Exam Report: 2.12.7 Practice Questions - Section 2.12

Date: 11/22/2015 5:09:15 pm
Time Spent: 3:11

Candidate: Belskis, Tomas
Login: t0mas9lt

Overall Performance

Your Score: 0%

Passing Score: 80%

Certification Ranking

Within your class: Within your school: Nationally:

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

You manage a single domain named widgets.com.

Organizational units (OUs) have been created for each company department. User and computer accounts have been moved into their corresponding OUs.

You define a password and account lockout policy for the domain. However, members of the Directors OU want to enforce longer passwords than are required for the rest of the users.

You need to make the change as easily as possible. Which should you do?

- Create a GPO linked to the Directors OU. Configure the password policy in the new GPO.
- Create a new domain. Move the contents of the Directors OU to the new domain. Configure the necessary password policy on the domain.
- Implement a granular password policy for the users in the Directors OU.
- In Active Directory Users and Computers, select all user accounts in the Directors OU. Edit the user account properties to require the longer password.

Explanation

Use granular password policies to force different password policy requirements for different users.

Password and account lockout policies are enforced only in GPOs linked to the domain, not to individual OUs. Prior to Windows Server 2008, the only way to configure different password policies was to create a different domain.

References

LabSim for Security Pro, Section 2.12.
[Questions.exm RT-SP-2.12-1]

Question 2: Incorrect

You manage a single domain named widgets.com.

Organizational units (OUs) have been created for each company department. User and

computer accounts have been moved into their corresponding OUs. You define a password and account lockout policy for the domain. However, members of the Directors OU want to enforce longer passwords than are required for the rest of the users.

You would like to define a granular password policy for these users. Which tool should you use?

- Active Directory Users and Computers
- Active Directory Sites and Services
- ADSI Edit
- Group Policy Management Console and Group Policy Management Editor
- Active Directory Domains and Trusts

Explanation

Use ADSI Edit or the Active Directory module for Windows PowerShell to define granular password policies.

Use the Group Policy Management Console and the Group Policy Management Editor to define password policies for an entire domain.

References

LabSim for Security Pro, Section 2.12.
[Questions.exm RT-SP-2.12-2]

Question 3: Incorrect

You manage a single domain named widgets.com.

Organizational units (OUs) have been created for each company department. User and computer accounts have been moved into their corresponding OUs. You define a password and account lockout policy for the domain. However, members of the Directors OU want to enforce longer passwords than are required for the rest of the users.

You need to make the change as easily as possible. Which should you do?

- Create a granular password policy. Apply the policy to all users in the Directors OU.
- Create a granular password policy. Create a distribution group. Apply the policy to the group. Add all users in the Directors OU to the group.
- Create a granular password policy. Apply the policy to all users in the widgets.com domain.
- Create a granular password policy. Apply the policy to the Directors OU.

Explanation

To use granular password policies:

- Create the Password Settings Object (PSO) with the necessary settings.
- Edit the msDS-PSOAppliesTo property in the PSO to identify the users or global security groups to which the policy applies.
- If the policy was applied to a group, add members to the group.

The msDS-PSOAppliesTo property in the PSO identifies the users to which the policy applies.

Using ADSI Edit, you can apply the policy to any object. However, only policies applied to user accounts or global security groups will be effective. To apply a policy to all users in an OU, add each user to the msDS-PSOAppliesTo property or use a global security group. Granular password policies cannot be applied to an e-mail distribution group.

References

LabSim for Security Pro, Section 2.12.
[Questions.exm RT-SP-2.12-3]

Question 4: Incorrect

You manage a single domain named widgets.com.

Organizational units (OUs) have been created for each company department. User and computer accounts have been moved into their corresponding OUs. Members of the Directors OU want to enforce longer passwords than are required for the rest of the users.

You define a new granular password policy with the required settings. All users in the Directors OU are currently members of the DirectorsGG group, a global security group in that OU. You apply the new password policy to that group. Matt Barnes is the chief financial officer. He would like his account to have even more strict password policies than is required for other members in the Directors OU.

Which should you do?

- Edit the existing password policy. Define exceptions for the required settings. Apply the exceptions to Matt's user account.
- Create a granular password policy for Matt. Apply the new policy directly to Matt's user account. Remove Matt from the DirectorsGG group.
- Create a granular password policy for Matt. Create a new group, and then make Matt a member of the group. Apply the new policy directly to the new group. Make sure the new policy has a higher precedence value than the value for the existing policy.
- Create a granular password policy for Matt. Apply the new policy directly to Matt's user account.

Explanation

To use a different set of policies for a specific user, create a PSO for the user, and apply it directly to the user account. If a PSO has been applied directly to a user, that PSO is in effect—regardless of the precedence value.

You could create a second group only for Matt's account and password policy. However, this policy must have a lower precedence value than the value set for the policy applied to the DirectorsGG group. Removing Matt's account from the DirectorsGG group is unnecessary and would probably affect his permissions to network resources.

References

LabSim for Security Pro, Section 2.12.
[Questions.exm RT-SP-2.12-5]

Question 5: Incorrect

Match each smart card attack on the left with the appropriate description on the right.

Software Attacks

Exploiting vulnerabilities in the card's protocols or encryption methods

Eavesdrop
ping

Capturing transmission data produced by the card as it is used

Fault
Generation

Deliberately inducing malfunctions in the card

Microprobi
ng

Accessing the chip surface directly to observe, manipulate, and interfere with the circuit

Explanation

Smart cards are subject to the following weaknesses:

- *Microprobing* is the process of accessing the chip surface directly to observe, manipulate, and interfere with the circuit.
- *Software attacks* exploit vulnerabilities in the card's protocols or encryption methods.
- *Eavesdropping* captures transmission data produced by the card as it is used.
- *Fault generation* deliberately induces malfunctions in the card.

References

LabSim for Security Pro, Section 2.12.
[Questions.exm RT-SP-2.12-6]