Exam Cram Notes: General Security Concepts – Fundamental Security Concepts

1. The CIA Triad

The **Confidentiality, Integrity, and Availability (CIA)** triad is the foundation of security principles:

- **Confidentiality –** Prevents unauthorized access to data.
    - Methods: **Encryption, Access Controls (ACLs), Multi-Factor Authentication (MFA)**
    - Example: Using AES encryption to protect sensitive files
- **Integrity –** Ensures data remains unchanged unless modified by an authorized entity.
    - Methods: **Hashing (SHA-256, MD5), Digital Signatures, Checksums**
    - Example: A digital signature verifying a software update is authentic
- **Availability –** Ensures data and resources are accessible when needed.
    - Methods: **Redundancy, Load Balancers, Disaster Recovery Plans (DRP)**
    - Example: Using backup generators to keep systems running during power failures

---

2. Non-Repudiation

- Ensures users **cannot deny** sending or receiving data.
- Implemented using **digital signatures** and **audit logs**.
- Example: Email services using **PGP (Pretty Good Privacy)** to verify sender identity.

---

3. Authentication, Authorization, and Accounting (AAA)

The **AAA model** secures access control and activity tracking:

- **Authentication –** Verifies identity (e.g., username + password, biometrics, MFA).
- **Authorization –** Determines what an authenticated user can access.
- **Accounting –** Logs user activity for auditing.

Example:
🔷 **Authentication –** User logs in with a password.
🔷 **Authorization –** User is granted access to specific folders.
🔷 **Accounting –** The system records login time and file access logs.

---

4. Zero Trust Architecture (ZTA)

- **Never trust, always verify –** Even internal users need authentication.

- Requires **continuous verification** using MFA, device checks, and behavior analysis.
- Example: Employees need to **re-authenticate** when switching networks, even within the same company.

---

5. Gap Analysis

- Identifies security weaknesses by comparing current security controls to best practices.
- Example: A company **reviews policies** and finds that MFA isn't enforced.

Key Exam Tips

✅ Memorize the **CIA triad** and how each component is applied.
✅ Understand how **AAA works** and how it differs from Zero Trust.
✅ Be prepared for **scenario-based questions** on non-repudiation and access control.
✅ Know how **gap analysis** identifies missing security controls.