# Basic Network Scanning with Nmap

## Objective

The goal of this task is to perform a basic network scan using Nmap to identify:

- Open ports

- Running services

- Operating system information

This helps understand exposure and possible security risks.

**Tools Used**

- Nmap (Network Mapper)

**Commands Executed**

1. **Host Discovery (Ping Scan)**
   **nmap -sn scanme.nmap.org**

2. **Full Port Scan**
   **nmap -p- scanme.nmap.org**

3. **3. Service Version Detection**
   **nmap -sV scanme.nmap.org**

4. **OS Fingerprinting**
   **nmap -O scanme.nmap.org**

5. **Aggressive Scan**

   **nmap -A scanme.nmap.org**

## Nmap Scan Results (From Uploaded Report)

According to your **nmap report.pdf**, these ports were found open:

- Host status: **Up**

- IP Address: **45.33.32.156**

- Scan Duration: **5.74 seconds**

🔍 Explanation of Results

**Port 22 — SSH (open)**

- Used for remote administration (Secure Shell)

- Risk: Vulnerable to brute-force attacks if weak passwords are used

- Recommendation: Use strong credentials & disable root login

◇ **Port 80 — HTTP (open)**

- Indicates the presence of a running web server (Apache/HTTP service)

- Risk: Outdated versions may contain known vulnerabilities

- Recommendation: Keep the web server patched and updated

◇ **Port 9929 — nping-echo (open)**

- Diagnostic port used by Nmap for echo testing

- Usually low-risk

- Purpose: Packet timing and response testing

◇ **Port 31337 — Elite (open)**

- Commonly seen in CTF labs or backdoor testing services

- Suspicious/unusual port number

- Risk: Could be misconfigured or intentionally exposed for testing

🌓 **Security Risk Assessment**

| Port | Service | Risk Level | Description |

|------|-------------|------------|-------------|

| 22 | SSH | High | Vulnerable to brute-force attempts |

| 80 | HTTP | Medium | Outdated web services may be exploited |

| 9929 | nping-echo | Low | Diagnostic port, minimal risk |

| 31337 | Elite | High | Often associated with test/backdoor services |

**Screenshots**

**All screenshots are included in the /screenshots/ folder.**