1. What is vulnerability scanning?

Vulnerability scanning is the process of automatically checking systems and networks for

security weaknesses that could be exploited by attackers.

2. Difference between vulnerability scanning and penetration testing?

Vulnerability scanning identifies potential weaknesses, while penetration testing actively

exploits them to evaluate the real-world impact of vulnerabilities.

3. What are some common vulnerabilities in personal computers?

Common vulnerabilities include outdated software, weak passwords, missing security

patches, open ports, and misconfigured firewalls.

4. How do scanners detect vulnerabilities?

Scanners compare system data against known vulnerability databases and check

configurations, software versions, and open ports for security flaws.

5. What is CVSS?

CVSS (Common Vulnerability Scoring System) is a standardized method to rate the severity

of security vulnerabilities on a scale from 0 to 10.

6. How often should vulnerability scans be performed?

Vulnerability scans should be performed regularly—at least monthly or after major

updates—to ensure new threats or misconfigurations are detected early.

7. What is a false positive in vulnerability scanning?

A false positive occurs when a scanner incorrectly flags something as a vulnerability even

though it poses no real security risk.

8. How do you prioritize vulnerabilities?

Vulnerabilities are prioritized based on severity scores (like CVSS), exploit availability,

potential business impact, and ease of remediation.