1. What is vulnerability scanning?

It's an automated process that scans a system, network, or application to find security weaknesses.
Think of it like a "health check-up" for computers — it identifies potential issues but doesn't exploit them.

2. Difference between vulnerability scanning and penetration testing?

Vulnerability Scanning	Penetration Testing
Automated	Mostly manual + tools
Finds weaknesses	Actively exploits weaknesses
Quick and routine	Deep, detailed, occasional
Broad coverage	Focused attack simulation
Low cost	Higher cost

3. What are some common vulnerabilities in personal computers?

Some usual suspects:

- **Outdated OS/software**
- **Weak passwords**
- **Unpatched browsers or plugins**
- **Disabled or outdated antivirus**
- **Open ports and unnecessary services running**
- **Malicious extensions or apps**
- **Misconfigured firewalls**

4. How do scanners detect vulnerabilities?

They use methods like:

- **Fingerprinting** (OS, services, versions)
- **Matching vs known CVE databases**
- **Port scanning**
- **Banner grabbing**
- **Config checks**
- **Simulated requests** (sometimes sending malformed packets to see reactions)

5. What is CVSS?

CVSS = Common Vulnerability Scoring System

It gives a standardized score (0–10) showing how severe a vulnerability is.
Example:

- **9.8 → Critical**
- **7.5 → High**

- **5.4 → Medium**
- **3.5 → Low**

6. How often should vulnerability scans be performed?

General recommendation:

- **Monthly** → For regular businesses
- **Weekly or daily** → For high-risk systems
- **After every major change** (new deployments, upgrades, patches)
- **After incidents**

7. What is a false positive in vulnerability scanning?

When the scanner reports a vulnerability, but it's actually **not real**.
Example: It says a port is vulnerable, but the patch is already applied.

False positives waste time, so verifying results is important.

8. How do you prioritize vulnerabilities?

Use these factors:

1. **CVSS score** (Critical first)
2. **Exploit availability** (Is there a working exploit?)
3. **Impact on business**
4. **Asset value** (Is the system important?)
5. **Exposure** (Internet-facing = fix ASAP)
6. **Dependencies** (Some fixes require other fixes first)

Many teams use a formula like:
Risk = Likelihood × Impact