Network Mapping

**Network Mapping Project using Nmap:**

**Project Objective:**

Create a comprehensive network map of a target network, identifying devices, services, and potential vulnerabilities.

**Tools Needed:**

1. Nmap

**Project Steps:**

**Phase 1: Network Discovery**

1. Perform an ICMP ping sweep to identify alive hosts: **nmap -sP (TARGET IP)** EX:192.168.1.1

2. Conduct a TCP SYN scan to identify open ports: **nmap -sS (TARGET IP)** EX:192.168.1.1

3. Use Nmap scripts to identify services and operating systems: **nmap -sC (TARGET IP)** EX:192.168.1.1

**Phase 2: Vulnerability Identification:**

1. Run Nmap vulnerability scanning scripts (e.g., **nmap -sV --script=vuln (TARGET IP)** EX:192.168.1.1.

2. Identify potential vulnerabilities and document findings.

**Phase 3: Network Scanning use Nmap:**

1. Commands nmap (particular ip or Network range)
2. Ex: (nmap 192.168.10.1) if we hit enter it will be scan the network and show the output the host who is connect the network.

**Example Nmap Commands:**

1. nmap -sP **(TARGET IP)** EX:192.168.1.1.

(ICMP ping sweep)

2. nmap -sS **(TARGET IP)** EX:192.168.1.1.

(TCP SYN scan)

3. nmap -sC **(TARGET IP)** EX:192.168.1.1.

(service and OS identification)

4. nmap -sV --script=vuln **(TARGET IP)** EX:192.168.1.1. (vulnerability scanning)

**Example Output :**

Nmap scan report for 192.168.1.100

Host is up (0.00044s latency).

Not shown: 995 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

139/tcp open netbios-ssn

445/tcp open microsoft-ds

MAC Address: 00:11:22:33:44:55 (Apple)

**step-by-step guide on how to install and use network mapping tools:**

**Installing Nmap:**

1. Visit the Nmap website and download the latest version. **/ It will be default in kali linux.**

2. Choose the correct installation package for your operating system (Windows, macOS, Linux).

3. Follow the installation instructions.

4. kali linux **type nmap hit enter** it will be default in kali linux and **type nmap -h** it will be show all the feature of nmap and how to use it.

**Using Nmap for Network Mapping:**

1. Open a **Root terminal in Kali linux** or command prompt.

2. Type **nmap -sP 192.168.10.1**(replace with your network IP range).

3. Press Enter to scan the network.

4. View the scan results.

**Basic Nmap Commands:**

1. nmap -sP 192.168.1.0/24 (ICMP ping sweep)

2. nmap -sS 192.168.1.0/24 (TCP SYN scan)

3. nmap -sC 192.168.1.0/24 (service and OS identification)

4. nmap -sV --script=vuln 192.168.1.0/24 (vulnerability