If you’re preparing for a **Vulnerability Assessment and Penetration Testing (VAPT)** role as a fresher, you should focus on networking, security concepts, tools, and hands-on testing methodologies. Below are some commonly asked **VAPT interview questions and answers** for freshers:

Basic VAPT Questions

1. What is the difference between Vulnerability Assessment (VA) and Penetration Testing (PT)?

Answer:

- **Vulnerability Assessment (VA):** Identifies security weaknesses in a system, network, or application without exploiting them. It is more focused on detecting known vulnerabilities using automated tools.
- **Penetration Testing (PT):** Actively attempts to exploit vulnerabilities to assess the security impact. It is a simulated cyberattack that evaluates the system’s ability to withstand threats.

---

2. What are the different types of penetration testing?

Answer:

- **Black Box Testing:** No prior knowledge of the target system. Simulates a real-world attacker.
- **White Box Testing:** Full knowledge of the system, including source code and network details.
- **Gray Box Testing:** Partial knowledge of the system, simulating an insider threat or a hacker with some access.

---

3. What are the key phases of penetration testing?

Answer:

1. **Planning & Reconnaissance** – Gathering information about the target.
2. **Scanning** – Identifying live hosts, open ports, and vulnerabilities.
3. **Exploitation** – Attempting to exploit discovered vulnerabilities.
4. **Post-Exploitation** – Assessing the impact and maintaining access.
5. **Reporting** – Documenting findings and recommending fixes.

---

4. What tools are commonly used in VAPT?

Answer:

- **Vulnerability Scanning:** Nessus, OpenVAS, Qualys
- **Network Scanning:** Nmap, Netcat
- **Exploitation:** Metasploit, SQLmap
- **Web Security:** Burp Suite, OWASP ZAP
- **Wireless Testing:** Aircrack-ng
- **Password Cracking:** John the Ripper, Hashcat

---

5. What is an OWASP Top 10 vulnerability?

Answer:
OWASP (Open Web Application Security Project) identifies the top 10 most critical web security risks. Some common vulnerabilities include:

1. **Injection (SQL, Command, etc.)**
2. **Broken Authentication**
3. **Sensitive Data Exposure**
4. **XML External Entities (XXE)**
5. **Broken Access Control**
6. **Security Misconfiguration**
7. **Cross-Site Scripting (XSS)**
8. **Insecure Deserialization**
9. **Using Components with Known Vulnerabilities**
10. **Insufficient Logging & Monitoring**

Technical VAPT Questions

6. What is the difference between SQL Injection and XSS?

Answer:

- **SQL Injection (SQLi):** Injects malicious SQL queries to manipulate the database.
- **Cross-Site Scripting (XSS):** Injects malicious scripts (JavaScript) into a web page to steal cookies, sessions, or perform unauthorized actions on behalf of a user.

---

7. How would you test for SQL Injection?

Answer:

- Use special characters like **' OR 1=1--**, **" OR "1"="1** in input fields.
- Use SQLmap to automate SQL injection testing.
- Observe error messages, unexpected database responses, or authentication bypass.

---

8. What is Privilege Escalation? How does it work?

Answer:
Privilege escalation is the process of gaining higher-level permissions on a system.

- **Vertical Escalation:** Gaining admin/root access from a lower-privileged user.
- **Horizontal Escalation:** Gaining access to another user's account.
- Exploitation techniques: Kernel exploits, misconfigured SUID files, weak credentials.

---

9. What is the difference between IDS and IPS?

Answer:

- **Intrusion Detection System (IDS):** Monitors network traffic and alerts administrators of suspicious activity but does not block attacks.
- **Intrusion Prevention System (IPS):** Monitors and actively blocks malicious traffic.

---

10. What are some common web application security headers?

Answer:

- **Content Security Policy (CSP)** – Prevents XSS by restricting script sources.
- **X-Frame-Options** – Prevents clickjacking attacks.
- **X-XSS-Protection** – Mitigates reflected XSS attacks.
- **Strict-Transport-Security (HSTS)** – Enforces HTTPS connections.

Scenario-Based Questions

11. A client’s web application is vulnerable to XSS. How would you mitigate it?

Answer:

- **Input Validation:** Restrict user input to allow only expected characters.
- **Output Encoding:** Encode user input before rendering it in HTML (e.g., `&lt;` for `<`).
- **Content Security Policy (CSP):** Block inline scripts and allow only trusted sources.
- **Use Secure Cookies & HTTPOnly flag:** Prevent script access to cookies.

---

12. You ran a vulnerability scan and found outdated software with a known CVE. What do you do?

Answer:

1. **Check the CVE details** – Assess its severity and exploitability.
2. **Update the software** – Patch the vulnerability if a fix is available.
3. **Apply mitigations** – If patching isn’t possible, use WAF, access controls, or disable vulnerable features.
4. **Document and report** – Provide a risk assessment to the client.

---

13. A company suspects a data breach. How would you investigate?

Answer:

- **Check logs** – Look for unusual login attempts or data transfers.
- **Scan for malware** – Identify potential backdoors.
- **Isolate compromised systems** – Prevent further data leakage.
- **Conduct forensics** – Extract evidence from memory, logs, and disk images.
- **Report findings** – Document and recommend security improvements.

HR Questions (General)

14. Why do you want to pursue a career in VAPT?

Answer:
"I am passionate about cybersecurity and ethical hacking. VAPT allows me to apply my analytical skills to identify and fix vulnerabilities before attackers exploit them. The constant learning and evolving nature of security keep me motivated."

---

15. Where do you see yourself in five years?

Answer:
"In five years, I aim to become a **Certified Penetration Tester** with expertise in **red teaming and cloud security assessments**. I also plan to contribute to open-source security projects and mentor aspiring security professionals."

Here are **more advanced VAPT interview questions and answers**, categorized into different topics.

Advanced VAPT Interview Questions and Answers

Network Security & Penetration Testing

1. What is ARP Spoofing? How can you prevent it?

Answer:
ARP Spoofing (or ARP Poisoning) is an attack where an attacker sends falsified ARP (Address Resolution Protocol) messages to associate their MAC address with the IP address of a legitimate device, such as a router. This allows the attacker to intercept, modify, or stop network traffic.

Prevention Measures:

- Use **Static ARP entries** to prevent unauthorized changes.
- Enable **ARP Spoofing Protection** in switches (Dynamic ARP Inspection).
- Use **encrypted communication (HTTPS, VPN)** to prevent data interception.

---

2. What is the difference between Active and Passive Reconnaissance?

Answer:

- **Active Reconnaissance:** Direct interaction with the target (e.g., scanning ports with Nmap, fingerprinting services). This can trigger security alerts.
- **Passive Reconnaissance:** Gathering information without directly interacting with the target (e.g., using WHOIS lookup, Google Dorking, OSINT tools like Maltego).

---

3. How do you check if a system is vulnerable to the EternalBlue exploit?

Answer:

- Use **Nmap NSE scripts**:

```
nmap --script smb-vuln-ms17-010 -p445 <target-ip>
```

- Use **Metasploit**:

```
use auxiliary/scanner/smb/smb_ms17_010
set RHOSTS <target-ip>
run
```

- If vulnerable, patch the system by installing **Microsoft Security Update MS17-010**.

---

4. How do you detect and prevent a Man-in-the-Middle (MitM) attack?

Answer:
Detection:

- Use **Wireshark** to analyze network traffic for anomalies.
- Run `arp -a` on Windows/Linux to check for duplicate ARP entries.
- Check for **SSL stripping** by monitoring HTTPS downgrade attempts.

Prevention:

- Use **SSL/TLS (HTTPS, SSH, VPN)** for encrypted communication.
- Implement **HSTS (HTTP Strict Transport Security)**.
- Enable **ARP Spoofing Protection** in network devices.

Web Application Security

5. How do you perform a Directory Bruteforce Attack?

Answer:
A directory brute-force attack finds hidden directories/files on a web server.

Using **Dirb**:

```
dirb http://example.com /usr/share/wordlists/dirb/common.txt
```

Using **Gobuster**:

```
gobuster dir -u http://example.com -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

Prevention:

- Disable directory listing.
- Use security headers like `X-Content-Type-Options: nosniff`.
- Implement **rate limiting and CAPTCHAs**.

---

6. What are the different types of Cross-Site Scripting (XSS)?

Answer:

- **Stored XSS:** Malicious script is permanently stored in the database and affects all users.
- **Reflected XSS:** Script is embedded in a URL and executed when a user clicks the link.
- **DOM-Based XSS:** JavaScript modifies the DOM, leading to script execution on the client-side.

Mitigation:

- Input validation and sanitization.
- Encode output using `htmlspecialchars()`.
- Implement **Content Security Policy (CSP)**.

---

7. How can you test for Server-Side Request Forgery (SSRF)?

Answer:
SSRF occurs when a server makes unintended HTTP requests.

Testing:

- Try payloads like:

  ```
  http://127.0.0.1/admin
  http://169.254.169.254/latest/meta-data/ # AWS metadata exposure
  ```

- Use Burp Suite to modify API request URLs.

Prevention:

- Restrict internal requests with a firewall.
- Validate and whitelist allowed URLs.
- Block private IP addresses (e.g., `10.0.0.0/8`, `192.168.0.0/16`).

Exploitation & Post-Exploitation

8. How would you escalate privileges on a Windows machine?

Answer:

- **Check for Misconfigured Services:**

```
sc qc <service-name>
```

- **Weak File Permissions on Executables:**

```
icacls C:\VulnerableApp.exe
```

- **Token Impersonation:** Using **mimikatz** to dump tokens.

Mitigation:

- Apply **least privilege principle**.
- Regularly update and patch systems.
- Disable unused services.

---

9. How do you maintain access after a successful exploitation?

Answer:

- **Backdoor Creation:** Add a new SSH key or user account.
- **Persistence Mechanisms:** Modify startup scripts (`.bashrc`, `cronjobs`, Windows Registry).
- **Covering Tracks:** Clear logs (`/var/log/auth.log`, Event Viewer).

Mitigation:

- Enable **system integrity monitoring** (OSSEC, Wazuh).
- Audit and review system logs frequently.
- Implement **file integrity checks**.

---

10. How do you crack a hashed password?

Answer:

1. **Check hash type** using `hashid`:

```
hashid <hash>
```

2. **Crack with Hashcat**:

```
hashcat -m 0 -a 0 hash.txt rockyou.txt
```

3. **Crack with John the Ripper**:

```
john --wordlist=rockyou.txt hash.txt
```

Prevention:

- Use **strong password hashing algorithms** (bcrypt, Argon2).
- Implement **multi-factor authentication (MFA)**.

Miscellaneous & Behavioral Questions

11. What is the difference between a Red Team, Blue Team, and Purple Team?

Answer:

- **Red Team:** Offensive security (ethical hackers simulate attacks).
- **Blue Team:** Defensive security (protects and monitors systems).
- **Purple Team:** A mix of both, ensuring security improvements through collaboration.

---

12. What are some common false positives in vulnerability scanning?

Answer:

- Misidentified services (e.g., OpenSSH flagged as outdated).
- HTTP headers triggering **false vulnerabilities**.
- Outdated libraries reported, but **unused in the application**.
- Debugging logs mistakenly considered as **information disclosure**.

---

13. How would you explain VAPT findings to a non-technical client?

Answer:

- Use **simple, non-technical terms**.
- Explain **real-world impact** (e.g., “This issue allows an attacker to steal user data”).
- Provide **actionable recommendations** instead of just listing vulnerabilities.
- Use **visuals or diagrams** to illustrate attack scenarios.

---

14. Why should we hire you for a VAPT role?

Answer:
"I have a **strong foundation in cybersecurity concepts** and hands-on experience in **penetration testing tools** like Nmap, Metasploit, and Burp Suite. I continuously improve my skills through **CTFs and security projects**. I am passionate about **identifying and fixing security flaws** to protect organizations from cyber threats."

Final Interview Tips

- **Show hands-on skills**: Mention **CTF challenges**, bug bounties, or labs like **Hack The Box, TryHackMe**.
- **Know basic Linux commands**: `netstat`, `tcpdump`, `iptables`, `whoami`, `uname -a`.
- **Stay updated**: Follow **CVE databases**, cybersecurity news, and OWASP updates.