Institute of Information Technology

University of Dhaka

Course Title

Information Security (CSE- 411)

Topic: Domain analysis using Nmap

Submitted By

Muktadul Islam
BSSE 12th batch
Roll No: 1215

Submitted To

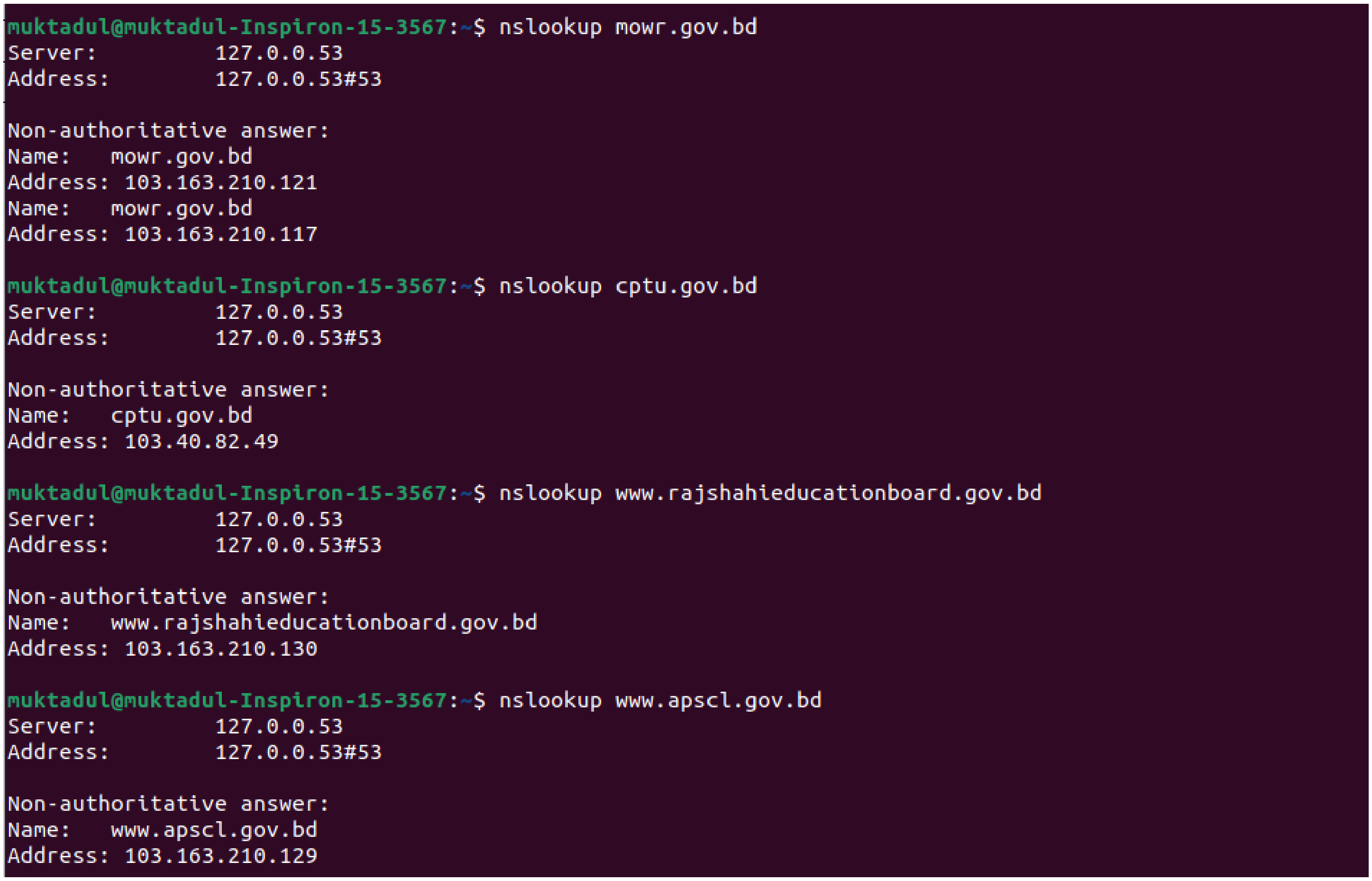
Mohammed Shafiul Alam Khan
Associate Professor & Director, IIT, DU

Date of Submission

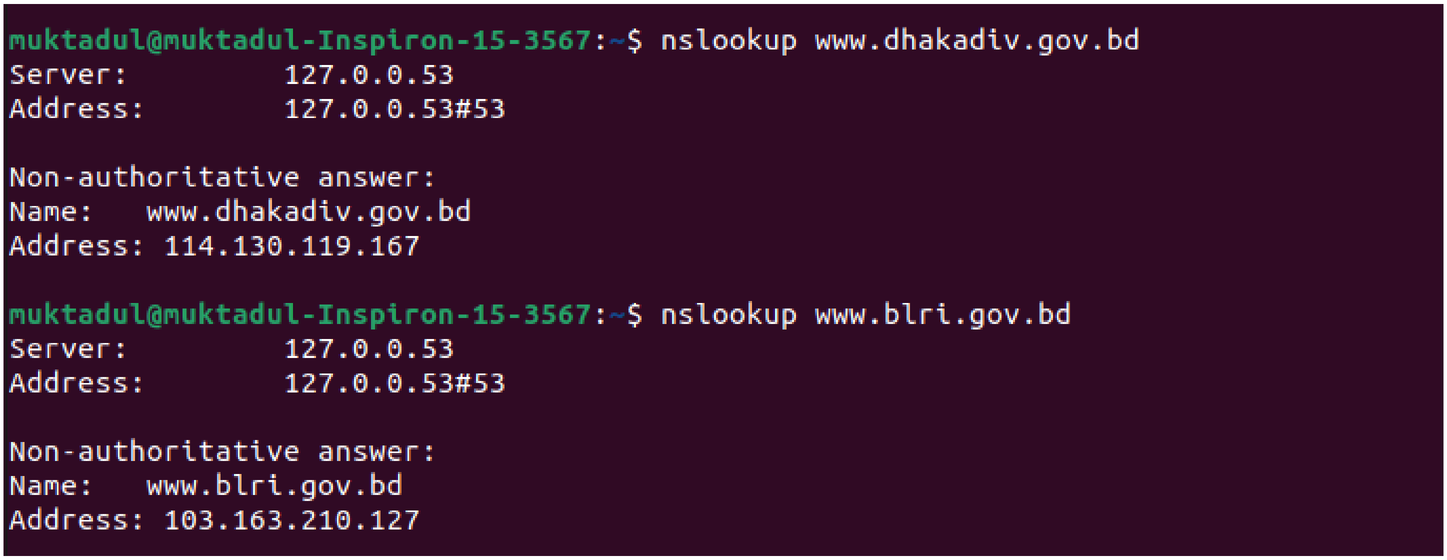
2nd October, 2022

The givens sites are and their IP addresses:

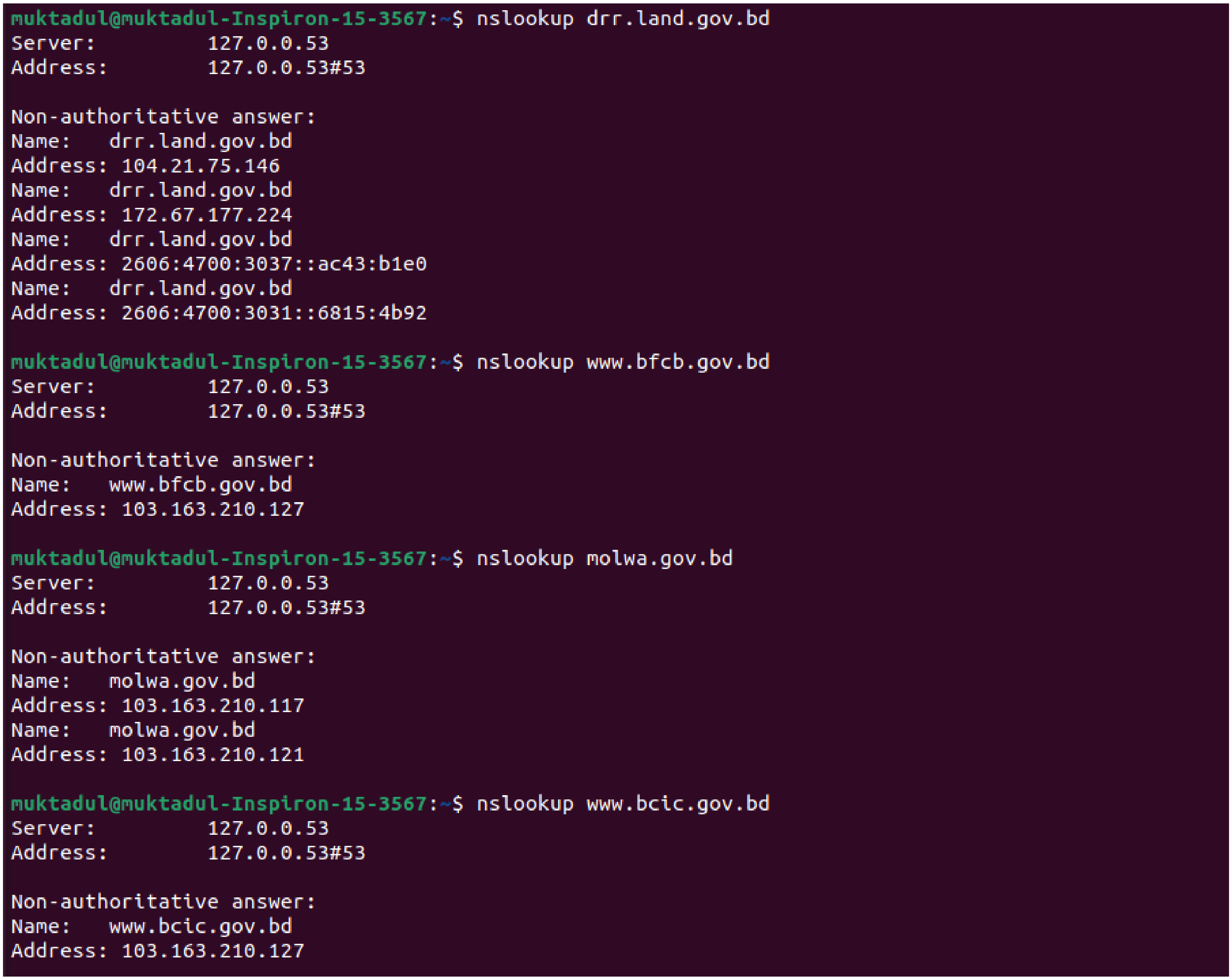
Serial No.	Domain	IP Address
01	https://cptu.gov.bd	103.40.82.49
02	https://mowr.gov.bd	103.163.210.121
03	http://www.rajshahieducationboard.gov.bd	103.163.210.130
04	http://www.apscl.gov.bd	103.163.210.129
05	http://www.dhakadiv.gov.bd	114.130.119.167
06	http://www.blri.gov.bd	103.163.210.127
07	http://drr.land.gov.bd	104.21.75.146
08	http://www.bfcb.gov.bd	103.163.210.127
09	https://molwa.gov.bd	103.163.210.117
10	http://www.bcic.gov.bd	103.163.210.127



```
muktadul@muktadul-Inspiron-15-3567:~$ nslookup mowr.gov.bd
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   mowr.gov.bd
Address: 103.163.210.121
Name:   mowr.gov.bd
Address: 103.163.210.117

muktadul@muktadul-Inspiron-15-3567:~$ nslookup cptu.gov.bd
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   cptu.gov.bd
Address: 103.40.82.49

muktadul@muktadul-Inspiron-15-3567:~$ nslookup www.rajshahieducationboard.gov.bd
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.rajshahieducationboard.gov.bd
Address: 103.163.210.130

muktadul@muktadul-Inspiron-15-3567:~$ nslookup www.apscl.gov.bd
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.apscl.gov.bd
Address: 103.163.210.129
```



```
muktadul@muktadul-Inspiron-15-3567:~$ nslookup www.dhakadiv.gov.bd
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.dhakadiv.gov.bd
Address: 114.130.119.167

muktadul@muktadul-Inspiron-15-3567:~$ nslookup www.blri.gov.bd
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.blri.gov.bd
Address: 103.163.210.127
```



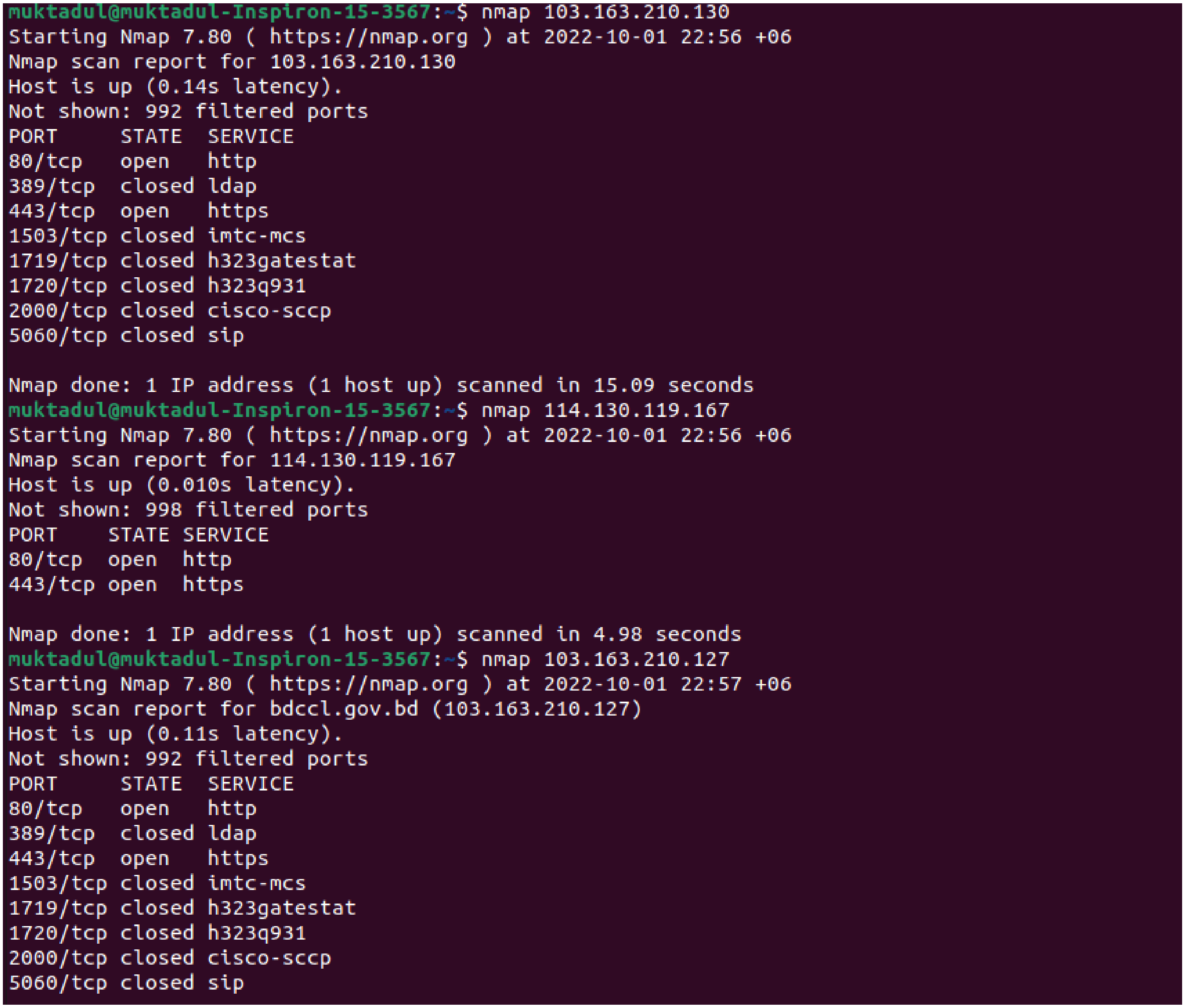
```
muktadul@muktadul-Inspiron-15-3567:~$ nslookup drr.land.gov.bd
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   drr.land.gov.bd
Address: 104.21.75.146
Name:   drr.land.gov.bd
Address: 172.67.177.224
Name:   drr.land.gov.bd
Address: 2606:4700:3037::ac43:b1e0
Name:   drr.land.gov.bd
Address: 2606:4700:3031::6815:4b92

muktadul@muktadul-Inspiron-15-3567:~$ nslookup www.bfcb.gov.bd
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.bfcb.gov.bd
Address: 103.163.210.127

muktadul@muktadul-Inspiron-15-3567:~$ nslookup molwa.gov.bd
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   molwa.gov.bd
Address: 103.163.210.117
Name:   molwa.gov.bd
Address: 103.163.210.121

muktadul@muktadul-Inspiron-15-3567:~$ nslookup www.bcic.gov.bd
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.bcic.gov.bd
Address: 103.163.210.127
```

So the selected IPs:

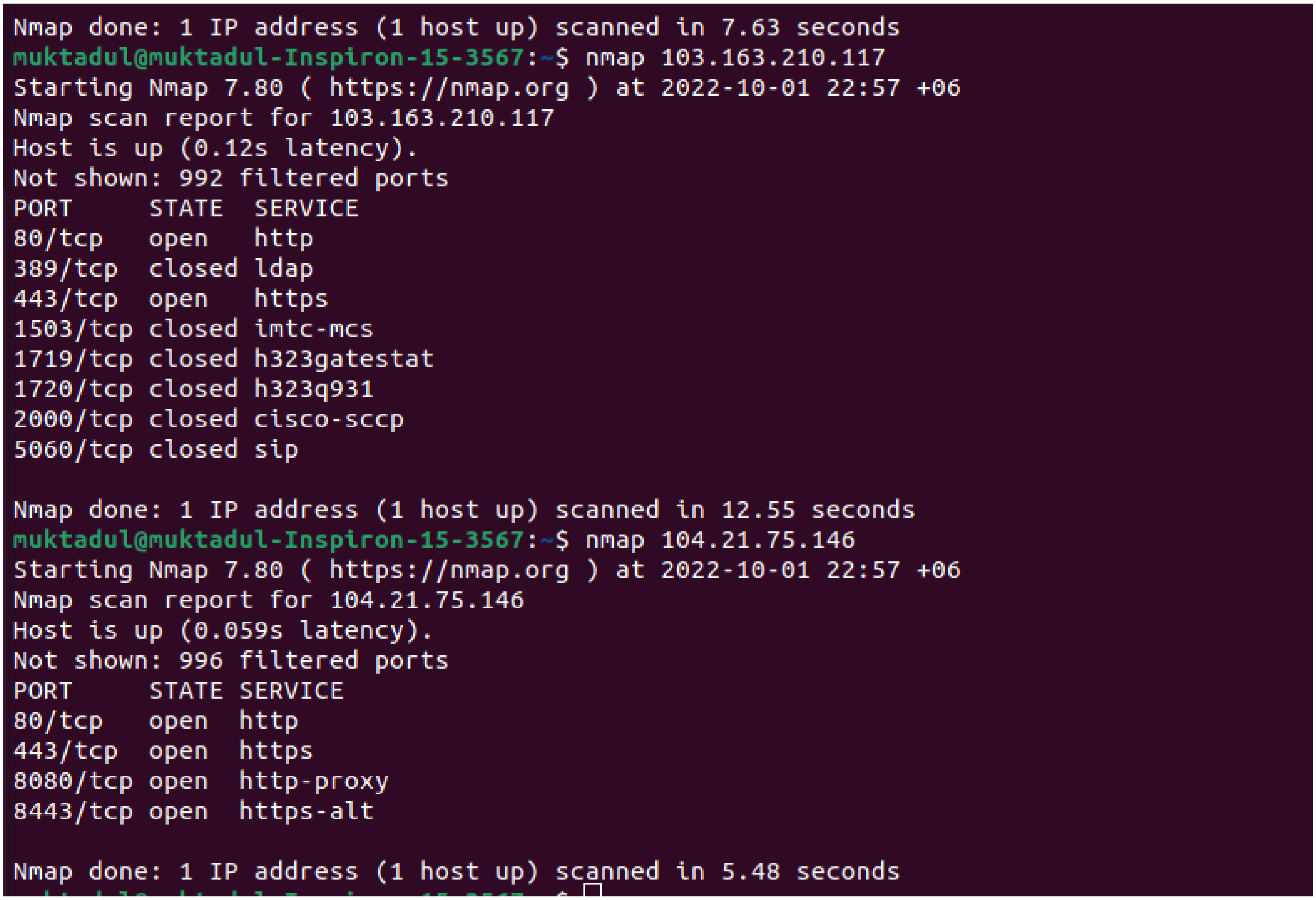
1. 103.163.210.130
2. 114.130.119.167
3. 103.163.210.127
4. 103.163.210.117
5. 104.21.75.146

Target Specification

1. Now we have to perform “nmap IP” to find it’s ports and protocols:



```
muktadul@muktadul-Inspiron-15-3567:~$ nmap 103.163.210.130
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 22:56 +06
Nmap scan report for 103.163.210.130
Host is up (0.14s latency).
Not shown: 992 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
389/tcp  closed ldap
443/tcp  open   https
1503/tcp closed imtc-mcs
1719/tcp closed h323gatestat
1720/tcp closed h323q931
2000/tcp closed cisco-sccp
5060/tcp closed sip

Nmap done: 1 IP address (1 host up) scanned in 15.09 seconds
muktadul@muktadul-Inspiron-15-3567:~$ nmap 114.130.119.167
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 22:56 +06
Nmap scan report for 114.130.119.167
Host is up (0.010s 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 4.98 seconds
muktadul@muktadul-Inspiron-15-3567:~$ nmap 103.163.210.127
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 22:57 +06
Nmap scan report for bdccl.gov.bd (103.163.210.127)
Host is up (0.11s latency).
Not shown: 992 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
389/tcp  closed ldap
443/tcp  open   https
1503/tcp closed imtc-mcs
1719/tcp closed h323gatestat
1720/tcp closed h323q931
2000/tcp closed cisco-sccp
5060/tcp closed sip
```



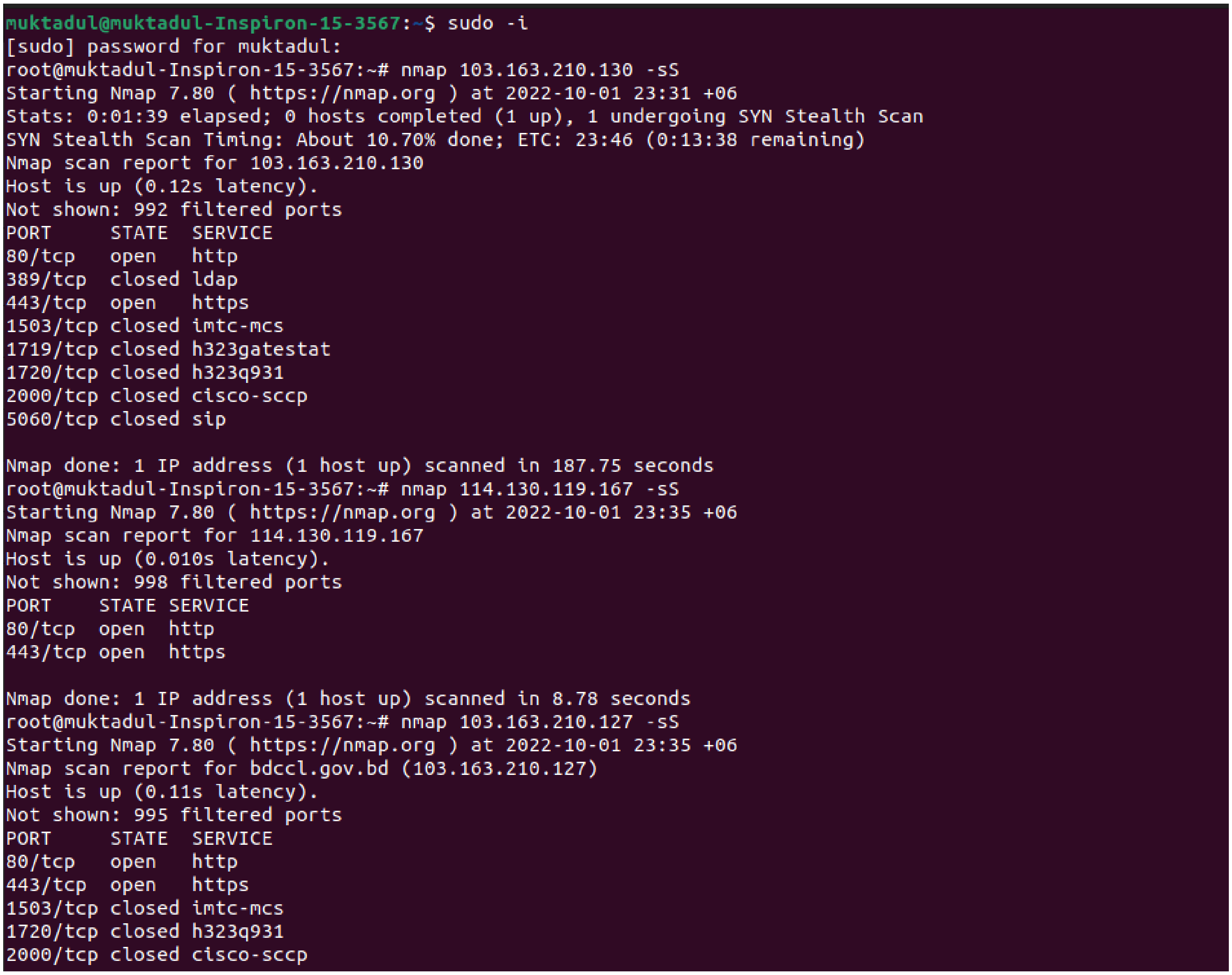
```
Nmap done: 1 IP address (1 host up) scanned in 7.63 seconds
muktadul@muktadul-Inspiron-15-3567:~$ nmap 103.163.210.117
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 22:57 +06
Nmap scan report for 103.163.210.117
Host is up (0.12s latency).
Not shown: 992 filtered ports
PORT      STATE  SERVICE
80/tcp    open   http
389/tcp   closed ldap
443/tcp   open   https
1503/tcp closed imtc-mcs
1719/tcp closed h323gatestat
1720/tcp closed h323q931
2000/tcp closed cisco-sccp
5060/tcp closed sip

Nmap done: 1 IP address (1 host up) scanned in 12.55 seconds
muktadul@muktadul-Inspiron-15-3567:~$ nmap 104.21.75.146
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 22:57 +06
Nmap scan report for 104.21.75.146
Host is up (0.059s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 5.48 seconds
```

Analysis:

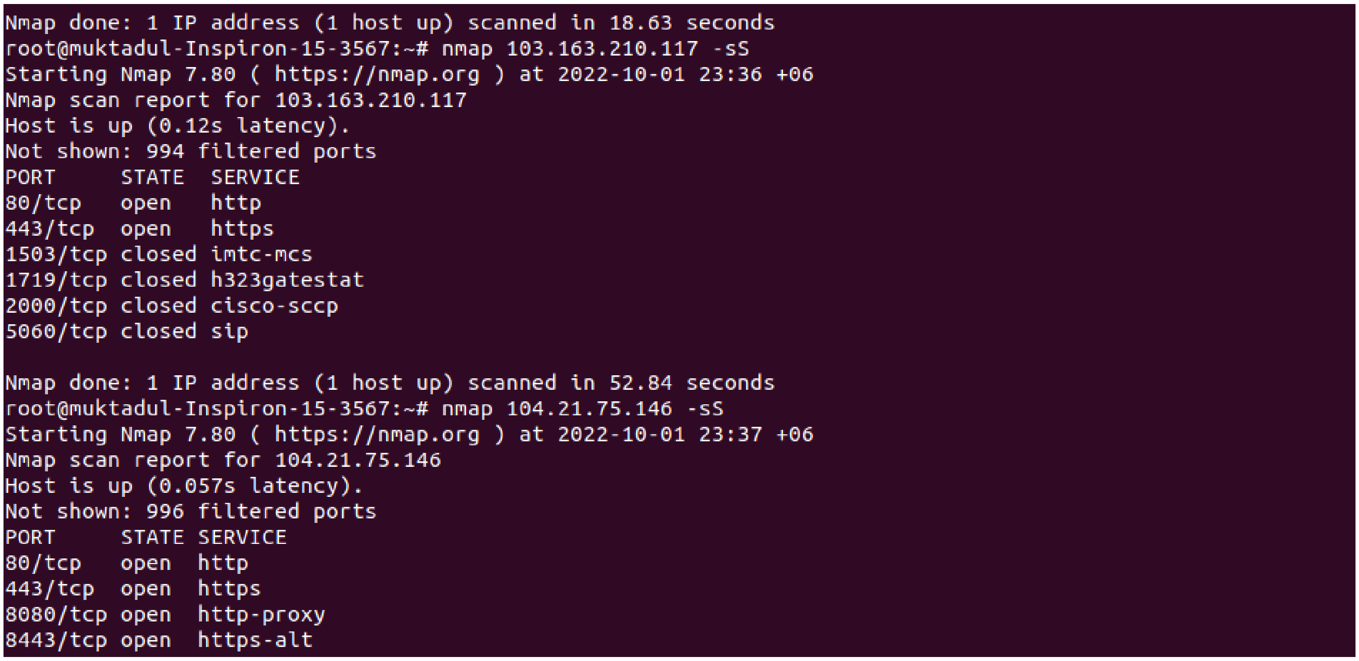
IP Address	Latency	Filtered Ports (Out of 1000)	Closed TCP Port (Out of 1000)	Open TCP Port (Out of 1000)
103.163.210.130	0.14 sec	992	6	2
114.130.119.167	0.01 sec	998	0	2
103.163.210.127	0.11 sec	992	6	2
103.163.210.117	0.12 sec	992	6	2
104.21.75.146	0.059 sec	996	0	4

Scan Techniques

1. Now we have to perform “nmap IP -sS” for TCP SYN port scan (Default).



```
muktadul@muktadul-Inspiron-15-3567:~$ sudo -i
[sudo] password for muktadul:
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.130 -sS
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 23:31 +06
Stats: 0:01:39 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 10.70% done; ETC: 23:46 (0:13:38 remaining)
Nmap scan report for 103.163.210.130
Host is up (0.12s latency).
Not shown: 992 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
389/tcp  closed ldap
443/tcp  open   https
1503/tcp closed imtc-mcs
1719/tcp closed h323gatestat
1720/tcp closed h323q931
2000/tcp closed cisco-sccp
5060/tcp closed sip

Nmap done: 1 IP address (1 host up) scanned in 187.75 seconds
root@muktadul-Inspiron-15-3567:~# nmap 114.130.119.167 -sS
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 23:35 +06
Nmap scan report for 114.130.119.167
Host is up (0.010s 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 8.78 seconds
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.127 -sS
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 23:35 +06
Nmap scan report for bdccl.gov.bd (103.163.210.127)
Host is up (0.11s latency).
Not shown: 995 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
1503/tcp closed imtc-mcs
1720/tcp closed h323q931
2000/tcp closed cisco-sccp
```

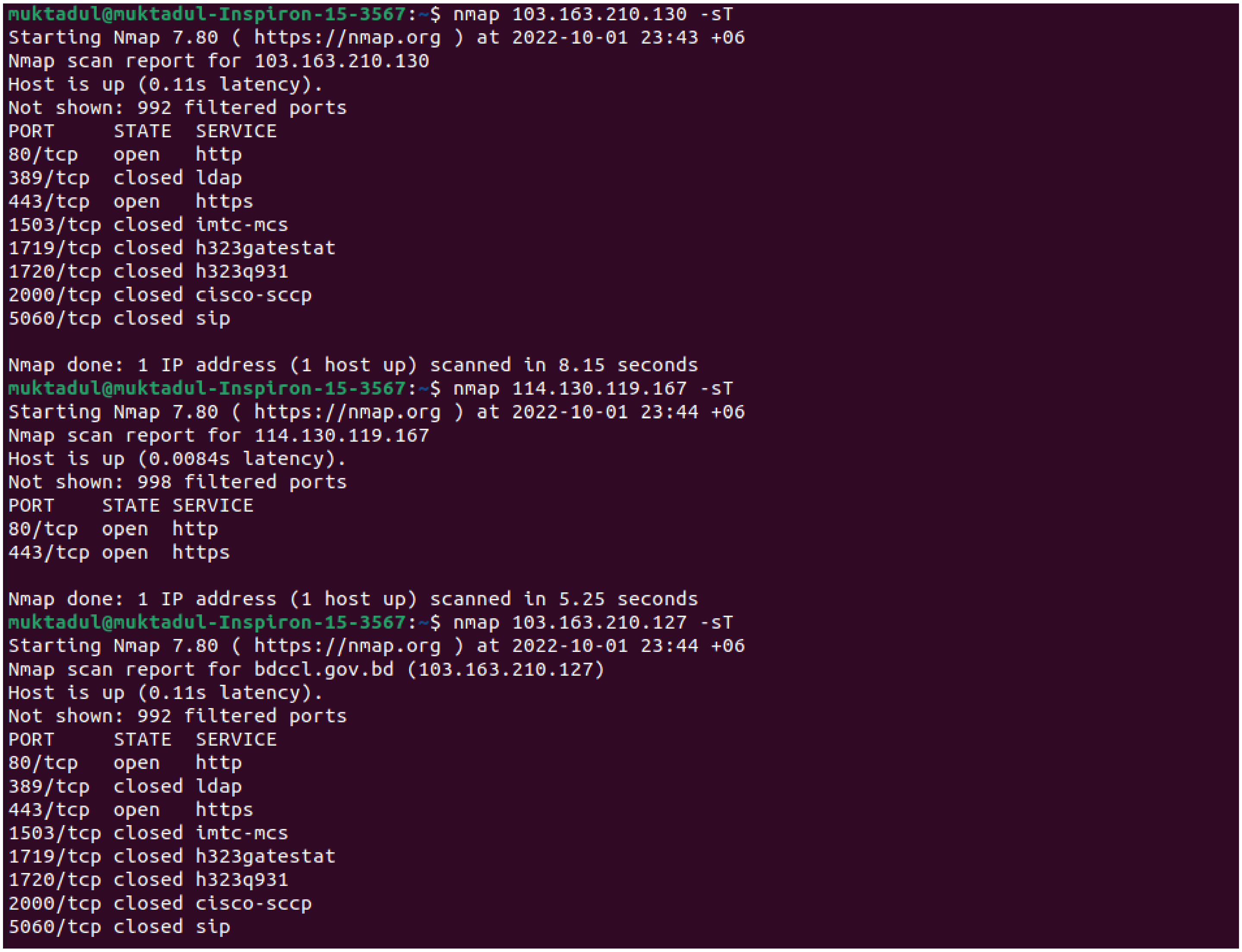


```
Nmap done: 1 IP address (1 host up) scanned in 18.63 seconds
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.117 -sS
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 23:36 +06
Nmap scan report for 103.163.210.117
Host is up (0.12s latency).
Not shown: 994 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
1503/tcp closed imtc-mcs
1719/tcp closed h323gatestat
2000/tcp closed cisco-sccp
5060/tcp closed sip

Nmap done: 1 IP address (1 host up) scanned in 52.84 seconds
root@muktadul-Inspiron-15-3567:~# nmap 104.21.75.146 -sS
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 23:37 +06
Nmap scan report for 104.21.75.146
Host is up (0.057s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt
```

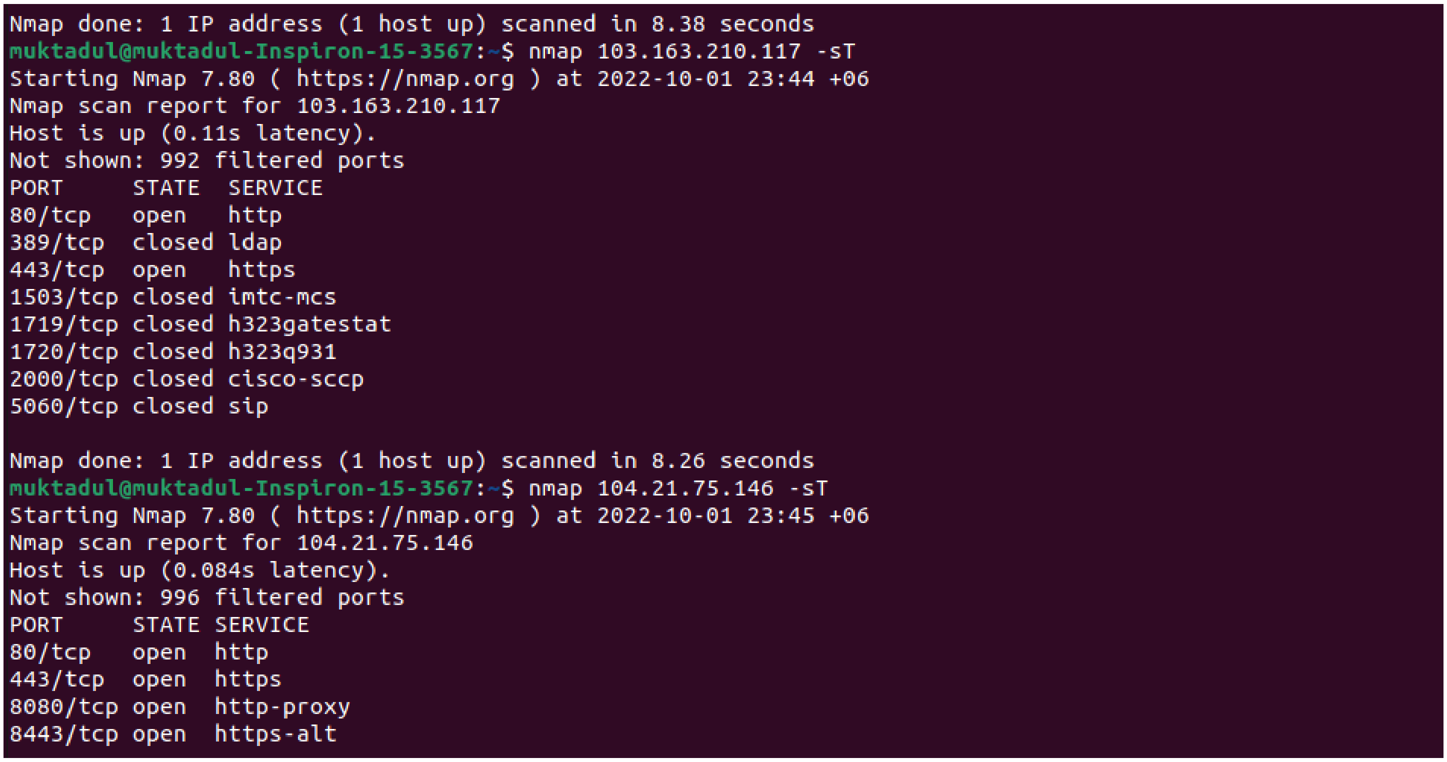
Analysis:

IP Address	Latency	Filtered Ports (Out of 1000)	Closed TCP SYN Port (Out of 1000)	Open TCP SYN Port (Out of 1000)
103.163.210.130	0.12 sec	992	6	2
114.130.119.167	0.01 sec	998	0	2
103.163.210.127	0.11 sec	995	3	2
103.163.210.117	0.12 sec	994	4	2
104.21.75.146	0.057 sec	996	0	4

2. **Now we have to perform “nmap IP -sT” for TCP SYN port scan (without root privilege):**



```
muktadul@muktadul-Inspiron-15-3567:~$ nmap 103.163.210.130 -sT
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 23:43 +06
Nmap scan report for 103.163.210.130
Host is up (0.11s latency).
Not shown: 992 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
389/tcp  closed ldap
443/tcp  open   https
1503/tcp closed imtc-mcs
1719/tcp closed h323gatestat
1720/tcp closed h323q931
2000/tcp closed cisco-sccp
5060/tcp closed sip

Nmap done: 1 IP address (1 host up) scanned in 8.15 seconds
muktadul@muktadul-Inspiron-15-3567:~$ nmap 114.130.119.167 -sT
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 23:44 +06
Nmap scan report for 114.130.119.167
Host is up (0.0084s 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 5.25 seconds
muktadul@muktadul-Inspiron-15-3567:~$ nmap 103.163.210.127 -sT
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 23:44 +06
Nmap scan report for bdccl.gov.bd (103.163.210.127)
Host is up (0.11s latency).
Not shown: 992 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
389/tcp  closed ldap
443/tcp  open   https
1503/tcp closed imtc-mcs
1719/tcp closed h323gatestat
1720/tcp closed h323q931
2000/tcp closed cisco-sccp
5060/tcp closed sip
```

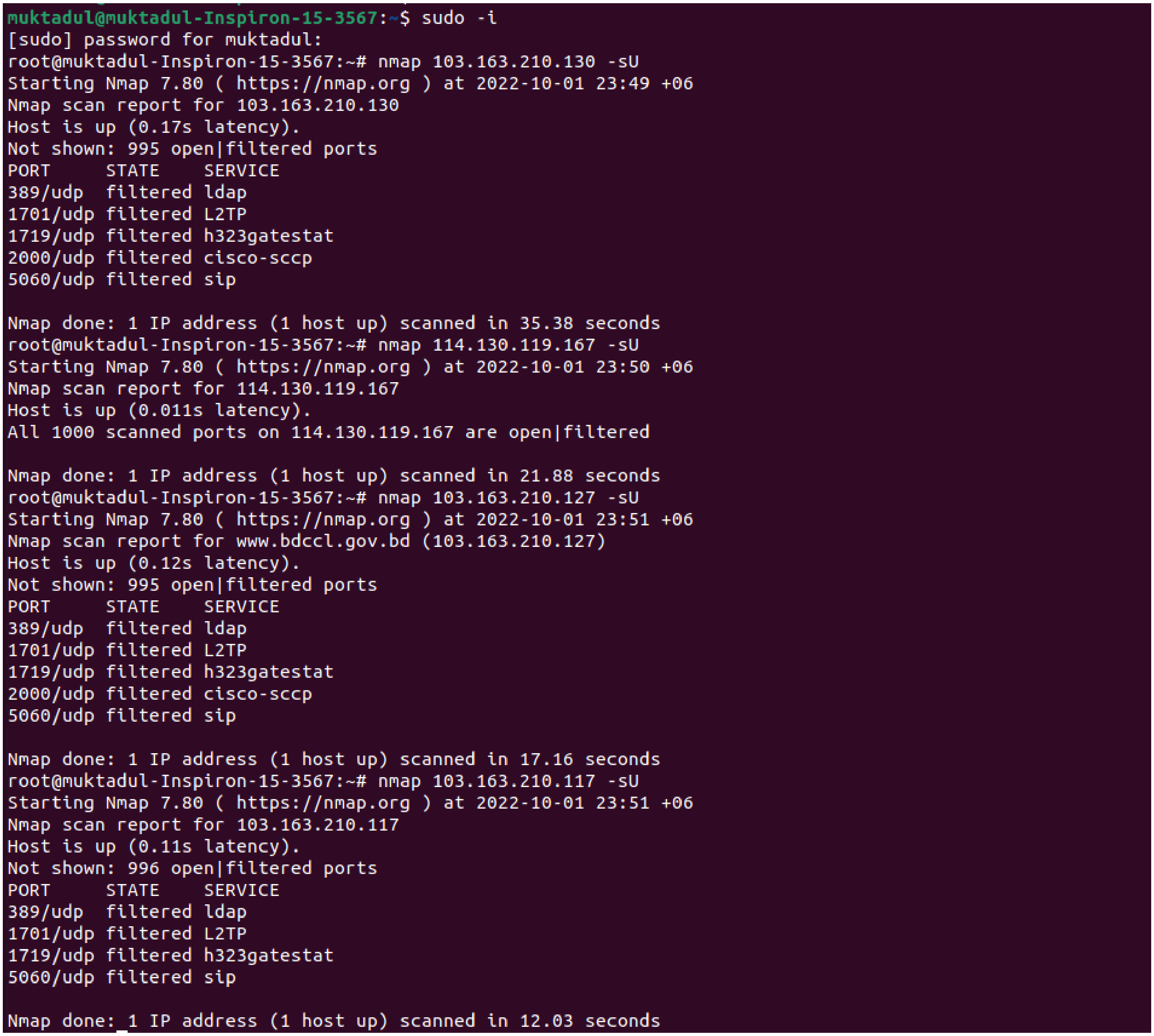


```
Nmap done: 1 IP address (1 host up) scanned in 8.38 seconds
muktadul@muktadul-Inspiron-15-3567:~$ nmap 103.163.210.117 -sT
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 23:44 +06
Nmap scan report for 103.163.210.117
Host is up (0.11s latency).
Not shown: 992 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
389/tcp  closed ldap
443/tcp  open   https
1503/tcp closed imtc-mcs
1719/tcp closed h323gatestat
1720/tcp closed h323q931
2000/tcp closed cisco-sccp
5060/tcp closed sip

Nmap done: 1 IP address (1 host up) scanned in 8.26 seconds
muktadul@muktadul-Inspiron-15-3567:~$ nmap 104.21.75.146 -sT
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 23:45 +06
Nmap scan report for 104.21.75.146
Host is up (0.084s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt
```

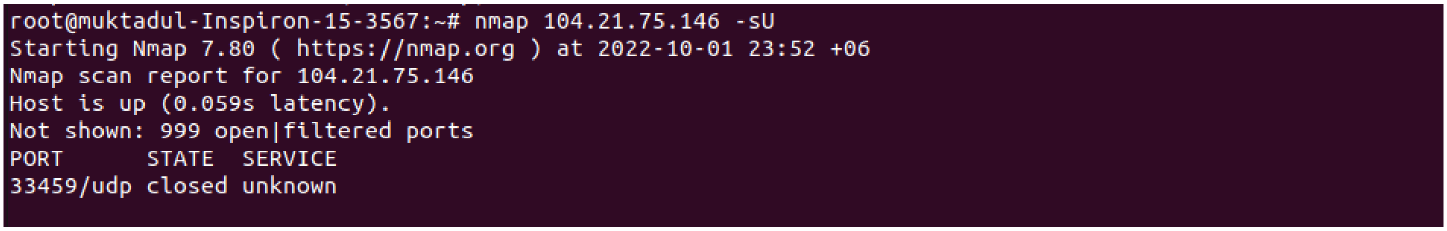
Analysis:

IP Address	Latency	Filtered Ports (Out of 1000)	Closed TCP SYN Port (Out of 1000)	Open TCP Port SYN (Out of 1000)
103.163.210.130	0.11 sec	992	6	2
114.130.119.167	0.0084 sec	998	0	2
103.163.210.127	0.11 sec	992	6	2
103.163.210.117	0.11 sec	992	6	2
104.21.75.146	0.084 sec	996	0	4

3. Now we have to perform “nmap IP -sU” for UDP port scan:



```
muktadul@muktadul-Inspiron-15-3567:~$ sudo -i
[sudo] password for muktadul:
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.130 -sU
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 23:49 +06
Nmap scan report for 103.163.210.130
Host is up (0.17s latency).
Not shown: 995 open|filtered ports
PORT     STATE    SERVICE
389/udp  filtered ldap
1701/udp filtered L2TP
1719/udp filtered h323gatestat
2000/udp filtered cisco-sccp
5060/udp filtered sip

Nmap done: 1 IP address (1 host up) scanned in 35.38 seconds
root@muktadul-Inspiron-15-3567:~# nmap 114.130.119.167 -sU
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 23:50 +06
Nmap scan report for 114.130.119.167
Host is up (0.011s latency).
All 1000 scanned ports on 114.130.119.167 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 21.88 seconds
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.127 -sU
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 23:51 +06
Nmap scan report for www.bdccl.gov.bd (103.163.210.127)
Host is up (0.12s latency).
Not shown: 995 open|filtered ports
PORT     STATE    SERVICE
389/udp  filtered ldap
1701/udp filtered L2TP
1719/udp filtered h323gatestat
2000/udp filtered cisco-sccp
5060/udp filtered sip

Nmap done: 1 IP address (1 host up) scanned in 17.16 seconds
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.117 -sU
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 23:51 +06
Nmap scan report for 103.163.210.117
Host is up (0.11s latency).
Not shown: 996 open|filtered ports
PORT     STATE    SERVICE
389/udp  filtered ldap
1701/udp filtered L2TP
1719/udp filtered h323gatestat
5060/udp filtered sip

Nmap done: 1 IP address (1 host up) scanned in 12.03 seconds
```

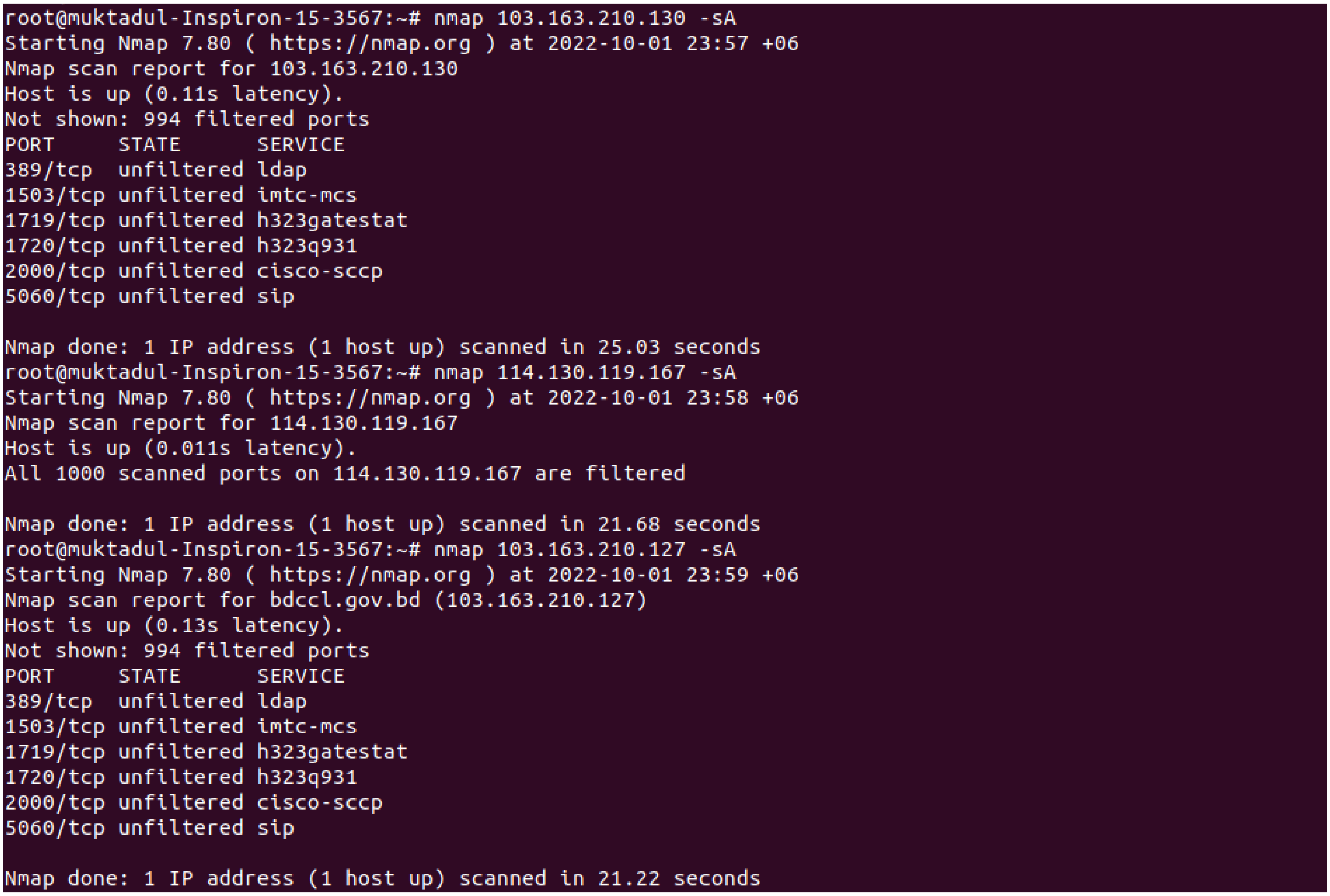


```
root@muktadul-Inspiron-15-3567:~# nmap 104.21.75.146 -sU
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 23:52 +06
Nmap scan report for 104.21.75.146
Host is up (0.059s latency).
Not shown: 999 open|filtered ports
PORT      STATE  SERVICE
33459/udp closed unknown
```

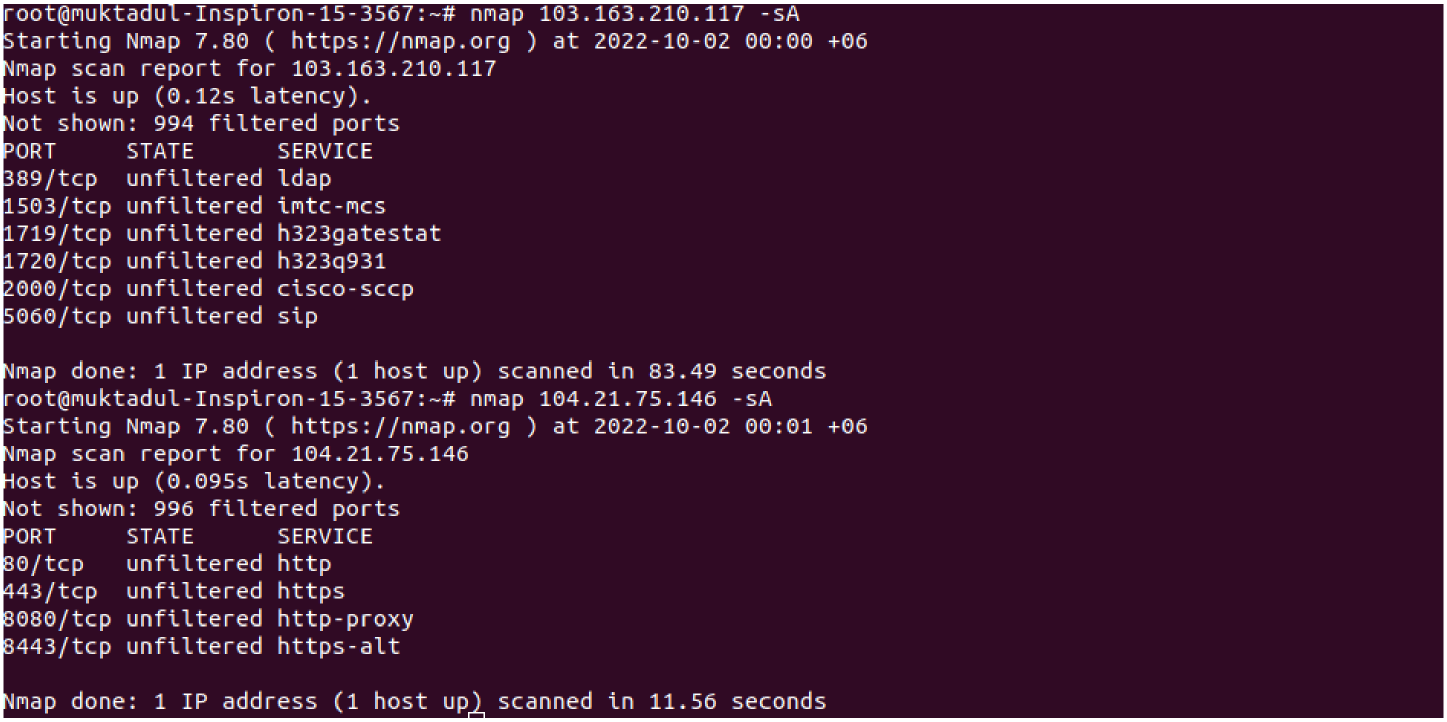
Analysis:

IP Address	Latency	Filtered UDP Ports (Out of 1000)	Closed UDP Ports (Out of 1000)
103.163.210.130	0.17 sec	5	0
114.130.119.167	0.011 sec	0	0
103.163.210.127	0.12 sec	5	0
103.163.210.117	0.11 sec	4	0
104.21.75.146	0.059 sec	0	1

4. Now we have to perform “nmap IP -sA” for TCP ACK port scan:



```
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.130 -sA
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 23:57 +06
Nmap scan report for 103.163.210.130
Host is up (0.11s latency).
Not shown: 994 filtered ports
PORT     STATE      SERVICE
389/tcp  unfiltered ldap
1503/tcp unfiltered imtc-mcs
1719/tcp unfiltered h323gatestat
1720/tcp unfiltered h323q931
2000/tcp unfiltered cisco-sccp
5060/tcp unfiltered sip

Nmap done: 1 IP address (1 host up) scanned in 25.03 seconds
root@muktadul-Inspiron-15-3567:~# nmap 114.130.119.167 -sA
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 23:58 +06
Nmap scan report for 114.130.119.167
Host is up (0.011s latency).
All 1000 scanned ports on 114.130.119.167 are filtered

Nmap done: 1 IP address (1 host up) scanned in 21.68 seconds
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.127 -sA
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 23:59 +06
Nmap scan report for bdccl.gov.bd (103.163.210.127)
Host is up (0.13s latency).
Not shown: 994 filtered ports
PORT     STATE      SERVICE
389/tcp  unfiltered ldap
1503/tcp unfiltered imtc-mcs
1719/tcp unfiltered h323gatestat
1720/tcp unfiltered h323q931
2000/tcp unfiltered cisco-sccp
5060/tcp unfiltered sip

Nmap done: 1 IP address (1 host up) scanned in 21.22 seconds
```



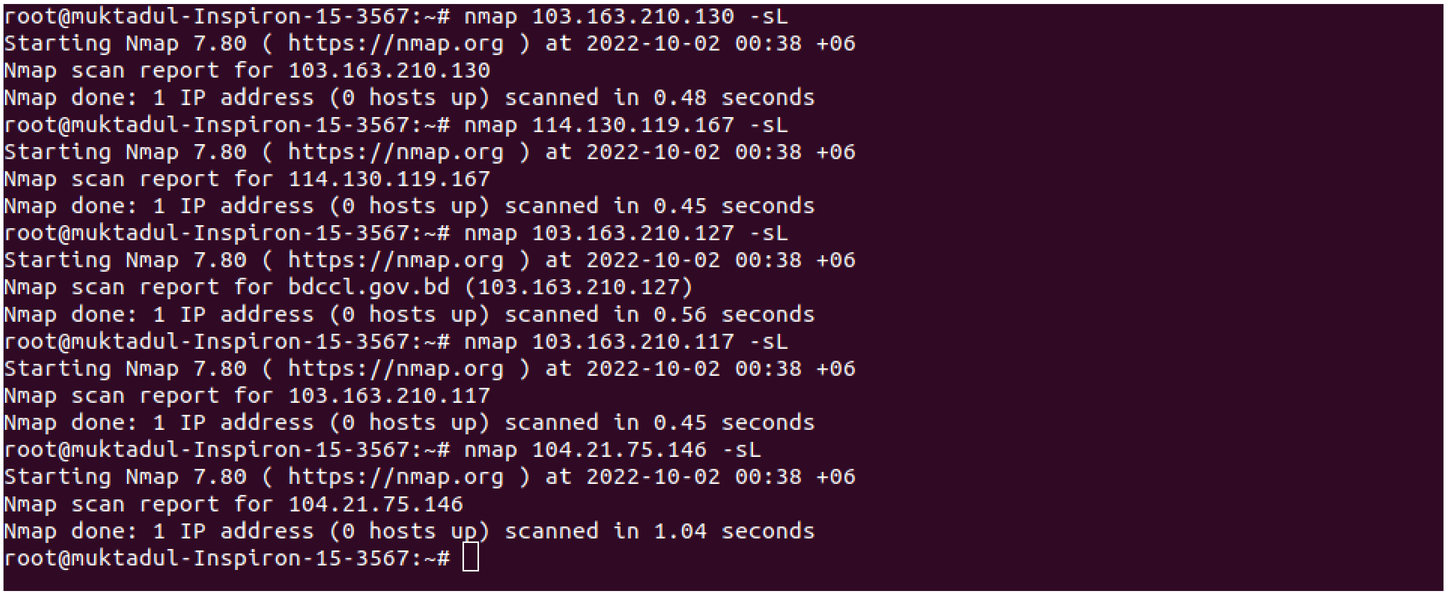
```
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.117 -sA
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 00:00 +06
Nmap scan report for 103.163.210.117
Host is up (0.12s latency).
Not shown: 994 filtered ports
PORT     STATE      SERVICE
389/tcp  unfiltered ldap
1503/tcp unfiltered imtc-mcs
1719/tcp unfiltered h323gatestat
1720/tcp unfiltered h323q931
2000/tcp unfiltered cisco-sccp
5060/tcp unfiltered sip

Nmap done: 1 IP address (1 host up) scanned in 83.49 seconds
root@muktadul-Inspiron-15-3567:~# nmap 104.21.75.146 -sA
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 00:01 +06
Nmap scan report for 104.21.75.146
Host is up (0.095s latency).
Not shown: 996 filtered ports
PORT     STATE      SERVICE
80/tcp   unfiltered http
443/tcp  unfiltered https
8080/tcp unfiltered http-proxy
8443/tcp unfiltered https-alt

Nmap done: 1 IP address (1 host up) scanned in 11.56 seconds
```

Analysis:

IP Address	Latency	Filtered TCP ACK Port (Out of 1000)
103.163.210.130	0.11 sec	6
114.130.119.167	0.011 sec	0
103.163.210.127	0.13 sec	6
103.163.210.117	0.12 sec	6
104.21.75.146	0.095 sec	4

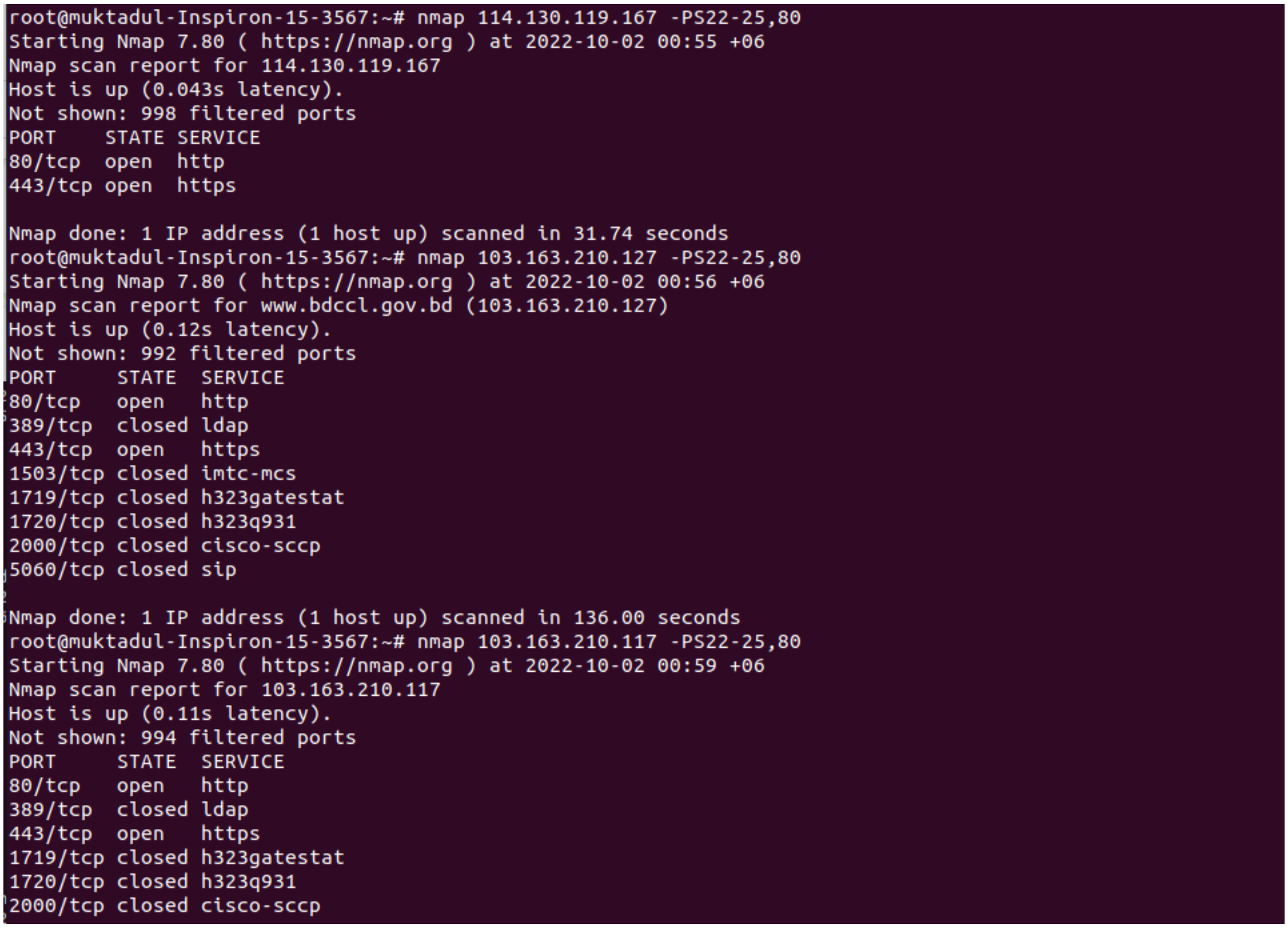
Host Discovery

1. Now we have to perform “nmap IP -sL” for No Scan. List targets only:

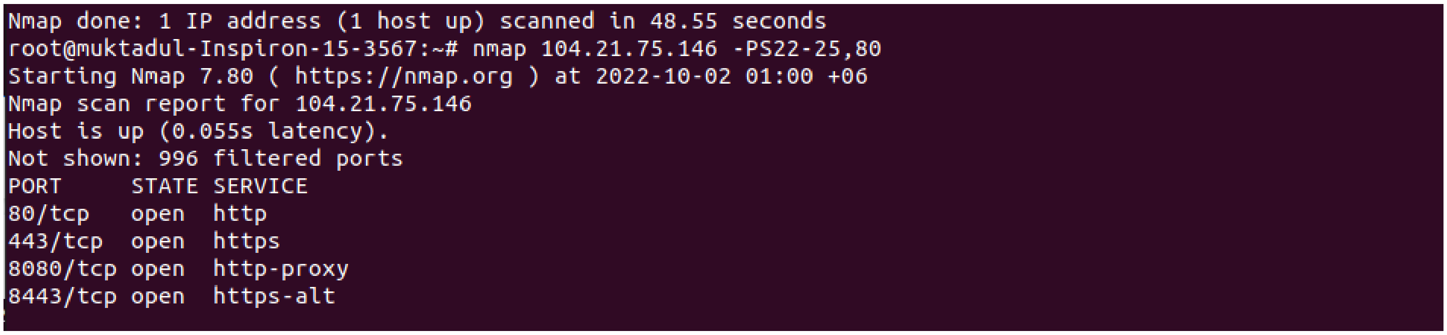


```
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.130 -sL
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 00:38 +06
Nmap scan report for 103.163.210.130
Nmap done: 1 IP address (0 hosts up) scanned in 0.48 seconds
root@muktadul-Inspiron-15-3567:~# nmap 114.130.119.167 -sL
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 00:38 +06
Nmap scan report for 114.130.119.167
Nmap done: 1 IP address (0 hosts up) scanned in 0.45 seconds
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.127 -sL
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 00:38 +06
Nmap scan report for bdccl.gov.bd (103.163.210.127)
Nmap done: 1 IP address (0 hosts up) scanned in 0.56 seconds
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.117 -sL
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 00:38 +06
Nmap scan report for 103.163.210.117
Nmap done: 1 IP address (0 hosts up) scanned in 0.45 seconds
root@muktadul-Inspiron-15-3567:~# nmap 104.21.75.146 -sL
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 00:38 +06
Nmap scan report for 104.21.75.146
Nmap done: 1 IP address (0 hosts up) scanned in 1.04 seconds
root@muktadul-Inspiron-15-3567:~# 
```

2. Now we have to perform “nmap IP -PS22-25,80” for TCP SYN discovery on port 22-25 and 80.

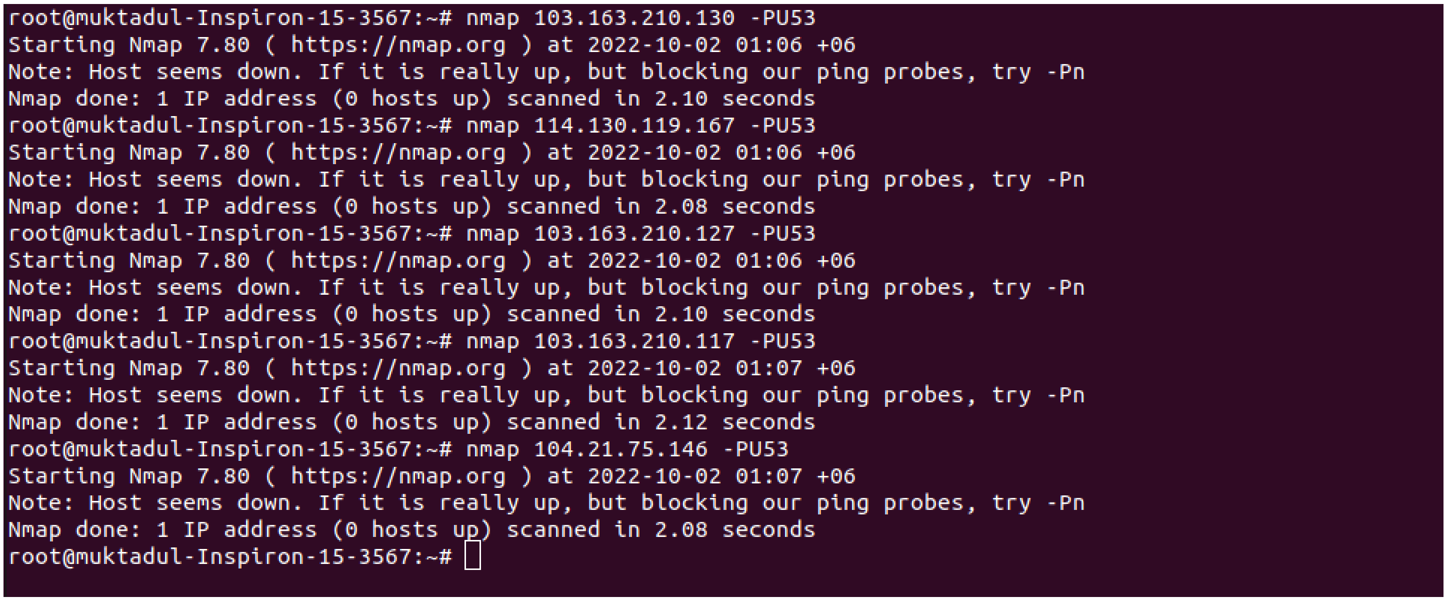


```
root@muktadul-Inspiron-15-3567:~# nmap 114.130.119.167 -PS22-25,80
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 00:55 +06
Nmap scan report for 114.130.119.167
Host is up (0.043s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 31.74 seconds
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.127 -PS22-25,80
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 00:56 +06
Nmap scan report for www.bdccl.gov.bd (103.163.210.127)
Host is up (0.12s latency).
Not shown: 992 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
389/tcp  closed ldap
443/tcp  open   https
1503/tcp closed imtc-mcs
1719/tcp closed h323gatestat
1720/tcp closed h323q931
2000/tcp closed cisco-sccp
5060/tcp closed sip

Nmap done: 1 IP address (1 host up) scanned in 136.00 seconds
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.117 -PS22-25,80
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 00:59 +06
Nmap scan report for 103.163.210.117
Host is up (0.11s latency).
Not shown: 994 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
389/tcp  closed ldap
443/tcp  open   https
1719/tcp closed h323gatestat
1720/tcp closed h323q931
2000/tcp closed cisco-sccp
```



```
Nmap done: 1 IP address (1 host up) scanned in 48.55 seconds
root@muktadul-Inspiron-15-3567:~# nmap 104.21.75.146 -PS22-25,80
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 01:00 +06
Nmap scan report for 104.21.75.146
Host is up (0.055s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt
```

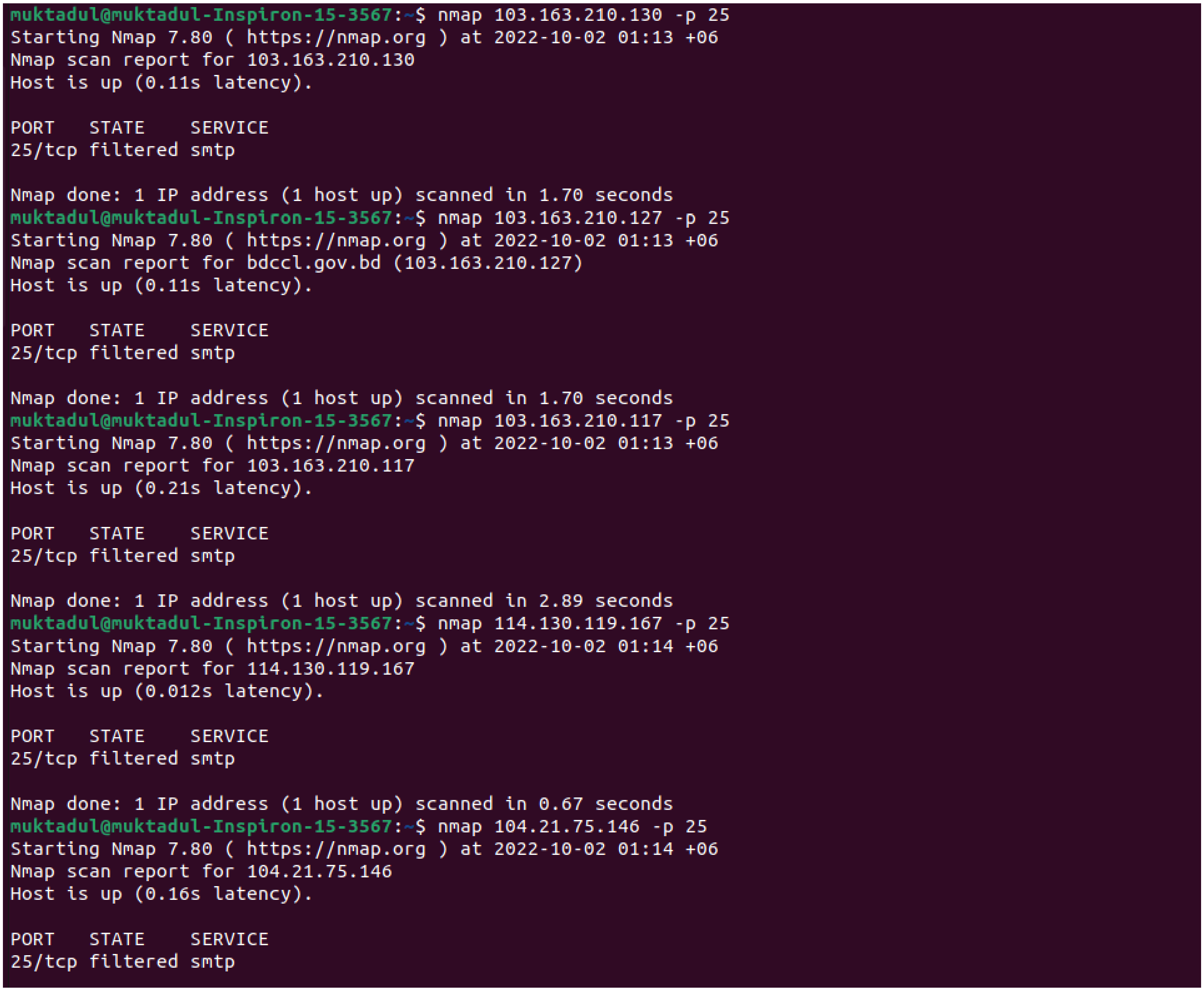
3. **Now we have to perform “nmap IP -PU53” for UDP discovery on port 53.**



```
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.130 -PU53
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 01:06 +06
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 2.10 seconds
root@muktadul-Inspiron-15-3567:~# nmap 114.130.119.167 -PU53
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 01:06 +06
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 2.08 seconds
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.127 -PU53
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 01:06 +06
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 2.10 seconds
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.117 -PU53
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 01:07 +06
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 2.12 seconds
root@muktadul-Inspiron-15-3567:~# nmap 104.21.75.146 -PU53
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 01:07 +06
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 2.08 seconds
root@muktadul-Inspiron-15-3567:~#
```

Port Specification

1. Now we have to perform “nmap IP -p x” for Port scan for port x:

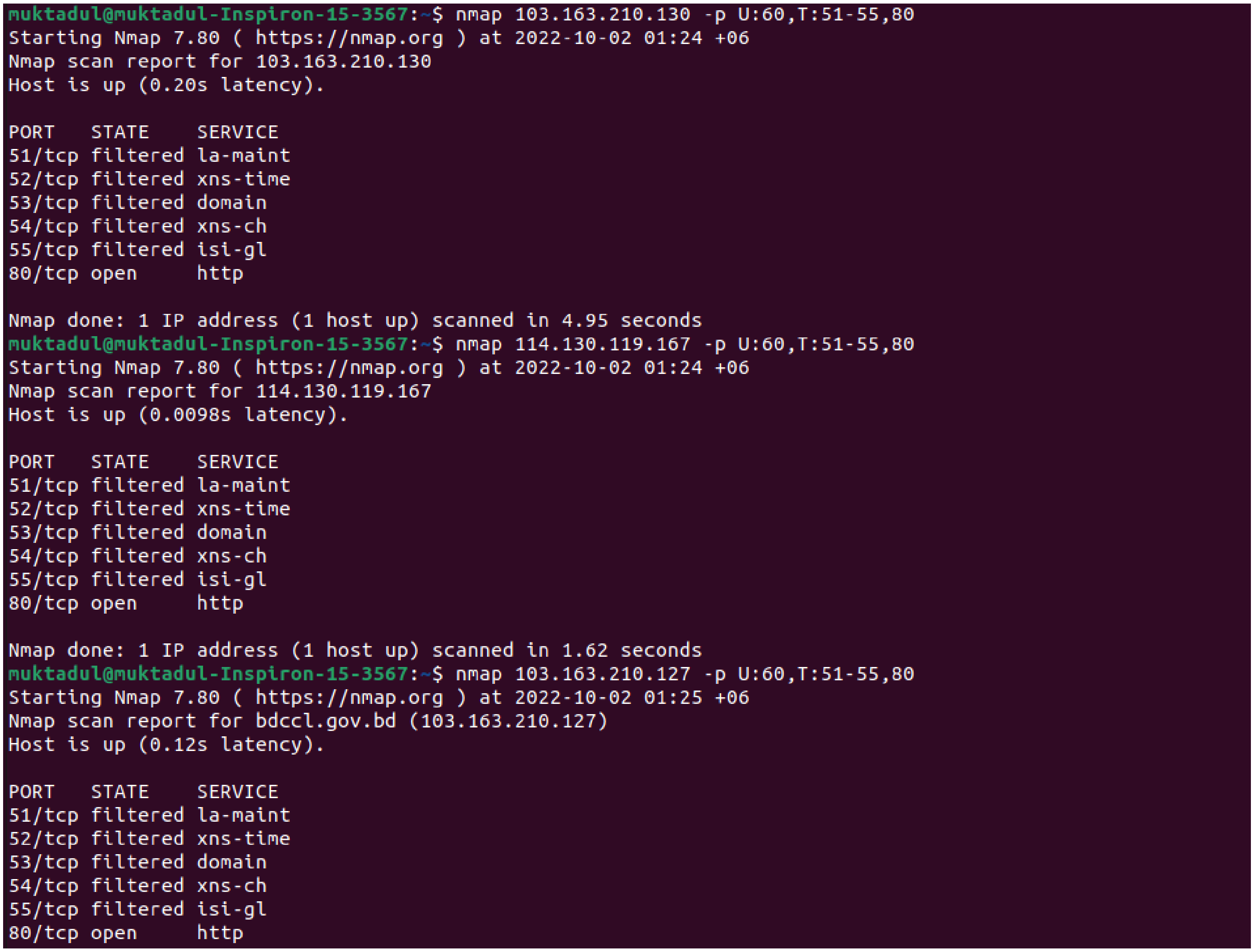


```
muktadul@muktadul-Inspiron-15-3567:~$ nmap 103.163.210.130 -p 25
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 01:13 +06
Nmap scan report for 103.163.210.130
Host is up (0.11s latency).

PORT   STATE    SERVICE
25/tcp filtered smtp

Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds
muktadul@muktadul-Inspiron-15-3567:~$ nmap 103.163.210.127 -p 25
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 01:13 +06
Nmap scan report for bdccl.gov.bd (103.163.210.127)
Host is up (0.11s latency).

PORT   STATE    SERVICE
25/tcp filtered smtp

Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds
muktadul@muktadul-Inspiron-15-3567:~$ nmap 103.163.210.117 -p 25
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 01:13 +06
Nmap scan report for 103.163.210.117
Host is up (0.21s latency).

PORT   STATE    SERVICE
25/tcp filtered smtp

Nmap done: 1 IP address (1 host up) scanned in 2.89 seconds
muktadul@muktadul-Inspiron-15-3567:~$ nmap 114.130.119.167 -p 25
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 01:14 +06
Nmap scan report for 114.130.119.167
Host is up (0.012s latency).

PORT   STATE    SERVICE
25/tcp filtered smtp

Nmap done: 1 IP address (1 host up) scanned in 0.67 seconds
muktadul@muktadul-Inspiron-15-3567:~$ nmap 104.21.75.146 -p 25
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 01:14 +06
Nmap scan report for 104.21.75.146
Host is up (0.16s latency).

PORT   STATE    SERVICE
25/tcp filtered smtp
```

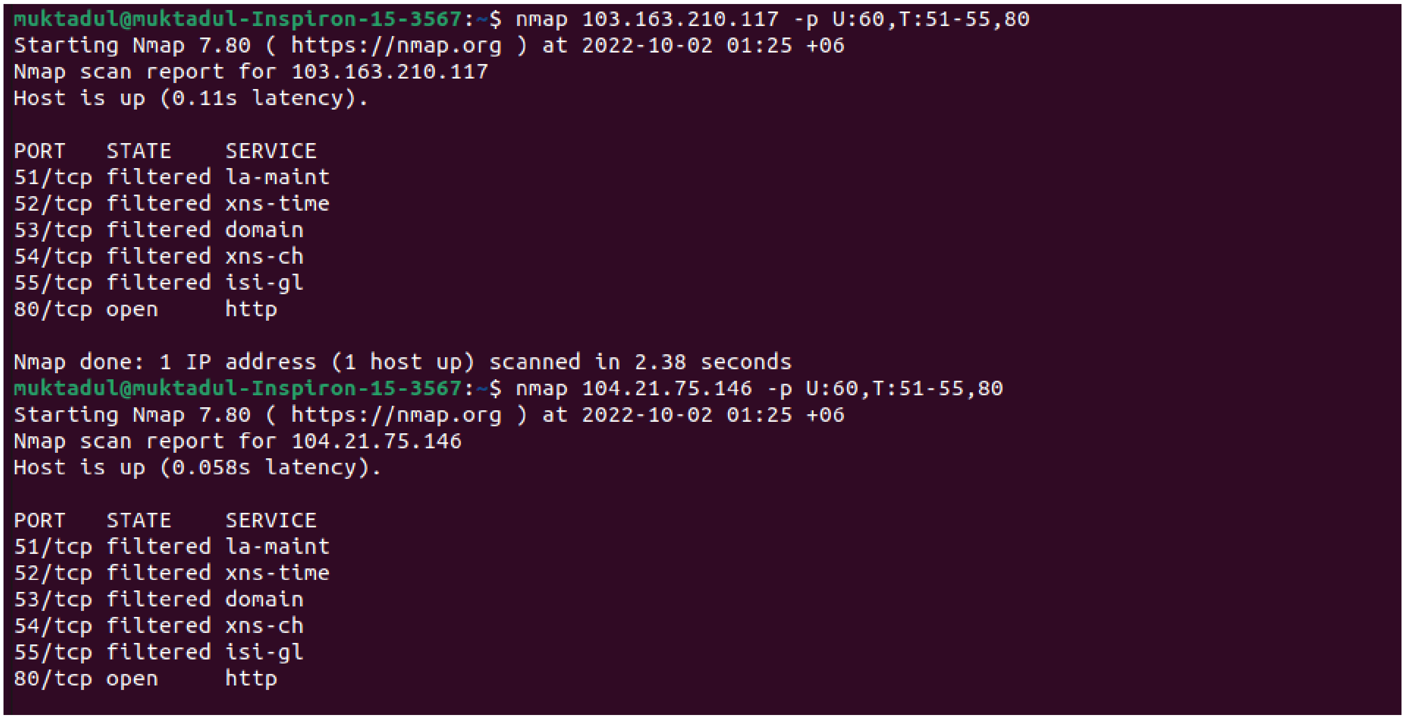
Analysis:

IP Address	Port	Service
103.163.210.130	25 / tcp	smtp
114.130.119.167	25 / tcp	smtp
103.163.210.127	25 / tcp	smtp
103.163.210.117	25 / tcp	smtp
104.21.75.146	25 / tcp	smtp

2. Now we have to perform “nmap IP -p U:60, T:51-55, 80” for Port scan multiple TCP and UDP ports



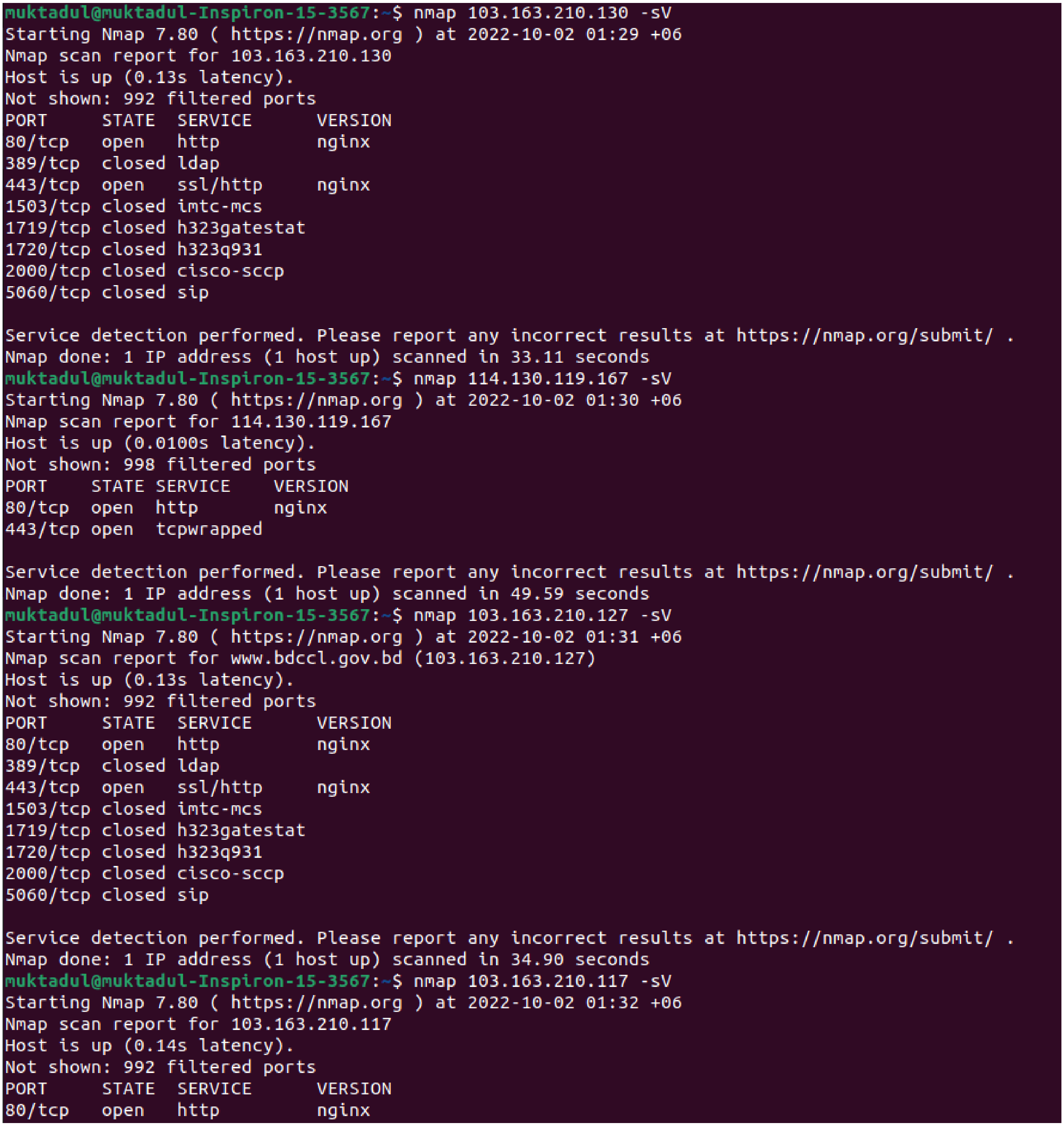
```
muktadul@muktadul-Inspiron-15-3567:~$ nmap 103.163.210.130 -p U:60,T:51-55,80
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 01:24 +06
Nmap scan report for 103.163.210.130
Host is up (0.20s latency).

PORT   STATE    SERVICE
51/tcp filtered la-maint
52/tcp filtered xns-time
53/tcp filtered domain
54/tcp filtered xns-ch
55/tcp filtered isi-gl
80/tcp open     http

Nmap done: 1 IP address (1 host up) scanned in 4.95 seconds
muktadul@muktadul-Inspiron-15-3567:~$ nmap 114.130.119.167 -p U:60,T:51-55,80
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 01:24 +06
Nmap scan report for 114.130.119.167
Host is up (0.0098s latency).

PORT   STATE    SERVICE
51/tcp filtered la-maint
52/tcp filtered xns-time
53/tcp filtered domain
54/tcp filtered xns-ch
55/tcp filtered isi-gl
80/tcp open     http

Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds
muktadul@muktadul-Inspiron-15-3567:~$ nmap 103.163.210.127 -p U:60,T:51-55,80
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 01:25 +06
Nmap scan report for bdccl.gov.bd (103.163.210.127)
Host is up (0.12s latency).

PORT   STATE    SERVICE
51/tcp filtered la-maint
52/tcp filtered xns-time
53/tcp filtered domain
54/tcp filtered xns-ch
55/tcp filtered isi-gl
80/tcp open     http
```



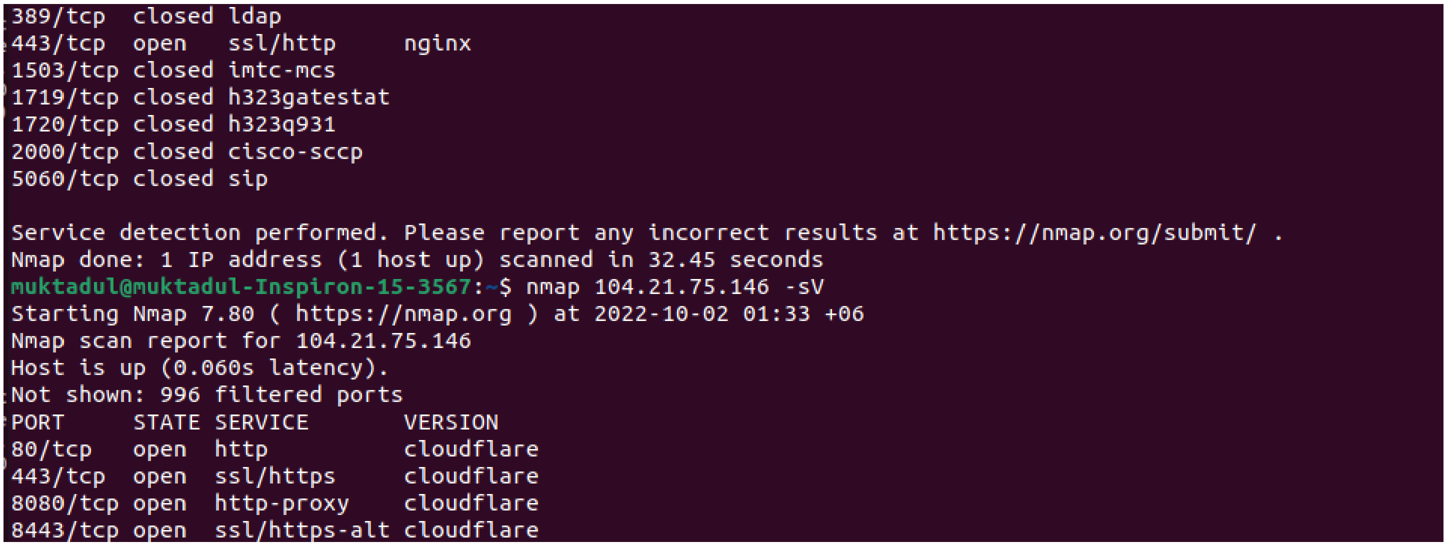
```
muktadul@muktadul-Inspiron-15-3567:~$ nmap 103.163.210.117 -p U:60,T:51-55,80
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 01:25 +06
Nmap scan report for 103.163.210.117
Host is up (0.11s latency).

PORT   STATE    SERVICE
51/tcp filtered la-maint
52/tcp filtered xns-time
53/tcp filtered domain
54/tcp filtered xns-ch
55/tcp filtered isi-gl
80/tcp open     http

Nmap done: 1 IP address (1 host up) scanned in 2.38 seconds
muktadul@muktadul-Inspiron-15-3567:~$ nmap 104.21.75.146 -p U:60,T:51-55,80
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 01:25 +06
Nmap scan report for 104.21.75.146
Host is up (0.058s latency).

PORT   STATE    SERVICE
51/tcp filtered la-maint
52/tcp filtered xns-time
53/tcp filtered domain
54/tcp filtered xns-ch
55/tcp filtered isi-gl
80/tcp open     http
```

Service and Version Detection

1. **Now we have to perform “nmap IP -sV” for Attempts to determine the version of the service running on port.**



```
muktadul@muktadul-Inspiron-15-3567:~$ nmap 103.163.210.130 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 01:29 +06
Nmap scan report for 103.163.210.130
Host is up (0.13s latency).
Not shown: 992 filtered ports
PORT     STATE  SERVICE      VERSION
80/tcp   open   http         nginx
389/tcp  closed ldap
443/tcp  open   ssl/http     nginx
1503/tcp closed imtc-mcs
1719/tcp closed h323gatestat
1720/tcp closed h323q931
2000/tcp closed cisco-sccp
5060/tcp closed sip

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.11 seconds
muktadul@muktadul-Inspiron-15-3567:~$ nmap 114.130.119.167 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 01:30 +06
Nmap scan report for 114.130.119.167
Host is up (0.0100s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE    VERSION
80/tcp  open  http       nginx
443/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.59 seconds
muktadul@muktadul-Inspiron-15-3567:~$ nmap 103.163.210.127 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 01:31 +06
Nmap scan report for www.bdccl.gov.bd (103.163.210.127)
Host is up (0.13s latency).
Not shown: 992 filtered ports
PORT     STATE  SERVICE      VERSION
80/tcp   open   http         nginx
389/tcp  closed ldap
443/tcp  open   ssl/http     nginx
1503/tcp closed imtc-mcs
1719/tcp closed h323gatestat
1720/tcp closed h323q931
2000/tcp closed cisco-sccp
5060/tcp closed sip

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.90 seconds
muktadul@muktadul-Inspiron-15-3567:~$ nmap 103.163.210.117 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 01:32 +06
Nmap scan report for 103.163.210.117
Host is up (0.14s latency).
Not shown: 992 filtered ports
PORT     STATE  SERVICE      VERSION
80/tcp   open   http         nginx
```



```
389/tcp  closed ldap
443/tcp  open   ssl/http     nginx
1503/tcp closed imtc-mcs
1719/tcp closed h323gatestat
1720/tcp closed h323q931
2000/tcp closed cisco-sccp
5060/tcp closed sip

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.45 seconds
muktadul@muktadul-Inspiron-15-3567:~$ nmap 104.21.75.146 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 01:33 +06
Nmap scan report for 104.21.75.146
Host is up (0.060s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          cloudflare
443/tcp  open  ssl/https     cloudflare
8080/tcp open  http-proxy    cloudflare
8443/tcp open  ssl/https-alt cloudflare
```

Analysis:

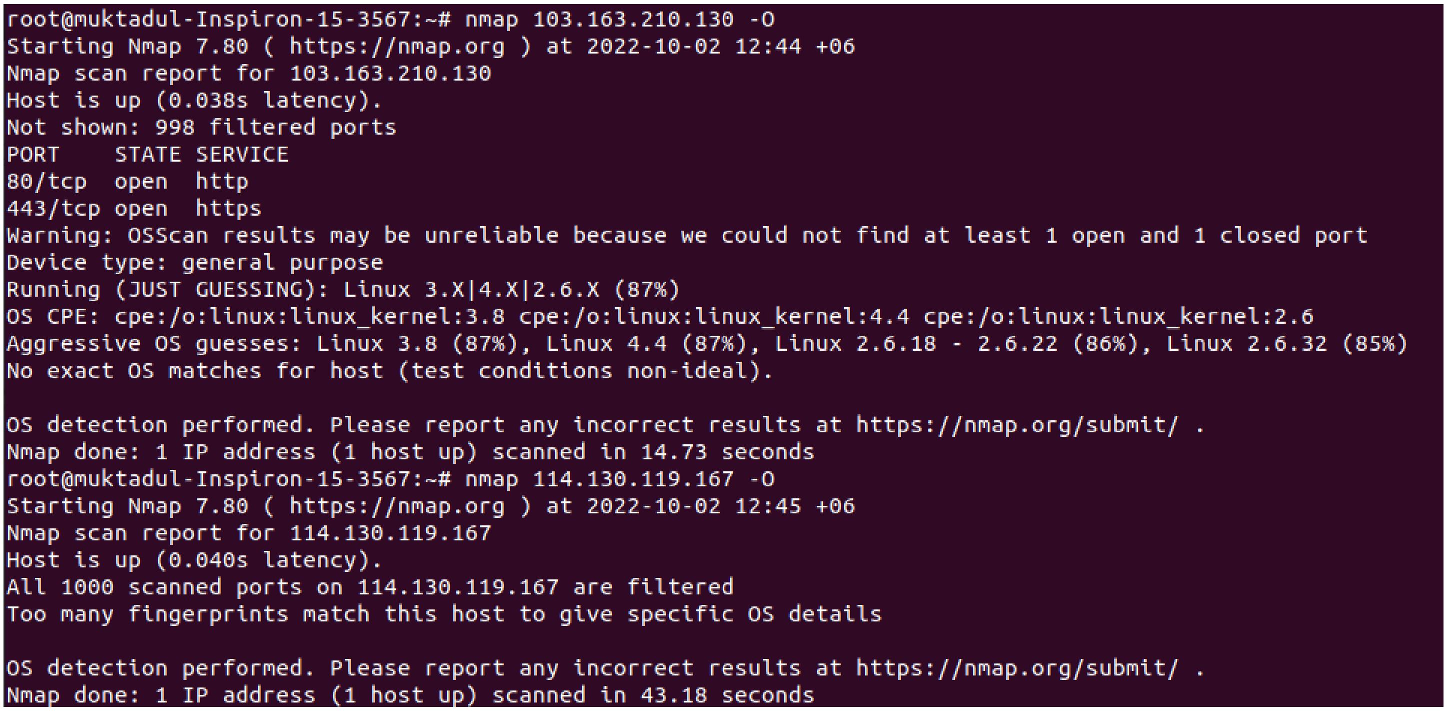
IP Address	Port	Service	Version
103.163.210.130	80 / tcp	http	nginx
	443 / tcp	ssl / http	nginx
114.130.119.167	80 / tcp	http	nginx
103.163.210.127	80 / tcp	http	nginx
	443 / tcp	ssl / http	nginx
103.163.210.117	80 / tcp	http	nginx
	443 / tcp	ssl / http	nginx
104.21.75.146	80 / tcp	http	cloudflare
	443 / tcp	ssl/https	cloudflare
	8080 / tcp	http-proxy	cloudflare
	8443 / tcp	ssl/https-alt	cloudflare

2. **Now we have to perform “nmap IP -sV --version-intensity 8” for Intensity level 8.**

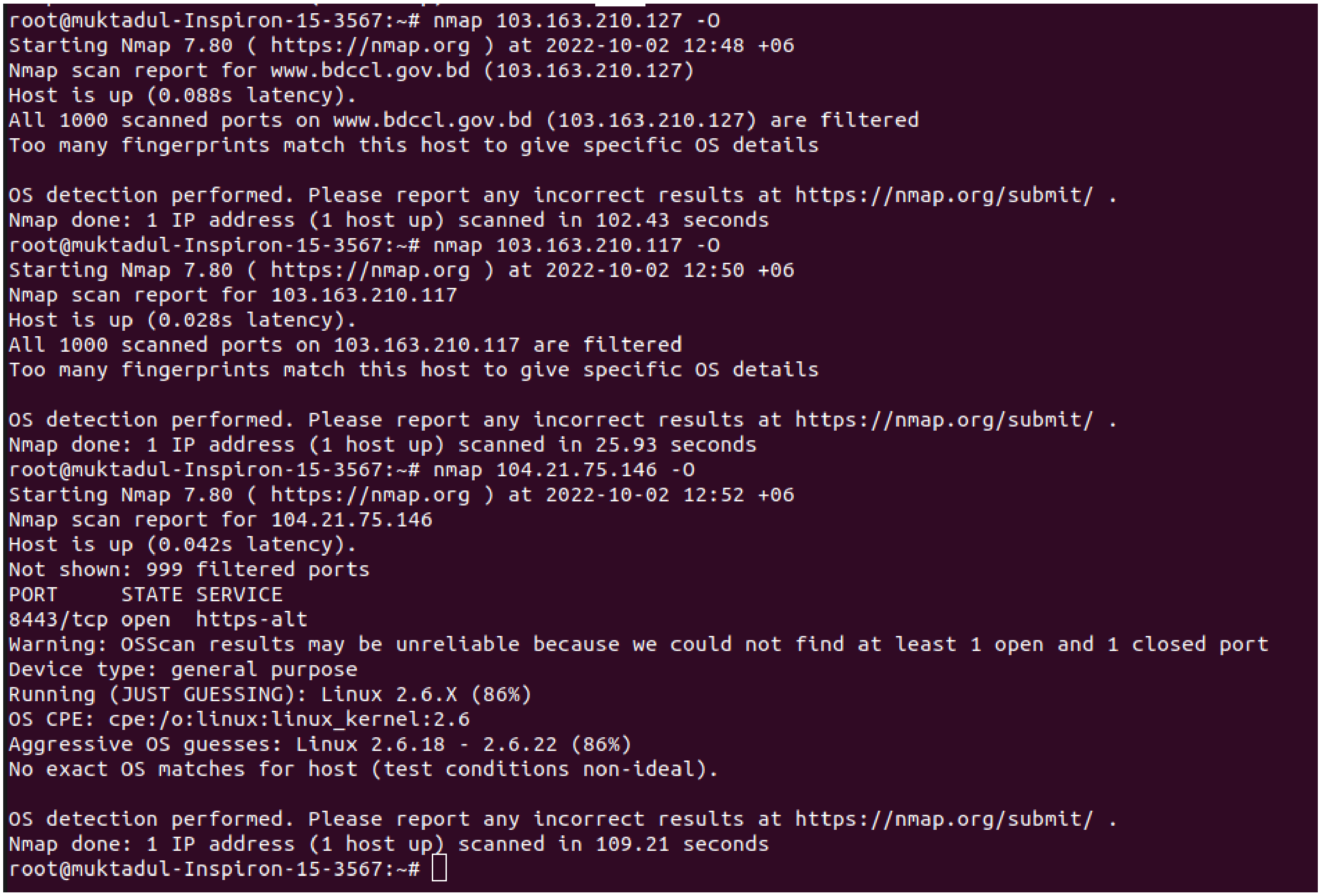
```
muktadul@muktadul-Inspiron-15-3567:~$ nmap 103.163.210.130 -sV-- version-intensity 8
Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
           <Lua scripts> is a comma-separated list of script-files or
           script-categories.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
Scantype - not supported
```

OS Detection

1. **Now we have to perform “nmap IP -O” for remote OS detection.**

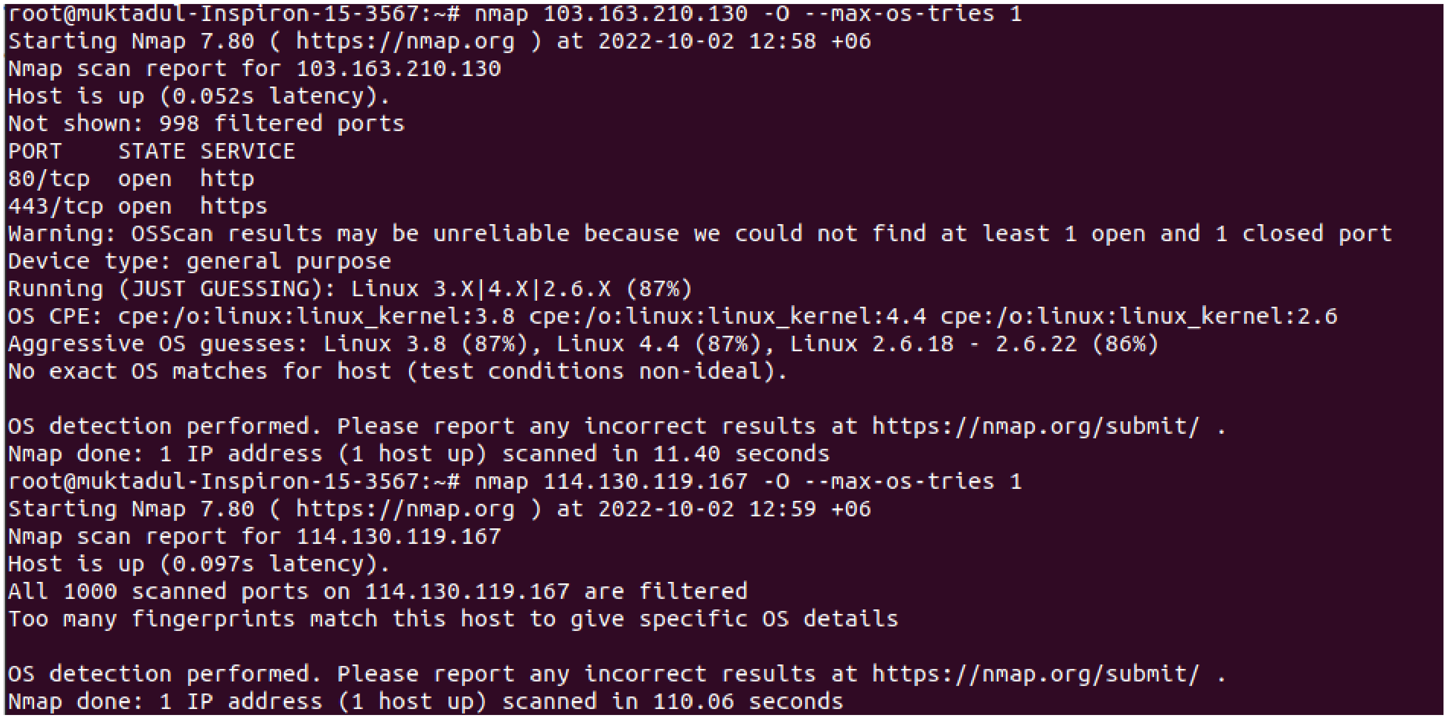


```
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.130 -O
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 12:44 +06
Nmap scan report for 103.163.210.130
Host is up (0.038s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X (87%)
OS CPE: cpe:/o:linux:linux_kernel:3.8 cpe:/o:linux:linux_kernel:4.4 cpe:/o:linux:linux_kernel:2.6
Aggressive OS guesses: Linux 3.8 (87%), Linux 4.4 (87%), Linux 2.6.18 - 2.6.22 (86%), Linux 2.6.32 (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.73 seconds
root@muktadul-Inspiron-15-3567:~# nmap 114.130.119.167 -O
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 12:45 +06
Nmap scan report for 114.130.119.167
Host is up (0.040s latency).
All 1000 scanned ports on 114.130.119.167 are filtered
Too many fingerprints match this host to give specific OS details

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.18 seconds
```

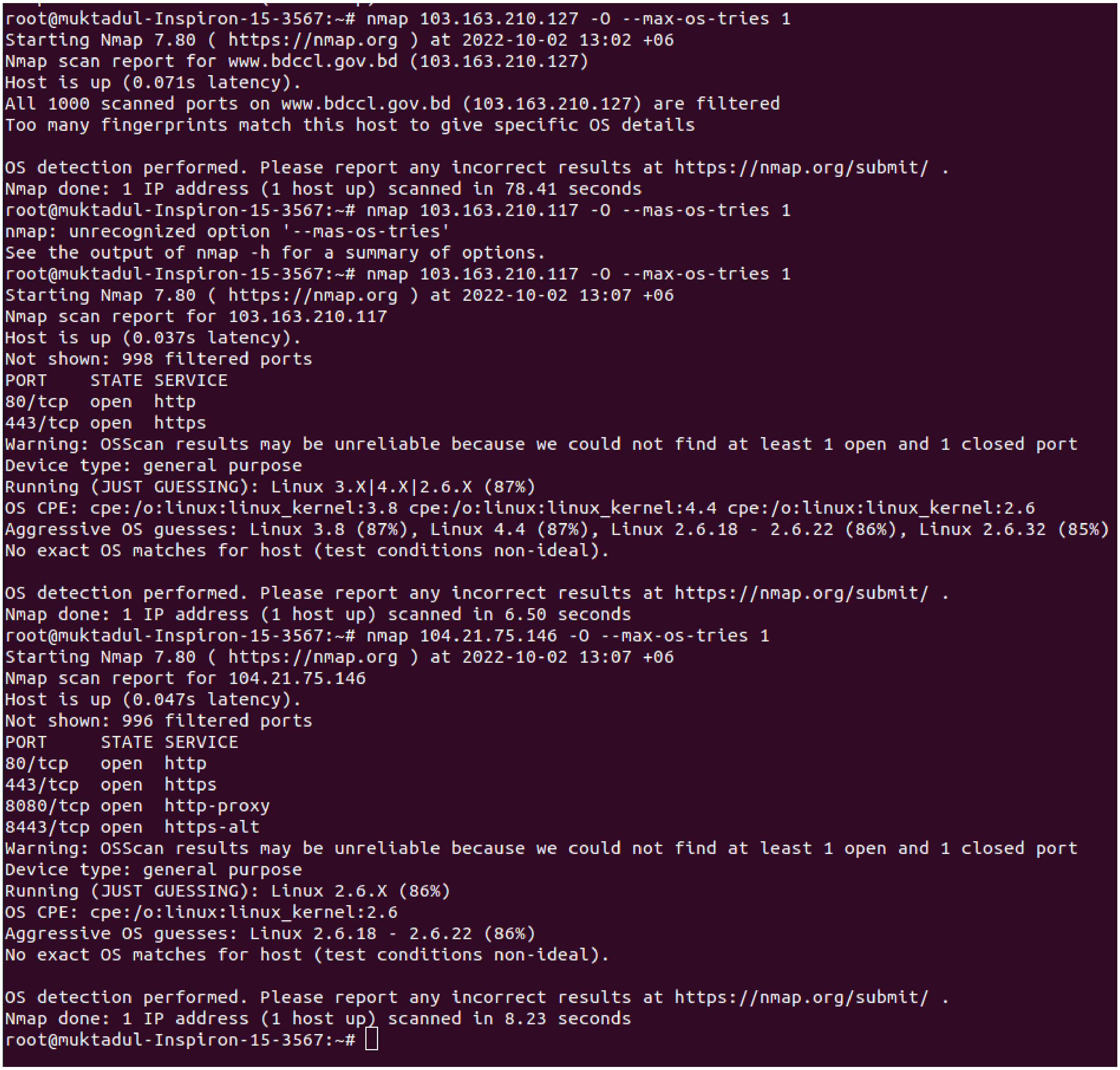


```
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.127 -O
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 12:48 +06
Nmap scan report for www.bdccl.gov.bd (103.163.210.127)
Host is up (0.088s latency).
All 1000 scanned ports on www.bdccl.gov.bd (103.163.210.127) are filtered
Too many fingerprints match this host to give specific OS details

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 102.43 seconds
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.117 -O
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 12:50 +06
Nmap scan report for 103.163.210.117
Host is up (0.028s latency).
All 1000 scanned ports on 103.163.210.117 are filtered
Too many fingerprints match this host to give specific OS details

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.93 seconds
root@muktadul-Inspiron-15-3567:~# nmap 104.21.75.146 -O
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 12:52 +06
Nmap scan report for 104.21.75.146
Host is up (0.042s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
8443/tcp open  https-alt
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 2.6.X (86%)
OS CPE: cpe:/o:linux:linux_kernel:2.6
Aggressive OS guesses: Linux 2.6.18 - 2.6.22 (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 109.21 seconds
root@muktadul-Inspiron-15-3567:~# 
```

2. **Now we have to perform “nmap IP -O --max-os-tries x” for the maximum number x of OS detection tries against a target.**



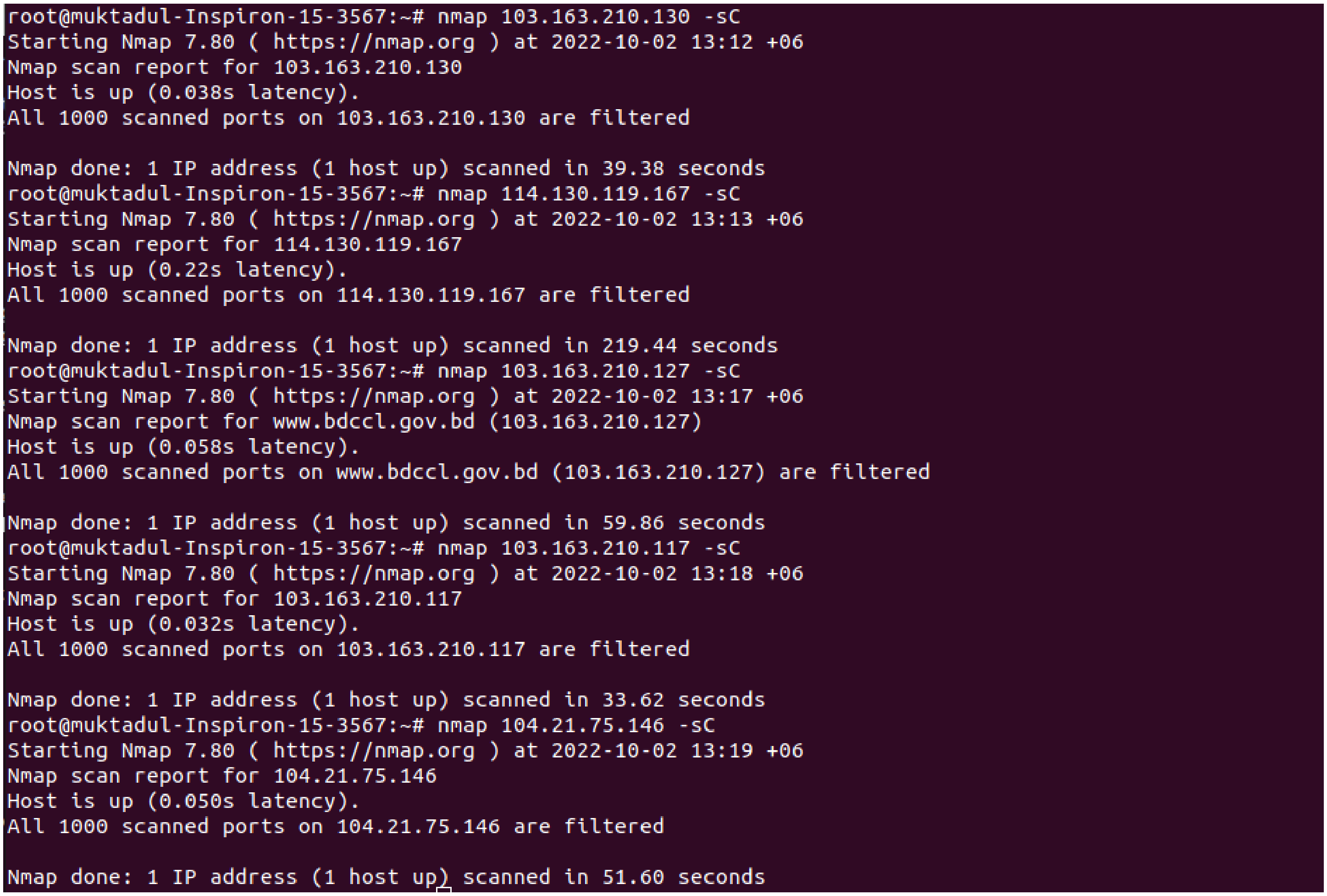
```
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.130 -O --max-os-tries 1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 12:58 +06
Nmap scan report for 103.163.210.130
Host is up (0.052s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X (87%)
OS CPE: cpe:/o:linux:linux_kernel:3.8 cpe:/o:linux:linux_kernel:4.4 cpe:/o:linux:linux_kernel:2.6
Aggressive OS guesses: Linux 3.8 (87%), Linux 4.4 (87%), Linux 2.6.18 - 2.6.22 (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.40 seconds
root@muktadul-Inspiron-15-3567:~# nmap 114.130.119.167 -O --max-os-tries 1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 12:59 +06
Nmap scan report for 114.130.119.167
Host is up (0.097s latency).
All 1000 scanned ports on 114.130.119.167 are filtered
Too many fingerprints match this host to give specific OS details

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 110.06 seconds
```



```
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.127 -O --max-os-tries 1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 13:02 +06
Nmap scan report for www.bdccl.gov.bd (103.163.210.127)
Host is up (0.071s latency).
All 1000 scanned ports on www.bdccl.gov.bd (103.163.210.127) are filtered
Too many fingerprints match this host to give specific OS details

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 78.41 seconds
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.117 -O --mas-os-tries 1
nmap: unrecognized option '--mas-os-tries'
See the output of nmap -h for a summary of options.
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.117 -O --max-os-tries 1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 13:07 +06
Nmap scan report for 103.163.210.117
Host is up (0.037s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
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 (JUST GUESSING): Linux 3.X|4.X|2.6.X (87%)
OS CPE: cpe:/o:linux:linux_kernel:3.8 cpe:/o:linux:linux_kernel:4.4 cpe:/o:linux:linux_kernel:2.6
Aggressive OS guesses: Linux 3.8 (87%), Linux 4.4 (87%), Linux 2.6.18 - 2.6.22 (86%), Linux 2.6.32 (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.50 seconds
root@muktadul-Inspiron-15-3567:~# nmap 104.21.75.146 -O --max-os-tries 1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 13:07 +06
Nmap scan report for 104.21.75.146
Host is up (0.047s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 2.6.X (86%)
OS CPE: cpe:/o:linux:linux_kernel:2.6
Aggressive OS guesses: Linux 2.6.18 - 2.6.22 (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.23 seconds
root@muktadul-Inspiron-15-3567:~# 
```

NSE Scripts

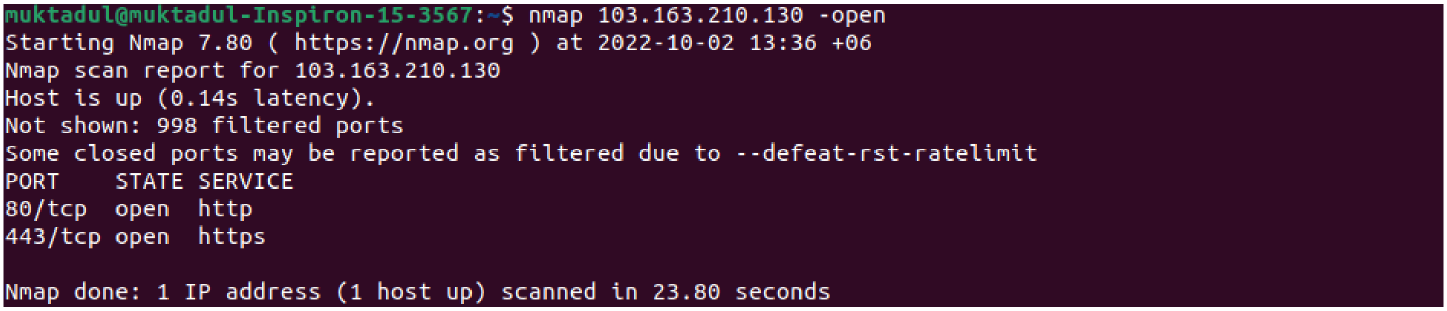
1. Now we have to perform “nmap IP -sC” for scan with default NSE scripts.



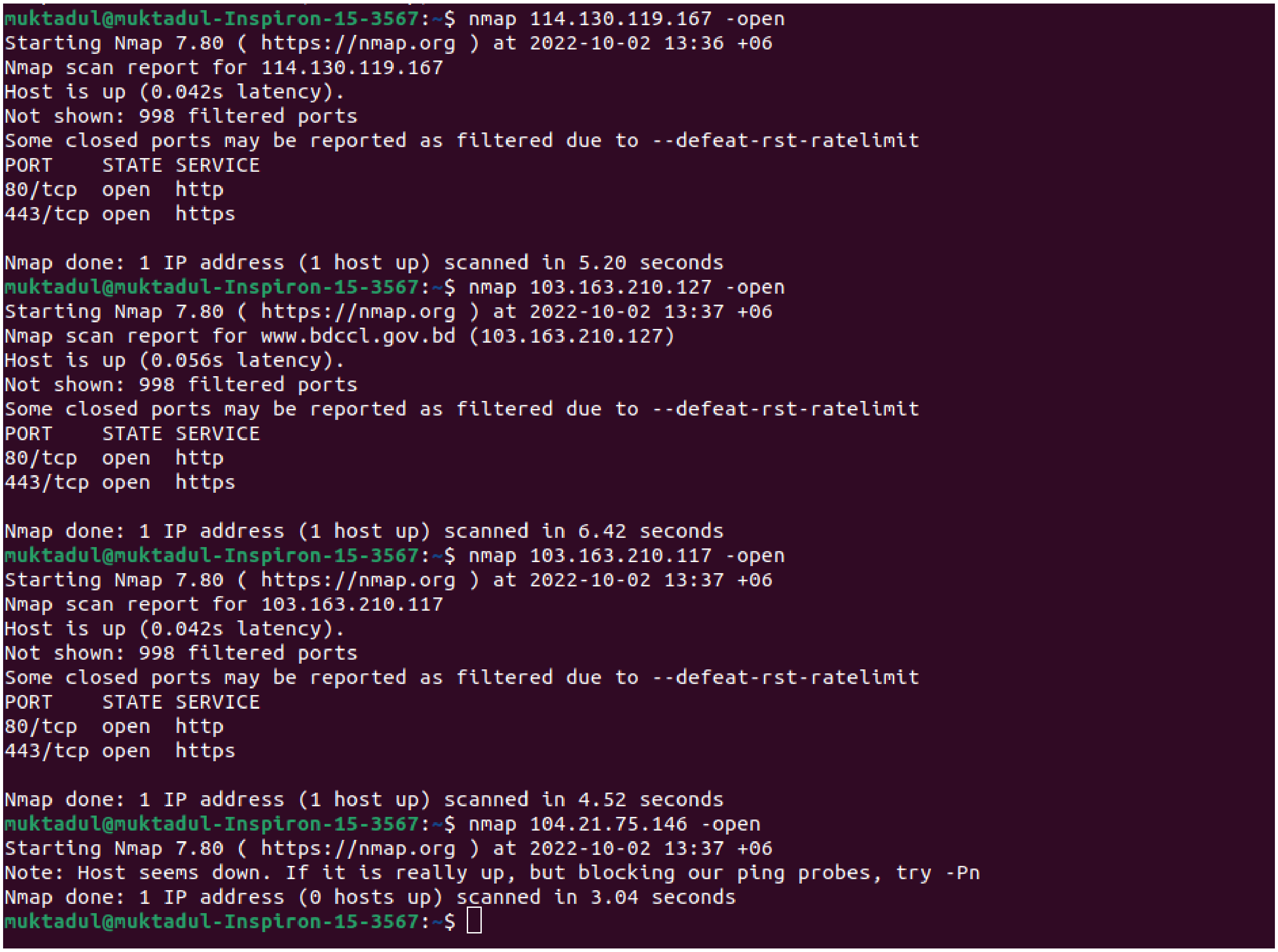
```
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.130 -sC
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 13:12 +06
Nmap scan report for 103.163.210.130
Host is up (0.038s latency).
All 1000 scanned ports on 103.163.210.130 are filtered

Nmap done: 1 IP address (1 host up) scanned in 39.38 seconds
root@muktadul-Inspiron-15-3567:~# nmap 114.130.119.167 -sC
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 13:13 +06
Nmap scan report for 114.130.119.167
Host is up (0.22s latency).
All 1000 scanned ports on 114.130.119.167 are filtered

Nmap done: 1 IP address (1 host up) scanned in 219.44 seconds
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.127 -sC
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 13:17 +06
Nmap scan report for www.bdccl.gov.bd (103.163.210.127)
Host is up (0.058s latency).
All 1000 scanned ports on www.bdccl.gov.bd (103.163.210.127) are filtered

Nmap done: 1 IP address (1 host up) scanned in 59.86 seconds
root@muktadul-Inspiron-15-3567:~# nmap 103.163.210.117 -sC
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 13:18 +06
Nmap scan report for 103.163.210.117
Host is up (0.032s latency).
All 1000 scanned ports on 103.163.210.117 are filtered

Nmap done: 1 IP address (1 host up) scanned in 33.62 seconds
root@muktadul-Inspiron-15-3567:~# nmap 104.21.75.146 -sC
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 13:19 +06
Nmap scan report for 104.21.75.146
Host is up (0.050s latency).
All 1000 scanned ports on 104.21.75.146 are filtered

Nmap done: 1 IP address (1 host up) scanned in 51.60 seconds
```

Firewall / IDS Evasion and Spoofing

1. Now we have to perform “nmap IP -open” for finding open ports.



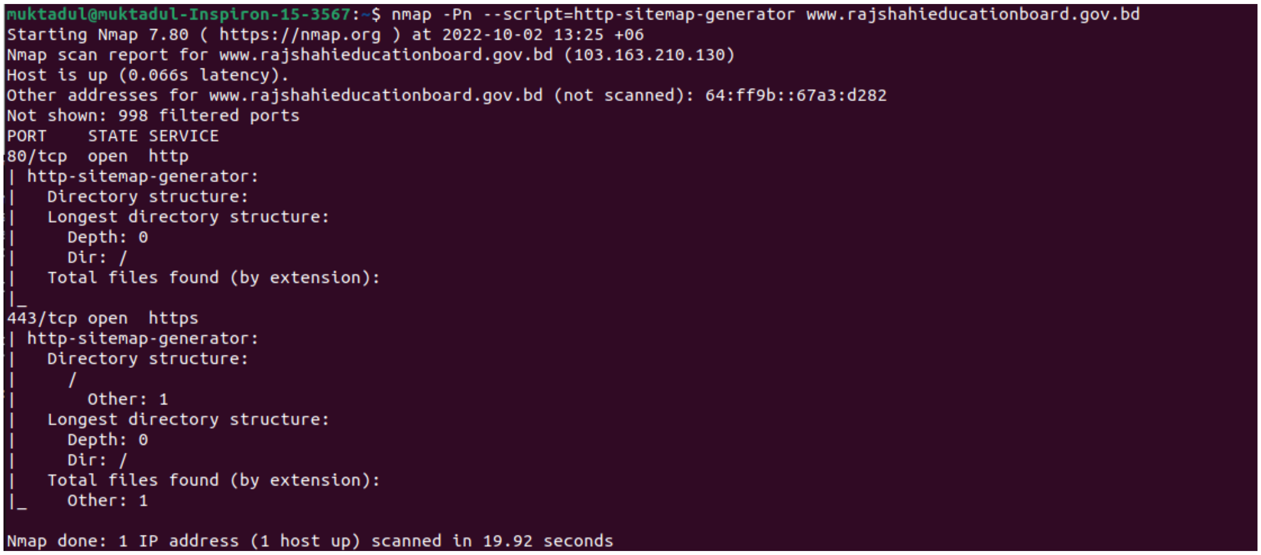
```
muktadul@muktadul-Inspiron-15-3567:~$ nmap 103.163.210.130 -open
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 13:36 +06
Nmap scan report for 103.163.210.130
Host is up (0.14s latency).
Not shown: 998 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 23.80 seconds
```



```
muktadul@muktadul-Inspiron-15-3567:~$ nmap 114.130.119.167 -open
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 13:36 +06
Nmap scan report for 114.130.119.167
Host is up (0.042s latency).
Not shown: 998 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.20 seconds
muktadul@muktadul-Inspiron-15-3567:~$ nmap 103.163.210.127 -open
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 13:37 +06
Nmap scan report for www.bdccl.gov.bd (103.163.210.127)
Host is up (0.056s latency).
Not shown: 998 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 6.42 seconds
muktadul@muktadul-Inspiron-15-3567:~$ nmap 103.163.210.117 -open
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 13:37 +06
Nmap scan report for 103.163.210.117
Host is up (0.042s latency).
Not shown: 998 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 4.52 seconds
muktadul@muktadul-Inspiron-15-3567:~$ nmap 104.21.75.146 -open
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 13:37 +06
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 3.04 seconds
muktadul@muktadul-Inspiron-15-3567:~$
```

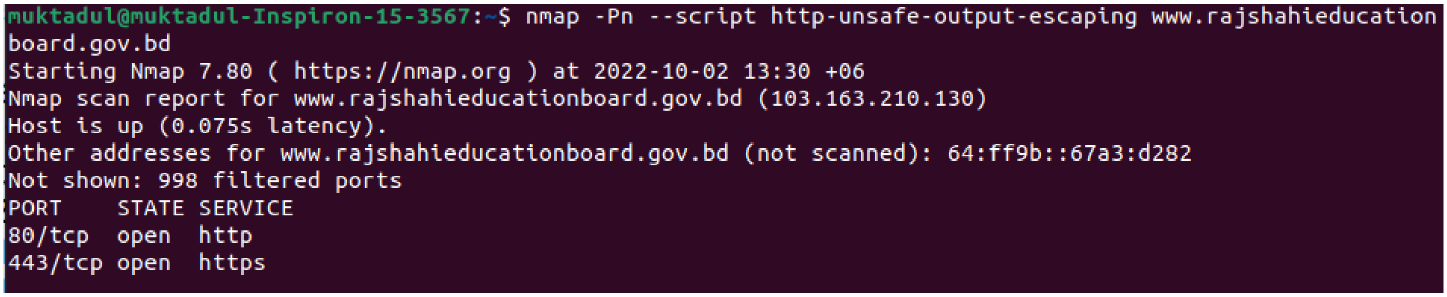
Useful NSE Script Examples

1. http site map generator:



```
muktadul@muktadul-Inspiron-15-3567:~$ nmap -Pn --script=http-sitemap-generator www.rajshahieducationboard.gov.bd
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 13:25 +06
Nmap scan report for www.rajshahieducationboard.gov.bd (103.163.210.130)
Host is up (0.066s latency).
Other addresses for www.rajshahieducationboard.gov.bd (not scanned): 64:ff9b::67a3:d282
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
| http-sitemap-generator:
|   Directory structure:
|   Longest directory structure:
|     Depth: 0
|     Dir: /
|   Total files found (by extension):
|_
443/tcp open  https
| http-sitemap-generator:
|   Directory structure:
|     /
|       Other: 1
|   Longest directory structure:
|     Depth: 0
|     Dir: /
|   Total files found (by extension):
|_    Other: 1

Nmap done: 1 IP address (1 host up) scanned in 19.92 seconds
```

2. Detect cross site scripting vulnerabilities:



```
muktadul@muktadul-Inspiron-15-3567:~$ nmap -Pn --script http-unsafe-output-escaping www.rajshahieducation
board.gov.bd
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 13:30 +06
Nmap scan report for www.rajshahieducationboard.gov.bd (103.163.210.130)
Host is up (0.075s latency).
Other addresses for www.rajshahieducationboard.gov.bd (not scanned): 64:ff9b::67a3:d282
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

3. Fast search for random web servers on port 80:

```
root@muktadul-Inspiron-15-3567:~# nmap -n -Pn -p 80 --open -sV -vvv --script banner,http-title -iR 1000
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 13:50 +06
NSE: Loaded 47 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 13:50
Completed NSE at 13:50, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 13:50
Completed NSE at 13:50, 0.00s elapsed
Initiating SYN Stealth Scan at 13:50
Scanning 1000 hosts [1 port/host]
Discovered open port 80/tcp on 104.76.21.3
Discovered open port 80/tcp on 20.126.172.21
Discovered open port 80/tcp on 84.239.77.66
Discovered open port 80/tcp on 168.44.248.56
Discovered open port 80/tcp on 42.193.117.91
Discovered open port 80/tcp on 44.241.30.92
Discovered open port 80/tcp on 3.22.248.90
Discovered open port 80/tcp on 101.167.171.163
Discovered open port 80/tcp on 23.73.123.188
Discovered open port 80/tcp on 52.209.250.194
Discovered open port 80/tcp on 175.246.66.202
Discovered open port 80/tcp on 20.100.30.200
Discovered open port 80/tcp on 45.207.15.209
Discovered open port 80/tcp on 163.152.212.30
Discovered open port 80/tcp on 147.78.131.88
Discovered open port 80/tcp on 47.110.71.173
Discovered open port 80/tcp on 103.40.100.213
Discovered open port 80/tcp on 41.225.219.226
Discovered open port 80/tcp on 5.8.46.119
Completed SYN Stealth Scan at 13:50, 24.61s elapsed (1000 total ports)
Initiating Service scan at 13:50
Scanning 19 services on 1000 hosts
Completed Service scan at 13:51, 30.77s elapsed (19 services on 1000 hosts)
NSE: Script scanning 1000 hosts.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 13:51
NSE Timing: About 92.87% done; ETC: 13:51 (0:00:02 remaining)
NSE Timing: About 99.53% done; ETC: 13:52 (0:00:00 remaining)
Completed NSE at 13:52, 63.57s elapsed
```

```
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 13:52
Completed NSE at 13:52, 15.52s elapsed
Nmap scan report for 101.167.171.163
Host is up, received user-set (0.30s latency).
Scanned at 2022-10-02 13:50:42 +06 for 114s

PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 42 Cross DVR httpd
Service Info: Device: media device

Nmap scan report for 84.239.77.66
Host is up, received user-set (0.26s latency).
Scanned at 2022-10-02 13:50:36 +06 for 119s

PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 46 nginx

Nmap scan report for 42.193.117.91
Host is up, received user-set (0.43s latency).
Scanned at 2022-10-02 13:50:38 +06 for 121s

PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 45 nginx

Nmap scan report for 104.76.21.3
Host is up, received user-set (0.30s latency).
Scanned at 2022-10-02 13:50:31 +06 for 127s

PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 49 AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)

Nmap scan report for 45.207.15.209
Host is up, received user-set (0.26s latency).
Scanned at 2022-10-02 13:50:44 +06 for 110s

PORT   STATE SERVICE REASON          VERSION
80/tcp open  http?   syn-ack ttl 243

Nmap scan report for 20.100.30.200
Host is up, received user-set (0.53s latency).
Scanned at 2022-10-02 13:50:44 +06 for 117s

PORT   STATE SERVICE REASON          VERSION
80/tcp open  http    syn-ack ttl 100
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 302 Found
|     Content-Type: text/html; charset=UTF-8
|     Content-Length: 164
|     Location: http://wdp.joycalls.com/?dest_url=
|     Cache-Control: no-cache
|     Connection: Close
|     <html><head><title>302 Found</title></head><body><h1>302 Found</h1><p>The document has 
moved <a href="http://wdp.joycalls.com/?dest_url=">here</a></p></body></html>
```

```
|   HTTPOptions:
|     HTTP/1.1 404 Site Not Found
|     Content-Length: 2775
|     Connection: close
|     Content-Type: text/html
|     Date: Sun, 02 Oct 2022 07:51:03 GMT
|     <!DOCTYPE html>
|     <html>
|     <head>
|     <title>Microsoft Azure Web App - Error 404</title>
|     <style type="text/css">
|     html {
|     height: 100%;
|     width: 100%;
|     #feature {
|     width: 960px;
|     margin: 75px auto 0 auto;
|     overflow: auto;
|     #content {
|     font-family: "Segoe UI";
|     font-weight: normal;
|     font-size: 22px;
|     color: #ffffff;
|     float: left;
|     margin-top: 68px;
|     margin-left: 0px;
|     vertical-align: middle;
|     #content h1 {
|     font-family: "Segoe UI Light";
|     color: #ffffff;
|_    font-weight: normal;
1 service unrecognized despite returning data. If you know the service/version, please submit the following
fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.80%I=7%D=10/2%Time=633942E8%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,151,"HTTP/1\.1\x20302\x20Found\r\nContent-Type:\x20text/html;\x2
SF:0charset=UTF-8\r\nContent-Length:\x20164\r\nLocation:\x20http://wdp\.jo
SF:ycalls\.com/\?dest_url=\r\nCache-Control:\x20no-cache\r\nConnection:\x2
SF:0Close\r\n\r\n<html><head><title>302\x20Found</title></head><body><h1>3
SF:02\x20Found</h1><p>The\x20document\x20has\x20moved\x20<a\x20href=\"http
SF:://wdp\.joycalls\.com/\?dest_url=\">here</a></p></body></html>")%r(HTTP
SF:Options,B5D,"HTTP/1\.1\x20404\x20Site\x20Not\x20Found\r\nContent-Length
SF::\x202775\r\nConnection:\x20close\r\nContent-Type:\x20text/html\r\nDate
SF::\x20Sun,\x2002\x20Oct\x202022\x2007:51:03\x20GMT\r\n\r\n<!DOCTYPE\x20h
SF:tml>\r\n<html>\r\n<head>\r\n\x20\x20\x20\x20<title>Microsoft\x20Azure\x
SF:20Web\x20App\x20-\x20Error\x20404</title>\r\n\x20\x20\x20\x20<style\x20
SF:type=\"text/css\">\r\n\x20\x20\x20\x20\x20\x20\x20\x20html\x20{\r\n\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20height:\x20100%;\r\n\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20width:\x20100%;\r\n\x20\x20\x2
SF:0\x20\x20\x20\x20\x20}\r\n\r\n\x20\x20\x20\x20\x20\x20\x20\x20#feature\
SF:x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20width:\x20960px
SF:;\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20margin:\x2075px\x2
SF:0auto\x200\x20auto;\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:overflow:\x20auto;\r\n\x20\x20\x20\x20\x20\x20\x20\x20}\r\n\r\n\x20\x20
SF:\x20\x20\x20\x20\x20\x20#content\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20font-family:\x20\"Segoe\x20UI\";\r\n\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20font-weight:\x20normal;\r\n\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x2022px;\r\n\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#ffffff;\r\n\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20float:\x20left;\r\n\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20margin-top:\x2068px;\r\n\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20margin-left:\x200px;\r\n\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20vertical-align:\x20middle;\r\n\x20\x20\
SF:x20\x20\x20\x20\x20\x20}\r\n\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20#content\x20h1\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20font-family:\x20\"Segoe\x20UI\x20Light\";\r\n\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20color:\x
SF:20#ffffff;\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20font-weight:\x20normal;\r\n\x20\x20\x20");

Nmap scan report for 41.225.219.226
Host is up, received user-set (0.28s latency).
Scanned at 2022-10-02 13:50:53 +06 for 102s

PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 45 Webs
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 302 Moved Temporarily
|     Content-Type: text/html; charset=UTF-8
|     Content-Length: 224
|     Location: http://wdp.joycalls.com/?dest_url=/nice%20ports%2C/Tri%6Eity.txt%2ebak
|     Cache-Control: no-cache
|     Connection: Close
|     <html><head><title>302 Moved Temporarily</title></head><body><h1>302 Moved
Temporarily</h1><p>The document has moved <a
href="http://wdp.joycalls.com/?dest_url=/nice%20ports%2C/Tri%6Eity.txt%2ebak">here</a></p></body></ht
ml>
|   GetRequest:
|     HTTP/1.0 200 OK
|     Date: Sun, 02 Oct 2022 08:57:18 GMT
|     Server: Webs
|     X-Frame-Options: SAMEORIGIN
|     ETag: "0-5d0-1e0"
|     Content-Length: 480
|     Content-Type: text/html
|     Connection: close
|     Last-Modified: Sun, 28 Jun 2020 02:17:11 GMT
|     <!doctype html>
|     <html>
|     <head>
|     <title></title>
|     <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
|     <meta http-equiv="X-UA-Compatible" content="IE=edge" >
|     <meta http-equiv="Pragma" content="no-cache" />
|     <meta http-equiv="Cache-Control" content="no-cache, must-revalidate" />
|     <meta http-equiv="Expires" content="0" />
|     </head>
|     <body>
|     </body>
|     <script>
|     window.location.href = "/doc/page/login.asp?_" + (new Date()).getTime();
|     </script>
|     </html>
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Date: Sun, 02 Oct 2022 08:57:21 GMT
|     Server: Webs
|     X-Frame-Options: SAMEORIGIN
|     Content-Length: 0
|     Content-Type: text/html
|     Connection: close
|_    Allow: OPTIONS,GET,HEAD,POST,PUT,DELETE
|_http-server-header: Webs
1 service unrecognized despite returning data. If you know the service/version, please submit the following
fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.80%I=7%D=10/2%Time=633942E9%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,2C5,"HTTP/1\.0\x20200\x20OK\r\nDate:\x20Sun,\x2002\x20Oct\x20202
SF:2\x2008:57:18\x20GMT\r\nServer:\x20Webs\r\nX-Frame-Options:\x20SAMEORIG
SF:IN\r\nETag:\x20\"0-5d0-1e0\"\r\nContent-Length:\x20480\r\nContent-Type:
SF:\x20text/html\r\nConnection:\x20close\r\nLast-Modified:\x20Sun,\x2028\x
SF:20Jun\x202020\x2002:17:11\x20GMT\r\n\r\n\xef\xbb\xbf<!doctype\x20html>\
SF:r\n<html>\r\n<head>\r\n\t<title></title>\r\n\t<meta\x20http-equiv=\"Con
SF:tent-Type\"\x20content=\"text/html;\x20charset=utf-8\"\x20/>\r\n\t<meta
SF:\x20http-equiv=\"X-UA-Compatible\"\x20content=\"IE=edge\"\x20>\r\n\t<me
SF:ta\x20http-equiv=\"Pragma\"\x20content=\"no-cache\"\x20/>\r\n\t<meta\x2
SF:0http-equiv=\"Cache-Control\"\x20content=\"no-cache,\x20must-revalidate
SF:\"\x20/>\r\n\t<meta\x20http-equiv=\"Expires\"\x20content=\"0\"\x20/>\r\
SF:n</head>\r\n<body>\r\n</body>\r\n<script>\r\n\twindow\.location\.href\x
SF:20=\x20\"/doc/page/login\.asp\?_\"\x20\+\x20\(new\x20Date\(\)\)\.getTim
SF:e\(\);\r\n</script>\r\n</html>")%r(HTTPOptions,CB,"HTTP/1\.0\x20200\x20
SF:OK\r\nDate:\x20Sun,\x2002\x20Oct\x202022\x2008:57:21\x20GMT\r\nServer:\
SF:x20Webs\r\nX-Frame-Options:\x20SAMEORIGIN\r\nContent-Length:\x200\r\nCo
SF:ntent-Type:\x20text/html\r\nConnection:\x20close\r\nAllow:\x20OPTIONS,G
SF:ET,HEAD,POST,PUT,DELETE\r\n\r\n")%r(FourOhFourRequest,1BD,"HTTP/1\.0\x2
SF:0302\x20Moved\x20Temporarily\r\nContent-Type:\x20text/html;\x20charset=
SF:UTF-8\r\nContent-Length:\x20224\r\nLocation:\x20http://wdp\.joycalls\.c
SF:om/\?dest_url=/nice%20ports%2C/Tri%6Eity\.txt%2ebak\r\nCache-Control:\x
SF:20no-cache\r\nConnection:\x20Close\r\n\r\n<html><head><title>302\x20Mov
SF:ed\x20Temporarily</title></head><body><h1>302\x20Moved\x20Temporarily</
SF:h1><p>The\x20document\x20has\x20moved\x20<a\x20href=\"http://wdp\.joyca
SF:lls\.com/\?dest_url=/nice%20ports%2C/Tri%6Eity\.txt%2ebak\">here</a></p
SF:></body></html>");

Nmap scan report for 103.40.100.213
Host is up, received user-set (0.32s latency).
Scanned at 2022-10-02 13:50:50 +06 for 106s

PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 49
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 302 Moved Temporarily
|     Content-Type: text/html; charset=UTF-8
|     Content-Length: 224
|     Location: http://wdp.joycalls.com/?dest_url=/nice%20ports%2C/Tri%6Eity.txt%2ebak
|     Cache-Control: no-cache
|     Connection: Close
|     <html><head><title>302 Moved Temporarily</title></head><body><h1>302 Moved
Temporarily</h1><p>The document has moved <a
href="http://wdp.joycalls.com/?dest_url=/nice%20ports%2C/Tri%6Eity.txt%2ebak">here</a></p></body></ht
ml>
|   GetRequest:
|     HTTP/1.0 302 Moved Temporarily
|     Content-Type: text/html; charset=UTF-8
|     Content-Length: 188
|     Location: http://wdp.joycalls.com/?dest_url=
|     Cache-Control: no-cache
|     Connection: Close
|     <html><head><title>302 Moved Temporarily</title></head><body><h1>302 Moved
Temporarily</h1><p>The document has moved <a
href="http://wdp.joycalls.com/?dest_url=">here</a></p></body></html>
|   HTTPOptions:
|     HTTP/1.0 204 No Content
|     Access-Control-Allow-Credentials: true
|     Access-Control-Allow-Headers:
|     Access-Control-Allow-Methods: POST, GET, OPTIONS
|     Access-Control-Allow-Origin:
|     Access-Control-Max-Age: 86400
|     Confighost: *
|     Content-Type:
|     Date: Sun, 02 Oct 2022 07:51:05 GMT
|   RTSPRequest, SIPOptions:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|_    Request
1 service unrecognized despite returning data. If you know the service/version, please submit the following
fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.80%I=7%D=10/2%Time=633942E8%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,175,"HTTP/1\.0\x20302\x20Moved\x20Temporarily\r\nContent-Type:\x
SF:20text/html;\x20charset=UTF-8\r\nContent-Length:\x20188\r\nLocation:\x2
SF:0http://wdp\.joycalls\.com/\?dest_url=\r\nCache-Control:\x20no-cache\r\
SF:nConnection:\x20Close\r\n\r\n<html><head><title>302\x20Moved\x20Tempora
SF:rily</title></head><body><h1>302\x20Moved\x20Temporarily</h1><p>The\x20
SF:document\x20has\x20moved\x20<a\x20href=\"http://wdp\.joycalls\.com/\?de
SF:st_url=\">here</a></p></body></html>")%r(HTTPOptions,117,"HTTP/1\.0\x20
SF:204\x20No\x20Content\r\nAccess-Control-Allow-Credentials:\x20true\r\nAc
SF:cess-Control-Allow-Headers:\x20\r\nAccess-Control-Allow-Methods:\x20POS
SF:T,\x20GET,\x20OPTIONS\r\nAccess-Control-Allow-Origin:\x20\r\nAccess-Con
SF:trol-Max-Age:\x2086400\r\nConfighost:\x20\*\r\nContent-Type:\x20\r\nDat
SF:e:\x20Sun,\x2002\x20Oct\x202022\x2007:51:05\x20GMT\r\n\r\n")%r(RTSPRequ
SF:est,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/pla
SF:in;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Reque
SF:st")%r(FourOhFourRequest,1BD,"HTTP/1\.0\x20302\x20Moved\x20Temporarily\
SF:r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\nContent-Length:\x202
SF:24\r\nLocation:\x20http://wdp\.joycalls\.com/\?dest_url=/nice%20ports%2
SF:C/Tri%6Eity\.txt%2ebak\r\nCache-Control:\x20no-cache\r\nConnection:\x20
SF:Close\r\n\r\n<html><head><title>302\x20Moved\x20Temporarily</title></he
SF:ad><body><h1>302\x20Moved\x20Temporarily</h1><p>The\x20document\x20has\
SF:x20moved\x20<a\x20href=\"http://wdp\.joycalls\.com/\?dest_url=/nice%20p
SF:orts%2C/Tri%6Eity\.txt%2ebak\">here</a></p></body></html>")%r(SIPOption
SF:s,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain
SF:;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request
SF:");

Nmap scan report for 175.246.66.202
Host is up, received user-set (0.53s latency).
Scanned at 2022-10-02 13:50:44 +06 for 117s

PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 44 lighttpd

Nmap scan report for 47.110.71.173
Host is up, received user-set (0.31s latency).
Scanned at 2022-10-02 13:50:49 +06 for 107s

PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 43 nginx

Nmap scan report for 44.241.30.92
Host is up, received user-set (0.44s latency).
Scanned at 2022-10-02 13:50:38 +06 for 122s

PORT   STATE SERVICE REASON          VERSION
80/tcp open  http    syn-ack ttl 221 awselb/2.0
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 301 Moved Permanently
|     Server: awselb/2.0
|     Date: Sun, 02 Oct 2022 07:51:07 GMT
|     Content-Type: text/html
|     Content-Length: 134
|     Connection: close
|     Location:
https://adg-453-prod-53887710.us-west-2.elb.amazonaws.com:443/nice%20ports%2C/Tri%6Eity.txt%2ebak
|     <html>
|     <head><title>301 Moved Permanently</title></head>
|     <body>
|     <center><h1>301 Moved Permanently</h1></center>
|     </body>
|     </html>
|   GetRequest:
|     HTTP/1.1 301 Moved Permanently
|     Server: awselb/2.0
|     Date: Sun, 02 Oct 2022 07:51:02 GMT
|     Content-Type: text/html
|     Content-Length: 134
|     Connection: close
|     Location: https://adg-453-prod-53887710.us-west-2.elb.amazonaws.com:443/
|     <html>
|     <head><title>301 Moved Permanently</title></head>
|     <body>
|     <center><h1>301 Moved Permanently</h1></center>
|     </body>
|     </html>
|   HTTPOptions:
|     HTTP/1.1 301 Moved Permanently
|     Server: awselb/2.0
|     Date: Sun, 02 Oct 2022 07:51:05 GMT
|     Content-Type: text/html
|     Content-Length: 134
|     Connection: close
|     Location: https://adg-453-prod-53887710.us-west-2.elb.amazonaws.com:443/
|     <html>
|     <head><title>301 Moved Permanently</title></head>
|     <body>
|     <center><h1>301 Moved Permanently</h1></center>
|     </body>
|     </html>
|   RPCCheck:
|     HTTP/1.1 400 Bad Request
|     Server: awselb/2.0
|     Date: Sun, 02 Oct 2022 07:51:13 GMT
|     Content-Type: text/html
|     Content-Length: 122
|     Connection: close
|     <html>
|     <head><title>400 Bad Request</title></head>
|     <body>
|     <center><h1>400 Bad Request</h1></center>
|     </body>
|     </html>
|   RTSPRequest:
|     <html>
|     <head><title>400 Bad Request</title></head>
|     <body>
|     <center><h1>400 Bad Request</h1></center>
|     </body>
|     </html>
|   X11Probe:
|     HTTP/1.1 400 Bad Request
|     Server: awselb/2.0
|     Date: Sun, 02 Oct 2022 07:51:06 GMT
|     Content-Type: text/html
|     Content-Length: 122
|     Connection: close
|     <html>
|     <head><title>400 Bad Request</title></head>
|     <body>
|     <center><h1>400 Bad Request</h1></center>
|     </body>
|_    </html>
|_http-server-header: awselb/2.0
1 service unrecognized despite returning data. If you know the service/version, please submit the following
fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.80%I=7%D=10/2%Time=633942E8%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,16C,"HTTP/1\.1\x20301\x20Moved\x20Permanently\r\nServer:\x20awse
SF:lb/2\.0\r\nDate:\x20Sun,\x2002\x20Oct\x202022\x2007:51:02\x20GMT\r\nCon
SF:tent-Type:\x20text/html\r\nContent-Length:\x20134\r\nConnection:\x20clo
SF:se\r\nLocation:\x20https://adg-453-prod-53887710\.us-west-2\.elb\.amazo
SF:naws\.com:443/\r\n\r\n<html>\r\n<head><title>301\x20Moved\x20Permanentl
SF:y</title></head>\r\n<body>\r\n<center><h1>301\x20Moved\x20Permanently</
SF:h1></center>\r\n</body>\r\n</html>\r\n")%r(HTTPOptions,16C,"HTTP/1\.1\x
SF:20301\x20Moved\x20Permanently\r\nServer:\x20awselb/2\.0\r\nDate:\x20Sun
SF:,\x2002\x20Oct\x202022\x2007:51:05\x20GMT\r\nContent-Type:\x20text/html
SF:\r\nContent-Length:\x20134\r\nConnection:\x20close\r\nLocation:\x20http
SF:s://adg-453-prod-53887710\.us-west-2\.elb\.amazonaws\.com:443/\r\n\r\n<
SF:html>\r\n<head><title>301\x20Moved\x20Permanently</title></head>\r\n<bo
SF:dy>\r\n<center><h1>301\x20Moved\x20Permanently</h1></center>\r\n</body>
SF:\r\n</html>\r\n")%r(RTSPRequest,7A,"<html>\r\n<head><title>400\x20Bad\x
SF:20Request</title></head>\r\n<body>\r\n<center><h1>400\x20Bad\x20Request
SF:</h1></center>\r\n</body>\r\n</html>\r\n")%r(X11Probe,110,"HTTP/1\.1\x2
SF:0400\x20Bad\x20Request\r\nServer:\x20awselb/2\.0\r\nDate:\x20Sun,\x2002
SF:\x20Oct\x202022\x2007:51:06\x20GMT\r\nContent-Type:\x20text/html\r\nCon
SF:tent-Length:\x20122\r\nConnection:\x20close\r\n\r\n<html>\r\n<head><tit
SF:le>400\x20Bad\x20Request</title></head>\r\n<body>\r\n<center><h1>400\x2
SF:0Bad\x20Request</h1></center>\r\n</body>\r\n</html>\r\n")%r(FourOhFourR
SF:equest,18F,"HTTP/1\.1\x20301\x20Moved\x20Permanently\r\nServer:\x20awse
SF:lb/2\.0\r\nDate:\x20Sun,\x2002\x20Oct\x202022\x2007:51:07\x20GMT\r\nCon
SF:tent-Type:\x20text/html\r\nContent-Length:\x20134\r\nConnection:\x20clo
SF:se\r\nLocation:\x20https://adg-453-prod-53887710\.us-west-2\.elb\.amazo
SF:naws\.com:443/nice%20ports%2C/Tri%6Eity\.txt%2ebak\r\n\r\n<html>\r\n<he
SF:ad><title>301\x20Moved\x20Permanently</title></head>\r\n<body>\r\n<cent
SF:er><h1>301\x20Moved\x20Permanently</h1></center>\r\n</body>\r\n</html>\
SF:r\n")%r(RPCCheck,110,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nServer:\x20
SF:awselb/2\.0\r\nDate:\x20Sun,\x2002\x20Oct\x202022\x2007:51:13\x20GMT\r\
SF:nContent-Type:\x20text/html\r\nContent-Length:\x20122\r\nConnection:\x2
SF:0close\r\n\r\n<html>\r\n<head><title>400\x20Bad\x20Request</title></hea
SF:d>\r\n<body>\r\n<center><h1>400\x20Bad\x20Request</h1></center>\r\n</bo
SF:dy>\r\n</html>\r\n");

Nmap scan report for 168.44.248.56
Host is up, received user-set (0.33s latency).
Scanned at 2022-10-02 13:50:36 +06 for 120s

PORT   STATE SERVICE REASON          VERSION
80/tcp open  http    syn-ack ttl 100 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 163.152.212.30
Host is up, received user-set (0.77s latency).
Scanned at 2022-10-02 13:50:47 +06 for 118s

PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 42 Apache httpd 2.2.26 ((Unix) mod_ssl/2.2.26 OpenSSL/1.0.1s DAV/2
PHP/5.2.6 mod_jk/1.2.37)

Nmap scan report for 5.8.46.119
Host is up, received user-set (0.32s latency).
Scanned at 2022-10-02 13:50:54 +06 for 102s

PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 45 nginx

Nmap scan report for 20.126.172.21
```

```
Host is up, received user-set (0.26s latency).
Scanned at 2022-10-02 13:50:34 +06 for 121s

PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 42 *
| fingerprint-strings:
|   HTTPOptions:
|     HTTP/1.1 403 Forbidden
|     Date: Sun, 02 Oct 2022 07:51:07 GMT
|     Server: *
|     Accept-Ranges: bytes
|     Content-Type: text/html
|     Vary: User-Agent
|     Connection: close
|     <!doctype html>
|     <html lang="en">
|     <head>
|     <meta charset="utf-8">
|     <title>SAP Commerce Cloud - Forbidden</title>
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <link rel="icon" type="image/x-icon" href="/mt_error/include/favicon.ico">
|     <style type="text/css">
|     @font-face {
|     font-family: '72';
|     src: url('/mt_error/include/72-Light.woff2') format('woff2'),
|     url('/mt_error/include/72-Light.woff') format('woff'),
|     url('/mt_error/include/72-Light.ttf') format('truetype');
|     font-style: normal;
|     font-weight: 200;
|     @font-face {
|     font-
|   RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     Date: Sun, 02 Oct 2022 07:51:08 GMT
|     Server: *
|     Content-Length: 226
|     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>
|_    </body></html>
|_http-server-header: *
1 service unrecognized despite returning data. If you know the service/version, please submit the following
fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.80%I=7%D=10/2%Time=633942EB%P=x86_64-pc-linux-gnu%r(HTTP
SF:Options,33DB,"HTTP/1\.1\x20403\x20Forbidden\r\nDate:\x20Sun,\x2002\x20O
SF:ct\x202022\x2007:51:07\x20GMT\r\nServer:\x20\*\r\nAccept-Ranges:\x20byt
SF:es\r\nContent-Type:\x20text/html\r\nVary:\x20User-Agent\r\nConnection:\
SF:x20close\r\n\r\n<!doctype\x20html>\n<html\x20lang=\"en\">\n\x20\x20\x20
SF:\x20<head>\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20charset=\"utf-8\">
```

```
SF:\n\x20\x20\x20\x20\x20\x20\x20\x20<title>SAP\x20Commerce\x20Cloud\x20-\
SF:x20Forbidden</title>\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20name=\"v
SF:iewport\"\x20content=\"width=device-width,\x20initial-scale=1\">\n\x20\
SF:x20\x20\x20\x20\x20\x20\x20<link\x20rel=\"icon\"\x20type=\"image/x-icon
SF:\"\x20href=\"/mt_error/include/favicon\.ico\">\n\x20\x20\x20\x20\x20\x2
SF:0\x20\x20<style\x20type=\"text/css\">\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20@font-face\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20font-family:\x20'72';\n\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20src:\x20url\('/mt_error/inclu
SF:de/72-Light\.woff2'\)\x20format\('woff2'\),\n\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20url\('/mt_error/i
SF:nclude/72-Light\.woff'\)\x20format\('woff'\),\n\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20url\('/mt_error
SF:/include/72-Light\.ttf'\)\x20format\('truetype'\);\n\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20font-style:\x20normal;\n\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20font-weig
SF:ht:\x20200;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20@font-face\x20{\n\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20font-")%r(RTSPReques
SF:t,183,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nDate:\x20Sun,\x2002\x20Oct
SF:\x202022\x2007:51:08\x20GMT\r\nServer:\x20\*\r\nContent-Length:\x20226\
SF:r\nConnection:\x20close\r\nContent-Type:\x20text/html;\x20charset=iso-8
SF:859-1\r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//IETF//DTD\x20HTML\x202
SF:\.0//EN\">\n<html><head>\n<title>400\x20Bad\x20Request</title>\n</head>
SF:<body>\n<h1>Bad\x20Request</h1>\n<p>Your\x20browser\x20sent\x20a\x20req
SF:uest\x20that\x20this\x20server\x20could\x20not\x20understand\.<br\x20/>
SF:\n</p>\n</body></html>\n");

Nmap scan report for 23.73.123.188
Host is up, received user-set (0.22s latency).
Scanned at 2022-10-02 13:50:43 +06 for 115s

PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 42 AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)

Nmap scan report for 3.22.248.90
Host is up, received user-set (0.44s latency).
Scanned at 2022-10-02 13:50:38 +06 for 121s

PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 35 Apache httpd 2.4.41
Service Info: Host: alphabetagold.rutasformativas.com

Nmap scan report for 147.78.131.88
Host is up, received user-set (0.34s latency).
Scanned at 2022-10-02 13:50:48 +06 for 109s

PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 46 nginx

Nmap scan report for 52.209.250.194
Host is up, received user-set (0.39s latency).
Scanned at 2022-10-02 13:50:44 +06 for 114s

PORT   STATE SERVICE REASON          VERSION
```

```
80/tcp open  http    syn-ack ttl 233 nginx

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 13:52
Completed NSE at 13:52, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 13:52
Completed NSE at 13:52, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1000 IP addresses (1000 hosts up) scanned in 134.88 seconds
           Raw packets sent: 1970 (86.680KB) | Rcvd: 57 (2.683KB)
```