Vulnerability Scanning Intervirew Questions_&_Answers

1. What is vulnerability scanning?

Vulnerability scanning is an **automated security assessment process** used to identify known weaknesses in systems, applications, and networks.
It involves using tools (like Nessus, OpenVAS, Qualys, or Nikto) to:

- Detect outdated software versions
- Identify missing security patches
- Spot misconfigurations
- Flag insecure services and ports
  The results are usually presented as a report containing vulnerabilities, severity levels, and remediation suggestions.
  Vulnerability scanning is typically **non-intrusive** and doesn't exploit vulnerabilities — it only detects them.

2. Difference between vulnerability scanning and penetration testing?

Feature	Vulnerability Scanning	Penetration Testing
Goal	Detect known security flaws	Actively exploit vulnerabilities
Approach	Automated scanning tools	Manual & automated exploitation
Output	List of vulnerabilities with severity	Detailed proof of concept, exploitation results, and security recommendations
Skill Requirement	Basic to intermediate	Advanced ethical hacking skills
Intrusiveness	Low (does not cause system damage)	Higher risk (can disrupt systems)
Frequency	Weekly, monthly, or per compliance needs	Once or twice a year, or after major system changes

3. What are some common vulnerabilities in personal computers?

- **Unpatched OS/software** – Leaving critical updates pending
- **Weak or reused passwords** – Easily guessed or cracked
- **Disabled antivirus/firewall** – Reduces defense against malware
- **Phishing susceptibility** – Falling for malicious email links/attachments
- **Default system settings** – Not hardened for security

- **Exposed services** – Open RDP, FTP, or SMB without security
- **Unencrypted storage** – Data readable if device is stolen

4. How do scanners detect vulnerabilities?
Vulnerability scanners identify weaknesses using multiple techniques:

- **Signature-based detection** – Matches software versions against a vulnerability database (e.g., NVD, CVE).
- **Banner grabbing** – Reads version and service banners from network services.
- **Heuristic analysis** – Uses patterns and rules to detect risky configurations.
- **Patch auditing** – Checks if installed software has the latest security patches.
- **Configuration auditing** – Compares system settings with security benchmarks (e.g., CIS Benchmarks).

5. What is CVSS?

The **Common Vulnerability Scoring System** is a standardized method for rating vulnerabilities from **0.0 to 10.0**:

- **0.0** – No risk
- **0.1–3.9** – Low severity
- **4.0–6.9** – Medium severity
- **7.0–8.9** – High severity
- **9.0–10.0** – Critical severity
  CVSS considers three main metric groups:
- **Base** – Intrinsic qualities of the vulnerability
- **Temporal** – Factors that change over time (e.g., exploit availability)
- **Environmental** – Impact on a specific organization's environment

6. How often should vulnerability scans be performed?
Best practices recommend:

- **Weekly/Bi-weekly** – Internet-facing systems
- **Monthly/Quarterly** – Internal systems and networks
- **Immediately after changes** – System upgrades, patching, or deployments
- **As per compliance** – E.g., PCI DSS requires quarterly scans by an Approved Scanning Vendor (ASV)

Frequent scanning reduces the window of exposure for newly discovered vulnerabilities.

7. What is a false positive in vulnerability scanning?
A **false positive** is when a scanner incorrectly flags a vulnerability that doesn't exist. Causes include:

- Outdated vulnerability definitions
- Misinterpretation of system responses
- Inaccurate fingerprinting of OS/software versions
  Handling false positives involves **manual verification** and adjusting scan configurations.

8. How do you prioritize vulnerabilities?
Prioritization ensures critical threats are addressed first:

1. **Severity Level** – Fix Critical and High vulnerabilities first (CVSS 7.0+).
2. **Exploit Availability** – Address vulnerabilities with public or active exploits immediately.
3. **Business Impact** – Focus on systems affecting critical operations.
4. **Attack Surface** – Internet-facing and publicly accessible systems take priority.
5. **Regulatory Compliance** – Fix vulnerabilities that could lead to non-compliance penalties.