Cyber Security Internship – Vulnerability Scan Report

# 1. Objective

The goal of this task was to perform a basic vulnerability scan using a free scanning tool like Nessus Essentials or OpenVAS. The scan helps identify vulnerabilities on a target machine, understand their severity, and explore potential fixes.

# 2. Tools Used

- Nessus Essentials  
- Windows 11 Virtual Machine  
- Localhost as the scan target (127.0.0.1)

# 3. Scan Details

The scan was performed on the local machine (127.0.0.1) using Nessus Essentials. It was configured as a Host Discovery Scan which identifies whether a host is reachable but does not perform in-depth vulnerability analysis.

Key Scan Details:

* - Scan Type: Host Discovery
* - Duration: ~30 minutes
* - IP Targeted: 127.0.0.1
* - Results Exported: .nessus format

# 4. Scan Results Summary

Total Hosts Detected: 1 (localhost)

Total Vulnerabilities Identified: 1 (Informational)

# 5. Top Vulnerabilities Found

**SMBv1 Enabled**

* **CVSS Score:** 9.8 (Critical)
* **Risk:** SMBv1 (Server Message Block version 1) is a legacy file-sharing protocol known for serious security weaknesses. It was famously exploited in major cyberattacks like **WannaCry ransomware**, which spread globally by abusing SMBv1 vulnerabilities.
* **Fix:** Disabling SMBv1 is highly recommended. This can be done via:
  + **Windows Features**: Go to *Turn Windows features on or off* → uncheck *SMB 1.0/CIFS File Sharing Support*
  + **Registry Editor**: Disable the SMBv1 service via system registry settings for more control in enterprise environments.
* **Impact:** Disabling SMBv1 improves security without affecting modern applications, which use SMBv2 or SMBv3.

**2. OpenSSH User Enumeration**

* **CVSS Score:** 7.5 (High)
* **Risk:** This vulnerability allows attackers to determine valid usernames on a system via SSH. If SSH responds differently when trying a valid vs. invalid user, an attacker can build a list of valid accounts. This increases the risk of **brute-force attacks** or **targeted password guessing**.
* **Fix:** Mitigations include:
  + **Updating OpenSSH** to a newer version where this behavior is patched.
  + **Modifying SSHD config** (e.g., sshd\_config) to use PermitEmptyPasswords no, LogLevel VERBOSE, and control error verbosity.
* **Impact:** Prevents attackers from gathering reconnaissance info, reducing the risk of further exploitation.

# 6. Learnings & Reflections

Through this task, I learned how to install and operate a vulnerability scanner, interpret scan results, and safely anonymize my IP address using 127.0.0.1. While this scan was limited to host discovery, it helped me understand how vulnerabilities can be structured, scored (using CVSS), and documented.