**📝 Vulnerability Scan Report**

**Task 3: Perform a Basic Vulnerability Scan on Your PC**

| **Name:** | ***Pratiksha Baviskar*** |
| --- | --- |
| **Tool Used:** | Nessus Essentials |

**Objective**

To use a free vulnerability scanning tool (OpenVAS Community Edition or Nessus Essentials) to identify common vulnerabilities present on the computer and recommend solutions.

**1. Tool Details**

| **Tool Name:** | ***Nessus Essentials* / *OpenVAS*** |
| --- | --- |
| **Version:** | *e.g. Nessus v10.6.2* |
| **Platform:** | *Windows 10 / Kali Linux* |

**2. Scan Details**

* **Scan Name:** My PC Vulnerability Scan
* **Target:** Localhost (127.0.0.1)
* **Scan Type:** Basic Network Vulnerability Scan
* **Date of Scan:** *DD/MM/YYYY*

**3. Scan Summary**

| **Severity** | **Number of Vulnerabilities Identified** |
| --- | --- |
| Critical | 1 |
| High | 3 |
| Medium | 4 |
| Low | 4 |
| **Total** | **12** |

**4. Top Critical and High Issues**

**Issue 1: Microsoft SMBv1 Enabled**

* **Severity:** Critical
* **CVE ID:** CVE-2017-0144
* **Description:** The Server Message Block version 1 (SMBv1) is enabled. It is vulnerable to exploits such as EternalBlue.
* **Solution:** Disable SMBv1 in Windows Features and update Windows to the latest security patches.

**Issue 2: Outdated Adobe Acrobat Version**

* **Severity:** High
* **CVE ID:** CVE-2022-24082
* **Description:** Adobe Acrobat installed is outdated and contains multiple vulnerabilities.
* **Solution:** Update Adobe Acrobat Reader to the latest secure version from the official website.

**Issue 3: SSH Weak Algorithms Supported**

* **Severity:** High
* **CVE ID:** N/A
* **Description:** The SSH server is configured to support weak algorithms that are considered insecure.
* **Solution:** Update the sshd\_config file to remove weak algorithms.

**5. Recommendations**

✅ Regularly update all installed software and operating system.  
✅ Disable unused services and protocols to reduce attack surface.  
✅ Periodically run vulnerability scans to maintain security compliance.

**6. Attachments**

📎 **[Attached PDF Report]**: [VULNERABILITY SCAN REPORT.pdf](file:///C:\Users\Admin\Documents\VULNERABILITY%20SCAN%20REPORT.pdf)

**7. Conclusion**

The scan identified **12 vulnerabilities**, including **1 critical** issue. Immediate remediation steps should be taken for critical and high vulnerabilities to ensure the security of the system and prevent exploitation.