

Ethical Hacking Interview Questions and Answers



About us

InfosecTrain is one of the finest Security and Technology Training and Consulting organization, focusing on a range of IT Security Trainings and Information Security Services. InfosecTrain was established in the year 2016 by a team of experienced and enthusiastic professionals, who have more than 15 years of industry experience. We provide professional training, certification & consulting services related to all areas of Information Technology and Cyber Security.

Ethical hacking is an exciting career opportunity for individuals with excellent problem-solving skills and a passion for information security. Ethical hackers are responsible for safeguarding the critical infrastructure of the organization. They organize penetration tests to identify the vulnerabilities and help the organization take necessary measures to prevent possible cyber-attacks. There has been an increased demand for Ethical hackers in government agencies (military and intelligence agencies) and private organizations in recent times. To become an ethical hacker requires a sound knowledge of networking and hacking systems.

This section outlines some of the frequently asked questions in an Ethical hacking job interview.

Question1: What cybersecurity news sources do you prefer to keep yourself updated?

Answer: An ethical hacker needs to stay updated about the latest vulnerabilities, exploits, and attacks. Social media handles such as Twitter can be the quickest way to get information. You can also mention Google alert, Reddit, tech news sites, and channels on slack or discord communication platforms.

Question2: How would you conduct an external penetration test?

Answer: This question is often asked in the interview to test your methodology and approach to conducting a penetration test. The interviewers can shoot this question providing specific scenarios and parameters. Sometimes, they will deliberately skip the details. So don't restrain yourself from asking for additional information.

Remember that external penetration testing starts with the pre-engagement phase. A penetration tester sits with the client, determines the engagement's scope, and signs a non-disclosure agreement with the client. Before starting the testing process, verify the IP addresses and domain names provided by the clients. Explain your approach, tools, and methods thoroughly.

Question3: What shortest method would you use to identify the operating system of your target?

Answer: Grabbing the banner using a telnet session is the quickest and easiest way to identify the target's operating system.

Question4: What is the difference between vulnerability assessment and penetration testing?

Answer: In the vulnerability assessment, Ethical hackers identify the vulnerabilities and fix them to prevent possible cyberattacks. On the other hand, penetration testing is a process of detecting vulnerabilities and exploiting them to analyze a real cyber attack's implications.

Question5: What are the steps performed by hackers to take down a system or network?

Answer: Following are the steps performed by hackers to take down the system or network:

- Reconnaissance: In this step, hackers try to collect all the information about the target.
- Scanning or Enumeration: In this step, hackers use the gathered information to scan for the target's network and system vulnerabilities.
- Gaining Access: After scanning and enumeration, hackers gain access to the target machine by exploiting vulnerabilities.
- Maintaining access: Once access is obtained to the system, hackers install malicious software to keep access in the future.
- Clearing the tracks: In this step, hackers destroy all the pieces of evidence to remain undetected from the team of digital forensic.

Question6: What is a Phishing attack?

Answer: Phishing is a type of social engineering attack in which Attackers create an urgency using threats, financial incentives, and impersonation of an authoritative organization to prompt a user to give their sensitive information, including the credit card details, usernames, and passwords.

Question7: What is a sniffing attack?

Answer: Sniffing refers to monitoring and analyzing incoming and outgoing data packets over a network. Packet sniffers are used to capturing the data packets. Motives behind sniffing attacks are stealing bank account information, getting usernames and passwords, and identity theft.

Question8: What is Blind SQL injection? How would you detect a Blind SQLi vulnerability on a web page?

Answer: Blind SQL injection, when attackers insert a malicious query as input, the database does not show any error. Therefore, it becomes difficult for them to identify and exploit the vulnerability.

The best method to detect Blind SQLi is Time based detection.

Databases including MySQL, MS-SQL use a function for delays. The attacker inserts the sleep () function in a query. The slower response from the database would mean the query got executed successfully, and Blind SQLi vulnerability is present on the web page.

Question9: What do you understand by the DDoS attack? What are its types?

Answer: The Distributed Denial of Services (DDoS) is an attack in which an attacker floods a network, server, or website with useless traffic so that it becomes inoperable for the intended user. The traffic may contain incoming requests for connection or fake data packets. There are three types of DDoS attacks.

- Volume-based DDoS attack
- Protocol DDoS attack
- Application DDoS attack

Question10: What is an SQL injection attack?

Answer: SQL injection is a method to hack a web application. In this method, the attacker executes malicious SQL statements to take control of the database server. Attackers use SQL vulnerabilities to retrieve or modify the data of the SQL database.

The following are the types of SQL injections:

- Error-based SQL injection
- Blind SQL injection
- Union-based SQL injection

Question11: What are the characteristics of a good vulnerability assessment report?

Answer: A good vulnerability assessment report needs to be detailed and basic in nature so that even stakeholders having no technical background can easily understand it. The report should contain information regarding the vulnerabilities, how you find them, and their impact on the enterprise's business environment. It should also explain the valuable solutions to fix the vulnerabilities and mitigate potential risks.

Question12: what is cow patty?

Answer: Cowpatty is a tool that can implement an offline dictionary-based attack on the WPA/WPA2 networks that are using PSK-based authentication.

Question13: What is a keylogger?

Answer: keylogger is a surveillance technology used by an attacker on a target computer to record and monitor keystrokes struck by the user. Keyloggers record the sensitive information typed by the target.

Question14: What is spoofing?

Answer: Spoofing is a scam in which an attacker impersonates a legitimate source or known contact of the target to obtain sensitive information. Hackers can use this information for illegal activities such as identity theft.

Following are some of the renowned spoofing attacks:

- DNS server spoofing
- ARP spoofing
- Website spoofing
- Caller ID spoofing

Question15: What is DNS cache poisoning?

Answer: DNS cache poisoning is also known as DNS Spoofing. It is an attack in which an attacker takes advantage of the vulnerabilities existing in the DNS (Domain name system) to divert the traffic from the original server to a fake one.

Conclusion

The questions and answers mentioned above will help you prepare for your job interview. There are other questions related to cybersecurity that you may face in the interview.

It is recommended to upgrade your existing knowledge and skills with cybersecurity certifications. Infosec Train offers a comprehensive training program for the CEH (Certified Ethical Hacker) certification that will help you to forge a promising career in the field of Ethical hacking.



IND: 1800-843-7890 (Toll Free) / US: +1 657-221-1127 /
UK : +44 7451 208413



sales@infosectrain.com



www.infosectrain.com