Task 9 : NETWORK VULNERABILITY SCANNING

1️⃣ Scan the Local Network

Find your local IP range

```
ipconfig     # Windows
```

```
ifconfig     # Linux / macOS
```

Example IP: 192.168.1.5
Network range: 192.168.1.0/24

Discover live hosts

```
nmap -sn 192.168.1.0/24
```

2️⃣ Identify Open Ports

```
nmap -p- 192.168.1.1
```

(Scans all 65,535 ports)

3️⃣ Detect Running Services

```
nmap -sV 192.168.1.1
```

4️⃣ Identify Operating System

```
nmap -O 192.168.1.1
```

5️⃣ Analyze Vulnerabilities

```
nmap --script vuln 192.168.1.1
```

This checks for:

- Outdated services
- Known CVEs
- Weak configurations

6️⃣ Save Scan Results

```
nmap -sV -O 192.168.1.1 -oN scan_report.txt
```

7️⃣ Interpret Risks (Example)

Port	Service	Risk
21	FTP	Unencrypted credentials
22	SSH	Brute-force attacks
80	HTTP	Vulnerable web apps

8️⃣ Document Findings (Deliverable)

📄 Network Scan Report

Target: Local Network (192.168.1.0/24)
Tool Used: Nmap
Date: DD/MM/YYYY

Findings:

- Detected **3 live hosts**
- Open ports: 22, 80, 443
- Services identified: SSH, Apache, HTTPS
- OS detected: Linux (Ubuntu)
- Vulnerabilities found:
  - Outdated Apache version
  - SSH password authentication enabled

Recommendations:

- Disable unused ports
- Update services
- Enable firewall rules
- Use SSH key-based authentication

🧠 Final Outcome

✔ Practical understanding of **network reconnaissance**
✔ Hands-on experience with **Nmap**
✔ Ability to analyze **security risks**

NAME: NITIN G N

Submission: Task 9

Date & Day: 29th January, Thursday

Internship: Elevate Labs

THANK YOU