Nmap Scanning - Getting Started
By Anmol K Sachan
Nmap is the most popular scanning tool used on the Internet, created by Gordon Lyon (Fyodor) (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.

```plaintext
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)
- `sl` (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

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

Scan UDP ports
nmap -sU -p 123,161,162 192.168.1.1
Scan selected ports - ignore discovery
nmap -Pn -F 192.168.1.1

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

```plaintext
C:\Program Files (x86)\Nmap\nmap.exe google.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-06 23:34 India Standard Time
Nmap scan report for google.com (216.58.200.174)
Host is up (0.027s latency).
rDNS record for 216.58.200.174: del11s06-in-f14.1e100.net
Not shown: 995 filtered ports
PORT  STATE  SERVICE
21/tcp  open  ftp
80/tcp  open  http
443/tcp  open  https
554/tcp  open  rtsp
1723/tcp  open  pptp
Nmap done: 1 IP address (1 host up) scanned in 25.66 seconds
```

Scan a single IP
nmap 192.168.1.1

```plaintext
C:\Program Files (x86)\Nmap\nmap 10.10.10.1
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-06 23:39 India Standard Time
Nmap scan report for 10.10.10.1
Host is up (0.019s latency).
Not shown: 997 filtered ports
PORT  STATE  SERVICE
21/tcp  open  ftp
554/tcp  open  rtsp
1723/tcp  open  pptp
Nmap done: 1 IP address (1 host up) scanned in 20.53 seconds
```

Scan a range of IPs
nmap 192.168.1.100-120

It scans the whole range of given 20 hosts on the network.
Scan a subnet
nmap 192.168.1.0/24
Scan targets from a text file
nmap -iL list-of-ips.txt

C:\Program Files (x86)\Nmap>nmap.exe -p 445 192.168.1.1
Starting Nmap 7.80 (https://nmap.org) at 2020-02-07 00:00 India Standard Time
Nmap scan report for 192.168.1.1
Host is up (0.0005s latency).
PORT STATE SERVICE
445/tcp open microsoft-ds

Nmap Port Selection

Scan a single Port
nmap -p 22 192.168.1.1

C:\Program Files (x86)\Nmap>nmap.exe -p 22 192.168.1.1
Starting Nmap 7.80 (https://nmap.org) at 2020-02-07 00:00 India Standard Time
Nmap scan report for 192.168.43.1
Host is up (0.0005s latency).
PORT STATE SERVICE
22/tcp open ssh

Scan a range of ports
nmap -p 1-100 192.168.1.1
nmap -F 192.168.1.1
nmap -p- 192.168.1.1
Service and OS Detection

Detect OS and Services
nmap -A 192.168.1.1

Standard service detection
nmap -sV 192.168.1.1
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
Save results in a format for grep
nmap -G outputfile.txt 192.168.1.1

Save in all formats
nmap -oA outputfile 192.168.1.1

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

```bash
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/