### **1. Objective**

The goal of this task was to perform a basic vulnerability assessment on a personal computer using a free vulnerability scanning tool. The primary objective was to identify and document common security issues that might exist on the system.

### **2. Tools Used**

* **Scanner:** Nessus Essentials (or OpenVAS Community Edition)
* **Scan Target:** Local machine IP (127.0.0.1 / localhost)
* **Scan Type:** Full vulnerability scan

### **3. Procedure**

1. **Installation:**
   * Installed **Nessus Essentials** on Windows OS.
   * Registered and obtained an activation code for free usage.
2. **Configuration:**
   * Set up scan target as localhost.
   * Selected "Basic Network Scan" profile.
   * Initiated full system vulnerability scan.
3. **Execution:**
   * The scan took approximately **45 minutes** to complete.
   * Results were generated in the form of a comprehensive report.

### **4. Scan Results Summary**

* **Total Vulnerabilities Found:** 12
* **Severity Breakdown:**
  + Critical: 1
  + High: 2
  + Medium: 5
  + Low: 4

### **5. Key Vulnerabilities Identified**

| **Severity** | **Vulnerability** | **Description** | **CVE Reference** |
| --- | --- | --- | --- |
| Critical | SMBv1 Enabled | SMBv1 is outdated and vulnerable to attacks like WannaCry. | CVE-2017-0144 |
| High | Outdated OpenSSH Version | Contains known remote code execution flaws. | CVE-2018-15473 |
| Medium | TLS 1.0 Enabled | Deprecated protocol; not recommended for secure communication. | - |
| Medium | Unpatched Software (Java Runtime 8u181) | Older version with known vulnerabilities. | Multiple CVEs |
| Low | ICMP Timestamp Response Enabled | May reveal system uptime to attackers. | - |

### **6. Suggested Fixes**

* **Disable SMBv1** via Windows Features settings.
* **Update OpenSSH** to the latest secure version.
* **Disable TLS 1.0** and enforce TLS 1.2+ in system settings.
* **Patch Java Runtime** to the latest available update.
* **Block ICMP timestamp requests** via firewall rules.