Exam Report: 7.4.6 Practice Questions

Date: 1/22/2020 5:14:07 pm
Time Spent: 1:36

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 40%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Which of the following solutions would you use to control the actions that users can perform on a computer, such as shutting down the system, logging on through the network, or loading and unloading device drivers?

- Group Policy
- NTFS permissions
- Account policies
- Account restrictions

Explanation

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

Account policies are specific Group Policy settings that control user passwords. Account restrictions are settings applied in the user account that restrict login hours or computers. Use NTFS permissions to control actions that users can perform on specific files or folders.

References

LabSim for Security Pro, Section 7.4.
[All Questions SecPro2017_v6.exm HARDEN_ENFORCE_01]

Question 2: Correct

For users who are members of the sales team, you want to force computers to use a specific desktop background and remove access to administrative tools from the Start menu.

Which solution should you use?

- Account restrictions
- Account policies
- File screens
- Group Policy

Explanation

Use Group Policy to control the desktop for groups of users or computers. For example, you can prevent access to specific desktop or Start menu features.

Account policies are specific Group Policy settings that control user passwords. Account restrictions are settings applied in the user account that restrict login hours or computers. Use file screens to control the types of files that can be saved within a folder.

References

LabSim for Security Pro, Section 7.4.
[All Questions SecPro2017_v6.exm HARDEN_ENFORCE_02]

Question 3: Incorrect

Arrange the Group Policy ojects (GPOs) in the order in which they are applied.

1
~~GPOs linked to the organizational unit that contains the object.~~
The Local Group Policy on the computer.

2
✓ GPOs linked to the domain that contains the user or computer object.

3
~~The Local Group Policy on the computer.~~
GPOs linked to the organizational unit that contains the object.

Explanation

GPOs are applied in the following order:

1. The Local Group Policy on the computer.
2. GPOs linked to the domain that contains the user or computer object.
3. GPOs linked to the organizational unit(s) that contain(s) the object (from the highest-level OU to the lowest-level OU).

References

LabSim for Security Pro, Section 7.4.
[All Questions SecPro2017_v6.exm HARDEN_ENFORCE_03]

Question 4: Incorrect

Match the Group Policy type on the left with the function that it can perform on the right. (Each item can be used more than once.)

Software that should be installed on a specific computer. ✓ Computer Configuration	Software that should be installed for a specific user. ✓ User Configuration	Scripts that should run at startup or shutdown. ✓ Computer Configuration
Scripts that should run at logon or logoff. ~~Computer Configuration~~ User Configuration	Network communication security settings. ✓ Computer Configuration	

Explanation

The default domain policy is separated into two areas, computer configuration and user configuration. Computer policies are applied as soon as the system is booted. User policies are not applied until the user logs in. Computer policies include:

- Software that should be installed on a specific computer
- Scripts that should run at startup or shutdown
- Password restrictions that must be met for all user accounts
- Network communication security settings
- Registry settings that apply to the computer (the HKEY_LOCAL_MACHINE subtree)

User policy settings include:

- Software that should be installed for a specific user
- Scripts that should run at login or logoff
- Internet Explorer user settings (such as favorites and security settings)
- Registry settings that apply to the current user (the HKEY_CURRENT_USER subtree)

References

LabSim for Security Pro, Section 7.4.
[All Questions SecPro2017_v6.exm HARDEN_ENFORCE_04]

Question 5: Incorrect

Which of the following is a snap-in that allows you to apply a template or compare a template to the existing security settings on your computer?

- The NSA Template snap-in
- The Microsoft Management Console snap-in
- ~~The Active Directory Security Template snap-in~~
- The Security Configuration and Analysis snap-in

Explanation

The Security Configuration and Analysis snap-in allows you to apply a template or compare a template to the existing security settings on your computer. This snap-in can be used for auditing to see if security settings configured in the past have been changed. A good security practice is to check the security setting frequently (every day if possible) to ensure that the controls set are still in effect and the system stays hardened.

You can obtain templates from the NSA that have predefined security settings the NSA considers appropriate for various Windows operating systems (but is not like a snap-in, which can be run regularly). The Microsoft Management Console (MMC) snap-ins are used with many group policy objects in Active Directory. There is no Active Directory Security Template snap-in.

References

LabSim for Security Pro, Section 7.4.
[All Questions SecPro2017_v6.exm HARDEN_ENFORCE_05]