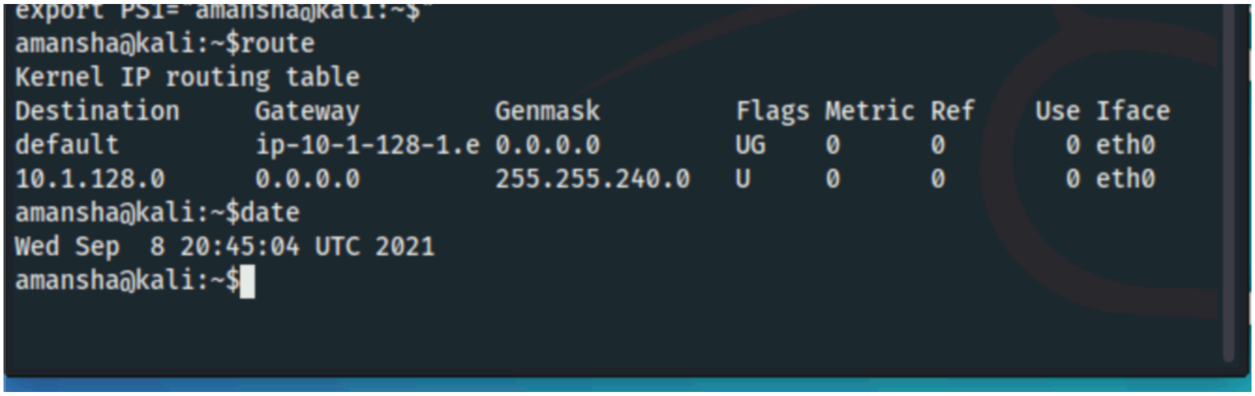
Amir Mansha
CYSE 425
Fall 2021
Lab 2-1

Task 3: Run the route command

In Task 3 I Ran the route terminal, My Network ID popped up and it is 10.1.128.0



```
export PS1='amansha@kali:~$'
amansha@kali:~$route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         ip-10-1-128-1.e 0.0.0.0         UG    0      0        0 eth0
10.1.128.0      0.0.0.0         255.255.240.0   U     0      0        0 eth0
amansha@kali:~$date
Wed Sep  8 20:45:04 UTC 2021
amansha@kali:~$
```

Task 4: Run the nmap command

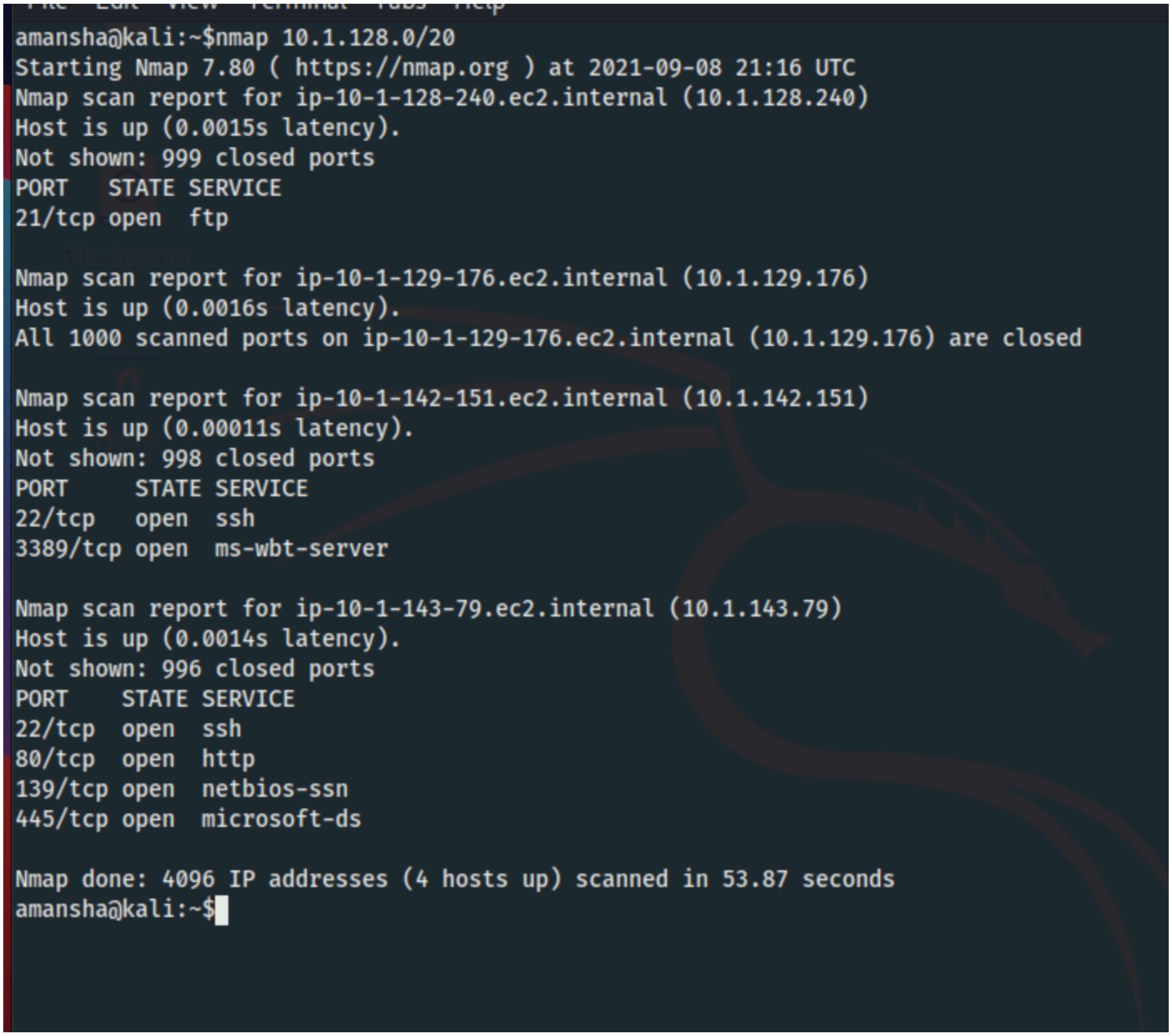
I Used the nmap command to scan the network for hosts
The 4 hosts IP Addresses that showed up are:

- 10.1.128.240
    - Open Ports:
    - 21/tcp
- 10.1.129.176
    - All ports are closed

- 10.1.142.151
    - Open Ports:
    - 22/tcp
    - 3389/tcp
- 10.1.143.79
    - 22/tcp
    - 80/tcp
    - 139/tcp

Amir Mansha
CYSE 425
Fall 2021
Lab 2-1

- 445/tcp

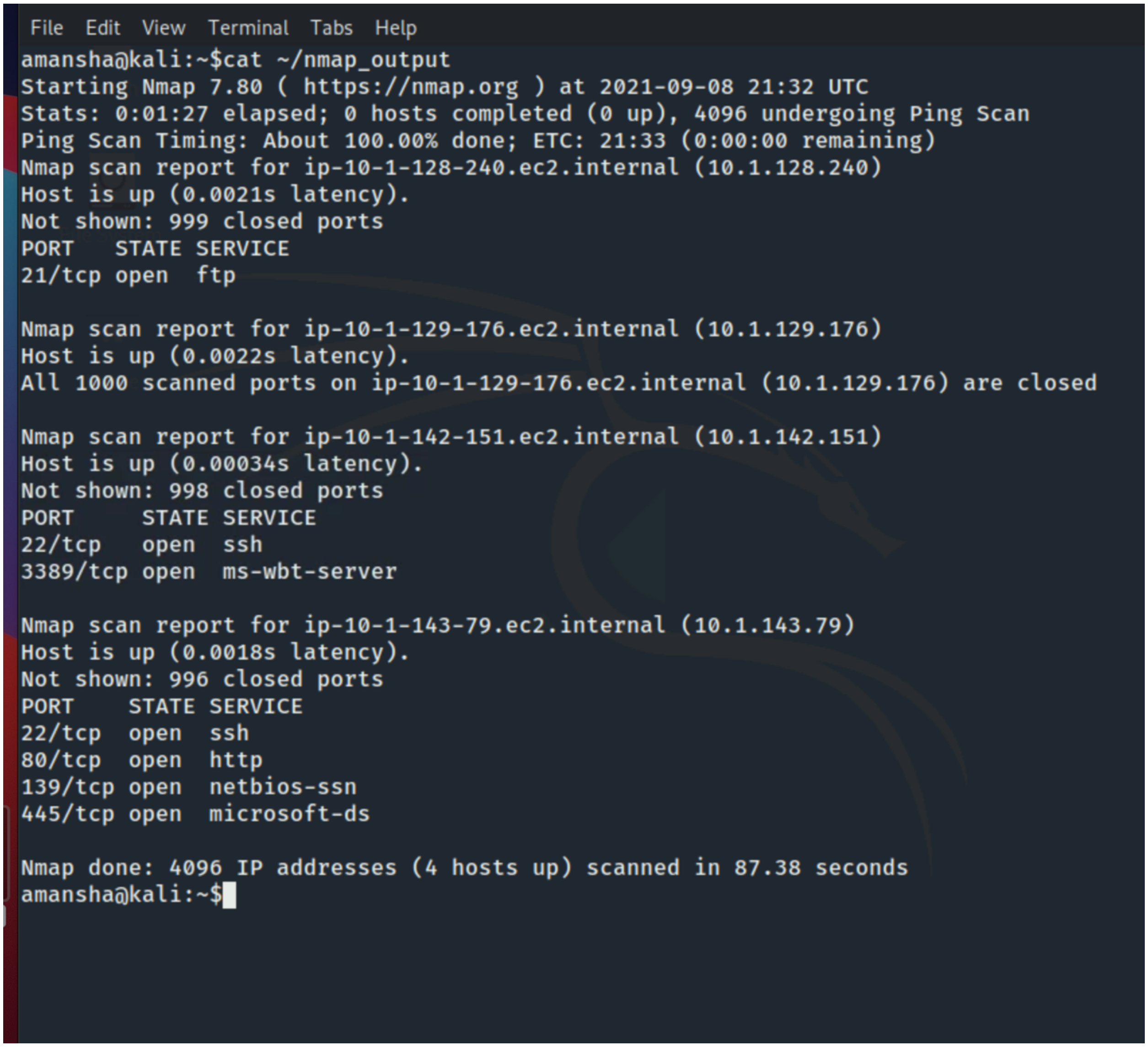


```
amansha@kali:~$nmap 10.1.128.0/20
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-08 21:16 UTC
Nmap scan report for ip-10-1-128-240.ec2.internal (10.1.128.240)
Host is up (0.0015s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp

Nmap scan report for ip-10-1-129-176.ec2.internal (10.1.129.176)
Host is up (0.0016s latency).
All 1000 scanned ports on ip-10-1-129-176.ec2.internal (10.1.129.176) are closed

Nmap scan report for ip-10-1-142-151.ec2.internal (10.1.142.151)
Host is up (0.00011s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server

Nmap scan report for ip-10-1-143-79.ec2.internal (10.1.143.79)
Host is up (0.0014s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 4096 IP addresses (4 hosts up) scanned in 53.87 seconds
amansha@kali:~$
```

Task 5: Save the nmap output to a file

I Used nmap command to save the file and then used the cat command to see if it saved

Amir Mansha
CYSE 425
Fall 2021
Lab 2-1

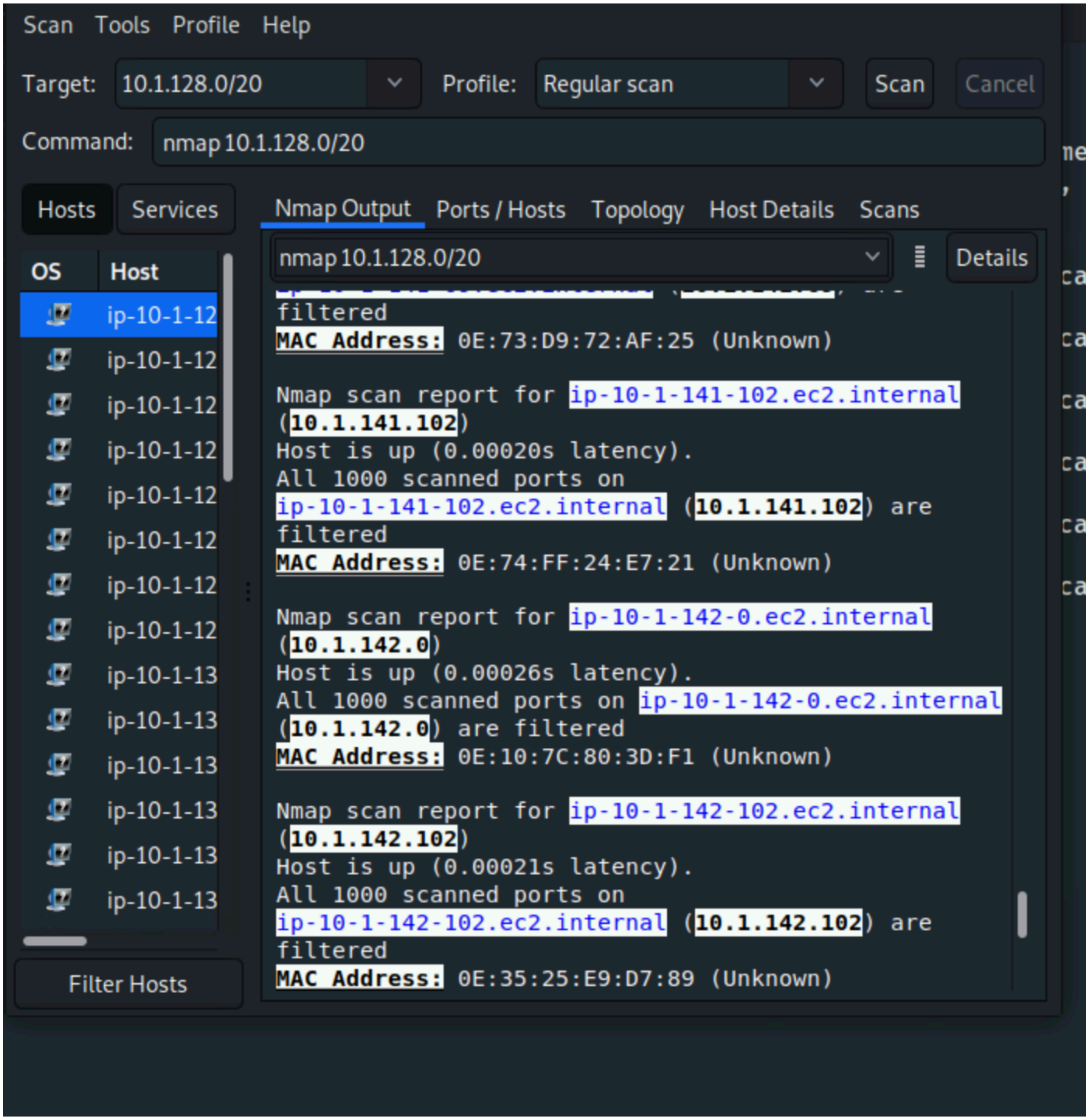


```
amansha@kali:~$cat ~/nmap_output
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-08 21:32 UTC
Stats: 0:01:27 elapsed; 0 hosts completed (0 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 100.00% done; ETC: 21:33 (0:00:00 remaining)
Nmap scan report for ip-10-1-128-240.ec2.internal (10.1.128.240)
Host is up (0.0021s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp

Nmap scan report for ip-10-1-129-176.ec2.internal (10.1.129.176)
Host is up (0.0022s latency).
All 1000 scanned ports on ip-10-1-129-176.ec2.internal (10.1.129.176) are closed

Nmap scan report for ip-10-1-142-151.ec2.internal (10.1.142.151)
Host is up (0.00034s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server

Nmap scan report for ip-10-1-143-79.ec2.internal (10.1.143.79)
Host is up (0.0018s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 4096 IP addresses (4 hosts up) scanned in 87.38 seconds
amansha@kali:~$
```

Task 6: Scan the network with Zenmap

I ran sudo command and started zenmap. However, I got different results. The amount of hosts I got In zenmap were way more

Amir Mansha
CYSE 425
Fall 2021
Lab 2-1



```
filtered
MAC Address: 0E:73:D9:72:AF:25 (Unknown)

Nmap scan report for ip-10-1-141-102.ec2.internal
(10.1.141.102)
Host is up (0.00020s latency).
All 1000 scanned ports on
ip-10-1-141-102.ec2.internal (10.1.141.102) are
filtered
MAC Address: 0E:74:FF:24:E7:21 (Unknown)

Nmap scan report for ip-10-1-142-0.ec2.internal
(10.1.142.0)
Host is up (0.00026s latency).
All 1000 scanned ports on ip-10-1-142-0.ec2.internal
(10.1.142.0) are filtered
MAC Address: 0E:10:7C:80:3D:F1 (Unknown)

Nmap scan report for ip-10-1-142-102.ec2.internal
(10.1.142.102)
Host is up (0.00021s latency).
All 1000 scanned ports on
ip-10-1-142-102.ec2.internal (10.1.142.102) are
filtered
MAC Address: 0E:35:25:E9:D7:89 (Unknown)
```