1. What is vulnerability scanning?
   Ans: Vulnerability scanning identifies potential security flaws in systems, networks, or applications using automated tools that could be exploited by attackers.

2. Difference between vulnerability scanning and penetration testing.
   Ans: Vulnerability scanning identifies potential overview of potential weaknesses, whereas penetration testing simulates real-world attacks to exploit those vulnerabilities.

3. What are some common vulnerabilities in personal computers?
   Ans: Common PC vulnerabilities include outdated software, weak passwords, misconfigurations, and malware infections.

4. How do scanners detect vulnerabilities?
   Ans: By comparing software versions, networks settings against known vulnerability databases.

5. What is CVSS?
   Ans: The Common Vulnerability Scoring System is a standardised framework that rates vulnerabilities based on their severity and potential impact and remediation level.

6. How often should vulnerability scans be performed?
   Ans: should be done quarterly, ideally after significant system changes or updates.

7. What is a false positive in vulnerability scanning?
   Ans: when a scanner flags an issue as a vulnerability when that doesn't exist—commonly due to incomplete information.

8. How do you prioritize vulnerabilities?
   Ans: based on the business risk, potential impact, and exploitability.