Analyzing websites using Nmap Tool

Abhijit Paul, 1201

<2022-10-02 >

Contents

1 Result of the Analysis

We will note down our important findings in the beginning because results essentially evaluates an experiment or analysis task.

1. SSL Certificate of almost all gov.bd websites will expire in 40 days. As almost all of the .gob.bd subdomains shares a single SSL Certificate of bangavhaban.gov.bd. However, eprocurement have its own SSL-Cert.

2. dhakasouthcity.gov.bd DNS entries are VERY inconsistent. The site or ip has been perhaps moved away to another site called addwire.com but dns query or reverse dns query gives results that shows that it is a functioning subdomain of .gov.bd.

3. eprocure.gov.bd is the most robust and secured .gov.bd website we have found.

4. Most govt servers have almost similar structure of services and ports open.

5. Most govt servers have almost similar version of operating system.

6. They also fall under same IP Block. `(103.163.210.0-255)`

7. All websites uses BDCCL datacenter.

8. All govt sites have Linux 2.6 OS running but Linux 2.6 versions have reached their End-of-life long ago (by 2015) according to Wikipedia .It may be a system level vulnerability.

9. 30 Vulnerabilities were found in dhakasouthcity.gov.bd, 25 of which are due to old SSH version.

2 Target Specification

The following sites were used to perform nmap analysis.

Sitename	IP Address	About
eprocure.gov.bd	103.40.82.19	Electronic Tender
moi.gov.bd	103.163.210.117	Ministry of Information
dhakasouthcity.gov.bd	170.10.162.208	Dhaka South City Corporation
shed.gov.bd	103.163.210.130	Secondary & Higher Secondady Education
bdpost.gov.bd	103.163.210.131	Digital Post Office

3 Scan Techniques

3.1 Scanning TCP Ports

For moi.gov.bd, the following TCP ports were found.

PORT	STATE	SERVICE
111/tcp	open	rpcbind
143/tcp	open	imap
443/tcp	open	https
465/tcp	open	smtps
587/tcp	open	submission
646/tcp	filtered	ldp
993/tcp	open	imaps
995/tcp	open	pop3s
2222/tcp	open	EtherNetIP-1
3306/tcp	open	mysql

For eprocure.gov.bd, the following TCP ports were found.

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https

For shed.gov.bd, the following TCP ports were found.

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

For dhakasouthcity.gov.bd, the following TCP ports were found.

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	filtered	ssh
25/tcp	open	smtp
26/tcp	open	rsftp
53/tcp	open	domain
80/tcp	open	http
110/tcp	open	pop3
111/tcp	open	rpcbind
143/tcp	open	imap
443/tcp	open	https
465/tcp	open	smtps
587/tcp	open	submission
646/tcp	filtered	ldp
993/tcp	open	imaps
995/tcp	open	pop3s
2222/tcp	open	EtherNetIP-1
3306/tcp	open	mysql

For bdpost.gov.bd, the following TCP ports were found.

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

3.2 Scanning Ports using ACK packet

It is a different port scanning as it does not find out whether a port is open or closed. Rather it finds out if the firewall filteres the packets for that port. It sends a empty ACK packet. If the packet goes through firewall and reaches the TCP port, they will return RST packet. If the firewall drops the packet, then no response will arrive. Thus, we can easily identify whether a port is filtered or unfiltered (firewall enabled or not).

We found the following results from TCP ACK scan.

1. moi,bdpost,shed has all ports unfiltered except for http and https.

2. eprocure has all ports filtered.

3. dhakasouthcity wensite is a special case.2 of its ports(ssh,ldp) are filtered. All other ports are unflitered.

3.2.1 Analysis of Output

We did notice one inconsistency here. That is, bdpost.gov.bd ACK scan contains `sip-service` unfiltered while SYN scan does not contain this port. We then looked into why this happened.

Is it due to random chances of unpredictable network condition? So we ran the experiment for the site again.

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

We can see that it was indeed due to random chances. The new TCP SYN scan output contains sip-service.

3.3 Scanning Ports using SYN packet/Stealth Scan

We get the **same output** as TCP Port scan, naturally.
However, we do need to understand that the difference between TCP port scan and SYN scan is that, TCP port scan establishes a connection with the port while TCP Syn only sends SYN packet and receives the SYN-ACK to confirm the TCP port is open. So it is possible to scan thousands of ports per second using this method.
It is called stealth scan because it never completes a full TCP connection. Because of the stealth and fastness of this method, it is the most popular TCP port scanning method.

3.4 Scanning UDP Ports

For eprocure.gov.bd, the following UDP ports were found.

```
All 1000 scanned ports on eprocure.gov.bd (103.40.82.19) are open|filtered
```

For moi.gov.bd, the following UDP ports were found.

PORT	STATE	SERVICE
389/udp	filtered	ldap
1701/udp	filtered	L2TP
1719/udp	filtered	h323gatestat
2000/udp	filtered	cisco-sccp
5060/udp	filtered	sip

For dhakasouthcity.gov.bd, the following UDP ports were found.

PORT	STATE	SERVICE
111/udp	open	rpcbind
137/udp	closed	netbios-ns
161/udp	open	snmp
177/udp	closed	xdmcp
427/udp	closed	svrloc
500/udp	closed	isakmp
520/udp	closed	route
623/udp	closed	asf-rmcp
626/udp	closed	serialnumberd
1645/udp	closed	radius
1812/udp	closed	radius
2049/udp	closed	nfs
5353/udp	closed	zeroconf
10080/udp	closed	amanda
17185/udp	closed	wdbrpc

For shed.gov.bd, the following UDP ports were found.

PORT	STATE	SERVICE
389/udp	filtered	ldap
1701/udp	filtered	L2TP
1719/udp	filtered	h323gatestat
2000/udp	filtered	cisco-sccp
5060/udp	filtered	sip

For bdpost.gov.bd, the following UDP ports were found.

PORT	STATE	SERVICE
389/udp	filtered	ldap
1701/udp	filtered	L2TP
1719/udp	filtered	h323gatestat
2000/udp	filtered	cisco-sccp
5060/udp	filtered	sip

3.4.1 Further Analysis

We found `OPEN|FILTERED` response after scanning UDP ports in eprocure.gov.bd This is a very interesting output. Each UDP protocol has different packet

format and nmap sends empty packets for most services. As a result, the UDP ports will drop the packet. It means, the port is open as no SMTP error message were returned. Or at least it was true in early internet. Nowadays, firewall are used in every server and the firewall can also drop packets. So there is no way to verify whether the packet drop was due to firewall or UDP service. So in 2004, a new version of nmap came out and it defined this new output: OPEN or FILTERED.

This issue can be managed if we send service-specific package instead of empty packets. The UDP port will reply to the packet in this case and thus, we can identify open ports from filtered ports. The service scanning command of nmap (`nmap -sUV -F felix.nmap.org`) sends service-specific packets by default. So we will use that to check if eprocure.gov.bd has any open UDP port.

4 Domain Analysis

Sitename	Domain IP	Extra IP	WhoIS
moi.gov.bd	103.163.210.121	103.163.210.117	BDCCL
bdpost.gov.bd	103.163.210.131	None	N/A
dhakasouthcity.gov.bd	170.10.162.208	None	N/A
eprocure.gov.bd	103.40.82.19	None	N/A
shed.gov.bd	103.163.210.130	None	N/A

For dhakasouthcity, **reverse DNS lookup** gave the following output.

```
170.10.162.208: addwire.com
```

5 Port Specification

We have already found open ports list from Scan Techniques Section. Now we will elaborate on what each of those ports do.

- ftp: File Transfer Protocol Service
- ssh: To remotely access server.

- smtp: Mail Transfer Protocol
- rsftp: Tools for communicating using SSH File Transfer Protocol(SFTP)
- domain: Authentication & Authorization in local network.
- http: Presenting webresource to interent.
- pop3: Old Mail Transfer Protocol
- rpcbind: Necessary for windows process communication between devices.
- imap: Combined with SMTP or pop3, it allows you to read emails.
- https: Secured HTTP
- smtps: SMTP with SSL or TLS cryptographic protocol.
- submission: User AGent for email
- ldp: Protocol to switch between protocols that router uses.
- imaps: IMAP but secured with TLS-SSL layers
- pop3s: POP3 but secured with TLS-SSL layers
- mysql: Database Management Service

6 Service & Version Detection

For bdpost.gov.bd, moi.gov.bd and shed.gov.bd, we were able to find the exact service software of only two service. We were not able to approximate their versions.

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	nginx
443/tcp	open	ssl/http	nginx

For eprocure.gov.bd, we were able to find the exact service-version software of two services.

PORT	STATE	SERVICE	VERSION
80/tcp	open	http-proxy	F5 BIG-IP load balancer http proxy
443/tcp	open	ssl/http	Apache httpd (JSP/2.3)

For dhakasouthcity.gov.bd, we were able to find exact service-version of Many services.

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	Pure-FTPd
22/tcp	filtered	ssh	
26/tcp	open	smtp	Exim smtpd 4.95
53/tcp	open	domain	PowerDNS Authoritative Server 4.4.1
80/tcp	open	http	LiteSpeed
110/tcp	open	pop3	Dovecot pop3d
111/tcp	open	rpcbind	2-4 (RPC #100000)
143/tcp	open	imap	Dovecot imapd
443/tcp	open	ssl	/https LiteSpeed
465/tcp	open	ssl	/smtp Exim smtpd 4.95
587/tcp	open	smtp	Exim smtpd 4.95
646/tcp	filtered	ldp	
995/tcp	open	pop3s	?
2222/tcp	open	ssh	OpenSSH 7.4 (protocol 2.0)
3306/tcp	open	mysql	MySQL 5.7.39-cll-lve

7 OS Detection

Website	OS Guess
shed.gov.bd	Linux 2.6.18 - 2.6.22 (89%)
moi.gov.bd	Linux 2.6.18 - 2.6.22 (89%)
eprocure.gov.bd	Linux 2.6.18 - 2.6.22 (97%)
dhakasouthcity.gov.bd	Linux 3.10 - 4.11 (95%)
bdpost.gov.bd	Linux 2.6.18 - 2.6.22 (89%)

7.1 Analysis

Linux 2.6 versions have reached their End-of-life long ago (by 2015) according to Wikipedia .It may be a system level vulnerability.

8 NSE Scripts

8.1 Default Script

The default script returned the OS version, service list, SSL-Certificate and version that we have already seen. So the outputs won't be recorded in the document but they will be in the experimentaiton folder for the respective sites.

8.2 Sitemap Generator Script

For bdpost.gov.bd,dhakasouthcity.gov.bd,eprocure.gov.bd,moi.gov.bd and shed.gov.bd, no sitemap was found. The system administrators have hidden the structure in their apache configuration file.

```
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
```

8.3 DNS-Brute script

DNS records hold a surprising amount of host information. By brute forcing them we can reveal additional targets.

For shed.gov.bd,bdpost.gov.bd,dhakasouthcity.gov.bd,eprocure.gov.bd,domain.gov.bd, we got the following outputs.

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

8.3.1 What are these Testing, Ntp, Lab servers?

Using `whois` command, we find that-

1. lab.gov.bd belongs to BDCCL. Perhaps it is their lab for govt website as BDCCL seems to be hosting almost all govt websites.

2. ntp.gov.bd belongs to Optimus Technology who has a Tier 3 datacenter in bangladesh.

3. testing.gov.bd brings an interesting result. Perhaps, as APINCC gives IP to all of asia pacific, this IP block happened to land to a chinese

company but we are not too sure about this.

```
China Telecom
descr: No.31,jingrong street
```

9 IDS Evasion

Surprisingly, all IDS script using `-D RND` came out empty. Is it due to random chances? So we ran the command again and indeed, it was due to random chances.

```
abhijit@abhijit-H81M-S2PV:~$ sudo nmap -D RND -sA shed.gov.bd
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-02 14:25 +06
Nmap scan report for shed.gov.bd (103.163.210.130)
Host is up (0.10s 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 9.36 seconds#+end_src
```

Perhaps as the commands were run at night, it was hard to find correct Random ip address to spoof for nmap.