Don Bosco Institute of Technology, Mumbai 400070
Department of Information Technology
Experiment No. : 8

Name: Mohammad Zaid Ansari Roll No.: 03 Date: 12/10/22

Title : Nmap

Problem Definition : Download and install nmap. Use it with different options to scan active nodes, open ports, perform os finger printing, do a ping scan, tcp port scan, udp port scan.

Pre-requisite : Networking commands

Theory :
Nmap - Network Mapper
Nmap is a security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich) used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses.The software provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap is also capable of adapting to network conditions including latency and congestion during a scan. Nmap is under development and refinement by its user community.
Nmap was originally a Linux-only utility, but it was ported to Microsoft Windows, Solaris, HP-UX, BSD variants (including Mac OS X), AmigaOS, and SGI IRIX. Linux is the most popular platform, followed closely by Windows.

Nmap features include:
Host discovery – Identifying hosts on a network. For example, listing the hosts that respond to TCP and/or ICMP requests or have a particular port open.

Port scanning – Enumerating the open ports on target hosts.
Version detection – Interrogating network services on remote devices to determine application name and version number.

OS detection – Determining the operating system and hardware characteristics of network devices.

Scriptable interaction with the target – using Nmap Scripting Engine (NSE) and Lua programming language.

Nmap can provide further information on targets, including reverse DNS names, device types, and MAC addresses.

Typical uses of Nmap:
7. Auditing the security of a device or firewall by identifying the network connections which can be made to, or through it.

8. Identifying open ports on a target host in preparation for auditing
9. Network inventory, network mapping, maintenance and asset management.
10. Auditing the security of a network by identifying new servers.
11. Generating traffic to hosts on a network.
12. Find and exploit vulnerabilities in a network.

Procedure/ Algorithm & result:

Commands that run on zenmap/nmap
nmap -sn 10.0.5.*
Displays the active nodes.

```
ubuntu@Ansari:~$ nmap -sn 172.17.0.*
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-12 01:21 IST
Nmap scan report for Ansari (172.17.0.1)
Host is up (0.00057s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 3.08 seconds
```

nmap -sn 10.0.5.237
Displays the whether specific node is active.

```
ubuntu@Ansari:~$ nmap -sn 172.17.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-12 01:24 IST
Nmap scan report for Ansari (172.17.0.1)
Host is up (0.00016s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
```

nmap -T5 10.0.5.237
Displays the ports of specific node.

```
ubuntu@Ansari:~$ nmap -T5 172.17.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-12 01:25 IST
Nmap scan report for Ansari (172.17.0.1)
Host is up (0.00013s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
8080/tcp open  http-proxy

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

nmap -A 10.0.5.237

Displays the operating system of specific node(OS finger printing).

```
ubuntu@Ansari:~$ nmap -A 172.17.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-12 01:26 IST
Nmap scan report for Ansari (172.17.0.1)
Host is up (0.00014s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
139/tcp  open  netbios-ssn Samba smbd 4.6.2
445/tcp  open  netbios-ssn Samba smbd 4.6.2
8080/tcp open  http        Jetty 10.0.11
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Jetty(10.0.11)
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: ANSARI, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-10-11T19:56:38
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.85 seconds
```

Commands that run on terminal

nmap -sP 10.0.5.237

Used for ping scanning of specific node.

```
ubuntu@Ansari:~$ nmap -sP 172.17.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-12 01:30 IST
Nmap scan report for Ansari (172.17.0.1)
Host is up (0.00015s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds
```

nmap -p T:80 10.0.5.237

Used for tcp scanning of specific node.

```
ubuntu@Ansari:~$ nmap -p T:80 172.17.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-12 01:31 IST
Nmap scan report for Ansari (172.17.0.1)
Host is up (0.00013s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

nmap -p U:53 10.0.5.237(since this command is not working for me)
nmap -p -su 10.0.5.237(using this command)
Used for udp scanning of specific node.

```
ubuntu@Ansari:~$ sudo nmap -sU 172.17.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-12 01:42 IST
Nmap scan report for Ansari (172.17.0.1)
Host is up (0.000012s latency).
Not shown: 996 closed ports
PORT     STATE         SERVICE
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
631/udp  open|filtered ipp
5353/udp open|filtered zeroconf
```

References :
1. http://www.cyberciti.biz/networking/nmap-command-examples-tutorials/
2. http://en.wikipedia.org/wiki/Nmap
Lab practice (optional) :
Questions (Short, Long, MCQs) (optional) :