**Exercise 1:**

Perform an Experiment for port scanning with NMAP

**Aim:**

To perform a port scanning experiment using Nmap to identify open ports on a target system and gain insight into its network security posture.

**Requirements:**

1. \*\*Nmap\*\*: Ensure that Nmap is installed on your system. You can download it from the official website (https://nmap.org/download.html) or install it using package managers like apt (for Linux)

2. \*\*Target System\*\*: Choose a target system or network to scan. Ensure that you have permission to perform the scan, as port scanning can be considered intrusive and may violate network policies or laws if conducted without authorization.

**What is Nmap?**

* Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications.
* Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.

# Why use Nmap?

* There are a number of reasons why security pros prefer Nmap over other scanning tools.
* First, Nmap helps you to quickly map out a network without sophisticated commands or configurations. It also supports simple commands (for example, to check if a host is up) and complex scripting through the Nmap scripting engine.
* Nmap (Network Mapper) is a powerful open-source tool used for network discovery, security auditing, and exploration. Its primary use is to scan networks, identify hosts, services, and operating systems, and detect vulnerabilities. Below are some of its key uses:

**How to scan ip address and ports with Nmap**

**Steps:**

**1. Identify the Target:**

- Determine the IP address or hostname of the target system or network you want to

scan.

**2. Determine Scan Type:**

- Decide on the type of scan you want to perform based on your objectives and the

level of intrusiveness allowed:

**3. Execute the Scan:**

- Open a terminal or command prompt.

- Use the following command syntax to perform Scan:

```

nmap –command [target]

```

Replace `[target]` with the IP address or hostname of the target system.

- Optionally, you can specify additional options to customize the scan according to

your requirements.

**4. Analyze the Results:**

- Once the scan is complete, Nmap will provide a detailed report indicating the status

of each scanned port (open, closed, filtered) and may include additional information

such as service versions, operating system detection, and potential vulnerabilities.

- Interpret the results to identify open ports, which could indicate services running on

the target system.

## Basic scans

1. **TCP scan —**Scans the list of ports up and running on a given TCP network.
   * nmap -sT 192.168.1.1 (any IP address)
   * (In above command s->scan , T->Tcp )
2. **Ping scan —**Scans the list of devices up and running on a given subnet.
   * nmap -sp 192.168.1.1

## Stealth scan

* + nmap -sS 192.168.1.1

## Version scanning

* + nmap -sV 192.168.1.1

## Oparating system scanning

* + nmap -sO 192.168.1.1

### ****Host Discovery****

Nmap helps in identifying active hosts on a network.

**Command**: nmap -sn <target>

This sends a ping to the target to see if it's alive without performing a full scan.

## Scanning Multiple Hosts

nmap 192.164.1.1 192.164.0.2 192.164.0.2

## port scanning

nmap -sT 192.168.1.1 –p8080 (any port no.)

### ****Detecting Vulnerabilities****

Nmap scripts (NSE - Nmap Scripting Engine) allow for more advanced tasks such as

vulnerability scanning, brute-forcing, etc.

**Command**: nmap --script <script\_name> <target>

For example, you can use --script vuln to check for common vulnerabilities.

### ****Aggressive Scanning****

Combines multiple features like OS detection, version detection, and traceroute into one command.

**Command**: nmap -A <target>

This provides detailed information about the target in one scan.

## UDP scanning (scans UDP ports)

* 1. nmap -sU 192.168.1.1

1. **Intensive Scan (-T4 or -T5): Faster scans, but may be more detectable.**

nmap -T4 -A -v 127.0.0.1

Comprehensive Scan (-A)\*\*: Enables OS detection, version detection,

script scanning, and traceroute.