EXPERIMENT NO.7

AIM: Perform network discovery using discovery tools (eg. Nmap, mrtg)

Theory:

1. What features does nmap include?

- Host discovery – Identifying hosts on a network. For example, listing the hosts that respond to TCP and/or ICMP requests or have a particular port open.
- Port scanning – Enumerating the open ports on target hosts.
- Version detection – Interrogating network services on remote devices to determine application name and version number.
- TCP/IP stack fingerprinting – Determining the operating system and hardware characteristics of network devices based on observations of network activity of said devices.
- Scriptable interaction with the target – using Nmap Scripting Engine (NSE) and Lua programming language.

Nmap can provide further information on targets, including reverse DNS names, device types, and MAC addresses.

2. What are the uses of Nmap?

- Auditing the security of a device or firewall by identifying the network connections which can be made to, or through it.
- Identifying open ports on a target host in preparation for auditing.
- Network inventory, network mapping, maintenance and asset management.
- Auditing the security of a network by identifying new servers.
- Generating traffic to hosts on a network, response analysis and response time measurement.
- Finding and exploiting vulnerabilities in a network.
- DNS queries and subdomain search

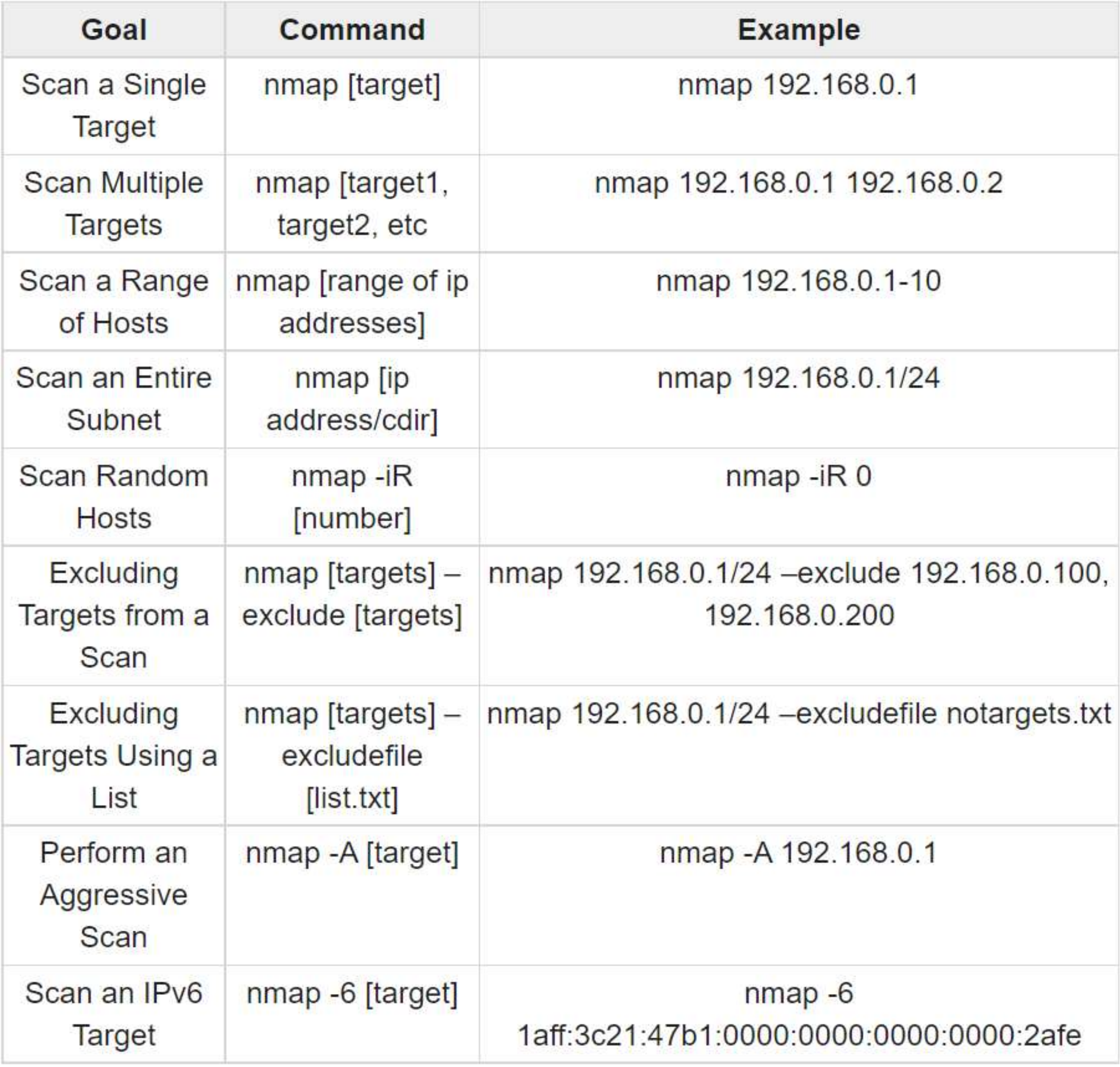
3. About Network Mapper(Nmap).

Nmap (Network Mapper) is a security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich) used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses. Unlike many simple port scanners that just send packets at some predefined constant rate, Nmap accounts for the network conditions (latency fluctuations, network congestion, the target interference with the scan) during the run. Also, owing to the large and active user community providing feedback and contributing to its features, Nmap has been able to extend its discovery capabilities beyond simply figuring out whether a host is up or down and which ports are open and closed; it can determine the operating system of the target, names and versions of the listening services, estimated uptime, type of device, and presence of a firewall.

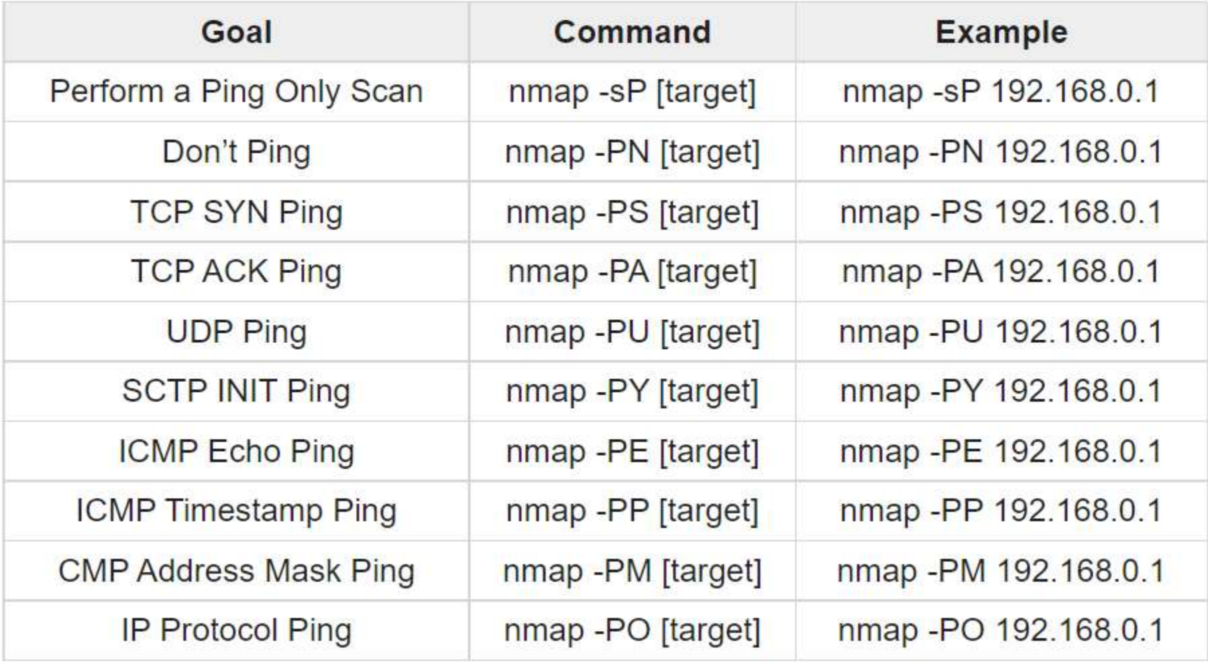
4. What are the Basic commands working in Nmap:

- For target specifications: nmap <target‘s URL or IP with spaces between them>
- For OS detection: nmap -O <target-host's URL or IP>
- For version detection: nmap -sV <target-host's URL or IP>

SYN scan is the default and most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. It is also relatively unobtrusive and stealthy since it never completes TCP connections



Goal	Command	Example
Scan a Single Target	nmap [target]	nmap 192.168.0.1
Scan Multiple Targets	nmap [target1, target2, etc	nmap 192.168.0.1 192.168.0.2
Scan a Range of Hosts	nmap [range of ip addresses]	nmap 192.168.0.1-10
Scan an Entire Subnet	nmap [ip address/cdir]	nmap 192.168.0.1/24
Scan Random Hosts	nmap -iR [number]	nmap -iR 0
Excluding Targets from a Scan	nmap [targets] –exclude [targets]	nmap 192.168.0.1/24 –exclude 192.168.0.100, 192.168.0.200
Excluding Targets Using a List	nmap [targets] –excludefile [list.txt]	nmap 192.168.0.1/24 –excludefile notargets.txt
Perform an Aggressive Scan	nmap -A [target]	nmap -A 192.168.0.1
Scan an IPv6 Target	nmap -6 [target]	nmap -6 1aff:3c21:47b1:0000:0000:0000:0000:2afe

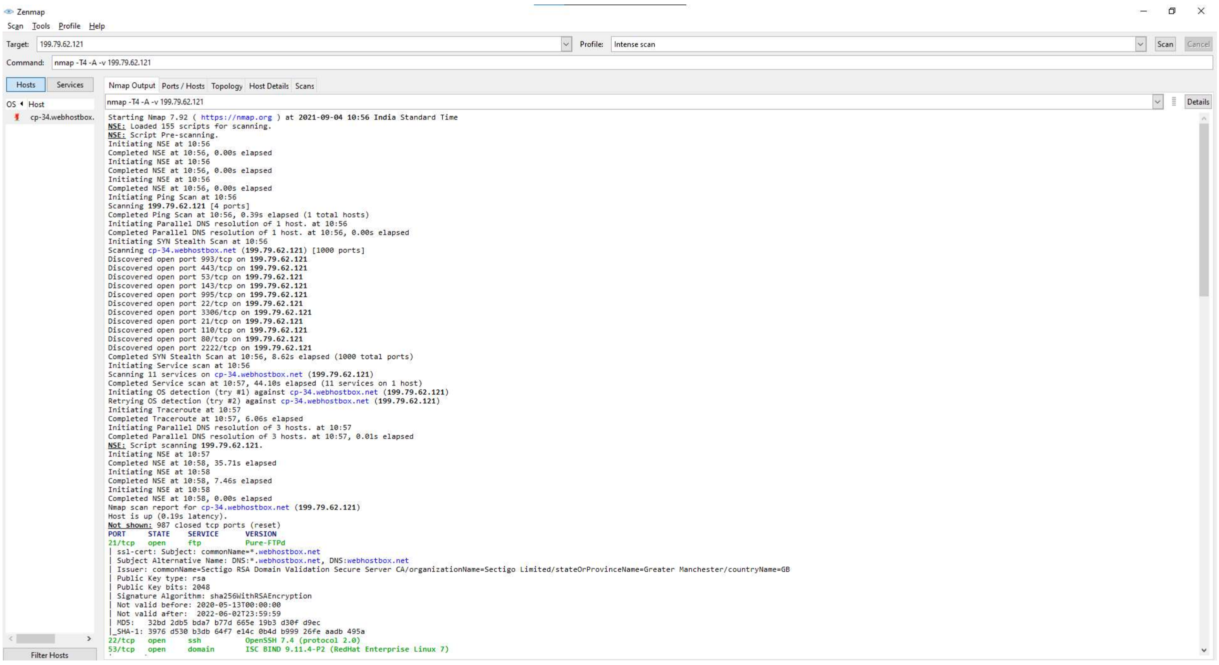


Goal	Command	Example
Perform a Ping Only Scan	nmap -sP [target]	nmap -sP 192.168.0.1
Don't Ping	nmap -PN [target]	nmap -PN 192.168.0.1
TCP SYN Ping	nmap -PS [target]	nmap -PS 192.168.0.1
TCP ACK Ping	nmap -PA [target]	nmap -PA 192.168.0.1
UDP Ping	nmap -PU [target]	nmap -PU 192.168.0.1
SCTP INIT Ping	nmap -PY [target]	nmap -PY 192.168.0.1
ICMP Echo Ping	nmap -PE [target]	nmap -PE 192.168.0.1
ICMP Timestamp Ping	nmap -PP [target]	nmap -PP 192.168.0.1
CMP Address Mask Ping	nmap -PM [target]	nmap -PM 192.168.0.1
IP Protocol Ping	nmap -PO [target]	nmap -PO 192.168.0.1

5. Algorithm\Implementation Steps\Installation Steps:

1. Download Nmap from www.nmap.org and install the Nmap Software with WinPcap Driver utility.
2. Execute the Nmap-Zenmap GUI tool from Program Menu or Desktop Icon
3. Type the Target Machine IP Address(ie.Guest OS or any website Address)
4. Perform the profiles shown in the utility.

Output:

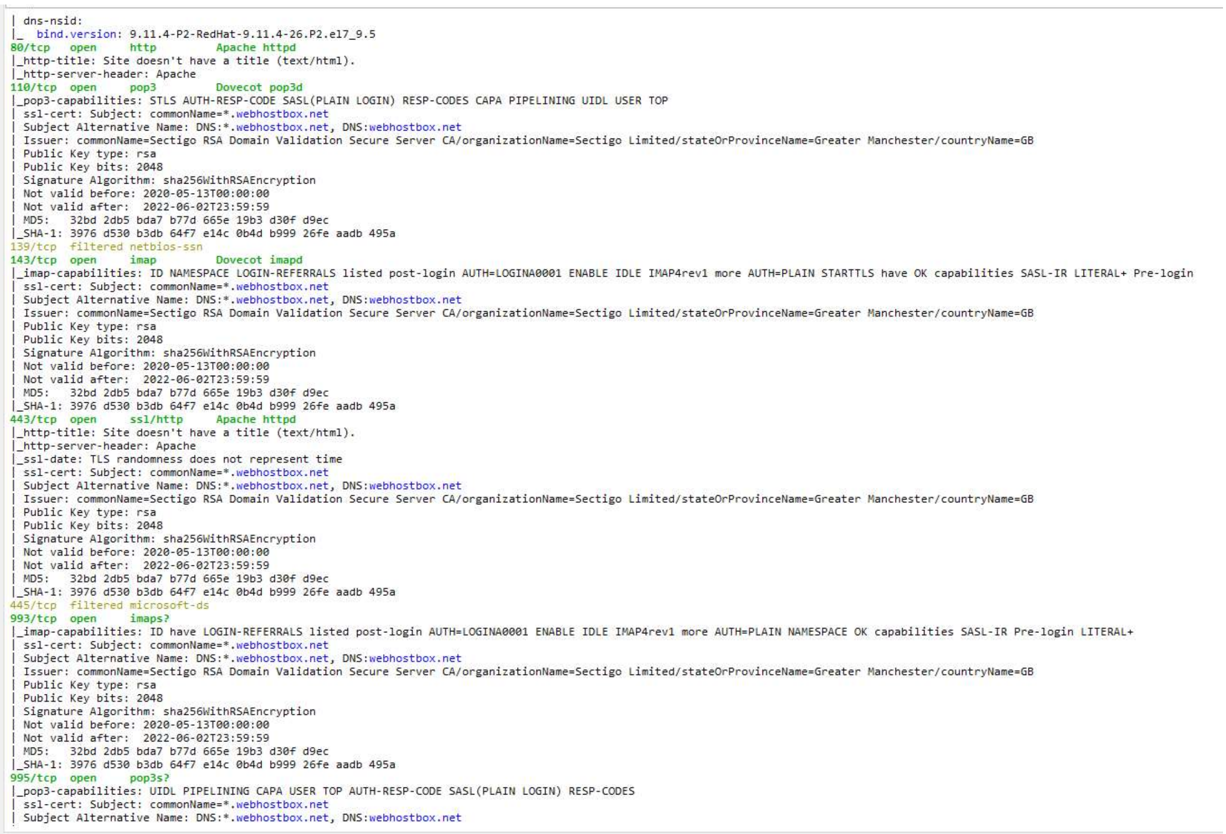


Target: 199.79.62.121

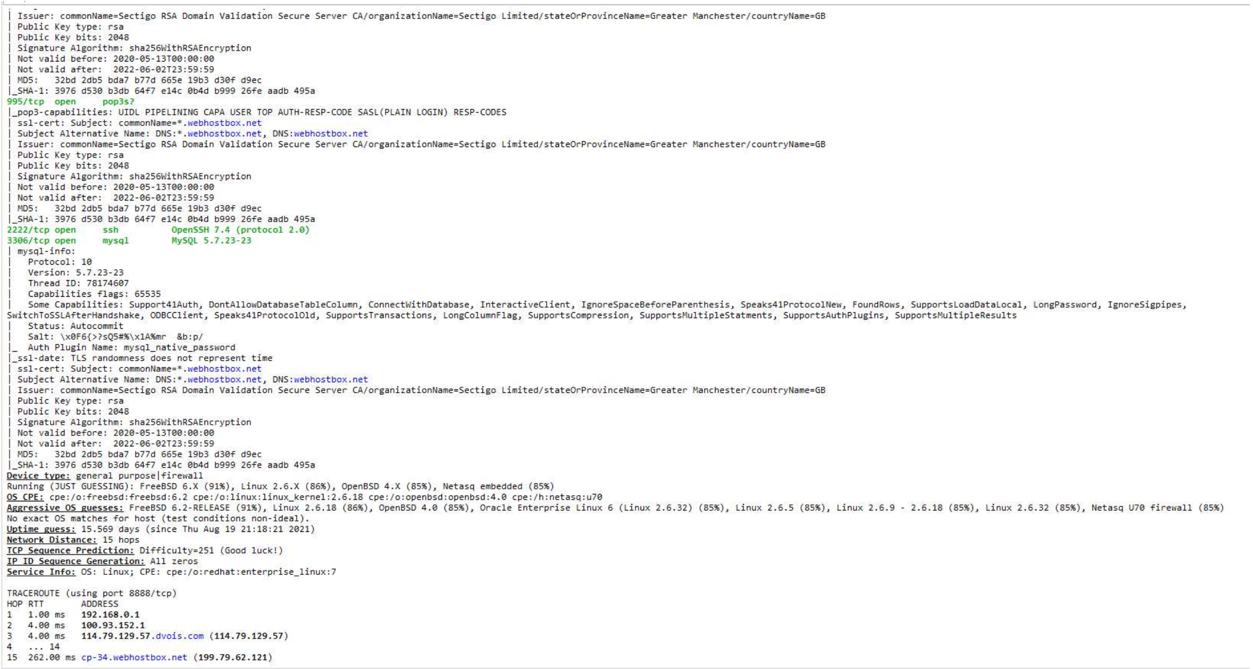
Profile: Intense scan

Command: nmap -T4 -A -v 199.79.62.121

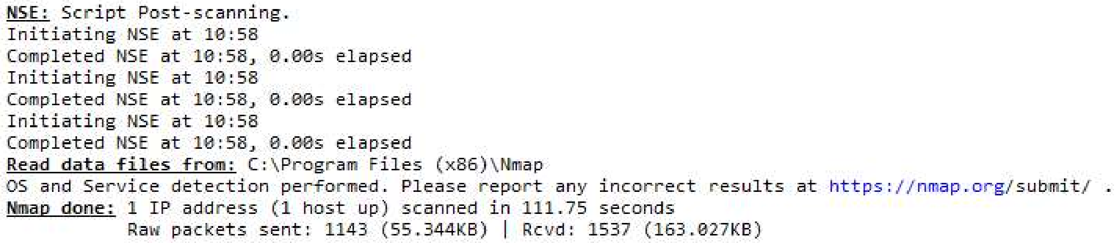
```
nmap -T4 -A -v 199.79.62.121

Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-04 10:56 India Standard Time
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:56
Completed NSE at 10:56, 0.00s elapsed
Initiating NSE at 10:56
Completed NSE at 10:56, 0.00s elapsed
Initiating NSE at 10:56
Completed NSE at 10:56, 0.00s elapsed
Initiating Ping Scan at 10:56
Scanning 199.79.62.121 [4 ports]
Completed Ping Scan at 10:56, 0.39s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:56
Completed Parallel DNS resolution of 1 host. at 10:56, 0.00s elapsed
Initiating SYN Stealth Scan at 10:56
Scanning cp-34.webhostbox.net (199.79.62.121) [1000 ports]
Discovered open port 993/tcp on 199.79.62.121
Discovered open port 443/tcp on 199.79.62.121
Discovered open port 53/tcp on 199.79.62.121
Discovered open port 143/tcp on 199.79.62.121
Discovered open port 995/tcp on 199.79.62.121
Discovered open port 22/tcp on 199.79.62.121
Discovered open port 3306/tcp on 199.79.62.121
Discovered open port 21/tcp on 199.79.62.121
Discovered open port 110/tcp on 199.79.62.121
Discovered open port 80/tcp on 199.79.62.121
Discovered open port 2222/tcp on 199.79.62.121
Completed SYN Stealth Scan at 10:56, 8.62s elapsed (1000 total ports)
Initiating Service scan at 10:56
Scanning 11 services on cp-34.webhostbox.net (199.79.62.121)
Completed Service scan at 10:57, 44.10s elapsed (11 services on 1 host)
Initiating OS detection (try #1) against cp-34.webhostbox.net (199.79.62.121)
Retrying OS detection (try #2) against cp-34.webhostbox.net (199.79.62.121)
Initiating Traceroute at 10:57
Completed Traceroute at 10:57, 6.06s elapsed
Initiating Parallel DNS resolution of 3 hosts. at 10:57
Completed Parallel DNS resolution of 3 hosts. at 10:57, 0.01s elapsed
NSE: Script scanning 199.79.62.121.
Initiating NSE at 10:57
Completed NSE at 10:58, 35.71s elapsed
Initiating NSE at 10:58
Completed NSE at 10:58, 7.46s elapsed
Initiating NSE at 10:58
Completed NSE at 10:58, 0.00s elapsed
Nmap scan report for cp-34.webhostbox.net (199.79.62.121)
Host is up (0.19s latency).
Not shown: 987 closed tcp ports (reset)
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          Pure-FTPd
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhostbox.net
| Issuer: commonName=Sectigo RSA Domain Validation Secure Server CA/organizationName=Sectigo Limited/stateOrProvinceName=Greater Manchester/countryName=GB
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-05-13T00:00:00
| Not valid after:  2022-06-02T23:59:59
| MD5:   32bd 2db5 bda7 b77d 665e 19b3 d30f d9ec
|_SHA-1: 3976 d530 b3db 64f7 e14c 0b4d b999 26fe aadb 495a
22/tcp   open     ssh          OpenSSH 7.4 (protocol 2.0)
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_9.5
80/tcp   open     http          Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
110/tcp  open     pop3          Dovecot pop3d
|_pop3-capabilities: STLS AUTH-RESP-CODE SASL(PLAIN LOGIN) RESP-CODES CAPA PIPELINING UIDL USER TOP
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhostbox.net
| Issuer: commonName=Sectigo RSA Domain Validation Secure Server CA/organizationName=Sectigo Limited/stateOrProvinceName=Greater Manchester/countryName=GB
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-05-13T00:00:00
| Not valid after:  2022-06-02T23:59:59
| MD5:   32bd 2db5 bda7 b77d 665e 19b3 d30f d9ec
|_SHA-1: 3976 d530 b3db 64f7 e14c 0b4d b999 26fe aadb 495a
139/tcp  filtered netbios-ssn
143/tcp  open     imap          Dovecot imapd
|_imap-capabilities: ID NAMESPACE LOGIN-REFERRALS listed post-login AUTH=LOGINA0001 ENABLE IDLE IMAP4rev1 more AUTH=PLAIN STARTTLS have OK capabilities SASL-IR LITERAL+ Pre-login
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhostbox.net
| Issuer: commonName=Sectigo RSA Domain Validation Secure Server CA/organizationName=Sectigo Limited/stateOrProvinceName=Greater Manchester/countryName=GB
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-05-13T00:00:00
| Not valid after:  2022-06-02T23:59:59
| MD5:   32bd 2db5 bda7 b77d 665e 19b3 d30f d9ec
|_SHA-1: 3976 d530 b3db 64f7 e14c 0b4d b999 26fe aadb 495a
443/tcp  open     ssl/http      Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhostbox.net
| Issuer: commonName=Sectigo RSA Domain Validation Secure Server CA/organizationName=Sectigo Limited/stateOrProvinceName=Greater Manchester/countryName=GB
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-05-13T00:00:00
| Not valid after:  2022-06-02T23:59:59
| MD5:   32bd 2db5 bda7 b77d 665e 19b3 d30f d9ec
|_SHA-1: 3976 d530 b3db 64f7 e14c 0b4d b999 26fe aadb 495a
445/tcp  filtered microsoft-ds
993/tcp  open     imaps?
|_imap-capabilities: ID have LOGIN-REFERRALS listed post-login AUTH=LOGINA0001 ENABLE IDLE IMAP4rev1 more AUTH=PLAIN NAMESPACE OK capabilities SASL-IR Pre-login LITERAL+
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhostbox.net
| Issuer: commonName=Sectigo RSA Domain Validation Secure Server CA/organizationName=Sectigo Limited/stateOrProvinceName=Greater Manchester/countryName=GB
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-05-13T00:00:00
| Not valid after:  2022-06-02T23:59:59
| MD5:   32bd 2db5 bda7 b77d 665e 19b3 d30f d9ec
|_SHA-1: 3976 d530 b3db 64f7 e14c 0b4d b999 26fe aadb 495a
995/tcp  open     pop3s?
|_pop3-capabilities: UIDL PIPELINING CAPA USER TOP AUTH-RESP-CODE SASL(PLAIN LOGIN) RESP-CODES
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhostbox.net
```

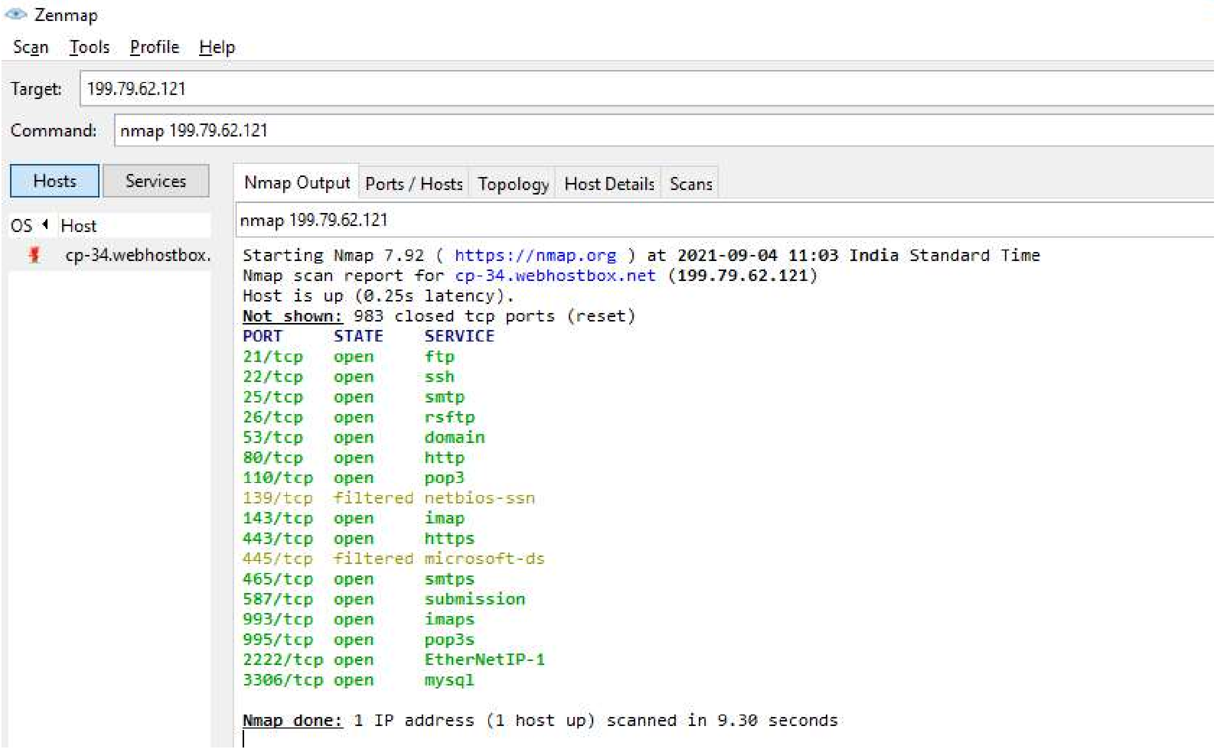


```
| Issuer: commonName=Sectigo RSA Domain Validation Secure Server CA/organizationName=Sectigo Limited/stateOrProvinceName=Greater Manchester/countryName=GB
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-05-13T00:00:00
| Not valid after:  2022-06-02T23:59:59
| MD5:   32bd 2db5 bda7 b77d 665e 19b3 d30f d9ec
|_SHA-1: 3976 d530 b3db 64f7 e14c 0b4d b999 26fe aadb 495a
995/tcp  open     pop3s?
|_pop3-capabilities: UIDL PIPELINING CAPA USER TOP AUTH-RESP-CODE SASL(PLAIN LOGIN) RESP-CODES
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhostbox.net
| Issuer: commonName=Sectigo RSA Domain Validation Secure Server CA/organizationName=Sectigo Limited/stateOrProvinceName=Greater Manchester/countryName=GB
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-05-13T00:00:00
| Not valid after:  2022-06-02T23:59:59
| MD5:   32bd 2db5 bda7 b77d 665e 19b3 d30f d9ec
|_SHA-1: 3976 d530 b3db 64f7 e14c 0b4d b999 26fe aadb 495a
2222/tcp open     ssh          OpenSSH 7.4 (protocol 2.0)
3306/tcp open     mysql        MySQL 5.7.23-23
| mysql-info:
|   Protocol: 10
|   Version: 5.7.23-23
|   Thread ID: 78174607
|   Capabilities flags: 65535
|   Some Capabilities: Support41Auth, DontAllowDatabaseTableColumn, ConnectWithDatabase, InteractiveClient, IgnoreSpaceBeforeParenthesis, Speaks41ProtocolNew, FoundRows, SupportsLoadDataLocal, LongPassword, IgnoreSigpipes,
SwitchToSSLAfterHandshake, ODBCClient, Speaks41ProtocolOld, SupportsTransactions, LongColumnFlag, SupportsCompression, SupportsMultipleStatments, SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: \x0F6{>?sQ5#%\x1A%mr  &b:p/
|_  Auth Plugin Name: mysql_native_password
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhostbox.net
| Issuer: commonName=Sectigo RSA Domain Validation Secure Server CA/organizationName=Sectigo Limited/stateOrProvinceName=Greater Manchester/countryName=GB
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-05-13T00:00:00
| Not valid after:  2022-06-02T23:59:59
| MD5:   32bd 2db5 bda7 b77d 665e 19b3 d30f d9ec
|_SHA-1: 3976 d530 b3db 64f7 e14c 0b4d b999 26fe aadb 495a
Device type: general purpose|firewall
Running (JUST GUESSING): FreeBSD 6.X (91%), Linux 2.6.X (86%), OpenBSD 4.X (85%), Netasq embedded (85%)
OS CPE: cpe:/o:freebsd:freebsd:6.2 cpe:/o:linux:linux_kernel:2.6.18 cpe:/o:openbsd:openbsd:4.0 cpe:/h:netasq:u70
Aggressive OS guesses: FreeBSD 6.2-RELEASE (91%), Linux 2.6.18 (86%), OpenBSD 4.0 (85%), Oracle Enterprise Linux 6 (Linux 2.6.32) (85%), Linux 2.6.5 (85%), Linux 2.6.9 - 2.6.18 (85%), Linux 2.6.32 (85%), Netasq U70 firewall (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 15.569 days (since Thu Aug 19 21:18:21 2021)
Network Distance: 15 hops
TCP Sequence Prediction: Difficulty=251 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7

TRACEROUTE (using port 8888/tcp)
HOP RTT       ADDRESS
1   1.00 ms   192.168.0.1
2   4.00 ms   100.93.152.1
3   4.00 ms   114.79.129.57.dvois.com (114.79.129.57)
4   ... 14
15  262.00 ms cp-34.webhostbox.net (199.79.62.121)
```



```
NSE: Script Post-scanning.
Initiating NSE at 10:58
Completed NSE at 10:58, 0.00s elapsed
Initiating NSE at 10:58
Completed NSE at 10:58, 0.00s elapsed
Initiating NSE at 10:58
Completed NSE at 10:58, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 111.75 seconds
           Raw packets sent: 1143 (55.344KB) | Rcvd: 1537 (163.027KB)
```

nmap:

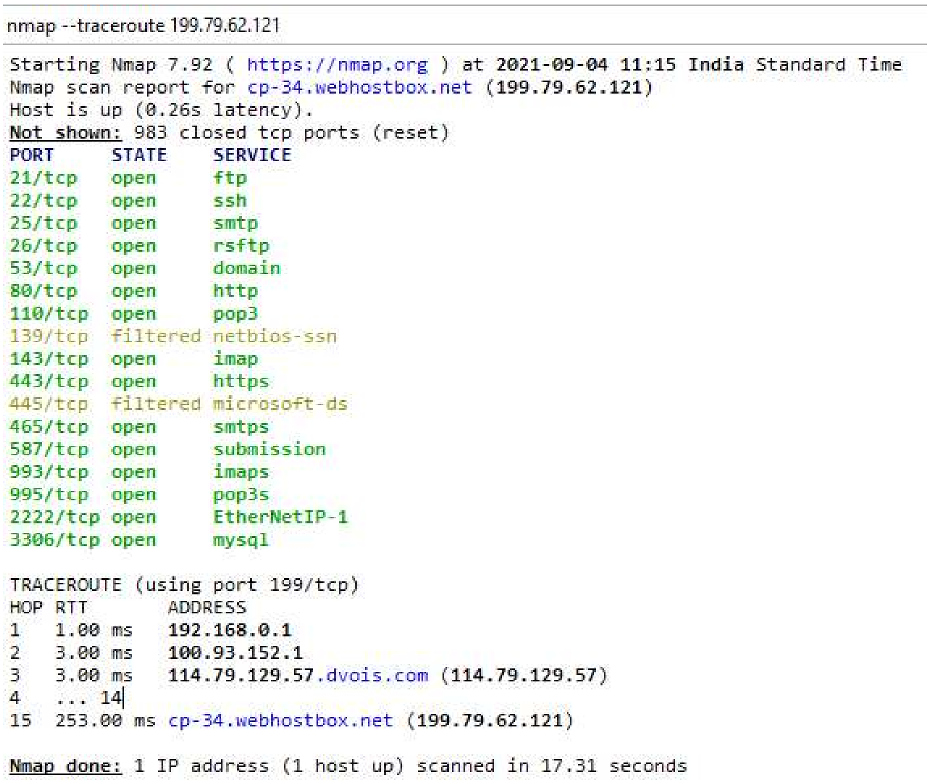


Target: 199.79.62.121

Command: nmap 199.79.62.121

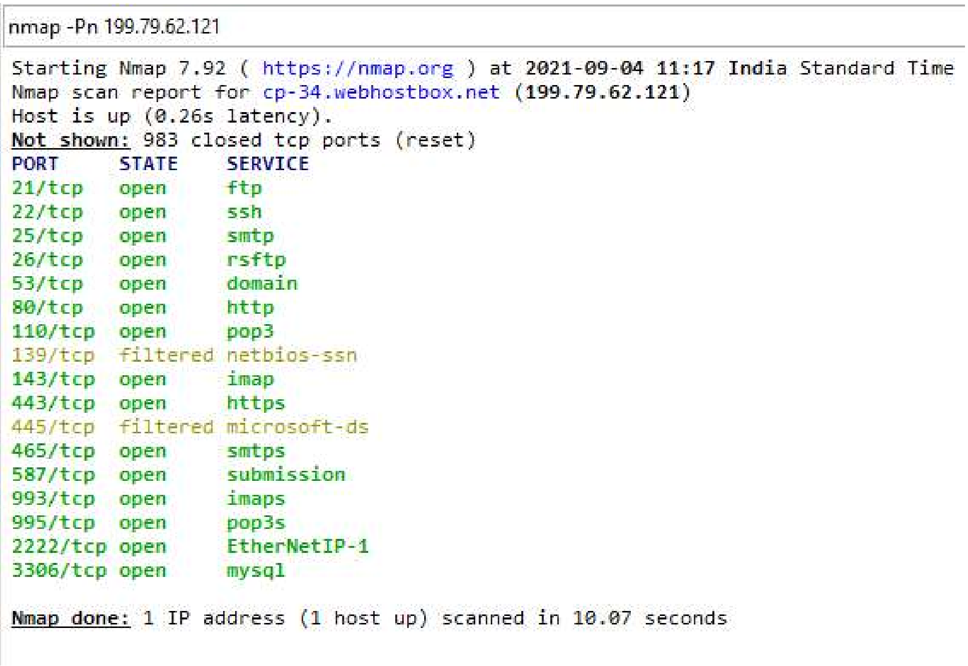
```
nmap 199.79.62.121

Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-04 11:03 India Standard Time
Nmap scan report for cp-34.webhostbox.net (199.79.62.121)
Host is up (0.25s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   open     smtp
26/tcp   open     rsftp
53/tcp   open     domain
80/tcp   open     http
110/tcp  open     pop3
139/tcp  filtered netbios-ssn
143/tcp  open     imap
443/tcp  open     https
445/tcp  filtered microsoft-ds
465/tcp  open     smtps
587/tcp  open     submission
993/tcp  open     imaps
995/tcp  open     pop3s
2222/tcp open     EtherNetIP-1
3306/tcp open     mysql

Nmap done: 1 IP address (1 host up) scanned in 9.30 seconds
```

traceroute:



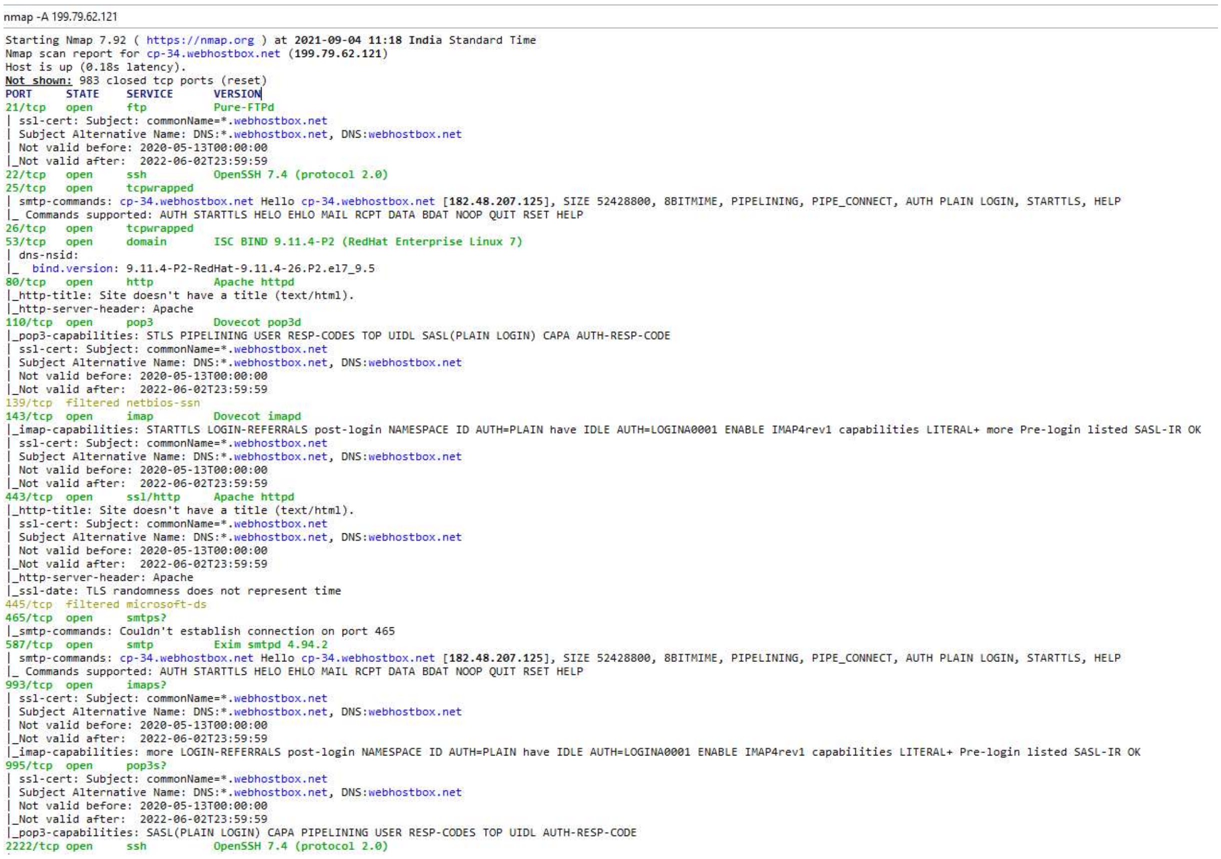
```
nmap --traceroute 199.79.62.121

Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-04 11:15 India Standard Time
Nmap scan report for cp-34.webhostbox.net (199.79.62.121)
Host is up (0.26s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   open     smtp
26/tcp   open     rsftp
53/tcp   open     domain
80/tcp   open     http
110/tcp  open     pop3
139/tcp  filtered netbios-ssn
143/tcp  open     imap
443/tcp  open     https
445/tcp  filtered microsoft-ds
465/tcp  open     smtps
587/tcp  open     submission
993/tcp  open     imaps
995/tcp  open     pop3s
2222/tcp open     EtherNetIP-1
3306/tcp open     mysql

TRACEROUTE (using port 199/tcp)
HOP RTT       ADDRESS
1   1.00 ms   192.168.0.1
2   3.00 ms   100.93.152.1
3   3.00 ms   114.79.129.57.dvois.com (114.79.129.57)
4   ... 14
15  253.00 ms cp-34.webhostbox.net (199.79.62.121)

Nmap done: 1 IP address (1 host up) scanned in 17.31 seconds
```

ip protocol:

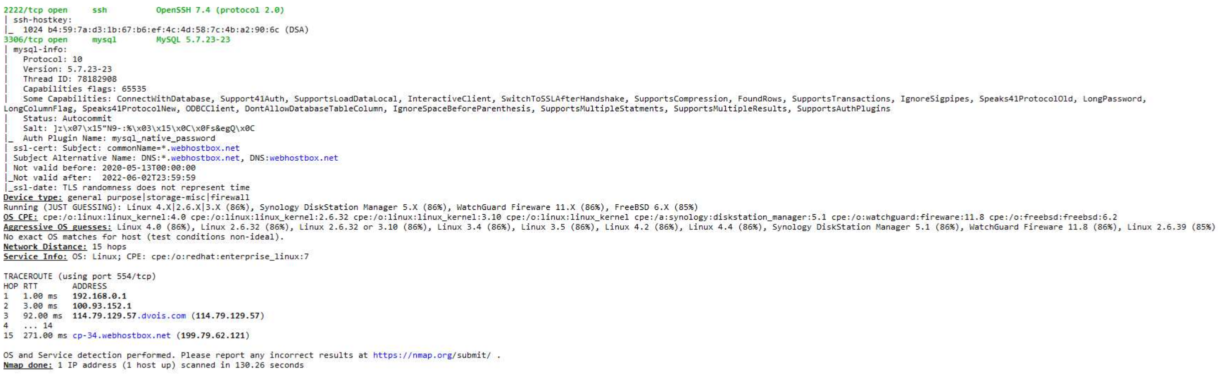


```
nmap -Pn 199.79.62.121

Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-04 11:17 India Standard Time
Nmap scan report for cp-34.webhostbox.net (199.79.62.121)
Host is up (0.26s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   open     smtp
26/tcp   open     rsftp
53/tcp   open     domain
80/tcp   open     http
110/tcp  open     pop3
139/tcp  filtered netbios-ssn
143/tcp  open     imap
443/tcp  open     https
445/tcp  filtered microsoft-ds
465/tcp  open     smtps
587/tcp  open     submission
993/tcp  open     imaps
995/tcp  open     pop3s
2222/tcp open     EtherNetIP-1
3306/tcp open     mysql

Nmap done: 1 IP address (1 host up) scanned in 10.07 seconds
```

aggressive scan of IP address:

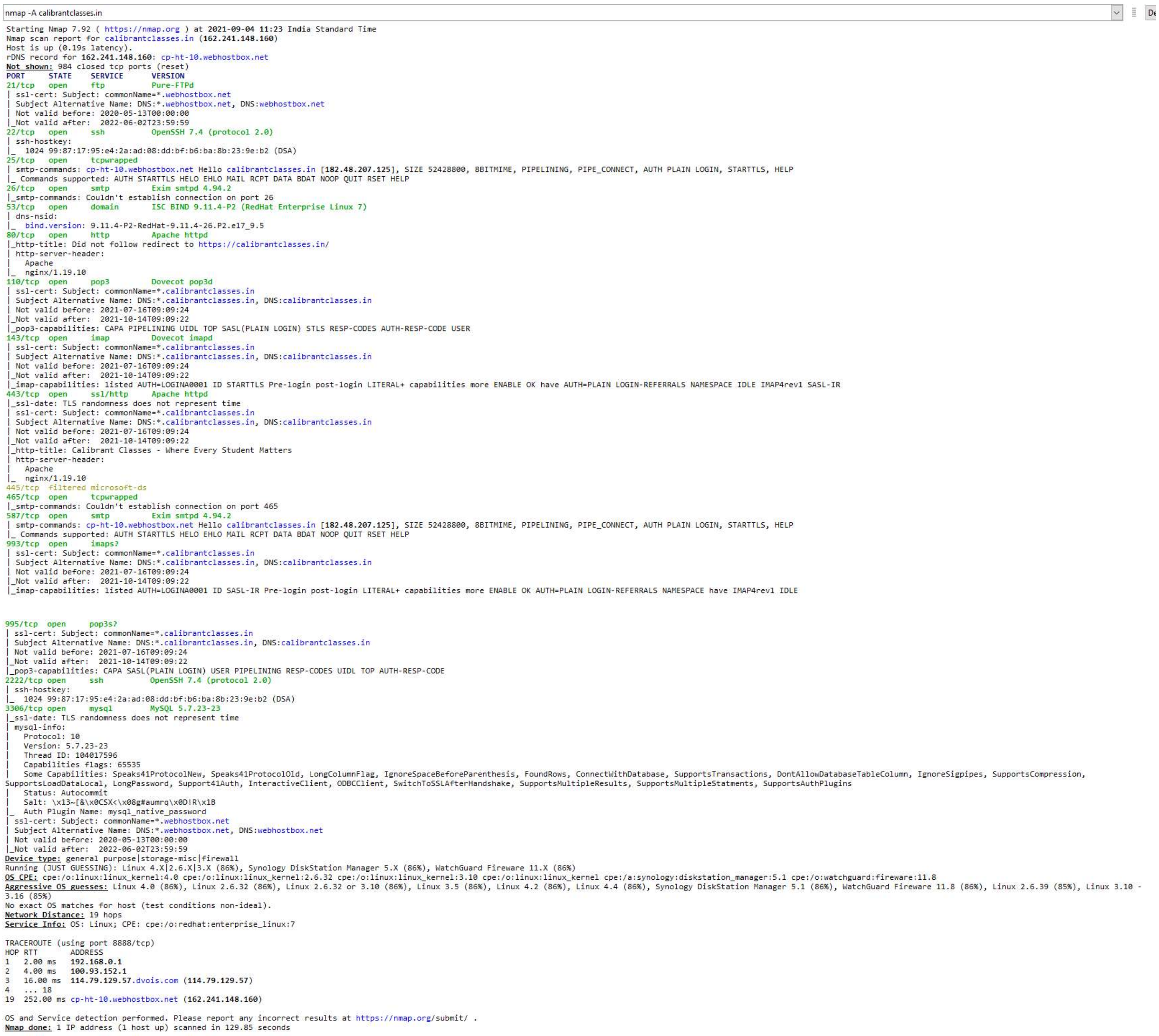


```
nmap -A 199.79.62.121

Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-04 11:18 India Standard Time
Nmap scan report for cp-34.webhostbox.net (199.79.62.121)
Host is up (0.18s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          Pure-FTPd
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhostbox.net
| Not valid before: 2020-05-13T00:00:00
|_Not valid after:  2022-06-02T23:59:59
22/tcp   open     ssh          OpenSSH 7.4 (protocol 2.0)
25/tcp   open     tcpwrapped
| smtp-commands: cp-34.webhostbox.net Hello cp-34.webhostbox.net [182.48.207.125], SIZE 52428800, 8BITMIME, PIPELINING, PIPE_CONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
26/tcp   open     tcpwrapped
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_9.5
80/tcp   open     http         Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
110/tcp  open     pop3         Dovecot pop3d
|_pop3-capabilities: STLS PIPELINING USER RESP-CODES TOP UIDL SASL(PLAIN LOGIN) CAPA AUTH-RESP-CODE
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhostbox.net
| Not valid before: 2020-05-13T00:00:00
|_Not valid after:  2022-06-02T23:59:59
139/tcp  filtered netbios-ssn
143/tcp  open     imap         Dovecot imapd
|_imap-capabilities: STARTTLS LOGIN-REFERRALS post-login NAMESPACE ID AUTH=PLAIN have IDLE AUTH=LOGINA0001 ENABLE IMAP4rev1 capabilities LITERAL+ more Pre-login listed SASL-IR OK
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhostbox.net
| Not valid before: 2020-05-13T00:00:00
|_Not valid after:  2022-06-02T23:59:59
443/tcp  open     ssl/http     Apache httpd
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhostbox.net
| Not valid before: 2020-05-13T00:00:00
|_Not valid after:  2022-06-02T23:59:59
|_http-server-header: Apache
|_ssl-date: TLS randomness does not represent time
445/tcp  filtered microsoft-ds
465/tcp  open     smtps?
|_smtp-commands: Couldn't establish connection on port 465
587/tcp  open     smtp         Exim smtpd 4.94.2
| smtp-commands: cp-34.webhostbox.net Hello cp-34.webhostbox.net [182.48.207.125], SIZE 52428800, 8BITMIME, PIPELINING, PIPE_CONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
993/tcp  open     imaps?
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhostbox.net
| Not valid before: 2020-05-13T00:00:00
|_Not valid after:  2022-06-02T23:59:59
|_imap-capabilities: more LOGIN-REFERRALS post-login NAMESPACE ID AUTH=PLAIN have IDLE AUTH=LOGINA0001 ENABLE IMAP4rev1 capabilities LITERAL+ Pre-login listed SASL-IR OK
995/tcp  open     pop3s?
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhostbox.net
| Not valid before: 2020-05-13T00:00:00
|_Not valid after:  2022-06-02T23:59:59
|_pop3-capabilities: SASL(PLAIN LOGIN) CAPA PIPELINING USER RESP-CODES TOP UIDL AUTH-RESP-CODE
2222/tcp open     ssh          OpenSSH 7.4 (protocol 2.0)
```



```
2222/tcp open     ssh          OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|_  1024 b4:59:7a:d3:1b:67:b6:ef:4c:4d:58:7c:4b:a2:90:6c (DSA)
3306/tcp open     mysql        MySQL 5.7.23-23
| mysql-info:
|   Protocol: 10
|   Version: 5.7.23-23
|   Thread ID: 78182908
|   Capabilities flags: 65535
|   Some Capabilities: ConnectWithDatabase, Support41Auth, SupportsLoadDataLocal, InteractiveClient, SwitchToSSLAfterHandshake, SupportsCompression, FoundRows, SupportsTransactions, IgnoreSigpipes, Speaks41ProtocolOld, LongPassword,
LongColumnFlag, Speaks41ProtocolNew, ODBCClient, DontAllowDatabaseTableColumn, IgnoreSpaceBeforeParenthesis, SupportsMultipleStatments, SupportsMultipleResults, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: ]z\x07\x15"N9-:%\x03\x15\x0C\x0Fs&egQ\x0C
|_  Auth Plugin Name: mysql_native_password
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhostbox.net
| Not valid before: 2020-05-13T00:00:00
|_Not valid after:  2022-06-02T23:59:59
|_ssl-date: TLS randomness does not represent time
Device type: general purpose|storage-misc|firewall
Running (JUST GUESSING): Linux 4.X|2.6.X|3.X (86%), Synology DiskStation Manager 5.X (86%), WatchGuard Fireware 11.X (86%), FreeBSD 6.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:4.0 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10 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 4.0 (86%), Linux 2.6.32 (86%), Linux 2.6.32 or 3.10 (86%), Linux 3.4 (86%), Linux 3.5 (86%), Linux 4.2 (86%), Linux 4.4 (86%), Synology DiskStation Manager 5.1 (86%), WatchGuard Fireware 11.8 (86%), Linux 2.6.39 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 15 hops
Service Info: OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7

TRACEROUTE (using port 554/tcp)
HOP RTT       ADDRESS
1   1.00 ms   192.168.0.1
2   3.00 ms   100.93.152.1
3   92.00 ms  114.79.129.57.dvois.com (114.79.129.57)
4   ... 14
15  271.00 ms cp-34.webhostbox.net (199.79.62.121)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 130.26 seconds
```

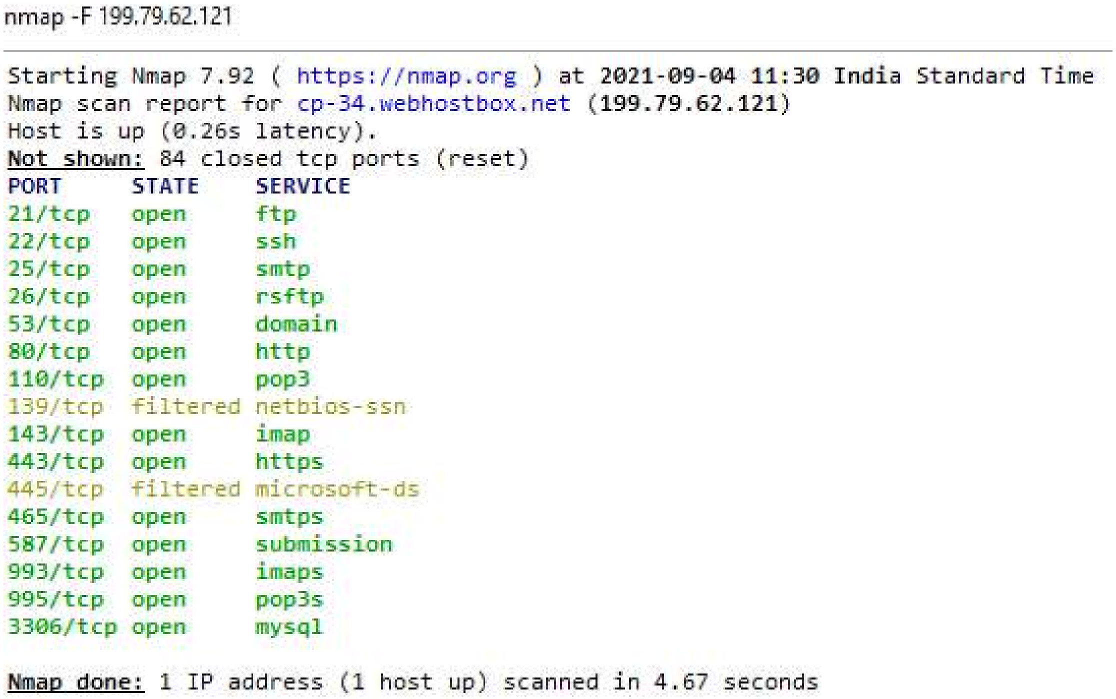
aggressive scan of website:



```
nmap -A calibrantclasses.in
```

```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-04 11:23 India Standard Time
Nmap scan report for calibrantclasses.in (162.241.148.160)
Host is up (0.19s latency).
rDNS record for 162.241.148.160: cp-ht-10.webhostbox.net
Not shown: 984 closed tcp ports (reset)
PORT     STATE    SERVICE     VERSION
21/tcp   open     ftp         Pure-FTPd
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhostbox.net
| Not valid before: 2020-05-13T00:00:00
|_Not valid after:  2022-06-02T23:59:59
22/tcp   open     ssh         OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|_  1024 99:87:17:95:e4:2a:ad:08:dd:bf:b6:ba:8b:23:9e:b2 (DSA)
25/tcp   open     tcpwrapped
| smtp-commands: cp-ht-10.webhostbox.net Hello calibrantclasses.in [182.48.207.125], SIZE 52428800, 8BITMIME, PIPELINING, PIPE_CONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
26/tcp   open     smtp        Exim smtpd 4.94.2
|_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_9.5
80/tcp   open     http        Apache httpd
|_http-title: Did not follow redirect to https://calibrantclasses.in/
| http-server-header:
|   Apache
|_  nginx/1.19.10
110/tcp  open     pop3        Dovecot pop3d
| ssl-cert: Subject: commonName=*.calibrantclasses.in
| Subject Alternative Name: DNS:*.calibrantclasses.in, DNS:calibrantclasses.in
| Not valid before: 2021-07-16T09:09:24
|_Not valid after:  2021-10-14T09:09:22
|_pop3-capabilities: CAPA PIPELINING UIDL TOP SASL(PLAIN LOGIN) STLS RESP-CODES AUTH-RESP-CODE USER
143/tcp  open     imap        Dovecot imapd
| ssl-cert: Subject: commonName=*.calibrantclasses.in
| Subject Alternative Name: DNS:*.calibrantclasses.in, DNS:calibrantclasses.in
| Not valid before: 2021-07-16T09:09:24
|_Not valid after:  2021-10-14T09:09:22
|_imap-capabilities: listed AUTH=LOGINA0001 ID STARTTLS Pre-login post-login LITERAL+ capabilities more ENABLE OK have AUTH=PLAIN LOGIN-REFERRALS NAMESPACE IDLE IMAP4rev1 SASL-IR
443/tcp  open     ssl/http    Apache httpd
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=*.calibrantclasses.in
| Subject Alternative Name: DNS:*.calibrantclasses.in, DNS:calibrantclasses.in
| Not valid before: 2021-07-16T09:09:24
|_Not valid after:  2021-10-14T09:09:22
|_http-title: Calibrant Classes - Where Every Student Matters
| http-server-header:
|   Apache
|_  nginx/1.19.10
445/tcp  filtered microsoft-ds
465/tcp  open     tcpwrapped
|_smtp-commands: Couldn't establish connection on port 465
587/tcp  open     smtp        Exim smtpd 4.94.2
| smtp-commands: cp-ht-10.webhostbox.net Hello calibrantclasses.in [182.48.207.125], SIZE 52428800, 8BITMIME, PIPELINING, PIPE_CONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
993/tcp  open     imaps?
| ssl-cert: Subject: commonName=*.calibrantclasses.in
| Subject Alternative Name: DNS:*.calibrantclasses.in, DNS:calibrantclasses.in
| Not valid before: 2021-07-16T09:09:24
|_Not valid after:  2021-10-14T09:09:22
|_imap-capabilities: listed AUTH=LOGINA0001 ID SASL-IR Pre-login post-login LITERAL+ capabilities more ENABLE OK AUTH=PLAIN LOGIN-REFERRALS NAMESPACE have IMAP4rev1 IDLE


995/tcp  open     pop3s?
| ssl-cert: Subject: commonName=*.calibrantclasses.in
| Subject Alternative Name: DNS:*.calibrantclasses.in, DNS:calibrantclasses.in
| Not valid before: 2021-07-16T09:09:24
|_Not valid after:  2021-10-14T09:09:22
|_pop3-capabilities: CAPA SASL(PLAIN LOGIN) USER PIPELINING RESP-CODES UIDL TOP AUTH-RESP-CODE
2222/tcp open     ssh         OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|_  1024 99:87:17:95:e4:2a:ad:08:dd:bf:b6:ba:8b:23:9e:b2 (DSA)
3306/tcp open     mysql       MySQL 5.7.23-23
|_ssl-date: TLS randomness does not represent time
| mysql-info:
|   Protocol: 10
|   Version: 5.7.23-23
|   Thread ID: 104017596
|   Capabilities flags: 65535
|   Some Capabilities: Speaks41ProtocolNew, Speaks41ProtocolOld, LongColumnFlag, IgnoreSpaceBeforeParenthesis, FoundRows, ConnectWithDatabase, SupportsTransactions, DontAllowDatabaseTableColumn, IgnoreSigpipes, SupportsCompression,
SupportsLoadDataLocal, LongPassword, Support41Auth, InteractiveClient, ODBCClient, SwitchToSSLAfterHandshake, SupportsMultipleResults, SupportsMultipleStatments, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: \x13~[&\x0CSX<\x08g#aumrq\x0D!R\x1B
|_  Auth Plugin Name: mysql_native_password
| ssl-cert: Subject: commonName=*.webhostbox.net
| Subject Alternative Name: DNS:*.webhostbox.net, DNS:webhostbox.net
| Not valid before: 2020-05-13T00:00:00
|_Not valid after:  2022-06-02T23:59:59
Device type: general purpose|storage-misc|firewall
Running (JUST GUESSING): Linux 4.X|2.6.X|3.X (86%), Synology DiskStation Manager 5.X (86%), WatchGuard Fireware 11.X (86%)
OS CPE: cpe:/o:linux:linux_kernel:4.0 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10 cpe:/o:linux:linux_kernel cpe:/a:synology:diskstation_manager:5.1 cpe:/o:watchguard:fireware:11.8
Aggressive OS guesses: Linux 4.0 (86%), Linux 2.6.32 (86%), Linux 2.6.32 or 3.10 (86%), Linux 3.5 (86%), Linux 4.2 (86%), Linux 4.4 (86%), Synology DiskStation Manager 5.1 (86%), WatchGuard Fireware 11.8 (86%), Linux 2.6.39 (85%), Linux 3.10 -
3.16 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 19 hops
Service Info: OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7

TRACEROUTE (using port 8888/tcp)
HOP RTT       ADDRESS
1   2.00 ms   192.168.0.1
2   4.00 ms   100.93.152.1
3   16.00 ms  114.79.129.57.dvois.com (114.79.129.57)
4   ... 18
19  252.00 ms cp-ht-10.webhostbox.net (162.241.148.160)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 129.85 seconds
```

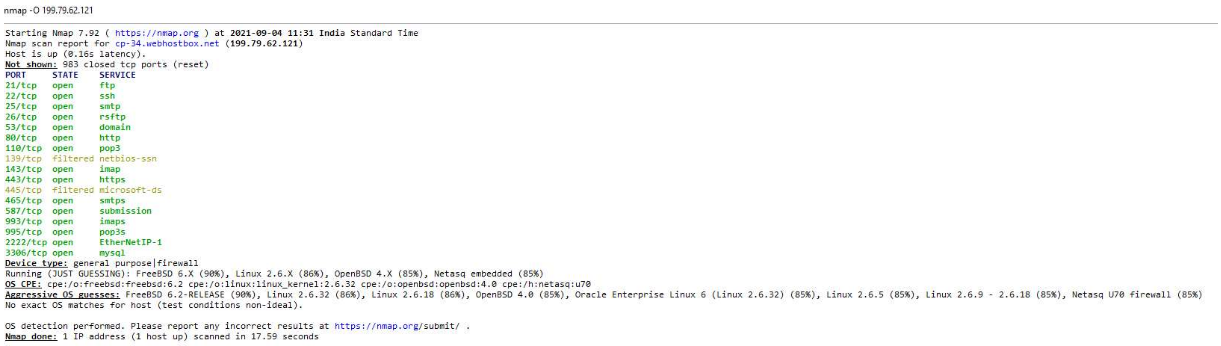
Fast Scan:



```
nmap -F 199.79.62.121
```

```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-04 11:30 India Standard Time
Nmap scan report for cp-34.webhostbox.net (199.79.62.121)
Host is up (0.26s latency).
Not shown: 84 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   open     smtp
26/tcp   open     rsftp
53/tcp   open     domain
80/tcp   open     http
110/tcp  open     pop3
139/tcp  filtered netbios-ssn
143/tcp  open     imap
443/tcp  open     https
445/tcp  filtered microsoft-ds
465/tcp  open     smtps
587/tcp  open     submission
993/tcp  open     imaps
995/tcp  open     pop3s
3306/tcp open     mysql

Nmap done: 1 IP address (1 host up) scanned in 4.67 seconds
```

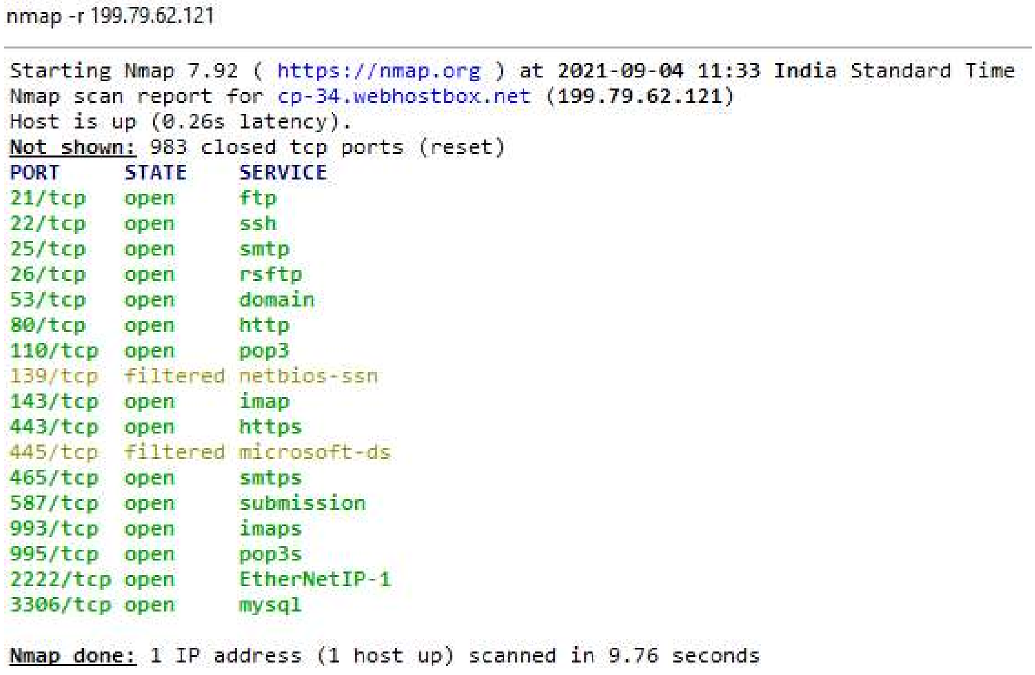
Os Detection:



```
nmap -O 199.79.62.121
```

```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-04 11:31 India Standard Time
Nmap scan report for cp-34.webhostbox.net (199.79.62.121)
Host is up (0.16s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   open     smtp
26/tcp   open     rsftp
53/tcp   open     domain
80/tcp   open     http
110/tcp  open     pop3
139/tcp  filtered netbios-ssn
143/tcp  open     imap
443/tcp  open     https
445/tcp  filtered microsoft-ds
465/tcp  open     smtps
587/tcp  open     submission
993/tcp  open     imaps
995/tcp  open     pop3s
2222/tcp open     EtherNetIP-1
3306/tcp open     mysql
Device type: general purpose|firewall
Running (JUST GUESSING): FreeBSD 6.X (90%), Linux 2.6.X (86%), OpenBSD 4.X (85%), Netasq embedded (85%)
OS CPE: cpe:/o:freebsd:freebsd:6.2 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:openbsd:openbsd:4.0 cpe:/h:netasq:u70
Aggressive OS guesses: FreeBSD 6.2-RELEASE (90%), Linux 2.6.32 (86%), Linux 2.6.18 (86%), OpenBSD 4.0 (85%), Oracle Enterprise Linux 6 (Linux 2.6.32) (85%), Linux 2.6.5 (85%), Linux 2.6.9 - 2.6.18 (85%), Netasq U70 firewall (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 17.59 seconds
```

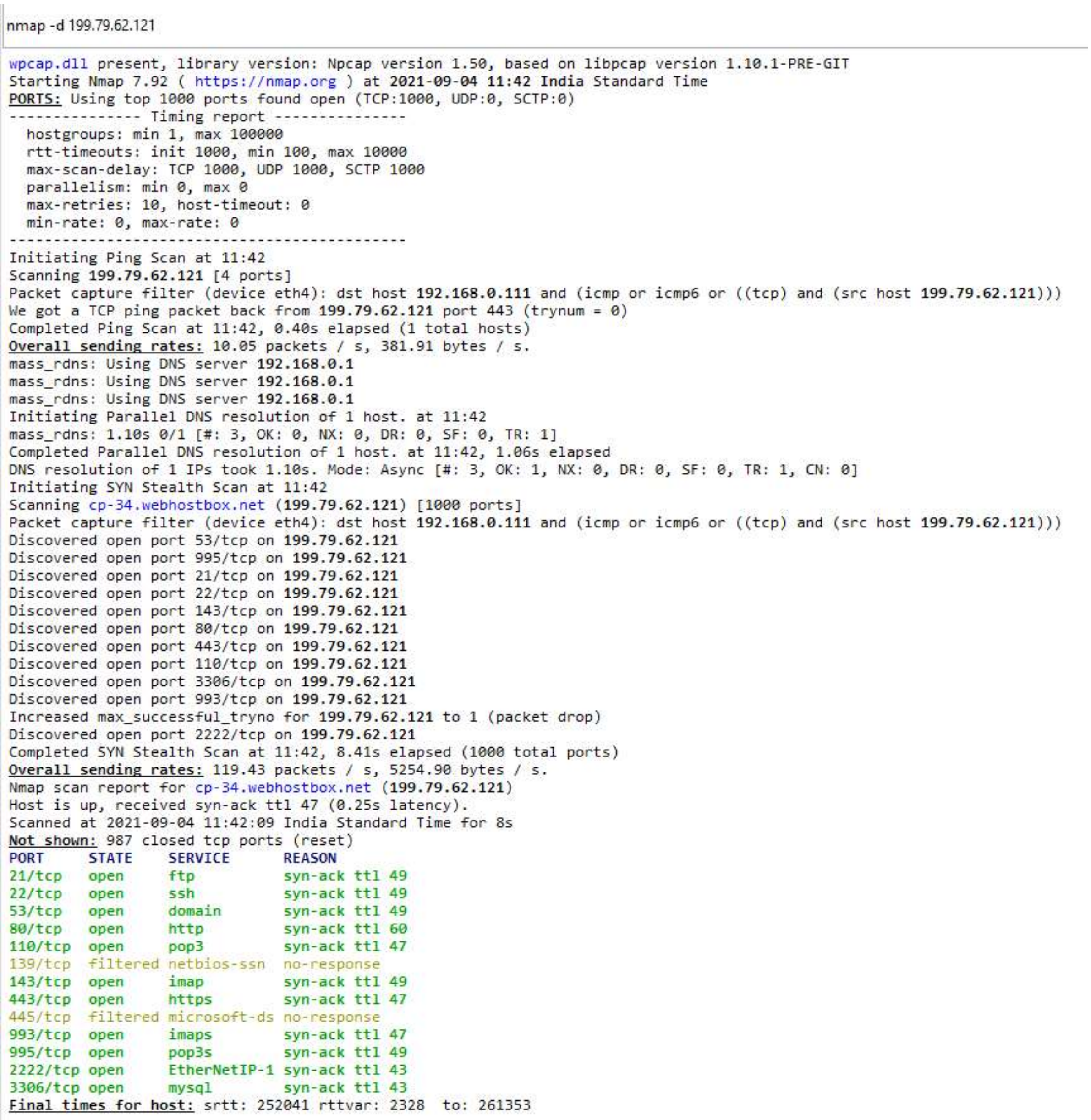
sequential port scan:



```
nmap -r 199.79.62.121
```

```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-04 11:33 India Standard Time
Nmap scan report for cp-34.webhostbox.net (199.79.62.121)
Host is up (0.26s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   open     smtp
26/tcp   open     rsftp
53/tcp   open     domain
80/tcp   open     http
110/tcp  open     pop3
139/tcp  filtered netbios-ssn
143/tcp  open     imap
443/tcp  open     https
445/tcp  filtered microsoft-ds
465/tcp  open     smtps
587/tcp  open     submission
993/tcp  open     imaps
995/tcp  open     pop3s
2222/tcp open     EtherNetIP-1
3306/tcp open     mysql

Nmap done: 1 IP address (1 host up) scanned in 9.76 seconds
```

debug:



```
nmap -d 199.79.62.121
```

```
wpcap.dll present, library version: Npcap version 1.50, based on libpcap version 1.10.1-PRE-GIT
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-04 11:42 India Standard Time
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
--------------- Timing report ---------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
---------------------------------------------
Initiating Ping Scan at 11:42
Scanning 199.79.62.121 [4 ports]
Packet capture filter (device eth4): dst host 192.168.0.111 and (icmp or icmp6 or ((tcp) and (src host 199.79.62.121)))
We got a TCP ping packet back from 199.79.62.121 port 443 (trynum = 0)
Completed Ping Scan at 11:42, 0.40s elapsed (1 total hosts)
Overall sending rates: 10.05 packets / s, 381.91 bytes / s.
mass_rdns: Using DNS server 192.168.0.1
mass_rdns: Using DNS server 192.168.0.1
mass_rdns: Using DNS server 192.168.0.1
Initiating Parallel DNS resolution of 1 host. at 11:42
mass_rdns: 1.10s 0/1 [#: 3, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 11:42, 1.06s elapsed
DNS resolution of 1 IPs took 1.10s. Mode: Async [#: 3, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 11:42
Scanning cp-34.webhostbox.net (199.79.62.121) [1000 ports]
Packet capture filter (device eth4): dst host 192.168.0.111 and (icmp or icmp6 or ((tcp) and (src host 199.79.62.121)))
Discovered open port 53/tcp on 199.79.62.121
Discovered open port 995/tcp on 199.79.62.121
Discovered open port 21/tcp on 199.79.62.121
Discovered open port 22/tcp on 199.79.62.121
Discovered open port 143/tcp on 199.79.62.121
Discovered open port 80/tcp on 199.79.62.121
Discovered open port 443/tcp on 199.79.62.121
Discovered open port 110/tcp on 199.79.62.121
Discovered open port 3306/tcp on 199.79.62.121
Discovered open port 993/tcp on 199.79.62.121
Increased max_successful_tryno for 199.79.62.121 to 1 (packet drop)
Discovered open port 2222/tcp on 199.79.62.121
Completed SYN Stealth Scan at 11:42, 8.41s elapsed (1000 total ports)
Overall sending rates: 119.43 packets / s, 5254.90 bytes / s.
Nmap scan report for cp-34.webhostbox.net (199.79.62.121)
Host is up, received syn-ack ttl 47 (0.25s latency).
Scanned at 2021-09-04 11:42:09 India Standard Time for 8s
Not shown: 987 closed tcp ports (reset)
PORT     STATE    SERVICE      REASON
21/tcp   open     ftp          syn-ack ttl 49
22/tcp   open     ssh          syn-ack ttl 49
53/tcp   open     domain       syn-ack ttl 49
80/tcp   open     http         syn-ack ttl 60
110/tcp  open     pop3         syn-ack ttl 47
139/tcp  filtered netbios-ssn  no-response
143/tcp  open     imap         syn-ack ttl 49
443/tcp  open     https        syn-ack ttl 47
445/tcp  filtered microsoft-ds no-response
993/tcp  open     imaps        syn-ack ttl 47
995/tcp  open     pop3s        syn-ack ttl 49
2222/tcp open     EtherNetIP-1 syn-ack ttl 43
3306/tcp open     mysql        syn-ack ttl 43
Final times for host: srtt: 252041 rttvar: 2328  to: 261353
```

CONCLUSION: Thus, we have studied different options to scan ports in Nmap