NMAP

Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications.

Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.

Gordon Lyon (pseudonym Fyodor) wrote Nmap as a tool to help map an entire network easily and to find its open ports and services.

Nmap helps you to quickly map out a network without sophisticated commands or configurations. It also supports simple commands (for example, to check if a host is up) and complex scripting through the Nmap scripting engine.

Features of Nmap,

- **Flexible Functionality:**
    - Supports advanced techniques for mapping networks with IP filters, firewalls, routers, etc.
    - Includes TCP & UDP port scanning, OS detection, version detection, ping sweeps, and more.
- **Powerful Scanning Capability:**
    - Successfully scans extensive networks with hundreds of thousands of machines.
- **Portability Across Operating Systems:**
    - Compatible with various operating systems, including Linux, Windows, FreeBSD, OpenBSD, and more.
- **Ease of Use:**
    - Both command line and graphical versions available.
    - User-friendly initiation with commands like "nmap -v -A targethost."
- **Free and Open-Source:**
    - Aligned with the goal of making the internet more secure.
    - Available for free download with full source code for modification and redistribution.
- **Comprehensive Documentation:**
    - Rich set of up-to-date man pages, whitepapers, tutorials, and a dedicated book.
- **Popularity and Inclusion:**
    - Thousands of daily downloads.
    - Included in various operating systems and ranked among the top ten programs on Freshmeat.Net.
- **Community Support:**

- Vibrant community of developers and users.
- Support through Nmap mailing lists.

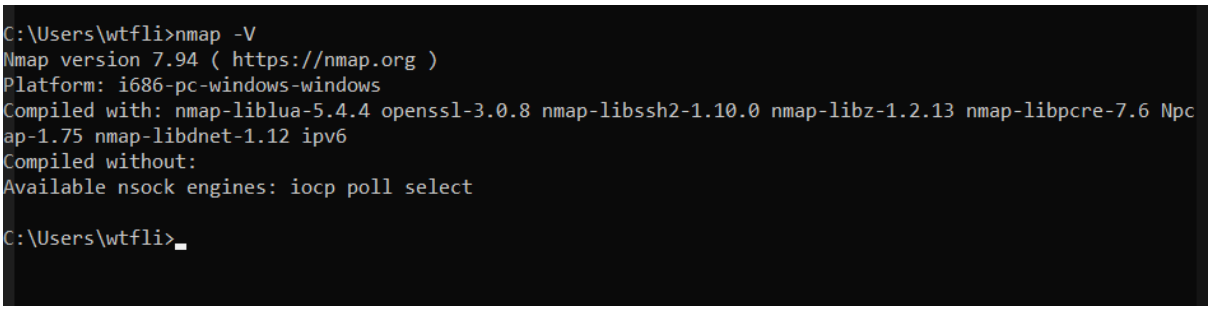
Other features of Nmap include:

- Ability to quickly recognize all the devices including servers, routers, switches, mobile devices, etc on single or multiple networks.
- Helps identify services running on a system including web servers, DNS servers, and other common applications. Nmap can also detect application versions with reasonable accuracy to help detect existing vulnerabilities.
- Nmap can find information about the operating system running on devices. It can provide detailed information like OS versions, making it easier to plan additional approaches during penetration testing.
- During security auditing and vulnerability scanning, you can use Nmap to attack systems using existing scripts from the Nmap Scripting Engine.
- Nmap has a graphical user interface called Zenmap. It helps you develop visual mappings of a network for better usability and reporting.

NMAP SCANNING

1. Find the version of nmap.

nmap –V



2. Single system scan using nmap. Scan 1000 common ports.

a) scan single IP address:

nmap 192.168.0.160

```
C:\Users\wtfli>nmap 192.168.201.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 08:21 India Standard Time
Nmap scan report for 192.168.201.1
Host is up (0.00020s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
5357/tcp  open  wsdapi
7070/tcp  open  realserver
10243/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
```

2b. scan single hostname:

nmap abc.com

```
C:\Users\wtfli>nmap paruluniversity.ac.in
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 07:53 India Standard Time
Nmap scan report for paruluniversity.ac.in (3.111.231.105)
Host is up (0.011s latency).
rDNS record for 3.111.231.105: ec2-3-111-231-105.ap-south-1.compute.amazonaws.com
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 57.95 seconds
```

3. Scan the ip address with Verbose information.

nmap -v 192.168.0.160

```
C:\Users\wtfli>nmap -v 192.168.201.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 07:54 India Standard Time
Initiating Parallel DNS resolution of 1 host. at 07:54
Completed Parallel DNS resolution of 1 host. at 07:54, 0.01s elapsed
Initiating SYN Stealth Scan at 07:54
Scanning 192.168.201.1 [1000 ports]
Discovered open port 135/tcp on 192.168.201.1
Discovered open port 445/tcp on 192.168.201.1
Discovered open port 139/tcp on 192.168.201.1
Discovered open port 554/tcp on 192.168.201.1
Discovered open port 10243/tcp on 192.168.201.1
Discovered open port 912/tcp on 192.168.201.1
Discovered open port 5357/tcp on 192.168.201.1
Discovered open port 2869/tcp on 192.168.201.1
Discovered open port 7070/tcp on 192.168.201.1
Discovered open port 902/tcp on 192.168.201.1
Completed SYN Stealth Scan at 07:54, 0.17s elapsed (1000 total ports)
Nmap scan report for 192.168.201.1
Host is up (0.00056s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
5357/tcp  open  wsdapi
7070/tcp  open  realserver
10243/tcp open  unknown

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 0.92 seconds
           Raw packets sent: 1000 (44.000KB) | Rcvd: 2010 (84.440KB)
```

4. Scan multiple IP addresses.

a. Scan IP addresses from different subnet:

#nmap 192.168.0.160 10.0.2.15

```
C:\Users\wtfli>nmap 192.168.201.1 10.0.2.15
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 07:55 India Standard Time
Nmap scan report for 192.168.201.1
Host is up (0.00035s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
5357/tcp  open  wsdapi
7070/tcp  open  realserver
10243/tcp open  unknown

Nmap done: 2 IP addresses (1 host up) scanned in 3.91 seconds
```

4b. Scan IP addresses from same subnet:

#nmap 192.168.0.1,160

```
C:\Users\wtfli>nmap 192.168.201.1,160
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 07:56 India Standard Time
Nmap scan report for 192.168.201.1
Host is up (0.00035s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
5357/tcp  open  wsdapi
7070/tcp  open  realserver
10243/tcp open  unknown

Nmap done: 2 IP addresses (1 host up) scanned in 2.23 seconds
```

4c. c) Scan IP addresses by range

#nmap 192.168.0.1-170

```
C:\Users\wtfli>nmap 192.168.201.1-170
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 07:56 India Standard Time
Nmap scan report for 192.168.201.1
Host is up (0.00057s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
5357/tcp  open  wsdapi
7070/tcp  open  realserver
10243/tcp open  unknown

Nmap scan report for 192.168.201.132
Host is up (0.0025s latency).
All 1000 scanned ports on 192.168.201.132 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:11:69:58 (VMware)

Nmap done: 170 IP addresses (2 hosts up) scanned in 8.89 seconds
```

5. Scan whole subnet.

nmap 192.168.0.*

```
C:\Users\wtfli>nmap 192.168.201.*
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 07:58 India Standard Time
Nmap scan report for 192.168.201.254
Host is up (0.00s latency).
All 1000 scanned ports on 192.168.201.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E3:B2:C4 (VMware)

Nmap scan report for 192.168.201.1
Host is up (0.00084s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
5357/tcp  open  wsdapi
7070/tcp  open  realserver
10243/tcp open  unknown

Nmap done: 256 IP addresses (2 hosts up) scanned in 33.18 seconds
```

6. Scan a network excluding hosts.

nmap 192.168.0.* --exclude 192.168.0.160

```
C:\Users\wtfli>nmap 192.168.201.* --exclude 192.168.201.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 08:24 India Standard Time
Nmap scan report for 192.168.201.254
Host is up (0.00067s latency).
All 1000 scanned ports on 192.168.201.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E3:B2:C4 (VMware)

Nmap done: 255 IP addresses (1 host up) scanned in 33.23 seconds
```

7. Scan a list of IP addresses from a file.

l.txt file have following id addresses:

192.168.0.160

10.0.2.15

nmap -iL 1.txt

```
C:\Users\wtfli>nmap -iL l.txt
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 08:01 India Standard Time
Nmap done: 2 IP addresses (0 hosts up) scanned in 5.24 seconds

C:\Users\wtfli>
```

8. Find Host ServiceVersion.

nmap -sV 192.168.0.160

```
C:\Users\wtfli>nmap -sV 192.168.201.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 08:03 India Standard Time
Nmap scan report for 192.168.201.1
Host is up (0.00081s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE         VERSION
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
554/tcp   open  rtsp?
902/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp   open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
2869/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7070/tcp  open  ssl/realserver?
10243/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 129.95 seconds
```

9. Aggressive scanning using nmap.

Or Find the details related to Operating System finger printing and

traceroute.

sudo nmap -A 192.168.0.160

```
C:\Users\wtfli>nmap -A 192.168.201.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 08:05 India Standard Time
Nmap scan report for 192.168.201.1
Host is up (0.025s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE         VERSION
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
554/tcp   open  rtsp?
902/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp   open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
2869/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
7070/tcp  open  ssl/realserver?
| ssl-cert: Subject: commonName=AnyDesk Client
| Not valid before: 2023-04-13T08:52:14
|_Not valid after:  2073-03-31T08:52:14
|_ssl-date: TLS randomness does not represent time
10243/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 2004
Network Distance: 0 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-12-26T02:37:16
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

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 191.41 seconds
```

10. Enable OS detection using nmap.

sudo nmap -O 192.168.0.160

```
C:\Users\wtfli>nmap -O 192.168.201.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 08:06 India Standard Time
Nmap scan report for 192.168.201.1
Host is up (0.00036s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
5357/tcp  open  wsdapi
7070/tcp  open  realserver
10243/tcp open  unknown
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 2004
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.97 seconds
```

11. Scan a host to detect firewall.

nmap -sA 192.168.0.160

```
C:\Users\wtfli>nmap -sA 192.168.201.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 08:25 India Standard Time
Nmap scan report for 192.168.201.1
Host is up (0.00019s latency).
All 1000 scanned ports on 192.168.201.1 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds

C:\Users\wtfli>
```

12. Perform Fast scan using nmap.

Scan 100 common ports which are listed in nmap service files.

nmap -F 192.168.0.160

```
C:\Users\wtfli>nmap -F 192.168.201.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 08:09 India Standard Time
Nmap scan report for 192.168.201.1
Host is up (0.00031s latency).
Not shown: 94 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
554/tcp  open  rtsp
5357/tcp open  wsdapi
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds
```

13. Find live hosts in network.

With -sP option, it skips port detection and other thing.

nmap -sP 192.168.0.*

```
C:\Users\wtfli>nmap -sP 192.168.201.*
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 08:10 India Standard Time
Nmap scan report for 192.168.201.254
Host is up (0.000095s latency).
MAC Address: 00:50:56:E3:B2:C4 (VMware)
Nmap scan report for 192.168.201.1
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 10.85 seconds

C:\Users\wtfli>
```

14. Perform a Stealthy scan.

This type of scan is undetected in network.

nmap -sS 192.168.0.160

```
C:\Users\wtfli>nmap -sS 192.168.201.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 08:11 India Standard Time
Nmap scan report for 192.168.201.1
Host is up (0.0010s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
5357/tcp  open  wsdapi
7070/tcp  open  realserver
10243/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds
```

15. Scan specific port using nmap.

(default nmap scans TCP ports.)

nmap -p 80 192.168.0.160

```
C:\Users\wtfli>nmap -p 80 192.168.201.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 08:12 India Standard Time
Nmap scan report for 192.168.201.1
Host is up (0.00s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
```

16. Scan multiple ports using nmap.

nmap -p 80,443 192.168.0.160

```
C:\Users\wtfli>nmap -p 80, 443 192.168.201.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 08:14 India Standard Time
Failed to resolve "443".
Nmap scan report for 192.168.201.1
Host is up (0.00s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 7.45 seconds
```

17. Scan ports by range using nmap.

nmap -p 75-80 192.168.0.160

```
C:\Users\wtfli>nmap -p 75-80 192.168.201.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 08:15 India Standard Time
Nmap scan report for 192.168.201.1
Host is up (0.00076s latency).

PORT   STATE  SERVICE
75/tcp closed priv-dial
76/tcp closed deos
77/tcp closed priv-rje
78/tcp closed vettcp
79/tcp closed finger
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
```

18. Scan all 65536 ports.

nmap -p- 192.168.0.160

```
C:\Users\wtfli>nmap -p- 192.168.201.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 08:16 India Standard Time
Nmap scan report for 192.168.201.1
Host is up (0.00078s latency).
Not shown: 65516 closed tcp ports (reset)
PORT      STATE    SERVICE
135/tcp   open     msrpc
137/tcp   filtered netbios-ns
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
554/tcp   open     rtsp
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
2869/tcp  open     icslap
5040/tcp  open     unknown
5357/tcp  open     wsdapi
7070/tcp  open     realserver
7680/tcp  open     pando-pub
10243/tcp open     unknown
49664/tcp open     unknown
49665/tcp open     unknown
49666/tcp open     unknown
49667/tcp open     unknown
49668/tcp open     unknown
49671/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 7.10 seconds
```

19. Scan open ports only.

nmap --open 192.168.0.160

```
C:\Users\wtfli>nmap --open 192.168.201.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 08:16 India Standard Time
Nmap scan report for 192.168.201.1
Host is up (0.00042s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
5357/tcp  open  wsdapi
7070/tcp  open  realserver
10243/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.85 seconds
```

20. Scan a TCP ports.

nmap -sT 192.168.0.160

```
C:\Users\wtfli>nmap -sT 192.168.201.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 08:17 India Standard Time
Nmap scan report for 192.168.201.1
Host is up (0.0029s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
5357/tcp  open  wsdapi
7070/tcp  open  realserver
10243/tcp open  unknown

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

21. Scan a UDP ports.

sudo nmap -sU 192.168.0.160

```
C:\Users\wtfli>nmap -sU 192.168.201.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 08:18 India Standard Time
Nmap scan report for 192.168.201.1
Host is up (0.00057s latency).
Not shown: 991 closed udp ports (port-unreach)
PORT     STATE         SERVICE
123/udp  open|filtered ntp
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
1900/udp open          upnp
3702/udp open|filtered ws-discovery
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open          zeroconf
5355/udp open|filtered llmnr

Nmap done: 1 IP address (1 host up) scanned in 308.02 seconds
```