Penetration Testing Interview Questions

Penetration Testing is an essential way of identifying, analyzing, and exploiting vulnerabilities in the system. It helps to identify the attack surfaces in the network and enhances the security posture of the organizations. This article is curated with the Penetration Testing interview question for those who want to crack the Pen-Tester interview.

1. What are the three primary approaches of Penetration Testing?

The three primary types of Penetration Testing methods are as follows:

- Black-Box Penetration Testing
- White-Box Penetration Testing
- Gray-Box Penetration Testing

2. What are the advantages of Penetration Testing?

The following are the significant advantages of Penetration Testing:

- Penetration Testing helps in identifying and prioritizing potential risks.

- It prevents attackers from exploiting the organization’s security posture.
- It helps to enhance the security posture.
- It assists an organization in identifying additional issues like bugs, technical glitches, viruses, etc.
- It abides by industry regulations and standards.

3. Define Cross-site scripting (XSS).

Cross-site scripting (XSS) is a malicious attack that exploits secure communication between users. It is a kind of injection in which malicious scripts are injected into trusted websites. As a result, the user is redirected to a malicious website, and data entered on the website can be accessed by the attackers leading to account compromise, privilege escalation, malware injection, etc.

4. What are the types of cross-site scripting?

The following are the types of cross-site scripting:

- Reflected XSS
- Stored XSS
- DOM-based XSS

5. List out the five stages of Penetration Testing.

The following are the five stages of Penetration Testing:

- Reconnaissance
- Scanning
- Vulnerability Assessment
- Exploitation
- Reporting

6. What are the types of Penetration Testing?

The types of Penetration Testing are as follows:

- Client-Side Application Testing
- Social Engineering Testing
- Mobile Application Testing

- Web Application Testing
- Wireless Penetration Testing
- Internal/External Infrastructure Penetration Testing

7. What is Vulnerability?

Vulnerability is a weakness or fault that creates an attack surface allowing attackers to exploit by achieving unauthorized access to the system. It can be exploited by various attacking methods such as SQL injection, Cross-site scripting (XSS), etc.

8. What is Data packet sniffing?

Data packet sniffing is a technique used to monitor and validate network traffic using algorithms. It also helps to identify unusual activities or unauthorized access to the network.

9. Define encryption and mention its types.

Encryption is a method of converting plaintext to cipher text using cryptography to encrypt the data. It ensures secure communication between both sender and recipient and maintains confidentiality. There are two types of encryptions:

- Symmetric Encryption
- Asymmetric Encryption

10. Define VAPT.

Vulnerability Assessment and Penetration Testing (VAPT) is a security assessment used to identify and address vulnerabilities in the organization’s network. The main aim of VAPT is to identify internal vulnerabilities and prevent external threats, and it helps to minimize the possibility of attackers achieving access to the system or network.

Penetration Testing with InfosecTrain

InfosecTrain is a well-known platform for IT security training and certification. Our certified and highly skilled trainers have designed specialized training courses for IT professionals meeting current industry trends and requirements. To become a Penetration Tester, you can enroll in the Pentester combo training course at InfosecTrain.