Task 3 – Basic Vulnerability Scan Report

Objective: Use free tools (OpenVAS/Nessus Essentials) to identify common vulnerabilities on the computer.

Tools Used:

- OpenVAS / Nessus Essentials (vulnerability scanner)
- Web browser (for research & fixing guidance)

Steps Followed:

- Installed and configured OpenVAS / Nessus Essentials (or used trial).
- Set up scan target: local machine IP (e.g., 127.0.0.1 or 192.168.1.5).
- Started a full vulnerability scan and waited for completion (30-60 mins typical).
- Reviewed the report, prioritized by severity (Critical, High, Medium, Low).
- Researched simple fixes for identified vulnerabilities.
- Documented the most critical findings and mitigation steps.
- Took screenshots of scan results (add to screenshots/ folder for repo).

Identified Vulnerabilities (Sample)

Severity	Vulnerability	Description	Suggested Fix
Critical	Default/Weak Credentials	Services using default or weak passwords (e.g., admin:admin).	Change default passwor
High	Outdated OpenSSH (CVE-XXXX-YYYY)	Unpatched SSH server with known remote code execution flaw.	Update OpenSSH to lates
High	SMBv1 Enabled	Old SMB protocol vulnerable to wormable exploits (e.g., WannaCry).	Disable SMBv1; enable S
Medium	Missing Security Updates	OS or installed apps missing recent security patches.	Run system updates and
Low	Weak TLS Configuration	Uses TLS 1.0/1.1 and weak ciphers.	Configure server to use T

Prioritization & CVSS

Use CVSS scores to prioritize remediation. Fix 'Critical' and 'High' issues first. Validate fixes by re-scanning after remediation.

General Recommendations

- Perform full system backups before major changes.
- Apply OS and application security updates promptly.
- Remove or disable unnecessary services and software.
- Harden configurations (disable legacy protocols like SMBv1, SSLv3).
- Use strong, unique passwords and enable multi-factor authentication.
- Schedule recurring vulnerability scans and monitor logs.
- Re-scan after fixes to confirm remediation.

Interview Questions & Answers

Q: What is vulnerability scanning?
A: Automated process of discovering known security weaknesses in systems or applications.

Q: Difference between vulnerability scanning and penetration testing?
A: Scanning is automated discovery; penetration testing attempts to exploit vulnerabilities manually for proof-of-concept.

Q: What are common vulnerabilities in personal computers?
A: Outdated software, weak passwords, open services, missing patches, and insecure configurations.

Q: How do scanners detect vulnerabilities?
A: By matching service versions and configurations against vulnerability databases (e.g., CVE/NVD).

Q: What is CVSS?
A: Common Vulnerability Scoring System — numeric scoring to indicate severity (0.0 to 10.0).

Q: How often should vulnerability scans be performed?
A: At minimum monthly for critical systems; weekly or daily for high-risk networks.

Q: What is a false positive?
A: A reported vulnerability that is not actually exploitable in the scanned environment.

Q: How to prioritize vulnerabilities?
A: By severity (CVSS), exploitability, and business impact; focus on Critical/High first.