Exam Report: 2.15.3 Practice Questions - Section 2.15

Date: 11/22/2015 11:40:44 pm
Time Spent: 11:48

Candidate: Belskis, Tomas
Login: t0mas9lt

Overall Performance

Your Score: 50%

Passing Score: 80%

Certification Ranking

Within your class:　　Within your school:　　Nationally:

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Correct

In an Identity Management System, what is the function of the Authoritative Source?

○ Coordinate the management of user identity across system boundaries.

➡ ● Specify the owner of a data item.

○ Remove a user from the system and revoke user rights to system resources.

○ Obtain the current password for a user through the p-sync system.

Explanation

Most items of data associated with identity have a conceptual owner. The owner of a data item is considered the *authoritative source* for the item. In general, only the authoritative source for a data item is allowed to make changes to the data item.

References

LabSim for Security Pro, Section 2.15.
[Questions.exm MI 4]

Question 2: Incorrect

In an Identity Management System, what is the function of the Identity Vault?

○ Implement the P-sync system.

● ~~Store the user's access to resources.~~

○ Coordinate the management of user identity across system boundaries.

➡ ○ Ensure that each employee has the appropriate level of access in each system.

Explanation

The Identity Vault serves as a repository for the identity of each user in the organization. Each user has an identity account that specifies the user's access to resources.

The identity vault becomes the authoritative source for each of the systems within the organization. The rights and restrictions identified for the user in the identity vault are applied to each of the systems.

References

LabSim for Security Pro, Section 2.15.
[Questions.exm MI 5]

Question 3: Correct

Because each of these systems uses its own unique set of authentication credentials, you must spend a considerable amount of time each week keeping user account information updated on each system. In addition, if a user changes his or her password on one system, it is not updated for the user's accounts on the other two systems.

Which should you do? (Select two. Each response is a part of the complete solution.)

□ Migrate the NoSQL database to Microsoft SQL Server.

□ Migrate GroupWise to Microsoft Exchange.

➡ ☑ Implement password synchronization.

➡ ☑ Implement an Identity Vault.

□ Migrate the Novell Open Enterprise Server system to Windows Server.

□ Migrate the Linux server to Windows Server.

Explanation

You should implement an Identity Management (IDM) system in this scenario. IDM centralizes management of user identity across all systems in an organization. To do this, you would:

- Implement an Identity Vault. The Identity Vault serves as repository for the identity of each user in the organization. Each user has an identity account that specifies the user's access to resources. The identity vault becomes the authoritative source for each of the systems within the organization. The rights and restrictions identified for the user in the identity vault are applied to each of the systems.
- Implement password synchronization. Password synchronization (P-sync) is a self-service password system implemented through IDM. P-sync increases efficiency and security by allowing users to manage their passwords throughout the system. P-sync allows users to access resources across the various systems with a single password.

In this scenario, it is not necessary to migrate any of the server systems to Windows Server or to migrate the GroupWise e-mail service to Microsoft Exchange. Migrating from a NoSQL database to a Microsoft SQL server database would be problematic as both systems use very different data structures. In addition, NoSQL is better suited to big data analysis than Microsoft SQL server.

References

LabSim for Security Pro, Section 2.15.
[Questions.exm RT-2.15-1]

Question 4: Incorrect

~~Identity Vault~~	Automated Provisioning

Allows users to manage their passwords throughout all systems

✓ Password Synchronization

Acts as the authoritative source for user credentials for each connected system

~~Automated Provisioning~~ Identity Vault

Serves as repository for the identity of each user

~~Automated De-provisioning~~ Identity Vault

Defines a permission a user has to access resources in connected systems

~~Authoritative Source~~ Entitlement

Removes a user from all systems and revokes all rights

~~Entitlement~~ Automated De-provisioning

Explanation

The following terms are used when describing an IDM deployment:

- An Identity Vault serves as repository for the identity of each user in the organization. Each user has an identity account that specifies the user's access to resources. The identity vault becomes the authoritative source for each of the systems within the organization. The rights and restrictions identified for the user in the identity vault are applied to each of the systems.
- *Automated provisioning* refers to Identity Management's ability to synchronize all aspects of user creation across all systems in an organization.
- *Automated de-provisioning* refers to the ability to remove the user from the system and revoke user rights to system resources when the user leaves the company.
- *Password synchronization* (P-sync) is a self-service password system implemented through IDM. P-sync increases efficiency and security by allowing users to manage their passwords throughout the system. P-sync allows users to access resources across the various systems with a single password.
- An *entitlement* defines the permissions a user has to access resources in the connected system.

References

LabSim for Security Pro, Section 2.15.
[Questions.exm RT-2.15-2]