internet.

nslookup

3)

```
[489labuser@co2061-20 ~]$ nslookup -q=a www.iastate.edu
Server:          129.186.1.200
Address:         129.186.1.200#53

Name:   www.iastate.edu
Address: 20.221.234.34

[489labuser@co2061-20 ~]$ nslookup -q=cname www.iastate.edu
Server:          129.186.1.200
Address:         129.186.1.200#53

*** Can't find www.iastate.edu: No answer

[489labuser@co2061-20 ~]$ nslookup -q=a www.microsoft.com
Server:          129.186.1.200
Address:         129.186.1.200#53

Non-authoritative answer:
www.microsoft.com      canonical name = www.microsoft.com-c-3.edgekey.net.
www.microsoft.com-c-3.edgekey.net canonical name = www.microsoft.com-c-3.edgekey.net.glob
alredir.akadns.net.
www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net canonical name = e13678.dscb.ak
amaiedge.net.
Name:   e13678.dscb.akamaiedge.net
Address: 23.203.17.160

[489labuser@co2061-20 ~]$ nslookup -q=a www.wikipedia.com
Server:          129.186.1.200
Address:         129.186.1.200#53

Non-authoritative answer:
www.wikipedia.com      canonical name = ncredir-lb.wikimedia.org.
Name:   ncredir-lb.wikimedia.org
Address: 208.80.154.232

[489labuser@co2061-20 ~]$ █
```

4)

```
[489labuser@co2061-20 ~]$ nslookup
> set type=MX
> ece.iastate.edu
Server:      129.186.1.200
Address:     129.186.1.200#53

ece.iastate.edu mail exchanger = 10 vulcan.ece.iastate.edu.
> □
```

5)

```
[489labuser@co2061-20 ~]$ nslookup
> 129.186.215.40
40.215.186.129.in-addr.arpa      name = spock.ee.iastate.edu.
```

ifconfig

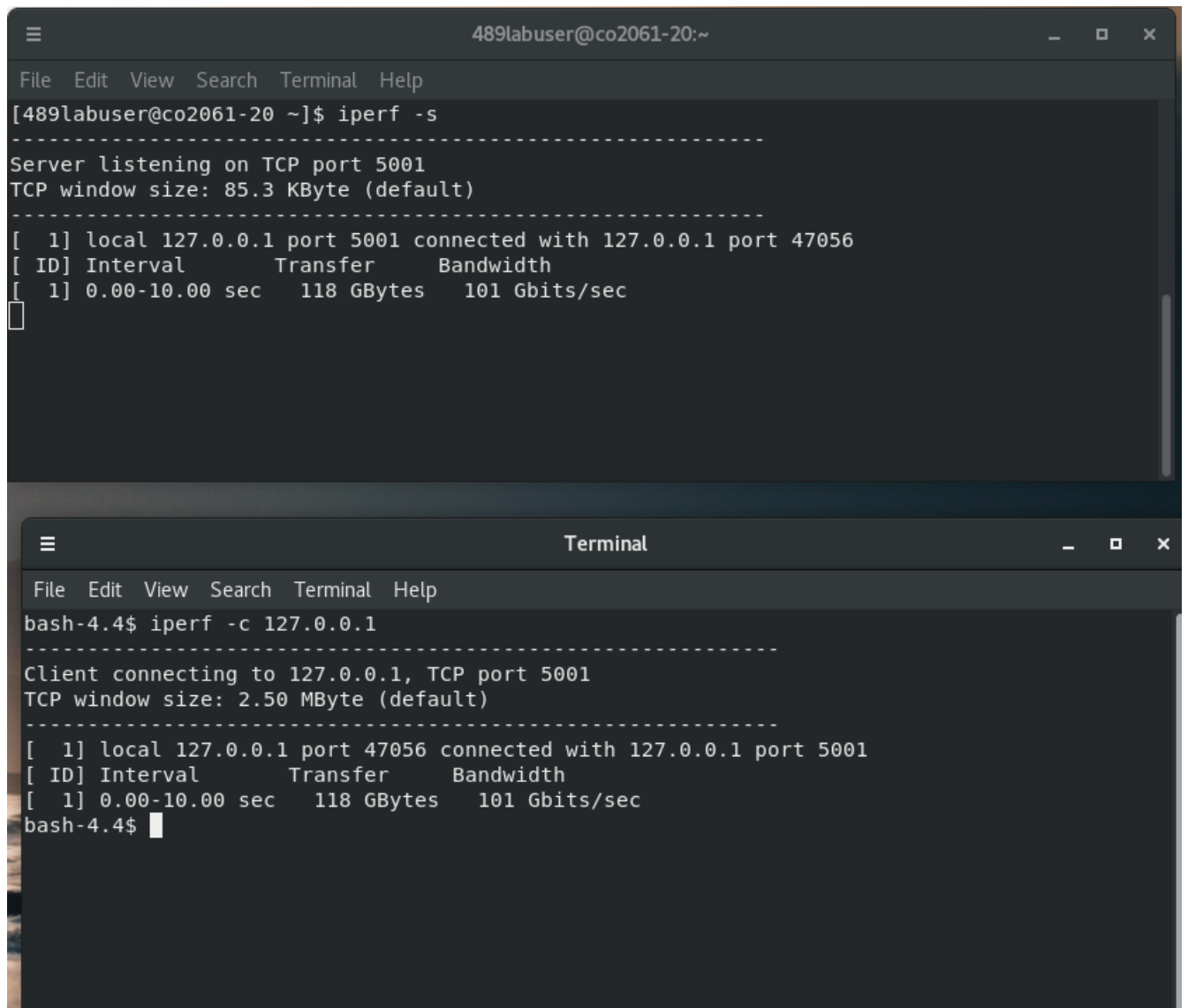
6)

```
[489labuser@co2061-20 ~]$ ifconfig enp3s0f0
enp3s0f0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.254.20  netmask 255.255.255.0  broadcast 192.168.254.255
    inet6 fe80::e63d:1aff:fea0:2c42  prefixlen 64  scopeid 0x20<link>
    ether e4:3d:1a:a0:2c:42  txqueuelen 1000  (Ethernet)
    RX packets 10078420  bytes 10262658522 (9.5 GiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 6456161  bytes 3995111653 (3.7 GiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
    device interrupt 16
```

IP address: 192.168.254.20

iperf

7)



The image shows two terminal windows. The top window is titled '489labuser@co2061-20:~' and shows the output of the command 'iperf -s'. It indicates the server is listening on TCP port 5001 with a window size of 85.3 KByte. A connection is established from 127.0.0.1 port 47056, and the bandwidth is measured as 101 Gbits/sec over a 10-second interval. The bottom window is titled 'Terminal' and shows the output of the command 'iperf -c 127.0.0.1'. It indicates the client is connecting to 127.0.0.1 on TCP port 5001 with a window size of 2.50 MByte. A connection is established from 127.0.0.1 port 47056, and the bandwidth is measured as 101 Gbits/sec over a 10-second interval.

```
489labuser@co2061-20:~$ iperf -s
-----
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
-----
[  1] local 127.0.0.1 port 5001 connected with 127.0.0.1 port 47056
[ ID] Interval      Transfer    Bandwidth
[  1] 0.00-10.00 sec  118 GBytes  101 Gbits/sec
bash-4.4$
```

```
bash-4.4$ iperf -c 127.0.0.1
-----
Client connecting to 127.0.0.1, TCP port 5001
TCP window size: 2.50 MByte (default)
-----
[  1] local 127.0.0.1 port 47056 connected with 127.0.0.1 port 5001
[ ID] Interval      Transfer    Bandwidth
[  1] 0.00-10.00 sec  118 GBytes  101 Gbits/sec
bash-4.4$
```

Using iperf we can measure the bandwidth. Above we run iperf -s on the server and iperf -c on the client. The bandwidth is 101 Gbps.

traceroute

```
[489labuser@co2061-20 ~]$ traceroute -n www.cmu.edu
traceroute to www.cmu.edu (128.2.42.52), 30 hops max, 60 byte packets
 1 192.168.254.254 0.601 ms 0.618 ms 0.619 ms
 2 129.186.5.253 1.270 ms 1.389 ms 1.685 ms
 3 129.186.0.194 1.033 ms 1.055 ms 129.186.0.192 1.059 ms
 4 129.186.0.139 1.201 ms 1.683 ms 129.186.0.137 1.648 ms
 5 129.186.254.245 1.303 ms 1.413 ms 129.186.254.255 1.180 ms
 6 192.188.159.233 1.233 ms 192.188.159.229 1.141 ms 192.188.159.233 1.046 ms
 7 192.188.159.101 0.875 ms 0.843 ms 0.841 ms
 8 192.188.159.106 1.761 ms 1.453 ms 1.257 ms
 9 192.188.159.159 1.791 ms 1.838 ms 1.928 ms
10 163.253.5.19 6.619 ms 6.598 ms 8.658 ms
11 163.253.1.52 34.595 ms 163.253.2.28 33.995 ms 163.253.1.56 34.609 ms
12 163.253.1.99 35.427 ms 163.253.1.95 35.398 ms 163.253.1.244 37.281 ms
13 163.253.2.19 35.313 ms 34.749 ms 34.598 ms
14 163.253.2.16 35.787 ms 35.629 ms 35.540 ms
15 163.253.1.138 34.785 ms 36.153 ms 36.119 ms
16 163.253.1.137 35.177 ms 36.171 ms 35.597 ms
17 163.253.5.33 32.736 ms 32.697 ms 32.670 ms
18 162.223.17.79 43.341 ms 43.302 ms 43.329 ms
19 128.2.255.181 43.173 ms 43.166 ms 43.174 ms
20 128.2.255.210 43.261 ms 43.268 ms 43.122 ms
21 128.2.42.52 43.190 ms 43.126 ms 43.334 ms
[489labuser@co2061-20 ~]$
```

```
[489labuser@co2061-20 ~]$ traceroute www.cmu.edu
traceroute to www.cmu.edu (128.2.42.52), 30 hops max, 60 byte packets
 1 gateway (192.168.254.254) 0.462 ms 0.430 ms 0.427 ms
 2 routerb-129-186-5-0.tele.iastate.edu (129.186.5.253) 1.098 ms 1.241 ms 1.571 ms
 3 e63-mpls-p-hu0-3-0-10--to--c12-mpls-pe-eth1-12.tele.iastate.edu (129.186.0.194) 1.056 ms 1.077 ms b31-mpls-p-hu0-3-0-10--to--c12-mpls-pe-eth1-1.tele.iastate.edu (129.186.0.192) 1.051 ms
 4 b31-mpls-pe-eth2-10--to--e63-mpls-p-hu0-2-0-1.tele.iastate.edu (129.186.0.141) 1.080 ms 1.550 ms 1.648 ms
 5 b31fr--b31fpe-vrrf-data.tele.iastate.edu (129.186.254.255) 1.213 ms 1.213 ms b31fr--e63fpe-vrrf-data.tele.iastate.edu (129.186.254.247) 1.564 ms
 6 e63be-eth2-2.fusion.tele.iastate.edu (192.188.159.231) 1.047 ms e63be-eth1-2.fusion.tele.iastate.edu (192.188.159.229) 1.635 ms e63be-eth2-2.fusion.tele.iastate.edu (192.188.159.231) 1.397 ms
 7 routerb-192-188-159-96.tele.iastate.edu (192.188.159.101) 1.246 ms 1.088 ms 1.047 ms
 8 rtr-e63be-vlan933.tele.iastate.edu (192.188.159.106) 1.725 ms 1.767 ms 2.014 ms
 9 rtr-b31isp1-be158.tele.iastate.edu (192.188.159.159) 1.644 ms 1.607 ms 1.954 ms
10 bundle-ether100-1420.core2.kans.net.internet2.edu (163.253.5.19) 7.530 ms 7.558 ms 9.575 ms
11 fourhundredge-0-0-0-21.4079.core1.kans.net.internet2.edu (163.253.1.52) 36.724 ms fourhundredge-0-0-0-4079.core1.chic.net.internet2.edu (163.253.2.28) 36.721 ms fourhundredge-0-0-0-21.4079.core1.kans.net.internet2.edu (163.253.1.52) 35.590 ms
12 fourhundredge-0-0-0-3.4079.core2.chic.net.internet2.edu (163.253.1.244) 35.746 ms 35.725 ms 35.766 ms
13 fourhundredge-0-0-0-3.4079.core2.eqch.net.internet2.edu (163.253.2.19) 35.647 ms 35.607 ms 35.618 ms
14 fourhundredge-0-0-0-4079.core2.clev.net.internet2.edu (163.253.2.16) 36.037 ms 33.994 ms 35.911 ms
15 fourhundredge-0-0-0-3.4079.core2.ashb.net.internet2.edu (163.253.1.138) 35.415 ms 34.234 ms 34.269 ms
16 fourhundredge-0-0-0-1.4079.core1.phil.net.internet2.edu (163.253.1.137) 34.085 ms 33.810 ms 33.824 ms
17 163.253.5.33 (163.253.5.33) 32.590 ms 32.713 ms 32.735 ms
18 162-223-17-79.static.firstlight.net (162.223.17.79) 42.934 ms 42.955 ms 42.837 ms
19 CORE255-POD-1-DCNS-8500.OW.CMU.NET (128.2.255.181) 57.943 ms 57.913 ms 56.903 ms
20 POD-D-DCNS-CORE255.OW.CMU.NET (128.2.255.210) 43.909 ms 43.290 ms 43.330 ms
21 WWW-CMU-PROD-VIP.ANDREW.CMU.EDU (128.2.42.52) 43.357 ms 43.322 ms 43.555 ms
[489labuser@co2061-20 ~]$
```

8)

Number of hops: 21

Routes/Gateway: 21 Routes. Gateways are the routers packet passes through

Latency: Latency is shown above in milliseconds, (43.190 + 43.190 + 43.126 + 43.334) ms

Reachability: Successfully reached destination 128.2.42.52

tcptraceroute

9)

```
[489labuser@co2061-20 ~]$ sudo tcptraceroute -q 2 www.ed.ac.uk
[sudo] password for 489labuser:
Running:
      traceroute -T -0 info -q 2 www.ed.ac.uk
traceroute to www.ed.ac.uk (23.185.0.1), 30 hops max, 60 byte packets
 1 _gateway (192.168.254.254)  0.301 ms  0.301 ms
 2 routera-129-186-5-0.tele.iastate.edu (129.186.5.252)  1.075 ms  1.381 ms
 3 b31-mpls-p-hu0-3-0-9--to--b11-mpls-pe-eth1-1.tele.iastate.edu (129.186.0.186)  0.673 ms e63-mpls
-p-hu0-3-0-9--to--b11-mpls-p-eth1-12.tele.iastate.edu (129.186.0.188)  0.778 ms
 4 b31-mpls-fpe-eth1-10--to--b31-mpls-p-hu0-2-0-1.tele.iastate.edu (129.186.0.135)  1.012 ms e63-mpl
ls-fpe-eth2-10--to--e63-mpls-p-hu0-3-0-1.tele.iastate.edu (129.186.0.139)  1.014 ms
 5 b31fr--b31fpe-vrf-data.tele.iastate.edu (129.186.254.255)  0.844 ms b31fr--e63fpe-vrf-data.tele.
iastate.edu (129.186.254.247)  1.054 ms
 6 b31be-eth1-2.fusion.tele.iastate.edu (192.188.159.227)  1.187 ms b31be-eth2-2.fusion.tele.iastat
e.edu (192.188.159.233)  1.183 ms
 7 routerb-192-188-159-96.tele.iastate.edu (192.188.159.101)  0.748 ms  0.827 ms
 8 rtr-b31be-vlan933.tele.iastate.edu (192.188.159.105)  1.734 ms  1.732 ms
 9 rtr-b31ispl-be152.tele.iastate.edu (192.188.159.153)  1.674 ms  1.653 ms
10 bundle-ether100.1421.core2.kans.net.internet2.edu (198.71.47.103)  7.596 ms  7.601 ms
11 fourhundredge-0-0-0-0.4079.core1.chic.net.internet2.edu (163.253.2.28)  17.544 ms  17.535 ms
12 fourhundredge-0-0-0-0.4079.core1.eqch.net.internet2.edu (163.253.1.207)  18.013 ms  20.164 ms
13 fourhundredge-0-0-0-49.4079.aggl.eqch.net.internet2.edu (163.253.1.215)  18.301 ms fourhundredge
-0-0-0-49.4079.agg2.eqch.net.internet2.edu (163.253.1.219)  18.370 ms
14 23.235.41.168 (23.235.41.168)  16.322 ms  16.348 ms
15 23.185.0.1 (23.185.0.1) <syn,ack>  16.620 ms  16.700 ms
```

```
[489labuser@co2061-20 ~]$ traceroute -n www.ed.ac.uk
traceroute to www.ed.ac.uk (23.185.0.1), 30 hops max, 60 byte packets
 1 192.168.254.254  0.554 ms  0.551 ms  0.529 ms
 2 129.186.5.252  1.153 ms  1.507 ms  1.560 ms
 3 129.186.0.188  1.021 ms 129.186.0.186  1.020 ms 129.186.0.188  1.041 ms
 4 129.186.0.139  1.143 ms 129.186.0.135  1.135 ms 129.186.0.139  1.490 ms
 5 129.186.254.255  1.212 ms  1.331 ms 129.186.254.245  1.334 ms
 6 192.188.159.233  1.325 ms 192.188.159.231  1.024 ms 192.188.159.233  1.020 ms
 7 192.188.159.101  0.925 ms  0.590 ms  0.590 ms
 8 192.188.159.105  1.155 ms  1.149 ms  1.538 ms
 9 192.188.159.153  1.372 ms  1.634 ms  1.730 ms
10 198.71.47.103  8.145 ms  8.166 ms  10.200 ms
11 163.253.2.28  19.190 ms  19.180 ms  19.094 ms
12 163.253.1.207  17.938 ms  19.640 ms  19.607 ms
13 163.253.1.219  18.992 ms  18.428 ms 163.253.1.215  18.402 ms
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 *
  * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
```

tcptraceroute uses TCP protocol rather than UDP or ICMP. Here we notice that TCP is more accessible. This is proved by having lesser number of hops compared to traceroute function.

We also notice that the latency is lesser in tcptraceroute. Both these functions call different protocols and it depends on choice of protocol to trace.

Nmap

10)

From ifconfig function we found that the IP address of interface enp3s0f0 was 192.168.254.20.

```
[489labuser@co2061-20 ~]$ nmap -Pn 192.168.254.20
Starting Nmap 7.70 ( https://nmap.org ) at 2023-10-22 16:44 CDT
Nmap scan report for 192.168.254.20
Host is up (0.000032s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
[489labuser@co2061-20 ~]$
```

This shows that ssh, port 22 is open.

tcpdump

11)

At first, when we run tcpdump icmp (tcpdump for icmp packets coming in) we don't see anything.

```
[489labuser@co2061-20 ~]$ sudo tcpdump icmp
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0f0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

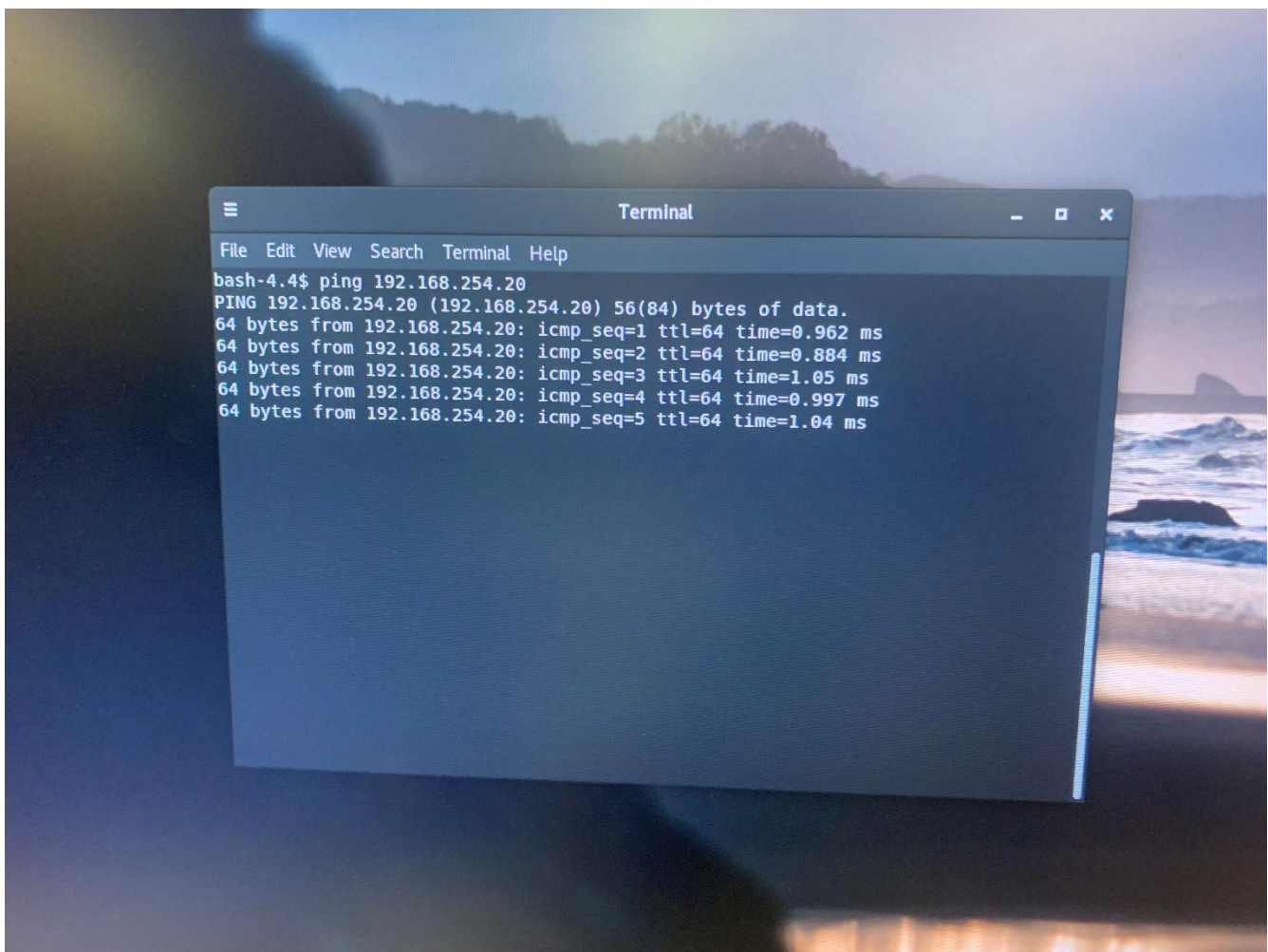
But when we ping 192.168.254.20 (enp3s0f0) for my computer from attacker's computer, we see this on my system.


```
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0
device interrupt 19 memory 0x72280000-722a0000

enp3s0f0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.254.19 netmask 255.255.255.0 broadcast 192.168.254.255
    inet6 fe80::e63d:1aff:fea0:3d7e prefixlen 64
    ether e4:3d:1a:a0:3d:7e txqueuelen 1000 (Ethernet)
    RX packets 26487675 bytes 21655295993 (20.1 GiB)
    RX errors 0 dropped 5 overruns 0 frame 0
    TX packets 21450241 bytes 14802718976 (13.7 GiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 16

enp3s0f1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.77.19 netmask 255.255.255.0 broadcast 192.168.77.255
    inet6 fe80::e63d:1aff:fea0:3d7f prefixlen 64 scopeid 0x20:::
    ether e4:3d:1a:a0:3d:7f txqueuelen 1000 (Ethernet)
    RX packets 55688 bytes 4155200 (4.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 55688 bytes 4155200 (4.0 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 17
```

Above is the Ip for the attacker's computer. From this computer we ping the IP of my computer. This is shown below.



When the ping is started, we see that the ‘sudo tcpdump icmp’ command on our system starts printing data.

```
[489labuser@co2061-20 ~]$ sudo tcpdump icmp
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0f0, link-type EN10MB (Ethernet), capture size 262144 bytes
17:06:45.764287 IP 192.168.254.19 > co2061-20.ece.iastate.edu: ICMP echo request, id 4, seq 1, length 64
17:06:45.764365 IP co2061-20.ece.iastate.edu > 192.168.254.19: ICMP echo reply, id 4, seq 1, length 64
17:06:46.765474 IP 192.168.254.19 > co2061-20.ece.iastate.edu: ICMP echo request, id 4, seq 2, length 64
17:06:46.765536 IP co2061-20.ece.iastate.edu > 192.168.254.19: ICMP echo reply, id 4, seq 2, length 64
17:06:47.766820 IP 192.168.254.19 > co2061-20.ece.iastate.edu: ICMP echo request, id 4, seq 3, length 64
17:06:47.766888 IP co2061-20.ece.iastate.edu > 192.168.254.19: ICMP echo reply, id 4, seq 3, length 64
17:06:48.768081 IP 192.168.254.19 > co2061-20.ece.iastate.edu: ICMP echo request, id 4, seq 4, length 64
17:06:48.768144 IP co2061-20.ece.iastate.edu > 192.168.254.19: ICMP echo reply, id 4, seq 4, length 64
17:06:49.768742 IP 192.168.254.19 > co2061-20.ece.iastate.edu: ICMP echo request, id 4, seq 5, length 64
```

This shows the IP address of the device (192.168.254.19) pinging my device.

Wireshark

12)

```
30 20.221.234.34 (20.221.234.34) <syn,ack> 26.538 ms 29.630 ms
[489labuser@co2061-20 nzaheer]$ sudo tcptraceroute -q 2 www.iastate.edu
```

We can use nslookup to find iastate.edu IP address, I used 129.168.215.40 from firefox and ran filtered tcp connections from wireshark. Below is the result I got.

Wireshark · Conversations · enp3s0f0									
Ethernet · 4		IPv4 · 8		IPv6		TCP · 8		UDP · 14	
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
192.168.254.20	56330	10.93.0.11	389	3	263	2	203	1	6
192.168.254.20	49746	23.210.14.58	80	6	396	3	198	3	19
192.168.254.20	49748	23.210.14.58	80	6	396	3	198	3	19
192.168.254.20	43168	34.107.221.82	80	6	396	3	198	3	19
192.168.254.20	43182	34.107.221.82	80	6	396	3	198	3	19
192.168.254.20	56304	129.186.215.40	80	2	148	2	148	0	
192.168.254.20	56320	129.186.215.40	80	2	148	2	148	0	
10.24.109.220	2049	192.168.254.20	691	11	2,758	4	1,256	7	1,50

☐ Name resolution
☐ Limit to display filter
☐ Absolute start time

Conversation Types ▼

Help

Copy ▼

Follow Stream...

Graph...

Close

13)

As I previously mentioned, running ifconfig on the other system, shows the IP to be, 192.168.254.19.

Using the custom filter we can check for the specific IP for ICMP protocol. This show that 784 bites were transmitted. Arrival time is displayed above

14)

traceroute:

Traceroute usually Pings the system, which usually uses the ICMP protocol.

Wireshark interface showing a packet capture on interface *enp3s0f0. The filter is `ip.src == 23.203.151.149`.

No.	Time	Source	Destination	Protocol	Length	Info
889	23.600921369	23.203.151.149	192.168.254.20	ICMP	70	Time-to-live exceeded (
890	23.600950030	23.203.151.149	192.168.254.20	ICMP	70	Time-to-live exceeded (
891	23.600956194	23.203.151.149	192.168.254.20	ICMP	70	Time-to-live exceeded (
1106	48.449146950	23.203.151.149	192.168.254.20	ICMP	70	Time-to-live exceeded (
1110	48.568155700	23.203.151.149	192.168.254.20	ICMP	70	Time-to-live exceeded (
1111	48.568196214	23.203.151.149	192.168.254.20	ICMP	70	Time-to-live exceeded (

Frame 889: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0

- Ethernet II, Src: IntelCor_89:77:75 (68:05:ca:89:77:75), Dst: e4:3d:1a:a0:2c:42 (e4:3d:1a:a0:2c:42)
- Internet Protocol Version 4, Src: 23.203.151.149, Dst: 192.168.254.20
- Internet Control Message Protocol

Hex dump:

```

0000  e4 3d 1a a0 2c 42 68 05  ca 89 77 75 08 00 45 00  ····,Bh···wu··E·
0010  00 38 08 55 40 00 f2 01  12 52 17 cb 97 95 c0 a8  ·8·U@··· ·R·····

```

Wireshark status: wireshark_enp3s0f0_202...22175856_n6mo6O.pcapn Packets: 1297 · Displayed: 6 (0.5%) · Dropped: 0 (0.0%) Profile: Default

Terminal window showing traceroute output:

```

489labuser@co2061-20:~
File Edit View Search Terminal Help
10 198.71.47.103 9.399 ms 9.390 ms 9.342 ms
11 163.253.2.28 19.335 ms 19.222 ms 19.187 ms
12 163.253.1.207 18.887 ms 18.891 ms 18.846 ms
13 163.253.1.217 17.530 ms 16.821 ms 163.253.1.219 18.380 ms
14 162.252.69.233 15.108 ms 15.071 ms 14.950 ms
15 23.203.151.149 22.836 ms * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
[489labuser@co2061-20 ~]$ traceroute -n www.ebay.com

```

tcptraceroute: TCP

Wireshark interface showing packet capture on *enp3s0f0. The filter is `ip.src == 184.25.173.37`.

No.	Time	Source	Destination	Protocol	Length	Info
113	4.875405172	184.25.173.37	192.168.254.20	TCP	74	80 → 46425 [SYN, ACK] S
114	4.875406912	184.25.173.37	192.168.254.20	TCP	74	80 → 58573 [SYN, ACK] S
117	4.875522518	184.25.173.37	192.168.254.20	TCP	74	80 → 33019 [SYN, ACK] S
119	4.880144202	184.25.173.37	192.168.254.20	TCP	74	80 → 34857 [SYN, ACK] S
121	4.885366507	184.25.173.37	192.168.254.20	TCP	74	80 → 48039 [SYN, ACK] S
123	4.885382281	184.25.173.37	192.168.254.20	TCP	74	80 → 44793 [SYN, ACK] S
128	5.944756240	184.25.173.37	192.168.254.20	TCP	74	[TCP Retransmission] 80

Frame 113 details:

- Frame 113: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
- Ethernet II, Src: IntelCor_89:77:75 (68:05:ca:89:77:75), Dst: e4:3d:1a:a0:2c:42 (e4:3d:1a:a0:2c:42)
- Internet Protocol Version 4, Src: 184.25.173.37, Dst: 192.168.254.20
- Transmission Control Protocol, Src Port: 80, Dst Port: 46425, Seq: 0, Ack: 1, Len: 0

Packet 113 hex dump:

```

0000  e4 3d 1a a0 2c 42 68 05 ca 89 77 75 08 00 45 00  .=. ., Bh . .wu . .E.
0010  00 3c 00 00 40 00 30 06 26 c0 b8 19 ad 25 c0 a8  .< . .@ . 0 . & . . . % .

```

Wireshark status: wireshark_enp3s0f0_202...22180325_VRGDRU.pcapng Packets: 134 · Displayed: 7 (5.2%) · Dropped: 0 (0.0%) Profile: Default

Terminal output showing traceroute results:

```

489labuser@co2061-20:~$ traceroute -T -0 info -n www.ebay.com
traceroute to www.ebay.com (184.25.173.37), 30 hops max, 60 byte packets
 1 192.168.254.254 0.314 ms 0.312 ms 0.394 ms
 2 129.186.5.252 1.027 ms 1.295 ms 1.447 ms
 3 129.186.0.188 0.714 ms 0.736 ms 0.818 ms
 4 129.186.0.139 1.282 ms 129.186.0.137 1.054 ms 129.186.0.141 1.003 ms
 5 129.186.254.255 0.980 ms 129.186.254.245 1.175 ms 129.186.254.247 1.008 ms
 6 192.188.159.229 1.064 ms 192.188.159.233 1.039 ms 192.188.159.231 1.105 ms
 7 192.188.159.101 0.690 ms 0.679 ms 0.693 ms
 8 192.188.159.121 1.299 ms 1.209 ms 1.440 ms
 9 192.188.159.153 1.268 ms 1.581 ms 1.772 ms
10 198.71.47.103 8.894 ms 8.844 ms 8.882 ms
11 163.253.2.28 19.208 ms 19.207 ms 19.168 ms
12 163.253.1.207 18.163 ms 18.184 ms 18.172 ms
13 163.253.1.217 18.248 ms 163.253.1.219 17.503 ms 163.253.1.217 17.482 ms
14 208.115.136.73 28.086 ms 162.252.69.233 14.921 ms 208.115.136.73 27.808 ms
15 23.203.151.173 15.401 ms * 15.088 ms
16 * * *
17 * * *
18 * * *
19 184.25.173.37 <syn,ack> 14.975 ms 14.855 ms 14.831 ms
[489labuser@co2061-20 ~]$

```

Since `tcptraceroute` traces the tcp pipeline, after adding the filter of the destination IP of ebay, we find the type of packets by `tcptraceroute` is TCP

