Ex1. Perform an Experiment for port scanning with nmap

Aim of the Experiment:

-To understand what a **network port** is, how to use **Nmap** to scan for open ports on a machine, and to distinguish between **ethical** and **unethical** uses of port scanning with real-world examples.

What is a Port?

Imagine a Computer as a Hotel:

- A **hotel** has many **rooms**.
- Each **room** serves a different purpose (e.g., dining, sleeping, storage).
- A **computer** is like a **hotel**, and **ports** are its **rooms**.

Definition:

-A **port** is a **communication endpoint** on a computer where data is received and sent. Each port is associated with a specific service or application.

Port Numbers:

- Ports are numbered from **0 to 65535**.
- Common Port Numbers:

Port Number	Protocol	Use
20, 21	FTP	File transfer
22	SSH	Secure remote login
23	Telnet	Unsecure remote login
25	SMTP	Sending email
53	DNS	Resolving domain names
80	HTTP	Web browsing
443	HTTPS	Secure web browsing
3306	MySQL	Database

Example:

- When you open https://www.google.com, your browser connects to **port 443** on Google's servers because it's using **HTTPS**.

What is Port Scanning?

-Port scanning is like checking which **doors (ports)** are open on a building (computer) to see which services are active. It helps in:

- Identifying vulnerabilities
- Auditing networks
- Ethical hacking

What is Nmap?

- **Nmap** = **Network Mapper**
- It's a powerful command-line tool used to:
  - Discover live hosts on a network
  - Identify open ports and services
  - Detect the operating system
  - Perform security audits

Tools Required:

Tool	Description
Nmap	Port scanner
Target Machine	Localhost / VM (Ubuntu, Windows, etc.)
OS	Kali Linux / Ubuntu / Windows
Network Setup	LAN or Virtual Network (do **not** scan public IPs without permission)

Types of Port States (Nmap output):

Port State	Meaning
Open	Service is listening (can connect)
Closed	No service is listening (but port exists)
Filtered	Port blocked by firewall
Unfiltered	Port accessible, but no info
**Open	Filtered**
**Closed	Filtered**

Step-by-Step Procedure:

A. Beginner – Basic Scan:

nmap <target_ip>

Example:

nmap 192.168.1.5

B. Intermediate – Detect Service Versions:

nmap -sV 192.168.1.5 `

- Shows version of services (e.g., Apache 2.4.41)

C. Expert – Aggressive Scan:

nmap -A 192.168.1.5

- Performs: OS Detection, Version detection, Script scanning, Traceroute

Sample/Expected Output:

```
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.9
80/tcp   open  http     Apache httpd 2.4.38
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
```

Complete Nmap Commands, Subcommands, Uses & Use Cases

1. Basic Scanning Commands

Command	Use	Example	Use Case
nmap <IP>	Basic scan	nmap 192.168.1.1	Discover open ports
nmap <domain>	Scan domain	nmap google.com	Scan web server

2. Port Scanning Options

Command	Use	Example	Use Case
-p <port>	Scan specific port	nmap -p 22 192.168.1.1	Check if SSH is open
-p-	Scan all 65535 ports	nmap -p- 192.168.1.1	Full port sweep
-F	Fast scan (top 100 ports)	nmap -F 192.168.1.1	Quick check for common services
-r	Scan ports in order	nmap -r 192.168.1.1	Ordered port scan
--top-ports <n>	Scan top N ports	nmap --top-ports 20 192.168.1.1	Fast scan on most used ports

3. Scan Techniques

Command	Technique	Use Case
-sS	TCP SYN scan (stealth)	Default and fast scan
-sT	TCP connect scan	When SYN scan fails (no root)
-sU	UDP scan	Scan services like DNS, SNMP
-sN	Null scan	Firewall evasion (advanced)

Command	Technique	Use Case
-sX	Xmas scan	IDS evasion
-sF	FIN scan	Stealth scan with FIN flags

4. Service & Version Detection

Command	Use	Example	Use Case
-sV	Detect service versions	nmap -sV 192.168.1.1	Check app versions (Apache, SSH)
--version-intensity <0-9>	Control version detection	nmap --version-intensity 5	Faster vs more accurate scans

5. OS Detection

Command	Use	Example	Use Case
-O	Detect OS	nmap -O 192.168.1.1	Find target OS type (Windows, Linux)
--osscan-guess	Guess OS aggressively	nmap -O --osscan-guess	Useful if detection is unclear

6. Aggressive Scan

Command	Use	Example	Use Case
-A	Aggressive scan (OS + version + script + traceroute)	nmap -A 192.168.1.1	Full audit of target

7. Script Scanning (Nmap Scripting Engine - NSE)

Command	Use	Example	Use Case
-sC	Run default scripts	nmap -sC 192.168.1.1	Check for common vulnerabilities
--script <script>	Run specific script	nmap --script http-title	Show webpage title
--script vuln	Run vulnerability scan scripts	nmap --script vuln	Check for CVEs, weak services

8. Timing & Performance

Command	Use	Example	Use Case
-T0 to -T5	Timing templates	nmap -T4 192.168.1.1	Faster scans (T4/T5) or stealthier (T0)
--min-rate	Set minimum packets/sec	nmap --min-rate 1000	Fast scans
--max-retries	Limit retries	nmap --max-retries 2	Avoid long scan times

9. Output Options

Command	Use	Example	Use Case
-oN	Normal output	nmap -oN scan.txt	Easy-to-read output
-oX	XML output	nmap -oX scan.xml	Parse in scripts
-oG	Grepable output	nmap -oG scan.grep	For scripting/automation
-oA	All formats	nmap -oA fullscan	Get .nmap, .xml, .grep files

10. Host Discovery

Command	Use	Example	Use Case
-sn	Ping scan only	nmap -sn 192.168.1.0/24	Find live hosts
-Pn	Disable ping	nmap -Pn 192.168.1.1	Scan hidden hosts (ICMP blocked)
-PS, -PA, -PU	TCP SYN, TCP ACK, UDP ping	nmap -PS80,443	Custom host discovery

11. Firewall/IDS Evasion

Command	Use	Example	Use Case
-f	Fragment packets	nmap -f 192.168.1.1	Bypass simple firewalls
--source-port <port>	Set source port	nmap --source-port 53	Fake DNS to bypass filters
-D RND:10	Decoy scanning	nmap -D RND:10 192.168.1.1	Hide real source IP
--data-length <n>	Add payload	nmap --data-length 50	Obfuscate scan packets

12. Scanning Multiple Targets

Command	Use	Example	Use Case
nmap 192.168.1.1-10	Scan range of IPs	nmap 192.168.1.1-254	Scan full subnet
nmap -iL list.txt	Input from file	nmap -iL ips.txt	Batch scan
nmap -iR 5	Scan 5 random hosts	nmap -iR 10	Random host scanning
nmap --exclude <ip>	Exclude IP	nmap --exclude 192.168.1.5	Skip specific systems

13. Real-World Use Cases

Use Case	Nmap Feature Used
Network Inventory	nmap -sP 192.168.0.0/24
Find Open Web Servers	nmap -p 80,443 -sV 192.168.1.0/24
Detect Vulnerabilities	nmap --script vuln
Audit SSH Security	nmap --script ssh* -p 22
Check Database Exposure	nmap -p 3306 --script mysql*
Identify IoT Devices	nmap -O -sV
Bypass Firewalls (Lab use only)	nmap -f or nmap -D RND:10

Next Steps After Mastering Nmap

1. Learn **Wireshark** for packet analysis
2. Master **Nmap Scripting Engine (NSE)** scripting (Lua-based)
3. Move into **Vulnerability Scanning** with tools like **Nessus**, **OpenVAS**
4. Practice on labs like **TryHackMe**, **Hack The Box**
5. Get certified: **CEH**, **OSCP**, or **CompTIA Security+**
6. Combine Nmap with **Metasploit Framework**
7. Scan and secure cloud systems (AWS, Azure, GCP)

Observations:

Command/Tool	Purpose/Observation

Real-Time Scenarios (Examples):

Legal Scenario:

-A security team scans their company's internal servers to find open ports for maintenance — **with permission**.

Illegal Scenario:

-A hacker scans a bank's website without permission and uses open ports to exploit a server — **without permission**, violates the **IT Act 66C/66D** in India.

Legal vs Illegal Use of Port Scanning:

Action	Legal	Illegal	Example
Scan your own PC/server	✅	❌	Test open services on localhost
Scan a public IP without asking	❌	✅	Scanning Netflix.com
Scan a friend's PC with permission	✅	❌	Lab practice
Scan government servers	❌	✅	Against the law

Additional Tips for Better Understanding:

- Use nmap localhost to safely test on your own machine.
- Use nmap -F for a **fast scan** (top 100 ports).
- Use nmap -O to detect the **OS** of the target (in aggressive mode).
- Always **log your scans** with on filename.txt.

Precautions and Ethics:

- **Never** scan unknown IPs without written permission.
- Respect **cyber laws** and **digital ethics**.
- Use tools only in labs, sandboxes, or for **certified penetration testing**.
- Educate others on legal/illegal boundaries of scanning.

What Can I Do If I Know Port Scanning Well?

- - Learn vulnerability assessment and penetration testing (VAPT)
- - Practice ethical hacking using platforms like Hack The Box, TryHackMe
- - Get certified (e.g., CEH, CompTIA Security+, OSCP)
- - Learn advanced tools like Wireshark, Nessus, Metasploit
- - Join bug bounty programs (HackerOne, Bugcrowd)

Conclusion/Result:

This experiment taught:

- The **concept of ports and services**
- **Nmap** usage at various levels (basic to advanced)
- The importance of **ethical hacking**
- Differences between **safe/unsafe**, **legal/illegal** scanning

Port scanning is a powerful tool — but with great power comes great responsibility!

Viva / Interview Questions:

1. What is a network port?
2. How does Nmap work?
3. What is the difference between TCP and UDP scanning?
4. What do you mean by "filtered" port?
5. What are ethical issues in port scanning?
6. What Indian law punishes illegal hacking or scanning?
7. Why do attackers use Nmap?
8. How can organizations protect their open ports?