**🛡️ Network Scanning Using Nmap: A Practical Approach**

**🔍 1. Host Discovery (Network Discovery)**

Used to find live hosts on a network.

**✅ Ping Scan (Check who’s online)**

bash

CopyEdit

nmap -sn 192.168.1.0/24

Scans entire subnet, showing which IPs are active.

**✅ Disable DNS resolution (faster scan)**

bash

CopyEdit

nmap -n -sn 192.168.1.0/24

**✅ List targets without sending packets**

bash

CopyEdit

nmap -sL 192.168.1.0/24

**📦 2. Port Scanning**

Used to find open ports on a target system.

**✅ Default TCP port scan**

bash

CopyEdit

nmap 192.168.1.10

**✅ Scan specific ports**

bash

CopyEdit

nmap -p 21,22,80,443 192.168.1.10

**✅ Scan all 65535 ports**

bash

CopyEdit

nmap -p- 192.168.1.10

**✅ TCP SYN Scan (Stealth scan)**

bash

CopyEdit

sudo nmap -sS 192.168.1.10

**✅ TCP Connect scan**

bash

CopyEdit

nmap -sT 192.168.1.10

**✅ UDP Port Scan**

bash

CopyEdit

sudo nmap -sU 192.168.1.10

**🔧 3. Service and Version Detection**

Identify which services are running and their versions.

**✅ Version detection**

bash

CopyEdit

nmap -sV 192.168.1.10

**✅ Aggressive scan (includes version, OS detection, script scanning)**

bash

CopyEdit

sudo nmap -A 192.168.1.10

**🧠 4. Operating System Detection**

Tries to guess the target OS.

**✅ OS Detection**

bash

CopyEdit

sudo nmap -O 192.168.1.10

**⚙️ 5. Nmap Scripting Engine (NSE)**

Advanced scanning using built-in scripts for vulnerabilities, brute-force, etc.

**✅ Run default scripts**

bash

CopyEdit

nmap -sC 192.168.1.10

**✅ Scan for known vulnerabilities**

bash

CopyEdit

nmap --script vuln 192.168.1.10

**✅ Run a specific script (e.g., HTTP title)**

bash

CopyEdit

nmap --script http-title 192.168.1.10

**📁 6. Scanning Multiple Targets**

**✅ Range of IPs**

bash

CopyEdit

nmap 192.168.1.1-100

**✅ Multiple targets**

bash

CopyEdit

nmap 192.168.1.10 192.168.1.11 192.168.1.12

**✅ From a file**

bash

CopyEdit

nmap -iL targets.txt

**📤 7. Output Formats**

Save scan results for documentation or automation.

**✅ Save in normal format**

bash

CopyEdit

nmap -oN output.txt 192.168.1.10

**✅ Save in XML format**

bash

CopyEdit

nmap -oX output.xml 192.168.1.10

**✅ Summary Table**

| **Purpose** | **Command Example** |
| --- | --- |
| Host Discovery | nmap -sn 192.168.1.0/24 |
| TCP Port Scan | nmap -p 1-1000 192.168.1.10 |
| UDP Port Scan | nmap -sU 192.168.1.10 |
| Service Detection | nmap -sV 192.168.1.10 |
| OS Detection | nmap -O 192.168.1.10 |
| Aggressive Scan | nmap -A 192.168.1.10 |
| Vulnerability Scan | nmap --script vuln 192.168.1.10 |
| Save Output | nmap -oN report.txt 192.168.1.10 |