Advanced Network Security – Question Bank (40 Questions)

1. What is network security, and why is it important in modern computing?

2. Explain the significance of network security in protecting sensitive information.

3. Describe the CIA triad and its key components.

4. As a network security analyst, define network security and explain its three primary goals. How would applying these goals improve an organization's security posture?

5. Explain the concept of network security architecture. Discuss at least five common threats to network security and propose appropriate countermeasures for each.

6. What are some common network security threats?

7. List and explain various network-layer threats. How can organizations protect against them using security policies and technologies?

8. How does risk assessment help in managing network security?

9. Describe the steps involved in risk assessment and management for a corporate network infrastructure.

10. Describe how security policies and standard operating procedures support a secure network environment. Give examples.

11. Discuss the role of firewalls in network security.

12. Describe the working of a firewall. What are the different types of firewalls? Highlight the key differences between a stateful and stateless firewall.

13. How do intrusion detection and prevention systems (IDS/IPS) enhance network security?

14. Compare IDS and IPS in terms of functionalities, roles, and deployment strategies.

15. Illustrate the placement and operation of IDS and IPS in a network architecture.

16. List the applications of Kerberos in secure system design.

17. Provide a detailed explanation of how the Kerberos authentication protocol functions. Include the ticket-based process and its components.

18. Explain the function of Extensible Authentication Protocol (EAP) and its common use cases.

19. Explain the purpose of LDAP in network authentication and its common applications.

20. Write a note on LDAP and its role in directory-based authentication.

21. Describe the working of the RSA algorithm with a complete step-by-step numerical example.

22. Compare symmetric and asymmetric encryption with examples.

23. Explain the Diffie-Hellman key exchange and its role in secure communication.

24. What are digital signatures? Illustrate how they are created and verified using the RSA algorithm.

25. What are the major challenges in key distribution, and how are they addressed in cryptographic systems?

26. Explain how public key infrastructure (PKI) supports secure communication.

27. Discuss key distribution methods used in public key cryptosystems. How do digital certificates and Certificate Authorities (CAs) help establish trust?

28. State the key principles of public key cryptosystems and their significance.

29. What are the main features of digital signatures and their advantages in secure communications?

30. Scenario-based: A government agency wants to secure inter-office communication. Explain how PKI enhances security with digital certificates and

CAs ensuring confidentiality, integrity, authentication, and non-repudiation.

31. Compare RADIUS and TACACS+ in terms of security features and functionality.

32. How do OAuth and OpenID Connect facilitate secure authentication?

33. Compare OpenID Connect with OAuth 2.0.

34. How does OAuth 2.0 protocol enable delegated authorization? Provide an example use case.

35. Describe the use of Security Assertion Markup Language (SAML) in authentication. How does it enable Single Sign-On (SSO)?

36. What are the advantages of using multi-factor authentication (MFA) in network security?

37. Explain the differences between session-based and token-based authentication methods.

38. Describe how SSL/TLS ensures secure communication. Include its purpose, working, and differences between SSL and TLS.

39. Scenario-based: How does SSL/TLS secure login and payment data on an e-commerce website? Briefly describe the handshake process.

40. Scenario-based: A company finds its Wi-Fi network was compromised using Aircrack-ng. Define Wi-Fi hacking, common attack techniques, and security recommendations.