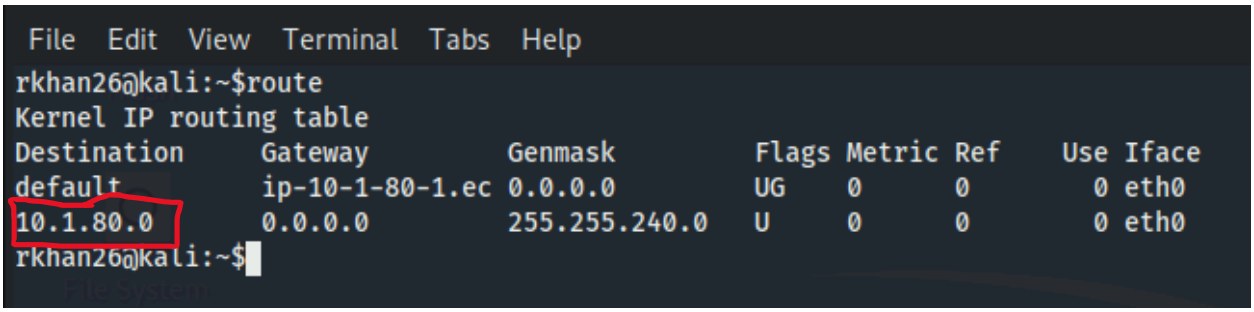
Roozah Khan
Laboratory Exercise 2-1 – Reconnaissance Lab Exercise

Task 3: Run the route command



I used the command route to find my network ID and my network ID is 10.1.80.0.

Task 4: Run the nmap command

```
rkhan26@kali:~$nmap 10.1.80.0/20
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-08 21:00 UTC
Nmap scan report for ip-10-1-82-83.ec2.internal (10.1.82.83)
Host is up (0.0025s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp

Nmap scan report for ip-10-1-90-125.ec2.internal (10.1.90.125)
Host is up (0.0030s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for ip-10-1-94-111.ec2.internal (10.1.94.111)
Host is up (0.0030s 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 scan report for ip-10-1-94-170.ec2.internal (10.1.94.170)
Host is up (0.00013s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server

Nmap done: 4096 IP addresses (4 hosts up) scanned in 54.90 seconds
rkhan26@kali:~$
```

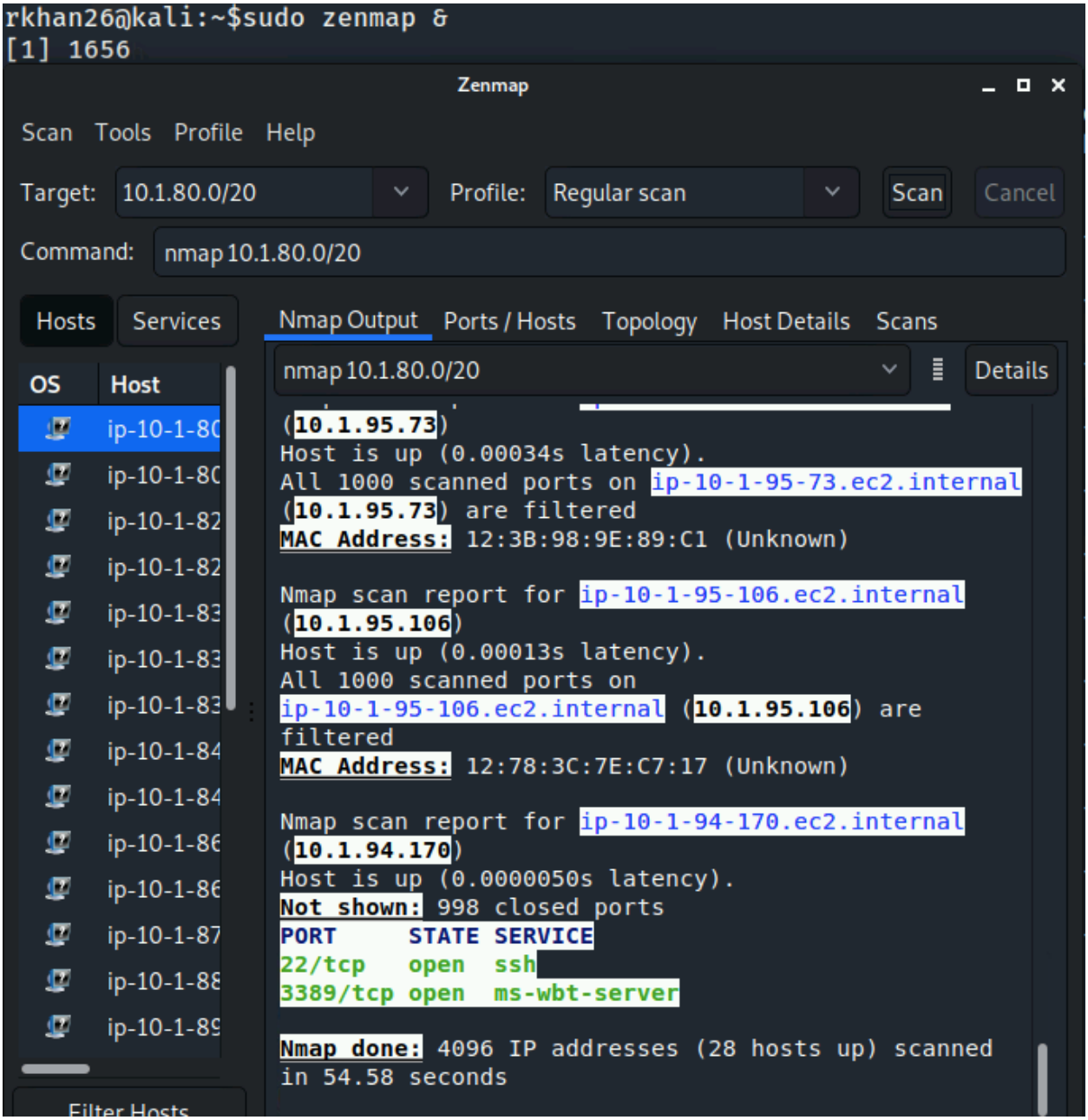
The IP addresses found for the 4 hosts are: 10.1.82.83, 10.1.90.125, 10.1.94.111, 10.1.94.170.
The open ports found for each host are:
21/tcp
80/tcp
22/tcp , 80/tcp, 139/tcp , 445/tcp
22/tcp, 3389/tcp

Task 5: Save the nmap output to a file

```
rkhan26@kali:~$nmap 10.1.80.0/20 > ~/nmap_output
rkhan26@kali:~$cat ~/nmap_output
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-08 21:33 UTC
Nmap scan report for ip-10-1-82-83.ec2.internal (10.1.82.83)
Host is up (0.0037s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp

Nmap scan report for ip-10-1-90-125.ec2.internal (10.1.90.125)
Host is up (0.0042s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for ip-10-1-94-111.ec2.internal (10.1.94.111)
Host is up (0.0040s 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 scan report for ip-10-1-94-170.ec2.internal (10.1.94.170)
Host is up (0.000095s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server

Nmap done: 4096 IP addresses (4 hosts up) scanned in 69.58 seconds
rkhan26@kali:~$
```

I used nmap command again to copy the output to a file called “nmap_output.” I used the cat command to view the contents in the file.

Task 6: Scan the network with Zenmap



I used the zenmap command to open up zenmap. The zenmap scan results and nmap scan results are different. The zenmap scan results has more results (hosts) than the nmap scan results. The Zenmap scan results include the nmap scan results but with more hosts.