INSTITUTE OF INFORMATION TECHNOLOGY

UNIVERSITY OF DHAKA

Report on Nmap Security Scan & Analysis

Course Title: Information Security

Course Code: SE 411

Submitted By

Istiaq Ahmed Fahad

BSSE 12th batch

Student ID: 1204

Submitted To

Dr. Mohammed Shafiul Alam Khan

Associate Professor,

IIT,

University of Dhaka.

Date of Submission

5th October 2022

Table of Contents

List of Websites **3**

Figure 1: Listing IP of given hostnames 4

Target Specification **5**

Scan Specific IP 5

Figure 2: Scan specific IP addresses 6

rDNS address 6

Scan Techniques **8**

TCP SYN port scan 8

UDP port scan 9

Figure 3: TCP-UDP port scanning 10

OS Detection **11**

Remote OS Detection (guess aggressively) 11

Figure 4: OS detection (aggressively) 12

Service and Version Detection **13**

Explore Version of Running Services 13

Figure 5: Service and Version detection 14

NSE Scripts **15**

Default NSE Scripts Scanning 15

Figure 6: Default NSE Scripts Scanning 16

Single NSE Script Scan 16

http-wordpress-users.nse 16

Figure 7: Specific Script (http-wordpress-users) Scanning 16

http-cookie-flags.nse 17

Figure 8: Specific Script (http-cookie-flags) Scanning 17

ssl-enum-ciphers.nse 17

dns-brute.nse 19

Figure 9: Specific Script (dns-brute) Scanning 19

Miscellaneous **20**

Site Map Generation 20

103.163.210.131 20

103.163.210.127 20

103.230.107.235 21

114.130.119.162 22

103.48.16.214 22

103.163.210.130 23

3.1.208.233 24

Output **25**

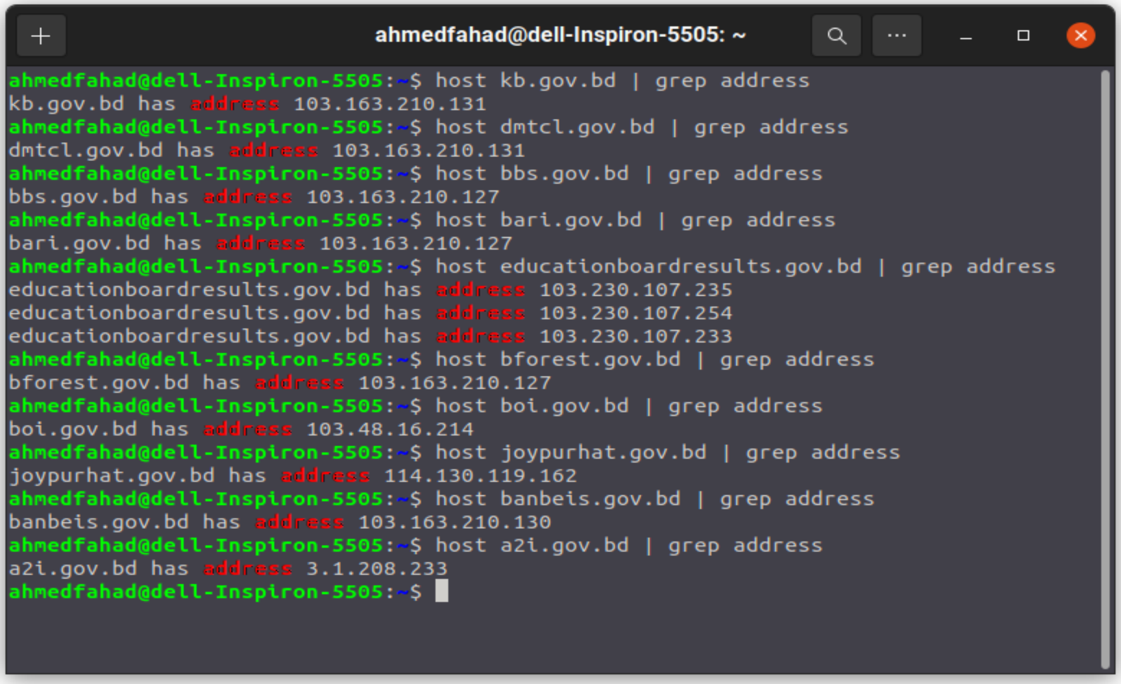
Nmap Security Scan & Analysis

Here we'll explore the details of network-related topics and security issues of the following websites using Nmap.

List of Websites

1. http://www.kb.gov.bd
2. http://dmtcl.gov.bd
3. http://www.bbs.gov.bd
4. http://www.bari.gov.bd
5. http://www.educationboardresults.gov.bd
6. http://www.bforest.gov.bd
7. http://www.boi.gov.bd
8. http://www.joypurhat.gov.bd
9. http://www.banbeis.gov.bd
10. https://a2i.gov.bd

But before jumping into the details of the scanning procedure we need to know the IP addresses of the following sites. We will use the **host <hostname>** command to find the IP address.



```
ahmedfahad@dell-Inspiron-5505:~$ host kb.gov.bd | grep address
kb.gov.bd has address 103.163.210.131
ahmedfahad@dell-Inspiron-5505:~$ host dmtcl.gov.bd | grep address
dmtcl.gov.bd has address 103.163.210.131
ahmedfahad@dell-Inspiron-5505:~$ host bbs.gov.bd | grep address
bbs.gov.bd has address 103.163.210.127
ahmedfahad@dell-Inspiron-5505:~$ host bari.gov.bd | grep address
bari.gov.bd has address 103.163.210.127
ahmedfahad@dell-Inspiron-5505:~$ host educationboardresults.gov.bd | grep address
educationboardresults.gov.bd has address 103.230.107.235
educationboardresults.gov.bd has address 103.230.107.254
educationboardresults.gov.bd has address 103.230.107.233
ahmedfahad@dell-Inspiron-5505:~$ host bforest.gov.bd | grep address
bforest.gov.bd has address 103.163.210.127
ahmedfahad@dell-Inspiron-5505:~$ host boi.gov.bd | grep address
boi.gov.bd has address 103.48.16.214
ahmedfahad@dell-Inspiron-5505:~$ host joypurhat.gov.bd | grep address
joypurhat.gov.bd has address 114.130.119.162
ahmedfahad@dell-Inspiron-5505:~$ host banbeis.gov.bd | grep address
banbeis.gov.bd has address 103.163.210.130
ahmedfahad@dell-Inspiron-5505:~$ host a2i.gov.bd | grep address
a2i.gov.bd has address 3.1.208.233
ahmedfahad@dell-Inspiron-5505:~$ 
```

Figure 1: Listing IP of given hostnames

List of websites & IP addresses

http://www.kb.gov.bd	103.163.210.131
http://dmtcl.gov.bd	103.163.210.131
http://www.bbs.gov.bd	103.163.210.127
http://www.bari.gov.bd	103.163.210.127
http://www.educationboardresults.gov.bd	103.230.107.235
http://www.bforest.gov.bd	103.163.210.127
http://www.boi.gov.bd	103.48.16.214
http://www.joypurhat.gov.bd	114.130.119.162
http://www.banbeis.gov.bd	103.163.210.130
https://a2i.gov.bd	3.1.208.233

Here we can observe 7 distinct IP addresses of given hostnames. In the following exploration, we'll execute our operations on the following distinct IP addresses.

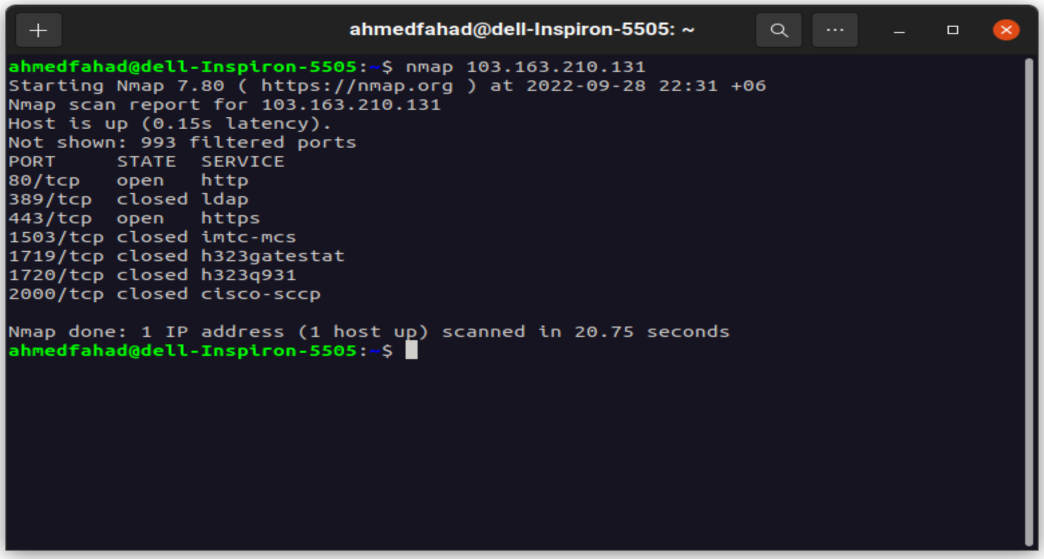
Target Specification

Scan Specific IP

In this segment we'll scan each IP to explore the *Ports, States, and Services* they actually provide through the **nmap <ip>** command.

IP Addresses	Scan Results
103.163.210.131 (http://www.kb.gov.bd, http://dmtcl.gov.bd)	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
103.163.210.127 (http://www.bbs.gov.bd, http://www.bari.gov.bd, http://www.bforest.gov.bd)	PORT STATE SERVICE **80/tcp open http** **443/tcp open https**
103.230.107.235 (http://www.educationboardresults.gov.bd)	PORT STATE SERVICE **80/tcp open http** 5060/tcp filtered sip 8899/tcp filtered ospf-lite
103.48.16.214 (http://www.boi.gov.bd)	PORT STATE SERVICE 25/tcp closed smtp **80/tcp open http** **443/tcp open https** 3000/tcp closed ppp **8080/tcp open http-proxy** **10000/tcp open snet-sensor-mgmt**
114.130.119.162 (http://www.joypurhat.gov.bd)	PORT STATE SERVICE **80/tcp open http** **443/tcp open https**
103.163.210.130 (http://www.banbeis.gov.bd)	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
3.1.208.233 (https://a2i.gov.bd)	PORT STATE SERVICE **22/tcp open ssh** **80/tcp open http** **443/tcp open https**



```
ahmedfahad@dell-Inspiron-5505:~$ nmap 103.163.210.131
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-28 22:31 +06
Nmap scan report for 103.163.210.131
Host is up (0.15s latency).
Not shown: 993 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

Nmap done: 1 IP address (1 host up) scanned in 20.75 seconds
ahmedfahad@dell-Inspiron-5505:~$ 
```

Figure 2: Scan specific IP addresses

From the following nmap scanning results, it can be concluded that almost all the hosts have HTTP and HTTPS port is in the open state. Some exceptions also occurred like http-proxy, and snet-sensor-mgmt and it's normal that some hosts might have some ports that can be open for their service purposes.

rDNS address

An rDNS (reverse DNS) lookup is the act of looking up internet hosts by their IP address. Here we execute the **nmap <hostname>** command and get the following rDNS for each IP address.

IP Addresses	rDNS
103.163.210.131 (http://www.kb.gov.bd, http://dmtcl.gov.bd)	Null

103.163.210.127 (http://www.bbs.gov.bd, http://www.bari.gov.bd, http://www.bforest.gov.bd)	bdccl.gov.bd
103.230.107.235 (http://www.educationboardresults.gov.bd)	Null
103.48.16.214 (http://www.boi.gov.bd)	Null
114.130.119.162 (http://www.joypurhat.gov.bd)	Null
103.163.210.130 (http://www.banbeis.gov.bd)	Null
3.1.208.233 (https://a2i.gov.bd)	ec2-3-1-208-233.ap-southeast-1.compute.amazonaws.com

Surprisingly only two of them have rDNS for looking at hosts by IP address.

Scan Techniques

TCP SYN port scan

Stealth Scan is also known as **SYN** Scan or **TCP SYN** Scan because it sends only one SYN packet in the TCP Handshake process. We'll run **nmap <ip> -sS** to get the TCP SYN port scan results.

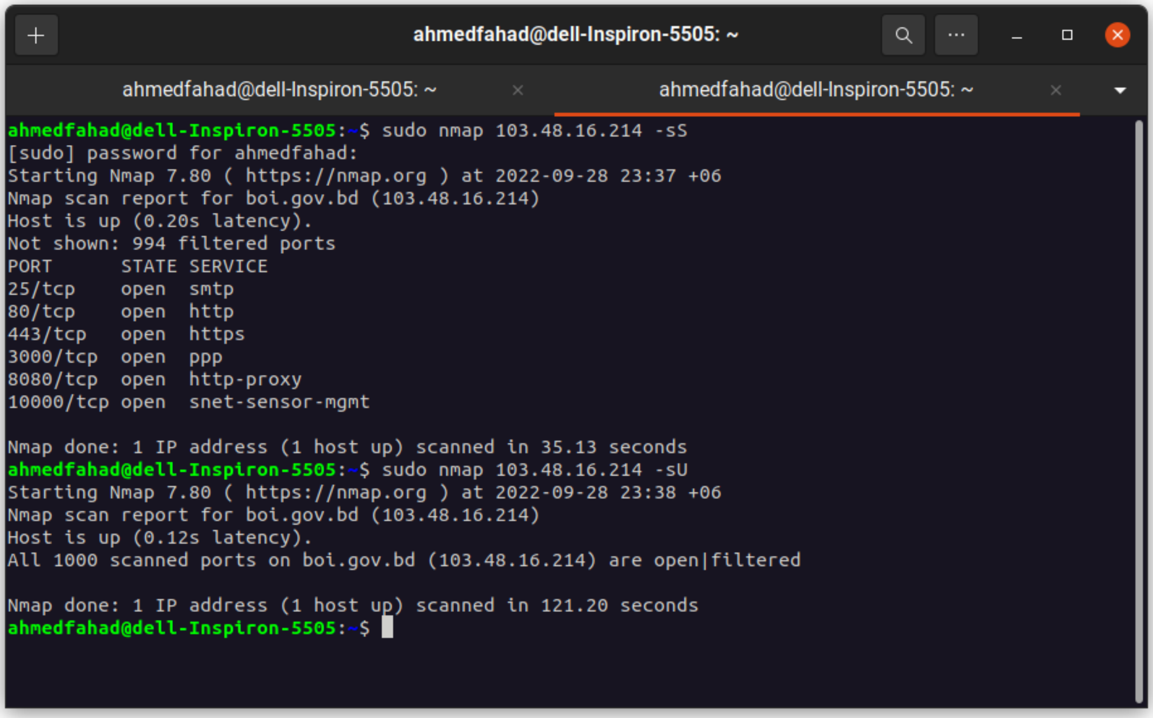
IP Addresses	Latency	Filtered Port
103.163.210.131 (http://www.kb.gov.bd, http://dmtcl.gov.bd)	0.058s	993
103.163.210.127 (http://www.bbs.gov.bd, http://www.bari.gov.bd, http://www.bforest.gov.bd)	0.058	998
103.230.107.235 (http://www.educationboardresults.gov.bd)	0.081s	998
103.48.16.214 (http://www.boi.gov.bd)	0.20s	994
114.130.119.162 (http://www.joypurhat.gov.bd)	0.050s	998
103.163.210.130 (http://www.banbeis.gov.bd)	0.13s	993
3.1.208.233 (https://a2i.gov.bd)	0.11s	997

UDP port scan

UDP Port Scan for quick testing of open UDP services and ports. With this scan type, nmap sends 0-byte *UDP* packets to each port on the target system. We'll run **nmap <ip> -sS** to get the TCP SYN port scan results.

IP Addresses	Latency	Filtered Port (Open)
103.163.210.131 (http://www.kb.gov.bd, http://dmtcl.gov.bd)	0.26s	1000
103.163.210.127 (http://www.bbs.gov.bd, http://www.bari.gov.bd, http://www.bforest.gov.bd)	0.075s	1000
103.230.107.235 (http://www.educationboardresults.gov.bd)	0.059s	996
103.48.16.214 (http://www.boi.gov.bd)	0.043s	1000
114.130.119.162 (http://www.joypurhat.gov.bd)	0.18s	1000
103.163.210.130 (http://www.banbeis.gov.bd)	0.16s	996
3.1.208.233 (https://a2i.gov.bd)	0.15s	1000

From the following **TCP SYN and UDP** port scanning result it’s observed that in most of the cases all UDP ports are open.



ahmedfahad@dell-Inspiron-5505: ~
ahmedfahad@dell-Inspiron-5505: ~
ahmedfahad@dell-Inspiron-5505: ~

```
ahmedfahad@dell-Inspiron-5505:~$ sudo nmap 103.48.16.214 -sS
[sudo] password for ahmedfahad:
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-28 23:37 +06
Nmap scan report for boi.gov.bd (103.48.16.214)
Host is up (0.20s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
3000/tcp  open  ppp
8080/tcp  open  http-proxy
10000/tcp open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 35.13 seconds
ahmedfahad@dell-Inspiron-5505:~$ sudo nmap 103.48.16.214 -sU
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-28 23:38 +06
Nmap scan report for boi.gov.bd (103.48.16.214)
Host is up (0.12s latency).
All 1000 scanned ports on boi.gov.bd (103.48.16.214) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 121.20 seconds
ahmedfahad@dell-Inspiron-5505:~$ 
```

Figure 3: TCP-UDP port scanning

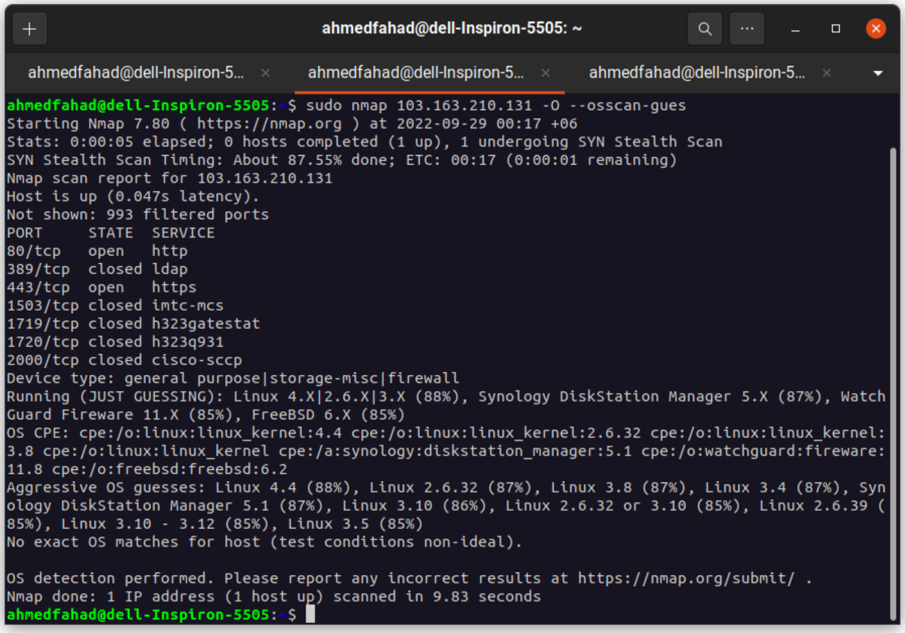
OS Detection

Remote OS Detection (guess aggressively)

OS guesses and fingerprints are shown followed by a percentage in parentheses which specifies how close each match was. OS is detected by **nmap <ip> -O** and **nmap <ip> -O --osscan-guess.**

IP Addresses	OS (Running)	OS (Guess Aggressively)
103.163.210.131 (http://www.kb.gov.bd, http://dmtcl.gov.bd)	**Linux** 4.X|2.6.X|3.X (88%), Synology DiskStation Manager 5.X (87%), WatchGuard Fireware 11.X (85%), FreeBSD 6.X (85%)	**Linux** 4.4 (88%), Linux 2.6.32 (87%), Linux 3.8 (87%), Linux 3.4 (87%), Synology DiskStation Manager 5.1 (87%), Linux 3.10 (86%), Linux 2.6.32 or 3.10 (85%),
103.163.210.127 (http://www.bbs.gov.bd, http://www.bari.gov.bd, http://www.bforest.gov.bd)	**Linux** 3.X|4.X|2.6.X (87%)	**Linux** 3.8 (87%), Linux 4.4 (87%), Linux 2.6.18 - 2.6.22 (86%)
103.230.107.235 (http://www.educationboardresults.gov.bd)	**F5 Networks embedded** (86%), FreeBSD 6.X (85%), OpenBSD 4.X (85%)	**F5 BIG-IP Edge Gateway** (86%), FreeBSD 6.2-RELEASE (85%), OpenBSD 4.0 (85%)
103.48.16.214 (http://www.boi.gov.bd)	Null	**Linksys BEFSR41 EtherFast router (98%)**, Siemens Simatic 300 programmable logic controller (96%),
114.130.119.162 (http://www.joypurhat.gov.bd)		**Linksys BEFSR41 EtherFast router** (98%), Siemens Simatic 300 programmable logic

	Null	controller (96%), D-Link DWL-624+ or DWL-2000AP, or TRENDnet TEW-432BRP WAP (96%)
103.163.210.130 (http://www.banbeis.gov.bd)	**Linux** 3.X|4.X (88%)	**Linux** 3.8 (88%), Linux 4.4 (88%)
3.1.208.233 (https://a2i.gov.bd)	**Crestron** 2-Series (87%), HP embedded (85%)	**Crestron** XPanel control system (87%), HP P2000 G3 NAS device (85%)


ahmedfahad@dell-Inspiron-5505: ~
ahmedfahad@dell-Inspiron-5...
ahmedfahad@dell-Inspiron-5...
ahmedfahad@dell-Inspiron-5...

```
ahmedfahad@dell-Inspiron-5505:~$ sudo nmap 103.163.210.131 -O --osscan-gues
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-29 00:17 +06
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 87.55% done; ETC: 00:17 (0:00:01 remaining)
Nmap scan report for 103.163.210.131
Host is up (0.047s latency).
Not shown: 993 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
Device type: general purpose|storage-misc|firewall
Running (JUST GUESSING): Linux 4.X|2.6.X|3.X (88%), Synology DiskStation Manager 5.X (87%), Watch
Guard Fireware 11.X (85%), FreeBSD 6.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:4.4 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:
3.8 cpe:/o:linux:linux_kernel cpe:/a:synology:diskstation_manager:5.1 cpe:/o:watchguard:fireware:
11.8 cpe:/o:freebsd:freebsd:6.2
Aggressive OS guesses: Linux 4.4 (88%), Linux 2.6.32 (87%), Linux 3.8 (87%), Linux 3.4 (87%), Syn
ology DiskStation Manager 5.1 (87%), Linux 3.10 (86%), Linux 2.6.32 or 3.10 (85%), Linux 2.6.39 (
85%), Linux 3.10 - 3.12 (85%), Linux 3.5 (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 9.83 seconds
ahmedfahad@dell-Inspiron-5505:~$ 
```

Figure 4: OS detection (aggressively)

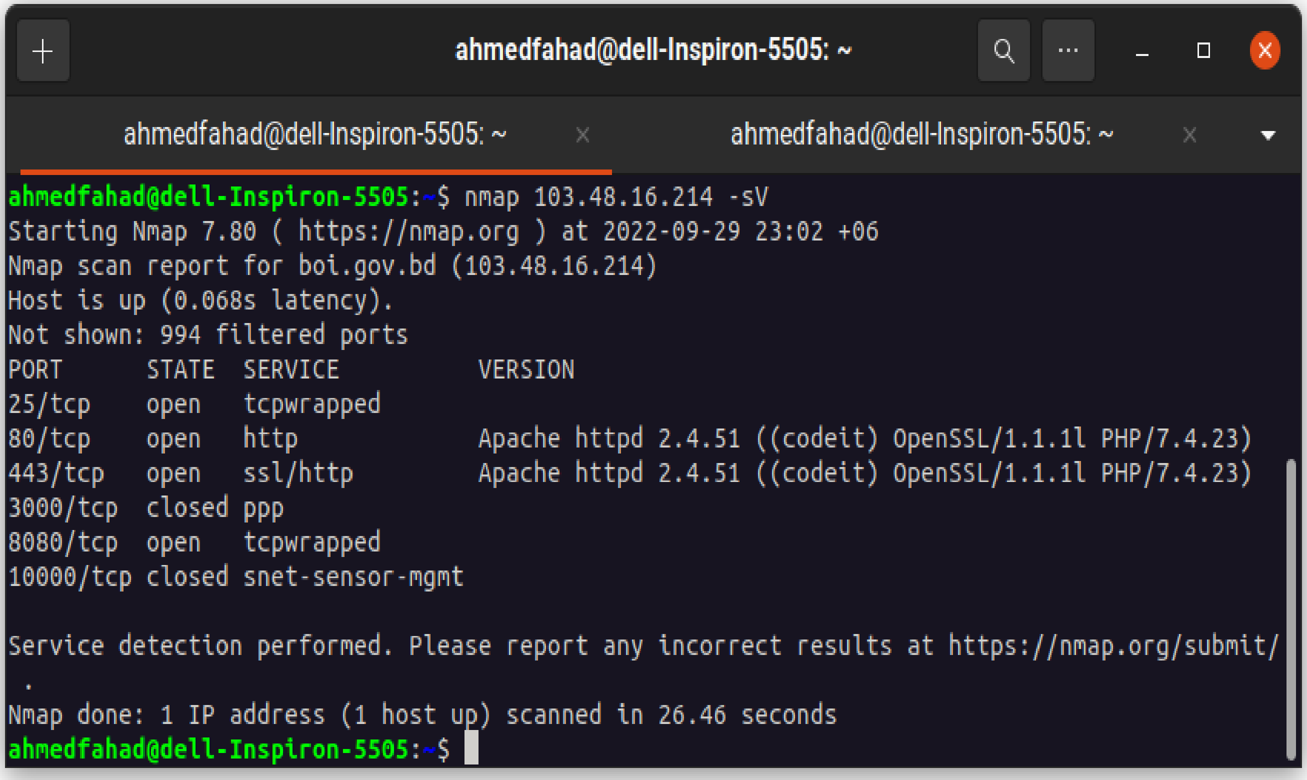
By analyzing the following OS scan information we can infer that in most of the cases we failed to find the exact OS for the given addresses. We obtained the approximate OS and their version from our scanning results. Almost all of them use **Linux** as their core OS.

Service and Version Detection

Explore Version of Running Services

The Nmap version scanning subsystem obtains all of this data by connecting to open ports and interrogating them for further information using probes. We'll run **nmap <ip> -sV** to explore the version of running services on the open ports of IP addresses.

IP Addresses	Services	Version
103.163.210.131 (http://www.kb.gov.bd, http://dmtcl.gov.bd)	http	nginx
	https	nginx
103.163.210.127 (http://www.bbs.gov.bd, http://www.bari.gov.bd, http://www.bforest.gov.bd)	http	nginx
	ssl/https	nginx
103.230.107.235 (http://www.educationboardresults.gov.bd)	http	Apache httpd 2.2.15 ((CentOS))
103.48.16.214 (http://www.boi.gov.bd)	http	Apache httpd 2.4.51 ((codeit) OpenSSL/1.1.1l PHP/7.4.23)
	https	Apache httpd 2.4.51 ((codeit) OpenSSL/1.1.1l PHP/7.4.23)
114.130.119.162 (http://www.joypurhat.gov.bd)	http	nginx
103.163.210.130 (http://www.banbeis.gov.bd)	http	nginx
	ssl/https	nginx
3.1.208.233 (https://a2i.gov.bd)	ssh	OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
	http	Apache httpd 2.4.52 ((Ubuntu))
	ssl/http	Apache httpd 2.4.52 ((Ubuntu))



ahmedfahad@dell-Inspiron-5505: ~
ahmedfahad@dell-Inspiron-5505: ~
ahmedfahad@dell-Inspiron-5505: ~

```
ahmedfahad@dell-Inspiron-5505:~$ nmap 103.48.16.214 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-29 23:02 +06
Nmap scan report for boi.gov.bd (103.48.16.214)
Host is up (0.068s latency).
Not shown: 994 filtered ports
PORT      STATE  SERVICE          VERSION
25/tcp    open   tcpwrapped
80/tcp    open   http             Apache httpd 2.4.51 ((codeit) OpenSSL/1.1.1l PHP/7.4.23)
443/tcp   open   ssl/http         Apache httpd 2.4.51 ((codeit) OpenSSL/1.1.1l PHP/7.4.23)
3000/tcp  closed ppp
8080/tcp  open   tcpwrapped
10000/tcp closed snet-sensor-mgmt

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
 .
Nmap done: 1 IP address (1 host up) scanned in 26.46 seconds
ahmedfahad@dell-Inspiron-5505:~$ 
```

Figure 5: Service and Version detection

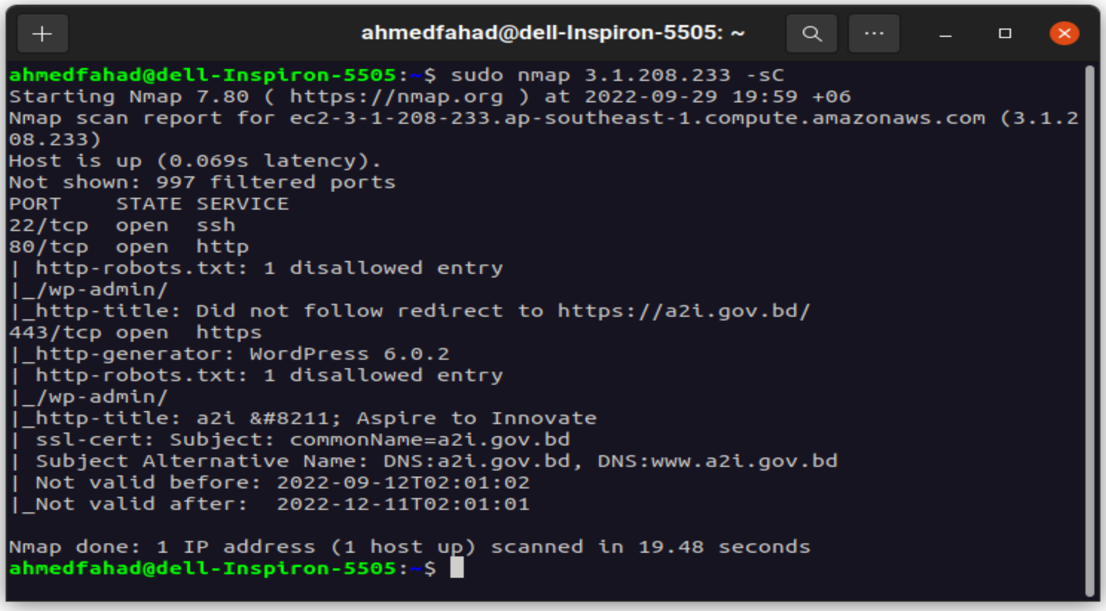
NSE Scripts

Default NSE Scripts Scanning

Nmap contains scripts for brute forcing dozens of protocols, including **http-brute , oracle-brute, snmp-brute** , etc. These scripts are the default set and are run when using the **-sC** or **-A** options rather than listing scripts with **--script** . In this segment, we'll look for ssl certificates, certificate validity, and alternative DNS addresses for the given IP addresses through
nmap <ip> -sC.

IP Addresses	SSL Certificate	Subject Alternative Name	Certificate Validity
103.163.210.131	commonName=*.dgfp.gov.bd	DNS:*.dgfp.gov.bd, DNS:dgfp.gov.bd	2022-11-18
103.163.210.127	commonName=*.portal.gov.bd	DNS:*.portal.gov.bd, DNS:portal.gov.bd	2021-07-14
103.230.107.235	443/tcp closed https		
103.48.16.214	commonName=bida.gov.bd	DNS:bida.gov.bd, DNS:www.bida.gov.bd	2022-12-29
114.130.119.162	443/tcp closed https		
103.163.210.130	commonName=portal.gov.bd	DNS:*.portal.gov.bd, DNS:portal.gov.bd	2022-11-12
3.1.208.233	commonName=a2i.gov.bd	DNS:a2i.gov.bd, DNS:www.a2i.gov.bd	2022-12-11

Among 7 IP addresses, we failed to discover two of the IP addresses as their **https** port is closed.



```
ahmedfahad@dell-Inspiron-5505:~$ sudo nmap 3.1.208.233 -sC
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-29 19:59 +06
Nmap scan report for ec2-3-1-208-233.ap-southeast-1.compute.amazonaws.com (3.1.2
08.233)
Host is up (0.069s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-title: Did not follow redirect to https://a2i.gov.bd/
443/tcp open  https
|_http-generator: WordPress 6.0.2
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-title: a2i &#8211; Aspire to Innovate
| ssl-cert: Subject: commonName=a2i.gov.bd
| Subject Alternative Name: DNS:a2i.gov.bd, DNS:www.a2i.gov.bd
| Not valid before: 2022-09-12T02:01:02
|_Not valid after:  2022-12-11T02:01:01

Nmap done: 1 IP address (1 host up) scanned in 19.48 seconds
ahmedfahad@dell-Inspiron-5505:~$ 
```

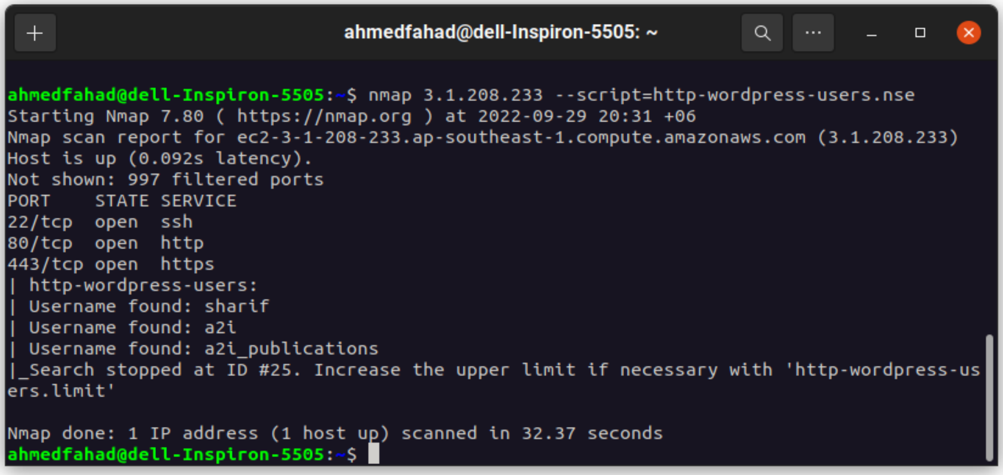
Figure 6: Default NSE Scripts Scanning

Single NSE Script Scan

Here we'll try to execute a single script against different IP addresses according to the info that we've discovered from our previous scanning.

http-wordpress-users.nse

From Default NSE Script Scan, we observe that **http-generator: WordPress 6.0.2** for IP **3.1.208.233**. Therefore we can run a script named **http-wordpress-users.nse** to find the active username for the following IP address.



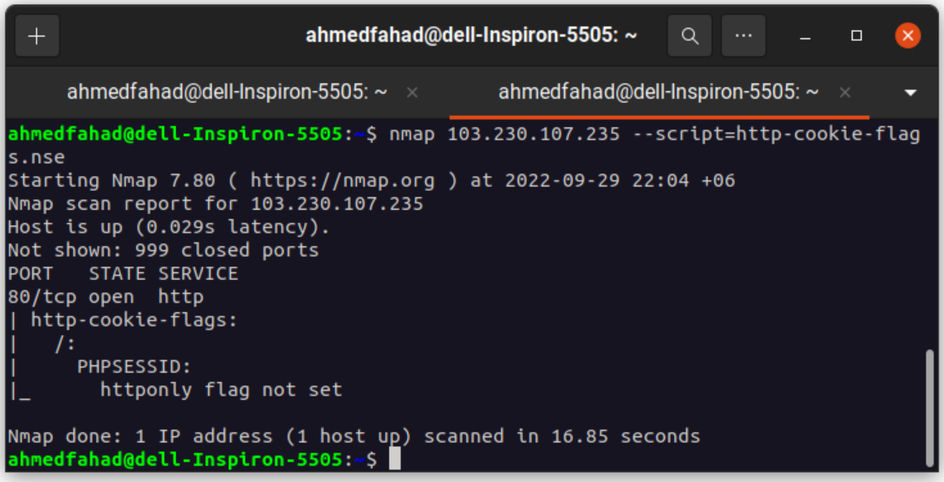
```
ahmedfahad@dell-Inspiron-5505:~$ nmap 3.1.208.233 --script=http-wordpress-users.nse
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-29 20:31 +06
Nmap scan report for ec2-3-1-208-233.ap-southeast-1.compute.amazonaws.com (3.1.208.233)
Host is up (0.092s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
| http-wordpress-users:
| Username found: sharif
| Username found: a2i
| Username found: a2i_publications
|_Search stopped at ID #25. Increase the upper limit if necessary with 'http-wordpress-us
ers.limit'

Nmap done: 1 IP address (1 host up) scanned in 32.37 seconds
ahmedfahad@dell-Inspiron-5505:~$ 
```

Figure 7: Specific Script (http-wordpress-users) Scanning

Following the screenshot of our result, we have got three active wordpress usernames for the given website. Usernames are: **sharif, a2i, a2i_publications.**

http-cookie-flags.nse

We can also scan for http cookie flag using built-in NES script **http-cookie-flags.nse** and the result is as follows:



ahmedfahad@dell-Inspiron-5505: ~
ahmedfahad@dell-Inspiron-5505: ~
ahmedfahad@dell-Inspiron-5505: ~

```
ahmedfahad@dell-Inspiron-5505:~$ nmap 103.230.107.235 --script=http-cookie-flag
s.nse
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-29 22:04 +06
Nmap scan report for 103.230.107.235
Host is up (0.029s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set

Nmap done: 1 IP address (1 host up) scanned in 16.85 seconds
ahmedfahad@dell-Inspiron-5505:~$ 
```

Figure 8: Specific Script (http-cookie-flags) Scanning

According to the scan report, the httponly **flag is not set** in that IP address. According to the Microsoft Developer Network, HttpOnly is an additional flag included in a Set-Cookie HTTP response header. Using the HttpOnly flag when generating a cookie **helps mitigate the risk of client side script** accessing the protected cookie (if the browser supports it). As the flag is not set it is possible that **sensitive information stored in the cookie may be exposed to unintended parties**.

ssl-enum-ciphers.nse

In this address the ssl/http port is open. So, we can try a script **ssl-enum-ciphers.nse** that repeatedly initiates SSLv3/TLS connections, each time trying a **new cipher or compressor** while recording whether a host accepts or rejects it. The end result is a **list of all the ciphersuites and compressors that a server accepts.**

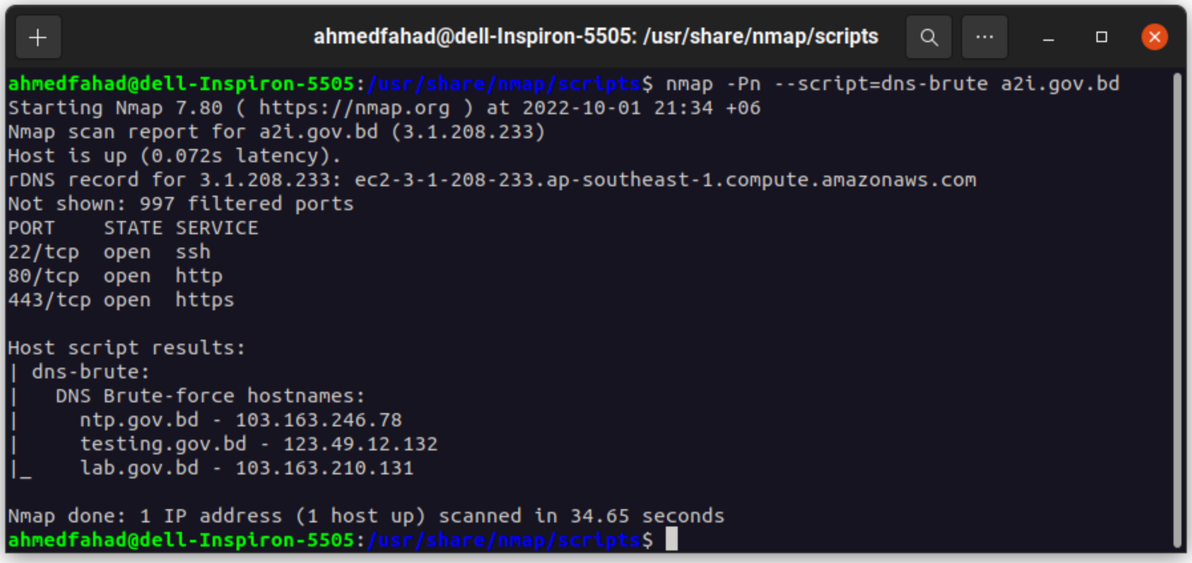
```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-29 22:25 +06
Nmap scan report for boi.gov.bd (103.48.16.214)
Host is up (0.0086s latency).
Not shown: 994 filtered ports
PORT          STATE  SERVICE
```

```
25/tcp  open   smtp
80/tcp  open   http
443/tcp   open   https
| ssl-enum-ciphers:
|   TLSv1.0:
|         ciphers:
|         TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|         TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|         TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 3072) - A
|         TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 3072) - A
|         compressors:
|         NULL
|         cipher preference: server
|         warnings:
|         Key exchange (dh 3072) of lower strength than certificate key
|         Key exchange (ecdh_x25519) of lower strength than certificate key
|   TLSv1.1:
|         ciphers:
|         TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|         TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|         TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 3072) - A
|         TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 3072) - A
|         compressors:
|         NULL
|         cipher preference: server
|         warnings:
|         Key exchange (dh 3072) of lower strength than certificate key
|         Key exchange (ecdh_x25519) of lower strength than certificate key
|   TLSv1.2:
|         ciphers:
|         TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|         TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A
|         TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|         TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (ecdh_x25519) - A
|         TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|         TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|         TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 3072) - A
|         TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 3072) - A
|         compressors:
|         NULL
|         cipher preference: server
|         warnings:
|         Key exchange (dh 3072) of lower strength than certificate key
|           Key exchange (ecdh_x25519) of lower strength than certificate key
|_  least strength: A
3000/tcp  open   ppp
8080/tcp  open   http-proxy
10000/tcp closed snet-sensor-mgmt
```

From the following scanning result, the orange colored text the cipher preferred for that IP. Also we can observe different versions of the ciphers for different TLSv1.n versions.

dns-brute.nse

The dns-brute.nse script attempts to enumerate **DNS hostnames** by brute force guessing of common **subdomains**.



```
ahmedfahad@dell-Inspiron-5505:/usr/share/nmap/scripts$ nmap -Pn --script=dns-brute a2i.gov.bd
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-01 21:34 +06
Nmap scan report for a2i.gov.bd (3.1.208.233)
Host is up (0.072s latency).
rDNS record for 3.1.208.233: ec2-3-1-208-233.ap-southeast-1.compute.amazonaws.com
Not shown: 997 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     ntp.gov.bd - 103.163.246.78
|     testing.gov.bd - 123.49.12.132
|_    lab.gov.bd - 103.163.210.131

Nmap done: 1 IP address (1 host up) scanned in 34.65 seconds
ahmedfahad@dell-Inspiron-5505:/usr/share/nmap/scripts$
```

Figure 9: Specific Script (dns-brute) Scanning

From the search results, its seen that all of these addresses have common dns hostnames and they are **lab.gov.bd - 103.163.210.131, ntp.gov.bd - 103.163.246.78, testing.gov.bd - 123.49.12.132**

Miscellaneous

Site Map Generation

A sitemap generator is a specific type of software that can automatically **create a list of pages that are contained within a website or online application.** By using the command **nmap -Pn --script=http-sitemap-generator <ip>** we get the result as follows:

103.163.210.131

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-29 23:35 +06
Nmap scan report for 103.163.210.131
Host is up (0.011s latency).
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 19.80 seconds
```

103.163.210.127

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-29 23:37 +06
Nmap scan report for bdccl.gov.bd (103.163.210.127)
```

```
Host is up (0.020s latency).
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 16.93 seconds
```

103.230.107.235

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-29 23:40 +06
Nmap scan report for 103.230.107.235
Host is up (0.83s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
| http-sitemap-generator:
|   Directory structure:
|         /
|         Other: 1; php: 2
|         /images/
|         gif: 3; jpg: 1; png: 2
|         /lib/
|         css: 1; js: 2
|   Longest directory structure:
```

```
|         Depth: 1
|         Dir: /lib/
|   Total files found (by extension):
|_        Other: 1; css: 1; gif: 3; jpg: 1; js: 2; php: 2; png: 2

Nmap done: 1 IP address (1 host up) scanned in 22.83 seconds
```

114.130.119.162

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-29 23:44 +06
Nmap scan report for 114.130.119.162
Host is up (0.038s latency).
Not shown: 998 filtered ports
PORT  STATE SERVICE
80/tcp  open  http
| http-sitemap-generator:
|   Directory structure:
|         /backend/backend/auth/
|         Other: 2
|   Longest directory structure:
|         Depth: 3
|         Dir: /backend/backend/auth/
|   Total files found (by extension):
|_        Other: 2
443/tcp open  https
| http-sitemap-generator:
|   Directory structure:
|   Longest directory structure:
|         Depth: 0
|         Dir: /
|   Total files found (by extension):
|_
```

103.48.16.214

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-29 23:41 +06
Nmap scan report for boi.gov.bd (103.48.16.214)
Host is up (0.0088s latency).
Not shown: 994 filtered ports
PORT            STATE  SERVICE
```

```
25/tcp  closed smtp
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:
|   Longest directory structure:
|          Depth: 0
|          Dir: /
|   Total files found (by extension):
|_
3000/tcp  open   ppp
8080/tcp  open   http-proxy
10000/tcp closed snet-sensor-mgmt
```

103.163.210.130

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-29 23:46 +06
Nmap scan report for 103.163.210.130
Host is up (0.054s latency).
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 22.48 seconds
```

3.1.208.233

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-29 23:49 +06
Nmap scan report for ec2-3-1-208-233.ap-southeast-1.compute.amazonaws.com
(3.1.208.233)
Host is up (0.075s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE
22/tcp  open  ssh
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
|         /a2i-publications/
|         Other: 1
|   Longest directory structure:
|         Depth: 1
|         Dir: /a2i-publications/
|   Total files found (by extension):
|_        Other: 2

Nmap done: 1 IP address (1 host up) scanned in 11.55 seconds
```

Output

Nmap scanning results can be represented as normal, xml or grep file format. To implement this query we have to execute **nmap <ip> -oA <filename>.**

gnmap format for IP 3.1.208.233

```
# Nmap 7.80 scan initiated Mon Oct  3 21:56:10 2022 as: nmap -oA 3.1.208.233 3.1.208.233
Host: 3.1.208.233 (ec2-3-1-208-233.ap-southeast-1.compute.amazonaws.com)
Status: Up
Host: 3.1.208.233 (ec2-3-1-208-233.ap-southeast-1.compute.amazonaws.com)
Ports: 22/open/tcp//ssh///, 80/open/tcp//http///, 443/open/tcp//https///    Ignored State: filtered
(997)
# Nmap done at Mon Oct  3 21:56:20 2022 -- 1 IP address (1 host up) scanned in 10.91
seconds
```

xml format for IP 3.1.208.233

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE nmaprun>
<?xml-stylesheet href="file:///usr/bin/../share/nmap/nmap.xsl" type="text/xsl"?>
<!-- Nmap 7.80 scan initiated Mon Oct  3 21:56:10 2022 as: nmap -oA 3.1.208.233
3.1.208.233 -->
<nmaprun scanner="nmap" args="nmap -oA 3.1.208.233 3.1.208.233" start="1664812570"
startstr="Mon Oct  3 21:56:10 2022" version="7.80" xmloutputversion="1.04">
<scaninfo type="connect" protocol="tcp" numservices="1000"
services="1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-1
11,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,280,30
1,306,311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,500,512-51
5,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,646,648,666-668,683,68
7,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,843,873,880,888,898
,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-1011,1021-1100,1102,1104
-1108,1110-1114,1117,1119,1121-1124,1126,1130-1132,1137-1138,1141,1145,1147-1149,1151
-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187,1192,1198-1199,1201,1213,1216-121
8,1233-1234,1236,1244,1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,1309-1311,
1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-1501,1503,1521,1524,15
33,1556,1580,1583,1594,1600,1641,1658,1666,1687-1688,1700,1717-1721,1723,1755,1761,
1782-1783,1801,1805,1812,1839-1840,1862-1864,1875,1900,1914,1935,1947,1971-1972,19
74,1984,1998-2010,2013,2020-2022,2030,2033-2035,2038,2040-2043,2045-2049,2065,2068
,2099-2100,2103,2105-2107,2111,2119,2121,2126,2135,2144,2160-2161,2170,2179,2190-21
91,2196,2200,2222,2251,2260,2288,2301,2323,2366,2381-2383,2393-2394,2399,2401,2492,
2500,2522,2525,2557,2601-2602,2604-2605,2607-2608,2638,2701-2702,2710,2717-2718,27
25,2800,2809,2811,2869,2875,2909-2910,2920,2967-2968,2998,3000-3001,3003,3005-3007,
3011,3013,3017,3030-3031,3052,3071,3077,3128,3168,3211,3221,3260-3261,3268-3269,32
83,3300-3301,3306,3322-3325,3333,3351,3367,3369-3372,3389-3390,3404,3476,3493,3517
,3527,3546,3551,3580,3659,3689-3690,3703,3737,3766,3784,3800-3801,3809,3814,3826-38
```

```
28,3851,3869,3871,3878,3880,3889,3905,3914,3918,3920,3945,3971,3986,3995,3998,4000-
4006,4045,4111,4125-4126,4129,4224,4242,4279,4321,4343,4443-4446,4449,4550,4567,46
62,4848,4899-4900,4998,5000-5004,5009,5030,5033,5050-5051,5054,5060-5061,5080,5087
,5100-5102,5120,5190,5200,5214,5221-5222,5225-5226,5269,5280,5298,5357,5405,5414,54
31-5432,5440,5500,5510,5544,5550,5555,5560,5566,5631,5633,5666,5678-5679,5718,5730,
5800-5802,5810-5811,5815,5822,5825,5850,5859,5862,5877,5900-5904,5906-5907,5910-59
11,5915,5922,5925,5950,5952,5959-5963,5987-5989,5998-6007,6009,6025,6059,6100-6101,
6106,6112,6123,6129,6156,6346,6389,6502,6510,6543,6547,6565-6567,6580,6646,6666-66
69,6689,6692,6699,6779,6788-6789,6792,6839,6881,6901,6969,7000-7002,7004,7007,7019,
7025,7070,7100,7103,7106,7200-7201,7402,7435,7443,7496,7512,7625,7627,7676,7741,77
77-7778,7800,7911,7920-7921,7937-7938,7999-8002,8007-8011,8021-8022,8031,8042,8045,
8080-8090,8093,8099-8100,8180-8181,8192-8194,8200,8222,8254,8290-8292,8300,8333,83
83,8400,8402,8443,8500,8600,8649,8651-8652,8654,8701,8800,8873,8888,8899,8994,9000-
9003,9009-9011,9040,9050,9071,9080-9081,9090-9091,9099-9103,9110-9111,9200,9207,92
20,9290,9415,9418,9485,9500,9502-9503,9535,9575,9593-9595,9618,9666,9876-9878,9898,
9900,9917,9929,9943-9944,9968,9998-10004,10009-10010,10012,10024-10025,10082,1018
0,10215,10243,10566,10616-10617,10621,10626,10628-10629,10778,11110-11111,11967,12
000,12174,12265,12345,13456,13722,13782-13783,14000,14238,14441-14442,15000,15002
-15004,15660,15742,16000-16001,16012,16016,16018,16080,16113,16992-16993,17877,17
988,18040,18101,18988,19101,19283,19315,19350,19780,19801,19842,20000,20005,20031
,20221-20222,20828,21571,22939,23502,24444,24800,25734-25735,26214,27000,27352-27
353,27355-27356,27715,28201,30000,30718,30951,31038,31337,32768-32785,33354,33899
,34571-34573,35500,38292,40193,40911,41511,42510,44176,44442-44443,44501,45100,48
080,49152-49161,49163,49165,49167,49175-49176,49400,49999-50003,50006,50300,50389
,50500,50636,50800,51103,51493,52673,52822,52848,52869,54045,54328,55055-55056,55
555,55600,56737-56738,57294,57797,58080,60020,60443,61532,61900,62078,63331,64623
,64680,65000,65129,65389"/>
<verbose level="0"/>
<debugging level="0"/>
<host starttime="1664812570" endtime="1664812580"><status state="up" reason="syn-ack"
reason_ttl="0"/>
<address addr="3.1.208.233" addrtype="ipv4"/>
<hostnames>
<hostname name="ec2-3-1-208-233.ap-southeast-1.compute.amazonaws.com" type="PTR"/>
</hostnames>
<ports><extraports state="filtered" count="997">
<extrareasons reason="no-responses" count="997"/>
</extraports>
<port protocol="tcp" portid="22"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="ssh" method="table" conf="3"/></port>
<port protocol="tcp" portid="80"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="http" method="table" conf="3"/></port>
<port protocol="tcp" portid="443"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="https" method="table" conf="3"/></port>
</ports>
<times srtt="88451" rttvar="30429" to="210167"/>
</host>
<runstats><finished time="1664812580" timestr="Mon Oct  3 21:56:20 2022" elapsed="10.91"
summary="Nmap done at Mon Oct  3 21:56:20 2022; 1 IP address (1 host up) scanned in
10.91 seconds" exit="success"/><hosts up="1" down="0" total="1"/>
```

```
</runstats>
</nmaprun>
```

nmap format for IP 3.1.208.233

```
# Nmap 7.80 scan initiated Mon Oct  3 21:56:10 2022 as: nmap -oA 3.1.208.233 3.1.208.233
Nmap scan report for ec2-3-1-208-233.ap-southeast-1.compute.amazonaws.com
(3.1.208.233)
Host is up (0.088s latency).
Not shown: 997 filtered ports
PORT  STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

# Nmap done at Mon Oct  3 21:56:20 2022 -- 1 IP address (1 host up) scanned in 10.91
seconds
```