Task 9: Network Vulnerability Scanning

Network Scan Report & Explanation

1. Scan Local Network

Network scanning is the process of discovering devices connected to a network.
In a local network, this means identifying computers, servers, routers, printers, or other devices that are active and reachable.

Purpose:

- To understand what devices exist on the network
- To detect unknown or unauthorized systems
- To create an inventory of network assets

---

2. Identify Open Ports

Ports are communication endpoints used by devices to send and receive data.
An open port means a service is actively listening and accepting connections.

Examples:

- Port 80 → Web service
- Port 22 → Secure remote access
- Port 443 → Secure web traffic

Why this matters:
Open ports can be entry points for attackers if they are misconfigured or unnecessary.

---

3. Detect Services

Service detection (also called service enumeration) identifies **what application or service** is running on an open port.

For example:

- A web server running on port 80
- An email service on port 25
- A database service on port 3306

Goal:
To understand *what software is exposed* to the network and whether it is needed or outdated.

---

4. Identify Operating System (OS)

OS detection attempts to determine the operating system of a device, such as:

- Windows
- Linux
- macOS
- Network devices (routers, firewalls)

Why it's important:
Different operating systems have different vulnerabilities.
Knowing the OS helps in applying the correct security patches and defenses.

---

5. Analyze Vulnerabilities

Vulnerability analysis compares detected services and operating systems against known security weaknesses.

Common issues found:

- Outdated software versions
- Weak or default configurations
- Services running unnecessarily

Result:
A list of potential security risks that could be exploited if left unpatched.

---

6. Save Scan Results

Scan results are saved for future reference and documentation.

Saved information usually includes:

- IP addresses
- Open ports
- Detected services
- OS details
- Vulnerability findings

Why saving matters:

- Helps track security improvements over time
- Useful for audits and compliance
- Supports incident response if something goes wrong

---

7. Interpret Risks

Not all vulnerabilities are equally dangerous. Risk interpretation evaluates:

- Severity of the vulnerability
- Likelihood of exploitation
- Impact if exploited

Example:
An exposed remote access service is a higher risk than an internal-only service.

---

8. Document Findings

Documentation summarizes everything in a clear, professional format.

Includes:

- Scope of the scan
- Tools used
- Key findings
- Risk assessment
- Recommendations

This document is shared with system administrators or management for action.
