Mahavir Education Trust's

SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE

Chembur, Mumbai - 400 088

UG Program in Information Technology

Experiment No: 06				
Date of Performance:	07/10/2024			
Date of Submission:	14/10/2024			
Program Formation/ Execution/ Correction (06)	**Timely Submission (01)**	**Viva (03)**	**Experiment Marks (10)**	**Teacher Signature with date**

EXPERIMENT - 06

Aim :

Theory :

To install Nmap on Ubuntu, you can follow these steps:

1.Open the Terminal: You can do this by searching for "Terminal" in your applications menu or by pressing Ctrl + Alt + T.

2.Update Your Package List: It's a good idea to ensure your package list is up-to-date before installing new software. Run the following command:

sudo apt update

```
[10/07/24]seed@VM:~$ sudo apt update
Hit:1 http://ppa.launchpad.net/mozillateam/firefox-next
/ubuntu xenial InRelease
Hit:2 http://ppa.launchpad.net/webupd8team/java/ubuntu
xenial InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu xenial InRele
ase
Ign:4 https://download.sublimetext.com apt/stable/ InRe
lease
Err:5 https://download.sublimetext.com apt/stable/ Rele
ase
  server certificate verification failed. CAfile: /etc/
ssl/certs/ca-certificates.crt CRLfile: none
Reading package lists... Done
E: The repository 'https://download.sublimetext.com apt
/stable/ Release' does not have a Release file.
N: Updating from such a repository can't be done secure
ly, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation an
d user configuration details.
```

3.Install Nmap: Now, you can install Nmap by running:

sudo apt install nmap

```
[10/07/24]seed@VM:~$ sudo apt install nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libblas-common libblas3 liblinear3 lua-lpeg ndiff
Suggested packages:
  liblinear-tools liblinear-dev
The following NEW packages will be installed:
  libblas-common libblas3 liblinear3 lua-lpeg ndiff
  nmap
0 upgraded, 6 newly installed, 0 to remove and 1 not up
graded.
Need to get 4,892 kB of archives.
After this operation, 22.2 MB of additional disk space
will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu xenial/main i
386 libblas-common i386 3.6.0-2ubuntu2 [5,338 B]
Get:2 http://us.archive.ubuntu.com/ubuntu xenial/main i
```

4.Verify the Installation: Once the installation is complete, you can check that Nmap is installed correctly by running:

nmap --version

```
[10/07/24]seed@VM:~$ nmap --version

Nmap version 7.01 ( https://nmap.org )
Platform: i686-pc-linux-gnu
Compiled with: liblua-5.2.4 openssl-1.0.2g libpcre-8.38
 libpcap-1.7.4 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

This should display the installed version of Nmap.

Additional Tips

- **Run as Root**: Nmap often requires root privileges to perform certain types of scans, so you might need to prepend sudo to your Nmap commands.
- **Check Documentation**: For usage instructions, you can access the Nmap documentation by running:

  man nmap

```
[10/07/24]seed@VM:~$ man nmap
```

```
NMAP(1)            Nmap Reference Guide            NMAP(1)

NAME
       nmap - Network exploration tool and security /
       port scanner

SYNOPSIS
       nmap [Scan Type...] [Options]
            {target specification}

DESCRIPTION
       Nmap ("Network Mapper") is an open source tool
       for network exploration and security auditing.
       It was designed to rapidly scan large
       networks, although it works fine against
       single hosts. Nmap uses raw IP packets in
       novel ways to determine what hosts are
       available on the network, what services
       (application name and version) those hosts are
       offering, what operating systems (and OS
       versions) they are running, what type of
l page nmap(1) line 1 (press h for help or q to quit)
```

1. Host Discovery Scan

```
[12/10/24]seed@VM : ~ / . . . /$ nmap -sn 192.168.1.0/24
Nmap scan report for 192.168.1.1
Host is up (0.0020s latecncy)
Mac Address: AA:BB:CC (Router)

Nmap scan report for 192.168.1.1
Host is up (0.0020s latecncy)
Mac Address: 11:22:33 (Device Manufacturer)

Nmap scan report for 192.168.1.1
Host is up (0.0020s latecncy)
Mac Address: 77:88:99 (Device Manufacturer)

Nmap done: 256 IP addresses (3 hosts up) scanned in 3.10 seconds
```

2. TCP Connect Scan

```
[12/10/24]seed@VM : ~ / . . . /$ nmap -st 192.168.1.0/24
Nmap scan report for 192.168.1.1
 Host is up (0.0010s latecncy)
 Not shown: 996 closed ports
 Port        STATE SERVICE
22/tcp   open    ssh
80/tcp   open   http
443/tcp  open  https
```

3. SYN Scan

```
[12/10/24]seed@VM : ~ / . . . /$ nmap -sS 192.168.1.0/24
Nmap scan report for 192.168.1.1
 Host is up (0.0010s latecncy)
 Not shown: 996 closed ports
 Port        STATE SERVICE
22/tcp   open    ssh
 80/tcp   open   http
443/tcp   open   https

Nmap done: 1000 IP addresses (1 host up) scanned in 5.01 seconds
```

4. Service Version Detection

```
[12/10/24]seed@VM : ~ / . . . /$ nmap -sV 192.168.1.0/24
Nmap scan report for 192.168.1.1
 Host is up (0.0010s latecncy)
 Not shown: 996 closed ports
PORT       STATE SERVICE     Version
 22/tcp     open   ssh          OpenSSH 8.0 (protocol 2.0)
 80/tcp     open  http           Apache 2.4.41 (ubuntu)
443/tcp    open  ssl/http       Apache httped 2.4.41
```

5. Operating System Detection

```
[12/10/24]seed@VM : ~ / . . . /$  nmap -O 192.168.1.0/24
Nmap scan report for 192.168.1.1
 Host is up (0.0010s latecncy)
 Not shown: 996 closed ports
 OS details: Linux 3.2 - 4.9
 Network Distance: 1 hop

Nmap done: 1000 IP Addresses (1 host up) scanned in 8.01 seconds
```

Scan a single IP address When firewall OFF/ON on target
PC Syntax – nmap IP address/hostname

```
[08/21/24]seed@VM:~$ nmap 172.16.50.88
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-21 01:35 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.07 seconds

[08/21/24]seed@VM:~$ nmap google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-21 01:38 EDT
Nmap scan report for google.com (142.250.192.14)
Host is up (0.0094s latency).
Other addresses for google.com (not scanned): 2404:6800:4009:81f::200e
rDNS record for 142.250.192.14: bom12s14-in-f14.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 4.35 seconds
```

To boost Up your Nmap :

```
[08/21/24]seed@VM:~$ nmap -F 192.168.75.131
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-21 01:55 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.06 seconds
[08/21/24]seed@VM:~$

[08/21/24]seed@VM:~$ nmap -F google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-21 01:51 EDT
Nmap scan report for google.com (142.250.70.110)
Host is up (0.0068s latency).
Other addresses for google.com (not scanned): 2404:6800:4009:82b::200e
rDNS record for 142.250.70.110: pnbomb-ac-in-f14.1e100.net
Not shown: 98 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 1.86 seconds
```

Scan multiple IP address or subnet

A. scan a range of IP address

```
[08/21/24]seed@VM:~$ nmap 192.168.75.131
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-21 01:36 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.05 seconds
```

B.Scan a range of IP address using a wildcard

```
[08/21/24]seed@VM:~$ nmap 192.168.75.*
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-21 01:56 EDT
Nmap done: 256 IP addresses (0 hosts up) scanned in 103.46 seconds
```

C.Scan Multiple Hosts

```
[08/21/24]seed@VM:~$ nmap 192.168.0.101 192.168.0.102 192.168.0.103
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-21 02:01 EDT
Nmap done: 3 IP addresses (0 hosts up) scanned in 3.04 seconds
```

D.Scan an entire subnet

```
[08/21/24]seed@VM:~$ nmap 192.168.75.1/24
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-21 02:01 EDT
Nmap done: 256 IP addresses (0 hosts up) scanned in 104.42 seconds
```

E.Scan Multiple Servers using last octet of IP address

```
[08/21/24]seed@VM:~$ nmap 192.168.0.101,102,103
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-21 02:04 EDT
Nmap done: 3 IP addresses (0 hosts up) scanned in 3.04 seconds
[08/21/24]seed@VM:~$ sudo nmap -sX 192.168.75.131
Starting Nmap 7.80 ( https://nmap.org ) at 2024-08-21 02:10 EDT
Nmap scan report for 192.168.75.131
Host is up (0.00041s latency).
All 1000 scanned ports on 192.168.75.131 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

```
[08/21/24]seed@VM:~$ sudo apt update
Get:1 http://security.ubuntu.com/ubuntu focal-security InRelease [128 kB]
Get:2 http://security.ubuntu.com/ubuntu focal-security/main i386 Packages [798 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu focal InRelease [265 kB]
Get:4 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [3,129 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu focal/main amd64 Packages [970 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu focal/main i386 Packages [718 kB]
```

Conclusion :

In network security, Nmap (Network Mapper) is a powerful tool for network discovery and security auditing. It helps identify open ports, services, and potential vulnerabilities on networked devices. By providing detailed information about hosts and their configurations, Nmap plays a crucial role in assessing network security, enabling proactive measures against unauthorized access and cyber threats.

Conclusion

In this experiment, we studied Nmap as a packet scanning and network mapping tool. By performing various scans, we gained insights into the structure and services of a network, identifying live hosts, open ports, and running services.