Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 2/28/2022 2:27:53 pm • Time spent: 09:42

Score: 90%

Passing Score: 80%

Question 1: ✓ Correct

A remote access user needs to gain access to resources on the server. Which of the following processes are performed by the remote access server to control access to resources?

- ○ Identity proofing and authentication
- ○ Identity proofing and authorization
- ○ Authentication and accounting
- ➡ ● Authentication and authorization
- ○ Authorization and accounting

EXPLANATION

A remote access server performs the following functions:

- Authentication is the process of proving identity. After devices agree on the authentication protocol to use, the login credentials are exchanged and login is allowed or denied.
- Authorization is the process of identifying the resources that a user can access over the remote access connection. Authorization is controlled through the use of network policies (remote access policies) as well as access control lists.

Accounting is an activity that tracks or logs the use of the remote access connection. Accounting is used to keep track of resource use but is not typically used to control resource use. If access is allowed or denied based on time limits, information provided by accounting might be used by authorization rules to allow or deny access.

Identification is the initial process of confirming the identity of a user requesting credentials and occurs when a users types in a user ID to log on.

Identity proofing occurs during the identification phase as the user proves that they are who they say they are in order to obtain credentials.

REFERENCES

5.7.2 Network Access Control Facts

6.1.6 Access Control Model Facts

6.3.3 Authorization Facts

6.9.2 Remote Access Facts

q_acct_crtl_authentication_01_secp7.question.fex

Question 2: ✓ Correct

Audit trails produced by auditing activities are which type of security control?

- ○ Directive
- ○ Preventative
- ○ Deterrent
- ➡ ● Detective

EXPLANATION

Audit trails produced by auditing activities are a detective security control. Audit trails are used to detect the occurrence of unwanted or illegal actions by users. Audit trails give administrators the ability to reconstruct historical events and locate aberrant activities. Once an issue is discovered in an audit trail, the collected information can be used to guide the corrective or recovery procedure to restore resources, prevent re-occurrence, and prosecute the perpetrator.

The security function of auditing the activities of user accounts on a secured system is considered a preventative or deterrent security control.

REFERENCES

6.1.3 Access Control Facts

q_acct_crtl_detective_secp7.question.fex

Question 3: ✓ Correct

Which of the following is used for identification?

○ PIN

○ Cognitive question

○ Password

➡ ● Username

EXPLANATION

Identification is the initial process of confirming the identity of a user requesting credentials and occurs when a users types in a user ID to log on. The username is used for identification, while a password, PIN, or some other cognitive information is used for authentication.

Authentication is the verification of the issued identification credentials. It is usually the second step after identification and establishes the user's identity, ensuring that users are who they say they are.

REFERENCES

6.1.3 Access Control Facts

q_acct_crtl_identification_secp7.question.fex

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?

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

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 those 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

6.1.4 Access Control Best Practices

q_acct_bstpract_least_01_secp7.question.fex

Question 5: ✕ Incorrect

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

- ○ Separation of duties
- ➡ ○ Need to Know
- ○ Ownership
- ○ Principle of least privilege
- ● ~~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. This is usually because he or she created the object.

REFERENCES

6.1.4 Access Control Best Practices

q_acct_bstpract_need_secp7.question.fex

▾ Question 6: ✓ Correct

Which of the following is an example of privilege escalation?

➡ ● Privilege creep

○ Separation of duties

○ Mandatory vacations

○ Principle of least privilege

EXPLANATION

Privilege creep occurs when a user's job position changes and he or she is 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

- 2.4.2 Vulnerability Concerns Facts
- 5.9.2 Device Vulnerability Facts
- 6.1.4 Access Control Best Practices

q_acct_bstpract_privilege_secp7.question.fex

Question 7: ✓ Correct

What is the primary purpose of separation of duties?

○ Increase the difficulty of performing administrative duties

○ Inform managers that they are not trusted

○ Grant a greater range of control to senior management

➡ ◉ Prevent conflicts of interest

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 administrative difficulty, informing managers that they are not trusted, or 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 this separation provides 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

6.1.4 Access Control Best Practices

q_acct_bstpract_separate_03_secp7.question.fex

Question 8: ✓ Correct

Which access control model is based on assigning attributes to objects and using Boolean logic to grant access based on the attributes of the subject?

- ○ Role-Based Access Control (RBAC)
- ➡ ● Attribute-Based Access Control (ABAC)
- ○ Rule-Based Access Control
- ○ Mandatory Access Control (MAC)

EXPLANATION

The ABAC model is based on assigning attributes to objects and using Boolean logic to grant access based on the attributes of the subject.

The MAC model is based on classification labels being assigned to objects and clearance labels being assigned to subjects. When a subject's clearance lines up with an objects classification, the subject is granted access.

The RBAC model grants access based on the subject's role in an organization.

The Rule-Based Access Control model grants access based on a set of rules or policies.

REFERENCES

6.1.6 Access Control Model Facts

q_acc_models_abac_secp7.question.fex

Question 9: ✓ Correct

You have implemented an access control method that only allows users who are managers to access specific data. Which type of access control model is being used?

- ○ DAC
- ➡ ● RBAC
- ○ MAC
- ○ DACL

EXPLANATION

Role-based access control (RBAC) allows access based on a role in an organization, not individual users. Roles are defined based on job description or a security-access level. Users are made members of a role and receive the permissions assigned to the role.

Discretionary access control (DAC) assigns access directly to subjects based on the discretion of the owner. Objects have a discretionary access control list (DACL) with entries for each subject. Owners add subjects to the DACL and assign rights or permissions. The permissions identify the actions the subject can perform on the object.

Mandatory access control (MAC) uses labels for both subjects (users who need access) and objects (resources with controlled access). When a subject's clearance lines up with an object's classification, and when the user has a need to know (referred to as a category), the user is granted access.

REFERENCES

6.1.6 Access Control Model Facts

q_acc_models_rbac_02_secp7.question.fex

Question 10: ✓ Correct

Which of the following is an example of rule-based access control?

➡ ● Router access control lists that allow or deny traffic based on the characteristics of an IP packet.

○ A computer file owner who grants access to the file by adding other users to an access control list.

○ A subject with a government clearance that allows access to government classification labels of Confidential, Secret, and Top Secret.

○ A member of the accounting team that is given access to the accounting department documents.

EXPLANATION

A router access control list that allows or denies traffic based on the characteristics of an IP packet is an example of rule-based access control.

A subject with a government clearance that allows access to government classification labels of Confidential, Secret, and Top Secret is an example of mandatory access control.

A member of the accounting team that is given access to the accounting department documents is an example of role-based access control.

A computer file owner who grants access to the file by adding other users to an access control list is an example of discretionary access control.

REFERENCES

6.1.6 Access Control Model Facts

q_acc_models_rule_secp7.question.fex