Chapter 3: Access Control Concepts - CC Exam Prep

### 🔐 ****Access Control Core Concepts****

| **Term** | **Simple Explanation** |
| --- | --- |
| **Subject** | The person, process, or device that wants to access something (e.g., a user). |
| **Object** | The thing the subject wants to access (e.g., file, database, device). |
| **Rule** | A condition or instruction that decides who can access what. |
| **Access Control** | The method used to allow or block someone from using a system or file. |
| **Principle of Least Privilege** | Only give people the minimum access they need to do their job. |

### 🛡️ ****Access Control Types****

| **Type** | **What It Means** |
| --- | --- |
| **Discretionary Access Control (DAC)** | The owner of the file or resource decides who can access it. |
| **Mandatory Access Control (MAC)** | The system enforces strict rules—users can't change them. |
| **Role-Based Access Control (RBAC)** | Access is based on the user’s role (e.g., admin, guest). |

### 🔐 ****Logical Access Controls (Tech-based)****

| **Term** | **Easy Meaning** |
| --- | --- |
| **Logical Access Controls** | Software or settings that control access to systems. |
| **Technical Controls** | Security steps built into software or hardware (e.g., firewalls). |
| **Log Anomaly** | Strange behavior in system logs that might be suspicious. |
| **Logging** | Recording actions taken on systems for review or investigation. |

### 🚪 ****Physical Access Controls (Real-world)****

| **Examples** | **Simple Explanation** |
| --- | --- |
| **Mantrap** | Two-door entry where one must close before the other opens. |
| **Turnstile** | A one-way rotating gate that lets one person through at a time. |
| **Swipe Cards, Badges, Cameras** | Tools used to allow or monitor access. |

### 👮 ****Security Models & Strategies****

| **Term** | **Simple Meaning** |
| --- | --- |
| **Defense in Depth** | Use multiple layers of security (people + tech + processes). |
| **Layered Defense** | Another term for defense in depth. |
| **Privileged Access Management** | Controlling high-level (admin) accounts very carefully. |
| **Privileged Account** | An account with extra powers, like admin access. |
| **Segregation of Duties** | Make sure no one person can complete a critical task alone. |

### 🔧 ****Provisioning & Management****

| **Term** | **Simple Explanation** |
| --- | --- |
| **User Provisioning** | Creating, updating, or deleting user accounts. |
| **Onboarding** | Giving a new user access to what they need. |
| **Offboarding** | Removing access after a person leaves. |

### 🔐 ****Other Important Terms****

| **Term** | **Simple Meaning** |
| --- | --- |
| **Audit** | Reviewing system activity to make sure security is working. |
| **Encrypt** | Scrambling data so only authorized users can read it. |
| **Firewall** | A system that blocks or allows traffic based on rules. |
| **Insider Threat** | Someone inside the company who could cause harm. |
| **Ransomware** | Malware that locks files and demands money to unlock them. |
| **Unix/Linux/iOS** | Types of operating systems used on different devices. |

# Practice MCQs Based on Chapter 3

1. 1. What does the Principle of Least Privilege mean?

* A. Giving all users admin rights
* B. Giving users no access unless requested
* C. Giving users only the minimum access they need
* D. Giving temporary access for all users

✅ Correct Answer: C

1. 2. Which type of access control is based on user roles?

* A. Discretionary Access Control (DAC)
* B. Mandatory Access Control (MAC)
* C. Role-Based Access Control (RBAC)
* D. Time-Based Access Control

✅ Correct Answer: C

1. 3. What is the main goal of defense in depth?

* A. Create backups regularly
* B. Use one strong firewall
* C. Use many layers of security to protect systems
* D. Hire more staff

✅ Correct Answer: C

1. 4. Which of the following is a physical access control?

* A. Password policy
* B. Encryption key
* C. Security guard
* D. Access logs

✅ Correct Answer: C

1. 5. Who decides access permissions in Discretionary Access Control (DAC)?

* A. The system admin only
* B. The government
* C. The owner of the object
* D. The security team

✅ Correct Answer: C

1. 6. What is a privileged account?

* A. An expired user account
* B. An account with no access
* C. An account with admin-level permissions
* D. A guest account

✅ Correct Answer: C

1. 7. What is user provisioning?

* A. Giving users access, changing or deleting it as needed
* B. Monitoring network logs
* C. Encrypting user files
* D. Blocking unused accounts

✅ Correct Answer: A

1. 8. What is the purpose of a mantrap?

* A. Allowing two people to enter at once
* B. Preventing tailgating by controlling access through two doors
* C. Enhancing video surveillance
* D. Managing user passwords

✅ Correct Answer: B

1. 9. Which one is considered a logical access control?

* A. Guard dog
* B. Swipe card
* C. Configuration setting in a software system
* D. Locked door

✅ Correct Answer: C

1. 10. What is an insider threat?

* A. A hacker from outside
* B. A broken system
* C. A trusted person who may cause harm
* D. A firewall update

✅ Correct Answer: C