Interview Questions and Answers—Task 3: Basic Vulnerability Scan

---

1. What is vulnerability scanning?

Vulnerability scanning is an automated process of identifying potential security weaknesses, misconfigurations, and outdated software in systems or networks.
Tools like **OpenVAS** or **Nessus** perform scans by comparing detected system information against a database of known vulnerabilities to assess the system's exposure level.

---

2. Difference between vulnerability scanning and penetration testing

Aspect	Vulnerability Scanning	Penetration Testing
Purpose	Detect potential weaknesses automatically	Exploit vulnerabilities to assess real-world impact
Method	Automated scanning and reporting	Manual or semi-automated exploitation
Depth	Broad but shallow	Deep and targeted
Tools Used	OpenVAS, Nessus, Qualys	Metasploit, Burp Suite, Cobalt Strike
Frequency	Regular and recurring	Periodically or before major system changes

In short, **vulnerability scanning finds issues**, while **penetration testing confirms and exploits them**.

---

3. What are some common vulnerabilities in personal computers?

Common vulnerabilities in personal computers include:

- Outdated operating system or unpatched software
- Weak or reused passwords
- Enabled but unnecessary services (e.g., SMBv1, RDP)
- Misconfigured firewalls or open ports
- Outdated antivirus definitions
- Insecure browser extensions or plugins
- Missing OS or driver updates

---

4. How do scanners detect vulnerabilities?

Vulnerability scanners like OpenVAS detect vulnerabilities by:

1. **Fingerprinting the target system** (identifying OS, services, and versions).
2. **Comparing gathered data** with known vulnerability databases (like CVE, NVT, or CPE entries).
3. **Testing configurations** (e.g., weak SSL/TLS settings, missing patches).
4. **Reporting findings** with severity levels and recommended remediations.

This process is **non-intrusive**, ensuring that no harm is done to the target system during scanning.

---

5. What is CVSS?

CVSS (Common Vulnerability Scoring System) is a standardized framework used to rate the severity of vulnerabilities.
It assigns scores from **0.0 to 10.0**, with higher scores indicating greater risk.
CVSS considers factors such as

- **Exploitability** (ease of attack)
- **Impact** (on confidentiality, integrity, and availability)
- **Scope and user interaction requirements**

Example:

- 9.0–10.0 → Critical
- 7.0–8.9 → High
- 4.0–6.9 → Medium
- 0.1–3.9 → Low

---

6. How often should vulnerability scans be performed?

Vulnerability scans should be performed **regularly**, typically:

- **Monthly or quarterly** for personal or small business systems.
- **Weekly or continuous** for enterprise environments with dynamic infrastructures.
  Additionally, scans should be performed:
- After major **system updates or patches**,
- Following **network or software changes**, or
- When **new vulnerabilities (CVEs)** are disclosed.

Regular scanning ensures ongoing awareness of security posture and helps prevent unpatched weaknesses.

---

7. What is a false positive in vulnerability scanning?

A **false positive** occurs when a scanner incorrectly identifies a vulnerability that doesn't actually exist.
This can happen due to:

- Incorrect banner or version detection
- Outdated vulnerability databases
- Misconfigured scan policies

Effective mitigation involves **manual verification**, **cross-checking with system data**, or performing a **re-scan with updated definitions**.

---

8. How do you prioritize vulnerabilities?

Vulnerabilities are prioritized based on a combination of:

1. **CVSS Score**—Severity level (Critical > High > Medium > Low).
2. **Exploit Availability**—Whether public exploits exist.
3. **Asset Criticality**—Importance of the affected system or data.
4. **Exposure Level**—Internal vs. external accessibility.
5. **Business Impact**—Potential operational or financial damage.

Typically, **critical and high** vulnerabilities are addressed immediately, while **medium and low** are scheduled for later remediation or monitored.