Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 3/1/2022 7:26:56 pm • Time spent: 05:00

Score: 80%

Passing Score: 80%

Question 1: ✔ Correct

Which security mechanism uses a unique list that meets the following specifications:

- The list is embedded directly in the object itself.
- The list defines which subjects have access to certain objects.
- The list specifies the level or type of access allowed to certain objects.

- ➡ ◉ User ACL
- ○ Conditional access
- ○ Mandatory access control
- ○ Hashing

EXPLANATION

A user ACL (user access control list) is a security mechanism that defines which subjects have access to certain objects and the level or type of access allowed. This security mechanism is unique for each object and embedded directly in the object itself.

Mandatory access control (MAC) is an access control system based on classifications of subjects and objects to define and control access.

Conditional access is a way to enforce access control while also encouraging users to be productive wherever they are.

Hashing is a cryptographic tool that creates an identification code that is employed to detect changes in data.

REFERENCES

4.3.3 File Permission Facts

5.3.2 Firewall Facts

5.13.3 Router Security Facts

6.3.3 Authorization Facts

q_authorize_acl_secp7.question.fex

Question 2: ✕ Incorrect

What is the process of controlling access to resources such as computers, files, or printers called?

- Authentication
- ~~Conditional access~~
- Mandatory access control
- Authorization

EXPLANATION

Authorization is the process of controlling access to resources such as computers, files, or printers.

Mandatory access control (MAC) is an access control system based on classifications of subjects and objects to define and control access.

Conditional access is a way to enforce access control while also encouraging users to be productive wherever they are.

Authentication is the verification of the issued identification 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_authorize_authorize_secp7.question.fex

Question 3: ✔ Correct

Which of the following objects identifies a set of users with similar access needs?

- Group
- DACL
- SACL
- Permissions

EXPLANATION

A group is an object that identifies a set of users with similar access needs. Microsoft systems have two kinds of groups, distribution groups and security groups. Only security groups can be used for controlling access to objects.

A discretionary access control list (DACL) is an implementation of discretionary access control (DAC).

A system access control list (SACL) is used by Microsoft for auditing in order to identify past actions performed by users on an object.

Permissions define the rights and access users and groups have with objects.

REFERENCES

6.3.3 Authorization Facts

q_authorize_group_secp7.question.fex

Question 4: ✔ Correct

Which of the following identifies the type of access that is allowed or denied for an object?

- User rights
- Permissions
- SACL
- DACL

EXPLANATION

Permissions define the rights and access users and groups have with objects. Permissions are applied to objects such as files and folders.

A discretionary access control list (DACL) is an implementation of discretionary access control (DAC).

On a Microsoft system, a user right is a privilege or action that can be taken on a system, such as logging on, shutting down, backing up the system, or modifying the system date and time.

A system access control list (SACL) is used by Microsoft for auditing in order to identify past actions performed by users on an object.

REFERENCES

6.3.3 Authorization Facts

q_authorize_permission_secp7.question.fex

Question 5: ✔ Correct

Which of the following is used by Microsoft for auditing in order to identify past actions performed by users on an object?

- Permissions
- DACL
- User rights
- SACL

EXPLANATION

A system access control list (SACL) is used by Microsoft for auditing in order to identify past actions performed by users on an object.

A discretionary access control list (DACL) is an implementation of discretionary access control (DAC).

On a Microsoft system, a user right is a privilege or action that can be taken on a system, such as logging on, shutting down, backing up the system, or modifying the system date and time.

Permissions define the rights and access users and groups have with objects. Permissions are applied to objects such as files and folders.

REFERENCES

4.3.3 File Permission Facts

5.3.2 Firewall Facts

5.13.3 Router Security Facts

6.3.3 Authorization Facts

q_authorize_sacl_secp7.question.fex

Question 6: ✔ Correct

Which type of group can be used for controlling access to objects?

- Authorization
- DACL
- Distribution
- Security

EXPLANATION

Only security groups can be used for controlling access to objects.

A discretionary access control list (DACL) is an implementation of discretionary access control (DAC).

Distribution groups cannot be used for controlling access to objects.

Authorization is the process of controlling access to resources such as computers, files, or printers.

REFERENCES

6.3.3 Authorization Facts

q_authorize_security_secp7.question.fex

Question 7: ✔ Correct

Marcus White has just been promoted to a manager. To give him access to the files that he needs, you make his user account a member of the Managers group, which has access to a special shared folder.

Later that afternoon, Marcus tells you that he is still unable to access the files reserved for the Managers group. What should you do?

- Add his user account to the ACL for the shared folder.
- Manually refresh Group Policy settings on his computer.
- Manually refresh Group Policy settings on the file server.
- ➡ Have Marcus log off and log back in.

EXPLANATION

On a Microsoft system, an access token is only generated during authentication. Changes made to group memberships or user rights do not take effect until the user logs in again and a new access token is created.

Use NTFS and share permissions, not Group Policy, to control access to files. In addition, Group Policy is periodically refreshed, and new settings are applied on a regular basis.

REFERENCES

6.3.3 Authorization Facts

q_authorize_token_01_secp7.question.fex

Question 8: ✔ Correct

Which of the following terms describes the component that is generated following authentication and is used to gain access to resources following login?

- Account policy
- Proxy
- Cookie
- ➡ Access token

EXPLANATION

When a security principal logs on, an access token is generated. The access token is used to control access to resources and contains the following information:

- The security identifier (SID) for the user or computer
- The SID for all groups the user or computer is a member of
- User rights granted to the security principal

When the security principal tries to access a resource or take an action, information in the access token is checked. For example, when a user tries to access a file, the access token is checked for the SID of the user and all groups. The SIDs are then compared to the SIDs in the object's DACL to identify permissions that apply.

Account policies in Group Policy control requirements for passwords, such as minimum length and expiration times.

Cookies are text files that are stored on a computer to save information about your preferences, browser settings, and web page preferences. Cookies identify you (or your browser) to websites.

A proxy is a server that stands between a client and destination servers.

REFERENCES

6.3.3 Authorization Facts

q_authorize_token_02_secp7.question.fex

Question 9: ✕ Incorrect

Lori Redford, who has been a member of the Project Management group, was recently promoted to manager of the team. She has been added as a member of the Managers group.

Several days after being promoted, Lori needs to have performance reviews with the team she manages. However, she cannot access the performance management system. As a member of the Managers group, she should have the Allow permission to access this system.

What is MOST likely preventing her from accessing this system?

- ~~She is still a member of the Project Management group, which has been denied permission to this system. However, being a member of the Managers group should allow her to access this system. Allow permissions always override Deny permissions. There must be an explicit permission entry that is preventing her from accessing the management system.~~
- Her user object has been assigned an explicit Deny permission to the performance management system.
- ➡ She is still a member of the Project Management group, which has been denied permission to this system. Deny permissions always override Allow permissions.
- Her user object has been assigned an explicit Allow permission to the performance management system, but she inherited the Deny permission assigned to the Project Management group (which she still belongs to). Inherited Deny permissions override explicit Allow permissions.

EXPLANATION

The most likely cause of this problem is that Lori is still a member of the Project Management group, which has been denied permission to this system. Deny permissions always override Allow permissions.

Allow permissions do not override Deny permissions unless the Allow permission is explicitly assigned and the Deny permission is inherited. It is unlikely that her user object has been assigned an explicit Deny permission to the performance management system since best practice is to assign permissions to groups, not to users.

REFERENCES

6.3.3 Authorization Facts

q_authorize_token_03_secp7.question.fex

Question 10: ✔ Correct

Which of the following is a privilege or action that can be taken on a system?

- Permissions
- DACL
- User rights
- SACL

EXPLANATION

On a Microsoft system, a user right is a privilege or action that can be taken on a system, such as logging on, shutting down, backing up the system, or modifying the system date and time. User rights apply to the entire system.

A discretionary access control list (DACL) is an implementation of discretionary access control (DAC).

Microsoft uses a system access control list (SACL) for auditing in order to identify past actions performed by users on an object.

Permissions define the rights and access users and groups have with objects. Permissions are applied to objects such as files and folders.

REFERENCES

6.3.3 Authorization Facts

q_authorize_user_secp7.question.fex