**Interview Questions**

**1. What is vulnerability scanning?**

Vulnerability scanning is an automated process of identifying security weaknesses in systems, networks, or applications. It helps detect missing patches, misconfigurations, and known vulnerabilities that attackers might exploit.

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

* Vulnerability Scanning: Automated, broad detection of known weaknesses. Focuses on finding vulnerabilities.
* Penetration Testing: Manual or semi-automated, simulates real attacks to exploit vulnerabilities and measure impact.

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

* Weak or reused passwords
* Missing security patches/updates
* Unsecured Wi-Fi configurations
* Outdated antivirus or firewall disabled
* Phishing or malware infections

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

Scanners use a vulnerability database (e.g., CVE) to check system configurations, open ports, services, and software versions. They compare this data with known weaknesses and report possible vulnerabilities.

**5. What is CVSS?**

CVSS (Common Vulnerability Scoring System) is a standardized method for rating the severity of security vulnerabilities, usually on a scale from 0 (low) to 10 (critical).

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

Vulnerability scans should be performed regularly—at least monthly or quarterly—and after major system changes (e.g., new software deployment, patching, or configuration changes).

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

A false positive occurs when a scanner reports a vulnerability that does not actually exist. It can waste time and resources if not validated.

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

Vulnerabilities are prioritized based on:

* Severity score (CVSS rating)
* Exploitability (is there a known exploit?)
* Asset criticality (how important the system is)
* Business impact (data sensitivity, availability needs)