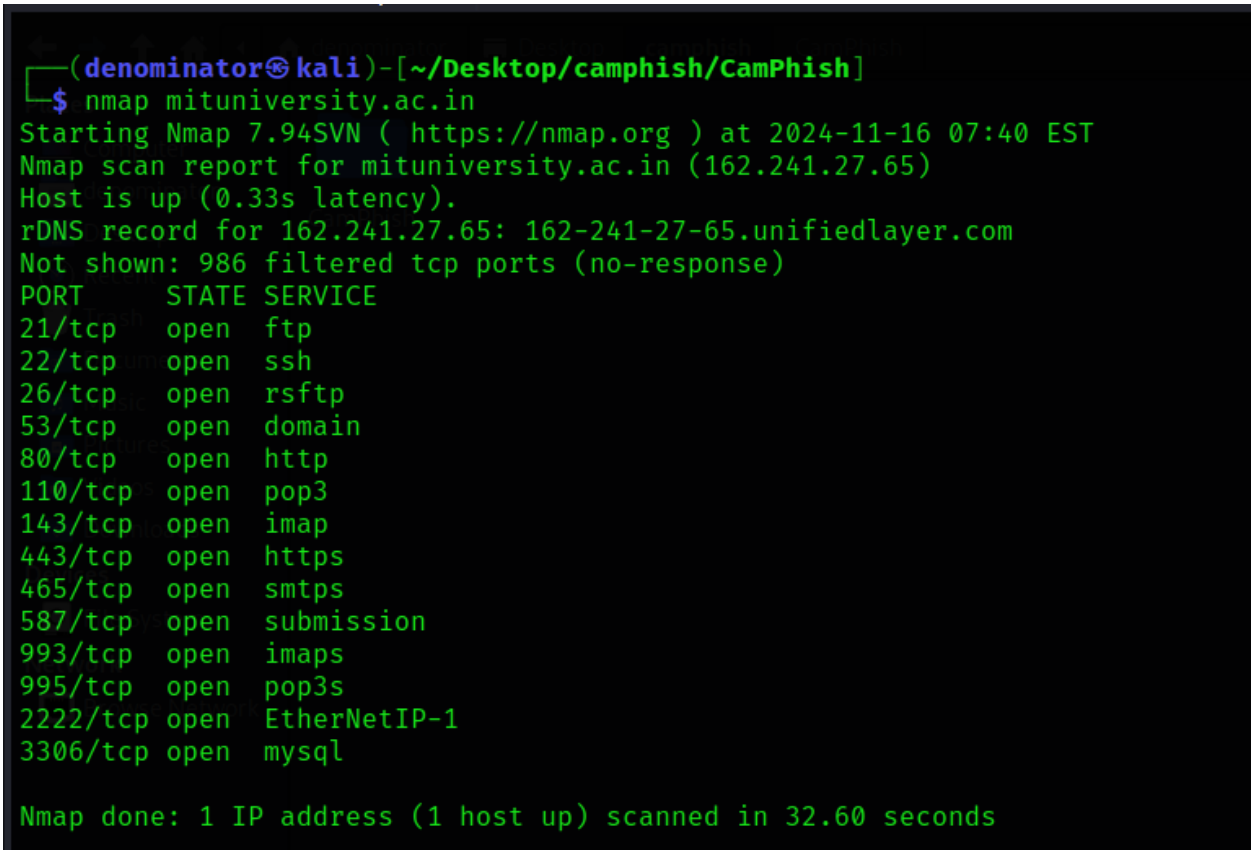
Nmap Scan

Basic Nmap scan:

command →

```
nmap http://mituniversity.ac.in
```

Output →



Default script and version scan:

command →

```
nmap -sC -sV http://mituniversity.ac.in
```

Output →

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-16 07:4
5 EST
Nmap scan report for mituniversity.ac.in (162.241.27.65)
Host is up (0.35s latency).
rDNS record for 162.241.27.65: 162-241-27-65.unifiedlayer.com
Not shown: 986 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      Pure-FTPd
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhost
box.net
| Not valid before: 2024-05-09T00:00:00
|_Not valid after:  2025-05-09T23:59:59
22/tcp   open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   1024 9f:44:17:ef:33:3b:9b:ac:de:29:65:05:17:ac:9e:1f (DS
A)
|   2048 c9:c9:58:d3:c5:53:bf:63:04:8d:33:ff:25:f3:33:2e (RS
A)
|_  256 03:ac:7d:be:52:02:56:df:f1:3b:06:47:51:f7:2d:82 (ECDS
A)
26/tcp   open  smtp     Exim smtpd 4.96.2
| smtp-commands: cs2000.webhostbox.net Hello mituniversity.a
c.in [152.58.21.243], SIZE 52428800, 8BITMIME, PIPELINING, PI
PECONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA
BDAT NOOP QUIT RSET HELP
| ssl-cert: Subject: commonName=mituniversity.ac.in
| Subject Alternative Name: DNS:mituniversity.ac.in, DNS:www.
mituniversity.ac.in
```

```
| Not valid before: 2024-09-22T18:51:16
|_Not valid after:  2024-12-21T18:51:15
53/tcp   open  domain   ISC BIND 9.11.4-P2 (RedHat Enterprise
Linux 7)
| dns-nsid:
|_  bind.version: 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9
80/tcp   open  http     Apache httpd
| http-server-header:
|   Apache
|_  nginx/1.25.5
|_http-title: Top University in Pune Maharashtra - MIT ADT Un
iversity
110/tcp  open  pop3     Dovecot pop3d
|_pop3-capabilities: PIPELINING USER UIDL AUTH-RESP-CODE RESP
-CODES STLS CAPA TOP SASL(PLAIN LOGIN)
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhost
box.net
| Not valid before: 2024-05-09T00:00:00
|_Not valid after:  2025-05-09T23:59:59
143/tcp  open  imap     Dovecot imapd
|_imap-capabilities: ENABLE capabilities LITERAL+ ID OK IMAP4
rev1 Pre-login have IDLE post-login SASL-IR AUTH=LOGINA0001 N
AMESPACE LOGIN-REFERRALS listed STARTTLS more AUTH=PLAIN
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhost
box.net
| Not valid before: 2024-05-09T00:00:00
|_Not valid after:  2025-05-09T23:59:59
443/tcp  open  ssl/http Apache httpd
| ssl-cert: Subject: commonName=mituniversity.ac.in
| Subject Alternative Name: DNS:mituniversity.ac.in, DNS:www.
mituniversity.ac.in
| Not valid before: 2024-09-22T18:51:16
|_Not valid after:  2024-12-21T18:51:15
|_http-title: Top University in Pune Maharashtra - MIT ADT Un
```

```
iversity
| http-server-header:
|   Apache
|_  nginx/1.25.5
|_ssl-date: TLS randomness does not represent time
465/tcp  open  ssl/smtp Exim smtpd 4.96.2
| smtp-commands: cs2000.webhostbox.net Hello mituniversity.a
c.in [152.58.21.243], SIZE 52428800, 8BITMIME, PIPELINING, PI
PECONNECT, AUTH PLAIN LOGIN, HELP
|_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOO
P QUIT RSET HELP
| ssl-cert: Subject: commonName=mituniversity.ac.in
| Subject Alternative Name: DNS:mituniversity.ac.in, DNS:www.
mituniversity.ac.in
| Not valid before: 2024-09-22T18:51:16
|_Not valid after:  2024-12-21T18:51:15
587/tcp  open  smtp     Exim smtpd 4.96.2
| smtp-commands: cs2000.webhostbox.net Hello mituniversity.a
c.in [152.58.21.243], SIZE 52428800, 8BITMIME, PIPELINING, PI
PECONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA
BDAT NOOP QUIT RSET HELP
| ssl-cert: Subject: commonName=mituniversity.ac.in
| Subject Alternative Name: DNS:mituniversity.ac.in, DNS:www.
mituniversity.ac.in
| Not valid before: 2024-09-22T18:51:16
|_Not valid after:  2024-12-21T18:51:15
993/tcp  open  imaps?
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhost
box.net
| Not valid before: 2024-05-09T00:00:00
|_Not valid after:  2025-05-09T23:59:59
995/tcp  open  pop3s?
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhost
```

```
box.net
| Not valid before: 2024-05-09T00:00:00
|_Not valid after:  2025-05-09T23:59:59
2222/tcp open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   1024 9f:44:17:ef:33:3b:9b:ac:de:29:65:05:17:ac:9e:1f (DS
A)
|_  2048 c9:c9:58:d3:c5:53:bf:63:04:8d:33:ff:25:f3:33:2e (RS
A)
3306/tcp open  mysql    MySQL 5.7.23-23
| mysql-info:
|   Protocol: 10
|   Version: 5.7.23-23
|   Thread ID: 5261646
|   Capabilities flags: 65535
|   Some Capabilities: Speaks41ProtocolNew, FoundRows, Suppor
t41Auth, SwitchToSSLAfterHandshake, SupportsLoadDataLocal, Su
pportsTransactions, LongPassword, IgnoreSpaceBeforeParenthesi
s, DontAllowDatabaseTableColumn, Speaks41ProtocolOld, Interac
tiveClient, ODBCClient, IgnoreSigpipes, SupportsCompression,
ConnectWithDatabase, LongColumnFlag, SupportsMultipleResults,
SupportsAuthPlugins, SupportsMultipleStatments
|   Status: Autocommit
|   Salt: \x0D6R\x10+iwx,`o"vc\x05}
| \x14h8
|_  Auth Plugin Name: mysql_native_password
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhost
box.net
| Not valid before: 2024-05-09T00:00:00
|_Not valid after:  2025-05-09T23:59:59
|_ssl-date: TLS randomness does not represent time
Service Info: Host: cs2000.webhostbox.net; OS: Linux; CPE: cp
e:/o:redhat:enterprise_linux:7

Service detection performed. Please report any incorrect resu
```

```
lts at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 235.44 seconds
```

Vulnerable script scan:

command →

```
nmap --script=vuln mituniversity.ac.in
```

Output →

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-16 07:5
8 EST
Nmap scan report for mituniversity.ac.in (162.241.27.65)
Host is up (0.35s latency).
rDNS record for 162.241.27.65: 162-241-27-65.unifiedlayer.com
Not shown: 986 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
26/tcp   open  rsftp
53/tcp   open  domain
80/tcp   open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabiliti
es.
| http-fileupload-exploiter:
|
|_    Couldn't find a file-type field.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-enum:
|   /blog/: Blog
|   //system.html: CMNC-200 IP Camera
|   /admin/: Possible admin folder
```

```
|   /test.php: Test page
|   /webmail/: Mail folder
|_  /robots.txt: Robots file
| http-dombased-xss:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinho
st=mituniversity.ac.in
|   Found the following indications of potential DOM based XS
S:
|
|     Source: document.write('<scr' + 'ipt type="text/javascr
ipt" src="http' + (location.protocol === 'https:' ? 's' : '')
|_    Pages: http://mituniversity.ac.in:80/
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-enum:
|   /blog/: Blog
|   //system.html: CMNC-200 IP Camera
|   /admin/: Possible admin folder
|   /test.php: Test page
|   /webmail/: Mail folder
|_  /robots.txt: Robots file
| http-fileupload-exploiter:
|
|_    Couldn't find a file-type field.
|_http-stored-xss: Couldn't find any stored XSS vulnerabiliti
es.
| http-dombased-xss:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinho
st=mituniversity.ac.in
|   Found the following indications of potential DOM based XS
S:
|
|     Source: document.write('<scr' + 'ipt type="text/javascr
ipt" src="http' + (location.protocol === 'https:' ? 's' : '')
```

```
|_    Pages: http://mituniversity.ac.in:443/
465/tcp  open  smtps
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
2222/tcp open  EtherNetIP-1
3306/tcp open  mysql
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (us
e -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 425.54 seconds
```

Aggressive Scan:

command →

```
sudo nmap -A mituniversity.ac.in -T5 -Pn
```

Output →

```
Nmap scan report for mituniversity.ac.in (162.241.27.65)
Host is up (0.13s latency).
rDNS record for 162.241.27.65: 162-241-27-65.unifiedlayer.com
Not shown: 986 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      Pure-FTPd
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhost
box.net
| Not valid before: 2024-05-09T00:00:00
|_Not valid after:  2025-05-09T23:59:59
```

```
22/tcp   open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   1024 9f:44:17:ef:33:3b:9b:ac:de:29:65:05:17:ac:9e:1f (DS
A)
|_  2048 c9:c9:58:d3:c5:53:bf:63:04:8d:33:ff:25:f3:33:2e (RS
A)
26/tcp   open  smtp     Exim smtpd 4.96.2
|_smtp-commands: Couldn't establish connection on port 26
53/tcp   open  domain   ISC BIND 9.11.4-P2 (RedHat Enterprise
Linux 7)
| dns-nsid:
|_  bind.version: 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9
80/tcp   open  http     Apache httpd
|_http-title: Top University in Pune Maharashtra - MIT ADT Un
iversity
| http-server-header:
|   Apache
|_  nginx/1.25.5
110/tcp  open  pop3     Dovecot pop3d
|_pop3-capabilities: SASL(PLAIN LOGIN) RESP-CODES PIPELINING
STLS TOP USER CAPA UIDL AUTH-RESP-CODE
143/tcp  open  imap     Dovecot imapd
|_imap-capabilities: SASL-IR LITERAL+ STARTTLS NAMESPACE AUTH
=PLAIN capabilities listed post-login Pre-login LOGIN-REFERRA
LS IDLE ID more ENABLE have IMAP4rev1 AUTH=LOGINA0001 OK
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhost
box.net
| Not valid before: 2024-05-09T00:00:00
|_Not valid after:  2025-05-09T23:59:59
443/tcp  open  ssl/http Apache httpd
|_http-server-header: Apache
| ssl-cert: Subject: commonName=mituniversity.ac.in
| Subject Alternative Name: DNS:mituniversity.ac.in, DNS:www.
mituniversity.ac.in
| Not valid before: 2024-09-22T18:51:16
```

```
|_Not valid after:  2024-12-21T18:51:15
|_http-title: Did not follow redirect to http://www.explorefr
eeresults.com/?dn=cs2000.webhostbox.net&pid=5POJ5651L&spfwd=1
|_ssl-date: TLS randomness does not represent time
465/tcp  open  ssl/smtp Exim smtpd 4.96.2
| ssl-cert: Subject: commonName=mituniversity.ac.in
| Subject Alternative Name: DNS:mituniversity.ac.in, DNS:www.
mituniversity.ac.in
| Not valid before: 2024-09-22T18:51:16
|_Not valid after:  2024-12-21T18:51:15
|_smtp-commands: cs2000.webhostbox.net Hello mituniversity.a
c.in [152.58.21.243], SIZE 52428800, 8BITMIME, PIPELINING, PI
PECONNECT, AUTH PLAIN LOGIN, HELP
587/tcp  open  smtp     Exim smtpd 4.96.2
| smtp-commands: cs2000.webhostbox.net Hello mituniversity.a
c.in [152.58.21.243], SIZE 52428800, 8BITMIME, PIPELINING, PI
PECONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA
BDAT NOOP QUIT RSET HELP
| ssl-cert: Subject: commonName=mituniversity.ac.in
| Subject Alternative Name: DNS:mituniversity.ac.in, DNS:www.
mituniversity.ac.in
| Not valid before: 2024-09-22T18:51:16
|_Not valid after:  2024-12-21T18:51:15
993/tcp  open  imaps?
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhost
box.net
| Not valid before: 2024-05-09T00:00:00
|_Not valid after:  2025-05-09T23:59:59
995/tcp  open  pop3s?
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhost
box.net
| Not valid before: 2024-05-09T00:00:00
|_Not valid after:  2025-05-09T23:59:59
```

```
2222/tcp open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|_  1024 9f:44:17:ef:33:3b:9b:ac:de:29:65:05:17:ac:9e:1f (DS
A)
3306/tcp open  mysql    MySQL 5.7.23-23
| mysql-info:
|   Protocol: 10
|   Version: 5.7.23-23
|   Thread ID: 5381341
|   Capabilities flags: 65535
|   Some Capabilities: IgnoreSpaceBeforeParenthesis, Supports
Compression, Support41Auth, Speaks41ProtocolOld, SupportsTran
sactions, SupportsLoadDataLocal, LongPassword, IgnoreSigpipe
s, SwitchToSSLAfterHandshake, ODBCClient, LongColumnFlag, Spe
aks41ProtocolNew, ConnectWithDatabase, DontAllowDatabaseTable
Column, FoundRows, InteractiveClient, SupportsMultipleStatmen
ts, SupportsMultipleResults, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: Bs\x01xAhIx>\x0D=\x01\x0DSf\x0C5\x0D\x0E_
|_  Auth Plugin Name: mysql_native_password
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhost
box.net
| Not valid before: 2024-05-09T00:00:00
|_Not valid after:  2025-05-09T23:59:59
|_ssl-date: TLS randomness does not represent time
Warning: OSScan results may be unreliable because we could no
t find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (91%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mod
e network gateway (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: cs2000.webhostbox.net; OS: Linux; CPE: cp
```

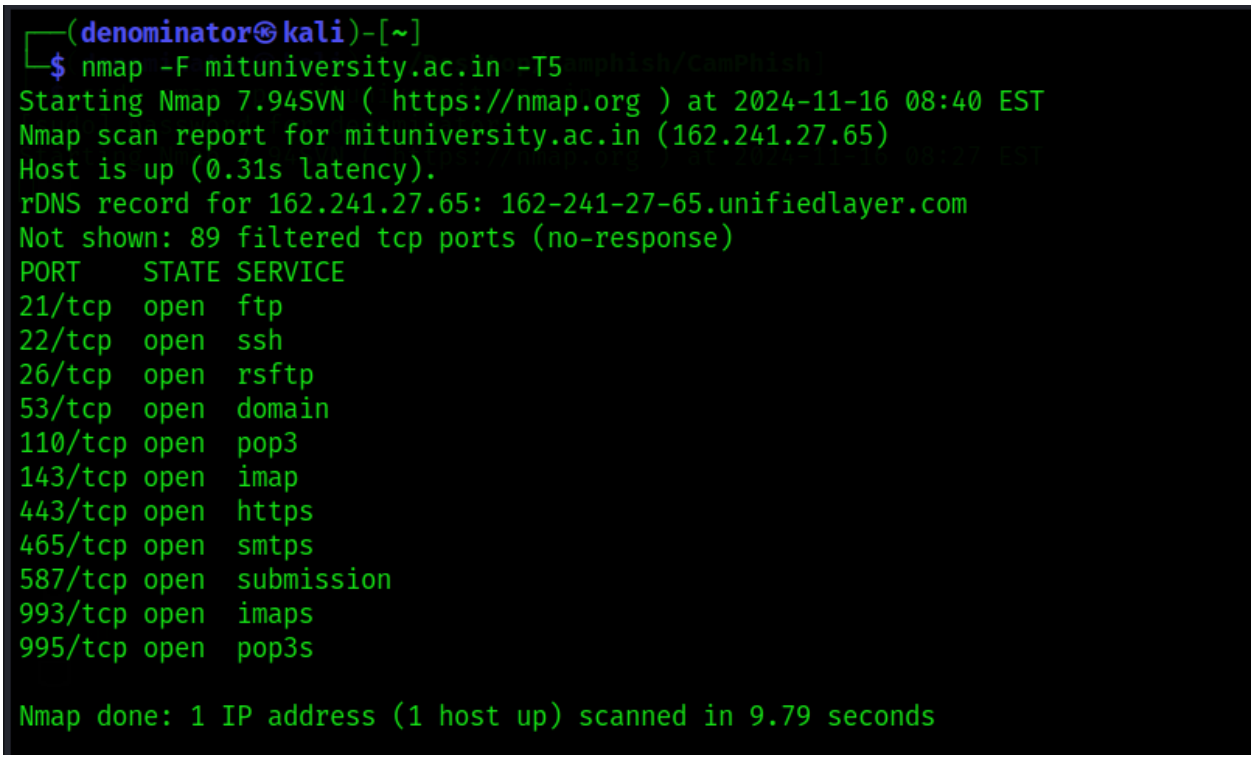
```
e:/o:redhat:enterprise_linux:7

TRACEROUTE (using port 993/tcp)
HOP RTT       ADDRESS
1   4.63 ms   10.0.2.2
2   296.98 ms 162-241-27-65.unifiedlayer.com (162.241.27.65)

OS and Service detection performed. Please report any incorre
ct results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 281.98 seconds
```

Top 100 ports scan:

command →

```
nmap -F mituniversity.ac.in
```

Output →


┌──(denominator㉿kali)-[~]
└─$ nmap -F mituniversity.ac.in -T5
Starting Nmap 7.94SVN (https://nmap.org) at 2024-11-16 08:40 EST
Nmap scan report for mituniversity.ac.in (162.241.27.65)
Host is up (0.31s latency).
rDNS record for 162.241.27.65: 162-241-27-65.unifiedlayer.com
Not shown: 89 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open ftp
22/tcp open ssh
26/tcp open rsftp
53/tcp open domain
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
Nmap done: 1 IP address (1 host up) scanned in 9.79 seconds