Task 3

Task 3 – Perform vulnerability scan on your PC

Objective: Use free tools to identify common vulnerability on your computer

1. Download & Install Nessus Essentials:

* Downloaded from <https://www.tenable.com/products/nessus/nessus-essentials>
* Installed in Kali Linux on virtualbox
* Registered for a **free activation code** (valid for 16 IPs per scan, 120 IPs/week limit)
* Command to start Nessus in kali linux

Sudo service nessusd start

* Accessed the Nessus web interface at: <https://localhost:8834/>

2. Configure a New Vulnerability Scan:

* Select New scan 🡪 click Advance vulnerability Scan
* Enter the name of the scan, description and target IP (Local Host IP)
* The scan will take 20 -30 min
* After the scan completed click the name of the scan, there we find the detail report of the vulnerability report.

3. Executive summary:

* The Nessus scan detected **18 vulnerabilities** on the Windows 11 host (Local IP)
* 1 Medium-risk vulnerability (SMB Signing not required)
* 17 Informational findings (mostly SMB and OS detection)
* No Critical or High vulnerabilities were found, indicating relatively good security hygiene.

4. Detailed Vulnerability Breakdown

* Medium-Risk Vulnerability
* SMB signing Not Required (Plugin ID:57608)
* CVSS Score: 5.3(Medium)
* Risk:
* Attackers could perform man-in-the-middle (MITM) attacks on SMB traffic.
* Could lead to session hijacking or data tampering.
* Key Information Finding
* Most findings relate to SMB protocol detection and OS fingerprinting, which are not direct threats but reveal system information to attackers:

|  |  |  |
| --- | --- | --- |
| Plugin ID | Finding | Implication |
| 45590 | Common Platform Enumeration (CPE) | Lists installed software versions |
| 10736 | DCE Services Enumeration | Detects RPC services |
| 100871 | SMB Versions Supported | Shows SMBv1/v2/v3 status |
| 106716 | SMB2/SMB3 Dialects | Confirms SMB protocol support |
| 42410 | NTLMSSP Authentication Disclosure | Reveals NetBIOS info |
| 10785 | SMB NativeLanManager Disclosure | Exposes Windows version |