## ****Network Scanning Using Nmap****

### ****1. Overview****

**Nmap** (Network Mapper) is an essential tool for discovering hosts, services, and security vulnerabilities within a network. It helps security professionals identify open ports and running services.

### ****2. Step-by-Step Guide****

#### ****Step 1: Install Nmap****

Download and install Nmap from [Nmap’s official website](https://nmap.org/).

Ensure the installation includes **Zenmap** (GUI version) if needed.

#### ****Step 2: Scan a Target Network****

Open a terminal and run a basic network scan:

nmap -sn <target-IP-range>

This command will detect **active hosts** in the network.

#### ****Step 3: Perform Port Scanning****

To scan open ports on a specific device, use:

nmap -p- <target-IP>

This helps identify **open ports** that might be vulnerable.

#### ****Step 4: Perform Service and Version Detection****

Run the following command to determine running services:

nmap -sV <target-IP>

This provides details about **applications and versions** on open ports.

#### ****Step 5: Conduct OS Detection****

To determine the operating system of a target device, use:

nmap -O <target-IP>

### ****3. Findings & Observations****

Detected active devices within the network.

Identified open ports that could be exploited.

Discovered running services and their versions.

### ****4. Mitigation Strategies****

Close **unnecessary open ports** and services. Use **firewall rules** to restrict scanning attempts. Regularly update and **patch vulnerabilities**.

