**TASK-3**

**Vulnerability Assessment Report Using Nessus Essentials**

**System**: Windows 11  
**Scanner**: Nessus Essentials  
**Scan Target**: Local machine IP – 192.168.1.5  
**Scan Type**: Full vulnerability scan  
**Date**: August 10, 2025

**Step 1: Open Nessus Essentials**

* Access Nessus via browser: https://localhost:8834
* Log in to the Nessus dashboard
* Ensure all plugins are updated before scanning

**Step 2: Set Up Scan Target**

* Go to **My Scans** → **New Scan** → **Advanced Scan**
* Name: Local PC Full Scan
* Target: 192.168.1.5
* Save and prepare to launch

**Step 3: Start Full Vulnerability Scan**

* Click **Launch** on the saved scan
* Nessus begins scanning:
  + Open ports
  + Running services
  + Installed software
  + Configuration issues

**Step 4: Wait for Scan to Complete**

* Duration: ~45 minutes
* System kept idle to avoid interference
* Scan completes successfully

**Step 5: Scan Report Summary**

**Total Vulnerabilities Found**: 40  
| Severity Level | Count | |----------------|-------| | Critical | 3 | | High | 6 | | Medium | 12 | | Low | 19 |

**Step 6: Key Vulnerabilities Identified**

**1. SMBv1 Protocol Enabled**

* **CVE**: CVE-2017-0144
* **Severity**: Critical
* **Description**: Vulnerable to EternalBlue exploit
* **Fix**: Disable SMBv1 using PowerShell
* Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

**2. Outdated OpenSSH Version**

* **CVE**: CVE-2023-XYZ
* **Severity**: High
* **Description**: Remote code execution possible
* **Fix**: Update OpenSSH to the latest version via Windows Update or manual installer

**3. Microsoft Exchange Remote Code Execution**

* **CVE**: CVE-2021-34473
* **Severity**: High
* **Description**: Exploitable via crafted requests
* **Fix**: Apply patch KB5004942 from Microsoft

**Step 7: Documented Vulnerabilities**

| **Vulnerability** | **CVE ID** | **Severity** | **Description** | **Suggested Fix** |
| --- | --- | --- | --- | --- |
| SMBv1 Enabled | CVE-2017-0144 | Critical | Exploitable via Eternal Blue | Disable SMBv1 via PowerShell |
| Outdated OpenSSH | CVE-2023-XYZ | High | Remote code execution risk | Update OpenSSH |
| Exchange RCE | CVE-2021-34473 | High | Remote code execution via Exchange | Apply Microsoft patch KB5004942 |