Exam Report: 13.7.11 Practice Questions

Date: 4/15/2020 5:02:43 pm
Time Spent: 1:56

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 47%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

Which of the following is an example of a strong password?

- a8bT11$yi
- Robert694
- at9iov45a
- desktop#7

Explanation

A strong password should not contain dictionary words or any part of the login name. They should include upper- and lower-case letters, numbers, and symbols. In addition, longer passwords are stronger than shorter passwords.

References

TestOut PC Pro - 13.7 Authentication
[e_auth_pp6.exam.xml Q_SEC_POL_01]

Question 2: 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 logon after three unsuccessful logon attempts.

Which of the following policies are BEST to configure? (Select TWO).

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

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 logon attempts.

Incorrect policy choices for this scenario include 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 7 characters. However, you cannot configure a longer password length requirement with this policy. Account lockout duration determines the length of time the account will be disabled (in minutes). When the time period expires, the account will be unlocked automatically.

References

TestOut PC Pro - 13.7 Authentication
[e_auth_pp6.exam.xml Q_SEC_POL_02]

Question 3: Incorrect

While trying to log on, a user accidentally typed the wrong password three times, and now the system is locked because he entered too many incorrect passwords. He still remembers his password, but he just typed it wrong. He needs access as quickly as possible.

Which of the following would allow the user to log on?

- ~~Change the password for the account~~
- Enable the account
- Have the user wait for the account to be unlocked automatically
- Unlock the account

Explanation

With the account lockout policy configured, an account will be locked (and cannot be used for logon) when a specified number of incorrect passwords are entered. You can unlock a locked account by editing the account properties in Local Users and Groups. Depending on the policy settings, locked accounts might be unlocked automatically after a period of time. However, to allow immediate access, manually unlock the account.

A disabled account cannot be used for logon. Accounts are not disabled automatically, and enabling an account does not unlock it. Changing the password is not required because the user still remembers the correct password.

References

TestOut PC Pro - 13.7 Authentication
[e_auth_pp6.exam.xml Q_SEC_POL_03]

Question 4: Correct

You manage two computers with the following user accounts:

• Wrk1 has user accounts Mary and Admin. The Mary account does not have a password set; the Admin account does.

You are working from Wrk2 and would like to access a shared folder on Wrk1.

Which of the following credentials would BEST allow you to access the shared folder?

- Type 'Mary' for the username and leave the password blank.
- Type 'Mary' for the username and specify the password.
- Type 'Admin' for the username and specify the password.
- Type 'Julia' for the username and leave the password blank.

Explanation

Type Admin for the username and specify the password. To access a shared folder or use Remote Desktop for a workgroup computer, you must supply a username and password that matches a user account configured on the computer you are trying to access. For Wrk1, you would use either Mary or Admin for the user account name. You cannot use the Mary account to access Wrk1 over the network. When accessing shared folders or Remote Desktop on a network computer, the user account must have been configured with a password. User accounts with blank passwords cannot be used to gain network access to a computer.

References

TestOut PC Pro - 13.7 Authentication
[e_auth_pp6.exam.xml Q_SEC_POL_04]

Question 5: Incorrect

A user is trying to log into her notebook computer. She enters the correct password for her user account, but the system won't let her authenticate, claiming the wrong password has been entered.

Which of the following is MOST likely causing the problem?

- The Scroll Lock key has been pressed, locking all input from the keyboard.
- The keyboard must be replaced.
- ~~The CPU is in power save mode, causing all login attempts to be denied.~~
- She has entered the wrong password too many times, causing Intruder Detection in Windows to lock the system.
- She has enabled Num Lock, causing numbers to be sent from the keyboard instead of letters.

Explanation

The most likely cause of this user's problem is that the Num Lock key sequence for the notebook system has been pressed causing the keyboard to send numbers in the place of letters. Turning Num Lock off should fix the problem.

References

TestOut PC Pro - 13.7 Authentication
[e_auth_pp6.exam.xml Q_SEC_POL_05]

Following your Windows installation, you enabled the built-in Administrator account. You remove the password for this account. You enable Remote Desktop on your computer using the default settings. From home, you try to access your computer using Remote Desktop using the Administrator account, but you are unable to log on.

Which of the following MUST be completed before you can access your computer using Remote Desktop?

- Unlock the Administrator account.
- Configure a password for the Administrator account.
- Disable fast user switching on the computer.
- ~~Make the Administrator account a member of the Remote Desktop Users group.~~

Explanation

When you access shared folders or Remote Desktop on a network computer, the user account must be configured with a password. User accounts with blank passwords cannot be used to gain network access to a computer. By default, members of the Administrators group are allowed Remote Desktop access. To allow non-administrators access, add them to the list of authorized users for Remote Desktop. The user accounts you specify are made members of the Remote Desktop Users group. Accounts are locked automatically through the account lockout settings when too many incorrect passwords have been entered. Fast user switching is only configurable on Windows XP and does not affect users' ability to log on with Remote Desktop.

References

TestOut PC Pro - 13.7 Authentication
[e_auth_pp6.exam.xml Q_SEC_POL_06]

Question 7: Incorrect

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 of the following policies are BEST to configure? (Select TWO).

- [x] ~~Maximum password age~~
- [ ] Minimum password length
- [x] Minimum password age
- [ ] Password complexity
- [ ] 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

References

TestOut PC Pro - 13.7 Authentication
[e_auth_pp6.exam.xml Q_SEC_POL_07]

Question 8: Incorrect

Employees currently access a data center using RFID badges. The company is concerned that an unauthorized person could gain access using a lost or stolen badge.

Which of the following could be implemented to increase the physical security?

- Security tokens
- Key fobs
- Biometric locks
- ~~Smart cards~~

Explanation

Biometric locks require a user to authenticate with a unique personal attribute such as their iris, fingerprint, or voice.

Smart cards can be lost or stolen as easily as any other badge. Key fobs contain a security code that changes at predetermined intervals. Like badges, they can be lost or stolen. Tokens are the security components used in devices to provide the holder of the token the proper access level. They can be transmitted via card readers, magnetic swipes, or wireless communication. The company's current RFID badges would include these tokens.

References

TestOut PC Pro - 13.7 Authentication
[e_auth_pp6.exam.xml Q_SEC_AUTH2_01]

Question 9: Incorrect

An employee working from home accesses the company network using a VPN connection. When connecting, the employee is prompted for a PIN that changes at predetermined intervals.

Which of the following will the employee MOST likely use to obtain the PIN?

- Entry control roster
- ~~RFID badge~~
- Fingerprint reader
- Key fob

Explanation

A key fob can be issued to the employee that presents a security code or PIN that changes at predetermined intervals. This PIN is synchronized to the master security system and provides authentication to initialize the VPN connection.

References

TestOut PC Pro - 13.7 Authentication
[e_auth_pp6.exam.xml Q_SEC_AUTH2_02]

Question 10: Correct

Which of the following is not a form of biometrics?

- Fingerprint
- Smart card
- Face recognition
- Retina scan

Explanation

A smart card is used in token-based authentication, so it is not a form of biometrics. Biometrics rely on personal characteristics (such as fingerprints, facial recognition, or a retina scan) to prove identity. A smart card is an example of the something you have authentication factor.

References

TestOut PC Pro - 13.7 Authentication
[e_auth_pp6.exam.xml Q_SEC_AUTH2_03]

Question 11: Correct

What do biometrics use to authenticate identity?

- Knowledge of passwords
- Biological attributes
- Possession of a device
- Ability to perform tasks

Explanation

Biometrics is based on biological attributes. Biometrics is a strong form of authentication because each person has unique characteristics. When these unique characteristics are used for authentication, they are more reliable and stronger than the best passwords. For example, no two people have the exact same fingerprint or retina pattern.

References

TestOut PC Pro - 13.7 Authentication
[e_auth_pp6.exam.xml Q_SEC_AUTH2_04]

Question 12: Incorrect

Which of the following security technologies stores identification information in a magnetic strip, radio frequency transmitter, or hardware contact to authorize access to a computer?

- SSID
- ~~Key fob~~
- Smart card
- ID badge

Explanation

A smart card contains identification information stored on a magnetic strip, radio frequency transmitter, or hardware contact that allow it to interact with a smart card reader to authorize access. The reader uses information on the card to allow or deny access.

A biometric is a physical characteristic of a human that can be scanned to control access. A key fob can be used for accessing an automobile, but is not used for computer access. An ID badge can be just a picture with a name on it and may or may not also be a smart card. In Windows, the Local Security Policy is a collection of settings that control how the system behaves. The SSID is the name of a wireless network.

References

TestOut PC Pro - 13.7 Authentication
[e_auth_pp6.exam.xml Q_SEC_AUTH2_05]

Question 13: Correct

Which of the following is the most common form of authentication?

- Username and password
- Photo ID
- Digital certificate on a smart card
- Fingerprint

Explanation

Passwords are the most common form of authentication. Most secure systems require only a username and password to provide users with access to the computing environment. Many forms of online intrusion attacks focus on stealing passwords. This makes using strong passwords very important. Without a strong password policy and properly trained users, the reliability of your security system is greatly diminished.

Photo ID, fingerprint, and digital certificate on a smart card are not the most common forms of authentication.

References

TestOut PC Pro - 13.7 Authentication
[e_auth_pp6.exam.xml Q_SEC_AUTH2_06]

Question 14: Correct

Which type of biometric authentication uses the ridges of your skin?

- [x] Fingerprint
- [ ] Face scan
- [ ] Keystroke dynamics

Explanation

Fingerprint biometrics use the ridges of your skin, which are known as ridge minutiae.

Retina scans use blood vein patters, facial scans use a facial pattern, and keystroke dynamics use a behavioral system.

References

TestOut PC Pro - 13.7 Authentication
[e_auth_pp6.exam.xml Q_SEC_AUTH2_07]

Question 15: Correct

Which of the following security measures is a form of biometrics?

- [ ] TPM
- [x] Fingerprint scanner
- [ ] BIOS password
- [ ] Chassis intrusion detection

Explanation

A fingerprint scanner is a type of biometrics. The fingerprint scanner uses the ridges of your skin known as ridge minutiae.

A Trusted Platform Module (TPM) is a special chip on the motherboard that generates and stores cryptographic keys to verify that the hardware has not changed. This value can be used to prevent the system from booting if the hardware has changed. Chassis intrusion detection helps you identify when a system case has been opened. A BIOS password controls access to the BIOS setup program.

References

TestOut PC Pro - 13.7 Authentication
[e_auth_pp6.exam.xml Q_SEC_AUTH2_08]