**TASK 3**

**INTERVIEW QUESTION**

**1. What is vulnerability scanning?**

Vulnerability scanning is an automated process of identifying security weaknesses or misconfigurations in systems, networks, or applications using tools like Nessus or OpenVAS.

**2. Difference between vulnerability scanning and penetration testing**

Vulnerability scanning detects and lists known security flaws automatically, while penetration testing manually exploits vulnerabilities to assess real-world impact.

**3. What are some common vulnerabilities in personal computers?**

Common vulnerabilities include weak passwords, outdated software, missing patches, open ports, malware infections, and unprotected Wi-Fi connections.

**4. How do scanners detect vulnerabilities?**

Scanners identify system details, compare them with known vulnerability databases, test configurations, and simulate attacks to find weaknesses.

**5. What is CVSS?**

CVSS (Common Vulnerability Scoring System) is a standard method to rate vulnerability severity on a scale from 0 to 10, helping prioritize fixes.

**6. How often should vulnerability scans be performed?**

Scans should be done regularly—typically monthly or quarterly—and after major updates, configuration changes, or security incidents.

**7. What is a false positive in vulnerability scanning?**

A false positive occurs when a scanner reports a vulnerability that doesn’t actually exist due to incorrect detection or outdated data.

**8. How do you prioritize vulnerabilities?**

Prioritize based on CVSS score, exploit availability, system importance, exposure level, and potential business impact—fix critical ones first.