■■■ Cybersecurity Interview Q&A; Guide

1■■ What is Cryptography?

■ Cryptography is the science of securing information by converting it into unreadable code (encryption) to protect it from unauthorized access. It ensures confidentiality, integrity, and authentication of data.

2■■ Difference between Symmetric and Asymmetric Encryption

■■ Symmetric uses the same key for encryption and decryption (e.g., AES), while Asymmetric uses two keys—Public and Private (e.g., RSA). Asymmetric is more secure but slower.

3■■ Difference between IDS and IPS

■ IDS (Intrusion Detection System) detects and alerts suspicious activities, whereas ■■ IPS (Intrusion Prevention System) detects and blocks malicious activities.

4■■ CIA Triad

■ Confidentiality – Protects data from unauthorized access. ■ Integrity – Ensures data consistency and accuracy. ■ Availability – Ensures resources are accessible when required.

5■■ Encryption vs Hashing

■ Encryption is reversible and used for confidentiality. ■ Hashing is one-way and used for data integrity (e.g., passwords).

6■■ What is a Firewall?

■ A Firewall filters incoming and outgoing traffic based on predefined security rules, acting as a barrier between trusted and untrusted networks.

7■■ VA vs PT

■ Vulnerability Assessment (VA) identifies system flaws, while ■■ Penetration Testing (PT) exploits those flaws to test security defenses.

8■■ Three-Way Handshake

■ A TCP connection setup process involving SYN, SYN-ACK, and ACK packets.

9■■ HTTP Response Codes

■ 200 – OK, ■ 403 – Forbidden, ■ 404 – Not Found, ■ 500 – Internal Error, ■ 301/302 – Redirect.

■ Traceroute

■■ A diagnostic tool that shows the path packets take across a network to identify latency or routing issues.

11■■ HIDS vs NIDS

■ HIDS monitors individual hosts, while ■ NIDS monitors traffic across network segments.

12■■ Steps to Set Up a Firewall

1■■ Define policies 2■■ Configure rules 3■■ Test inbound/outbound traffic 4■■ Monitor & update regularly.

13■■ SSL Encryption

■ SSL (Secure Socket Layer) encrypts data between browser and server, ensuring secure HTTPS communication.

14■■ Steps to Secure a Server

■ Update OS, ■ Enable Firewall, ■ Disable unused ports, ■ Use strong passwords, ■ Enable logging & monitoring.

15■■ Data Leakage

■ Unintentional exposure of sensitive data via email, cloud, or external drives.

16■■ Common Cyber Attacks

■ Phishing, ■ DDoS, ■ Malware, ■ Spoofing, ■ SQL Injection, ■ Brute Force.

17■■ Brute Force Attack

■ Repeatedly guessing passwords until success. ■■ Prevent using strong passwords, account lockout, CAPTCHA, and 2FA.

18■■ Port Scanning

■ Scanning for open ports & services to identify vulnerabilities.

19■■ OSI Model (7 Layers)

1. Physical ■ 2. Data Link ■ 3. Network ■ 4. Transport ■ 5. Session ■ 6. Presentation ■■ 7. Application ■

20■■ VPN

■■ A Virtual Private Network encrypts your connection to maintain privacy and anonymity over public networks.

21■■ Risk, Vulnerability & Threat

■■ Risk: Possible damage if a threat exploits a vulnerability. ■ Vulnerability: Weakness in a system. ■ Threat: Potential cause of harm.

22■■ Preventing Identity Theft

■ Use strong passwords, ■ enable 2FA, ■ avoid public Wi-Fi for sensitive tasks, ■ monitor credit activity.

23■■ Hacker Types

■ Black Hat – Malicious ■ White Hat – Ethical ■ Gray Hat – Mix of both

24■■ Patch Management Frequency

■■ Apply patches monthly or immediately after critical updates.

25■■ Resetting BIOS Password

■ Remove CMOS battery or use hardware jumper to reset BIOS settings.

26■■ MITM Attack

■ Attacker intercepts communication between parties. ■■ Prevent: HTTPS, VPNs, strong encryption.

27■■ DDoS Attack

■ Overloads server with traffic. ■■ Prevent: CDNs, rate limiting, DDoS protection tools.

28■■ XSS Attack

■ Injects malicious scripts into websites. ■■ Prevent: Input validation & output encoding.

29■■ ARP

■ Maps IP addresses to MAC addresses for LAN communication.

30■■ Port Blocking

■ Restricts specific ports to prevent unauthorized access within a LAN.

31■■ TCP/IP Internet Layer Protocols

■ IP, ■ ICMP, ■ ARP, ■ IGMP.

32■■ Botnet

■ A network of compromised computers controlled remotely for attacks or spam.

33■■ Salted Hashes

■ Random data added before hashing passwords to prevent rainbow table attacks.

34■■ SSL vs TLS

■ TLS (Transport Layer Security) is the newer, stronger version of SSL.

35■■ Data Protection in Transit vs At Rest

■ In Transit: Data moving across network (use TLS) ■ At Rest: Stored data (use AES, BitLocker).

36■■ Two-Factor Authentication (2FA)

■ Adds an extra login layer—password + OTP/email/code.

37■■ Cognitive Cybersecurity

■ Uses AI & ML to detect, predict, and respond to cyber threats intelligently.

38■■ VPN vs VLAN

■ VPN secures internet traffic; ■ VLAN segments internal network traffic.

39■■ Phishing

■ Tricks users into sharing sensitive data. ■■ Prevent: Awareness, spam filters, URL inspection.

40■■ SQL Injection

■ Injects malicious SQL commands into input fields. ■■ Prevent: Input validation, parameterized queries, least privilege.