1. What is vulnerability scanning?

Vulnerability scanning is the automated process of identifying security weaknesses in computer systems, networks, or applications. It helps detect known vulnerabilities that attackers might exploit.

2. Difference between vulnerability scanning and penetration testing?

Vulnerability scanning is automated and focuses on identifying known vulnerabilities, while penetration testing is manual or semi-automated and involves exploiting vulnerabilities to assess the system's defenses.

3. What are some common vulnerabilities in personal computers?

Common vulnerabilities include unpatched software, weak passwords, outdated operating systems, open ports, misconfigured security settings, and the presence of malware or spyware.

4. How do scanners detect vulnerabilities?

Scanners detect vulnerabilities by comparing system information with databases of known issues, analyzing configurations, and checking for missing patches, weak settings, or insecure software versions.

5. What is CVSS?

CVSS (Common Vulnerability Scoring System) is a standardized framework used to rate the severity of security vulnerabilities. It provides a numerical score (0.0 to 10.0) based on exploitability, impact, and other factors.

6. How often should vulnerability scans be performed?

Vulnerability scans should be conducted regularly, such as monthly or quarterly, and also after significant changes like system upgrades or new deployments. Critical systems may require more frequent scanning.

7. What is a false positive in vulnerability scanning?

A false positive occurs when a scanner reports a vulnerability that does not actually exist or is not exploitable in the current environment. It can result from misconfigurations or overly broad detection signatures.

8. How do you prioritize vulnerabilities?

Vulnerabilities are prioritized based on severity (CVSS score), asset value, exploitability, and exposure. High-risk and easily exploitable issues on critical systems should be addressed first.