3 LESSON

Understanding Security Policies

OBJECTIVE DOMAIN MATRIX

Skill/Concept	Exam Objective	Objective Number
Using Password Policies to Enhance Security	Understand password policies	2.3
Protecting Domain User Account Passwords	Understand password policies	2.3

KEY TERMS

acceptable use policy
account lockout
cracked password
Credential Guard
Device Guard
fine-grained password policy
Group Policy Object (GPO)
password policy
Password Settings Object (PSO)
security policy
sniffers
strong password
virtual secure mode (VSM)

One of the foundations of information security is the protection of networks, systems, and most important of all, data. At the foundation of all information security policies, procedures, and processes is the need to protect data.

At the foundation of much of today's data protection is the password. Think about your life. Passwords are used to secure voice mail, ATM access, an email account, a Facebook account, and a host of other things. In order to keep these accounts secure, it is important to select strong passwords. In this lesson, we will be discussing what goes into creating a strong password, and how to configure password settings to ensure that passwords in an environment stay secure.

Let's take a minute and think about a specific instance where a strong password is critical. A good example is an ATM password—that's the password (or PIN) that is needed to keep someone from using your ATM card to steal your money.

■ Using Password Policies to Enhance Security

THE BOTTOM LINE

There are a variety of configuration settings that can be used on systems to ensure that users are required to set and maintain strong passwords. As hard as it can be to believe, left to their own devices, many users will still select weak passwords when securing their accounts. With user education and system controls, users can reduce the risk of weak passwords compromising their applications.

CERTIFICATION READY
How can a company enforce the use of stronger passwords?
Objective 2.3

A basic component of an information security program is ensuring that employees select and use ***strong passwords***. The strength of a password can be determined by examining the length, complexity, and randomness of the password.

Microsoft provides several controls that can be used to ensure the security associated with passwords is maintained. These include:

- Password complexity
- Account lockout
- Password length
- Password history
- Time between password changes
- Group Policies that enforce password security
- Education on common attack methods

Using Password Complexity to Make a Stronger Password

Password complexity deals with the characters used to make up the password. A complex password will use characters from at least three of the following categories:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Numeric characters (0 through 9)
- Non-alphanumeric characters (such as !, @, #, $, %, ^, &)

Microsoft's password complexity settings, when enabled, require characters from three of these categories by default on domain controllers, and the domain can be configured to require this setting for all passwords.

The password complexity settings can either be enabled or disabled. There are no additional configurations available.

There is one very important thing to be aware of when enforcing password complexity. It is not a guarantee that users will not still use easily guessable passwords. The password "Summer2010" meets the current complexity guidelines required by the Windows password complexity setting. It's also a terrible password, because it is very easily guessable and memorable should someone only catch a quick glimpse of it.

Some password selection methods that should be avoided include words that can be found in a dictionary, derivatives of user IDs, and common character sequences such as "123456" or "QWERTY." Likewise, personal details such as a spouse's/partner's name, license plate, Social Security number, and birthday should be avoided. Finally, avoid passwords that are based on proper names, geographical locations, common acronyms, and slang terms.

Some methods for selecting strong passwords include:

- Bump characters in a word a certain number of letters up or down the alphabet. A shift three letters translation of "AArdvark!!" becomes "DDvgzdvn!!"
- Create acronyms from words in a song, a poem, or another known sequence of words. The phrase "Ask not what you can do for your country?" yields the password "Anwycdfyc?" Add $$ to arrive at the strong password $$Anwycdfyc?
- Combine a number of personal facts like birthdates and favorite colors, foods, and so on with special characters to create passwords like: "##Yell0w419" or "$^327p!zZ@"

TAKE NOTE* One of the easiest ways to set a complex password is to start with a dictionary word and use character substitution to make it complex. For example, *computer* becomes C0mput3r. However, be sure to not use words that are easy to guess—like *computer*!

Using Account Lockout to Prevent Hacking

Account lockout refers to the number of incorrect logon attempts permitted before the system will lock the account. Each bad logon attempt increments the bad logon counter, and when the counter exceeds the account lockout threshold, no further logon attempts will be permitted.

This setting is critical because one of the most common password attacks (discussed later in the lesson) involves repeatedly attempting to logon with guessed passwords. Microsoft provides three separate settings with respect to account lockout:

- **Account lockout duration:** This setting determines the length of time a lockout will remain in place before another logon attempt can be made. This can be set from 0 to 99,999 minutes. If set to 0, an administrator will need to manually unlock the account; no automatic unlocking will occur.
- **Account lockout threshold:** This setting determines the number of failed logons permitted before the account lockout occurs. This can be set from 0 (no account lockouts) to 999 attempts before lockout.
- **Reset account lockout counter after:** This setting determines the period of time, in minutes, that must elapse before the account lockout counter is reset to 0 bad logon attempts. If an account lockout threshold is set, the reset account lockout threshold must be less than or equal to the account lockout duration.

Commonly, account lockout settings range from 3 to 10 attempts, with the account lockout duration setting and the reset account lockout counter after setting usually set anywhere from 30 to 60 minutes. While some users complain when they don't get as many attempts to log on as they can use, this is a critical configuration to set to ensure that an environment remains secure.

Examining Password Length

The length of a password is a key component of ensuring the strength of a password. Password length is the number of characters used in a password. A password with 2 characters is considered very insecure, because there is a very limited set of unique passwords that can be made using 2 characters. A 2-character password is considered trivial to guess.

On the other side of the spectrum is the 14-character password. While extremely secure relative to a 2-character password, a 14-character password is very difficult for most users to remember. This is when they generally start breaking out the note paper and writing the passwords down, defeating any security benefits that might have been gained from requiring a 14-character password in the first place.

The trick to setting a minimum password length is balancing usability with security. Microsoft permits setting a minimum password length ranging from 1 to 14 characters (a setting of 0 means no password is required, which is never the appropriate setting in a production environment). The generally accepted minimum password length is 8 characters.

Using Password History to Enforce Security

Password history is the setting that determines the number of unique passwords that must be used before a password can be reused. This setting prevents the recycling of the same passwords through a system. The longer the period of time a password is used, the greater the chance it can be compromised.

Microsoft allows a password history setting between 0 and 24. A fairly common setting in standard environments is 10, although Windows Server 2008 and higher defaults to 24 for domain controllers and domain member computers.

Setting Time Between Password Changes

The final password setting to be aware of is the time between password changes. Two settings are available:

- **Minimum Password Age:** The minimum password age setting controls how many days a user must wait before they can reset their password. This can be set to a value from 1 to 998 days. If set to 0, passwords can be changed immediately. Using a setting that is too low could allow users to defeat the password history settings. For example, if this is set to 0, and the password history is set to 10, all a user would need to do is reset their password 10 times, one right after another, and then they could go back to their original password. This setting must be set to a lower value than the maximum password age, unless the maximum password age is set to 0, which means passwords never expire. A good setting is typically 10 days or more, although this can vary widely depending on administrator preferences.
- **Maximum Password Age:** The maximum password age setting controls the maximum period of time permitted before a user is forced to reset their password. This can be set from 1 to 999 days, or to 0 if passwords are set to never expire. A general rule for this setting is 90 days for user accounts, although for administrative accounts, it's generally a good idea to reset the passwords more frequently. In high security areas, 30 days is not an uncommon setting.

TAKE NOTE*

Passwords should always expire, unless under unique circumstances, such as service accounts for running applications. While this may add some additional administrative overhead to some processes, passwords that don't expire can be a serious security issue in virtually all environments.

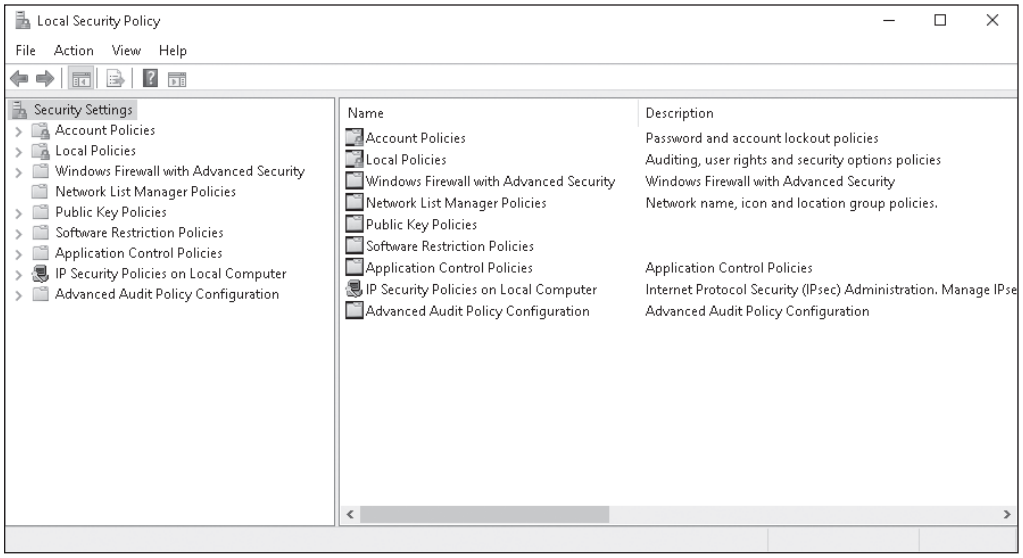
We have discussed the different settings that can be used to ensure the best password security for an environment. Let's look at how to review those settings on a Windows 10 workstation.

REVIEW THE PASSWORD SETTINGS ON A WINDOWS 10 WORKSTATION

GET READY. Before you begin these steps, launch the Administrative Tools, Local Security Policy (see Figure 3-1). To review the password settings on a Windows 10 workstation, perform the following steps.

Figure 3-1

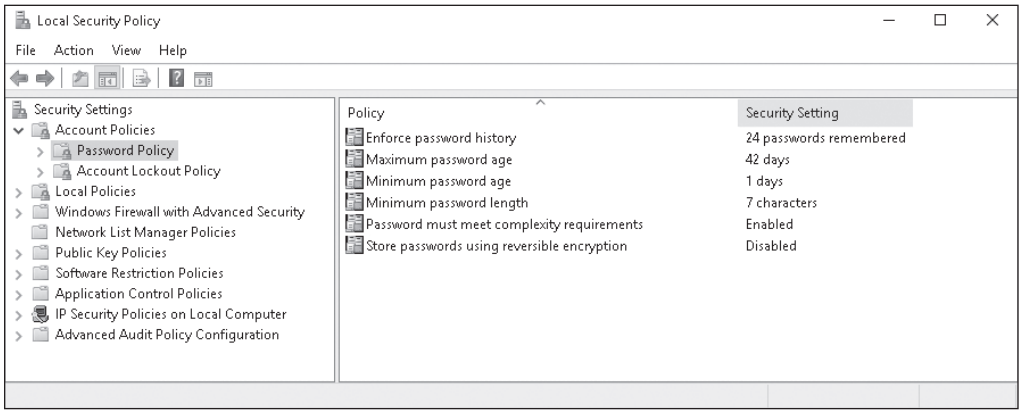
The Local Security Policy window



1. In the Local Security Policy snap-in, click **Account Policies**.
2. Double-click **Password Policy**. The password settings we've discussed appear in the right pane. See Figure 3-2.

Figure 3-2

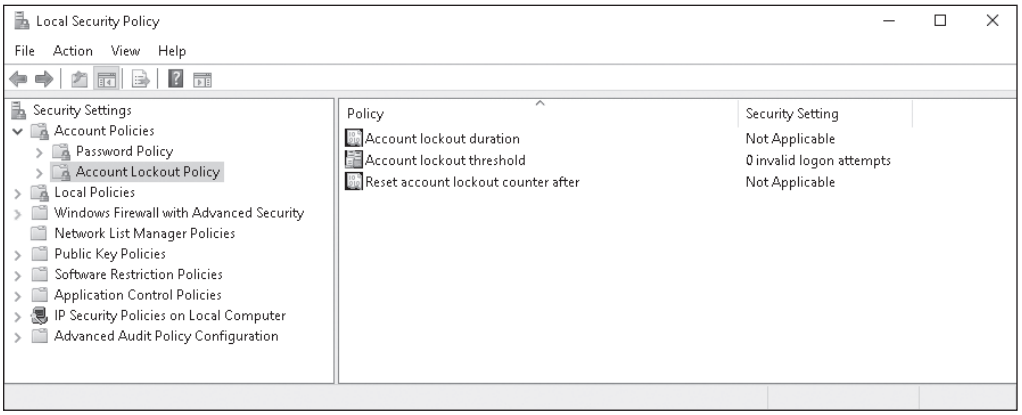
The password settings available as part of the Password Policy



3. Click **Account Lockout Policy**. The account lockout settings we've discussed appear in the right pane. See Figure 3-3.

Figure 3-3

The account lockout settings available as part of the Account Lockout Policy



TAKE NOTE*

The password settings for a Windows Server 2016 domain are configured differently than on a standalone host or client. In the example, we are reviewing the current password settings. We'll look at changing them using a GPO in the next section.

Now that we have looked at setting these policies on a local client, let's take a look at how Group Policies can be used to set these properties for members of a domain.

Using Password Group Policies to Enforce Password Security

Before we look at using a Group Policy to enforce password settings, we should probably discuss the details of a Group Policy (also known as a Group Policy Object).

A ***Group Policy Object (GPO)*** is a set of rules which allow an administrator granular control over the configuration of objects in Active Directory (AD), including user accounts, operating systems, applications, and other AD objects. GPOs are used for centralized management and configuration of the Active Directory environment. Let's look at how we can use GPOs to enforce password controls in Active Directory.

TAKE NOTE*

Windows Server 2008 fundamentally changed the mechanism for setting password attributes in Active Directory. We will look at the legacy GPO model for enforcing password controls as well as a high-level example of how to perform a similar function in a Windows Server 2016 Active Directory.

USE A GROUP POLICY TO ENFORCE PASSWORD CONTROLS ON SYSTEMS IN A DOMAIN

GET READY. Before you begin these steps, be sure to log on to a Windows Server 2016 domain controller as domain administrator. To use a group policy to enforce password controls on systems in a domain, perform the following steps.

1. In Server Manager, click **Tools > Group Policy Management**.
2. In the Group Policy Management window, if necessary, expand **Forest: Adatum.com > Domains > Adatum.com**.
3. Right-click the **Default Domain Policy** GPO and choose **Edit**.

4. In the Group Policy Management Editor window, navigate to the **Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy** node.
5. Click the **Account Lockout Policy** node.
6. After configuring the settings as needed, close the **Group Policy Object Editor**.
7. Close the Group Policy Management window.

Configuring and Applying Password Settings Objects

If it is necessary to use different password policies for different sets of users, use fine-grained password policies, which are applied to user objects or global security groups.

CERTIFICATION READY
Which Active Directory feature provides fine-grained password policies?
Objective 2.3

Fine-grained password policies allow you to specify multiple password policies within a single domain so that different restrictions for password and account lockout policies can be applied to different sets of users in a domain. To use a fine-grained password policy, the domain functional level must be at least Windows Server 2008. To enable fine-grained password policies, first create a ***Password Settings Object (PSO)***. Then, configure the same settings that are configured for the password and account lockout policies. In the Windows Server 2016 environment, PSOs can be created and applied by using the Active Directory Administrative Center (ADAC) or Windows PowerShell.

CREATE AND CONFIGURE THE PASSWORD SETTINGS CONTAINER

GET READY. To create and configure the Password Settings Container, perform the following steps.

1. Open **Server Manager**.
2. Click **Tools > Active Directory Administrative Center**. The ADAC opens.
3. In the ADAC navigation pane, click the arrow next to the domain and click the **System** folder. Then, scroll down and double-click **Password Settings Container**.
4. In the Tasks pane, click **New > Password Settings**. The Create Password Settings window opens (see Figure 3-4).

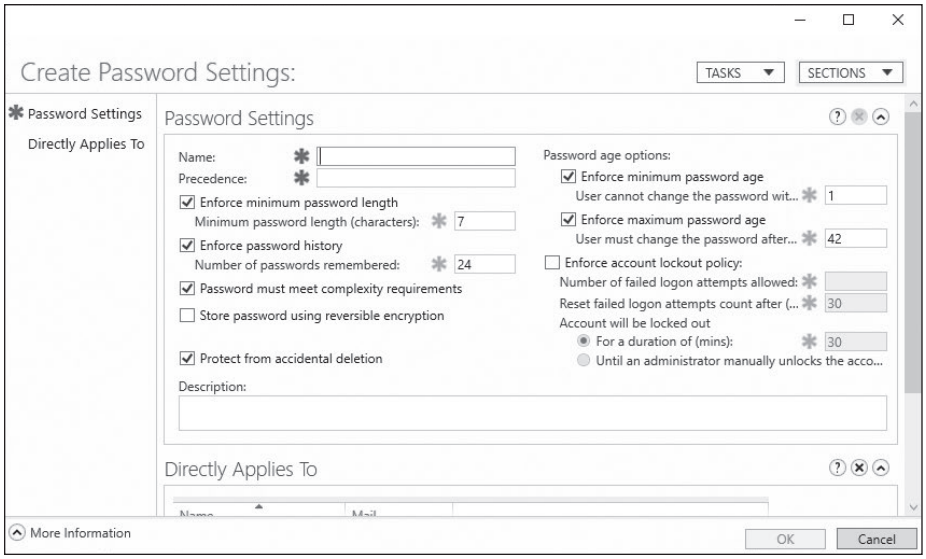


Figure 3-4
Creating a new Password Settings Container

5. In the **Name** text box, type a name for the Password Settings Container.
6. In the Precedence text box, type a Precedence number. Passwords with a lower precedence number overwrite the Password Settings Containers with a higher precedence number.
7. Fill in or edit the appropriate fields for the settings that you want to use.
8. Under Directly Applies To, click **Add**. In the Select Users or Groups dialog box, specify the name of the user or group that the Password Settings Container should affect and click **OK**.
9. Click **OK** to submit the creation of the PSO.
10. Close the ADAC.

Establishing Password Procedures

Passwords are the most common form of authentication, and IT help desks spend a lot of time managing calls from users who cannot log on because they forgot their passwords or their accounts have been compromised.

CERTIFICATION READY
How can you establish a password reset procedure that allows passwords to be changed quickly, but securely?
Objective 2.3

Every organization should develop a ***security policy***, which is a written document that describes how a system, organization, or other entity is secured. The security policy should include an ***acceptable use policy***, which describes the constraints and practices that users must agree to in order to access the corporate network, corporate resources, and the internet. It is also important to specify a ***password policy***, which dictates the length and complexity requirements for passwords and how often a password should be changed. It can also specify whether multi-factor authentication should be used and whether a lockout policy is used when a user has attempted to log on several times using the incorrect password.

It is important that users periodically change their passwords. They should also change their passwords when their accounts have been compromised. When a user cannot access a system and their password needs to be changed, be careful with how the password change is communicated to the user. As a general rule, forgotten or new passwords should not be emailed to the user, because they can be intercepted by anyone who has control of their email account. If email absolutely must be used, send a password reset link that contains a token that will expire after a short period of time and can only be used once. If a caller calls in or sends an email to request a new password, use a procedure that requires the caller to prove their identity as an authorized user. Users should not use secret questions (such as their mother's maiden name or their pet's name), because many of these answers can be guessed through social engineering or by searching the internet for user profiles.

One way to authorize users is to use voicemail. When a user needs to use a PIN to retrieve phone messages, inform the user that you will call them back and that they are *not* to answer the phone (so that you can leave a voice mail). Because the user should be the only one who knows the PIN to retrieve her voicemail, their use of the PIN to retrieve their voicemail will be used to prove the user's identity. Alternatively, provide the password to their manager, who is local to the user account. In both situations, indicate that the password must be changed as soon as the user logs on. When changing an application password, also send emails or messages to all the user's devices, notifying the user of the password change. If an unauthorized user attempts to get the password changed, the authorized user will be notified and he should be trained to contact the help desk to report that he did not request a password change.

Understanding Common Attack Methods

Passwords have long been recognized as one of the weak links in many security programs. While tokens, smart cards, and biometrics are gaining traction in the business world for securing key systems and data, a significant amount of confidential and private data is still being secured with passwords. Passwords are considered a weak link for two main reasons.

First, users select their own passwords. While many users will select strong passwords in line with your standards, and some tools exist to enforce password attributes like password complexity and minimum password length, there are going to be users who will continue to select weak passwords. Attackers are aware of this and will try to exploit those users.

Second, even strong passwords are vulnerable to attack through a variety of different mechanisms, including those discussed in the following sections.

DICTIONARY ATTACK/BRUTE FORCE ATTACK

A dictionary attack (also known as a brute force attack) uses a dictionary containing an extensive list of potential passwords that the attacker then tries in conjunction with a user ID to attempt to guess the correct password. This is known as a dictionary attack because the earliest versions of this attack actually used lists of words from the dictionary as the basis of their attacks. Now, custom dictionaries with likely passwords are available for download from the internet, along with applications that can use them against your systems.

Another, more crude type of brute force attack doesn't rely on lists of passwords, but instead tries all the combinations of the permitted character types. While this type of attack was historically considered ineffective, improvements in processor and network performance have made it more usable, although not nearly as effective as a dictionary attack.

These types of attacks tend to be more successful when the password length is 7 characters or less. Each additional character adds a significant number of possible passwords. These attacks are often successful because users will sometimes use common words with the first letter capitalized and then append a number to meet the complexity guidelines. These are the easiest passwords for users to remember, but they are also the easiest for an attacker to compromise.

The account lockout settings discussed earlier in the lesson are a critical defense against this type of attack, because an account lockout will either slow or stop a brute force attack in its tracks after the configured number of incorrect logon attempts is reached.

MORE INFORMATION

Lesson 1 provides more details on keylogging.

PHYSICAL ATTACK

Any time a computer can be physically accessed by an attacker, the computer is at risk. Physical attacks on a computer can completely bypass almost all security mechanisms, by capturing the passwords and other critical data directly from the keyboard when a software or hardware keylogger is used. In fact, if an encryption key passes through a keylogger, even the encrypted data can be jeopardized.

Some other physical attacks include the use of a hidden camera to tape keystrokes, or even the removal and duplication (or direct theft) of a hard drive. While not specifically a password attack, by removing a hard drive, attackers can frequently bypass password controls by mounting the drive remotely, and accessing data directly from the drive, without an intervening operating system.

LEAKED OR SHARED PASSWORDS

While not strictly an attack, another challenge that is commonly encountered when dealing with users in an office environment is the leaked or shared password. Users tend to trust their co-workers. They all work for the same company, and in many cases, they have access to similar information within the company. As a result, a user could easily be convinced to share their password with a co-worker who felt they "needed it." This practice is especially

problematic in environments with high turnover, because there is no way to tell who in the last crop of employees might be someone who still has a friend's user ID and password for continued access to the production network. Users will frequently justify the sharing of account information as critical to "getting the job done" or stating that it's "more convenient."

Even if the user doesn't deliberately provide their password to another employee, the casual work environment frequently makes it easy for an employee to watch as their co-worker keys in their user ID and password.

Finally, employee spouses/partners, children, and other relatives could end up with access to an environment because of their close relationship with that employee.

User awareness is the best way to combat this type of attack. Providing users with a greater understanding of the risks and impact of these types of behaviors can go a long way towards keeping passwords under the control of only authorized users. In addition, the minimum password age and maximum password age settings, as well as the password history setting, will help mitigate this risk. Even if someone does get a password they shouldn't have, when the maximum password age limit hits, you can force a reset of all passwords, including shared ones.

CRACKED PASSWORDS

A ***cracked password*** frequently relies on more than just a password attack. In a cracked password attack, the attacker gets access to an encrypted password file from a workstation or server. Once they have access, the attacker will start running password cracking tools against the file, with an eye towards breaking as many passwords as possible, then leveraging them to further compromise the company's network and systems.

Passwords that are stored in an encrypted state are harder to break than passwords that are stored in clear text or in a hashed state. With today's computing power, even encrypted password stores are being compromised by password cracking attacks.

If a password store has been compromised, every employee with an account on the compromised system should change their passwords immediately.

It is possible to use the same tools that potential attackers might use to audit the security of your password stores. Trying to crack your own password file is a common practice for testing the security of a password store. In addition, if any passwords are found to be compromised and are weak, the users can be asked to change them to more secure passwords.

NETWORK/WIRELESS SNIFFER

If an attacker can gain access to your internal network, your wireless network, or even an internet access point used by your employees, they have the ability to use a specialized tool known as a sniffer to try to intercept unencrypted passwords. While applications have become more secure in recent years, there are still a number of applications that pass sensitive information like passwords across the network in clear text, where they can be read by anyone with the ability to view the data as it traverses the network.

Sniffers are specially designed software (and in some cases hardware) applications which capture network packets as they traverse the network and display them for the attacker. Sniffers are valid forms of test equipment, used to identify network and application issues, but the technology was rapidly co-opted by attackers as an easy way to grab logon credentials.

In addition to attacks against a wired network, there are now sniffers that can capture wireless data as well. When connected to a business wireless network at the local coffee shop or while attending a meeting at a hotel, a user is potentially at risk of having their data pulled literally out of the air and made available to an attacker. The use of encryption remains the best mechanism for combating this type of attack.

Another area of concern with sniffers is wireless keyboards. At its core, a wireless keyboard is a broadcast technology that sends keystrokes from the keyboard to the receiver connected to the computer. If a receiver is tuned to the same frequency close enough to the computer, every keystroke entered into the wireless keyboard can be captured, without needing a keylogger installed. Most wireless keyboards now support additional security like encrypted connections, but they are still broadcasting any information that is input, and as long as we enter most data through the keyboard, this will be a significant potential source for an attacker to exploit. Many companies will only permit their employees to use wired keyboards in the office to mitigate this risk.

GUESSED PASSWORDS

While not as prevalent an issue as it was in times past, there is still the possibility that someone could sit down at your computer and guess your password. As we have seen in countless movies, the attacker is familiar with the person whose system they are trying to compromise, or they look around the office and see a postcard from a trip, or pictures of the kids with their names on them to ascertain the password. If the user does not follow the corporate rules and set a strong, not easily guessable password, and instead selects a password based on a spouse's/partner's, child's, or pet's name and birthday, the attacker could guess the password and access the employee's data.

That being said, this type of attack is almost never seen these days. With the widespread availability of password cracking tools, the type of individual targeting required to guess someone's password is seldom worth the effort. It is generally much easier to leverage an attack against one of the other vectors available. Typically, only co-workers or close friends will try to guess a user's password.

■ Protecting Domain User Account Passwords

THE BOTTOM LINE

Over the years, malware has changed dramatically and has become quite sophisticated. Microsoft developed Device Guard and Credential Guard, which complement each other in protecting the system against malware.

CERTIFICATION READY
Which mechanisms used with Windows 10 help protect the domain user account passwords?
Objective 2.3

Device Guard helps harden a computer system against malware by running only trusted applications, thereby preventing malicious code from running. ***Credential Guard*** isolates and hardens key system and user security information. Both technologies are available only through Windows 10 Enterprise.

Device Guard and Credential Guard use Windows 10 ***virtual secure mode (VSM)*** which, in turn, uses the processor's virtualization to protect the PC, including data and credential tokens on the system's disks. By using hardware virtualization, Windows 10 is organized into multiple containers. Windows runs one container; the Active Directory security tokens that allow access to your organization's resources run in another container. Each container is isolated from the other. Therefore, if Windows is compromised by malware, the tokens are protected because they are isolated in their own encrypted container.

Following are requirements for using VSM:

- UEFI running in Native Mode (not Compatibility/CSM/Legacy mode)
- 64-bit version of Windows 10 Enterprise
- 64-bit processor that supports Second Layer Address Translation (SLAT) and Virtualization Extensions (such as Intel VT or AMD V)

A Trusted Platform Module (TPM) is recommended.

Use the following procedure to install Hyper-V and Isolated User Mode after meeting these requirements.

INSTALL HYPER-V AND ISOLATED USER MODE ON WINDOWS 10

GET READY. To install Hyper-V and Isolated User Mode on Windows 10 Enterprise, perform the following steps.

1. On LON-CL1, right-click the **Start** button and choose **Programs and Features**.
2. Click the **Turn Windows features on or off** option.
3. In the Windows Features dialog box, select **Isolated User Mode** and **Hyper-V Platform**, and then click **OK**.

Next, enable Device Guard and Credential Guard with group policy.

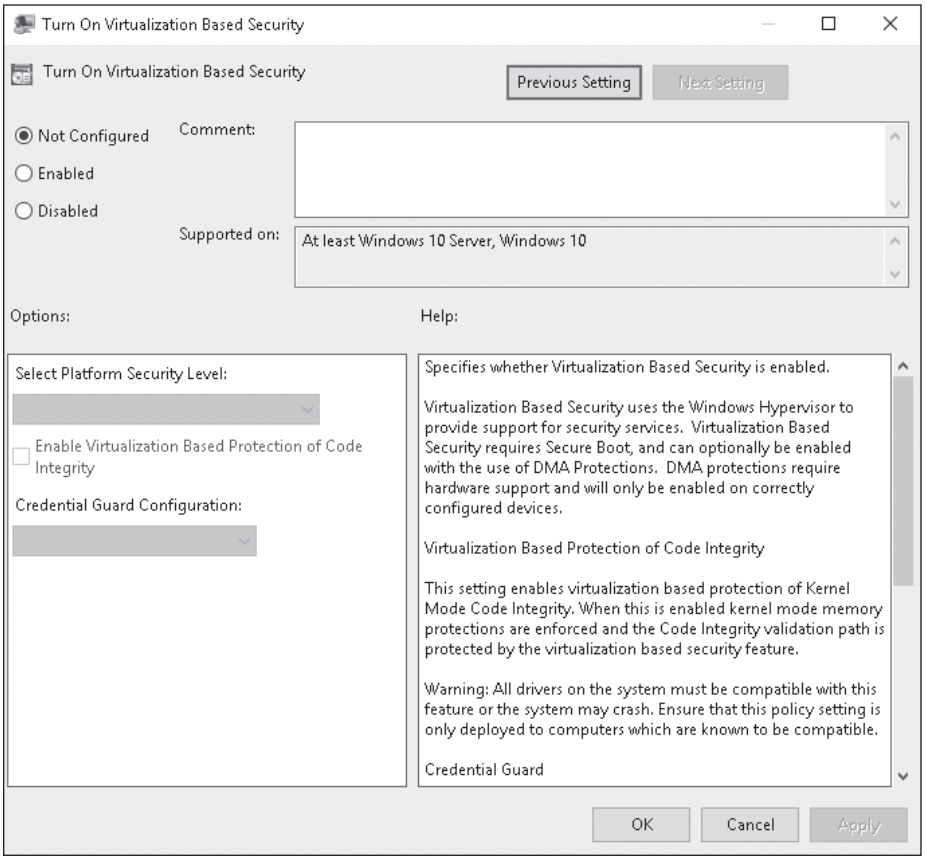
ENABLE DEVICE GUARD AND CREDENTIAL GUARD

GET READY. To enable Device Guard and Credential Guard, perform the following steps.

1. Open a GPO and then navigate to **Computer Configuration\Administrative Templates\System\Device Guard\Turn On Virtualization Based Security** (as shown in Figure 3-5).

Figure 3-5

Turning on virtualization based security



4. Click **Enabled**.
5. To enable Device Guard, select **Enable Virtualization Based Protection of Code Integrity**.
6. To enable Credential Guard, select **Enable Credential Guard**.
7. Close the Turn On Virtualization Based Security window by clicking **OK**.

SKILL SUMMARY

In this lesson, you learned:

- The strength of a password can be determined by examining the length, complexity, and randomness of the password.
- A complex password will use characters from at least three of the following categories: uppercase characters, lowercase characters, numeric characters, and non-alphanumeric characters.
- Account lockout refers to the number of incorrect logon attempts permitted before the system will lock the account.
- The length of a password is a key component of ensuring the strength of a password.
- The minimum password age setting controls how many days a user must wait before they can reset their password.
- The maximum password age setting controls the maximum period of time permitted before a user is forced to reset their password.
- A Group Policy Object (GPO) is a set of rules which allow an administrator granular control over the configuration of objects in Active Directory (AD), including user accounts, operating systems, applications, and other AD objects.
- Passwords have long been recognized as one of the weak links in many security programs.
- A dictionary attack (also known as a brute force attack) uses a dictionary containing an extensive list of potential passwords that the attacker then tries in conjunction with a user ID to attempt to guess the correct password.
- A brute force attack tries all the combinations of the permitted character types.
- Physical attacks on a computer can completely bypass almost all security mechanisms, by capturing the passwords and other critical data directly from the keyboard when a software or hardware keylogger is used.
- In a cracked password attack, the attacker gets access to an encrypted password file from a workstation or server. Once they have access, the attacker will start running password cracking tools against the file.
- If an attacker can gain access to your internal network, your wireless network, or even an internet access point used by your employees, they have the ability to use a specialized tool known as a sniffer to try to intercept unencrypted passwords.
- While not as prevalent an issue as it was in times past, there is still the possibility that someone could sit down at your computer and guess your password.
- Device Guard helps harden a computer system against malware by running only trusted applications, thereby preventing malicious code from running.
- Credential Guard isolates and hardens key system and user security information. The Credential Guard and Device Guard technologies are available only through Windows 10 Enterprise.

■ Knowledge Assessment

Multiple Choice

Select the correct answer(s) for each of the following questions.

1. Which of the following are *not* valid password controls? (Choose all that apply.)

a. Minimum Password Age
b. Maximum Password Age
c. Maximum Password Length
d. Account Lockout Threshold
e. Password History

2. Which of the following would be an acceptable password on a Windows 10 Pro system with Password Complexity enabled and a minimum password length set to 8? (Choose all that apply.)

a. Summer2010
b. $$Thx17
c. ^^RGood4U
d. Password
e. St@rTr3k

3. Which of the following is the maximum setting for Minimum Password Age?

a. 14
b. 999
c. 998
d. 256

4. Which of the following corresponds with the minimum and maximum password history settings for securing a Windows 10 Pro workstation image? (Choose the best answer.)

a. 0, 14
b. 1, 14
c. 0, 24
d. 1, 24
e. 0, 998

5. Which of the following are common password attacks? (Choose all that apply.)

a. Cracking
b. Phreaking
c. Phishing
d. Leaking
e. Brute force

6. Which of the following refers to a form of brute force password attack that uses an extensive list of pre-defined passwords? (Choose the best answer.)

a. Bible
b. Cracking
c. Guessing
d. Dictionary

7. Which setting should be applied to ensure that a possible dictionary attack against a Windows application server has a limited chance at success? (Choose the best answer.)

a. Minimum Password Length
b. Account Lockout Threshold
c. Password History
d. Maximum Password Age

8. Which Administrative Tool should be used to configure password control settings on a new standalone server?
   a. Active Directory Users and Computers
   b. Computer Management
   c. Security Service
   d. Local Security Policy
9. Which two features in Windows Server 2008 and higher permit the use of fine-grained password policies? (Choose two.)
   a. Global Policy Object
   b. Password Settings Container
   c. Password Settings Object
   d. Password Policy
10. Which of the following explains why a minimum password age would be set?
    a. To ensure that no one can guess a password
    b. To stop someone from trying over and over to guess a password
    c. To make sure a user cannot reset a password multiple times until he or she can reuse his or her original password
    d. To automatically reset a password
11. Which of the following uses the processor's virtualization to protect the PC, including data and credential tokens on the system's disks?
    a. Virtual smart cards
    b. Device Guard
    c. Credential Guard
    d. Windows Hello
12. In Windows 10, which component is used by Device Guard and Credential Guard to protect the PC?
    a. Windows Store
    b. Virtual smart cards
    c. Windows Hello
    d. Virtual secure mode

Fill in the Blank

Complete the following sentences by writing the correct word or words in the blanks provided.

1. A set of rules which allow an administrator granular control over the configuration of objects in Active Directory (AD), including user accounts, operating systems, applications, and other AD objects is known as a _____.
2. The number of incorrect logon attempts permitted before the system will lock the account is known as _____.
3. The setting which determines the number of unique passwords that must be used before a password can be reused is the _____.
4. A type of attack that uses an extensive list of potential passwords is known as a _____.
5. Using special software to read data as it is broadcasted on a network is called _____ the network.
6. The _____ option needs to be less than or equal to the Account Lockout Duration.
7. The highest setting that account lockout duration can use is _____.

8. In a Windows Server 2016 Active Directory, the _____ automatically applies in the event that a fine-grained password policy has not been set.
9. The three configuration settings for account lockout are _____, _____, and _____.
10. A _____ is a type of account that might be configured so that the password will not expire.

■ Business Case Scenarios

Scenario 3-1: Understanding Long Passwords

For each scenario, specify the number of possible passwords based on the number of possible combinations.

a. Let's say you have a four-digit personal identification number (PIN). Each digit can be 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9, giving a total of 10 possible numbers for each digit. If a PIN is 4 digits, each digit can be any one of the 10 possible numbers. How many combinations can you have?

b. Let's say you can use a 4-letter password and each password can be a lowercase letter (a-z). There are 26 letters. If you have 4 letters, how many combinations do you have?

c. Let's say you have 6-letter passwords and each password can be a lowercase letter (a-z). How many combinations are there?

d. Let's say you have 8-letter passwords and each password can be a lowercase letter (a-z). How many combinations are there?

e. Let's say you have 8-letter passwords and each password can be a lowercase letter (a-z) or uppercase letter (A-Z). How many combinations are there?

f. Let's say you have 8-letter passwords, each password can be a lowercase letter (a-z), uppercase letter (A-Z), a digit (0-9), or a special character ~ ` ! @ # $ % ^ & * ( ) _ - + = { [}] | \ : ; " ' < , > . ? or / . How many combinations are there?

Scenario 3-2: Using Keys and Passwords

The CIO at the Contoso Corporation indicates that he just received a message on his computer stating that he must change his password. He wants to know why he should change the password to a relatively long password on a regular basis. Describe your explanation.

Scenario 3-3: Managing User Accounts

As an administrator with the Contoso Corporation, you have been tasked with managing user accounts. Describe the steps necessary to creating a standard account for John Adams on a computer running Windows 10. You will then change John Adams (JAdams) to an administrator account and then set the password for John Adams to Pa$$w0rd.

Scenario 3-4: Configuring a Local Security Policy

As an administrator with the Contoso Corporation, you have been tasked with configuring a local security policy. On a computer running Windows 10, open the Group Policy Management window to access the Local Group Policy. View the Password Policy and Account Lockout Policy and record the default settings for Password Policy and Account Lockout Policy.

Workplace Ready

Understanding Group Policies

Group Policies refers to one of the most powerful features that is included with Active Directory. Besides configuring password policies and account lockout policies, it can be used to assign user rights that define what a user can do on a computer. It can also be used to install software, prevent other software from being installed, lock down a computer, standardize a working environment, and preconfigure Windows. With Group Policies configuration, there are thousands of possible settings.