INFOSECTRAIN

Top Pen Tester Interview Q & A

that You Should Know

www.infosectrain.com
sales@infosectrain.com

Description

Pen testing is another name of penetration testing. It is a level of assessment used to assess the security of a system or web application. It is used to determine the faults or weaknesses of system features and is also valuable for obtaining the comprehensive details of a target system's risk assessment. It is a procedure that is part of a comprehensive system security audit.

If you seek a job in penetration testing, you should prepare for the Pen Tester interview. Each interview is indeed unique based on the job profile. We have compiled a list of the most relevant Pen Tester interview questions and answers to help you succeed in your interview.

1. Explain Penetration testing and why is it important?

A Cybersecurity Specialist aims to discover and exploit weaknesses in a computer system during penetration testing. A simulated attack aims to find any vulnerabilities in a system's defenses that attackers could exploit. Penetration testing involves Security Analysts attempting to access resources without knowing usernames, passwords, or other traditional methods of access. Only the authorization granted by the organization divides hackers from security specialists.

2. What are the Network Penetration Phases?

Penetration testing is divided into 5 phases:

Reconnaissance: It is the process of gathering information about the target. It can be done in either a passive or active manner. During this phase, you will discover more about the target business and how it operates.

Scanning: This is an important stage of penetration testing. During this step, scanning is performed to identify vulnerabilities in the network, as well as software and operating systems utilized by devices. As a result of this activity, the pen tester is familiar with services running, open ports, firewall identification, weaknesses, software platforms, and so on.

Gaining access: During this stage, the Pen Tester begins carrying out the attack by acquiring access to insecure devices and servers. This is made possible by the application of tools.

As a Pen Tester gets access to a vulnerable system, he or she attempts to retrieve as much data as possible while remaining covert.

Covering tracks: During this phase, the Pen Tester takes all required efforts to conceal the intrusion and any controls that may have been left behind for future interactions.

3. What is XSS, also known as Cross-Site Scripting?

Cross-Site Scripting (XSS) attacks are a sort of injection in which harmful tools are injected into trustworthy websites. When an attacker uses an online application to deliver the malicious script, usually in the form of a browser-side script, to a different user, XSS assault occurs.

4. What are the benefits and drawbacks of Linux and Windows?

Factors	Linux	Windows
Price	Available for free	Paid
Utilization Effort	Difficult for beginners	User-friendly
Reliability	More reliable and secure	Less reliable and secure
Software Installation	Both premium and free software are available for installation.	Both premium and free software are available for installation.
Hardware	Initially, hardware compatibility was a problem. However, the bulk of physical appliances now support Linux.	Windows has never had a problem with hardware compatibility.
Security	Operating System that is extremely safe	Because inexperienced users utilize this OS it is vulnerable to attackers
Support	Online community support is available to help with any problem	Microsoft support is available online, and there are numerous publications available to help you diagnose any problem

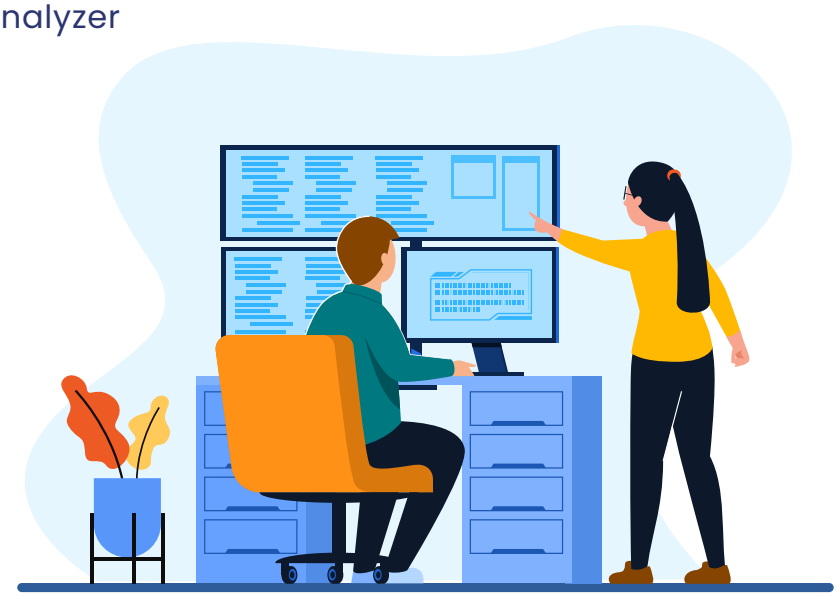
5. With the Diffie-Hellman key exchange, what type of penetration is possible?

Diffie–Hellman key exchange (DH), one of the original public-key protocols, securely exchanges cryptographic keys over a public channel. This protocol is commonly found in protocols such as IPSec and SSL/TLS. Receiving and sending devices in a network uses this protocol to generate a secret shared key that may be used to encrypt data.

6. What kinds of tools are available for packet sniffing?

Packet sniffing collects network traffic and sees traffic on a complete network or only a specific part of it. Here is the list of top packet Sniffing tools:

- Auvik
- SolarWinds Network Packet Sniffer
- Wireshark
- Paessler PRTG
- ManageEngine NetFlow Analyzer
- Tcpdump
- Windump
- NetworkMiner
- Colasoft Capsa
- Telerik Fiddler
- kismet



7. What exactly is intrusion detection?

Intrusion detection protects IT infrastructure from cyber attacks.
It detects security breaches from the outside as well as inside a network.
Intrusion detection is responsible for a wide range of tasks, including traffic monitoring and analysis, detecting attack patterns, verifying the integrity of data on servers, checking for policy violations, and so on.

8. Make a list of the elements that can lead to security flaws.

Vulnerabilities in security are caused by a variety of circumstances.
Here are a few examples:

- Weak passwords
- Input validation is not performed by the web application
- Sensitive information is stored in plain text
- The session ID does not modify it logging in
- Errors expose important infrastructure information
- The installed software has not been updated

9. List the advantages that an intrusion detection system can bring.

Here are some advantages to employing an Intrusion Detection System (IDS):

- Assists in the detection of security issues and Denial of Service attacks
- Examine the traffic for unusual and abstract behavior
- Detect cross-site scripting, SQL injection, and other types of threats
- To protect vulnerable assets, provide temporary updates for known vulnerabilities.

10. Define SQL injection?

It is an attack in which a person adds untrusted data into the program, resulting in the leakage of confidential database information.

11. How does SSL/TLS work?

While data is transmitted from source to destination, the SSL/TLS layer ensures confidentiality and integrity.

1. By typing the website address, the user initiates the connection. By delivering a message to the website's server, the browser establishes SSL/TLS communication.

2. The public key or certificate is returned to the user's browser by the website's server.

3. The browser of the user looks for a public key or a certificate. If everything is in order, it generates a symmetric key and returns it to the website's server. The communication fails if the certificate is invalid.

4. When the website's server receives the symmetric key, it delivers the key and encrypts the required data.

5. The SSL/TLS handshake completes when the user's browser decrypts the material with a symmetric key. The user can now access the content because the connection has been established.

12. What certifications are most in-demand for penetration testing?

There is no doubt that there is an infinite number of certifications available in the Cybersecurity area. However, if a Pen Tester wants to be acknowledged as the best in their area, the following certifications are indeed:

- CEH (Certified Ethical Hacker) certification
- Offensive Cyber Security certification
- CompTIA Pen Test+ certification
- Different Security Testing certification

13. What are the most commonly targeted ports during penetration testing?

For the port scan, you can use the Nmap tool. Following is a list of frequent ports to concentrate on during penetration testing:

- FTP (port 20, 21)
- SSH (port 22)
- Telnet (port 23)
- SMTP (port 25)
- HTTP (port 80)
- NTP (port 123)
- HTTPS (port 443)

14. Why should we execute a penetration test if we are currently undertaking vulnerability scanning?

In general, vulnerability scanning identifies flaws based on vulnerability signatures accessible in the scanning program. While penetration testing assists in determining the level of data destruction and risk in the event of a cyber attack.

15. Is it possible for a penetration test to compromise any system?

Every system has some kind of security flaw, which researchers may or may not be aware of. No system is entirely secure, and thus if adequate penetration testing is performed, every system can be broken by a Security Analyst. If the network is more secure, it will take the Security Analyst longer to break it, and likewise. Time can range from a few days to months.

16. What are the objectives of a pen testing exercise?

The objectives are as follows:

- To examine adherence to the organization's security policies that have been developed and executed.
- To examine employee proactivity and awareness of the security environment in which they work.
- To completely understand how a company entity might be confronted with a significant security breach, as well as how soon they respond to it and resume normal business operations after being affected.

17. What are the three types of pen testing methodologies?

These are the three types:

- Black-box testing
- White-box testing
- Gray-box testing

Black-Box Testing: When a Pen Tester is operating in a black-box environment, he or she has no idea what target(s) they will assault. As a result, pentesting can take a long time, and automated approaches are heavily relied on to expedite the process.

White-Box Testing: Clear-box testing is another term for this type of pen test. In some circumstances, the Pen Tester has a thorough understanding of the Web service they are about to attack, as well as its basic source code.

Gray-Box Testing: This method of pentesting combines black-box and white-box pentesting to uncover weaknesses. That is, they have a good idea of what they're going to attack.

18. What are the teams capable of performing a pentest?

The following are the teams:

- Red team
- Blue team
- Purple team

Red team: This team is in charge of launching the real threat in order to breach the business's or industry's defenses and expose any holes that are uncovered.

Blue team: The primary goal of the Blue Team is to prevent any cyber-attacks launched by the Red Team. They adopt a proactive approach while also keeping a high sense of security concern.

Purple team: This is a hybrid of the Red Team and the Blue Team. The Purple Team's main task is to help both of these teams. As a result, the Purple Team's Pen Testers cannot be influenced in any way and must retain a neutral perspective.

19. Is social engineering performed by pen testing?

In general, social engineering does not come under the scope of penetration testing. However, several organizations increasingly consider social engineering when performing pen-testing.

20. Are denial-of-service assaults tested as well?

Penetration testing also includes Denial-of-Service (DoS) attacks. There are numerous methods available to determine whether a system is vulnerable to DoS assaults.

www.infosectrain.com | sales@infosectrain.com