NFSU

विद्या अमृतं अश्नुते

National Forensic Sciences University

Knowledge | Wisdom | Fulfilment

An Institution of National Importance
(Ministry of Home Affairs, Government of India)

Cyber Security Role

Top 50 Questions and Answers

Placement Cell, NFSU Goa
January 31, 2025

Cyber Security - Top 50 Questions

1. **What is the difference between symmetric and asymmetric encryption?**
   Symmetric encryption uses a single key for both encryption and decryption, while asymmetric encryption uses a pair of public and private keys.

2. **Can you explain what a firewall is and how it works?**
   A firewall is a security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

3. **What is a VPN, and why is it important for cybersecurity?**
   A VPN (Virtual Private Network) encrypts internet traffic and masks the user's IP address, ensuring privacy and securing communications over untrusted networks.

4. **How does a DDoS attack work, and how can you mitigate it?**
   A DDoS (Distributed Denial of Service) attack overwhelms a server with traffic, disrupting services. Mitigation involves traffic filtering, rate limiting, and using DDoS protection services.

5. **What is a zero-day vulnerability, and how would you address it?**
   A zero-day vulnerability is an unpatched security flaw. It can be addressed by applying patches once discovered or using intrusion detection/prevention systems to mitigate its impact.

6. **Explain the concept of phishing and how to recognize phishing emails.**
   Phishing is a social engineering attack where attackers impersonate legitimate entities to steal information. Phishing emails often contain suspicious links or attachments.

7. **What is a Security Operations Center (SoC), and what role does it play in cybersecurity?**
   A SoC is a centralized unit that monitors, detects, and responds to security incidents in real-time to protect an organization's infrastructure.

8. **What are the primary differences between IDS and IPS?**
   An IDS (Intrusion Detection System) detects and alerts on potential threats, while an IPS (Intrusion Prevention System) actively blocks detected threats.

9. **How do you secure a web application from common attacks like SQL Injection?**
   To secure a web application from SQL Injection, use prepared statements, parameterized queries, and input validation to prevent malicious input.

10. **What is the role of SIEM (Security Information and Event Management)?**
    SIEM systems collect and aggregate log data from various sources, helping to detect, analyze, and respond to potential security incidents.

11. **What is multi-factor authentication (MFA), and why is it important?**
    MFA requires users to provide multiple forms of verification (e.g., password + fingerprint), making it more difficult for attackers to gain unauthorized access.

12. **What are the best practices for password management?**
    Use strong, unique passwords, implement password managers, and enable multi-factor authentication (MFA) to secure accounts.

13. **What is encryption, and why is it important in cybersecurity?**
    Encryption converts data into a secure format that can only be read by authorized parties, ensuring data privacy and integrity.

14. **What is the purpose of a DMZ (Demilitarized Zone) in network security?**
    A DMZ separates an organization's internal network from external networks, offering an additional layer of security for web servers and other public-facing services.

15. **How do you handle a potential malware infection in an organization?**
    Contain the infection by isolating affected systems, analyze the malware, remove it using antivirus tools, and restore from backups if necessary.

16. **What is a man-in-the-middle (MITM) attack, and how can you prevent it?**
    A MITM attack occurs when an attacker intercepts and potentially alters communication between two parties. Prevent it using encryption (TLS/SSL) and secure communication protocols.

17. **What is network segmentation, and why is it important?**
    Network segmentation divides a network into smaller segments, enhancing security by limiting the spread of attacks and containing threats to isolated parts of the network.

18. **What are the key principles of least privilege in cybersecurity?**
    The principle of least privilege ensures that users and systems only have access to the resources necessary for their job, minimizing exposure to potential threats.

19. **What is the difference between a public key and private key in cryptography?**
    A public key encrypts data, while a private key decrypts it. The public key is shared openly, and the private key is kept secret to ensure secure communication.

20. **What is social engineering, and how can you defend against it?**
    Social engineering involves manipulating individuals to gain confidential information. Defend against it with awareness training, strict security policies, and verifying identities.

21. **How would you secure cloud services?**
    Secure cloud services by using encryption, access controls, multi-factor authentication (MFA), and regular audits to ensure compliance and reduce vulnerabilities.

22. **What is a patch management process?**
    Patch management involves regularly updating software and systems to fix security vulnerabilities and improve performance.

23. **What is a vulnerability scanner, and how does it help in cybersecurity?**
    A vulnerability scanner automatically detects and assesses weaknesses in systems and networks, helping security teams prioritize fixes before attackers exploit them.

24. **What is a honeypot in cybersecurity?**
    A honeypot is a decoy system or network designed to attract and monitor attackers, providing insights into attack methods and helping to detect vulnerabilities.

25. **How do you manage and respond to insider threats?**
Respond to insider threats by monitoring user activity, implementing strict access controls, and performing regular audits to detect suspicious behavior.

26. **What is the purpose of a penetration test?**
A penetration test simulates an attack on a system to identify vulnerabilities before malicious actors can exploit them.

27. **How do you ensure secure communication between two parties?**
Secure communication is achieved through encryption, using protocols like TLS/SSL, and authenticating both parties through digital certificates.

28. **What is the difference between a public and a private network?**
A public network is open to external users, while a private network is restricted to authorized individuals, offering greater security.

29. **How do you prevent unauthorized access to a network?**
Prevent unauthorized access by using strong passwords, encryption, multi-factor authentication (MFA), and regular monitoring for suspicious activity.

30. **What are the best practices for securing a wireless network?**
Use WPA3 encryption, set strong passwords, disable WPS, and regularly monitor for unauthorized devices connected to the network.

31. **What is a keylogger, and how can it be detected and prevented?**
A keylogger is malware that records keystrokes. It can be detected through anti-malware software and prevented by installing security updates and avoiding untrusted software.

32. **What is ransomware, and how can you protect against it?**
Ransomware encrypts files and demands payment for decryption. Protection involves regular backups, security awareness training, and strong endpoint defenses.

33. **What are cookies in web security, and how should they be managed?**
Cookies store user data for web applications. They should be managed by using secure, HttpOnly, and SameSite flags to protect against cross-site scripting (XSS) attacks.

34. **What is an ACL (Access Control List)?**
An ACL is a list of rules that specifies which users or systems are allowed or denied access to certain resources.

35. **What is a Distributed Denial of Service (DDoS) attack?**
A DDoS attack aims to overwhelm a network or server by flooding it with a large volume of traffic, causing disruption and making the service unavailable.

36. **What is a web application firewall (WAF), and how does it work?**
A WAF protects web applications by filtering and monitoring HTTP traffic to detect and block malicious requests, such as SQL injections or cross-site scripting (XSS).

37. **What is the difference between a virus, a worm, and a trojan?**
A virus attaches to legitimate programs, a worm spreads independently, and a trojan disguises itself as a legitimate file to execute malicious actions.

Cyber Security - Top 50 Questions

38. **What is a Public Key Infrastructure (PKI)?**
    PKI is a framework that uses public and private keys to securely exchange data, ensuring confidentiality, authenticity, and integrity.

39. **What is the role of an SSL/TLS certificate in web security?**
    SSL/TLS certificates encrypt data between a web server and client, providing a secure channel to prevent data interception and tampering.

40. **What is the principle of defense in depth?**
    Defense in depth is a layered security approach that uses multiple levels of defense (firewalls, encryption, access control) to protect systems from threats.

41. **What is an advanced persistent threat (APT)?**
    APT is a prolonged and targeted cyberattack where attackers gain unauthorized access to a system and remain undetected to steal sensitive data.

42. **What is the CIA triad in cybersecurity?**
    The CIA triad stands for Confidentiality, Integrity, and Availability, which are the core principles in securing information systems and data.

43. **What is data masking, and when should it be used?**
    Data masking involves obfuscating sensitive data to protect it while ensuring that it remains usable for testing or analysis purposes.

44. **What is an IPsec VPN?**
    IPsec (Internet Protocol Security) VPN secures internet protocol communications by encrypting and authenticating data packets at the IP layer.

45. **What is the difference between an internal and external threat?**
    An internal threat comes from within an organization (employees or insiders), while an external threat comes from outside (hackers or malicious actors).

46. **What is the purpose of a security audit?**
    A security audit involves reviewing an organization's security policies, procedures, and systems to identify vulnerabilities and ensure compliance with security standards.

47. **What is an attack surface?**
    The attack surface refers to the sum of all points where unauthorized access to a system can occur, including hardware, software, and network interfaces.

48. **What are security patches, and why are they important?**
    Security patches are updates to software or systems that fix vulnerabilities. They are important because they prevent attackers from exploiting known flaws.

49. **What is the difference between confidentiality and privacy?**
    Confidentiality refers to protecting data from unauthorized access, while privacy relates to the control individuals have over their personal information.

50. **What are the steps involved in an incident response process?**
    The incident response process typically involves preparation, detection, containment, eradication, recovery, and lessons learned to handle a security breach effectively.