COMPUTER NETWORKS
LAB 10

NAME - KAPAROTU VENKATA SURYA THARANI
USN - 22BTRAD018
BRANCH - AIDE

Q- Explain and run an Nmap scan.

It is used by network administrators to detect the devices currently running on the system and the port number by which the devices are connected.

Nmap is a useful tool for network scanning and auditing purposes.

- It can search for hosts connected to the Network.
- It can search for free ports on the target host.
- It detects all services running on the host with the help of the operating system.
- It also detects any flaws or potential vulnerabilities in a networked system

Basic scan: The simplest scan you can run is the basic TCP SYN scan, which checks for open ports on the target. To perform this scan, enter the following command:

nmap <ip address> where is the actual IP address or hostname of your target.
This command will scan the most common 1,000 ports by default. It will display the open ports and the services running on them.

```
C:\Users\kvsth>nmap 172.20.252.93
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-19 13:39 India Standard Time
Nmap scan report for 172.20.252.93
Host is up (0.00043s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

Nmap provides numerous scan options to customize and fine-tune your scans. Here are a few commonly used options:

- **-p or --ports**: Specify the ports you want to scan. For example, to scan ports 80 and 443,

```
C:\Users\kvsth>nmap -p 80,443 172.20.252.93
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-19 14:27 India Standard Time
Nmap scan report for 172.20.252.93
Host is up (0.0010s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

-sV: Enables service/version detection. Nmap will attempt to identify the services running on open ports.

```
C:\Users\kvsth>nmap -sV 172.20.252.93
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-19 14:29 India Standard Time
Nmap scan report for 172.20.252.93
Host is up (0.00051s latency).
Not shown: 997 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?
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 6.91 seconds
```

-O: Performs operating system detection to identify the target's operating system.

```
C:\Users\kvsth>nmap -O 172.20.252.93
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-19 14:30 India Standard Time
Nmap scan report for 172.20.252.93
Host is up (0.00044s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1607
OS details: Microsoft Windows 10 1607
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 1.39 seconds
```

"--top-ports" parameter along with a specific number lets you scan the top X most common ports for that host.

Here we got the top 10 ports in the device whose ip address is specified.

```
C:\Users\kvsth>nmap --top-ports 10 172.20.252.93
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-19 16:59 India Standard Time
Nmap scan report for 172.20.252.93
Host is up (0.00076s latency).

PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   closed ssh
23/tcp   closed telnet
25/tcp   closed smtp
80/tcp   closed http
110/tcp  closed pop3
139/tcp  open   netbios-ssn
443/tcp  closed https
445/tcp  open   microsoft-ds
3389/tcp closed ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

We can **scan a particular range** of IP addresses in the given IP address of the host.
Like in this example it will scan 9 consecutive ip ranges from 172.20.252.85-93.

```
C:\Users\kvsth>nmap 172.20.252.85-93
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-19 17:11 India Standard Time
Nmap scan report for 172.20.252.89
Host is up (0.019s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
1042/tcp open  afrog
1043/tcp open  boinc
MAC Address: F4:26:79:1B:AC:BF (Intel Corporate)

Nmap scan report for 172.20.252.93
Host is up (0.00071s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 9 IP addresses (2 hosts up) scanned in 14.42 seconds
```