49 Ethical Hacking Interview Questions to Ask Your Applicants

Questions

1. Can you explain what ethical hacking is and how it differs from malicious hacking?

2. What are the common types of vulnerabilities you would look for during a penetration test?

3. How do you stay updated with the latest security threats and hacking techniques?

4. Describe a time when you discovered a critical vulnerability. How did you handle the situation?

5. What tools and software do you prefer for penetration testing, and why?

6. How do you ensure that your ethical hacking activities comply with legal and ethical standards?

7. Can you walk me through the steps you would take to conduct a security audit for a company?

8. What is the OWASP Top Ten, and why is it important for web application security?

9. How do you approach reporting and documenting vulnerabilities you find during an assessment?

10. What strategies would you use to test the security of a wireless network?

11. What steps would you take if you found a vulnerability in a company's system during a penetration test?

12. How would you approach securing an organization's email system?

13. What methods would you use to ensure the security of a web application?

14. How would you handle a situation where you suspect an insider threat within the organization?

15. Can you explain the significance of network segmentation in cybersecurity?

16. How would you respond to a detected security breach in an organization?

17. What is your approach to conducting a risk assessment for a new IT system?

18. How do you ensure that third-party vendors comply with security policies?

19. How would you explain the concept of 'defense in depth' and its importance in cybersecurity?

20. Can you describe a time when you had to perform a social engineering test? What approach did you take?

21. What is the difference between black box, white box, and gray box penetration testing?

22. How would you go about testing for SQL injection vulnerabilities in a web application?

23. Explain the concept of 'privilege escalation' and provide an example of how it might occur.

24. What are some common methods for bypassing antivirus software, and how would you detect them?

25. How do you approach securing containerized environments, such as those using Docker?

26. Can you explain the concept of 'zero-day vulnerabilities' and their significance in ethical hacking?

27. What strategies would you employ to test the security of an IoT device?

28. How would you go about conducting a secure code review? What are the key areas you would focus on?

29. Explain the concept of 'buffer overflow' and how you would test for this vulnerability.

30. What are some common techniques for breaking or bypassing two-factor authentication?

31. How would you approach testing the security of a mobile application?

32. Can you explain the MITRE ATT&CK framework and its relevance to ethical hacking?

33. What methods would you use to test for cross-site scripting (XSS) vulnerabilities in a web application?

34. Can you explain the methodology you use for penetration testing?

35. How do you prioritize vulnerabilities once they are identified?

36. What techniques do you use to evade detection during a penetration test?

37. How do you handle false positives during a penetration test?

38. What steps do you take to ensure the confidentiality of client data during a penetration test?

39. How do you adapt your penetration testing approach for different types of organizations (e.g., financial institutions vs. small businesses)?

40. Can you describe a situation where you had to collaborate with other teams during a penetration test?

41. What are the main differences between SSL and TLS, and why is this distinction important?

42. Can you explain the principle of least privilege and how it applies to user access control?

43. What are the security implications of using outdated security protocols?