

CSS Experiment: 1-B

Aim: Analyse the tool nmap and use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, xmas scan etc.

Nmap

1. Nmap is a network scanner
2. Nmap is used to discover hosts and services on a computer network by sending packets and analysing the responses.
3. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.

Nmap Commands

1. Port Scanning

It automatically scans a number of the most ‘popular’ ports for a host. To run the command:

- `nmap -top-ports <ip>`
- `nmap --top-ports 20 <ip>`

Replace the “20” with the number of ports to scan, and Nmap quickly scans that many ports. It returns a concise output that details the status of the most common ports, and this lets you quickly see whether you have any unnecessarily open ports.

```
root@kali:~# nmap --top-ports 20 10.0.2.15
Starting Nmap 7.70 ( https://nmap.org ) at 2022-02-16 00:17 EST
Nmap scan report for 10.0.2.15
Host is up (0.0000080s latency).

PORT      STATE SERVICE
21/tcp    closed ftp
22/tcp    closed ssh
23/tcp    closed telnet
25/tcp    closed smtp
53/tcp    closed domain
80/tcp    closed http
110/tcp   closed pop3
111/tcp   closed rpcbind
135/tcp   closed msrpc
139/tcp   closed netbios-ssn
143/tcp   closed imap
443/tcp   closed https
445/tcp   closed microsoft-ds
993/tcp   closed imaps
995/tcp   closed pop3s
1723/tcp  closed pptp
3306/tcp  closed mysql
3389/tcp  closed ms-wbt-server
5900/tcp  closed vnc
8080/tcp  closed http-proxy
```

2. OS Fingerprinting

OS scanning is one of the most powerful features of Nmap. When using this type of scan, Nmap sends TCP and UDP packets to a particular port, and then analyses its response. It compares this response to a database of 2600 operating systems, and returns information on the OS (and version) of a host.

To run OS scan, type the following command

- `nmap -O <target IP>`

```
root@kali:~# nmap -o 10.0.2.15
Starting Nmap 7.70 ( https://nmap.org ) at 2022-02-16 00:13 EST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.06 seconds
```

3. Ping Scan

A ping scan returns information on every active IP on your network

To run Ping scan, type the following command

- `nmap -sP <target IP>`

```
root@kali:~# nmap -sP 10.0.2.15
Starting Nmap 7.70 ( https://nmap.org ) at 2022-02-16 00:24 EST
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.00 seconds
```

4. TCP Port Scan

One of the best things is the Nmap command to check open ports, and the second-best thing about Nmap is its power to work with TCP and UDP without any hiccups. Several services are limited to just TCP, but people understand the advantage of scanning UDP-based services. Here are the examples of both these services that are allowed by Nmap.

To run TCP Port scan, type the following command

- `nmap -sT <target IP>`

```
root@kali:~# nmap -sT 10.0.2.15
Starting Nmap 7.70 ( https://nmap.org ) at 2022-02-16 00:20 EST
Nmap scan report for 10.0.2.15
Host is up (0.00013s latency).
All 1000 scanned ports on 10.0.2.15 are closed
```

5. UDP Port Scan

To run UDP Port scan, type the following command

- `nmap -sU localhost`

```

root@kali:~# nmap -sU localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2022-02-16 00:21 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000010s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed ports
PORT      STATE      SERVICE
68/udp    open|filtered dhcpc

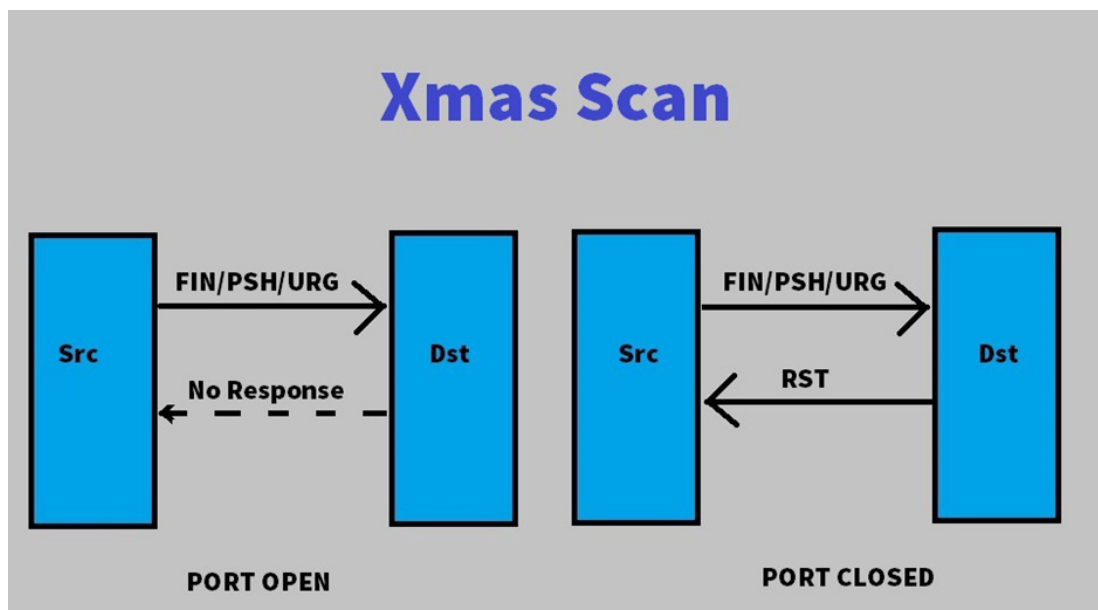
```

6. XMAS Scan

It Sets the FIN, PSF, and URG flags, lighting the packet up like a Christmas tree.

To run XMAS Scan, type the following command

- `nmap -sX <target IP>`



As we can see in the above picture when we send a packet with FIN/PSH/URG flag to set and send it to destination if we don't get any response from Destination we will know that Port is OPEN. if we get RST in return then we know that the Port is Closed.

```

root@kali:~# nmap -sX 10.0.2.15
Starting Nmap 7.70 ( https://nmap.org ) at 2022-02-16 00:50 EST
Nmap scan report for 10.0.2.15
Host is up (0.0000080s latency).
All 1000 scanned ports on 10.0.2.15 are closed

```

Conclusion: Successfully analysed the tool nmap and used it with various options to scan open ports, perform OS fingerprinting, perform a ping scan, tcp port scan, udp port scan, xmas scan, and so on.

Name: Deep Kothari

Class: TE-COMP-B

Roll No: 23