ASSIGNMENT-2

TASK-1:

1. TITLE: Perform scanning on any 3 websites which have open ports

2. OBJECTIVE OF TASK: Scan all 3 targets using the list command and

Scan all 65,535 ports for 3 websites in a single command so that we scan and gather information of targets open ports and many key information of domain

3. STEP BY STEP PROCEDURE:

1. Open the websites below mentioned as target for running the list command.

WEBSITE 1: https://patel-hospital.org.pk

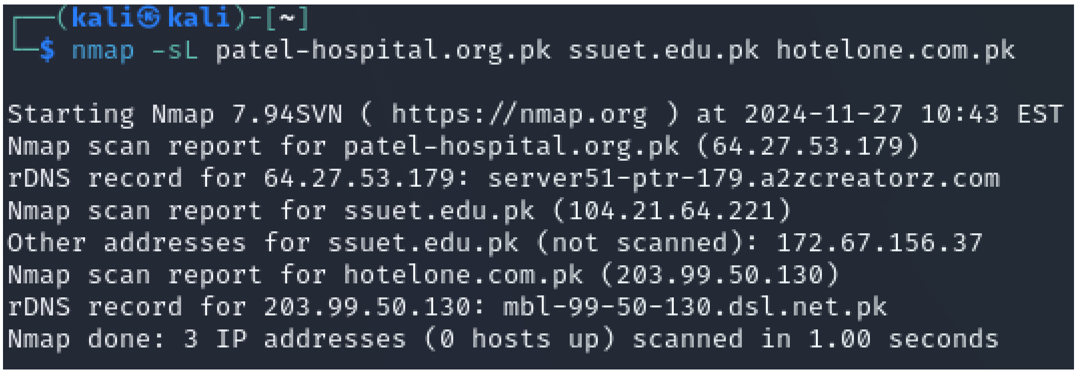
WEBSITE 2: https://www.ssuet.edu.pk

WEBSITE 3: https://www.hotelone.com.pk

2. Now use nmap command with '-sL'to run the list of domains at a time to get information of websites.

SYNTAX: nmap –sL <ip addresses> or <websites url>

USING NMAP AT LIST COMMAND



```
┌──(kali㉿kali)-[~]
└─$ nmap -sL patel-hospital.org.pk ssuet.edu.pk hotelone.com.pk

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-27 10:43 EST
Nmap scan report for patel-hospital.org.pk (64.27.53.179)
rDNS record for 64.27.53.179: server51-ptr-179.a2zcreatorz.com
Nmap scan report for ssuet.edu.pk (104.21.64.221)
Other addresses for ssuet.edu.pk (not scanned): 172.67.156.37
Nmap scan report for hotelone.com.pk (203.99.50.130)
rDNS record for 203.99.50.130: mbl-99-50-130.dsl.net.pk
Nmap done: 3 IP addresses (0 hosts up) scanned in 1.00 seconds
```

3. Here we complete the list command, by this we get ip's, record for dns, and many key information of respective domains we scan

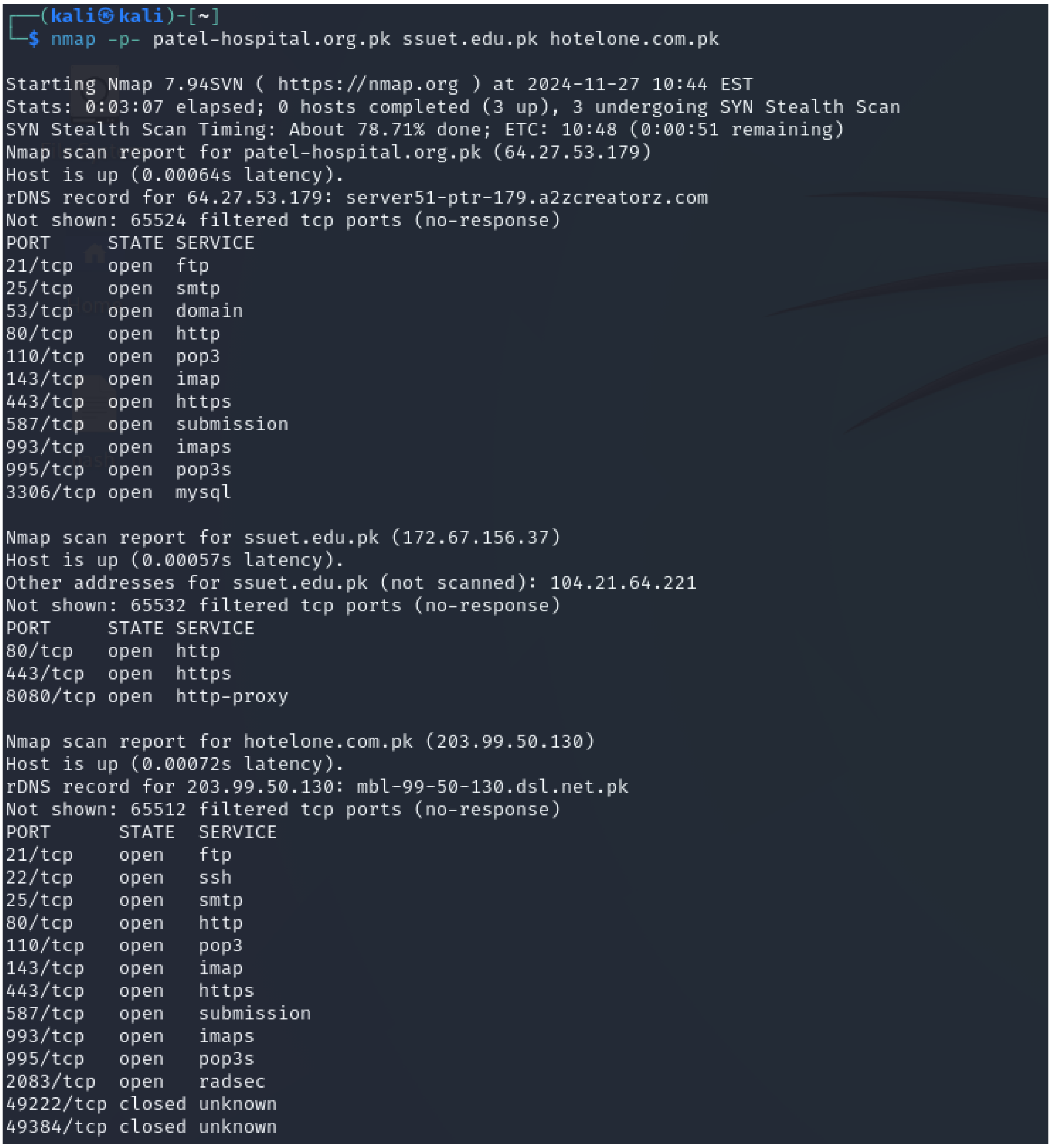
4. Now after we done the scan of all the 65,535 ip addresses to known how many open ports are in the respected domain

5. To done we use nmap command with specify with the '-p-'to scan all the ports

SYNTAX: nmap -p- <ip addresses> or <websites>

6. Now we done the scans successfully then it shows the all ip addresses are in the give domain

USING -P- FOR SCANING ALL THE 63535 PORTS AT ALL THE WEBSITES AT ONCE



```
┌──(kali㉿kali)-[~]
└─$ nmap -p- patel-hospital.org.pk ssuet.edu.pk hotelone.com.pk

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-27 10:44 EST
Stats: 0:03:07 elapsed; 0 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 78.71% done; ETC: 10:48 (0:00:51 remaining)
Nmap scan report for patel-hospital.org.pk (64.27.53.179)
Host is up (0.00064s latency).
rDNS record for 64.27.53.179: server51-ptr-179.a2zcreatorz.com
Not shown: 65524 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
3306/tcp open  mysql

Nmap scan report for ssuet.edu.pk (172.67.156.37)
Host is up (0.00057s latency).
Other addresses for ssuet.edu.pk (not scanned): 104.21.64.221
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Nmap scan report for hotelone.com.pk (203.99.50.130)
Host is up (0.00072s latency).
rDNS record for 203.99.50.130: mbl-99-50-130.dsl.net.pk
Not shown: 65512 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    open   ftp
22/tcp    open   ssh
25/tcp    open   smtp
80/tcp    open   http
110/tcp   open   pop3
143/tcp   open   imap
443/tcp   open   https
587/tcp   open   submission
993/tcp   open   imaps
995/tcp   open   pop3s
2083/tcp  open   radsec
49222/tcp closed unknown
49384/tcp closed unknown
```

5. CONCLUSION: here we done the nmap scan on the targeted websites to get and known about the open ports of the respected websites.

6. SUMMARY OF THE TASK: Here targets are chosen from the internet by selecting from specific google dork and then we open kali Linux and then go to the command prompt enter the details of the specific urls and then we done the list command and all ports scan to identified the open ports and many more details of respected domain

TASK-2:

1. TITLE: Perform different types of scanning method on open ports

2. OBJECTIVE OF THE TASK: The objective is to done the Service Version Scan and Aggressive Scan on the websites to gather information of the websites.

WEBSITE 1: https://patel-hospital.org.pk

WEBSITE 2: https://www.ssuet.edu.pk

WEBSITE 3: https://www.hotelone.com.pk

3. STEP BY STEP PROCEDURE:

1. First select the targets to done the service version scan and Aggressive scan.

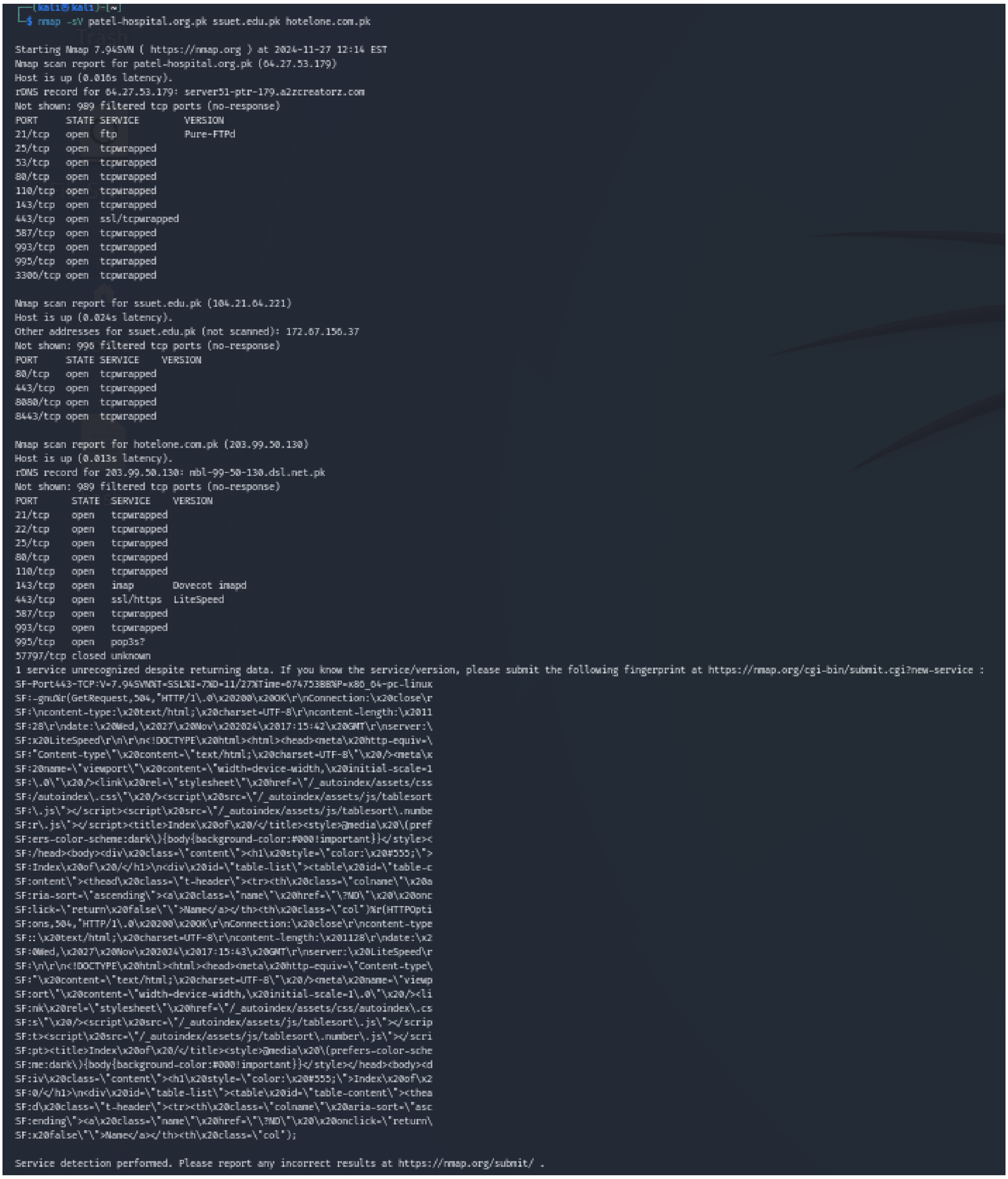
2. Now go to kali Linux and the open command prompt to use nmap command.

3. Now use the nmap with –sV to scan and known the service or port version for information gathering and making payload

SYNTAX: nmap –sV <ip addresses> or <websites url's>

4. By above format we done the scanning and we get the open ports with specific version of the port details.

Service version scan done on all 3 websites



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV patel-hospital.org.pk ssuet.edu.pk hotelone.com.pk

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-27 12:14 EST
Nmap scan report for patel-hospital.org.pk (64.27.53.179)
Host is up (0.016s latency).
rDNS record for 64.27.53.179: server51-ptr-179.a2zcreatorz.com
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE SERVICE        VERSION
21/tcp   open  ftp            Pure-FTPd
25/tcp   open  tcpwrapped
53/tcp   open  tcpwrapped
80/tcp   open  tcpwrapped
110/tcp  open  tcpwrapped
143/tcp  open  tcpwrapped
443/tcp  open  ssl/tcpwrapped
587/tcp  open  tcpwrapped
993/tcp  open  tcpwrapped
995/tcp  open  tcpwrapped
3306/tcp open  tcpwrapped

Nmap scan report for ssuet.edu.pk (104.21.64.221)
Host is up (0.024s latency).
Other addresses for ssuet.edu.pk (not scanned): 172.67.156.37
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
80/tcp   open  tcpwrapped
443/tcp  open  tcpwrapped
8080/tcp open  tcpwrapped
8443/tcp open  tcpwrapped

Nmap scan report for hotelone.com.pk (203.99.50.130)
Host is up (0.013s latency).
rDNS record for 203.99.50.130: mbl-99-50-130.dsl.net.pk
Not shown: 989 filtered tcp ports (no-response)
PORT      STATE  SERVICE    VERSION
21/tcp    open   tcpwrapped
22/tcp    open   tcpwrapped
25/tcp    open   tcpwrapped
80/tcp    open   tcpwrapped
110/tcp   open   tcpwrapped
143/tcp   open   imap       Dovecot imapd
443/tcp   open   ssl/https  LiteSpeed
587/tcp   open   tcpwrapped
993/tcp   open   tcpwrapped
995/tcp   open   pop3s?
57797/tcp closed unknown
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-Port443-TCP:V=7.94SVN%T=SSL%I=7%D=11/27%Time=674753BB%P=x86_64-pc-linux
SF:-gnu%r(GetRequest,504,"HTTP/1\.0\x20200\x20OK\r\nConnection:\x20close\r
SF:\ncontent-type:\x20text/html;\x20charset=UTF-8\r\ncontent-length:\x2011
SF:28\r\ndate:\x20Wed,\x2027\x20Nov\x202024\x2017:15:42\x20GMT\r\nserver:\
SF:x20LiteSpeed\r\n\r\n<!DOCTYPE\x20html><html><head><meta\x20http-equiv=\
SF:"Content-type\"\x20content=\"text/html;\x20charset=UTF-8\"\x20/><meta\x
SF:20name=\"viewport\"\x20content=\"width=device-width,\x20initial-scale=1
SF:\.0\"\x20/><link\x20rel=\"stylesheet\"\x20href=\"/_autoindex/assets/css
SF:/autoindex\.css\"\x20/><script\x20src=\"/_autoindex/assets/js/tablesort
SF:\.js\"></script><script\x20src=\"/_autoindex/assets/js/tablesort\.numbe
SF:r\.js\"></script><title>Index\x20of\x20/</title><style>@media\x20\(pref
SF:ers-color-scheme:dark\){body{background-color:#000!important}}</style><
SF:/head><body><div\x20class=\"content\"><h1\x20style=\"color:\x20#555;\">
SF:Index\x20of\x20/</h1>\n<div\x20id=\"table-list\"><table\x20id=\"table-c
SF:ontent\"><thead\x20class=\"t-header\"><tr><th\x20class=\"colname\"\x20a
SF:ria-sort=\"ascending\"><a\x20class=\"name\"\x20href=\"\?ND\"\x20\x20onc
SF:lick=\"return\x20false\"\">Name</a></th><th\x20class=\"col")%r(HTTPOpti
SF:ons,504,"HTTP/1\.0\x20200\x20OK\r\nConnection:\x20close\r\ncontent-type
SF::\x20text/html;\x20charset=UTF-8\r\ncontent-length:\x201128\r\ndate:\x2
SF:0Wed,\x2027\x20Nov\x202024\x2017:15:43\x20GMT\r\nserver:\x20LiteSpeed\r
SF:\n\r\n<!DOCTYPE\x20html><html><head><meta\x20http-equiv=\"Content-type\
SF:"\x20content=\"text/html;\x20charset=UTF-8\"\x20/><meta\x20name=\"viewp
SF:ort\"\x20content=\"width=device-width,\x20initial-scale=1\.0\"\x20/><li
SF:nk\x20rel=\"stylesheet\"\x20href=\"/_autoindex/assets/css/autoindex\.cs
SF:s\"\x20/><script\x20src=\"/_autoindex/assets/js/tablesort\.js\"></scrip
SF:t><script\x20src=\"/_autoindex/assets/js/tablesort\.number\.js\"></scri
SF:pt><title>Index\x20of\x20/</title><style>@media\x20\(prefers-color-sche
SF:me:dark\){body{background-color:#000!important}}</style></head><body><d
SF:iv\x20class=\"content\"><h1\x20style=\"color:\x20#555;\">Index\x20of\x2
SF:0/</h1>\n<div\x20id=\"table-list\"><table\x20id=\"table-content\"><thea
SF:d\x20class=\"t-header\"><tr><th\x20class=\"colname\"\x20aria-sort=\"asc
SF:ending\"><a\x20class=\"name\"\x20href=\"\?ND\"\x20\x20onclick=\"return\
SF:x20false\"\">Name</a></th><th\x20class=\"col");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

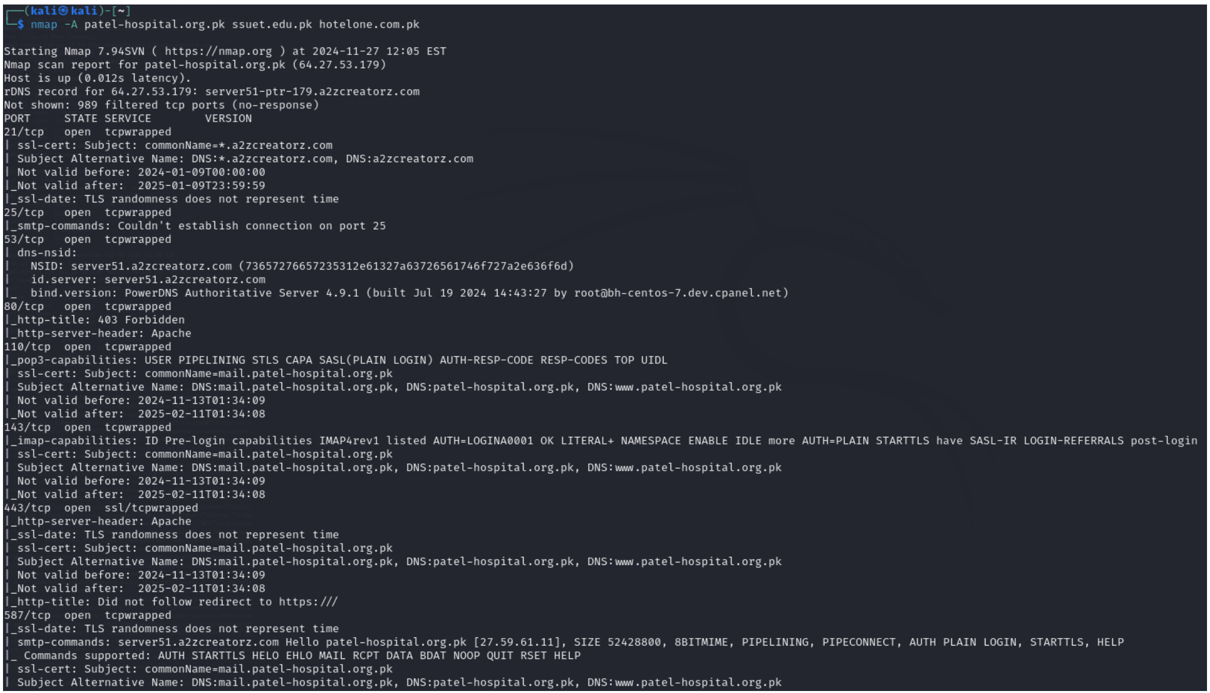
5. Now we done the aggressive scan on the given targets using nmap.

6. Here we done it in kali Linux by using nmap + -A.

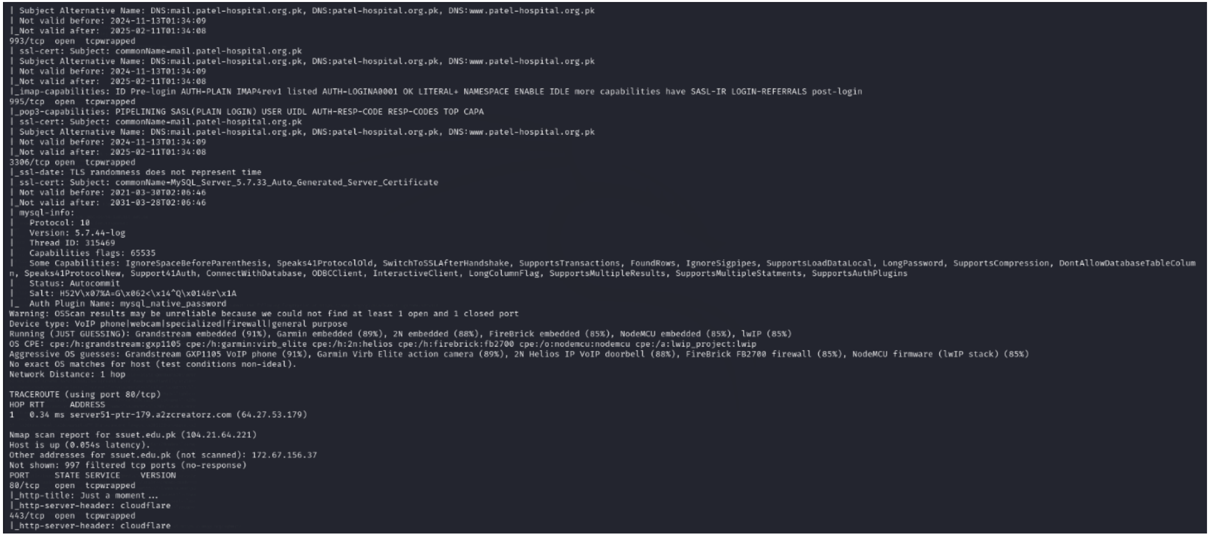
SYNTAX: nmap –A <ip addresses> or <websites url's>

7. now by above format we done the aggressive scan on the mentioned targeted websites

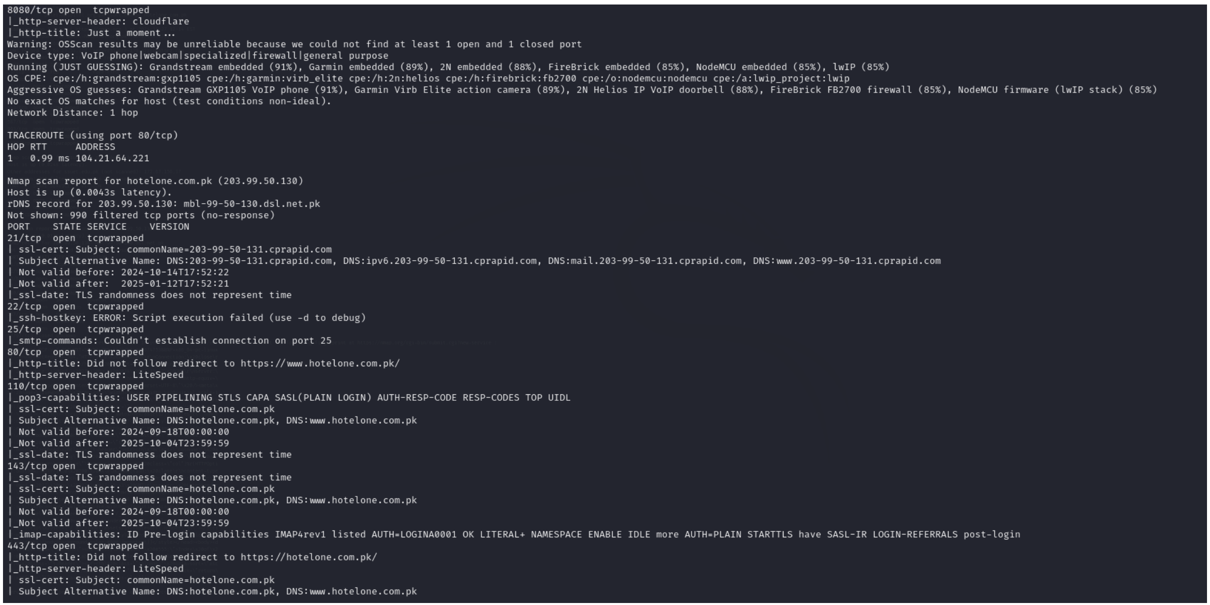
AGGRESSIVE SCAN ON THE 3 WEBSITES



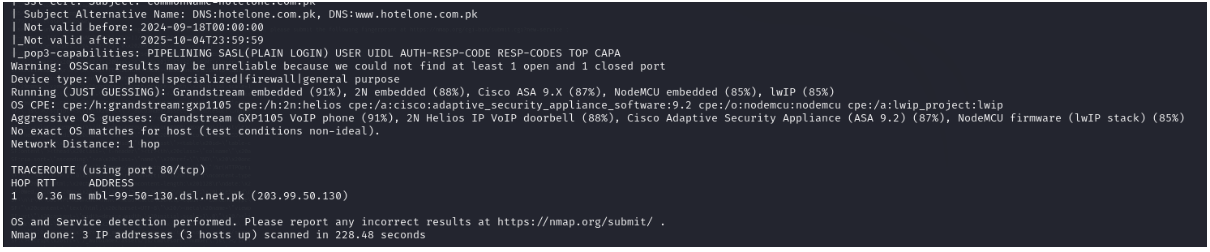
```
┌──(kali㉿kali)-[~]
└─$ nmap -A patel-hospital.org.pk ssuet.edu.pk hotelone.com.pk

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-27 12:05 EST
Nmap scan report for patel-hospital.org.pk (64.27.53.179)
Host is up (0.012s latency).
rDNS record for 64.27.53.179: server51-ptr-179.a2zcreatorz.com
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE SERVICE        VERSION
21/tcp   open  tcpwrapped
| ssl-cert: Subject: commonName=*.a2zcreatorz.com
| Subject Alternative Name: DNS:*.a2zcreatorz.com, DNS:a2zcreatorz.com
| Not valid before: 2024-01-09T00:00:00
|_Not valid after:  2025-01-09T23:59:59
|_ssl-date: TLS randomness does not represent time
25/tcp   open  tcpwrapped
|_smtp-commands: Couldn't establish connection on port 25
53/tcp   open  tcpwrapped
| dns-nsid:
|   NSID: server51.a2zcreatorz.com (736572766572353312e61327a63726561746f727a2e636f6d)
|   id.server: server51.a2zcreatorz.com
|_  bind.version: PowerDNS Authoritative Server 4.9.1 (built Jul 19 2024 14:43:27 by root@bh-centos-7.dev.cpanel.net)
80/tcp   open  tcpwrapped
|_http-title: 403 Forbidden
|_http-server-header: Apache
110/tcp  open  tcpwrapped
|_pop3-capabilities: USER PIPELINING STLS CAPA SASL(PLAIN LOGIN) AUTH-RESP-CODE RESP-CODES TOP UIDL
| ssl-cert: Subject: commonName=mail.patel-hospital.org.pk
| Subject Alternative Name: DNS:mail.patel-hospital.org.pk, DNS:patel-hospital.org.pk, DNS:www.patel-hospital.org.pk
| Not valid before: 2024-11-13T01:34:09
|_Not valid after:  2025-02-11T01:34:08
143/tcp  open  tcpwrapped
|_imap-capabilities: ID Pre-login capabilities IMAP4rev1 listed AUTH=LOGINA0001 OK LITERAL+ NAMESPACE ENABLE IDLE more AUTH=PLAIN STARTTLS have SASL-IR LOGIN-REFERRALS post-login
| ssl-cert: Subject: commonName=mail.patel-hospital.org.pk
| Subject Alternative Name: DNS:mail.patel-hospital.org.pk, DNS:patel-hospital.org.pk, DNS:www.patel-hospital.org.pk
| Not valid before: 2024-11-13T01:34:09
|_Not valid after:  2025-02-11T01:34:08
443/tcp  open  ssl/tcpwrapped
|_http-server-header: Apache
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=mail.patel-hospital.org.pk
| Subject Alternative Name: DNS:mail.patel-hospital.org.pk, DNS:patel-hospital.org.pk, DNS:www.patel-hospital.org.pk
| Not valid before: 2024-11-13T01:34:09
|_Not valid after:  2025-02-11T01:34:08
|_http-title: Did not follow redirect to https:///
587/tcp  open  tcpwrapped
|_ssl-date: TLS randomness does not represent time
| smtp-commands: server51.a2zcreatorz.com Hello patel-hospital.org.pk [27.59.61.11], SIZE 52428800, 8BITMIME, PIPELINING, PIPECONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
| ssl-cert: Subject: commonName=mail.patel-hospital.org.pk
| Subject Alternative Name: DNS:mail.patel-hospital.org.pk, DNS:patel-hospital.org.pk, DNS:www.patel-hospital.org.pk
```



```
| Subject Alternative Name: DNS:mail.patel-hospital.org.pk, DNS:patel-hospital.org.pk, DNS:www.patel-hospital.org.pk
| Not valid before: 2024-11-13T01:34:09
|_Not valid after:  2025-02-11T01:34:08
993/tcp  open  tcpwrapped
| ssl-cert: Subject: commonName=mail.patel-hospital.org.pk
| Subject Alternative Name: DNS:mail.patel-hospital.org.pk, DNS:patel-hospital.org.pk, DNS:www.patel-hospital.org.pk
| Not valid before: 2024-11-13T01:34:09
|_Not valid after:  2025-02-11T01:34:08
|_imap-capabilities: ID Pre-login AUTH-PLAIN IMAP4rev1 listed AUTH-LOGINA0001 OK LITERAL+ NAMESPACE ENABLE IDLE more capabilities have SASL-IR LOGIN-REFERRALS post-login
995/tcp  open  tcpwrapped
|_pop3-capabilities: PIPELINING SASL(PLAIN LOGIN) USER UIDL AUTH-RESP-CODE RESP-CODES TOP CAPA
| ssl-cert: Subject: commonName=mail.patel-hospital.org.pk
| Subject Alternative Name: DNS:mail.patel-hospital.org.pk, DNS:patel-hospital.org.pk, DNS:www.patel-hospital.org.pk
| Not valid before: 2024-11-13T01:34:09
|_Not valid after:  2025-02-11T01:34:08
3306/tcp open  tcpwrapped
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=MySQL_Server_5.7.33_Auto_Generated_Server_Certificate
| Not valid before: 2021-03-30T02:06:46
|_Not valid after:  2031-03-28T02:06:46
| mysql-info:
|   Protocol: 10
|   Version: 5.7.44-log
|   Thread ID: 315469
|   Capabilities flags: 65535
|   Some Capabilities: IgnoreSpaceBeforeParenthesis, Speaks41ProtocolOld, SwitchToSSLAfterHandshake, SupportsTransactions, FoundRows, IgnoreSigpipes, SupportsLoadDataLocal, LongPassword, SupportsCompression, DontAllowDatabaseTableColum
n, Speaks41ProtocolNew, Support41Auth, ConnectWithDatabase, ODBCClient, InteractiveClient, LongColumnFlag, SupportsMultipleResults, SupportsMultipleStatments, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: H52V\x07%A=G\x062<\x14^Q\x014&r\x1A
|_  Auth Plugin Name: mysql_native_password
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP phone|webcam|specialized|firewall|general purpose
Running (JUST GUESSING): Grandstream embedded (91%), Garmin embedded (89%), 2N embedded (88%), FireBrick embedded (85%), NodeMCU embedded (85%), lwIP (85%)
OS CPE: cpe:/h:grandstream:gxp1105 cpe:/h:garmin:virb_elite cpe:/h:2n:helios cpe:/h:firebrick:fb2700 cpe:/o:nodemcu:nodemcu cpe:/a:lwip_project:lwip
Aggressive OS guesses: Grandstream GXP1105 VoIP phone (91%), Garmin Virb Elite action camera (89%), 2N Helios IP VoIP doorbell (88%), FireBrick FB2700 firewall (85%), NodeMCU firmware (lwIP stack) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.34 ms server51-ptr-179.a2zcreatorz.com (64.27.53.179)

Nmap scan report for ssuet.edu.pk (104.21.64.221)
Host is up (0.054s latency).
Other addresses for ssuet.edu.pk (not scanned): 172.67.156.37
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
80/tcp   open  tcpwrapped
|_http-title: Just a moment...
|_http-server-header: cloudflare
443/tcp  open  tcpwrapped
|_http-server-header: cloudflare
```



```
8080/tcp open  tcpwrapped
|_http-server-header: cloudflare
|_http-title: Just a moment...
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP phone|webcam|specialized|firewall|general purpose
Running (JUST GUESSING): Grandstream embedded (91%), Garmin embedded (89%), 2N embedded (88%), FireBrick embedded (85%), NodeMCU embedded (85%), lwIP (85%)
OS CPE: cpe:/h:grandstream:gxp1105 cpe:/h:garmin:virb_elite cpe:/h:2n:helios cpe:/h:firebrick:fb2700 cpe:/o:nodemcu:nodemcu cpe:/a:lwip_project:lwip
Aggressive OS guesses: Grandstream GXP1105 VoIP phone (91%), Garmin Virb Elite action camera (89%), 2N Helios IP VoIP doorbell (88%), FireBrick FB2700 firewall (85%), NodeMCU firmware (lwIP stack) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.99 ms 104.21.64.221

Nmap scan report for hotelone.com.pk (203.99.50.130)
Host is up (0.0043s latency).
rDNS record for 203.99.50.130: mbl-99-50-130.dsl.net.pk
Not shown: 990 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
21/tcp  open  tcpwrapped
| ssl-cert: Subject: commonName=203-99-50-131.cprapid.com
| Subject Alternative Name: DNS:203-99-50-131.cprapid.com, DNS:ipv6.203-99-50-131.cprapid.com, DNS:mail.203-99-50-131.cprapid.com, DNS:www.203-99-50-131.cprapid.com
| Not valid before: 2024-10-14T17:52:22
|_Not valid after:  2025-01-12T17:52:21
|_ssl-date: TLS randomness does not represent time
22/tcp  open  tcpwrapped
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
25/tcp  open  tcpwrapped
|_smtp-commands: Couldn't establish connection on port 25
80/tcp  open  tcpwrapped
|_http-title: Did not follow redirect to https://www.hotelone.com.pk/
|_http-server-header: LiteSpeed
110/tcp open  tcpwrapped
|_pop3-capabilities: USER PIPELINING STLS CAPA SASL(PLAIN LOGIN) AUTH-RESP-CODE RESP-CODES TOP UIDL
| ssl-cert: Subject: commonName=hotelone.com.pk
| Subject Alternative Name: DNS:hotelone.com.pk, DNS:www.hotelone.com.pk
| Not valid before: 2024-09-18T00:00:00
|_Not valid after:  2025-10-04T23:59:59
|_ssl-date: TLS randomness does not represent time
143/tcp open  tcpwrapped
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=hotelone.com.pk
| Subject Alternative Name: DNS:hotelone.com.pk, DNS:www.hotelone.com.pk
| Not valid before: 2024-09-18T00:00:00
|_Not valid after:  2025-10-04T23:59:59
|_imap-capabilities: ID Pre-login capabilities IMAP4rev1 listed AUTH=LOGINA0001 OK LITERAL+ NAMESPACE ENABLE IDLE more AUTH=PLAIN STARTTLS have SASL-IR LOGIN-REFERRALS post-login
443/tcp open  tcpwrapped
|_http-title: Did not follow redirect to https://hotelone.com.pk/
|_http-server-header: LiteSpeed
| ssl-cert: Subject: commonName=hotelone.com.pk
| Subject Alternative Name: DNS:hotelone.com.pk, DNS:www.hotelone.com.pk
```



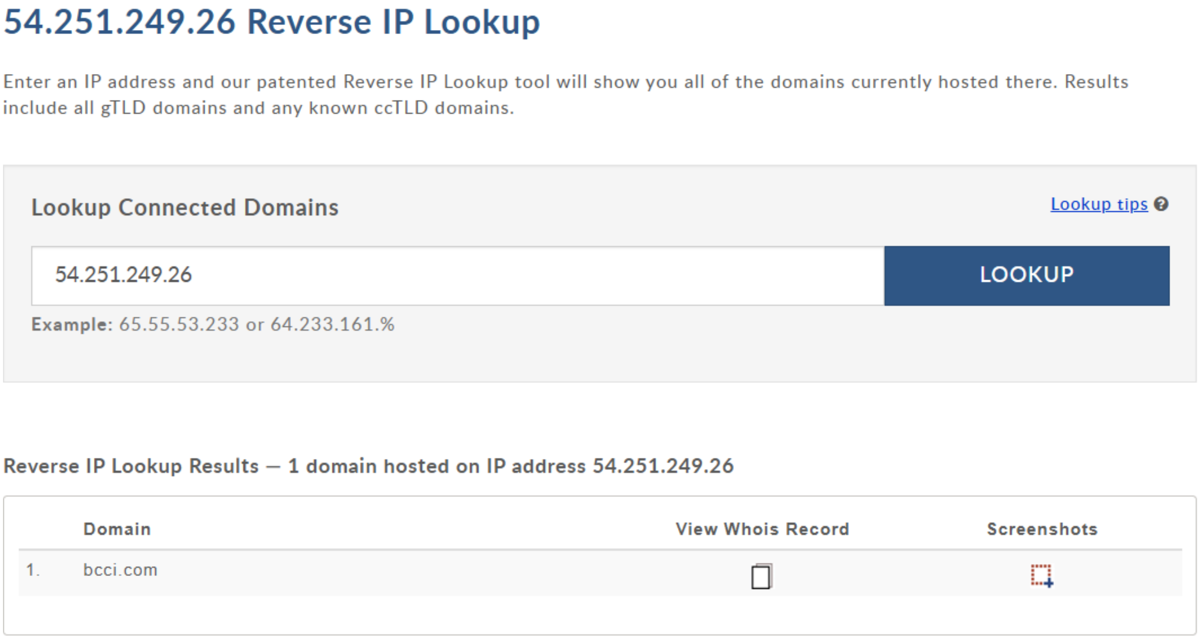
```
| ssl-cert: Subject: commonName=hotelone.com.pk
| Subject Alternative Name: DNS:hotelone.com.pk, DNS:www.hotelone.com.pk
| Not valid before: 2024-09-18T00:00:00
|_Not valid after:  2025-10-04T23:59:59
|_pop3-capabilities: PIPELINING SASL(PLAIN LOGIN) USER UIDL AUTH-RESP-CODE RESP-CODES TOP CAPA
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP phone|specialized|firewall|general purpose
Running (JUST GUESSING): Grandstream embedded (91%), 2N embedded (88%), Cisco ASA 9.X (87%), NodeMCU embedded (85%), lwIP (85%)
OS CPE: cpe:/h:grandstream:gxp1105 cpe:/h:2n:helios cpe:/a:cisco:adaptive_security_appliance_software:9.2 cpe:/o:nodemcu:nodemcu cpe:/a:lwip_project:lwip
Aggressive OS guesses: Grandstream GXP1105 VoIP phone (91%), 2N Helios IP VoIP doorbell (88%), Cisco Adaptive Security Appliance (ASA 9.2) (87%), NodeMCU firmware (lwIP stack) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.36 ms mbl-99-50-130.dsl.net.pk (203.99.50.130)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 3 IP addresses (3 hosts up) scanned in 228.48 seconds
```

8. Now we have another task is to find domain of the give ip addresses.

9. To find it we need to open reverse ip lookup

10. The reason we use the reverse ip lookup for to known the domains which are sharing the ip addresses.

11. Now we enter the ip address in the reverse ip lookup to get the domain name



54.251.249.26 Reverse IP Lookup

Enter an IP address and our patented Reverse IP Lookup tool will show you all of the domains currently hosted there. Results include all gTLD domains and any known ccTLD domains.

Lookup Connected Domains

54.251.249.26

Example: 65.55.53.233 or 64.233.161.%

Reverse IP Lookup Results — 1 domain hosted on IP address 54.251.249.26

	Domain	View Whois Record	Screenshots
1.	bcci.com	☐	⬚

4. CONCLUSION: by this we done the service version scan and aggressive scan of the provided websites.

5. SUMMARY OF THE TASK: first we open the browser and select the targets from internet and then we open kali Linux and done the scans of the targets like service version scan and aggressive scan.

TASK-3:

1. TITLE: Perform Different Enumerations on any Pakistan website

FTP Enumeration, HTTP Enumeration, SSL Enumeration, SMTP Enumeration

2. OBJECTIVE OF THE TASK: the objective is the ftp enumeration, http enumeration, ssl enumeration, smtp enumeration to gather information on these various ports.

3. STEP BY STEP PROCEDURE:

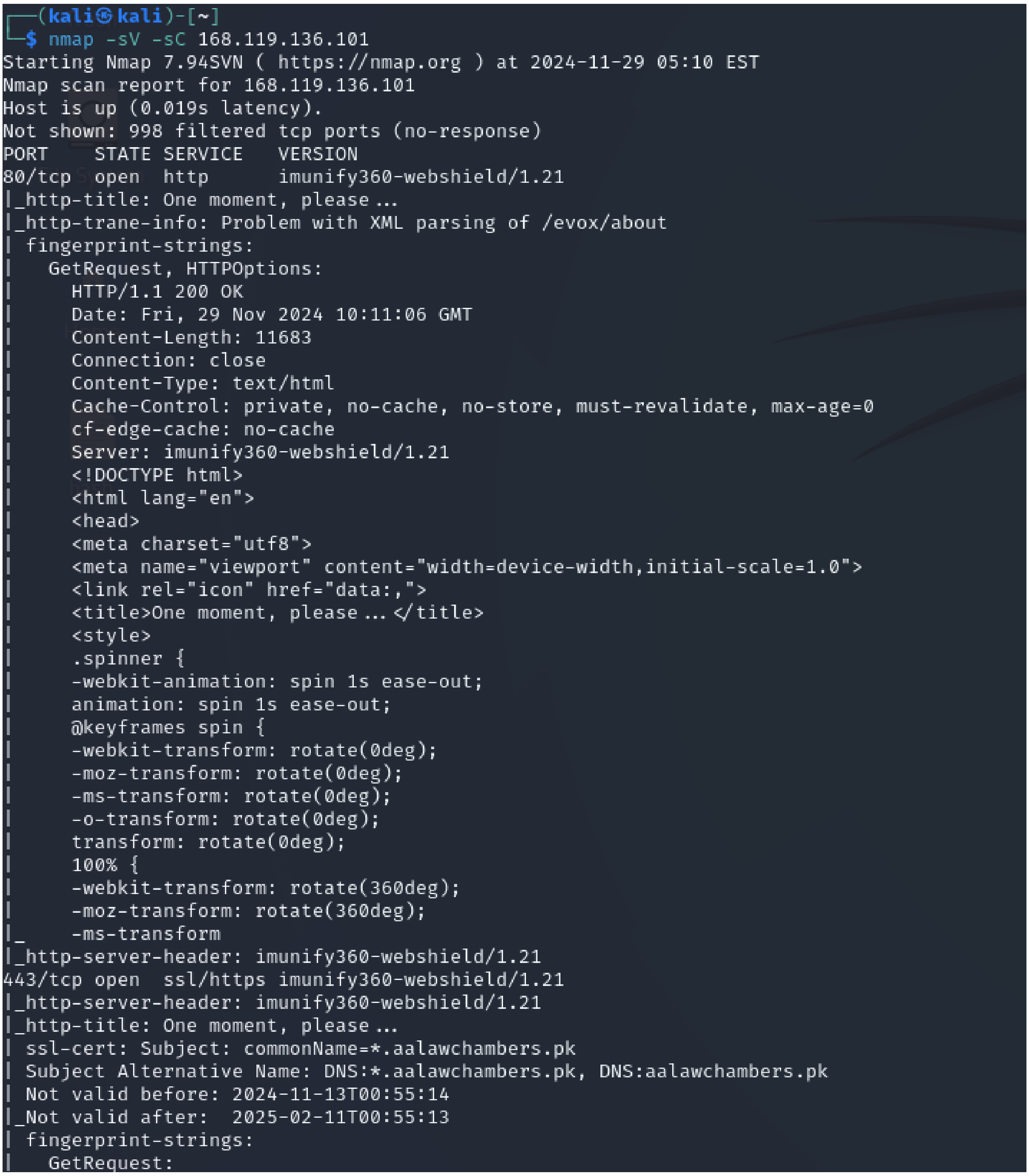
1. Now the get the websites from the internet and note ip for fast enumeration

2. Now note the website ip addresses and add to the kali for ftp enumeration

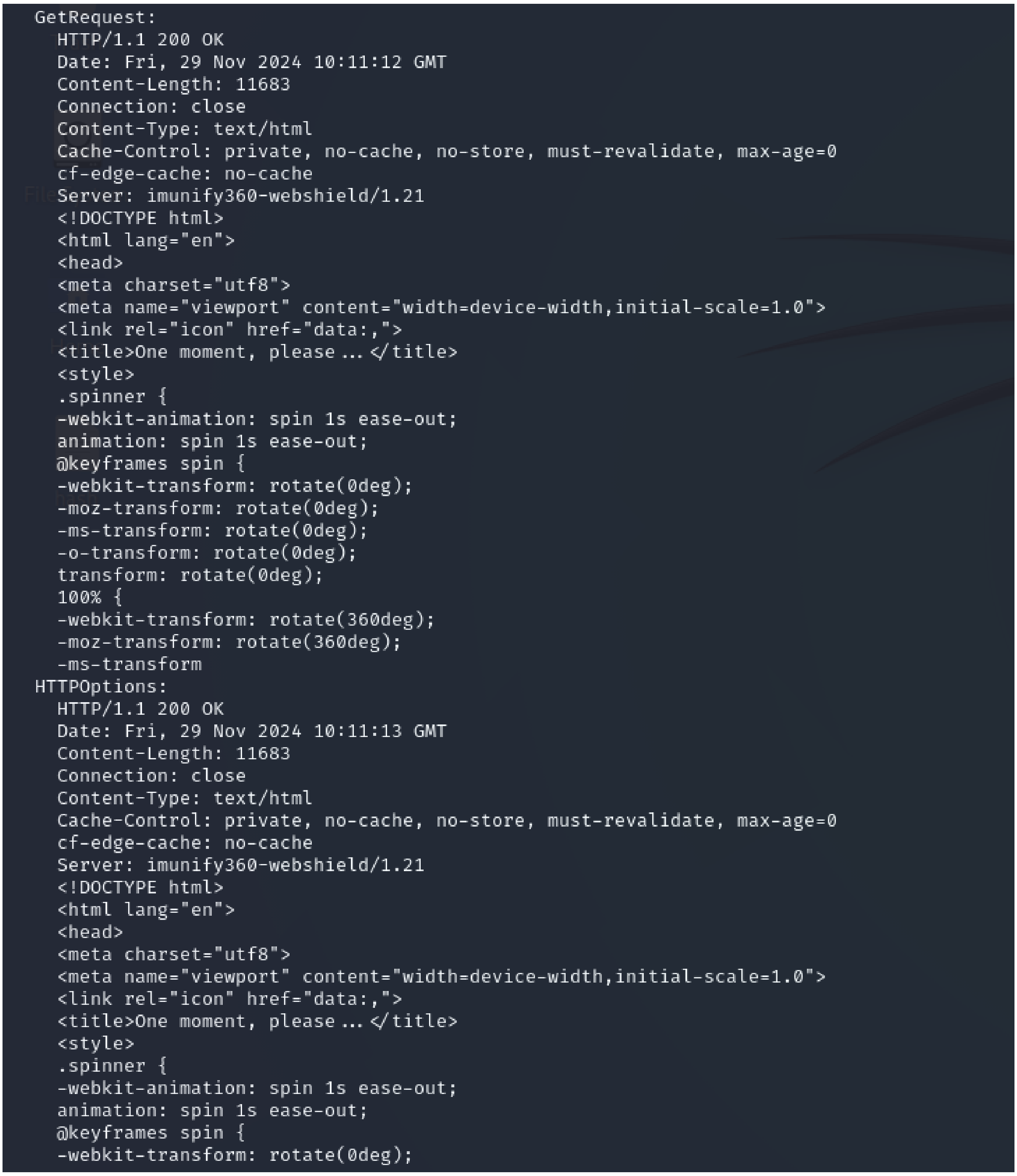
ENUMERTION WEBSITE: https://www.af.org.pk

Here the FTP of enumeration

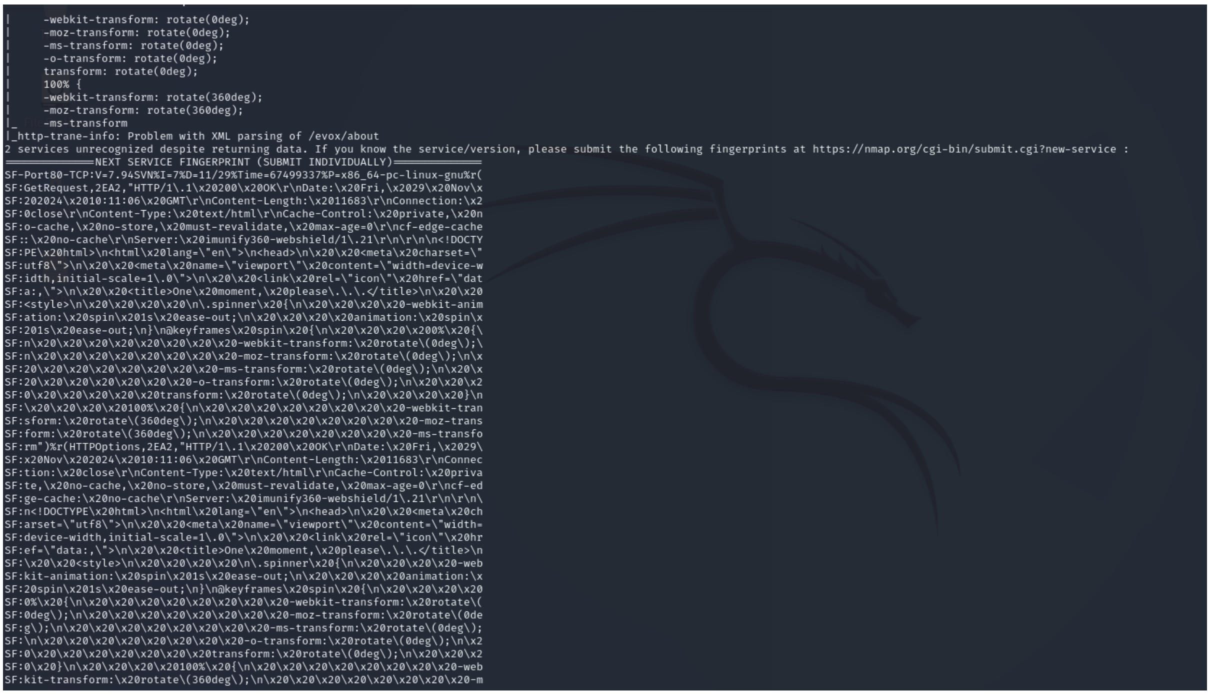
SYNTAX: NMAP –sV –sC <ip addresses>



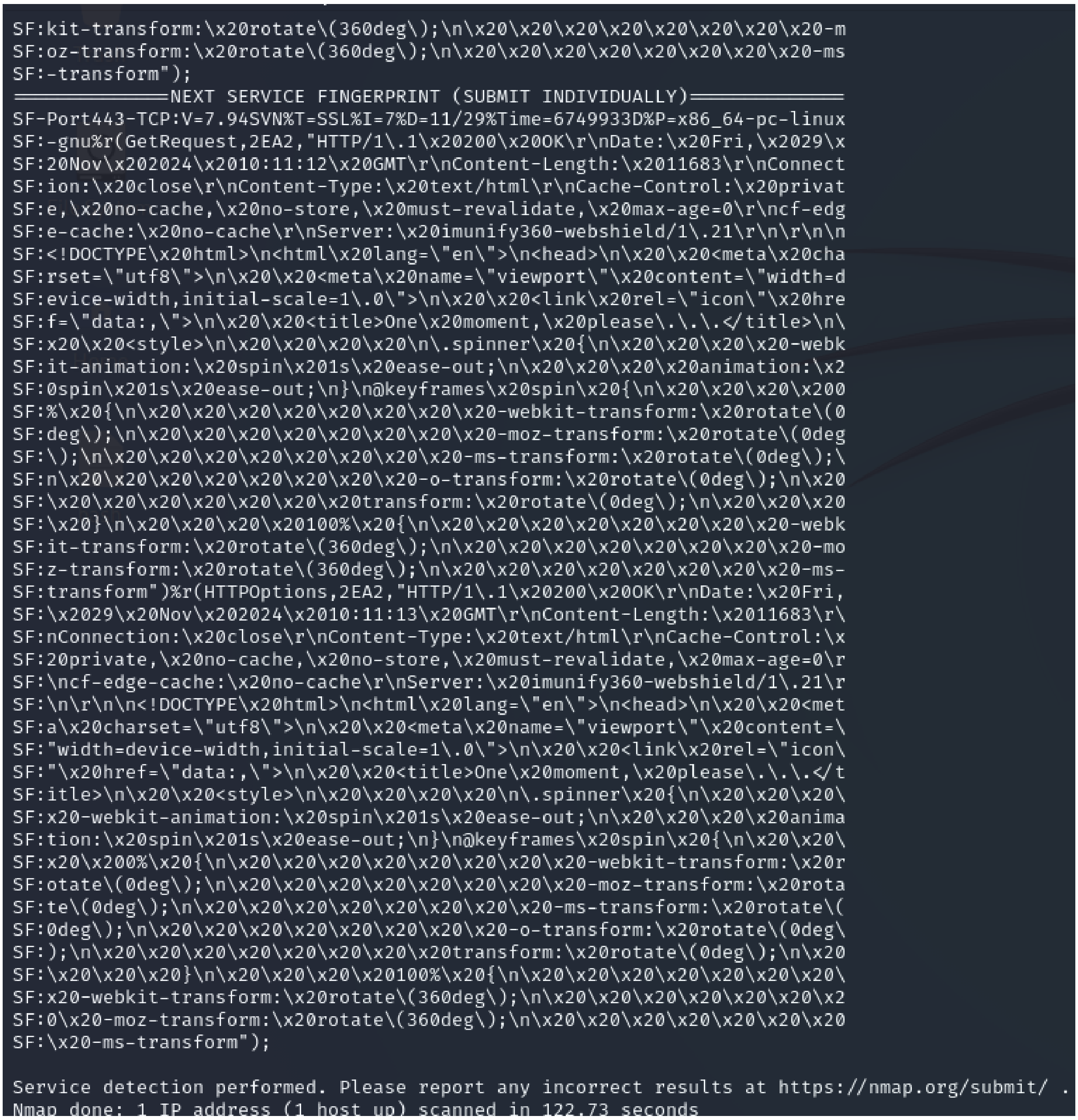
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC 168.119.136.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-29 05:10 EST
Nmap scan report for 168.119.136.101
Host is up (0.019s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE   VERSION
80/tcp  open  http      imunify360-webshield/1.21
|_http-title: One moment, please...
|_http-trane-info: Problem with XML parsing of /evox/about
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.1 200 OK
|     Date: Fri, 29 Nov 2024 10:11:06 GMT
|     Content-Length: 11683
|     Connection: close
|     Content-Type: text/html
|     Cache-Control: private, no-cache, no-store, must-revalidate, max-age=0
|     cf-edge-cache: no-cache
|     Server: imunify360-webshield/1.21
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta charset="utf8">
|     <meta name="viewport" content="width=device-width,initial-scale=1.0">
|     <link rel="icon" href="data:,">
|     <title>One moment, please...</title>
|     <style>
|     .spinner {
|     -webkit-animation: spin 1s ease-out;
|     animation: spin 1s ease-out;
|     @keyframes spin {
|     -webkit-transform: rotate(0deg);
|     -moz-transform: rotate(0deg);
|     -ms-transform: rotate(0deg);
|     -o-transform: rotate(0deg);
|     transform: rotate(0deg);
|     100% {
|     -webkit-transform: rotate(360deg);
|     -moz-transform: rotate(360deg);
|_    -ms-transform
|_http-server-header: imunify360-webshield/1.21
443/tcp open  ssl/https imunify360-webshield/1.21
|_http-server-header: imunify360-webshield/1.21
|_http-title: One moment, please...
| ssl-cert: Subject: commonName=*.aalawchambers.pk
| Subject Alternative Name: DNS:*.aalawchambers.pk, DNS:aalawchambers.pk
| Not valid before: 2024-11-13T00:55:14
|_Not valid after:  2025-02-11T00:55:13
| fingerprint-strings:
|   GetRequest:
```



```
  GetRequest:
    HTTP/1.1 200 OK
    Date: Fri, 29 Nov 2024 10:11:12 GMT
    Content-Length: 11683
    Connection: close
    Content-Type: text/html
    Cache-Control: private, no-cache, no-store, must-revalidate, max-age=0
    cf-edge-cache: no-cache
    Server: imunify360-webshield/1.21
    <!DOCTYPE html>
    <html lang="en">
    <head>
    <meta charset="utf8">
    <meta name="viewport" content="width=device-width,initial-scale=1.0">
    <link rel="icon" href="data:,">
    <title>One moment, please...</title>
    <style>
    .spinner {
    -webkit-animation: spin 1s ease-out;
    animation: spin 1s ease-out;
    @keyframes spin {
    -webkit-transform: rotate(0deg);
    -moz-transform: rotate(0deg);
    -ms-transform: rotate(0deg);
    -o-transform: rotate(0deg);
    transform: rotate(0deg);
    100% {
    -webkit-transform: rotate(360deg);
    -moz-transform: rotate(360deg);
    -ms-transform
  HTTPOptions:
    HTTP/1.1 200 OK
    Date: Fri, 29 Nov 2024 10:11:13 GMT
    Content-Length: 11683
    Connection: close
    Content-Type: text/html
    Cache-Control: private, no-cache, no-store, must-revalidate, max-age=0
    cf-edge-cache: no-cache
    Server: imunify360-webshield/1.21
    <!DOCTYPE html>
    <html lang="en">
    <head>
    <meta charset="utf8">
    <meta name="viewport" content="width=device-width,initial-scale=1.0">
    <link rel="icon" href="data:,">
    <title>One moment, please...</title>
    <style>
    .spinner {
    -webkit-animation: spin 1s ease-out;
    animation: spin 1s ease-out;
    @keyframes spin {
    -webkit-transform: rotate(0deg);
```



```
|     -webkit-transform: rotate(0deg);
|     -moz-transform: rotate(0deg);
|     -ms-transform: rotate(0deg);
|     -o-transform: rotate(0deg);
|     transform: rotate(0deg);
|     100% {
|     -webkit-transform: rotate(360deg);
|     -moz-transform: rotate(360deg);
|_    -ms-transform
|_http-trane-info: Problem with XML parsing of /evox/about
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.94SVN%I=7%D=11/29%Time=67499337%P=x86_64-pc-linux-gnu%r(
SF:GetRequest,2EA2,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Fri,\x2029\x20Nov\x
SF:202024\x2010:11:06\x20GMT\r\nContent-Length:\x2011683\r\nConnection:\x2
SF:0close\r\nContent-Type:\x20text/html\r\nCache-Control:\x20private,\x20n
SF:o-cache,\x20no-store,\x20must-revalidate,\x20max-age=0\r\ncf-edge-cache
SF::\x20no-cache\r\nServer:\x20imunify360-webshield/1\.21\r\n\r\n\n<!DOCTY
SF:PE\x20html>\n<html\x20lang=\"en\">\n<head>\n\x20\x20<meta\x20charset=\"
SF:utf8\">\n\x20\x20<meta\x20name=\"viewport\"\x20content=\"width=device-w
SF:idth,initial-scale=1\.0\">\n\x20\x20<link\x20rel=\"icon\"\x20href=\"dat
SF:a:,\">\n\x20\x20<title>One\x20moment,\x20please\.\.\.</title>\n\x20\x20
SF:<style>\n\x20\x20\x20\x20\n\.spinner\x20{\n\x20\x20\x20\x20-webkit-anim
SF:ation:\x20spin\x201s\x20ease-out;\n\x20\x20\x20\x20animation:\x20spin\x
SF:201s\x20ease-out;\n}\n@keyframes\x20spin\x20{\n\x20\x20\x20\x200%\x20{\
SF:n\x20\x20\x20\x20\x20\x20\x20\x20-webkit-transform:\x20rotate\(0deg\);\
SF:n\x20\x20\x20\x20\x20\x20\x20\x20-moz-transform:\x20rotate\(0deg\);\n\x
SF:20\x20\x20\x20\x20\x20\x20\x20-ms-transform:\x20rotate\(0deg\);\n\x20\x
SF:20\x20\x20\x20\x20\x20\x20-o-transform:\x20rotate\(0deg\);\n\x20\x20\x2
SF:0\x20\x20\x20\x20\x20transform:\x20rotate\(0deg\);\n\x20\x20\x20\x20}\n
SF:\x20\x20\x20\x20100%\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20-webkit-tran
SF:sform:\x20rotate\(360deg\);\n\x20\x20\x20\x20\x20\x20\x20\x20-moz-trans
SF:form:\x20rotate\(360deg\);\n\x20\x20\x20\x20\x20\x20\x20\x20-ms-transfo
SF:rm")%r(HTTPOptions,2EA2,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Fri,\x2029\
SF:x20Nov\x202024\x2010:11:06\x20GMT\r\nContent-Length:\x2011683\r\nConnec
SF:tion:\x20close\r\nContent-Type:\x20text/html\r\nCache-Control:\x20priva
SF:te,\x20no-cache,\x20no-store,\x20must-revalidate,\x20max-age=0\r\ncf-ed
SF:ge-cache:\x20no-cache\r\nServer:\x20imunify360-webshield/1\.21\r\n\r\n\
SF:n<!DOCTYPE\x20html>\n<html\x20lang=\"en\">\n<head>\n\x20\x20<meta\x20ch
SF:arset=\"utf8\">\n\x20\x20<meta\x20name=\"viewport\"\x20content=\"width=
SF:device-width,initial-scale=1\.0\">\n\x20\x20<link\x20rel=\"icon\"\x20hr
SF:ef=\"data:,\">\n\x20\x20<title>One\x20moment,\x20please\.\.\.</title>\n
SF:\x20\x20<style>\n\x20\x20\x20\x20\n\.spinner\x20{\n\x20\x20\x20\x20-web
SF:kit-animation:\x20spin\x201s\x20ease-out;\n\x20\x20\x20\x20animation:\x
SF:20spin\x201s\x20ease-out;\n}\n@keyframes\x20spin\x20{\n\x20\x20\x20\x20
SF:0%\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20-webkit-transform:\x20rotate\(
SF:0deg\);\n\x20\x20\x20\x20\x20\x20\x20\x20-moz-transform:\x20rotate\(0de
SF:g\);\n\x20\x20\x20\x20\x20\x20\x20\x20-ms-transform:\x20rotate\(0deg\);
SF:\n\x20\x20\x20\x20\x20\x20\x20\x20-o-transform:\x20rotate\(0deg\);\n\x2
SF:0\x20\x20\x20\x20\x20\x20\x20transform:\x20rotate\(0deg\);\n\x20\x20\x2
SF:0\x20}\n\x20\x20\x20\x20100%\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20-web
SF:kit-transform:\x20rotate\(360deg\);\n\x20\x20\x20\x20\x20\x20\x20\x20-m
```



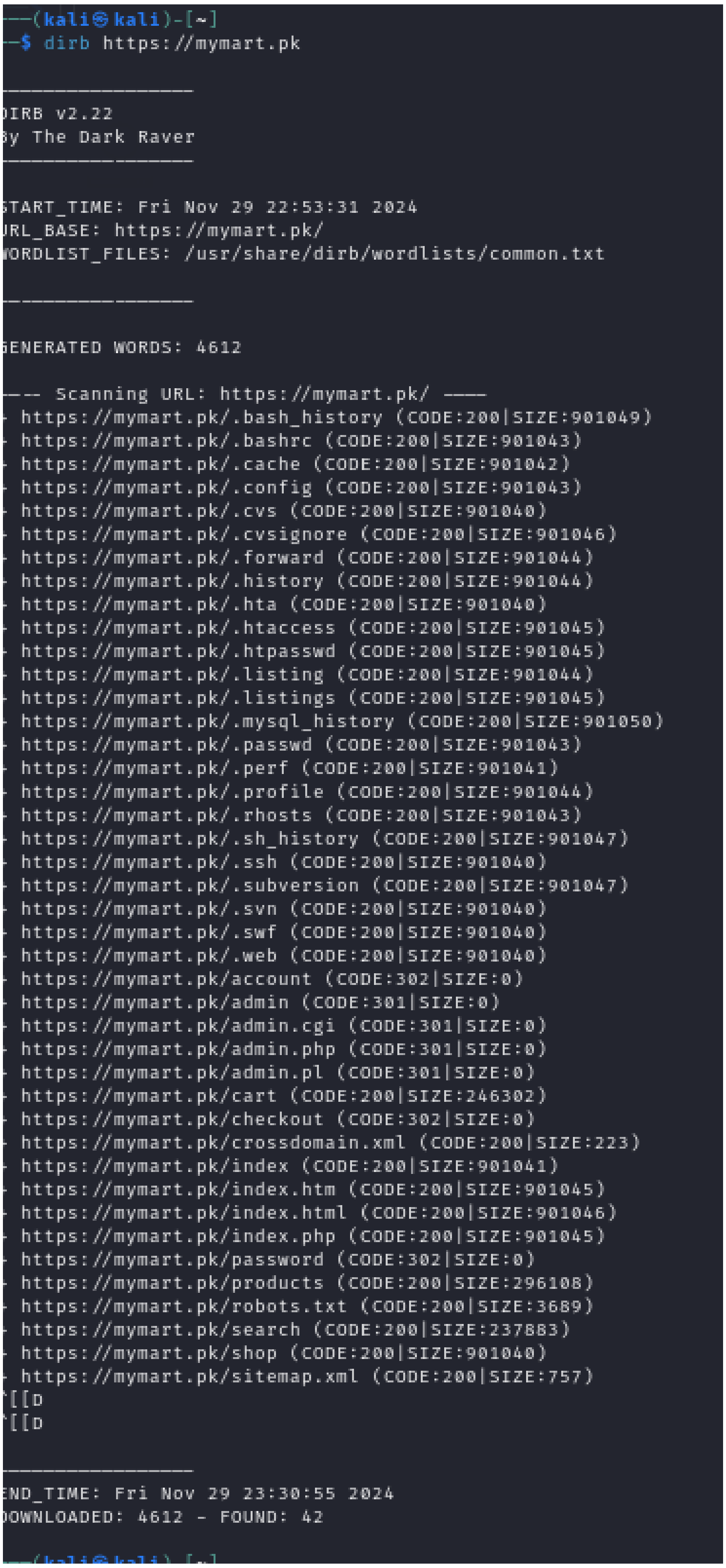
```
SF:kit-transform:\x20rotate\(360deg\);\n\x20\x20\x20\x20\x20\x20\x20\x20-m
SF:oz-transform:\x20rotate\(360deg\);\n\x20\x20\x20\x20\x20\x20\x20\x20-ms
SF:-transform");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=7.94SVN%T=SSL%I=7%D=11/29%Time=6749933D%P=x86_64-pc-linux
SF:-gnu%r(GetRequest,2EA2,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Fri,\x2029\x
SF:20Nov\x202024\x2010:11:12\x20GMT\r\nContent-Length:\x2011683\r\nConnect
SF:ion:\x20close\r\nContent-Type:\x20text/html\r\nCache-Control:\x20privat
SF:e,\x20no-cache,\x20no-store,\x20must-revalidate,\x20max-age=0\r\ncf-edg
SF:e-cache:\x20no-cache\r\nServer:\x20imunify360-webshield/1\.21\r\n\r\n\n
SF:<!DOCTYPE\x20html>\n<html\x20lang=\"en\">\n<head>\n\x20\x20<meta\x20cha
SF:rset=\"utf8\">\n\x20\x20<meta\x20name=\"viewport\"\x20content=\"width=d
SF:evice-width,initial-scale=1\.0\">\n\x20\x20<link\x20rel=\"icon\"\x20hre
SF:f=\"data:,\">\n\x20\x20<title>One\x20moment,\x20please\.\.\.</title>\n\
SF:x20\x20<style>\n\x20\x20\x20\x20\n\.spinner\x20{\n\x20\x20\x20\x20-webk
SF:it-animation:\x20spin\x201s\x20ease-out;\n\x20\x20\x20\x20animation:\x2
SF:0spin\x201s\x20ease-out;\n}\n@keyframes\x20spin\x20{\n\x20\x20\x20\x200
SF:%\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20-webkit-transform:\x20rotate\(0
SF:deg\);\n\x20\x20\x20\x20\x20\x20\x20\x20-moz-transform:\x20rotate\(0deg
SF:\);\n\x20\x20\x20\x20\x20\x20\x20\x20-ms-transform:\x20rotate\(0deg\);\
SF:n\x20\x20\x20\x20\x20\x20\x20\x20-o-transform:\x20rotate\(0deg\);\n\x20
SF:\x20\x20\x20\x20\x20\x20\x20transform:\x20rotate\(0deg\);\n\x20\x20\x20
SF:\x20}\n\x20\x20\x20\x20100%\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20-webk
SF:it-transform:\x20rotate\(360deg\);\n\x20\x20\x20\x20\x20\x20\x20\x20-mo
SF:z-transform:\x20rotate\(360deg\);\n\x20\x20\x20\x20\x20\x20\x20\x20-ms-
SF:transform")%r(HTTPOptions,2EA2,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Fri,
SF:\x2029\x20Nov\x202024\x2010:11:13\x20GMT\r\nContent-Length:\x2011683\r\
SF:nConnection:\x20close\r\nContent-Type:\x20text/html\r\nCache-Control:\x
SF:20private,\x20no-cache,\x20no-store,\x20must-revalidate,\x20max-age=0\r
SF:\ncf-edge-cache:\x20no-cache\r\nServer:\x20imunify360-webshield/1\.21\r
SF:\n\r\n\n<!DOCTYPE\x20html>\n<html\x20lang=\"en\">\n<head>\n\x20\x20<met
SF:a\x20charset=\"utf8\">\n\x20\x20<meta\x20name=\"viewport\"\x20content=\
SF:"width=device-width,initial-scale=1\.0\">\n\x20\x20<link\x20rel=\"icon\
SF:"\x20href=\"data:,\">\n\x20\x20<title>One\x20moment,\x20please\.\.\.</t
SF:itle>\n\x20\x20<style>\n\x20\x20\x20\x20\n\.spinner\x20{\n\x20\x20\x20\
SF:x20-webkit-animation:\x20spin\x201s\x20ease-out;\n\x20\x20\x20\x20anima
SF:tion:\x20spin\x201s\x20ease-out;\n}\n@keyframes\x20spin\x20{\n\x20\x20\
SF:x20\x200%\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20-webkit-transform:\x20r
SF:otate\(0deg\);\n\x20\x20\x20\x20\x20\x20\x20\x20-moz-transform:\x20rota
SF:te\(0deg\);\n\x20\x20\x20\x20\x20\x20\x20\x20-ms-transform:\x20rotate\(
SF:0deg\);\n\x20\x20\x20\x20\x20\x20\x20\x20-o-transform:\x20rotate\(0deg\
SF:);\n\x20\x20\x20\x20\x20\x20\x20\x20transform:\x20rotate\(0deg\);\n\x20
SF:\x20\x20\x20}\n\x20\x20\x20\x20100%\x20{\n\x20\x20\x20\x20\x20\x20\x20\
SF:x20-webkit-transform:\x20rotate\(360deg\);\n\x20\x20\x20\x20\x20\x20\x2
SF:0\x20-moz-transform:\x20rotate\(360deg\);\n\x20\x20\x20\x20\x20\x20\x20
SF:\x20-ms-transform");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 122.73 seconds
```

3. Https enumeration done by using the various commands

4. By this we get more details of the system HTTPS and extension webs

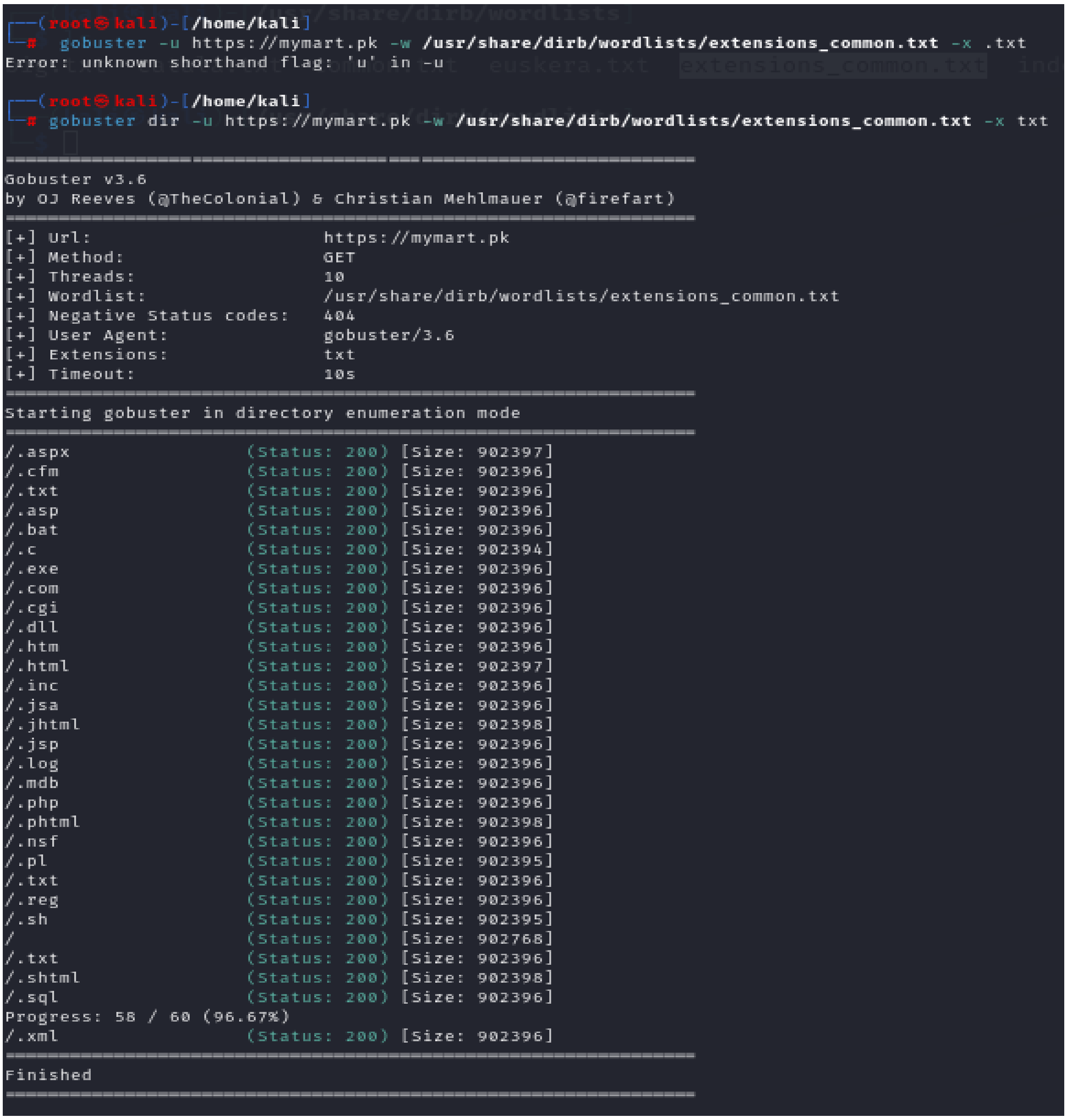
5. Here I use drib gets all the extension website urls in the websites

HTTPS ENUMERATION:



```
┌──(kali㉿kali)-[~]
└─$ dirb https://mymart.pk

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Nov 29 22:53:31 2024
URL_BASE: https://mymart.pk/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://mymart.pk/ ----
+ https://mymart.pk/.bash_history (CODE:200|SIZE:901049)
+ https://mymart.pk/.bashrc (CODE:200|SIZE:901043)
+ https://mymart.pk/.cache (CODE:200|SIZE:901042)
+ https://mymart.pk/.config (CODE:200|SIZE:901043)
+ https://mymart.pk/.cvs (CODE:200|SIZE:901040)
+ https://mymart.pk/.cvsignore (CODE:200|SIZE:901046)
+ https://mymart.pk/.forward (CODE:200|SIZE:901044)
+ https://mymart.pk/.history (CODE:200|SIZE:901044)
+ https://mymart.pk/.hta (CODE:200|SIZE:901040)
+ https://mymart.pk/.htaccess (CODE:200|SIZE:901045)
+ https://mymart.pk/.htpasswd (CODE:200|SIZE:901045)
+ https://mymart.pk/.listing (CODE:200|SIZE:901044)
+ https://mymart.pk/.listings (CODE:200|SIZE:901045)
+ https://mymart.pk/.mysql_history (CODE:200|SIZE:901050)
+ https://mymart.pk/.passwd (CODE:200|SIZE:901043)
+ https://mymart.pk/.perf (CODE:200|SIZE:901041)
+ https://mymart.pk/.profile (CODE:200|SIZE:901044)
+ https://mymart.pk/.rhosts (CODE:200|SIZE:901043)
+ https://mymart.pk/.sh_history (CODE:200|SIZE:901047)
+ https://mymart.pk/.ssh (CODE:200|SIZE:901040)
+ https://mymart.pk/.subversion (CODE:200|SIZE:901047)
+ https://mymart.pk/.svn (CODE:200|SIZE:901040)
+ https://mymart.pk/.swf (CODE:200|SIZE:901040)
+ https://mymart.pk/.web (CODE:200|SIZE:901040)
+ https://mymart.pk/account (CODE:302|SIZE:0)
+ https://mymart.pk/admin (CODE:301|SIZE:0)
+ https://mymart.pk/admin.cgi (CODE:301|SIZE:0)
+ https://mymart.pk/admin.php (CODE:301|SIZE:0)
+ https://mymart.pk/admin.pl (CODE:301|SIZE:0)
+ https://mymart.pk/cart (CODE:200|SIZE:246302)
+ https://mymart.pk/checkout (CODE:302|SIZE:0)
+ https://mymart.pk/crossdomain.xml (CODE:200|SIZE:223)
+ https://mymart.pk/index (CODE:200|SIZE:901041)
+ https://mymart.pk/index.htm (CODE:200|SIZE:901045)
+ https://mymart.pk/index.html (CODE:200|SIZE:901046)
+ https://mymart.pk/index.php (CODE:200|SIZE:901045)
+ https://mymart.pk/password (CODE:302|SIZE:0)
+ https://mymart.pk/products (CODE:200|SIZE:296108)
+ https://mymart.pk/robots.txt (CODE:200|SIZE:3689)
+ https://mymart.pk/search (CODE:200|SIZE:237883)
+ https://mymart.pk/shop (CODE:200|SIZE:901040)
+ https://mymart.pk/sitemap.xml (CODE:200|SIZE:757)
^[[D
^[[D

-----------------
END_TIME: Fri Nov 29 23:30:55 2024
DOWNLOADED: 4612 - FOUND: 42

┌──(kali㉿kali)-[~]
```

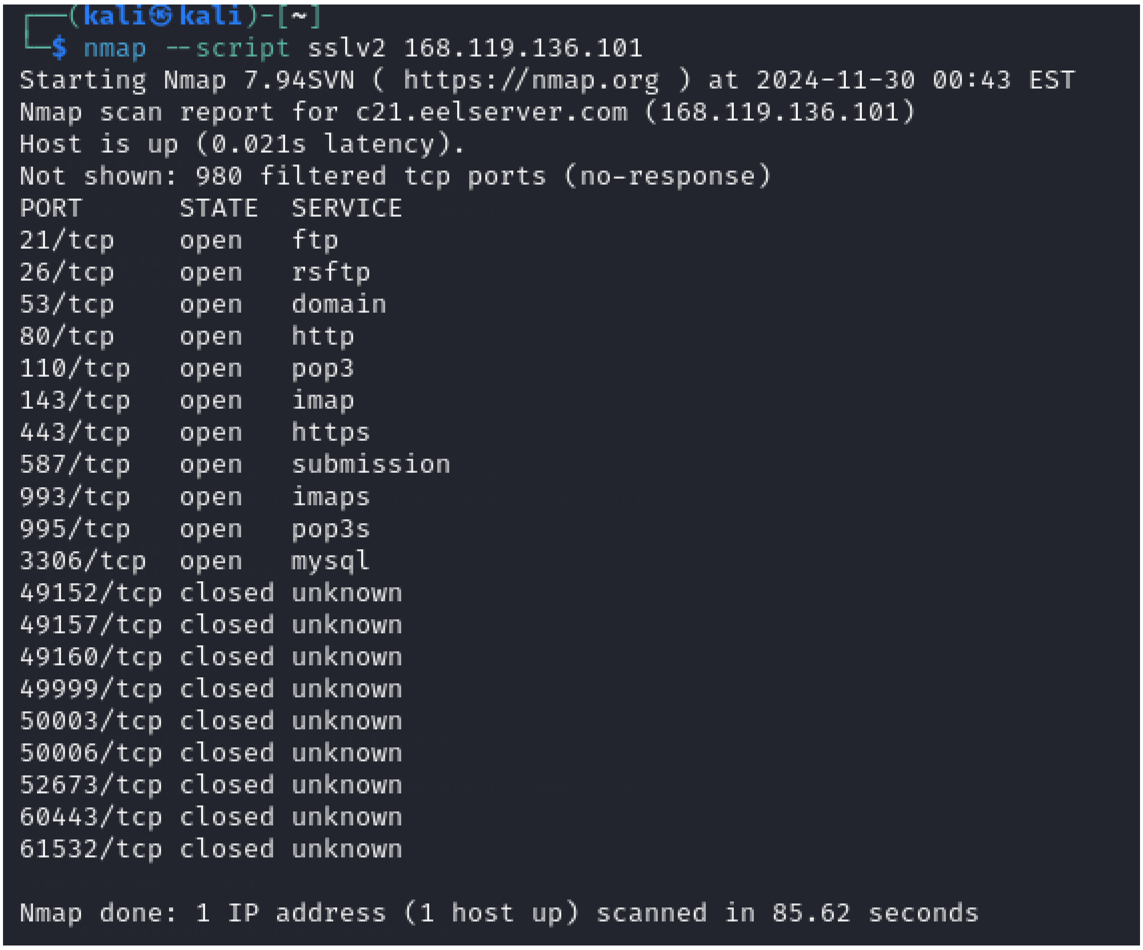
6. Gobuster using for https to accesses the all file in the website



```
┌──(root㉿kali)-[/home/kali]
└─#  gobuster -u https://mymart.pk -w /usr/share/dirb/wordlists/extensions_common.txt -x .txt
Error: unknown shorthand flag: 'u' in -u

┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u https://mymart.pk -w /usr/share/dirb/wordlists/extensions_common.txt -x txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://mymart.pk
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/extensions_common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.aspx                (Status: 200) [Size: 902397]
/.cfm                 (Status: 200) [Size: 902396]
/.txt                 (Status: 200) [Size: 902396]
/.asp                 (Status: 200) [Size: 902396]
/.bat                 (Status: 200) [Size: 902396]
/.c                   (Status: 200) [Size: 902394]
/.exe                 (Status: 200) [Size: 902396]
/.com                 (Status: 200) [Size: 902396]
/.cgi                 (Status: 200) [Size: 902396]
/.dll                 (Status: 200) [Size: 902396]
/.htm                 (Status: 200) [Size: 902396]
/.html                (Status: 200) [Size: 902397]
/.inc                 (Status: 200) [Size: 902396]
/.jsa                 (Status: 200) [Size: 902396]
/.jhtml               (Status: 200) [Size: 902398]
/.jsp                 (Status: 200) [Size: 902396]
/.log                 (Status: 200) [Size: 902396]
/.mdb                 (Status: 200) [Size: 902396]
/.php                 (Status: 200) [Size: 902396]
/.phtml               (Status: 200) [Size: 902398]
/.nsf                 (Status: 200) [Size: 902396]
/.pl                  (Status: 200) [Size: 902395]
/.txt                 (Status: 200) [Size: 902396]
/.reg                 (Status: 200) [Size: 902396]
/.sh                  (Status: 200) [Size: 902395]
/                     (Status: 200) [Size: 902768]
/.txt                 (Status: 200) [Size: 902396]
/.shtml               (Status: 200) [Size: 902398]
/.sql                 (Status: 200) [Size: 902396]
Progress: 58 / 60 (96.67%)
/.xml                 (Status: 200) [Size: 902396]
===============================================================
Finished
===============================================================
```

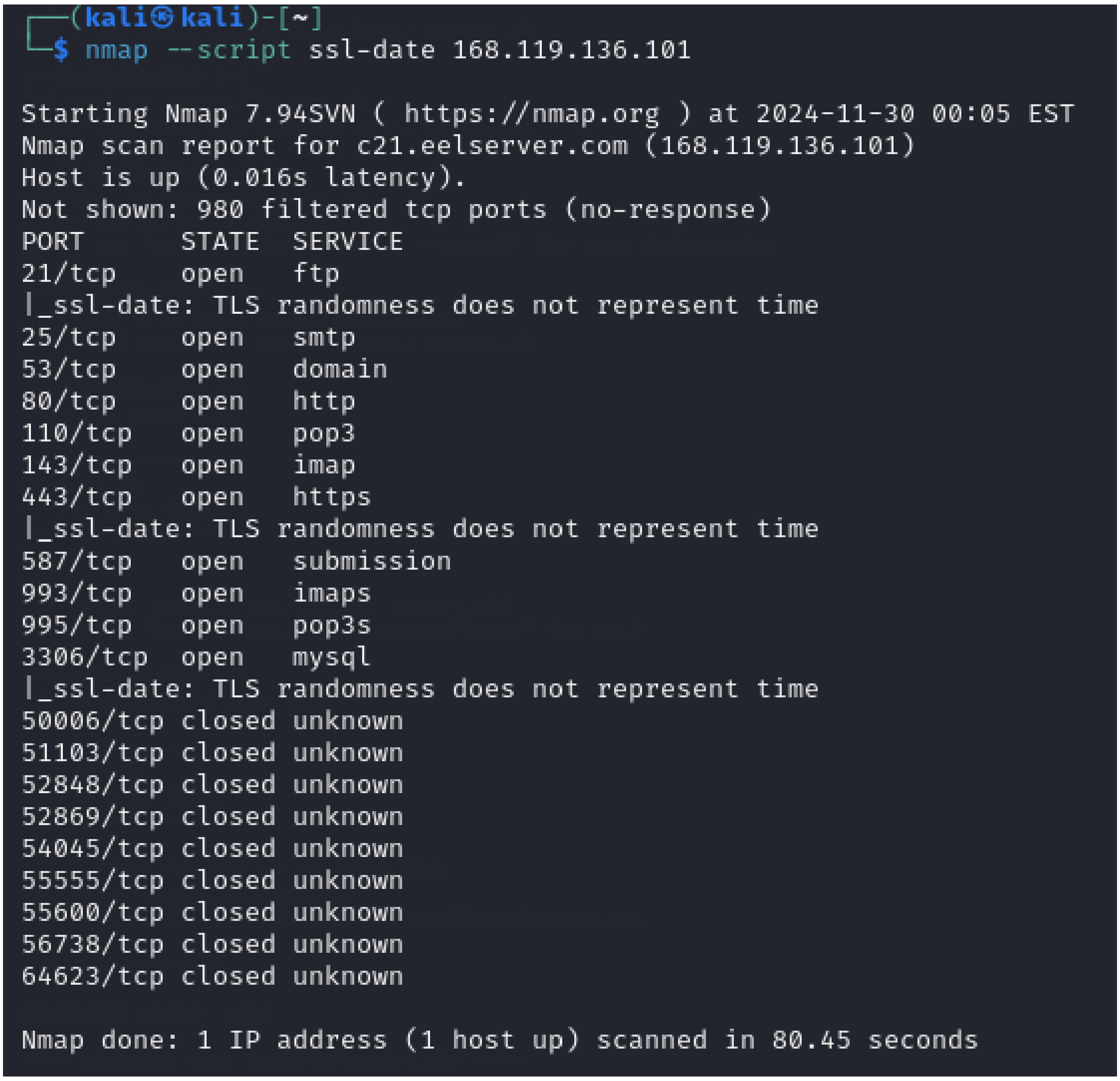
7. Now we done the ssl enumeration to gather information from website

SSL ENUMERATION:

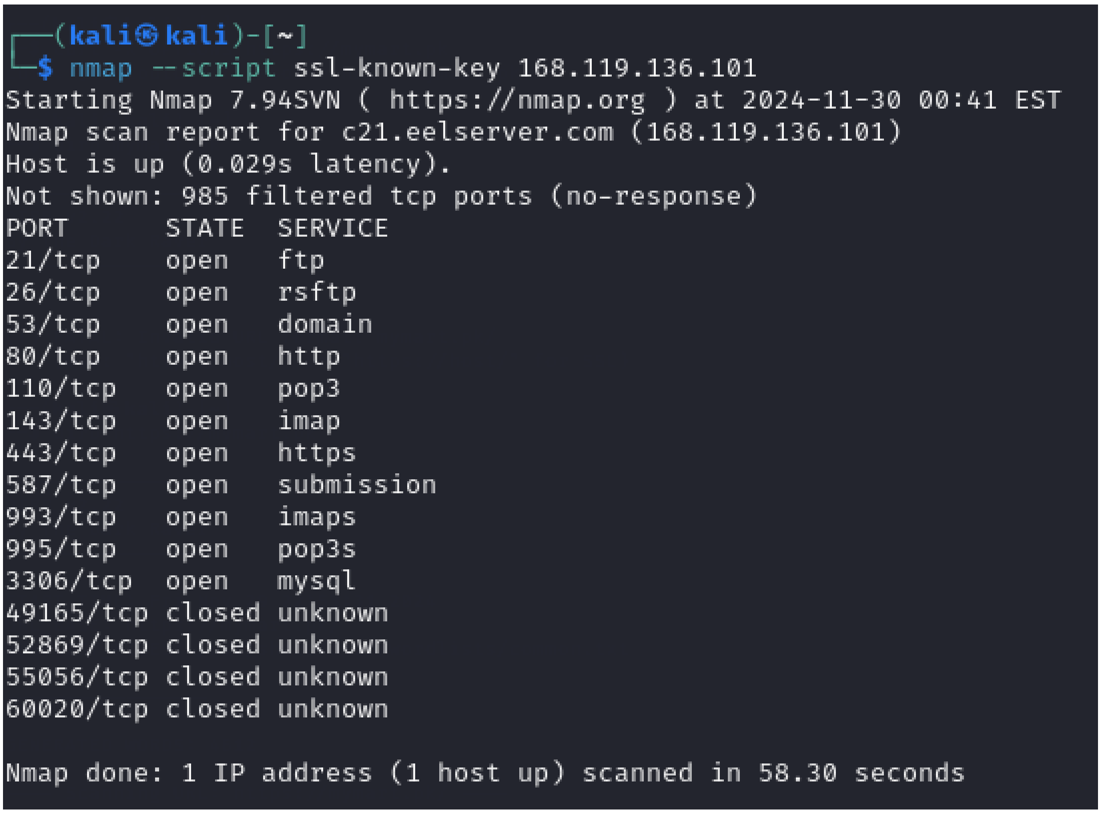


```
┌──(kali㉿kali)-[~]
└─$ nmap --script sslv2 168.119.136.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-30 00:43 EST
Nmap scan report for c21.eelserver.com (168.119.136.101)
Host is up (0.021s latency).
Not shown: 980 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    open   ftp
26/tcp    open   rsftp
53/tcp    open   domain
80/tcp    open   http
110/tcp   open   pop3
143/tcp   open   imap
443/tcp   open   https
587/tcp   open   submission
993/tcp   open   imaps
995/tcp   open   pop3s
3306/tcp  open   mysql
49152/tcp closed unknown
49157/tcp closed unknown
49160/tcp closed unknown
49999/tcp closed unknown
50003/tcp closed unknown
50006/tcp closed unknown
52673/tcp closed unknown
60443/tcp closed unknown
61532/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 85.62 seconds
```

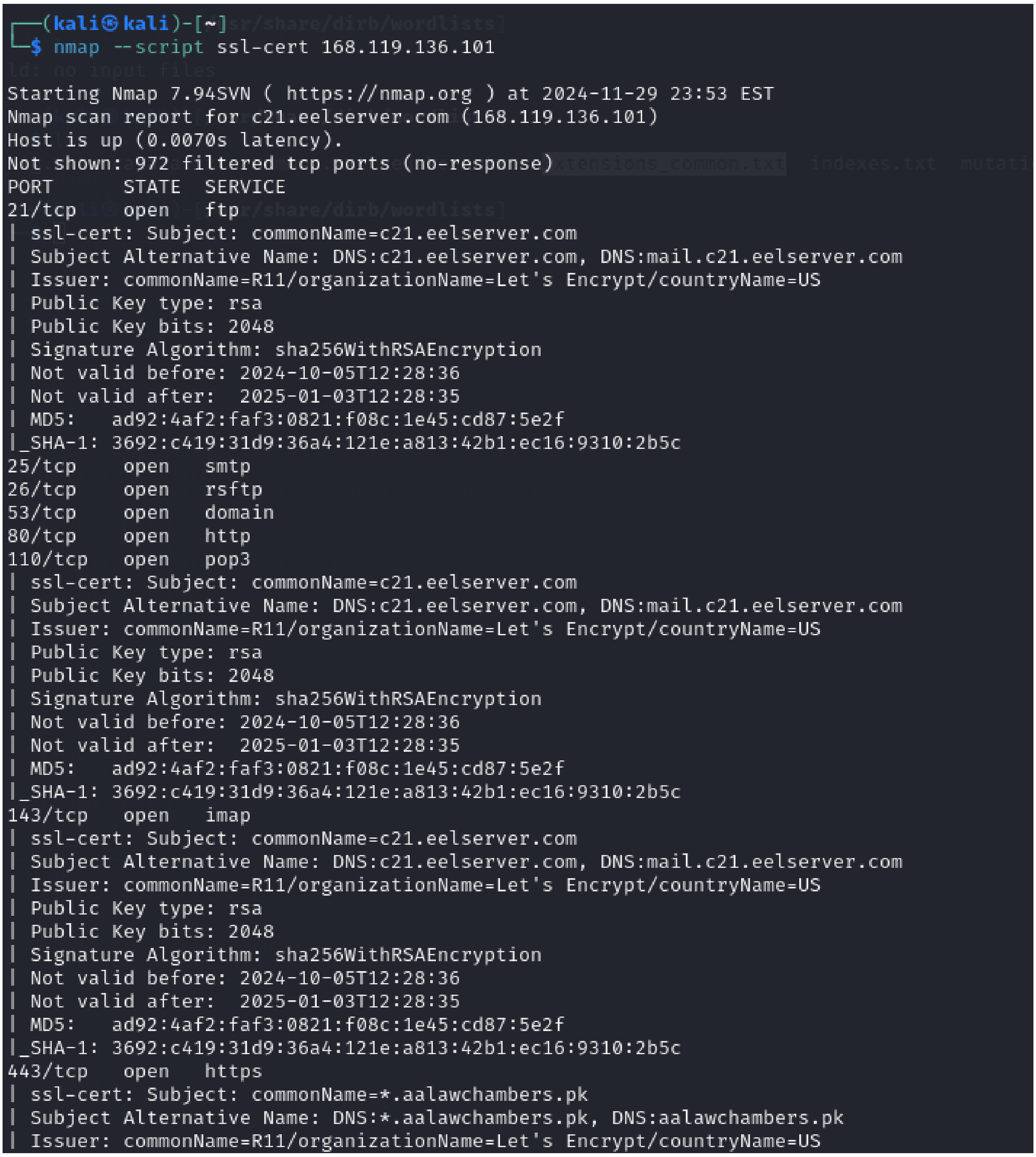
8. Now we done the ssl-date script to gather date and various information gathering.



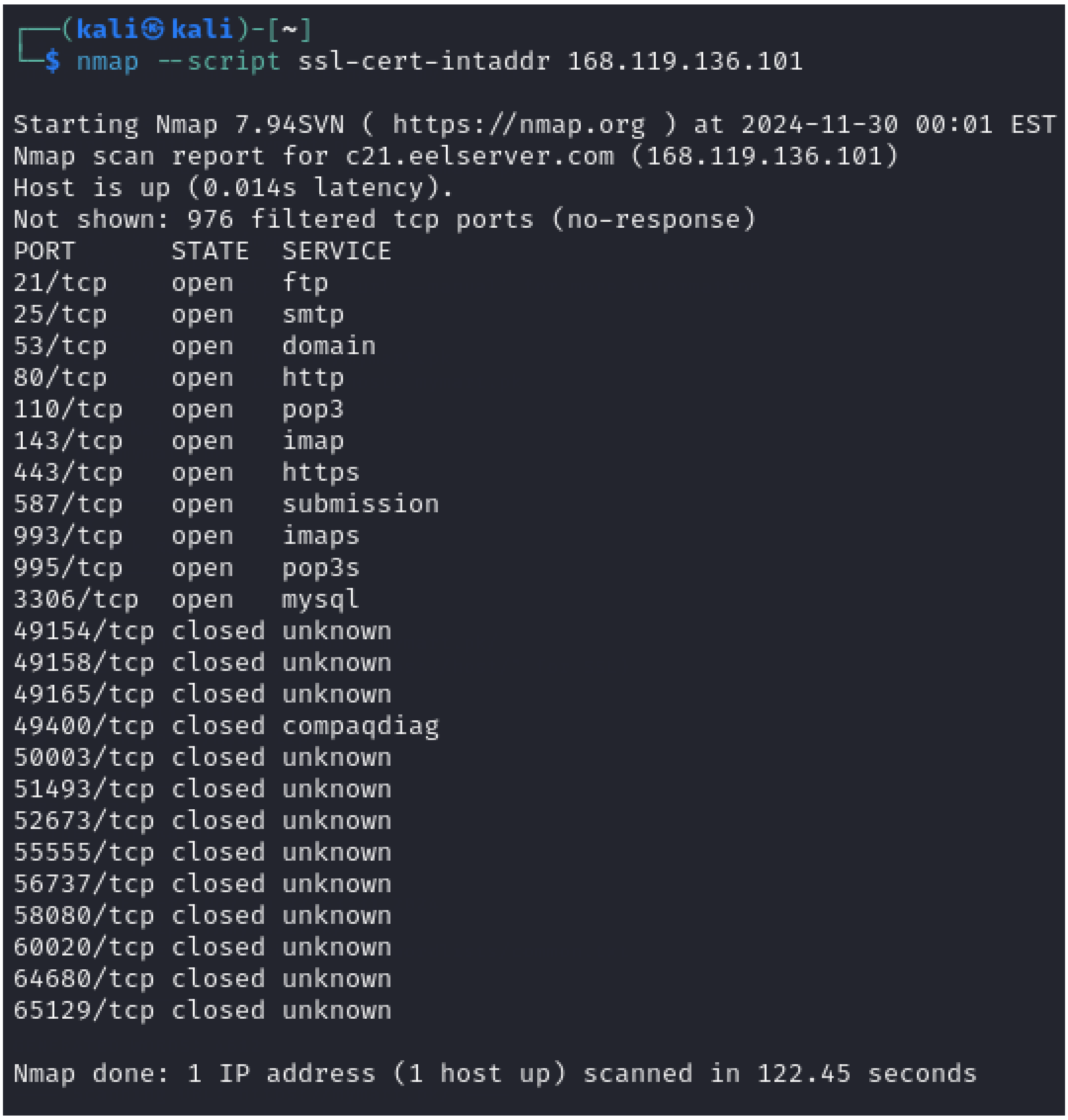
```
┌──(kali㉿kali)-[~]
└─$ nmap --script ssl-date 168.119.136.101

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-30 00:05 EST
Nmap scan report for c21.eelserver.com (168.119.136.101)
Host is up (0.016s latency).
Not shown: 980 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    open   ftp
|_ssl-date: TLS randomness does not represent time
25/tcp    open   smtp
53/tcp    open   domain
80/tcp    open   http
110/tcp   open   pop3
143/tcp   open   imap
443/tcp   open   https
|_ssl-date: TLS randomness does not represent time
587/tcp   open   submission
993/tcp   open   imaps
995/tcp   open   pop3s
3306/tcp  open   mysql
|_ssl-date: TLS randomness does not represent time
50006/tcp closed unknown
51103/tcp closed unknown
52848/tcp closed unknown
52869/tcp closed unknown
54045/tcp closed unknown
55555/tcp closed unknown
55600/tcp closed unknown
56738/tcp closed unknown
64623/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 80.45 seconds
```



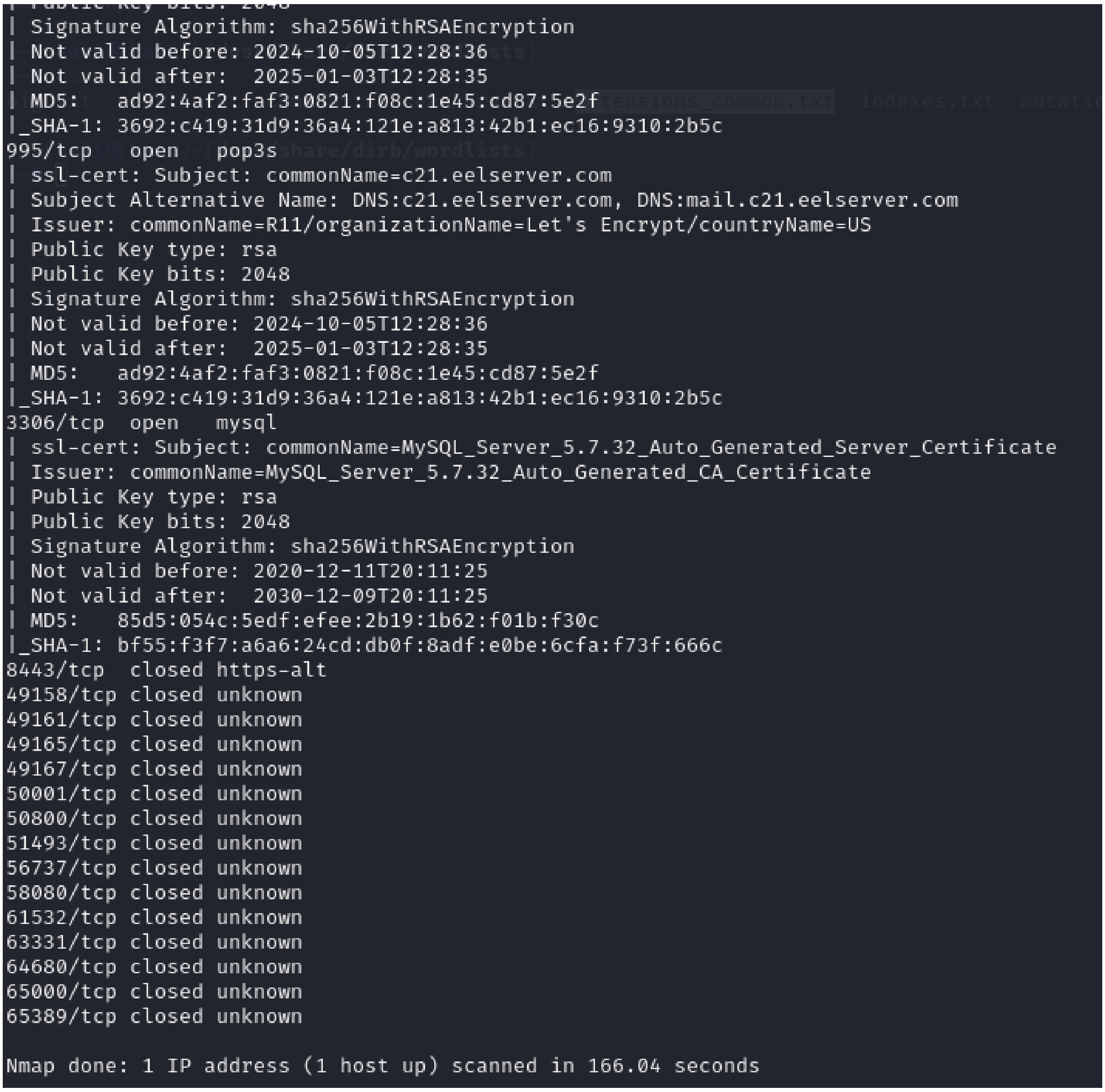
```
┌──(kali㉿kali)-[~]
└─$ nmap --script ssl-known-key 168.119.136.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-30 00:41 EST
Nmap scan report for c21.eelserver.com (168.119.136.101)
Host is up (0.029s latency).
Not shown: 985 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    open   ftp
26/tcp    open   rsftp
53/tcp    open   domain
80/tcp    open   http
110/tcp   open   pop3
143/tcp   open   imap
443/tcp   open   https
587/tcp   open   submission
993/tcp   open   imaps
995/tcp   open   pop3s
3306/tcp  open   mysql
49165/tcp closed unknown
52869/tcp closed unknown
55056/tcp closed unknown
60020/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 58.30 seconds
```



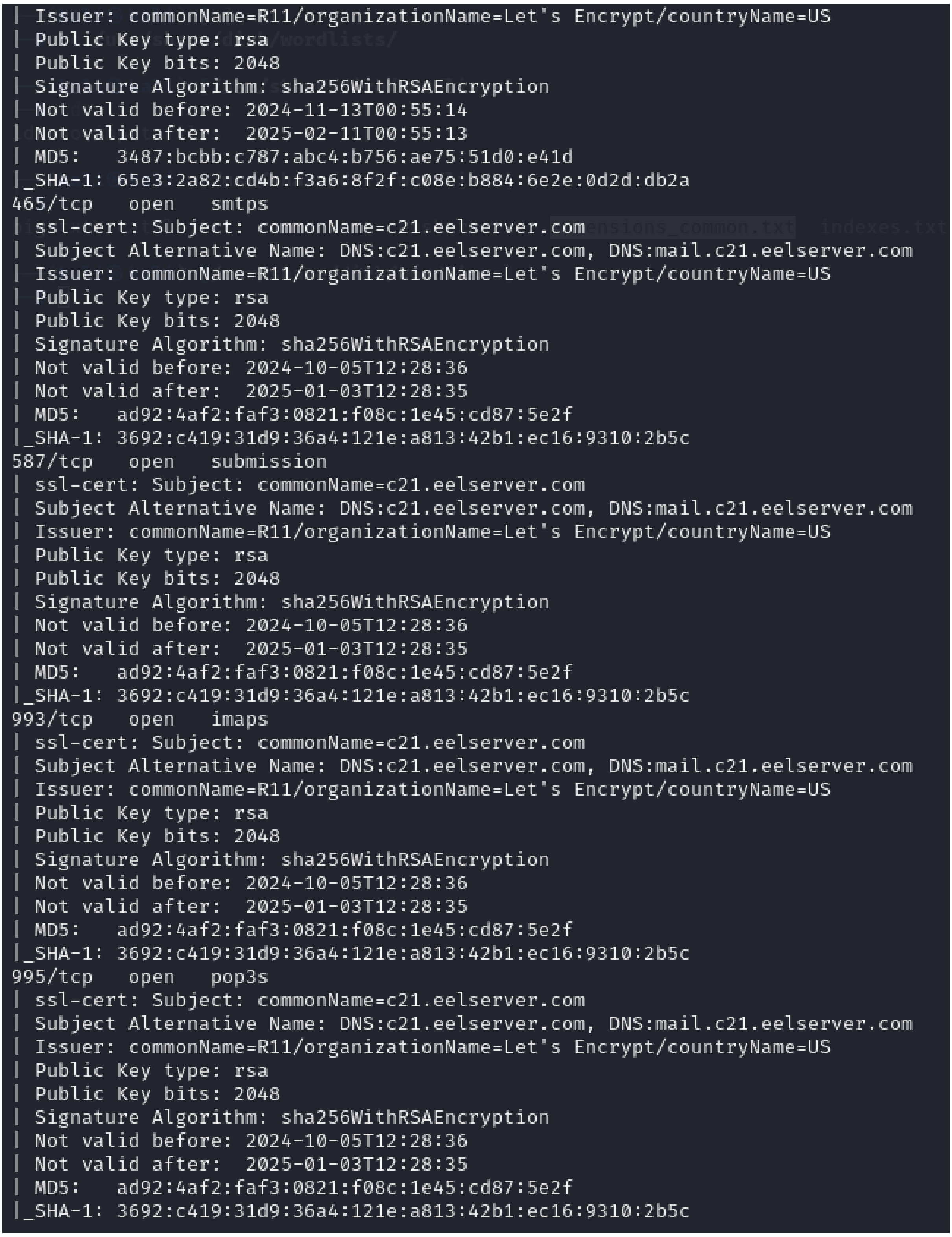
```
┌──(kali㉿kali)-[~]
└─$ nmap --script ssl-cert 168.119.136.101

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-29 23:53 EST
Nmap scan report for c21.eelserver.com (168.119.136.101)
Host is up (0.0070s latency).
Not shown: 972 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    open   ftp
| ssl-cert: Subject: commonName=c21.eelserver.com
| Subject Alternative Name: DNS:c21.eelserver.com, DNS:mail.c21.eelserver.com
| Issuer: commonName=R11/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-10-05T12:28:36
| Not valid after:  2025-01-03T12:28:35
| MD5:   ad92:4af2:faf3:0821:f08c:1e45:cd87:5e2f
|_SHA-1: 3692:c419:31d9:36a4:121e:a813:42b1:ec16:9310:2b5c
25/tcp    open   smtp
26/tcp    open   rsftp
53/tcp    open   domain
80/tcp    open   http
110/tcp   open   pop3
| ssl-cert: Subject: commonName=c21.eelserver.com
| Subject Alternative Name: DNS:c21.eelserver.com, DNS:mail.c21.eelserver.com
| Issuer: commonName=R11/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-10-05T12:28:36
| Not valid after:  2025-01-03T12:28:35
| MD5:   ad92:4af2:faf3:0821:f08c:1e45:cd87:5e2f
|_SHA-1: 3692:c419:31d9:36a4:121e:a813:42b1:ec16:9310:2b5c
143/tcp   open   imap
| ssl-cert: Subject: commonName=c21.eelserver.com
| Subject Alternative Name: DNS:c21.eelserver.com, DNS:mail.c21.eelserver.com
| Issuer: commonName=R11/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-10-05T12:28:36
| Not valid after:  2025-01-03T12:28:35
| MD5:   ad92:4af2:faf3:0821:f08c:1e45:cd87:5e2f
|_SHA-1: 3692:c419:31d9:36a4:121e:a813:42b1:ec16:9310:2b5c
443/tcp   open   https
| ssl-cert: Subject: commonName=*.aalawchambers.pk
| Subject Alternative Name: DNS:*.aalawchambers.pk, DNS:aalawchambers.pk
| Issuer: commonName=R11/organizationName=Let's Encrypt/countryName=US
```



```
┌──(kali㉿kali)-[~]
└─$ nmap --script ssl-cert-intaddr 168.119.136.101

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-30 00:01 EST
Nmap scan report for c21.eelserver.com (168.119.136.101)
Host is up (0.014s latency).
Not shown: 976 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    open   ftp
25/tcp    open   smtp
53/tcp    open   domain
80/tcp    open   http
110/tcp   open   pop3
143/tcp   open   imap
443/tcp   open   https
587/tcp   open   submission
993/tcp   open   imaps
995/tcp   open   pop3s
3306/tcp  open   mysql
49154/tcp closed unknown
49158/tcp closed unknown
49165/tcp closed unknown
49400/tcp closed compaqdiag
50003/tcp closed unknown
51493/tcp closed unknown
52673/tcp closed unknown
55555/tcp closed unknown
56737/tcp closed unknown
58080/tcp closed unknown
60020/tcp closed unknown
64680/tcp closed unknown
65129/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 122.45 seconds
```



```
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-10-05T12:28:36
| Not valid after:  2025-01-03T12:28:35
| MD5:   ad92:4af2:faf3:0821:f08c:1e45:cd87:5e2f
|_SHA-1: 3692:c419:31d9:36a4:121e:a813:42b1:ec16:9310:2b5c
995/tcp   open   pop3s
| ssl-cert: Subject: commonName=c21.eelserver.com
| Subject Alternative Name: DNS:c21.eelserver.com, DNS:mail.c21.eelserver.com
| Issuer: commonName=R11/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-10-05T12:28:36
| Not valid after:  2025-01-03T12:28:35
| MD5:   ad92:4af2:faf3:0821:f08c:1e45:cd87:5e2f
|_SHA-1: 3692:c419:31d9:36a4:121e:a813:42b1:ec16:9310:2b5c
3306/tcp  open   mysql
| ssl-cert: Subject: commonName=MySQL_Server_5.7.32_Auto_Generated_Server_Certificate
| Issuer: commonName=MySQL_Server_5.7.32_Auto_Generated_CA_Certificate
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-12-11T20:11:25
| Not valid after:  2030-12-09T20:11:25
| MD5:   85d5:054c:5edf:efee:2b19:1b62:f01b:f30c
|_SHA-1: bf55:f3f7:a6a6:24cd:db0f:8adf:e0be:6cfa:f73f:666c
8443/tcp  closed https-alt
49158/tcp closed unknown
49161/tcp closed unknown
49165/tcp closed unknown
49167/tcp closed unknown
50001/tcp closed unknown
50800/tcp closed unknown
51493/tcp closed unknown
56737/tcp closed unknown
58080/tcp closed unknown
61532/tcp closed unknown
63331/tcp closed unknown
64680/tcp closed unknown
65000/tcp closed unknown
65389/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 166.04 seconds
```

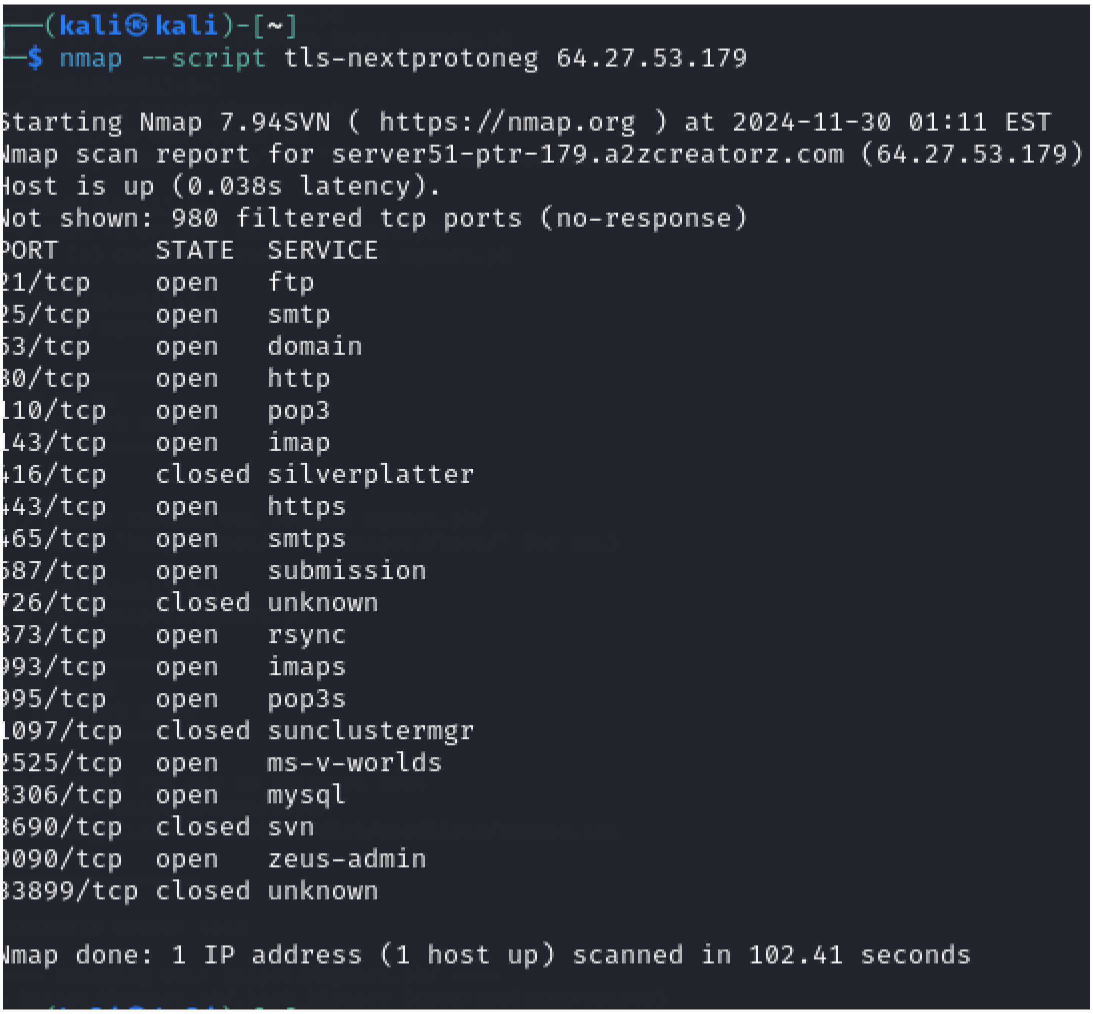


```
| Issuer: commonName=R11/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-11-13T00:55:14
| Not valid after:  2025-02-11T00:55:13
| MD5:   3487:bcbb:c787:abc4:b756:ae75:51d0:e41d
|_SHA-1: 65e3:2a82:cd4b:f3a6:8f2f:c08e:b884:6e2e:0d2d:db2a
465/tcp   open   smtps
| ssl-cert: Subject: commonName=c21.eelserver.com
| Subject Alternative Name: DNS:c21.eelserver.com, DNS:mail.c21.eelserver.com
| Issuer: commonName=R11/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-10-05T12:28:36
| Not valid after:  2025-01-03T12:28:35
| MD5:   ad92:4af2:faf3:0821:f08c:1e45:cd87:5e2f
|_SHA-1: 3692:c419:31d9:36a4:121e:a813:42b1:ec16:9310:2b5c
587/tcp   open   submission
| ssl-cert: Subject: commonName=c21.eelserver.com
| Subject Alternative Name: DNS:c21.eelserver.com, DNS:mail.c21.eelserver.com
| Issuer: commonName=R11/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-10-05T12:28:36
| Not valid after:  2025-01-03T12:28:35
| MD5:   ad92:4af2:faf3:0821:f08c:1e45:cd87:5e2f
|_SHA-1: 3692:c419:31d9:36a4:121e:a813:42b1:ec16:9310:2b5c
993/tcp   open   imaps
| ssl-cert: Subject: commonName=c21.eelserver.com
| Subject Alternative Name: DNS:c21.eelserver.com, DNS:mail.c21.eelserver.com
| Issuer: commonName=R11/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-10-05T12:28:36
| Not valid after:  2025-01-03T12:28:35
| MD5:   ad92:4af2:faf3:0821:f08c:1e45:cd87:5e2f
|_SHA-1: 3692:c419:31d9:36a4:121e:a813:42b1:ec16:9310:2b5c
995/tcp   open   pop3s
| ssl-cert: Subject: commonName=c21.eelserver.com
| Subject Alternative Name: DNS:c21.eelserver.com, DNS:mail.c21.eelserver.com
| Issuer: commonName=R11/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-10-05T12:28:36
| Not valid after:  2025-01-03T12:28:35
| MD5:   ad92:4af2:faf3:0821:f08c:1e45:cd87:5e2f
|_SHA-1: 3692:c419:31d9:36a4:121e:a813:42b1:ec16:9310:2b5c
```

9. Now we done the SMTP enumeration gather information of the website

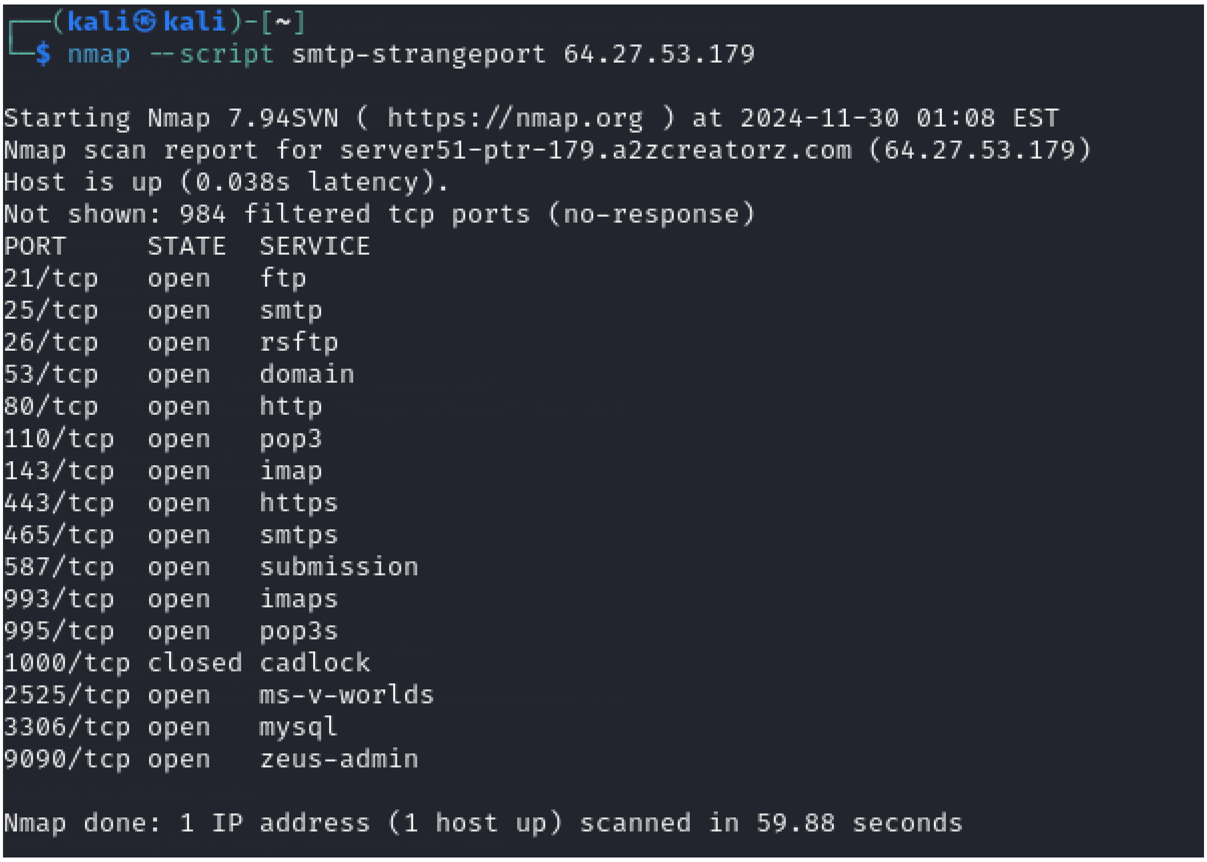
SMTP ENUMERATION:

10. Here we done the tls-nextprotoneg to diagnosis the website and gather for open ports



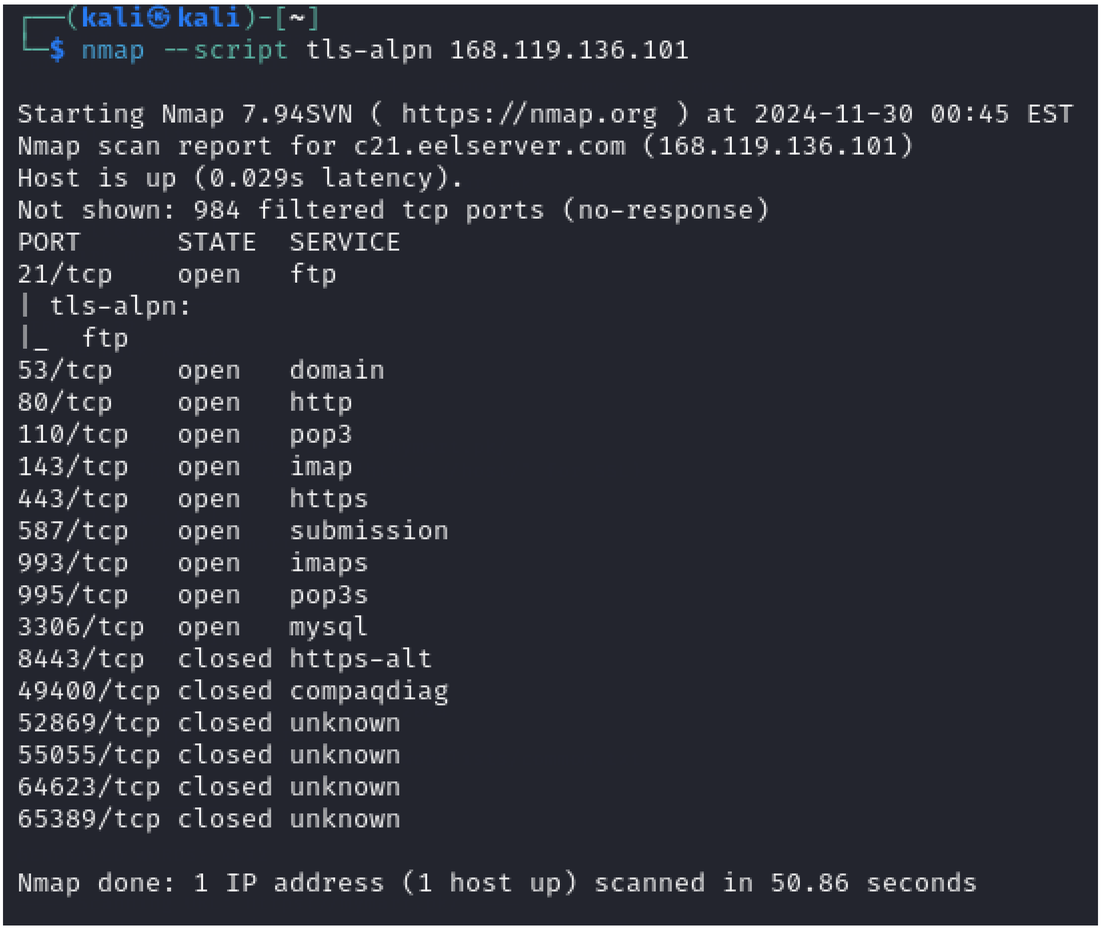
```
┌──(kali㉿kali)-[~]
└─$ nmap --script tls-nextprotoneg 64.27.53.179

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-30 01:11 EST
Nmap scan report for server51-ptr-179.a2zcreatorz.com (64.27.53.179)
Host is up (0.038s latency).
Not shown: 980 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    open   ftp
25/tcp    open   smtp
53/tcp    open   domain
80/tcp    open   http
110/tcp   open   pop3
143/tcp   open   imap
416/tcp   closed silverplatter
443/tcp   open   https
465/tcp   open   smtps
587/tcp   open   submission
726/tcp   closed unknown
873/tcp   open   rsync
993/tcp   open   imaps
995/tcp   open   pop3s
1097/tcp  closed sunclustermgr
2525/tcp  open   ms-v-worlds
3306/tcp  open   mysql
3690/tcp  closed svn
9090/tcp  open   zeus-admin
33899/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 102.41 seconds
```

11. The smtp-strangeport use to detect SMTP servers running on non-standard ports.



```
┌──(kali㉿kali)-[~]
└─$ nmap --script smtp-strangeport 64.27.53.179

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-30 01:08 EST
Nmap scan report for server51-ptr-179.a2zcreatorz.com (64.27.53.179)
Host is up (0.038s latency).
Not shown: 984 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
25/tcp   open   smtp
26/tcp   open   rsftp
53/tcp   open   domain
80/tcp   open   http
110/tcp  open   pop3
143/tcp  open   imap
443/tcp  open   https
465/tcp  open   smtps
587/tcp  open   submission
993/tcp  open   imaps
995/tcp  open   pop3s
1000/tcp closed cadlock
2525/tcp open   ms-v-worlds
3306/tcp open   mysql
9090/tcp open   zeus-admin

Nmap done: 1 IP address (1 host up) scanned in 59.88 seconds
```

12. Application-Layer protocol Negotiation is used to negotiate client to server.



```
┌──(kali㉿kali)-[~]
└─$ nmap --script tls-alpn 168.119.136.101

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-30 00:45 EST
Nmap scan report for c21.eelserver.com (168.119.136.101)
Host is up (0.029s latency).
Not shown: 984 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    open   ftp
| tls-alpn: 
|_  ftp
53/tcp    open   domain
80/tcp    open   http
110/tcp   open   pop3
143/tcp   open   imap
443/tcp   open   https
587/tcp   open   submission
993/tcp   open   imaps
995/tcp   open   pop3s
3306/tcp  open   mysql
8443/tcp  closed https-alt
49400/tcp closed compaqdiag
52869/tcp closed unknown
55055/tcp closed unknown
64623/tcp closed unknown
65389/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 50.86 seconds
```

4. CONCLUSION: here we do various enumerations to gathering the information of the websites.

5. SUMMARY OF THE TASKS: here first go to the websites and access the site enumeration for open ports to gather more details here we done the various types of the enumerations like ftp, https, ssl, smtp. Here we done a website having the specified open ports to done the enumeration.