🔐 Cybersecurity Interview Questions and Answers (1–50)

1. What is Cybersecurity?

Answer: Cybersecurity is the practice of protecting systems, networks, and data from digital attacks, unauthorized access, or damage.

2. What is the CIA Triad?

Answer: Confidentiality, Integrity, and Availability – the three core principles of cybersecurity.

3. What is a firewall?

Answer: A security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

4. What is the difference between IDS and IPS?

Answer: IDS (Intrusion Detection System) detects threats, while IPS (Intrusion Prevention System) detects and blocks threats.

5. What is malware?

Answer: Malicious software designed to disrupt, damage, or gain unauthorized access to systems.

6. What are different types of malware?

Answer: Virus, Worm, Trojan, Ransomware, Spyware, Adware.

7. What is phishing?

Answer: A social engineering attack to trick users into revealing sensitive information like passwords or credit card numbers.

8. What is a DDoS attack?

Answer: Distributed Denial of Service – overwhelms a system with traffic to render it unavailable.

9. What is encryption?

Answer: The process of converting data into a coded form to prevent unauthorized access.

10. What is the difference between symmetric and asymmetric encryption?

Answer: Symmetric uses one key for encryption and decryption; asymmetric uses a public and private key pair.

11. What is hashing?

Answer: Transforming data into a fixed-length string, often used to store passwords securely.

12. What is a VPN?

Answer: Virtual Private Network – creates a secure tunnel between your device and the internet.

13. What is multi-factor authentication (MFA)?

Answer: Security method requiring two or more verification steps to access a system.

14. What is penetration testing?

Answer: Simulated cyberattack to identify vulnerabilities in systems or networks.

15. What is vulnerability assessment?

Answer: The process of identifying, classifying, and prioritizing system vulnerabilities.

16. What is social engineering?

Answer: Manipulating people into revealing confidential information.

17. What is SQL injection?

Answer: A code injection attack that allows execution of malicious SQL statements.

18. What is cross-site scripting (XSS)?

Answer: A vulnerability where attackers inject malicious scripts into websites.

19. What is a zero-day vulnerability?

Answer: A software flaw unknown to the vendor, exploited before it is patched.

20. What is patch management?

Answer: The process of managing updates for software to fix vulnerabilities.

21. What is a brute-force attack?

Answer: An attack that tries all possible password combinations to gain access.

22. What is port scanning?

Answer: Technique to identify open ports and services on a host.

23. What is the difference between white hat, black hat, and gray hat hackers?

Answer:

- White Hat: Ethical hacker
- Black Hat: Malicious hacker
- Gray Hat: A mix of both

24. What is a digital certificate?

Answer: An electronic document used to prove ownership of a public key.

25. What is SSL/TLS?

Answer: Protocols that provide secure communication over a computer network.

26. What is a security policy?

Answer: A document that outlines the rules for computer security in an organization.

27. What is role-based access control (RBAC)?

Answer: Permissions are assigned based on a user's role within the organization.

28. What is the principle of least privilege?

Answer: Users are given the minimum level of access required to perform their duties.

29. What is BYOD risk in cybersecurity?

Answer: Bring Your Own Device policies can expose corporate networks to untrusted devices.

30. What is a honeypot?

Answer: A decoy system used to attract and monitor attackers.

31. What is network segmentation?

Answer: Dividing a network into smaller parts to enhance security.

32. What is endpoint security?

Answer: Securing endpoints like laptops and smartphones from threats.

33. What is data loss prevention (DLP)?

Answer: Technology that prevents sensitive data from leaving the organization.

34. What is log monitoring?

Answer: Tracking system logs for suspicious activities.

35. What is an attack surface?

Answer: The sum of all possible entry points where an attacker can exploit a system.

36. What is the difference between risk, threat, and vulnerability?

Answer:

- Risk: Potential loss
- Threat: Possible danger
- Vulnerability: Weakness exploited by threats

37. What is ransomware?

Answer: Malware that locks data and demands ransom to unlock it.

38. What is the role of antivirus software?

Answer: Detects and removes malicious software from devices.

39. What is SIEM?

Answer: Security Information and Event Management – collects and analyzes log data in real-time.

40. What is ISO/IEC 27001?

Answer: An international standard for managing information security.

41. What is SOC?

Answer: Security Operations Center – a team that monitors and responds to security incidents.

42. What is a man-in-the-middle (MITM) attack?

Answer: An attacker secretly intercepts and relays messages between two parties.

43. What is sandboxing?

Answer: Running untrusted applications in a secure environment.

44. What is an insider threat?

Answer: A threat from within the organization (e.g., employees or contractors).

45. What is authentication vs. authorization?

Answer:

- Authentication: Verifying identity
- Authorization: Granting access to resources

46. What is blockchain's role in cybersecurity?

Answer: Ensures data integrity through decentralized and immutable records.

47. What is steganography?

Answer: Hiding data within another file (e.g., image or audio).

48. What is sniffing?

Answer: Capturing network packets to analyze data.

49. What is spear phishing?

Answer: A targeted phishing attack aimed at a specific individual or organization.

50. What steps should you take after a data breach?

Answer: Contain the breach, assess damage, notify affected parties, and implement security improvements.