Exam Report: 2.3.4 Practice Questions

Date: 1/13/2020 11:04:01 am
Time Spent: 12:42

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 75%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Which type of media preparation is sufficient for media that will be reused in a different security contexts within your organization?

- Destruction
- Sanitization
- Formatting
- Deletion

Explanation

Sanitize media that will be reused in a different security context. *Sanitization* is the process of cleaning a device by having all data remnants removed. Sanitization is necessary because deleting, overwriting, and reformatting does not remove all data remnants, even when performed multiple times.

Formatting is typically sufficient for media that will be reused within the same security context. Destroy media that has reached the end of its useful lifetime.

References

LabSim for Security Pro, Section 2.3.
[All Questions SecPro2017_v6.exm ACC_CTRL_01]

Question 2: Correct

Which of the following is an example of *privilege escalation*?

- Principle of least privilege
- Separation of duties
- Creeping privileges
- Mandatory vacations

Explanation

Creeping privileges occur when a user's job position changes and they are granted a new set of access privileges for their new work tasks, but their previous access privileges are not removed. As a result, the user accumulates privileges over time that are not necessary for their current work tasks. This is a form of privilege escalation.

Principle of least privilege and separation of duties are countermeasures against privilege escalation. Mandatory vacations are used to perform peer reviews, which requires cross-trained personnel and help detect mistakes and fraud.

References

LabSim for Security Pro, Section 2.3.
[All Questions SecPro2017_v6.exm ACC_CTRL_02]

Question 3: Correct

Which security principle prevents any one administrator from having sufficient access to compromise the security of the overall IT solution?

- Separation of duties
- Need to know
- Dual administrator accounts
- Principle of least privilege

Explanation

Separation of duties is the security principle that states that no single user is granted sufficient privileges to compromise the security of an entire environment. Usually, this principle is implemented by dividing administrative privileges among several administrators.

The principle of least privilege states that users should have the minimal amount of access necessary to perform their work tasks. A dual administrator accounts policy of ensures that each administrator has a privileged-level account and a normal user-level account. Need to know is an access control tool used in mandatory access control environments to implement granular control over access to segmented and classified data.

References

LabSim for Security Pro, Section 2.3.
[All Questions SecPro2017_v6.exm ACC_CTRL_03]

Question 4: Correct

You assign access permissions so that users can only access the resources required to accomplish their specific work tasks. Which security principle are you complying with?

- Cross-training
- Principle of least privilege
- Need to know
- Job rotation

Explanation

The principle of least privilege is the assignment of access permissions so that users can only access the resources required to accomplish their specific work tasks.

Job rotation and cross-training involve training groups of employees how to perform multiple job roles and periodically rotating roles. Need to know is a feature of MAC environments where data within your classification level is compartmentalized and requires specific work task needs for privilege access.

References

LabSim for Security Pro, Section 2.3.
[All Questions SecPro2017_v6.exm ACC_CTRL_04]

Question 5: Incorrect

An access control list (ACL) contains a list of users and allowed permissions. What is it called if the ACL automatically prevents access to anyone who is **not** on the list?

- ~~Explicit deny~~
- Implicit allow
- Explicit allow
-

Implicit deny

Explanation

With *implicit deny*, users or groups that are not specifically given access to a resource are denied access. Implicit deny means that there is an assumed or unstated deny that prevents access to anyone not explicitly on the list.

Explicit deny identifies users or objects that are not granted access. Explicit allow specifically identifies the objects that are allowed access. Implicit allow is a policy that allows access unless it is explicitly denied (this ACL type is rarely used).

References

LabSim for Security Pro, Section 2.3.
[All Questions SecPro2017_v6.exm ACC_CTRL_05]

Question 6: Correct

You want to make sure that any reimbursement checks issued by your company cannot be issued by a single person. Which security principle should you implement to accomplish this goal?

- Job rotation
- Separation of duties
- Mandatory vacations
- Implicit deny
- Least privilege

Explanation

Separation of duties is the policy of requiring more than one person participate in completing a task. It helps prevent insider attacks because no one person has end-to-end control, and no one person is irreplaceable.

Job rotation is a technique where users are cross-trained in multiple job positions and responsibilities are regularly rotated between personnel. Job rotation is used for training purposes, but also allows for oversight of past transactions. As jobs rotate, personnel in new positions have the chance to review actions taken by others in that same position and catch security problems.

A requirement for *mandatory vacations* requires employees to take vacations of specified length. These vacations can be used to audit actions taken by the employee and provide a passage of time where problems caused by misconduct could become evident.

The principle of least privilege states that users or groups are given only the access they need to do their job and nothing more. With *implicit deny*, users or groups that are not specifically given access to a resource are denied access.

References

LabSim for Security Pro, Section 2.3.
[All Questions SecPro2017_v6.exm ACC_CTRL_06]

Question 7: Correct

You are concerned that the accountant in your organization might have the chance to modify financial information and steal from the company. You want to periodically have another person take over all accounting responsibilities to catch any irregularities.

Which security principle are you implementing by periodically shifting accounting responsibilities?

- Job rotation
- Need to know
- Least privilege
- Separation of duties

Explicit deny

Explanation

Job rotation is a technique where users are cross-trained in multiple job positions and responsibilities are regularly rotated between personnel. Job rotation can be used for training purposes, but also allows for oversight of past transactions. As jobs rotate, personnel in new positions have the chance to review actions taken by others in that same position and catch security problems.

Separation of duties is the policy of requiring more than one person to complete a task. The principle of least privilege states that users or groups are given only the access they need to do their job and nothing more. With explicit deny, users are specifically prevented from gaining access to a resource. *Need to know* describes the restriction of data that is highly sensitive and is usually referenced in government and military context.

References

LabSim for Security Pro, Section 2.3.
[All Questions SecPro2017_v6.exm ACC_CTRL_07]

Question 8: Incorrect

You want to implement an access control list where only the users you specifically authorize have access to the resource. Anyone not on the list should be prevented from having access.

Which of the following methods of access control will the access list use?

~~Implicit allow, explicit deny~~

Explicit allow, implicit deny

Explicit allow, explicit deny

Implicit allow, implicit deny

Explanation

The access list will use explicit allow--users who are allowed access are specifically identified. The access list will also use implicit deny--users who are not explicitly allowed access are denied access.

Explicit deny identifies users or objects that are denied access. Implicit allow allows access unless it is explicitly denied and is rarely implemented.

References

LabSim for Security Pro, Section 2.3.
[All Questions SecPro2017_v6.exm ACC_CTRL_08]

Question 9: Incorrect

Which of the following principles is implemented in a mandatory access control model to determine object access by classification level?

Need to know

Least privilege

Ownership

Separation of duties

~~Clearance~~

Explanation

Need to know is used with mandatory access control environments to implement granular control over access to segmented and classified data.

Separation of duties is the security principle that states that no single user is granted sufficient privileges to compromise the security of an entire environment. *Clearance* is the subject classification label that grants a user access to a specific security domain in a mandatory access control environment. *Ownership*

is the access right in a discretionary access control environment that gives a user complete control over an object usually because she created it.

References

LabSim for Security Pro, Section 2.3.
[All Questions SecPro2017_v6.exm ACC_CTRL_09]

Question 10: Correct

What is the primary purpose of separation of duties?

- Increase the difficulty of performing administration
- Grant a greater range of control to senior management
- Prevent conflicts of interest
- Inform managers that they are not trusted

Explanation

The primary purpose of separation of duties is to prevent conflicts of interest by dividing administrative powers between several trusted administrators. This prevents a single person from having all of the privileges over an environment, which would create a primary target for attack and a single point of failure.

Increasing administration difficulty, informing managers that they are not trusted, and granting a greater range of control to senior management are not the primary purposes of separation of duties. Separation of duties might seem to increase administrative difficulty, but it provides a significant security benefits. A manager is informed they are not trusted when they are not given any responsibility, as opposed to a reasonable portion of responsibility. Senior management already has full control over their organization.

References

LabSim for Security Pro, Section 2.3.
[All Questions SecPro2017_v6.exm ACC_CTRL_10]

Question 11: Correct

Separation of duties is an example of which type of access control?

- Corrective
- Preventive
- Compensative
- Detective

Explanation

Preventive access controls deter intrusion or attacks (for example, separation of duties or dual-custody processes).

Detective access controls search for details about the attack or the attacker (for example, intrusion detection systems). Corrective access controls implement short-term repairs to restore basic functionality following an attack. Compensative access controls are alternatives to primary access controls.

References

LabSim for Security Pro, Section 2.3.
[All Questions SecPro2017_v6.exm ACC_CTRL_11]

Question 12: Correct

Need to know access is required to access which types of resources?

- Resources with unique ownership
- Low-security resources
-

- Compartmentalized resources
- High-security resources

Explanation

Need to know access is required to retrieve compartmentalized resources. Within any classification level of a MAC environment, data can be compartmentalized and requires the additional access control clearance of need to know for access clearance.

Need to know is not specifically limited to or required by either high- or low-security resources. In a MAC environment, there is no concept of ownership.

References

LabSim for Security Pro, Section 2.3.
[All Questions SecPro2017_v6.exm ACC_CTRL_12]