Exam Report: 8.13.11 Practice Questions

Date: 1/27/2020 9:10:16 pm
Time Spent: 2:00

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 27%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

Which of the following is the single best rule to enforce when designing complex passwords?

- Longer passwords
- Computer-generated passwords
- ~~Force use of all four types of characters (uppercase, lowercase, numbers, symbols)~~
- Maximum password age

Explanation

The best rule for complex passwords is this: the longer is better. The longer a password is, the harder a password cracking tool must work to break or guess the password.

Computer-generated passwords may be complex, but they are usually difficult to remember. The more difficult a password is to remember, the more likely it is that someone will write it down, making it insecure. Maximum password age is important, but a short password changed often is weaker than a long password that is static for a longer period of time. Requiring the use of all four character types is important, but not as important as overall password length.

References

LabSim for Security Pro, Section 8.13.
[All Questions SecPro2017_v6.exm HRDN_USR_AUTH_01]

Question 2: Incorrect

For users on your network, you want to automatically lock user accounts if four incorrect passwords are used within 10 minutes.

What should you do?

- ~~Configure account expiration in the user accounts~~
- Configure password policies in Group Policy
- Configure the enable/disable feature in the user accounts
- Configure day/time restrictions in the user accounts
- Configure account lockout policies in Group Policy

Explanation

Account lockout disables a user account after a specified number of incorrect login attempts. The account lockout threshold identifies the number of incorrect login attempts. The account lockout counter identifies a time period for keeping track of incorrect attempts (such as 10 minutes) .

If account lockout locks a user account, use the unlock feature to allow login. Use the enable/disable

feature to prevent or allow login using the user account.

Configure account (password) policies in Group Policy to enforce rules about the composition of passwords, such as minimum length, complexity, and history requirements. Use account expiration in a user account to disable an account after a specific day. Use day/time restrictions to prevent login during certain days or hours.

References

LabSim for Security Pro, Section 8.13.
[All Questions SecPro2017_v6.exm HRDN_USR_AUTH_02]

Question 3: Correct

You want to make sure that all users have passwords over eight characters in length and that passwords must be changed every 30 days.

What should you do?

- Configure account lockout policies in Group Policy
- Configure expiration settings in the user accounts
- Configure account policies in Group Policy
- Configure day/time settings in the user accounts

Explanation

Configure account (password) policies in Group Policy to enforce rules about the composition of passwords, such as minimum length, complexity, and history requirements.

Use account expiration in a user account to disable an account after a specific day. Use day/time restrictions to prevent login during certain days or hours. Account lockout disables a user account after a specified number of incorrect login attempts.

References

LabSim for Security Pro, Section 8.13.
[All Questions SecPro2017_v6.exm HRDN_USR_AUTH_03]

Question 4: Incorrect

You have hired 10 new temporary workers who will be with the company for 3 months.

How can you make sure that these users can only log on during regular business hours?

- Configure account lockout in Group Policy
- ~~Configure account policies in Group Policy~~
- Configure account expiration in the user accounts
- Configure day/time restrictions in the user accounts

Explanation

Use day/time restrictions to limit the days and hours when users can log on.

Configure account expiration to disable an account after a specific date. Use account policies in Group Policy to configure requirements for passwords. Use account lockout settings in Group Policy to automatically lock accounts when a specific number of incorrect passwords are entered.

References

LabSim for Security Pro, Section 8.13.
[All Questions SecPro2017_v6.exm HRDN_USR_AUTH_04]

Question 5: Correct

You are configuring the local security policy of a Windows system. You want to prevent users from reusing old passwords. You also want to force them to use a new password for at least five days before changing it again.

Which policies should you configure? (Select two.)

- [ ] Password complexity
- [x] Minimum password age
- [ ] Maximum password age
- [x] Enforce password history

Explanation

Set the Enforce password history policy to prevent users from reusing old passwords. Set the Minimum password age policy to prevent users from changing passwords too soon. Passwords must remain the same for at least the time period specified.

Use the Maximum password age policy to force periodic changes to the password. After the maximum password age has been reached, the user must change the password. Use the Password complexity to require that passwords include letters, numbers, and symbols. This makes it harder for hackers to guess or crack passwords.

References

LabSim for Security Pro, Section 8.13.
[All Questions SecPro2017_v6.exm HRDN_USR_AUTH_05]

Question 6: Incorrect

You are configuring the Local Security policy of a Windows system. You want to require users to create passwords that are at least 10 characters long. You also want to prevent login after three unsuccessful login attempts.

Which policies should you configure? (Select two.)

- [ ] Enforce password history
- [x] ~~Maximum password age~~
- [ ] Account lockout threshold
- [x] Minimum password length
- [ ] Account lockout duration
- [ ] Password complexity

Explanation

Set the Minimum password length policy to require a password equal to or longer than the specified length. Set the Account lockout threshold policy to lock an account after the specified number of incorrect login attempts.

The following lists explains the incorrect policy choices for this scenario:

- Enforce password history requires users to input a unique (previously unused) password when changing the password. This prevents users from reusing previous passwords.
- Maximum password age forces users to change the password after the specified time interval.
- Password complexity prevents using passwords that are easy to guess or easy to crack. It forces passwords to include letters, symbols, and numbers, and also requires passwords of at least seven characters. However, you cannot configure a longer password length requirement with this policy.
- Account lockout duration determines the length of time the account is disabled (in minutes). When the time period expires, the account is unlocked automatically.

References

LabSim for Security Pro, Section 8.13.
[All Questions SecPro2017_v6.exm HRDN_USR_AUTH_06]

Question 7: Correct

You have just configured the password policy and set the minimum password age to 10.

What will be the effect of this configuration?

- The password must be entered within 10 minutes of the login prompt being displayed.
- The previous 10 passwords cannot be reused.
- ➡ Users cannot change the password for 10 days.
- The password must contain 10 or more characters.
- Users must change the password at least every 10 days.

Explanation

The minimum password age setting prevents users from changing the password too frequently. After the password is changed, it cannot be changed again for at least 10 days.

The maximum password age setting determines how frequently a password must be changed. The minimum password length setting controls the minimum number of characters in the password. Password history is used to prevent previous passwords from being reused.

References

LabSim for Security Pro, Section 8.13.
[All Questions SecPro2017_v6.exm HRDN_USR_AUTH_07]

Question 8: Incorrect

You have implemented account lockout with a clipping level of 4.

What will be the effect of this setting?

- ~~Password hashes will be generated using a salt value of four.~~
- Incorrect login attempts during the past four hours will be tracked.
- Locked accounts will remain locked for four hours.
- ➡ The account will be locked after four incorrect attempts.

Explanation

The clipping level specifies the number of incorrect attempts that will trigger account lockout. In this example, four incorrect passwords would lock the user account.

Account lockout duration specifies how long the account remains locked. Incorrect login attempts are typically cleared after a successful login or after a predetermined time passes. The salt value is a random value that ensures that hashes of the same password result in different hashes.

References

LabSim for Security Pro, Section 8.13.
[All Questions SecPro2017_v6.exm HRDN_USR_AUTH_08]

Question 9: Incorrect

Which of the following is **not** an important aspect of password management?

- Train users to create complex passwords that are easy to remember.
- ➡ Enable account lockout.
- Always store passwords in a secure medium.
- ~~Prevent use of personal information in a password.~~

Explanation

Account lockout is not a password management mechanism; rather, it is an access control mechanism to protect against attempted compromise of user accounts.
Password management includes preventing personal information in passwords, training users on how to create complex passwords that are easy to remember, and ensuring that passwords are always stored securely.

References

LabSim for Security Pro, Section 8.13.
[All Questions SecPro2017_v6.exm HRDN_USR_AUTH_09]

Question 10: Incorrect

You are teaching new users about security and passwords.

Which of the following is the best example of a secure password?

- ~~Stiles_2031~~
- T1a73gZ9!
- 8181952
- JoHnSmITh

Explanation

The most secure password is T1a73gZ9! because it is eight or more characters in length and combines upper and lowercase characters, special symbols, and numbers.

The least secure password is 8181952 because it appears to be a birthday. JoHnSmITh is not secure because it is still a name. Stiles_2031 is more secure, but not as secure as random numbers and letters.

References

LabSim for Security Pro, Section 8.13.
[All Questions SecPro2017_v6.exm HRDN_USR_AUTH_10]

Question 11: Incorrect

Upon running a security audit in your organization, you discover that several sales employees are using the same domain user account to log in and update the company's customer database.

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

- ~~Apply the Group Policy object to the container where the sales user accounts reside.~~
- Delete the account that the sales employees are currently using.
- ~~Implement a Group Policy object that implements time-of-day login restrictions.~~
- Implement a Group Policy object that restricts simultaneous logins to one.
- Train sales employees to use their own user accounts to update the customer database.

Explanation

You should prohibit the use of shared user accounts. Allowing multiple users to share an account increases the likelihood of the account being compromised. Because the account is shared, users tend to take security for the account less seriously. In the scenario, the following tasks need to be completed:

- The existing shared user account needs to be deleted. Until you delete the account, users will continue to use it for authentication. You could just change the password on the account, but there is a high chance that the new password would be shared again.
- Train sales employees to use their own user accounts to update the customer database. Ensure that these accounts have the level of access required for users to access the database.

Applying time of day or concurrent logon restrictions in a Group Policy object will not address the issue in this scenario.

References

LabSim for Security Pro, Section 8.13.
[All Questions SecPro2017_v6.exm HRDN_USR_AUTH_11]