Exam Report: 8.1.7 Practice Questions

Date: 1/23/2020 3:48:31 pm
Time Spent: 20:37

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 20%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Correct

What form of access control is based on job descriptions?

○ Mandatory access control (MAC)

○ Discretionary access control (DAC)

➡ ◉ Role-based access control (RBAC)

○ Location-based access control (LBAC)

Explanation

RBAC is based on job descriptions.

DAC is based on identity. MAC is based on rules. LBAC is based on geography or logical designations.

References

LabSim for Security Pro, Section 8.1.
[All Questions SecPro2017_v6.exm ACC_MODS_05]

Question 2: Incorrect

Which access control type is used to implement short-term repairs to restore basic functionality following an attack?

➡ ○ Corrective

○ Compensative

◉ ~~Recovery~~

○ Detective

Explanation

Corrective access controls are used for short-term repairs and to restore basic functionality. Following the implementation of corrective controls, an incident might also require *recovery* access control methods, which are long-term activities that restore full functionality.

Compensative access controls are alternatives to primary access controls. *Detective* access controls search for details about the attack or the attacker.

References

LabSim for Security Pro, Section 8.1.
[All Questions SecPro2017_v6.exm ACC_MODS_06]

Question 3: Incorrect

Encryption is which type of access control?

➡ ○ Technical

○ Physical

● ~~Restrictive~~

○ Administrative

Explanation

Technical controls are computer mechanisms that restrict access. Examples are encryption, one-time passwords, access control lists, and firewall rules.

Administrative controls are policies that describe accepted practices. Examples are directive policies and employee awareness training. Physical controls restrict physical access. Examples are perimeter security, site location, networking cables, and employee segregation.

References

LabSim for Security Pro, Section 8.1.
[All Questions SecPro2017_v6.exm ACC_MODS_07]

▼ **Question 4:** Incorrect

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

➡ ○ Detective

○ Deterrent

○ Directive

● ~~Preventative~~

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

LabSim for Security Pro, Section 8.1.
[All Questions SecPro2017_v6.exm ACC_MODS_08]

▼ **Question 5:** Correct

Which access control model is based on multilevel security where objects are assigned a security classification and subjects are granted a security clearance which allows them to access objects at or below that security classification?

➡ ● Mandatory Access Control (MAC)

○ Attribute-Based Access Control (ABAC)

○ Role-Based Access Control (RBAC)

○ Discretionary Access Control (DAC)

Explanation

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

The DAC model grants access directly to subjects based on the object owners discretion.
The RBAC model grants access based on the subjects role in an organization.

The ABAC model grants access when the subject meets all the attributes that are assigned to an object.

References

LabSim for Security Pro, Section 8.1.
[All Questions SecPro2017_v6.exm ACC_MODS_21||/]

▼ **Question 6:** Incorrect

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?

● ~~Rule-Based Access Control~~

➡ ○ Attribute-Based Access Control (ABAC)

○ Role-Based Access Control (RBAC)

○ 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 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 subjects role in an organization.

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

References

LabSim for Security Pro, Section 8.1.
[All Questions SecPro2017_v6.exm ACC_MODS_23||/]

▼ **Question 7:** Incorrect

Which of the following is an example of a Rule Based Access Control (RBAC)?

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

➡ ○ Router access control lists that allows or denies traffic based on the characteristics of an IP packet?

● ~~A member of the accounting team is given access to the accounting department documents.~~

○ A subject with a government clearance that allows access to government classification labels of confidential, secret and top secret.

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 is given access to the accounting department documents is an example of Role-Based Access Control.

A computer file owner grants access to the file by adding other users to an access control list is an example of Discretionary Access Control.

References

LabSim for Security Pro, Section 8.1.
[All Questions SecPro2017_v6.exm ACC_MODS_22||/]

Question 8: Incorrect

Which form of access control enforces security based on user identities and allows individual users to define access controls over owned resources?

○ MAC

➡ ○ DAC

● ~~RBAC~~

○ TBAC

Explanation

DAC (discretionary access control) uses identities to control resource access. Users can make their own decisions about how much access to grant to other users.

RBAC (role-based access control), MAC (mandatory access control), and TBAC (task-based access control) enforce security based on rules.

- The rules of RBAC are job descriptions
- The rules of MAC are classifications
- The rules of TBAC are work tasks

References

LabSim for Security Pro, Section 8.1.
[All Questions SecPro2017_v6.exm ACC_MODS_09]

Question 9: Incorrect

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 used?

○ MAC

○ DACL

● ~~DAC~~

➡ ○ RBAC

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 (or decision) 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

LabSim for Security Pro, Section 8.1.
[All Questions SecPro2017_v6.exm ACC_MODS_13]

Question 10: Incorrect

You have a system that allows the owner of a file to identify users and their permissions to the file. Which type of access control model is implemented?

● ~~RBAC (based on rules)~~

○ MAC

○ RBAC (based on roles)

➡ ○ DAC

Explanation

This is an example of a discretionary access control list (DACL), which uses the Discretionary Access Control (DAC) model. With DAC, individuals use their own discretion (decisions or preferences) for assigning permissions and allowing or denying access.

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.

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.

Rule-based access control (RBAC) uses characteristics of objects or subjects along with rules to restrict access. Access control entries identify a set of characteristics that are be examined for a match. If all characteristics match, access is either allowed or denied based on the rule.

References

LabSim for Security Pro, Section 8.1.
[All Questions SecPro2017_v6.exm ACC_MODS_14]

▼ **Question 11:** Incorrect

A router access control list uses information in a packet, such as the destination IP address and port number, to make allow or deny forwarding decisions.

This is an example of which kind of access control model?

○ MAC

● ~~DAC~~

○ RBAC

➡ ○ RSBAC

Explanation

Rule set-based access control (RSBAC) uses characteristics of objects or subjects along with rules to restrict access. Access control entries identify a set of characteristics that are examined for a match. If all characteristics match, access is either allowed or denied based on the rule. An example of a rule-based access control implementation is a router access control list that allows or denies traffic based on characteristics within the packet (such as IP address or port number).

Discretionary access control (DAC) assigns access directly to subjects based on the discretion (or decision) 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.

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.

References

LabSim for Security Pro, Section 8.1.
[All Questions SecPro2017_v6.exm ACC_MODS_15]

▼ **Question 12:** Incorrect

Which of the following is the term for the process of validating a subject's identity?

➡ ○ Authentication

○ Auditing

○ Authorization

● ~~Identification~~

Explanation

Authentication is the process of validating a subject's identity. It includes the identification process, the user providing input to prove identity, and the system accepting that input as valid.

Authorization is granting or denying a subject's access to an object based on the level of permissions or the actions allowed on the object. *Identification* identifies the subject. Examples include a user name or a user ID number. *Auditing* is maintaining a record of a subject's activity within the information system.

References

LabSim for Security Pro, Section 8.1.
[All Questions SecPro2017_v6.exm ACC_MODS_16]

Question 13: Incorrect

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

● ~~Authentication and accounting~~

○ Identity proofing and authorization

➡ ○ 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.

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

References

LabSim for Security Pro, Section 8.1.
[All Questions SecPro2017_v6.exm ACC_MODS_18]

Question 14: Incorrect

Which of the following defines an *object* as an entity in the context of access control?

➡ ○ Data, applications, systems, networks, and physical space.

○ Users, applications, or processes that need to be given access.

○ Resources, policies, and systems.

● ~~Policies, procedures, and technologies that are implemented within a system.~~

Explanation

Objects are entities that represent data, applications, systems, networks, and physical space.

Subjects are the users, applications, or processes that need access to objects. The access control system includes the policies, procedures, and technologies that are implemented to control a subject's access to an object.

References

LabSim for Security Pro, Section 8.1.
[All Questions SecPro2017_v6.exm ACC_MODS_19]

▼ **Question 15:** Correct

Which access control model manages rights and permissions based on job descriptions and responsibilities?

○ Task-based access control (TBAC)

➡ ● Role-based access control (RBAC)

○ Mandatory access control (MAC)

○ Discretionary access control (DAC)

Explanation

Role-based access control (RBAC) is the access control model that manages rights and permissions based on job descriptions. RBAC focuses on job descriptions or work tasks instead of employing user accounts to define access. RBAC is best suited for environments that have a high rate of employee turnover. By defining access based on roles rather than individuals, administration is simplified when granting a new person access to common activities.

DAC is based on user accounts. MAC is based on security labels, classifications, or clearances. TBAC is based on work tasks.

References

LabSim for Security Pro, Section 8.1.
[All Questions SecPro2017_v6.exm ACC_MODS_20]