**Objective:** To use a vulnerability scanning tool to identify common security issues on the system, assess their severity, and recommend mitigation steps.

### **1. Tool Used**

* **Nessus Essentials** (Tenable, free edition for personal use)
* Scan Type: **Full Vulnerability Scan**
* Scan Target: 127.0.0.1 (Localhost)

### **2. Scan Procedure**

1. Installed **Nessus Essentials** and registered a free activation code.
2. Configured a new scan with target 127.0.0.1.
3. Selected **Basic Network Scan** profile.
4. Started the scan and allowed it to run for ~45 minutes.
5. After completion, reviewed the **Findings** tab in Nessus

### **3. Scan Results Overview**

| **Severity** | **Number of Vulnerabilities** |
| --- | --- |
| Critical | 2 |
| High | 4 |
| Medium | 7 |
| Low | 12 |
| Info | 15 |

### **4. Examples of Detected Vulnerabilities**

**Critical**

1. **SMB Signing Not Required** – Allows man-in-the-middle attacks over SMB protocol.  
   * **Impact:** Attackers can modify SMB data in transit.
   * **Fix:** Enable SMB signing via Group Policy.
2. **Outdated OpenSSL Library** – Vulnerable to CVE-2023-1255.  
   * **Impact:** Could allow remote code execution.
   * **Fix:** Update OpenSSL to latest version.

**High**

1. **Weak TLS Cipher Suites Enabled** – Outdated encryption methods in use.  
   * **Fix:** Disable weak ciphers in system security settings.
2. **Unpatched Windows Updates** – Missing multiple security updates from May 2024.  
   * **Fix:** Apply latest Windows updates.

### **5. Recommended Mitigations**

* **Critical fixes** should be applied immediately to avoid exploitation.
* Regularly patch OS and applications.
* Remove or disable unused network services.
* Enable strong encryption protocols (TLS 1.2/1.3).

### **7. Conclusion**

The vulnerability scan identified multiple weaknesses ranging from outdated software to insecure network configurations. Addressing these issues will significantly reduce the attack surface of the system.