CYBER SECURITY INTERNSHIP – TASK 9

Network Vulnerability Scanning Using Nmap

---

1. Introduction

Network vulnerability scanning is an important process in cyber security that helps identify open ports, running services, and potential security risks in a system. By scanning a network, security professionals can understand the attack surface and take necessary steps to secure systems.

This task focuses on performing a basic network scan using **Nmap** on the local system.

---

2. Tool Used

- **Nmap (Network Mapper)**
  Nmap is a free and open-source tool used for network discovery and security auditing. It is widely used to scan networks and identify open ports and services.

---

3. Target Description

The target selected for this scan was the **localhost (127.0.0.1)**, which represents the user's own system. Scanning localhost is safe and ensures that no unauthorized systems are tested.

---

4. Scan Command Used

The following Nmap command was executed:

```
nmap 127.0.0.1
```

This command performs a basic TCP port scan on the local system.

---

5. Scan Results

The Nmap scan reported that the host was active and reachable. Out of 1000 TCP ports scanned, **996 ports were found to be closed**, which indicates a reduced attack surface.

The following open ports were identified:

Port	State	Service	Description
135/tcp	Open	msrpc	Windows Remote Procedure Call
445/tcp	Open	microsoft-ds	SMB file sharing service
1755/tcp	Open	wms	Windows Media services
1761/tcp	Open	landesk-rc	Remote management service

---

6. Analysis of Findings

Open ports indicate services that are actively listening for connections. While these services are legitimate Windows services, they can become potential attack points if not properly secured.

Most of the scanned ports were closed, which is a positive security indicator. However, unnecessary services should be reviewed and disabled if not required.

---

7. Security Risks Identified

- Open ports may expose the system to unauthorized access
- Services like SMB (port 445) are commonly targeted by attackers
- Remote management services increase the attack surface

---

8. Recommendations

To improve security, the following measures are recommended:

- Disable unnecessary services
- Close unused ports
- Use a firewall to restrict access
- Keep the operating system updated
- Monitor network activity regularly