EXPERIMENT- 9

Aim:- How to run Nmap scan

Nmap (http://nmap.org)

Nmap is a free, open source and multi-platform network security scanner used for network discovery and security auditing. Amongst other things, it allows you to create a network inventory, manage service upgrade schedules, monitor host or service uptime and scan for open ports and services on a host.
This post will focus on how to use Nmap to scan for open ports. Nmap can be extremely useful for helping you get to the root of the problem you are investigating, verify firewall rules or validate if your routing tables are configured correctly.

To get started, download and install Nmap from the nmap.org website and then launch a command prompt.

1. nmap.scanme.org is a server, the NMAP team spun up to allow you to test tool functionality.

```
C:\Windows\system32\cmd.exe

C:\Users\admin>nmap scanme.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-27 13:32 India Standard Time
Nmap scan report for scanme.org (45.33.32.156)
Host is up (0.23s latency).
rDNS record for 45.33.32.156: scanme.nmap.org
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 261.92 seconds
```

When the scan is complete, you should see an Nmap scan report similar to the one shown in the image above. This confirms Nmap is installed and operating correctly.

You will notice the information returned is PORT | STATE | SERVICE. Before we take a deeper dive into the commands, it would be valuable to know what the different

‘STATES’ mean. The Nmap Reference Guide provides a pretty comprehensive explanation, but I’ll give you a brief summary here.

STATE	Description
Open	The target port actively responds to TCP/UDP/SCTP requests.
Closed	The target port is active but not listening.
Filtered	A firewall or packet filtering device is preventing the port state being returned.
Unfiltered	The target port is reachable but Nmap cannot determine if it is open or closed.
Open/Filtered	Nmap cannot determine if the target port is open or filtered.
Closed/Filtered	Nmap cannot determine if the target port is closed or filtered.

Let us now look at some commands we can use for scanning open ports.

Nmap Port Scanning Commands

2. In any of the commands below, Nmap only shows you ports with an “Open” state.

nmap [ip_address]

nmap 172.16.131.2

C:\Windows\system32\cmd.exe

```
C:\Users\admin>nmap 172.16.131.2
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-27 13:45 India Standard Time
Nmap scan report for 172.16.131.2
Host is up (0.000060s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

3. The “–open” parameter

In any of the commands below, you can specify the “–open” parameter in your Nmap command to have Nmap only show you ports with an “Open” state.

nmap –open [ip_address]

nmap open 172.16.131.2

C:\Windows\system32\cmd.exe

```
C:\Users\admin>nmap open 172.16.131.2
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-27 13:46 India Standard Time
Failed to resolve "open".
Nmap scan report for 172.16.131.2
Host is up (0.00012s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 2.45 seconds
```

4. Scanning the entire port range

nmap -p- [ip_address]

This command will initiate a scan against the target host looking for all ports (1-65535).

nmap -p- 172.16.131.2

C:\Windows\system32\cmd.exe

```
C:\Users\admin>nmap -p- 172.16.131.2
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-27 13:47 India Standard Time
Nmap scan report for 172.16.131.2
Host is up (0.00078s latency).
Not shown: 65519 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
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
3389/tcp  open     ms-wbt-server
5040/tcp  open     unknown
7680/tcp  open     pando-pub
49664/tcp open     unknown
49665/tcp open     unknown
49666/tcp open     unknown
49667/tcp open     unknown
49668/tcp open     unknown
49669/tcp open     unknown
49671/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 3.53 seconds
```

5. Scanning a single port

nmap -p 80 [ip_address]

This command will initiate a default scan against the target host and look for port 80.

nmap -p 80 172.16.131.2

C:\Windows\system32\cmd.exe

```
C:\Users\admin>nmap -p 80 172.16.131.2
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-27 13:48 India Standard Time
Nmap scan report for 172.16.131.2
Host is up (0.0010s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

6. Scanning a specific range of ports

nmap -p 1-200 [ip_address]

This command will initiate a default scan against the target host and look for ports between the range of 1-200.

nmap -p 1-200 172.16.131.2

C:\Windows\system32\cmd.exe

```
C:\Users\admin>nmap -p 1-200 172.16.131.2
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-27 13:48 India Standard Time
Nmap scan report for 172.16.131.2
Host is up (0.00050s latency).
Not shown: 197 closed tcp ports (reset)
PORT    STATE    SERVICE
135/tcp open     msrpc
137/tcp filtered netbios-ns
139/tcp open     netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds
```

7. Scanning the top 100 ports (fast scan)

nmap -F [ip_address]

This command will initiate a fast scan against the target host looking only for the top 100 common TCP ports.

nmap -F 172.16.131.2

C:\Windows\system32\cmd.exe

```
C:\Users\admin>nmap -F 172.16.131.2
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-27 13:49 India Standard Time
Nmap scan report for 172.16.131.2
Host is up (0.00038s latency).
Not shown: 96 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

8. Scanning multiple TCP/UDP ports

nmap -p U:53,67-68,T:21-25,80,135 [ip_address]

This command will initiate a scan against the target host looking only for specified UDP and TCP ports.

nmap -p U:53,67-68,T:21-25,80,135 172.16.131.2

C:\Windows\system32\cmd.exe

```
C:\Users\admin>nmap -p U:53,67-68,T:21-25,80,135 172.16.131.2
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-27 13:50 India Standard Time
WARNING: Your ports include "U:" but you haven't specified UDP scan with -sU.
Nmap scan report for 172.16.131.2
Host is up (0.0015s latency).

PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   closed ssh
23/tcp   closed telnet
24/tcp   closed priv-mail
25/tcp   closed smtp
80/tcp   closed http
135/tcp  open   msrpc

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

9. Scanning for specific service names

nmap -p http,ssh,msrpc,microsoft-ds [ip_address]

This command will initiate a scan against the target host looking for ports associated with specified service names.

nmap -p http,ssh,msrpc,microsoft-ds 172.16.131.2

C:\Windows\system32\cmd.exe

```
C:\Users\admin>nmap -p http,ssh,msrpc,microsoft-ds 172.16.131.2
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-27 14:09 India Standard Time
Nmap scan report for 172.16.131.2
Host is up (0.0010s latency).

PORT      STATE  SERVICE
22/tcp    closed ssh
80/tcp    closed http
135/tcp   open   msrpc
445/tcp   open   microsoft-ds
8008/tcp  closed http

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```