Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 3/2/2022 7:46:46 pm • Time spent: 03:45

Score: 50% Passing Score: 80%

Question 1: ✔ 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 day/time settings in user accounts
- Configure account lockout policies in Group Policy
- ➡ Configure account policies in Group Policy
- Configure expiration settings in 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

6.6.9 Hardening Authentication Facts

q_harden_auth_complex_01_secp7.question.fex

Question 2: ✔ Correct

You are teaching new users about security and passwords.

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

- Stiles_2031
- T1a73gZ9! ➡
- JoHnSmITh
- 8181952

EXPLANATION

The most secure password is T1a73gZ9! because it is eight or more characters in length and combines uppercase 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

6.6.9 Hardening Authentication Facts

q_harden_auth_complex_03_secp7.question.fex

Question 3: ✔ 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.)

- [x] Minimum password age
- [ ] Maximum password age
- [ ] Password must meet complexity requirements
- [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 must meet complexity requirements* policy to require that passwords include letters, numbers, and symbols. This makes it harder for hackers to guess or crack passwords.

REFERENCES

6.6.9 Hardening Authentication Facts

q_harden_auth_history_secp7.question.fex

Question 4: ✕ Incorrect

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

What should you do?

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

EXPLANATION

Account lockout disables a user account after a specified number of incorrect login attempts. The account lockout threshold identifies the allowed 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

6.6.9 Hardening Authentication Facts

q_harden_auth_lockout_secp7.question.fex

Question 5: ✔ Correct

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

What is the effect of this configuration?

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

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 that must be in the password. Password history is used to prevent previous passwords from being reused.

REFERENCES

6.6.9 Hardening Authentication Facts

q_harden_auth_reuse_secp7.question.fex

Question 6: ✕ 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 part of a complete solution.)

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

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 can 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 login restrictions in a Group Policy object does not address the issue in this scenario.

REFERENCES

6.6.9 Hardening Authentication Facts

q_harden_auth_rshared_secp7.question.fex

Question 7: ✕ Incorrect

You have hired ten new temporary employees to be with the company for three months.

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

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

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

6.6.9 Hardening Authentication Facts

q_harden_auth_time_secp7.question.fex

Question 8: ✔ Correct

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

Software attacks

✔ Exploits vulnerabilities in a card's protocols or encryption methods

Eavesdropping

✔ Captures transmission data produced by a card as it is used

Fault generation

✔ Deliberately induces malfunctions in a card

Microprobing

✔ Accesses the chip's surface directly to observe, manipulate, and interfere with a circuit

EXPLANATION

Smart cards are subject to the following weaknesses:

- Microprobing is the process of accessing a chip's 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 a card.

REFERENCES

6.6.12 Smart Card Authentication Facts

q_smartcard_auth_attack_secp7.question.fex

Question 9: ✕ 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 of the following actions should you take?

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

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

6.6.12 Smart Card Authentication Facts

q_smartcard_auth_complex_01_secp7.question.fex

Question 10: ✕ 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, which is a global security group in that OU. You apply the new password policy to that group. Matt Barnes is the chief financial officer, and he would like his account to have even more strict password policies than are required for other members in the Directors OU.

What should you do?

- Create a granular password policy for Matt. Apply the new policy directly to Matt's user account. Remove Matt from the DirectorsGG group.
- 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.
- ~~Create a granular password policy for Matt. Create a new group, make Matt a member of the group, and then 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.~~

EXPLANATION

To use a different set of policies for a specific user, create a Password Settings Object (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

6.6.12 Smart Card Authentication Facts

q_smartcard_auth_complex_02_secp7.question.fex