Key Concepts of Domain 5: Identity and Access Management (IAM)

Key Concepts (Detailed)

1 Identification:

1. Process of asserting an identity (e.g., user ID).
2. Key components:
    1. Unique identifiers for every user.
    2. Ensuring no duplication to maintain accountability.

2 Authentication:

1. Ensures that the identity is valid.
2. Techniques:
    1. **Knowledge-Based**: Passwords, PINs.
    2. **Possession-Based**: Smart cards, hardware tokens.
    3. **Biometric-Based**: Fingerprints, iris scans.
3. Strengthened by Multifactor Authentication (MFA).

3 Authorization:

1. Decides what an authenticated user can access, often based on policies:
    1. Role-Based Access Control (RBAC): Access based on roles (e.g., admin, user).
    2. Attribute-Based Access Control (ABAC): Policies based on attributes like time of access, location, etc.
    3. Mandatory Access Control (MAC): Centralized control based on classification levels (e.g., Top Secret).
    4. Discretionary Access Control (DAC): Resource owner decides access permissions.

4 Accounting (Auditing):

1. Tracks user actions for compliance, troubleshooting, and accountability.

5 Access Control Models:

1. **RBAC**: Assigns roles to users and grants permissions based on roles.
2. **ABAC**: Uses dynamic rules (e.g., time of day, device type).
3. **MAC**: Used in military and high-security settings (e.g., Top Secret data).

4. **DAC**: Common in businesses, offering flexibility.

6 Access Control Technologies:

1. SSO: Centralized login.
2. Federated Identity Management: Trust-based sharing of identities across organizations (e.g., SAML, OAuth).
3. Privileged Access Management (PAM): Monitors and secures admin accounts.

7 Biometrics:

1. Accuracy measured via:
    1. **False Acceptance Rate (FAR)**: Unauthorized users mistakenly authenticated.
    2. **False Rejection Rate (FRR)**: Authorized users mistakenly denied.
    3. **Crossover Error Rate (CER)**: Point where FAR and FRR are equal (lower CER = better system).

8 Password Security:

1. Strong passwords = Higher entropy (complexity + length).
2. Password policies: Regular updates, avoiding reuse.

9 IAM Lifecycle:

1. Account creation → Access provisioning → Access review → Deprovisioning.

---

10 Basic to Advanced Expected Questions with Answers

Basic-Level Questions

What are the three main factors of authentication?

Answer:

1. Something you know (password).
2. Something you have (smart card).
3. Something you are (biometrics).

What is the purpose of Single Sign-On (SSO)?

Answer: To allow users to log in once and access multiple systems without needing to authenticate again.

What is the principle of Least Privilege?

Answer: It ensures that users or systems only have the permissions they need to perform their tasks.

Define False Acceptance Rate (FAR).

Answer: The percentage of unauthorized users wrongly granted access by a biometric system.

Intermediate-Level Questions

How does Mandatory Access Control (MAC) differ from Discretionary Access Control (DAC)?

Answer:

1. MAC: Central authority enforces rules, typically in classified environments (e.g., government).
2. DAC: Resource owners decide access permissions, offering more flexibility.

What are two advantages of Federated Identity Management (FIM)?

Answer:

3. Allows users to use one identity across multiple organizations.
4. Reduces the need to maintain separate identities for different systems.

Explain how RBAC enhances security.

Answer: It assigns access based on roles, minimizing the risk of privilege abuse and simplifying access management.

Advanced-Level Questions

What is the purpose of OAuth, and how does it work?

> **Answer**: OAuth is a token-based protocol for authorization. It allows third-party applications limited access to a user's resources without exposing their credentials.

What is the relationship between SAML and Federated Identity Management?

> **Answer**: SAML (Security Assertion Markup Language) is a protocol that enables Federated Identity Management by allowing secure sharing of identity and authentication data between parties.

Why is the Crossover Error Rate (CER) important in evaluating biometric systems?

> **Answer**: CER indicates the optimal balance between FAR and FRR. A lower CER suggests a more reliable biometric system.

---

5 Scenario-Based Questions

Scenario: **A company uses role-based access control. A marketing manager is promoted to a senior role and gains additional permissions but forgets to relinquish old access rights. Which security principle has been violated?**

> **Answer**: The principle of Least Privilege. Proper access reviews and deprovisioning were not performed.

Scenario: An attacker gains access to a user's account after intercepting their session cookie. How can this risk be mitigated?

> **Answer**: Use session encryption (e.g., HTTPS), implement short session timeouts, and enable MFA.

Scenario: **A bank’s ATM system uses both a physical card (factor 1) and a PIN (factor 2) for authentication. What type of authentication is this?**

> **Answer**: Multifactor Authentication (MFA).

Scenario: **A user logs into an application using SSO. After logging out of the main portal, the session remains active in one of the connected systems. What feature is missing?**

Answer: Single Logout (SLO), which ensures that logging out from one system logs the user out of all linked systems.

Scenario: **A developer accidentally hardcodes passwords in source code stored on a public repository. What IAM risk does this represent?**

Answer: Credential exposure, which could lead to unauthorized access and data breaches.

---

5 Numerical-Based Questions

Question: A password consists of 12 characters, each chosen from 94 possible symbols. Calculate the entropy of the password.

Answer:
Entropy = log⁡2(9412)≈78.9\log_2(94^{12}) \approx 78.9log2(9412)≈78.9 bits.
Explanation: Higher entropy makes brute-force attacks more difficult.

Question: A biometric system has a FAR of 0.02% and an FRR of 0.04%. What does the CER represent?

Answer: CER is the point where FAR = FRR. The CER for this system would be closer to 0.03%, indicating balance.

Question: A brute-force attack targets a system where passwords are 8 characters long and consist of lowercase letters only (26 possibilities). How many attempts are needed?

Answer: 268=208,827,064,57626^8 = 208,827,064,576268=208,827,064,576 attempts.

Question: If a password policy increases the minimum length from 8 to 10 characters with the same 62 possible symbols, how does this impact the search space?

Answer:
Old search space: 628≈218 trillion62^8 \approx 218 \text{ trillion}628≈218 trillion.
New search space: 6210≈8.39 quadrillion62^{10} \approx 8.39 \text{ quadrillion}6210≈8.39 quadrillion.
Explanation: Significantly increases resistance to brute-force attacks.

Question: A biometric system logs 1,000 authentication attempts. 2 unauthorized users are accepted (FAR), and 5 authorized users are rejected (FRR). Calculate the FAR and FRR percentages.

Answer:
FAR = 21,000×100=0.2%\frac{2}{1,000} \times 100 = 0.2\%1,0002 ×100=0.2%.
FRR = 51,000×100=0.5%\frac{5}{1,000} \times 100 = 0.5\%1,0005 ×100=0.5%.

One-Page Summary of Key Points

1. **Core Concepts**: Identification, Authentication, Authorization, and Accounting (IAAA).
2. **Access Control Models**: MAC, DAC, RBAC, ABAC.
3. **Authentication Methods**: Passwords, MFA, biometrics (FAR, FRR, CER).
4. **Federation**: SAML, OAuth, OpenID Connect.
5. **Best Practices**: Least Privilege, Separation of Duties, Periodic Audits.
6. **Access Control Mechanisms**: SSO, FIM, Directory Services.
7. **Password Security**: High entropy, MFA, password rotation.
8. **Common Threats**: Phishing, brute force, privilege escalation.

Exam Tips and Points to Memorize

1. **Biometric Metrics**: FAR, FRR, CER (lower CER = better system).
2. **IAM Principles**: Least Privilege, Separation of Duties.
3. **Key Protocols**: SAML, OAuth, OpenID Connect.
4. **SSO Risks**: Single point of failure mitigated by MFA.
5. **Common Access Control Models**: Know when to apply MAC, DAC, RBAC, ABAC.
6. **Attack Mitigation**: Strong passwords, account lockout policies, encryption.
7. **Password Entropy Formula**:
   Entropy=log⁡2(Possible Symbolsn)\text{Entropy} = \log_2 (\text{Possible Symbols}^n)Entropy=log2 (Possible Symbolsn).
8. **Directory Services**: Examples include Active Directory, LDAP.