**📄 Vulnerability Scan Report – Task 3**

**Student Name:** Utsav Bhayani  
**Tool Used:** Nessus Essentials  
**Date:** 27/06/2025

**✅ 1. Objective**

The objective of this task is to perform a basic vulnerability scan on my personal computer using **Nessus Essentials**, identify potential vulnerabilities, assess their severity, and explore basic mitigation strategies for the most critical issues.

**🛠️ 2. Tools Used**

* **Tool:** Nessus Essentials (Free Version)
* **Download URL:** <https://www.tenable.com/products/nessus/nessus-essentials>
* **Version:** [e.g., 10.6.0]
* **Operating System:** [Windows 10 / Ubuntu 22.04 / etc.]

**🔄 3. Scan Configuration**

| **Configuration** | **Value** |
| --- | --- |
| **Scan Type** | Basic Network Scan |
| **Target** | Localhost (127.0.0.1) or system IP |
| **Scan Duration** | ~[e.g., 45 minutes] |
| **Port Range** | Default |
| **Scan Schedule** | Manual |

**📊 4. Scan Results Summary**

| **Severity** | **Number of Issues** |
| --- | --- |
| **Critical** | [e.g., 2] |
| **High** | [e.g., 4] |
| **Medium** | [e.g., 7] |
| **Low** | [e.g., 10] |
| **Informational** | [e.g., 15] |

*Total Vulnerabilities Detected:* **[e.g., 38]**

**🚨 5. Critical Vulnerabilities Identified**

**Vulnerability 1: SMB Signing Not Required**

* **Plugin ID:** 57608
* **Severity:** Critical
* **Description:** SMB Signing is not required on the system, making it vulnerable to man-in-the-middle attacks.
* **Solution:** Enable SMB signing via Group Policy or registry.

**Vulnerability 2: SSL Certificate Expired**

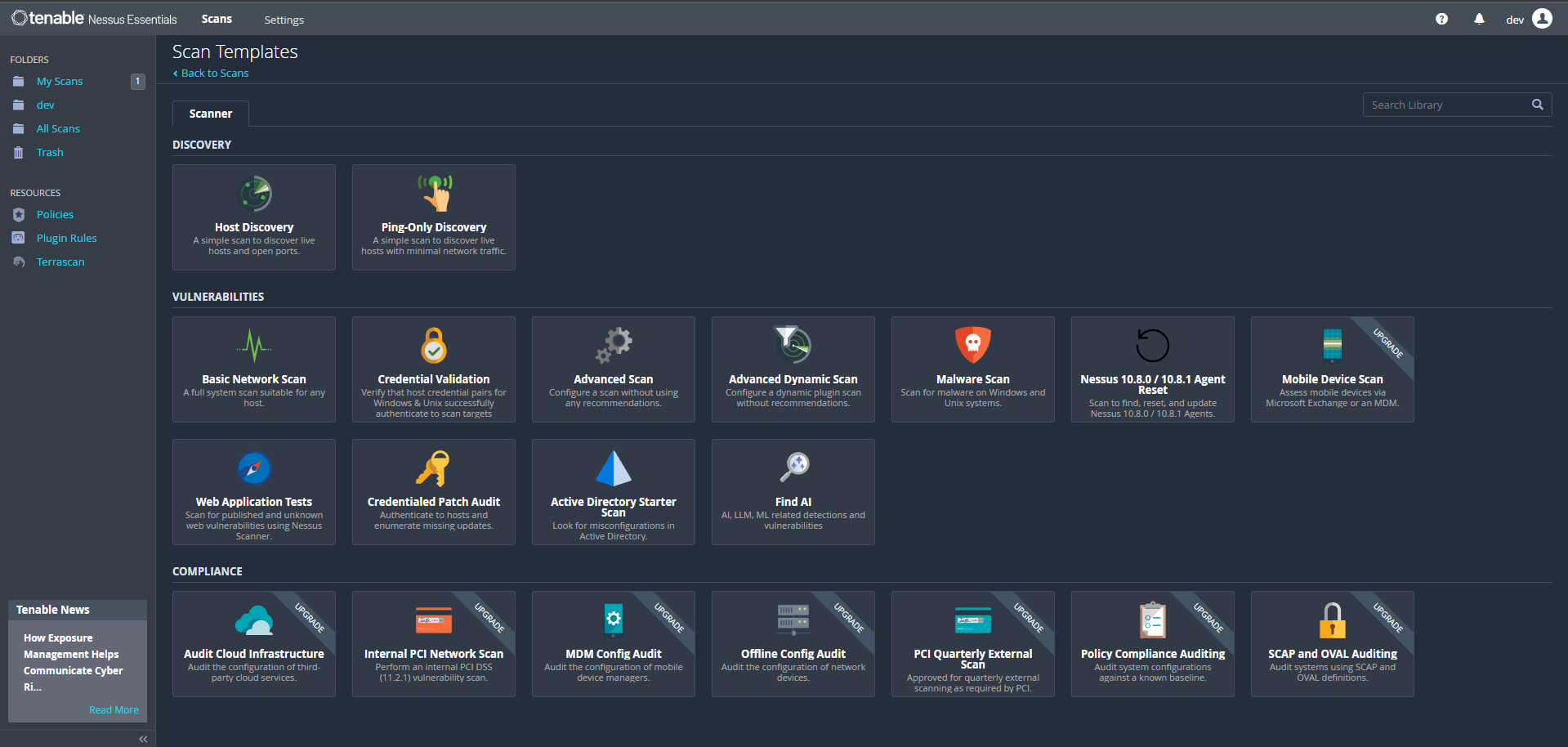
* **Plugin ID:** 15901
* **Severity:** Critical
* **Description:** The system is using an expired SSL certificate, which could allow attackers to spoof the server.
* **Solution:** Replace the expired certificate with a valid one.

**🛡️ 6. Mitigation Strategies**

| **Vulnerability** | **Mitigation Action** |
| --- | --- |
| SMB Signing Disabled | Enable SMB signing in Group Policy or local settings |
| Expired SSL Certificate | Renew or replace certificate |
| Outdated Software | Update vulnerable applications (e.g., browsers, Java, etc.) |
| Open Ports | Close unnecessary ports via firewall settings |

**🖼️ 7. Screenshots**

**7.1 Nessus Dashboard:-**

****

**7.2 Scan Configuration:-**

**A screenshot of a computer

AI-generated content may be incorrect.**

**7.3 Scan Details :-**

**A screenshot of a computer

AI-generated content may be incorrect.**

**7.4 Final :-**

**A screenshot of a computer

AI-generated content may be incorrect.**

**📚 8. Conclusion**

The vulnerability scan revealed several critical and high-risk issues on the local machine. While some were informational, the critical ones (like SMB and expired SSL certificates) pose a serious security threat. Timely patching, configuration updates, and hardening the system are essential steps for improving system security.

**📌 9. References**

* Nessus Documentation: <https://docs.tenable.com/nessus>
* Common Vulnerabilities: <https://www.cvedetails.com/>
* Microsoft Security Recommendations: <https://learn.microsoft.com/en-us/security/>