TOP 100 Interview Questions

PART 1

TOP 100 INTERVIEW QUESTIONS PART 1

1. How would you define cybersecurity, and what makes it crucial?

Cybersecurity is the practice of securing systems, networks, and data from unauthorized access, attacks, or damage. It plays a critical role in maintaining the confidentiality, accuracy, and accessibility of information, helping to protect organizations from data breaches, financial loss, and cyber threats.

---

2. What does the CIA triad stand for, and why is it important?

The CIA triad consists of three key components: Confidentiality, Integrity, and Availability. These principles guide cybersecurity practices by ensuring that sensitive data remains private, unaltered, and accessible to authorized users when needed.

---

3. Can you explain the difference between a vulnerability, a threat, and a risk?

- **Vulnerability:** A system weakness that could be exploited by an attacker.
- **Threat:** Any event or action with the potential to cause harm to a system or data.
- **Risk:** The potential impact and likelihood of a threat exploiting a vulnerability.

---

4. How do you stay current with evolving cybersecurity trends?

I keep up with industry advancements by reading cybersecurity blogs, subscribing to newsletters, attending webinars, and participating in conferences and online communities.

---

5. What are the primary layers of security within a system?

The main security layers include network security, application security, data security, endpoint protection, and physical security. These layers work together to establish a robust defence strategy.

---

6. What is multi-factor authentication (MFA), and why is it valuable?

MFA is a security measure that requires users to verify their identity through two or more factors, such as a password (something you know), a physical token (something you have), or biometrics (something you are). It reduces the risk of unauthorized access by adding multiple layers of security.

---

7. What do you mean by "Defence in Depth"?

Defence in Depth is a cybersecurity strategy that employs multiple layers of security controls. Each layer adds redundancy, making it more challenging for attackers to compromise the entire system.

---

8. How do authentication and authorization differ?

- **Authentication** confirms the identity of a user or system.
- **Authorization** determines what actions or resources an authenticated user is permitted to access.

---

9. What is a security policy, and why is it essential?

A security policy is a formal set of guidelines and rules designed to protect an organization's IT assets. It ensures compliance, mitigates risks, and provides a framework for responding to security incidents.

---

10. Describe the principle of "least privilege."

The principle of least privilege dictates that users should only have the minimum level of access required to perform their tasks. This minimizes the potential for accidental or malicious misuse of privileges.

---

11. What is the purpose of a firewall?

A firewall acts as a security barrier that monitors and controls network traffic based on predefined rules. Its primary role is to protect systems from unauthorized access by filtering incoming and outgoing data.

---

12. How do TCP and UDP differ?

- **TCP (Transmission Control Protocol):** A connection-oriented protocol that ensures reliable data transmission by verifying delivery.
- **UDP (User Datagram Protocol):** A connectionless protocol that prioritizes speed over reliability, making it suitable for applications like video streaming.

---

13. What is a VPN, and how does it enhance security?

A Virtual Private Network (VPN) encrypts internet connections, creating a secure communication channel over public network. It hides the user's IP address, safeguarding sensitive data from interception.

---

14. What role does DNS play in networking?

The Domain Name System (DNS) converts human-readable domain names (e.g., www.example.com) into IP addresses, enabling devices to locate and communicate with websites and services.

---

15. How does the TCP three-way handshake work?

The TCP three-way handshake establishes a reliable connection between a client and a server through three steps:

1. **SYN:** The client requests a connection.
2. **SYN-ACK:** The server acknowledges the request.
3. **ACK:** The client confirms the acknowledgment, finalizing the connection.

TOP 100 INTERVIEW QUESTIONS PART 1

16. What is a DMZ in a network, and why is it used?

A Demilitarized Zone (DMZ) is a buffer network that separates internal systems from untrusted external networks (e.g., the internet). It provides an additional layer of security by isolating critical resources.

---

17. How does NAT (Network Address Translation) improve security?

NAT masks internal IP addresses by translating them into a single public IP address, reducing the exposure of internal systems to external threats.

---

18. What is ARP poisoning, and how can it be prevented?

ARP poisoning involves manipulating the ARP cache to intercept or redirect traffic. Preventive measures include using static ARP entries, enabling encrypted traffic, and deploying dynamic ARP inspection.

---

19. What is MAC flooding, and what impact does it have on network switches?

MAC flooding overwhelms a switch's MAC address table, causing it to broadcast all traffic to every port, which can be mitigated by enabling port security to limit the number of MAC addresses per port.

---

20. How do stateful and stateless firewalls differ?

- **Stateful firewalls:** Track the state of active connections and allow or block traffic based on connection context.
- **Stateless firewalls:** Filter traffic solely based on predefined rules, without considering the connection state.

---

21. What distinguishes hashing from encryption?

Hashing is a one-way process that converts data into a fixed-length string, primarily used for verification. Encryption, on the other hand, is a reversible process that secures data by transforming it into an unreadable format, which can be decrypted with the correct key.

---

22. Can you name some widely used encryption algorithms?

Common encryption algorithms include AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), and DES (Data Encryption Standard).

---

23. What is a digital signature, and how does it function?

A digital signature is a cryptographic tool that verifies the authenticity and integrity of a message or document. It works by using the sender's private key to create the signature, which can be validated with their public key.

---

24. What is Public Key Infrastructure (PKI)?

PKI is a framework that manages public-key encryption through the use of digital certificates, certificate authorities, and secure key management to ensure secure communication.

---

25. How is a secure key exchange achieved in asymmetric encryption?

Protocols like Diffie-Hellman and RSA facilitate secure key exchanges by enabling parties to share public keys while keeping private keys confidential.

---

26. What is a nonce, and why is it used in cryptography?

A nonce is a unique, one-time-use number included in cryptographic processes to prevent replay attacks and ensure that each transaction or encryption instance is unique.

---

27. What are rainbow tables, and how can they be countered?

Rainbow tables are precomputed databases used to reverse cryptographic hash functions quickly. They can be mitigated by adding a unique salt to each password before hashing.

---

28. How does steganography differ from cryptography?

Steganography conceals information within other files or media, making its presence undetectable, while cryptography secures information by converting it into an unreadable format.

---

29. How do you verify the authenticity of a digital certificate?

By validating the certificate's signature using the issuing certificate authority's public key and ensuring it hasn't expired or been revoked.

---

30. What is Perfect Forward Secrecy (PFS), and why is it significant?

PFS ensures that even if a private key is compromised, past communications remain secure by generating unique session keys for each connection.

---

31. What is the distinction between a public key and a private key in asymmetric encryption?

A public key is used to encrypt data and can be shared freely, while a private key decrypts the data and must remain confidential to ensure secure communication.

TOP 100 INTERVIEW QUESTIONS PART 1

32. What is a buffer overflow attack?

A buffer overflow occurs when more data is written to a buffer than it can hold, potentially overwriting adjacent memory and allowing attackers to execute malicious code or crash the system.

---

33. What is a botnet, and how does it operate?

A botnet is a collection of compromised devices controlled by an attacker to perform malicious activities such as launching DDoS attacks, sending spam, or stealing sensitive data.

---

34. How would you explain SQL Injection?

SQL Injection is a type of attack where malicious SQL code is inserted into input fields or queries, enabling attackers to manipulate the database, extract sensitive information, or execute unauthorized commands.

---

35. What is DNS Spoofing?

DNS Spoofing, also known as DNS cache poisoning, involves altering DNS records to redirect users to fraudulent websites, often used in phishing or malware distribution.

---

36. What is an Advanced Persistent Threat (APT)?

An APT is a long-term, targeted cyberattack designed to infiltrate and extract data from an organization. It involves sophisticated methods, such as exploiting vulnerabilities over time, and is often carried out by well-funded attackers, including state-sponsored groups.

---

37. What is a vulnerability assessment?

A vulnerability assessment is the process of systematically identifying, evaluating, and prioritizing security weaknesses in a system, network, or application. Its goal is to mitigate vulnerabilities before attackers can exploit them.

---

38. What is penetration testing, and why is it conducted?

Penetration testing, or pen testing, is a simulated cyberattack performed to identify and exploit security vulnerabilities in a system. It helps assess the effectiveness of security controls and prevents real-world attacks by uncovering weaknesses.

---

39. How does a vulnerability scanner differ from a network scanner?

- **Vulnerability scanner:** Identifies known security flaws, such as outdated software or misconfigurations.
- **Network scanner:** Detects active devices, open ports, and running services in a network.

While the former highlights security risks, the latter provides a detailed map of network components.

---

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

- **Virus:** Attaches itself to a host file or program and requires user action to spread.
- **Worm:** A standalone malware that replicates itself across networks without needing a host, spreading autonomously.

---

41. What is phishing, and how can organizations protect against it?

Phishing is a social engineering attack where victims are tricked into providing sensitive information, such as login credentials or financial details. Organizations can combat phishing through employee training, email filtering, multi-factor authentication (MFA), and regular phishing simulations.

---

42. How do ransomware and spyware differ?

- **Ransomware:** Encrypts a victim's files and demands payment for decryption.
- **Spyware:** Covertly monitors and collects information about the victim's activities without their consent.

Ransomware focuses on extortion, while spyware centers on surveillance.

---

43. What is a Distributed Denial of Service (DDoS) attack, and how is it mitigated?

A DDoS attack overwhelms a target system or network with excessive traffic from multiple sources, causing it to become inaccessible. Mitigation techniques include traffic filtering, rate limiting, using content delivery networks (CDNs), and deploying specialized anti-DDoS solutions.

---

44. What does privilege escalation mean?

Privilege escalation occurs when an attacker gains higher access levels than initially authorized. It can be:

- **Vertical:** Gaining administrative privileges.
- **Horizontal:** Accessing another user's data.

Mitigation includes enforcing least privilege and regularly reviewing access permissions.

---

45. How do attackers exploit social engineering to access systems?

Social engineering manipulates human behavior to obtain confidential information or system access. Attackers may impersonate trusted entities or exploit psychological triggers like urgency or fear to deceive victims.

---

46. What are zero-day vulnerabilities, and how can they be mitigated?

Zero-day vulnerabilities are software flaws unknown to the vendor, with no available patches. They are exploited by attackers before discovery or remediation. Mitigation

strategies include using intrusion detection systems, threat intelligence, and promptly patching software as updates become available.

---

47. What is ransomware, and how can organizations protect themselves?

Ransomware is malicious software that locks systems or encrypts data, demanding payment for access. Preventative measures include regular data backups, employee awareness training, endpoint protection, and ensuring all software is up-to-date.

---

48. What is an insider threat, and how can it be managed?

An insider threat comes from individuals within an organization, such as employees or contractors, who misuse their access to cause harm. Countermeasures include monitoring user activity, implementing strict access controls, and conducting regular audits.

---

49. What is a rootkit, and how can it be detected?

A rootkit is a type of malware designed to hide its presence on a system, making detection difficult. Detection involves using anti-malware tools, monitoring unusual system behaviours, analysing network traffic, and manually inspecting system processes.

---

50. What distinguishes a worm from a virus?

While both are forms of malware, a worm operates independently, spreading across networks without requiring a host program. In contrast, a virus attaches to a legitimate file or program and requires user action to propagate.

DID YOU FIND THIS DOCUMENT USEFUL

WWW.MINISTRYOFSECURITY.CO

FOLLOW FOR FREE INFOSEC CHECKLISTS | PLAYBOOKS TRAININGS | VIDEOS