

# Day 9: Network Vulnerability Scanning

## What is Port Scanning?

Port scanning means checking which ports on a computer or device are open. A port is like a door number (0–65535) that services (like web server, email) listen on. Scanning finds out if doors are open, closed, or blocked.

## Open vs Closed vs Filtered Ports

- Open → A program is listening and accepts connections (good for service, but risky if unnecessary).
- Closed → No program is listening, but the machine answers "no thanks" (RST packet in TCP).
- Filtered → Firewall or network blocks probes — Nmap can't tell if open or closed (no response or ICMP error).

## What is Nmap?

Nmap (Network Mapper) is the most popular free tool for network scanning. It discovers devices, open ports, running services, operating systems, and sometimes vulnerabilities.

## What is Service Enumeration?

After finding open ports, Nmap asks the service "who are you?" and gets version info (e.g., Apache 2.4.41, SSH OpenSSH 8.2p1). This helps know if the version has known bugs.

## Why Scanning is Important?

- Find unknown/unsecured devices on your network.
- See what services are exposed to attackers.
- Check for old/outdated software with vulnerabilities.
- Part of ethical hacking, penetration testing, and defense (know your attack surface). Without scanning, you can't protect what you don't see.

## Basic Nmap Steps (as per task)

1. Scan local network (e.g., `nmap 192.168.1.0/24`).
2. Find open ports (`-p-` for all, or default top 1000).
3. Detect services (`-sV`).
4. Identify OS (`-O`).
5. Check vulnerabilities (using NSE scripts: `-sC` or `--script vuln`).
6. Save output (`-oN report.txt`).
7. Read and understand risks (e.g., old software = high risk).