BHARATIYA VIDYA BHAVAN'S
SARDAR PATEL INSTITUTE OF TECHNOLOGY
(Empowered Autonomous Institute Affiliated to Mumbai University)
Department Of Computer Engineering

Name	Manish Shashikant Jadhav
UID	2023301005
Subject	Computer Communication and Networks (CCN)
Experiment No.	8
Aim	Network Mapping using nmap.
Task 1:	**1. Installation and Setup:** • **Install NMAP on your system if not already installed. (https://www.geeksforgeeks.org/nmap-command-in-linux-with-examples/)** • **Familiarize yourself with the basic syntax and options of NMAP.**
Task 2:	**2. Basic Scanning:** • **Perform a simple ping scan on a target IP address to determine its availability.**

```
manishj@ubuntu:~/Desktop/ccn8$ sudo apt-get install nmap
[sudo] password for manishj:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libblas3 liblinear4 liblua5.3-0 lua-lpeg nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  libblas3 liblinear4 liblua5.3-0 lua-lpeg nmap nmap-common
0 upgraded, 6 newly installed, 0 to remove and 316 not upgraded.
Need to get 5,669 kB of archives.
After this operation, 26.8 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu focal/main amd64 libblas3 amd64 3.9.0
-1build1 [142 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 liblinear4 amd64
 2.3.0+dfsg-3build1 [41.7 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu focal/main amd64 liblua5.3-0 amd64 5.
3.3-1.1ubuntu2 [116 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 lua-lpeg amd64 1
.0.2-1 [31.4 kB]
```

```
manishj@ubuntu:~/Desktop/ccn8$ nmap -sn 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-01 07:41 PDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -P
n
Nmap done: 1 IP address (0 hosts up) scanned in 3.00 seconds
manishj@ubuntu:~/Desktop/ccn8$
```

	• **Conduct a TCP SYN scan on a target IP range to identify open ports.**
	`manishj@ubuntu:~/Desktop/ccn8$ nmap -sS 192.168.1.0/24`
	`You requested a scan type which requires root privileges.`
	`QUITTING!`
	`manishj@ubuntu:~/Desktop/ccn8$`

Task 3:	**3. Service Version Detection:**
	• **Perform a service version detection scan on a target IP to identify the version of services running on open ports.**
	`manishj@ubuntu:~/Desktop/ccn8$ nmap -sV 192.168.1.1`
	`Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-01 07:45 PDT`
	`Note: Host seems down. If it is really up, but blocking our ping probes, try -P n`
	`Nmap done: 1 IP address (0 hosts up) scanned in 3.32 seconds`
	`manishj@ubuntu:~/Desktop/ccn8$`

Task 4:	**4. Operating System Detection:**
	• **Use NMAP to detect the operating system of a target device.**
	`manishj@ubuntu:~/Desktop/ccn8$ nmap -O 192.168.1.1`
	`TCP/IP fingerprinting (for OS scan) requires root privileges.`
	`QUITTING!`
	`manishj@ubuntu:~/Desktop/ccn8$`

Task 5:	**5. Scripting with NMAP:**
	• **Write a simple NMAP script to automate a scanning task of your choice.**
	`manishj@ubuntu:~/Desktop/ccn8$ nmap --script http-enum 192.168.1.1`
	`Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-01 07:51 PDT`
	`Note: Host seems down. If it is really up, but blocking our ping probes, try -P n`
	`Nmap done: 1 IP address (0 hosts up) scanned in 3.36 seconds`
	`manishj@ubuntu:~/Desktop/ccn8$`

Objectives:	**1. Scan a given network range and identify all active hosts.**
	`manishj@ubuntu:~/Desktop/ccn8$ nmap -sn 192.168.1.20`
	`Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-01 07:56 PDT`
	`Note: Host seems down. If it is really up, but blocking our ping probes, try -P n`
	`Nmap done: 1 IP address (0 hosts up) scanned in 3.01 seconds`
	`manishj@ubuntu:~/Desktop/ccn8$`

2. **Identify the top 5 most commonly open ports on a specific target.**

```
manishj@ubuntu:~/Desktop/ccn8$ nmap -sS -p- --top-ports 5 192.168.1.1
You requested a scan type which requires root privileges.
QUITTING!
manishj@ubuntu:~/Desktop/ccn8$
```

3. **Determine the MAC address of a target device using NMAP.**

```
manishj@ubuntu:~/Desktop/ccn8$ nmap -sn -n -Pn -sP 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-01 09:12 PDT
Nmap scan report for 192.168.1.1
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.00 seconds
manishj@ubuntu:~/Desktop/ccn8$
```

4. **Perform a scan to detect the presence of HTTP and HTTPS services on a target network.**

```
manishj@ubuntu:~/Desktop/ccn8$ nmap -sSV -p 80,443 192.168.1.0/24
You requested a scan type which requires root privileges.
QUITTING!
manishj@ubuntu:~/Desktop/ccn8$
```

5. **Find out if a particular host has FTP service running on it.**

```
manishj@ubuntu:~/Desktop/ccn8$ nmap -sS -p 21 192.168.1.1
You requested a scan type which requires root privileges.
QUITTING!
manishj@ubuntu:~/Desktop/ccn8$
```

6. **Identify the SSH version running on a given host.**

```
manishj@ubuntu:~/Desktop/ccn8$ nmap -sV -p 22 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-01 09:14 PDT
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 3.62 seconds
manishj@ubuntu:~/Desktop/ccn8$ nmap -sV -Pn 22 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-01 09:15 PDT

manishj@ubuntu:~/Desktop/ccn8$
```

7. **Scan a range of IP addresses and list all hosts that have Telnet service running.**

```
manishj@ubuntu:~/Desktop/ccn8$ nmap -sS -p 23 192.168.1.0/24
You requested a scan type which requires root privileges.
QUITTING!
manishj@ubuntu:~/Desktop/ccn8$
```

8. **Determine the operating system of a target host using NMAP.**

```
manishj@ubuntu:~/Desktop/ccn8$ nmap -O 192.168.1.1
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!
manishj@ubuntu:~/Desktop/ccn8$
```

9. **Identify any SQL services running on a given network.**

```
manishj@ubuntu:~/Desktop/ccn8$ nmap -sV -p 1433,1434,1521,3306,5432,5900 192.168.
1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-01 09:18 PDT
Nmap done: 256 IP addresses (0 hosts up) scanned in 105.46 seconds
```

10. **Find out if a specific host has Remote Desktop Protocol (RDP) enabled.**

```
manishj@ubuntu:~/Desktop/ccn8$ nmap -sV -p 3389 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-01 09:27 PDT
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 3.32 seconds
manishj@ubuntu:~/Desktop/ccn8$ S
```

11. **Scan a target network and determine if any hosts are running DNS services.**

```
manishj@ubuntu:~/Desktop/ccn8$ nmap -sSV -p 53 192.168.1.0/24
You requested a scan type which requires root privileges.
QUITTING!
manishj@ubuntu:~/Desktop/ccn8$
```

12. **Detect if a host has SNMP (Simple Network Management Protocol) enabled.**

```
manishj@ubuntu:~/Desktop/ccn8$ nmap -sU -p 161 192.168.1.1
You requested a scan type which requires root privileges.
QUITTING!
manishj@ubuntu:~/Desktop/ccn8$
```

13. Perform a scan to identify any SMTP (Simple Mail Transfer Protocol) servers on a network.

```
manishj@ubuntu:~/Desktop/ccn8$ nmap -sSV -p 25,465,587 192.168.1.0/24
You requested a scan type which requires root privileges.
QUITTING!
manishj@ubuntu:~/Desktop/ccn8$
```

14. Determine if a target network has any active FTP servers allowing anonymous login.

```
manishj@ubuntu:~/Desktop/ccn8$ nmap --script ftp-anon 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-01 09:32 PDT
Nmap done: 256 IP addresses (0 hosts up) scanned in 105.42 seconds
manishj@ubuntu:~/Desktop/ccn8$
```

15. Find out if any hosts in a network are running vulnerable versions of the Apache HTTP server.

```
manishj@ubuntu:~/Desktop/ccn8$ nmap --script http-vuln* 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-01 09:35 PDT
Nmap done: 256 IP addresses (0 hosts up) scanned in 105.57 seconds
manishj@ubuntu:~/Desktop/ccn8$
```

16. Detect if a target host has any open NFS (Network File System) shares.

17. Identify the presence of any MySQL database servers on a given network.

18. Scan a network to determine if any hosts have the Remote Procedure Call (RPC) service running.

19. Detect if a specific host has any open VNC (Virtual Network Computing) ports.

20. Perform a scan to identify any hosts with the Secure Shell (SSH) service running on non-default ports.

Conclusion	Hence, by completing this experiment I came to know about Installation and configuration of FTP server.