71 Cyber Security interview questions (and answers) to assess candidates

Questions

1. What is the difference between a virus and a worm?

2. Can you explain what multi-factor authentication is and why it is important?

3. What does the acronym VPN stand for and how does it enhance security?

4. Describe what a firewall does in a network.

5. What is encryption, and why is it essential in cyber security?

6. Can you explain what a DDoS attack is and how it impacts a business?

7. What is the principle of least privilege, and how does it apply to user access?

8. What are some common types of phishing attacks?

9. What steps would you take if you discovered a security breach?

10. What is the role of an Intrusion Detection System (IDS)?

11. Can you explain the concept of 'defense in depth'?

12. What are some key indicators of a potential security threat?

13. What is social engineering and why is it a concern in cyber security?

14. How do you stay updated on the latest security threats?

15. What is the importance of regular software updates and patch management?

16. Can you describe what a security audit entails?

17. How would you explain the concept of 'zero trust' in cybersecurity to a non-technical colleague?

18. What steps would you take to secure a newly set up Windows 10 workstation?

19. Can you explain the difference between symmetric and asymmetric encryption?

20. How would you go about investigating a potential data breach?

21. What is the OWASP Top 10, and why is it important for web application security?

22. How would you explain the concept of 'defense in depth' to a non-technical manager?

23. What are some common indicators of compromise (IoCs) that you would look for in a potential security incident?

24. How would you go about educating employees about phishing attacks?

25. How would you handle a situation where a colleague accidentally clicks on a phishing link?

26. Can you explain how a Public Key Infrastructure (PKI) works and its importance in securing communications?

27. Describe the process you would follow to conduct a vulnerability assessment on a corporate network.

28. What are some techniques you would use to identify and mitigate insider threats?

29. How do you ensure compliance with data protection regulations like GDPR or CCPA in your security strategies?

30. Discuss your experience with implementing and managing Security Information and Event Management (SIEM) systems.

31. What steps would you take to secure a cloud environment, such as AWS or Azure?

32. Explain the importance of penetration testing and how it fits into a company's overall security posture.

33. How do you handle and analyze security logs to identify unusual activity or potential threats?

34. Describe a time when you had to respond to a security incident. What was your approach and the outcome?

35. What is a man-in-the-middle attack and how can you prevent it?

36. How do you prioritize security tasks and vulnerabilities when managing multiple projects?

37. Can you explain what role machine learning and artificial intelligence play in modern cyber security?

38. Describe your experience with network segmentation. Why is it important and how do you implement it?

39. What are the key differences between threat, vulnerability, and risk?

40. How do you approach creating and implementing a Disaster Recovery Plan (DRP) for an organization?

41. What measures do you take to secure mobile devices within a corporate environment?

42. How do you ensure that third-party vendors comply with your organization's security policies and standards?

43. Can you describe what threat hunting is and how it differs from traditional threat detection?

44. How do you approach creating and implementing security policies for an organization?

45. Explain what network segmentation is and why it is important for threat mitigation.

46. What are some common techniques for mitigating phishing attacks?

47. How would you go about securing a remote workforce?

48. Can you explain the concept of 'zero-day vulnerability' and how you would protect against it?

49. What measures would you take to secure data stored in the cloud?

50. Can you explain the differences between TCP and UDP, and in what scenarios you would use each?

51. What is SSL/TLS, and how does it secure data transmitted over the internet?

52. Describe the function and importance of IPsec in network security.

53. How do you ensure secure communication in a public Wi-Fi environment?

54. What is the function of the Secure Shell (SSH) protocol?

55. Can you explain the differences between HTTPS and HTTP, and why HTTPS is preferred?

56. What are the main security features of the DNSSEC protocol?

57. How does the Simple Network Management Protocol (SNMP) impact network security?

58. What is a VPN protocol, and which ones would you recommend for secure communication?

59. Explain what Transport Layer Security (TLS) certificates are and how they work.

60. What role does the Kerberos protocol play in network security?

61. Can you describe what the Security Association (SA) is in the context of IPsec?

62. How would you respond if a colleague reported suspicious activity on their computer that could indicate a malware infection?

63. Imagine you notice unauthorized access attempts on a critical server. What immediate steps would you take to investigate and mitigate the situation?

64. If you were tasked with developing a new incident response plan, what key elements would you prioritize to ensure its effectiveness?

65. Describe a scenario where you had to convince management to invest in a new security initiative. What strategies did you use?

66. How would you handle a situation where a software update caused significant downtime for critical systems?

67. If you were leading a team dealing with a ransomware attack, what actions would you take to manage the crisis and communicate with affected stakeholders?

68. What approach would you take to assess the security posture of a third-party vendor before entering into a partnership?

69. If you discovered a major vulnerability in a widely used application, how would you decide whether to disclose it publicly or keep it confidential?