Task 3: Perform a Basic Vulnerability Scan on Your PC

Objective: Use free tools to identify common vulnerabilities on your computer.

Tools: Nessus Essentials and Metasploitable2 as the vulnerable target.

Deliverables: Vulnerability scan report with identified issues.

Steps Followed:

1. Installed Nessus Essentials on Kali Linux.
2. Configured the scan with Metasploitable2's IP as the target (192.168.1.3).
3. Started a full vulnerability scan using Nessus.
4. Waited for the scan to complete (approximately 20–30 minutes).
5. Reviewed the vulnerability report generated by Nessus Essentials.
6. Researched suggested fixes for the top vulnerabilities.
7. Documented the most critical vulnerabilities in the report.
8. Captured screenshots and exported the final report in PDF format.

Scan Summary:

Target: Metasploitable2 (192.168.1.3)
Total Vulnerabilities: 121
Severity: 8 Critical, 6 High, 21 Medium, 8 Low, 78 Informational

Top 3 Critical Vulnerabilities:

1. Apache Tomcat AJP Connector Request Injection (Ghostcat)
- Severity: Critical (CVSS 9.8)
- Description: Allows attackers to read/include files via AJP connector.
- Fix: Upgrade Tomcat or disable AJP connector.

2. Bind Shell Backdoor Detection
- Severity: Critical (CVSS 9.8)
- Description: Detects a backdoor that could allow remote command execution.
- Fix: Remove unauthorized services and re-secure the host.

3. SSL Version 2 and 3 Protocol Detection
- Severity: Critical (CVSS 9.8)
- Description: Outdated SSL protocols make the system vulnerable to known attacks.
- Fix: Disable SSLv2 and SSLv3, and enforce TLS 1.2+.