Task 9: Network Vulnerability Scanning

By : Nroupsinh Gohil

Objective:

The objective of this task is to perform network vulnerability scanning to identify live hosts, open ports, running services, operating systems, and potential security risks in a local network using the Nmap tool.

Tool Used:

- Nmap (Network Mapper)

Step-by-Step Procedure:

1. Identifying Local Network

The local IP address was identified using system network commands. Based on the IP address, the network range was determined.

Example:

Local IP: 192.168.1.5

Network Range: 192.168.1.0/24

---

2. Scanning the Network for Live Hosts

A basic scan was performed to identify active devices and open ports in the network.

Command used:

nmap 192.168.1.0/24

---

3. Scanning a Specific Target

One active host was selected for detailed analysis.

Command:

nmap 192.168.1.1

This scan revealed open and closed ports on the target system.

---

4. Service and Version Detection

To identify services running on open ports and their versions:

nmap -sV 192.168.1.1

---

5. Operating System Detection

OS detection was performed to identify the operating system of the target machine.

nmap -O 192.168.1.1

---

6. Saving Scan Results

Scan results were saved for documentation and analysis.

nmap -sV -O 192.168.1.1 -oN scan_report.txt

Observations:

Port	Service	Risk
22	SSH	Brute-force attacks
80	HTTP	Web vulnerabilities
443	HTTPS	Certificate misconfigurations
445	SMB	Ransomware risk

Risk Analysis:

- Open ports increase attack surface.
- Outdated services can be exploited.
- Unnecessary services should be disabled.
- Firewalls and strong authentication are recommended.

Conclusion:

This task helped in understanding how attackers identify vulnerable systems. Network scanning is a critical step in securing systems and preventing unauthorized access.