Nmap Scanning - Getting Started

By Anmol K Sachan

Nmap is the most popular scanning tool used on the Internet, created by Gordon Lyon(Fyodar) (http://www.insecure.org) , it was featured in the Matrix Reloaded movie.

Nmap Free Security Scanner, Port Scanner, & Network Exploration Tool is an open source software for Linux, Windows, UNIX, FreeBSD, etc.

Zenmap is GUI version for nmap.

Written in: C, C++, Python, Lua

Refer to help or manual in unix/linux for reading more.
man nmap

Standard **TCP communications** are controlled by flags in the TCP packet header.

The flags are as follows:

Synchronize - also called "SYN”
Used to initiate a connection between hosts.

Acknowledgement - also called "ACK”
Used in establishing a connection between hosts

Push - "PSH”
Instructs receiving system to send all buffered data immediately

Urgent - "URG”
States that the data contained in the packet should be processed immediately

Finish - also called "FIN"
Tells remote system that there will be no more transmissions

Reset - also called "RST”
Also used to reset a connection.

SYN Scanning:
Syn scanning, a technique that is widely across the Internet today.
The syn scan, also called the "half open" scan, is the ability to determine a ports state without making a full connection to the host.

Many systems do not log the attempt, and discard it as a communications error.
You must first learn 3-way handshake to understand the Syn scan.

How **3-way handshake** works?

192.168.1.2:2342 ----------syn----------> 192.168.1.3:80

192.168.1.2:2342 <---------syn/ack---------- 192.168.1.3:80

192.168.1.2:2342 ----------ack----------> 192.168.1.3:80

Connection Established

Stealth Scan

Computer A Computer B

192.168.1.2:2342 ----------syn----------> 192.168.1.3:80

192.168.1.2:2342 <---------syn/ack---------- 192.168.1.3:80

192.168.1.2:2342 ----------RST----------> 192.168.1.3:80

Xmas Scan

Xmas scan directed at open port:

Computer A Computer B

192.5.5.92:4031 ----------FIN/URG/PSH----------->192.5.5.110:23

192.5.5.92:4031 <----------NO RESPONSE----------192.5.5.110:23

Xmas scan directed at closed port:

192.5.5.92:4031 ----------FIN/URG/PSH----------->192.5.5.110:23

192.5.5.92:4031<----------RST/ACK----------192.5.5.110:23

XMAS scan only works OS system's TCP/IP implementation is developed according to **RFC 793**.

FIN Scan

Computer A Computer B

FIN scan directed at open port:

192.5.5.92:4031 ----------FIN---------->192.5.5.110:23

192.5.5.92:4031 <----------NO RESPONSE----------192.5.5.110:23

FIN scan directed at closed port:

192.5.5.92:4031 ----------FIN----------192.5.5.110:23

192.5.5.92:4031<----------RST/ACK----------192.5.5.110:23

FIN scan only works OS system's TCP/IP implementation is developed according to RFC 793.

NULL Scan

Computer A Computer B

NULL scan directed at open port:

192.5.5.92:4031 ----------NO FLAGS SET---------->192.5.5.110:23

192.5.5.92:4031 <----------NO RESPONSE----------192.5.5.110:23

NULL scan directed at closed port:

192.5.5.92:4031 ----------NO FLAGS SET---------192.5.5.110:23

192.5.5.92:4031<----------RST/ACK----------192.5.5.110:23

NULL scan only works OS system's TCP/IP implementation is developed according to RFC 793.

ICMP echo scanning

This isn't really port scanning, since ICMP doesn't have a port abstraction.

But it is sometimes useful to determine what hosts in a network are up by pinging them all.

nmap -P cert.org/24 152.148.0.0/16

Scan Options

-sT (TcpConnect)

-sS (SYN scan)

-sF (Fin Scan)

-sX (Xmas Scan)

-sN (Null Scan)

-sP (Ping Scan)

-sU (UDP scans)

-sO (Protocol Scan)

-sI (Idle Scan)

-sA (Ack Scan)

-sW (Window Scan)

-sR (RPC scan)

-sL (List/Dns Scan)

Nmap Port Scan types

Scan using TCP connect
nmap -sT 192.168.1.1

```
Nmap done: 1 IP address (1 host up) scanned in 17.88 seconds

C:\Program Files (x86)\Nmap>nmap.exe -sT 192.168.43.50
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-07 00:07 India Standard Time
Nmap scan report for 192.168.43.50
Host is up (0.00075s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
5357/tcp  open  wsdapi
49160/tcp open  unknown
```

Scan using TCP SYN scan (default)
nmap -sS 192.168.1.1

```
Nmap done: 1 IP address (1 host up) scanned in 47.43 seconds

C:\Program Files (x86)\Nmap>nmap.exe -sS 192.168.43.50
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-07 00:08 India Standard Time
Nmap scan report for 192.168.43.50
Host is up (0.0015s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
5357/tcp  open  wsdapi
49160/tcp open  unknown
```

Scan UDP ports
nmap -sU -p 123,161,162 192.168.1.1

```
C:\Program Files (x86)\Nmap>nmap.exe -sU -p 123,161,162 192.168.43.50
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-07 00:09 India Standard Time
Nmap scan report for 192.168.43.50
Host is up (0.0050s latency).

PORT    STATE  SERVICE
123/udp closed ntp
161/udp closed snmp
162/udp closed snmptrap

Nmap done: 1 IP address (1 host up) scanned in 5.51 seconds
```

Scan selected ports - ignore discovery
nmap -Pn -F 192.168.1.1

```
C:\Program Files (x86)\Nmap>nmap.exe -Pn -F 192.168.43.50
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-07 00:09 India Standard Time
Nmap scan report for 192.168.43.50
Host is up (0.00067s latency).
Not shown: 95 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 5.74 seconds
```

Ping Detection

-P0 (don’t ping)

-PT (TCP ping)

-PS (SYN ping)

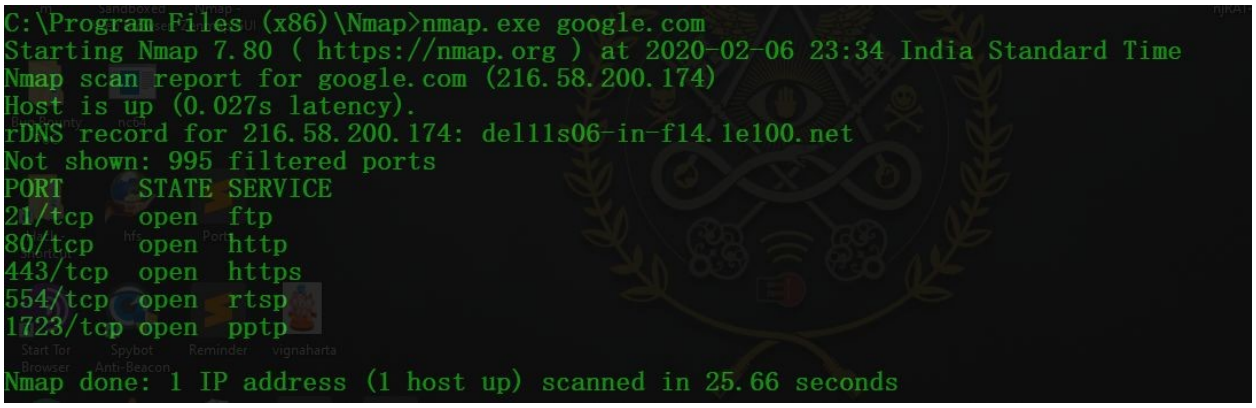
-PI (ICMP ping)

-PB (= PT + PI)

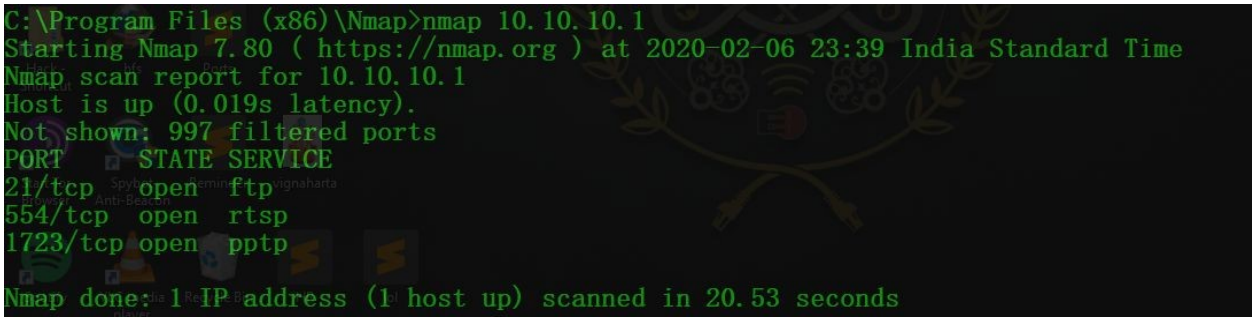
-PP (ICMP timestamp)

-PM (ICMP netmask)

A quick simple scan on google.com reveals a little about our target:
Scan a host
nmap www.testhostname.com



Scan a single IP
nmap 192.168.1.1



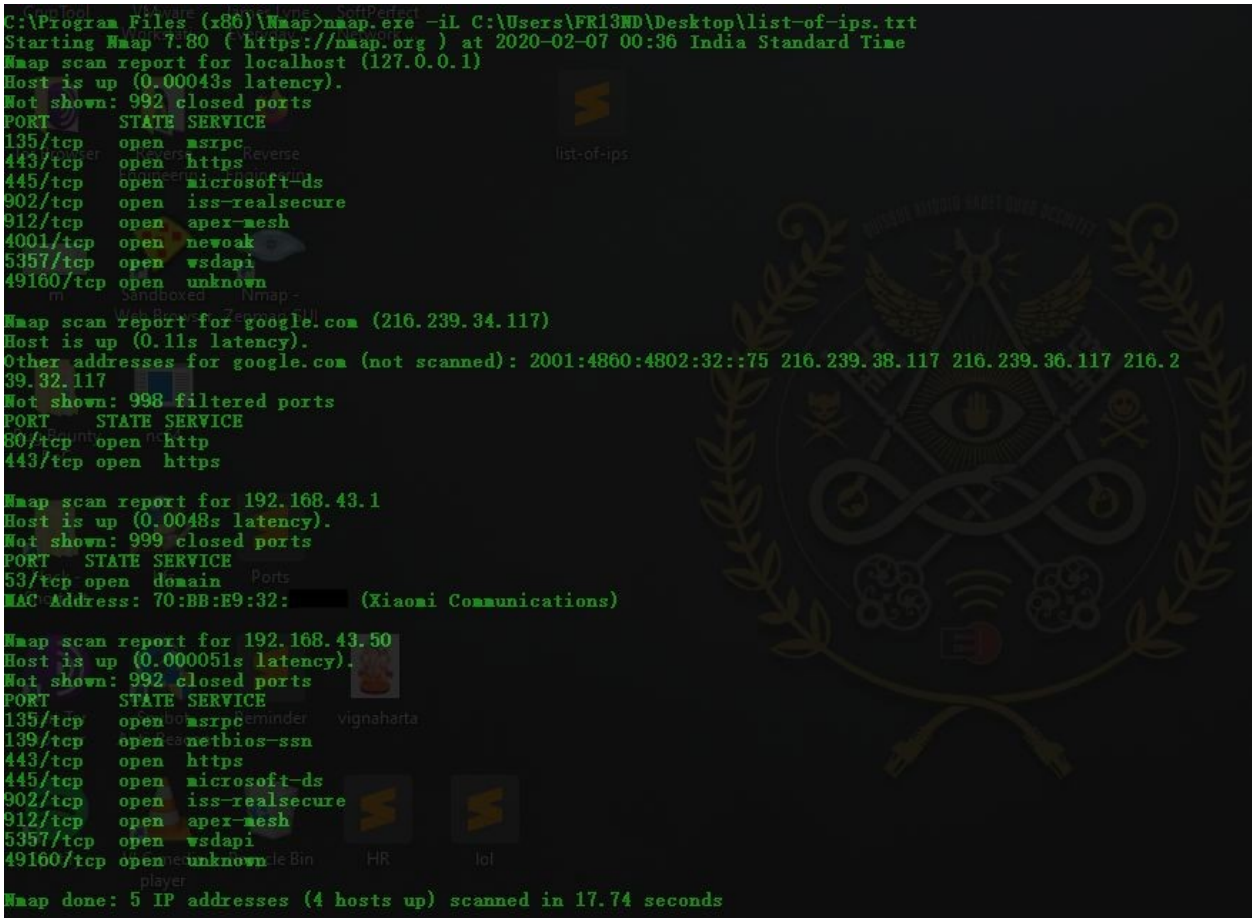
Scan a range of IPs
nmap 192.168.1.100-120
It scans the whole range of given 20 hosts on the network.

```
Nmap scan report for 100.115.23.119
Host is up (0.035s latency).
All 1000 scanned ports on 100.115.23.119 are filtered
MAC Address: FE:FF:0A:46:96:60 (Unknown)

Nmap scan report for 100.115.23.120
Host is up (0.035s latency).
All 1000 scanned ports on 100.115.23.120 are filtered
MAC Address: FE:FF:0A:46:96:60 (Unknown)

Nmap scan report for 100.115.23.103
Host is up (0.00013s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
5357/tcp  open  wsdapi
49160/tcp open  unknown

Nmap done: 21 IP addresses (21 hosts up) scanned in 647.66 seconds
```

Scan a subnet
nmap 192.168.1.0/24

```
C:\Program Files (x86)\Nmap>nmap.exe 192.168.43.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-07 00:31 India Standard Time
Nmap scan report for 192.168.43.1
Host is up (0.0051s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 70:BB:E9:32:[redacted] (Xiaomi Communications)

Nmap scan report for 192.168.43.221
Host is up (0.012s latency).
All 1000 scanned ports on 192.168.43.221 are closed
MAC Address: F0:18:98:9B:[redacted] (Apple)

Nmap scan report for 192.168.43.50
Host is up (0.000070s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
5357/tcp  open  wsdapi
49160/tcp open  unknown
```

Scan targets from a text file
nmap -iL list-of-ips.txt



Nmap Port Selection

Scan a single Port
nmap -p 22 192.168.1.1

Scan a range of ports

nmap -p 1-100 192.168.1.1

```
C:\Program Files (x86)\Nmap>nmap.exe -p 1-1000 192.168.43.50
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-07 00:04 India Standard Time
Nmap scan report for 192.168.43.50
Host is up (0.0011s latency).
Not shown: 993 closed ports
PORT    STATE    SERVICE
135/tcp open     msrpc
137/tcp filtered netbios-ns
139/tcp open     netbios-ssn
443/tcp open     https
445/tcp open     microsoft-ds
902/tcp open     iss-realsecure
912/tcp open     apex-mesh

Nmap done: 1 IP address (1 host up) scanned in 6.61 seconds
```

Scan 100 most common ports (Fast)
nmap -F 192.168.1.1

```
C:\Program Files (x86)\Nmap>nmap.exe -F 192.168.43.50
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-07 00:05 India Standard Time
Nmap scan report for 192.168.43.50
Host is up (0.0011s latency).
Not shown: 95 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
```

Scan all 65535 ports
nmap -p- 192.168.1.1

```
C:\Program Files (x86)\Nmap>nmap.exe -p- 192.168.43.50
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-07 00:06 India Standard Time
Nmap scan report for 192.168.43.50
Host is up (0.000077s latency).
Not shown: 65518 closed ports
PORT      STATE    SERVICE
135/tcp   open     msrpc
137/tcp   filtered netbios-ns
139/tcp   open     netbios-ssn
443/tcp   open     https
445/tcp   open     microsoft-ds
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
5040/tcp  open     unknown
5357/tcp  open     wsdapi
7680/tcp  open     pando-pub
49160/tcp open     unknown
49664/tcp open     unknown
49665/tcp open     unknown
49666/tcp open     unknown
49667/tcp open     unknown
49668/tcp open     unknown
49669/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 17.88 seconds
```

Service and OS Detection

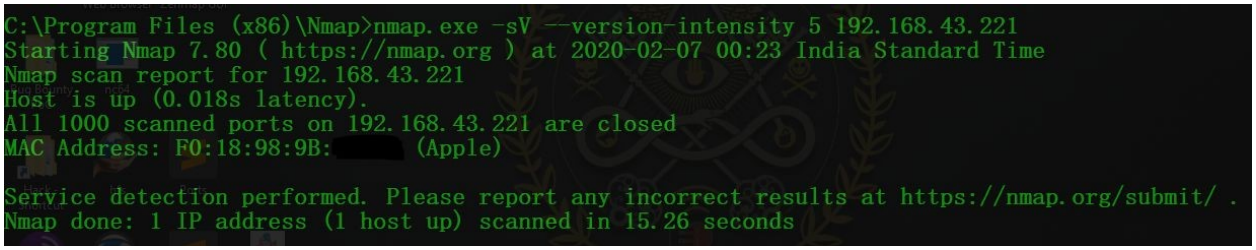
Detect OS and Services
nmap -A 192.168.1.1

```
C:\Program Files (x86)\Nmap>nmap.exe -A 192.168.43.221
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-07 00:22 India Standard Time
Nmap scan report for 192.168.43.221
Host is up (0.039s latency).
All 1000 scanned ports on 192.168.43.221 are closed
MAC Address: F0:18:98:9B:[redacted] (Apple)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   39.42 ms 192.168.43.221

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 25.10 seconds
```

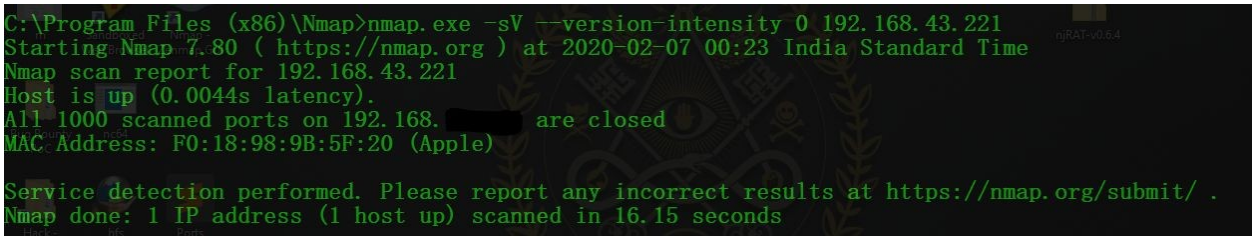
Standard service detection
nmap -sV 192.168.1.1

```
C:\Program Files (x86)\Nmap>nmap.exe -sV 192.168.43.221
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-07 00:22 India Standard Time
Nmap scan report for 192.168.43.221
Host is up (0.0072s latency).
All 1000 scanned ports on 192.168.43.221 are closed
MAC Address: F0:18:98:9B:[redacted] (Apple)
```

More aggressive Service Detection
nmap -sV --version-intensity 5 192.168.1.1

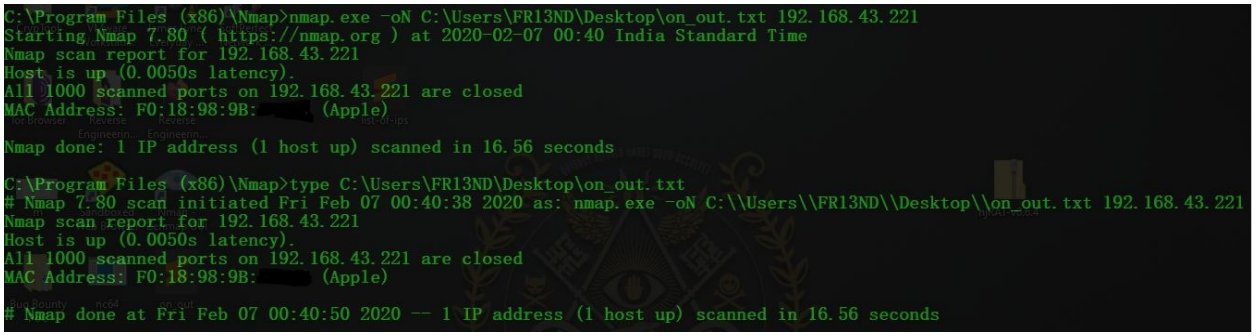


Lighter banner grabbing detection
nmap -sV --version-intensity 0 192.168.1.1



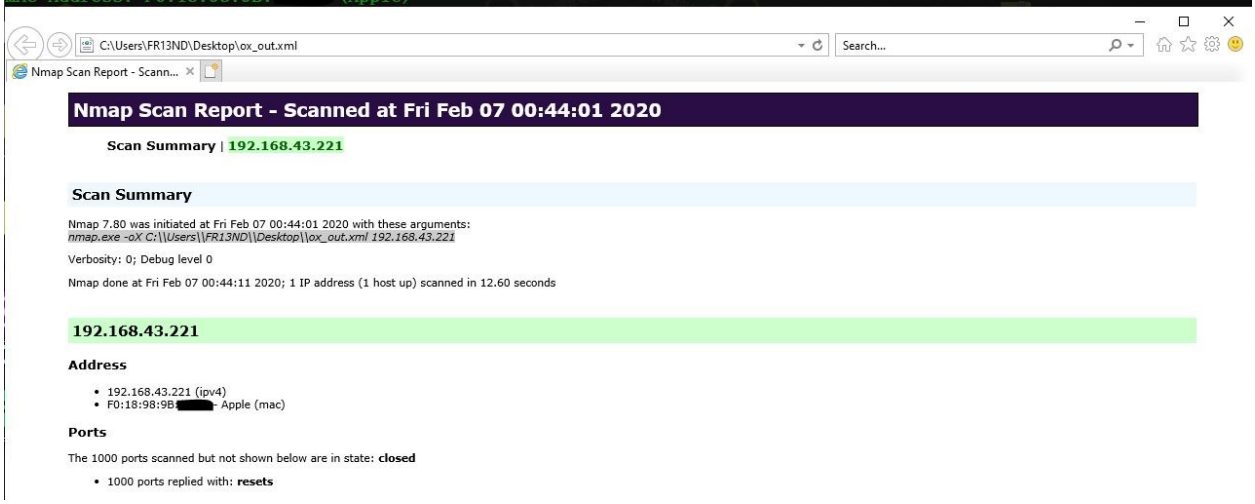
Nmap Output Formats

Save default output to file
nmap -oN outputfile.txt 192.168.1.1



Save results as XML
nmap -oX outputfile.xml 192.168.1.1

```
C:\Program Files (x86)\Nmap>nmap.exe -oX C:\Users\FR13ND\Desktop\ox_out.xml 192.168.43.221
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-07 00:43 India Standard Time
Nmap scan report for 192.168.43.221
Host is up (0.0057s latency).
All 1000 scanned ports on 192.168.43.221 are closed
MAC Address: F0:18:98:9B:[redacted] (Apple)
```



Save results in a format for grep
nmap -oG outputfile.txt 192.168.1.1

```
C:\Program Files (x86)\Nmap>nmap.exe -oG C:\Users\FR13ND\Desktop\og_out.txt 192.168.43.221
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-07 00:48 India Standard Time
Nmap scan report for 192.168.43.221
Host is up (0.0047s latency).
All 1000 scanned ports on 192.168.43.221 are closed
MAC Address: F0:18:98:9B:[redacted] (Apple)

Nmap done: 1 IP address (1 host up) scanned in 12.90 seconds

C:\Program Files (x86)\Nmap>type C:\Users\FR13ND\Desktop\og_out.txt
# Nmap 7.80 scan initiated Fri Feb 07 00:48:27 2020 as: nmap.exe -oG C:\\Users\\FR13ND\\Desktop\\og_out.txt 192.168.43.221

Host: 192.168.43.221 () Status: Up
Host: 192.168.43.221 () Status: Up
# Nmap done at Fri Feb 07 00:48:38 2020 -- 1 IP address (1 host up) scanned in 12.90 seconds
```

Save in all formats
nmap -oA outputfile 192.168.1.1

```
C:\Program Files (x86)\Nmap>nmap.exe -oA C:\Users\FR13ND\Desktop\oa_out 192.168.43.221
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-07 00:49 India Standard Time
Nmap scan report for 192.168.43.221
Host is up (0.0057s latency).
All 1000 scanned ports on 192.168.43.221 are closed
MAC Address: F0:18:98:9B[redacted] (Apple)

Nmap done: 1 IP address (1 host up) scanned in 14.19 seconds
```

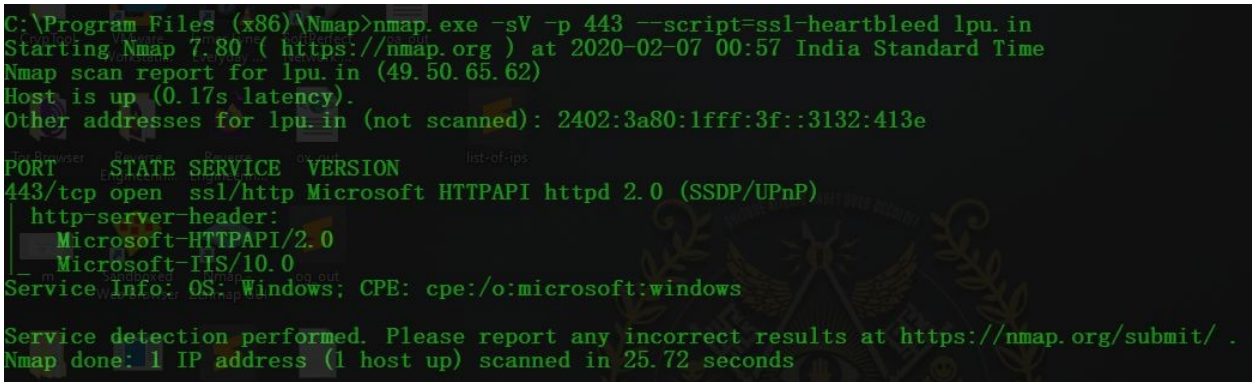
IP Address information

Find Information about IP address
nmap --script=asn-query,whois,ip-geolocation-maxmind 192.168.1.0/24

Detect Heartbleed SSL Vulnerability (CVE-2014-0160)

Heartbleed is a security bug in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security protocol. It was introduced into the software in 2012 and publicly disclosed in April 2014. Heartbleed may be exploited regardless of whether the vulnerable OpenSSL instance is running as a TLS server or client.
Reference: heartbleed.com

nmap.exe -sV -p 443 --script=ssl-heartbleed lpu.in



Zenmap is the official Nmap Security Scanner GUI.
It is a multi-platform (Linux, Windows, Mac OS X, BSD, etc.) free and open source application which aims to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users.

Source: nmap.org/zenmap/