use technical words as appropriate.
use bulleted points it was good.

ChatGPT

Questions:

1. Explain 3D's (Defense, Detection, and Deterrence) aspects of security.
2. Explain various Application-layer attacks.
3. Write a short note on CIA Triad Model.
4. Explain how Onion Defence Model is better for security.
5. What is Zone of Trust? Explain its importance.
6. What are the various countermeasures to minimize attack risks?
7. Explain different types of Authentication.
8. How does Kerberos Authentication Process occur?
9. Write a short note on Certificate-Based Authentication.
10. What is Extensible Authentication Protocol (EAP)? Explain its types.
11. Explain the role of PKI in Security in Computing.
12. "Each security layer serves a specific purpose." Explain in the context of Database Security Layers.
13. Explain different layers of two-tier network fundamentals.

Answers:

1. 3D's of security:
    - Defense encompasses preventive measures.
    - Detection involves identifying anomalies or breaches.
    - Deterrence aims to discourage potential attackers through deterrent measures, such as visible security measures or penalties.
2. Application-layer attacks:
    - Target vulnerabilities in software applications.
    - Examples include SQL injection, cross-site scripting (XSS), and buffer overflow attacks.
3. CIA Triad Model:
    - Ensures Confidentiality, Integrity, and Availability of data.
    - Forms the foundation for designing robust security policies and measures.
4. Onion Defence Model:
    - Implements multiple layers of security, akin to layers of an onion.
    - Offers enhanced protection through the sequential arrangement of defense mechanisms, making it harder for attackers to penetrate.
5. Zone of Trust:
    - Designates secure network segments where communication is considered safe.
    - Ensures that sensitive data remains protected within trusted boundaries, enhancing overall security posture.

6. Countermeasures to minimize risks:
    - Regular patching and updates to address known vulnerabilities.
    - Implementation of firewalls, intrusion detection systems, and antivirus software.
    - Employee training on security best practices to mitigate human error.
7. Authentication types:
    - Password-based authentication using usernames and passwords.
    - Biometric authentication methods like fingerprint scanning or facial recognition.
    - Token-based authentication utilizing physical or digital tokens for verification.
8. Kerberos Authentication:
    - Utilizes tickets issued by a Key Distribution Center (KDC) for authentication.
    - Involves a series of exchanges between the client, server, and KDC to verify identities securely.
9. Certificate-Based Authentication:
    - Relies on digital certificates issued by trusted Certificate Authorities (CAs) to verify the identity of entities.
    - Ensures secure communication by confirming the authenticity of parties involved.
10. Extensible Authentication Protocol (EAP):
    - Framework supporting various authentication methods beyond passwords.
    - Includes EAP-TLS for certificate-based authentication and EAP-PEAP for password-based authentication, among others.
11. PKI in Security:
    - Establishes a trusted framework for secure communication through digital certificates.
    - Comprises certificate authorities (CAs), registration authorities (RAs), and other supporting infrastructure.
12. Database Security Layers:
    - Each layer enforces specific access controls to protect data integrity and confidentiality.
    - Examples include authentication mechanisms, authorization rules, and encryption protocols.
13. Two-tier network fundamentals:
    - Divided into client and server layers for simplified network management.
    - Enhances security by segregating user-facing and backend systems, reducing attack surface and potential risks.