Exam Report: 8.3.5 Practice Questions

Date: 1/23/2020 4:37:20 pm
Time Spent: 8:54

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 40%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

Which of the following information is typically **not** included in an access token?

- User rights
- Group membership
- ~~User security identifier~~
- User account password

Explanation

The access token does not contain the user account password. The password is only used during authentication. Following authentication, the access token is used to gain access to resources.

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

- The 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.

References

LabSim for Security Pro, Section 8.3.
[All Questions SecPro2017_v6.exm AUTHORIZE_01]

Question 2: 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
- Access token
- Proxy
- Cookie

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 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. They identify you (or your browser) to websites. A *proxy* is a server that stands between a client and destination servers.

References

LabSim for Security Pro, Section 8.3.
[All Questions SecPro2017_v6.exm AUTHORIZE_03]

Question 3: Incorrect

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
- Have Marcus log off and log back in
- ~~Manually refresh Group Policy settings on the file server~~

Explanation

On a Microsoft system, the 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, with new settings applied on a regular basis.

References

LabSim for Security Pro, Section 8.3.
[All Questions SecPro2017_v6.exm AUTHORIZE_02]

Question 4: Incorrect

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

- Hashing
- User ACL
- Kerberos
- ~~Mandatory access control~~

Explanation

A user ACL (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. Kerberos is a form of single sign-on that uses hashed passwords to verify a user's identity. Hashing is a cryptographic tool that creates an identification code that is employed to detect changes in data.

References

LabSim for Security Pro, Section 8.3.
[All Questions SecPro2017_v6.exm AUTHORIZE_04]

Question 5: Correct

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 but 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. Deny permissions always override Allow permissions.
- ( ) Her user object has been assigned an explicit Deny permission to the performance management system.
- ( ) Her user object has been assigned an explicit Allow permission to the performance management system, but she inherits the Deny permission assigned to the Project Management group (which she still belongs to). Inherited Deny permissions override explicit Allow permissions.
- ( ) 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.

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

LabSim for Security Pro, Section 8.3.
[All Questions SecPro2017_v6.exm AUTHORIZE_05]