Exp 4

Aim : Perform network discovery using discovery tools such as Nmap.

Objective: To learn nmap installation and use this to scan different ports.

Theory:

How to Install NMAP in Linux

Most of the today's Linux distributions like Red Hat, CentOS, Fedoro, Debian and Ubuntu have included Nmap in their default package management repositories called Yum and APT. The both tools are used to install and manage software packages and updates. To install Nmap on distribution specific use the following command.

```
# yum install nmap [on Red Hat based systems]
```

```
$ sudo apt-get install nmap [on Debian based systems]
```

How to use NMAP in Linux

1. Scan a System with Hostname and IP Address

Scan using Hostname

```
[root@server1 ~]# nmap server2.tecmint.com
```

Scan using IP Address

```
[root@server1 ~]# nmap 192.168.0.101
```

2. Scan using "-v" option

This option gives more detailed information about the remote machine.

```
[root@server1 ~]# nmap -v server2.tecmint.com
```

3. Scan Multiple Hosts

Scan multiple hosts by simply writing their IP addresses or hostnames with Nmap.

```
[root@server1 ~]# nmap 192.168.0.101 192.168.0.102 192.168.0.103
```

4. Scan a whole Subnet

Scan a whole subnet or IP range with Nmap by providing * wildcard with it.

```
[root@server1 ~]# nmap 192.168.0.*
```

5. Scan list of Hosts from a File

If more hosts to scan and all host details are written in a file, nmap can read that file and perform scans. Create a text file called —nmaptest.txt‖ and define all the IP addresses or hostname of the server .

```
[root@server1 ~]# cat > nmaptest.txt
localhost
server2.tecmint.com
192.168.0.101
```

Next, run the following command with —iL‖ option with nmap command to scan all listed IP address in the file.

```
[root@server1 ~]# nmap -iL nmaptest.txt
```

6. Scan an IP Address Range

Specify an IP range while performing scan with Nmap.

```
[root@server1 ~]# nmap 192.168.0.101-110
```

7. Scan OS information and Traceroute

To detect which OS and version is running on the remote host. To enable OS & version detection, script scanning and traceroute, we can use —-A‖ option with NMAP.

```
[root@server1 ~]# nmap -A 192.168.0.101
```

8. Enable OS Detection with Nmap

Use the option —-O‖ and —-osscan-guess‖ also helps to discover OS information.

```
[root@server1 ~]# nmap -O server2.tecmint.com
```

9. Scan a Host to Detect Firewall

To perform a scan on a remote host to detect if any packet filters or Firewall.

```
 [root@server1 ~]# nmap -sA 192.168.0.101
```

10. Find out Live hosts in a Network

To check which hosts are live and up in Network, this option nmap skips port detection and other things.

```
[root@server1 ~]# nmap -sP 192.168.0.*
```

11. Perform a Fast Scan

To perform a fast scan with —-F‖ option to scans for the ports listed in the nmap-services files and leaves all other ports.

```
[root@server1 ~]# nmap -F 192.168.0.101
```

12. Find Nmap version

To find out Nmap version you are running on your machine with —-V‖ option.

```
[root@server1 ~]# nmap –V
```

13. Scan for specific Port

There are various options to discover ports on remote machine with Nmap. Specify the port to scan with —-p‖ option, by default nmap scans only TCP ports.

```
[root@server1 ~]# nmap -p 80 server2.tecmint.com
```

14. Check most commonly used Ports with TCP Syn

```
[root@server1 ~]# nmap -sT 192.168.0.101
```

15. Scan a UDP Port

```
[root@server1 ~]# nmap -sU 53 server2.tecmint.com
```

16. Find Host Services version Numbers

To find out service‘s versions which are running on remote hosts with ―-sVǁ option.

```
[root@server1 ~]# nmap -sV 192.168.0.101
```

CONCLUSION:

The Nmap Network Mapper is an open source and a very versatile tool for Linux system/ network administrators. Nmap is used for exploring networks, perform security scans, network audit and finding open ports on remote machine. It scans for Live hosts, Operating systems, packet filters and open ports running on remote hosts.

Questions:

1. What is Nmap used for?
2. What are feature of Nmap?
3. Why do hackers use Nmap?
4. Write a Nmap command to scan targets from a file.
5. How to write Nmap command for specific ports and services?