<CHN>CHAPTER ELEVEN

<CHT>AUTHENTICATION AND ACCOUNT MANAGEMENT

<COOT>Labs included in this chapter

* <COOH1>Lab 11.1 Setting a Minimum Password Length Policy
* Lab 11.2 Setting Password History and Minimum Password Age Policies
* Lab 11.3 Enforcing Password Complexity Requirements
* Lab 11.4 Setting Policies for Account Lockouts and Log on Hours
* Lab 11.5 Restricting Access to Programs

<COOBT>CompTIA Security+ Exam Objectives

<COOB>Domain Lab

<COOB>Technologies and Tools 11.1, 11.2, 11.3, 11.4, 11.5

Identity and Access Management 11.1, 11.2, 11.3, 11.4, 11.5

Cryptography and PKI 11.5

# <H1>Lab 11.1 Setting a Minimum Password Length Policy

<H2>Objectives

<TX1>Security controls can be broadly classified either as social or technical—or perhaps more realistically, as unenforceable or enforceable. Social controls depend on the user’s cooperation. A policy stating that users may not share their passwords with anyone else is unenforceable because there is no way to be certain the user complies. On the other hand, a policy stating that users must include a minimum of nine characters in their passwords can be enforced through group policies in Windows Server 2016.

<TX2>Active Directory is a hierarchical database that includes container objects: sites, domains, and organizational units. These container objects can hold user accounts, group accounts, and other logical representations of network elements. Once placed inside a container object, these elements can be controlled by Group Policy Objects (GPO). A GPO is a series of policy settings that can be linked to a container object. GPOs are what make Active Directory a very flexible tool—for example, if a GPO is linked to a domain, all the objects subject to its policies (user, computer, or both) are subject to those policies. So, if a GPO linked to the domain contains a computer policy requiring the use of Internet Protocol Security (IPsec) for all communications, all computers in the domain are required to use IPsec to protect transmissions. If a policy specifies the minimum password length to be nine characters, all computers in the domain are subject to that policy. This is an example of a technical security control; it does not rely on the user’s cooperation. The user has no choice but to comply.

<TX2>After completing this lab, you will be able to:

* <BL>Describe the minimum password length configuration options in Active Directory
* Create, implement, and test minimum password length policies
* Create, implement, and test group policy objects

**<H2>Materials Required**

<H1>This lab requires the following:

* <BL>Windows Server 2016
* Windows 10 VM

**<H2>Activity**

<FE1TX1>Estimated completion time: **15–20 minutes**

<TX1>In this lab, you create a minimum password length policy using the Group Policy Management console and then test your policy.

1. <NL\_FIRST>Log on to the Windows Server as Administrator.
2. <NL\_MID>In Server Manager, click Tools, and then click Active Directory Users and Computers.
3. If necessary, expand your domain, click the Users folder, and verify that an account for the domain user Martin Sheppard exists. If this account does not exist, create the account following the directions in Lab 6.3.
4. Close Active Directory Users and Computers.
5. Click Tools, and double-click Group Policy Management. Expand your forest, expand Domains, expand your domain, right-click the Default Domain Policy, and click Edit.
6. In the Group Policy Management Editor window, if necessary, expand the Computer Configuration section of the Default Domain Policy, expand Policies, expand Windows Settings, expand Security Settings, expand Account Policies, and click Password Policy. In the right pane, double-click the Minimum password length policy.
7. Notice the Explain tab, where you can learn more about the security policy being configured. Also notice that the Minimum password length policy is already defined in this GPO as being seven characters. Use the spin box to increase this number to nine characters. Click OK, close the Group Policy Management Editor. In the Group Policy Management console, right-click Domain Controllers and click Group Policy Update. Click Yes and then click Close. The policy has now been updated on the domain controller.
8. From Windows 10 VM, log on as msheppard with the password Pa$$word. This password does not meet the minimum password length. Why was it accepted?
9. Press Ctrl+Alt+Del and select Change a password. Enter the old password Pa$$word in the Old password box, enter the new password PASSwor8 in the New password box and the Confirm password box, then press Enter. Why did you receive the “Unable to update the password” error?
10. Click OK and attempt to change the password again. This time, use Pa$$wordP as the new password. What was the result? Log out and log in as administrator with the password Pa$$word. Use the same procedure as in Step 9 of this lab to change the administrator’s password to PASSwor8. What was the result? Consider the error message “Unable to update the password. The value provided for the new password does not meet the length, complexity, or history requirements of the domain.” Do you think security is increased or decreased by the error message being nonspecific about which parameter of the password requirements of the domain was not met? Do you think it is more secure or less secure to require that domain administrators follow the same password policies as domain users?
11. From Windows Server, prepare to edit the Default Domain Controllers GPO as performed in Steps 5 and 6 of this lab. Return the Minimum password length policy setting to seven characters, close the Group Policy Management Editor console and force the Group Policy Management to update as seen in Step 7.
12. From Windows 10 VM, log on as msheppard and reset his password to Pa$$word. What was the result? This error is not because of the password length. We will address this error message in the next lab.
13. Log off both systems.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.3 Given a scenario, troubleshoot common security issues.
* 4.1 Compare and contrast identity and access management concepts.
* 4.3 Given a scenario, implement identity and access management controls.
* 4.4 Given a scenario, differentiate common account management practices.

**<H2>Review Questions**

1. <MULT>Which of the following is a correct statement about password policies in a typical business environment?
2. <MULTA>The longer the password, the more secure it is.
3. **The shorter the password, the less secure it is.**
4. Based on the number of user accounts in a domain, there is a mathematically optimum setting for minimum password length.
5. When users share a password, security is enhanced because everyone is a suspect if malicious actions occur.
6. <MULT>What is the maximum number of characters that can be specified in a Minimum password length account policy in Windows Server 2016?
7. <MULTA>10
8. **14**
9. 24
10. There is no maximum.
11. <TF>When a minimum password length is configured in the Default Domain Policy, all member computers in the domain are automatically configured to use the same minimum password length in their local security databases. **True** or False?
12. <FIB>Minimum password length requirements on a member server in a Windows Server 2016 domain \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
13. **<FIBA>cannot be modified on the server’s Local Security Policy**
14. can be modified on the server’s Local Security Policy, but only by a domain administrator
15. can be modified on the server’s Local Security Policy, but only by a domain administrator or the administrator of the local computer
16. can be modified on the server’s Local Security Policy by anyone who has Write permissions to the Local Security Policy
17. <FIB>The gpupdate /force command \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
18. **<FIBA>reapplies all policy settings**
19. reapplies all policy settings that have changed since the last application of group policies
20. causes the next foreground policy application to be done synchronously
21. can be run by any user

# <H1>Lab 11.2 Setting Password History and Minimum Password Age Policies

**<H2>Objectives**

<TX1>In Lab 11.1, the user Martin Sheppard changed his password from Pa$$word to Pa$$wordP to comply with the new minimum password length policy. However, when the old policy was reinstated, he was prevented from changing his password back to Pa$$word. The error message mentioned several possible policies that his action might have violated. In this lab, we investigate two password policies that may have been responsible: the Enforce password history policy and the Minimum password age policy.

<TX2>The Enforce password history policy prevents users from changing their passwords to ones they have already used within a given number of previous passwords. The number of passwords that Active Directory “remembers” can be configured. On the one hand, it seems reasonable to let employees reuse passwords; they’re more likely to remember them and less likely to write them down—a serious security problem. On the other hand, if users are forced to change their passwords regularly and they change them to ones they’ve previously used, it is the same as not changing passwords at all.

<TX2>The Minimum password age policy prevents users from changing their passwords until a minimum number of days have elapsed. On the face of it, this seems odd: if an administrator wants users to be able to change their passwords at all, shouldn’t they be allowed to change them whenever they deem it necessary? For example, if a user suspects that a passerby has “shoulder surfed” (observed the password being entered), the user should change the password immediately, right? With a Minimum password age policy in effect, this might not be possible. The user would have to call the help desk (or, in a smaller organization, the network administrator) to have the password reset. This creates a security vulnerability.

<TX2>However, without a Minimum password age policy in effect, the Enforce password history policy can easily be circumvented by users. If there are no restrictions regarding when users can change their passwords, when the maximum password age has been reached, and users are forced to change their passwords, they can simply change the passwords repeatedly, cycling through the “remembered” passwords until they can restore the original password. Once again, the security benefits of requiring users to change passwords regularly would be effectively eliminated.

<TX2>A sensible implementation of these policies based on an assessment of the risks and benefits to business efficiency will usually provide an acceptable compromise between information security and user satisfaction. This is an ongoing burden for the security officer: maintaining a balance between security needs and business needs.

<TX2>After completing this lab, you will be able to:

* <BL>Explain how password history and minimum password age policies can increase resource security
* Configure, implement, and test password history and minimum password age policies

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows Server 2016
* Windows 10 VM

**<H2>Activity**

<FE1TX1>Estimated completion time: **15–20 minutes**

<TX1>In this lab, you configure and test password history and minimum password age policies.

1. <NL\_FIRST>Log on to Windows Server as Administrator.
2. <NL\_MID>Access the Group Policy Management console and edit the Default Domain Policy following the procedure described in Lab 11.1, Step 5.
3. In the Group Policy Management Editor window, if necessary, expand the Computer Configuration section of the Default Domain Policy, expand Policies, expand Windows Settings, expand Security Settings, expand Account Policies, and click Password Policy. In the right pane, double-click Enforce password history. The default is 24 passwords remembered. Change the number to 0 and click OK. Close the Group Policy Management Editor. From a command prompt, run gpupdate /force.
4. Log on to Windows 10 VM as martin sheppard with the password Pa$$wordP. Press Ctrl+Alt+Del and select Change a password and change his password to PASSword9. This should fail. Why?
5. Return to Windows Server and access the Group Policy Management console. Using the directions in Step 3 to access Password Policy, edit the Minimum password age policy to a value of 0 days. Close the Group Policy Management Editor. From a command prompt, run gpupdate /force.
6. From Windows 10 VM, reset the password for msheppard, as in Step 4, to Pa$$word9. This should succeed. Press Ctrl+Alt+Del, select Change a password, and change his password back to Pa$$word. This, too, succeeds. At this point, no matter how often Martin Sheppard is required to change his password, by changing it once and immediately changing it back to his favorite password, he will have circumvented an important security control. If passwords do not change regularly, when one password is compromised, the systems to which that user had access are compromised indefinitely.
7. Return to Windows Server and set the Password Policies for the domain as follows: Enforce password history—0 passwords remembered, Minimum password age—0 days (so that you can experiment with changing passwords), Password must meet complexity requirements—Disabled. Leave the other Password Policies as they were. From a command prompt, run gpupdate /force.
8. Close all windows and log off both systems.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.3 Given a scenario, troubleshoot common security issues.
* 4.1 Compare and contrast identity and access management concepts.
* 4.3 Given a scenario, implement identity and access management controls.
* 4.4 Given a scenario, differentiate common account management practices.

**<H2>Review Questions**

1. <MULT>Which of the following statements regarding the Enforce password history policy is true?
2. <MULTA>Once an Enforce password history policy is enabled, users can never reuse a password.
3. If Enforce password history is set to 10 and minimum password age is set to 10, a user can configure a previous password only after 1,000 days have elapsed.
4. If Enforce password history is set to 10 and minimum password age is set to 0, users can configure a previous password every 10 days.
5. **If Enforce password history is set to 10 and minimum password age is set to 10, a user can configure a previous password only after 100 days have elapsed.**
6. <FIB>You have just installed a stand-alone Windows Server 2016 and then added the DNS server role. The default value for the Enforce password history policy is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
7. **<FIBA>0**
8. 7
9. 12
10. 24
11. <FIB>You have just installed Windows Server 2016 as the first domain controller in the first domain in the forest using default settings wherever possible. Then you installed Windows Server 2016 on another system using default settings wherever possible, joined it to the domain, and added the DNS server role. The Enforce password history policy on the DNS server is set to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
12. <FIBA>0
13. 7
14. 12
15. **24**
16. <MULT>Which of the following is a correct statement? (Choose all that apply.)
17. **<MULTA>The Enforce password history policy is designed to prevent immediate password reuse.**
18. **The Minimum password age policy is designed to prevent immediate password reuse.**
19. **Used together, the Enforce password history policy and the Minimum password age policy make it difficult for users to maintain the same passwords when forced to change passwords.**
20. Used together, the Enforce password history policy and the Minimum password age policy make it impossible for users to maintain the same passwords when forced to change passwords.
21. <TF>The Enforce password history policy allows domain administrators to inspect a user’s previous passwords for compliance with established security policies. True or **False**?

# <H1>Lab 11.3 Enforcing Password Complexity Requirements

**<H2>Objectives**

<TX1>At the conclusion of Lab 11.2, you disabled the password complexity policy in the Default Domain GPO. A social policy stating that users must use strong passwords and avoid easy-to-crack passwords (such as the user’s Social Security number) cannot be enforced without technical controls, however. One way to enforce a social policy, which is favored by a surprising number of network and security administrators, is to audit users’ passwords by periodically using password-cracking programs. Weak passwords are cracked in a matter of seconds, and then the users who created these passwords are sent an email asking them to comply with security policies and create stronger passwords. Why administrators would use this approach without including the technical implementation of password complexity requirements is not clear, however.

<TX2>Care must be taken even if passwords are complex. For example, the password you are using in these labs is very weak even though it meets the password complexity requirements; it is based on a dictionary word, and password cracking programs are well aware that “$” may mean “s” or “S” and that “@” may mean “a” or “A.” There is definitely a place for password auditing by administrators when a technical control requiring password complexity is in place, but it is not a substitute for technical password complexity controls. When you think about it, requiring administrators to audit passwords periodically is a social, not a technical, control. If the administrator is too busy or forgets to implement the password audits, the policy goes unenforced. In this lab, you examine password complexity requirements in a Windows Server 2016 domain.

<TX2>After completing this lab, you will be able to:

* <BL>Define the requirements for password complexity in a Windows Server 2016 environment
* Configure, implement, and test password complexity policies

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows Server 2016
* Windows 10 VM

**<H2>Activity**

<FE1TX1>Estimated completion time: **15–20 minutes**

<TX1>In this lab, you configure and test password complexity policies.

1. <NL\_FIRST>Log on to Windows 10 VM as msheppard using the password Pa$$word. Using the methods demonstrated in this chapter, change Martin Sheppard’s password to bootsismydog. While this password exceeds the minimum password length policy, a password-cracking program would break this password in milliseconds.
2. <NL\_MID>Log on to Windows Server as Administrator and, using the methods demonstrated in this chapter, enable the password policy Password must meet complexity requirements in the Default Domain GPO, and then run the **gpupdate /force** command.
3. Return to Windows 10 VM and change Martin Sheppard’s password to tabbyismycat. This should fail. Try to change Martin Sheppard’s password again, this time to TabbyIsMyCat. This should fail as well. Why?
4. Try to change Martin Sheppard’s password to TabbyIsMyC@t. This succeeds. Can you figure out what the specific complexity requirements are?
5. Change Martin Sheppard’s password from TabbyIsMyC@t to tabbyismyc@t. This fails. The only password that has been successful is TabbyIsMyC@t.
6. Still, these are all weak passwords because they contain words found in the dictionary. One way around this is to use the first letters of words in a memorable text, such as a song or a poem. For example, Vladimir Nabokov’s eerie poem/novel Pale Fire begins with the following line: “I am the shadow of the waxwing slain, by the false azure of the windowpane.” The password “i@Tsotw$bTfaotw” could be generated from this line. The use of “@” for “a” and “$” for “s” may be too obvious, but the capitalization of every other “t” and the apparent randomness of the letters along with the length of the word makes this a strong password and not all that hard to remember if you remember Nabokov’s poem. Try changing Martin Sheppard’s password to i@Tsotw$bTfaotw.
7. Change Martin Sheppard’s password back to Pa$$word and close all windows and log off both systems.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.3 Given a scenario, troubleshoot common security issues.
* 4.1 Compare and contrast identity and access management concepts.
* 4.3 Given a scenario, implement identity and access management controls.
* 4.4 Given a scenario, differentiate common account management practices.

**<H2>Review Questions**

1. <TF>When the Password must meet complexity requirements policy is enforced, only a domain administrator can assign a password to a user that does not meet the password complexity requirements. True or **False**?
2. <MULT>In a Windows Server 2016 domain environment, if the Password must meet complexity requirements policy is enabled, passwords must contain at least three of the following character types. (Choose all that apply.)
3. **<MULTA>An uppercase letter**
4. **A lowercase letter**
5. **A number**
6. A space or backspace
7. **Nonalphabetic characters (!, $, #, %, etc.)**
8. <TF>A password that uses uppercase letters and lowercase letters but consists of words found in the dictionary is just as easy to crack as the same password spelled in all lowercase letters. True or **False**?
9. <MULT>Which of the following statements regarding the password complexity policy is correct? (Choose all that apply.)
10. **<MULTA>After the initial installation of a Windows Server 2016 domain controller, the Password must meet complexity requirements option is enabled.**
11. After the initial installation of a Windows Server 2016 stand-alone server, the Password must meet complexity requirements option is enabled.
12. After the initial installation of a Windows Server 2016 stand-alone server, the Password must meet complexity requirements option is not configured.
13. **After the initial installation of a Windows Server 2016 member server, the Password must meet complexity requirements option is enabled.**
14. <MULT>Which of the following is a true statement about the Windows Server 2016 Password must meet complexity requirements policy? (Choose all that apply.)
15. **<MULTA>A password must be at least six characters in length.**
16. **A password may not contain the user’s account name.**
17. **A password may not contain parts of the user’s full name that exceed two consecutive characters.**
18. **Password complexity requirements are enforced when passwords are changed or created.**

# <H1>Lab 11.4 Setting Policies for Account Lockouts and Log on Hours

**<H2>Objectives**

<TX1>When an attacker wants to break a password on a remote system (assuming passwords are not being sent in the clear, as in FTP or Telnet), the attacker’s first objective is to copy the system’s password file. Typically, operating systems don’t store the passwords; they store encrypted versions of the passwords. The most convenient method for attackers is to copy the file to their own machines and then crack them at their leisure, when they can’t be detected. However, an experienced attacker can successfully access a machine simply by trying various passwords.

<TX2>Because so many users select weak passwords when given the opportunity, the experienced attacker can often guess the password in a few attempts. Here are the most common passwords: “qwerty,” “asdf,” “123456,” “123123,” “password,” “letmein,” all blank spaces, the user’s name, and (oddly) “monkey.” One way to limit password guessing is to limit the number of times incorrect login attempts will be allowed before the account is locked.

<TX2>After completing this lab, you will be able to:

* <BL>Define the account lockout policies in a Windows Server 2016 environment
* Configure, implement, and test account lockout policies
* Unlock Active Directory user accounts

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows Server 2016
* Windows 10 VM

**<H2>Activity**

<FE1TX1>Estimated completion time: **15–20 minutes**

<TX1>In this lab, you configure and test account lockout policies.

1. <NL\_FIRST>Log on to Windows Server and access the Default Domain Policy, Account Policies section in the Group Policy Management Editor using the methods demonstrated earlier in this chapter.
2. <NL\_MID>Click Account Lockout Policy (see Figure 11-1).

**[Insert Figure 11-1 Here]**

1. Double-click Account lockout threshold, set the invalid logon attempts to 3, and click OK. The Suggested Value Changes window appears (see Figure 11-2).

**[Insert Figure 11-2 Here]**

1. The policy you just configured will lock out an account after three invalid logon attempts. The policy, Account lockout duration, determines how long that account will remain locked after the third invalid logon attempt. If you accept the suggested setting, a user whose account is locked out can try to log on again after 30 minutes. Another policy, Reset account lockout counter after, determines how long, after the maximum permitted invalid logon attempts, users must wait before they are allowed three attempts again. If users know that after the third invalid logon attempt their account will be locked, they can stop after three failed attempts and then wait for the account lockout counter to be reset. In the suggested values shown in Figure 12-2, there isn’t much difference; users would have to wait 30 minutes whether they waited to reset the counter or waited for the account to be reset. Click OK on the Suggested Value Changes window and then set the Reset account lockout counter after policy to 2 minutes. (This low number is not consistent with best practices for security, but it will enable you to test the policies in a reasonable amount of time in class.) Click OK. Close the Group Policy Management Editor. Run gpupdate /force from a command prompt.
2. Create a user on the Windows Server named Pell Jones, username pjones with the password Pa$$word. Verify that the account is configured correctly by logging in. Log off and then log on as pjones with the password password. This will fail. Repeat this process two more times. The threshold of three invalid attempts has been reached. Attempt this invalid logon once more. Notice the error message. Attempt to log on with the correct password, Pa$$word. When the account is locked, even the correct password won’t work. The user must wait for the account lockout duration or contact the network administrator to reset the account. In some organizations where high security is required, the account lockout threshold will be set to zero, meaning that users must contact the network administrator to have the account unlocked. In our case, you can wait 2 minutes, but you still cannot log on. You have now triggered the account lockout action; and because the account lockout duration is 30 minutes, you have to wait 30 minutes before you can have another three chances to log on.
3. On Windows Server, open Active Directory Users and Computers and, in the Users container in your domain, double-click the user account for Pell Jones and click the Account tab (see Figure 11-3). Place a check mark in the box to the left of Unlock account. This account is currently locked out on this Active Directory Domain Controller.

**[Insert Figure 11-3 Here]**

1. Click the Logon Hours button. Select all the blue boxes in the schedule grid and then click the Logon Denied radio button. Then select a time-period that is not current. For example, you can use the 11:00 PM to 12:00 AM period on Sunday through Saturday (see Figure 11-4). Click the Logon Permitted button, then click OK on the Logon Hours for Pell Jones window and click Apply on the Pell Jones Properties window. Run gpupdate /force from a command prompt.

**[Insert Figure 11-4 Here]**

1. Return to Windows 10 VM and log on as pjones with the password Pa$$word. What is the result? Why?
2. Return to Windows Server and reset the permitted logon hours for Pell Jones to all hours. Close all windows and log off both systems.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.3 Given a scenario, troubleshoot common security issues.
* 4.1 Compare and contrast identity and access management concepts.
* 4.3 Given a scenario, implement identity and access management controls.
* 4.4 Given a scenario, differentiate common account management practices.

**<H2>Review Questions**

1. <MULT>The following policies are set in a GPO linked to the Windows Server 2016 domain acme.com:

Enforce password history 7 passwords remembered

Maximum password age 30 days

Minimum password age 3 days

Minimum password length 7 characters

Passwords must meet complexity requirements Enabled

Account lockout duration 60 minutes

Account lockout threshold 7 invalid logon attempts

Reset account lockout counter after 7 minutes

<TX2>Dolores Haze is a domain user in the acme.com domain. One morning, when she is logging on to the domain, an information message appears on the screen stating that she is required to change her password. She must enter her old password, enter a new password, and then confirm the new password. When she does this, and clicks the OK button, she receives the following error message: “Unable to update the password. The value provided for the new password does not meet the length, complexity, or history requirements of the domain.” Which one of the following statements is most likely to be true?

1. <MULTA>The new password was one she used less than a year ago.
2. She did not enter her old password correctly.
3. The new password did not meet the password complexity requirements of the domain.
4. **It is not possible to determine the specific reason.**
5. <MULT>The acme.com Windows Server 2016 domain has the same policies in effect as in Question 1 of this lab. Emma Bovary is a domain user in the acme.com domain. One morning, she enters the wrong domain account password for her account three times. Which of the following statements is correct?
6. <MULTA>She must wait 1 hour before attempting to log on again.
7. She must wait 7 minutes before attempting to log on again.
8. Her password does not meet the password complexity requirements of the domain.
9. **She does not have to wait before attempting to log on again.**
10. <MULT>The acme.com Windows Server 2016 domain has the same policies in effect as in Question 1 of this lab. Gerald Murphy is a domain user in the acme.com domain. Suspecting that a passing contract worker saw his password as he entered it, Gerald resets his domain account password. He enters the following password and confirms it: G3raldm. The system will not let him complete this action. Which of the following statements is most likely to be true?
11. **<MULTA>He reset his password yesterday.**
12. The password is not long enough.
13. The password does not meet the password complexity requirements of the domain.
14. He used the same password eight months ago.
15. <MULT>The acme.com Windows Server 2016 domain has the same policies in effect as in Question 1 of this lab. Eleanor Lanahan is a domain user in the acme.com domain. Eleanor is distracted and has entered her domain account password incorrectly seven times. Which of the following is a correct statement?
16. <MULTA>She should wait 1 hour before attempting to log on again.
17. **She should wait 7 minutes before attempting to log on again.**
18. She should not use any of the seven passwords she has used before.
19. Her password does not meet password complexity requirements of the domain.
20. <MULT>The acme.com Windows Server 2016 domain has the same policies in effect as in Question 1 of this lab. Walter Mitty is a domain user in the acme.com domain. Walter successfully resets his domain account password and completes his morning work. After returning from lunch and having forgotten that he had reset his password in the morning, Walter uses his previous password when attempting to log on and receives an error message stating that either the username or password is incorrect. He is sure he is using the correct password and repeats the procedures several times, always getting the same error message. Then he is shocked to receive a message stating that his account has been locked out. He is furious because he has a lot of work to do (he had taken an extra hour for lunch and now is far behind in his assignments). He goes to his supervisor to complain about the inept IT department. Which of the following is a true statement? (Choose all that apply.)
21. **<MULTA>Walter has attempted to log on eight times.**
22. Walter has attempted to log on seven times.
23. Walter could have waited 7 minutes and attempted to log on again instead of going to his supervisor.
24. **Walter could have waited an hour and attempted to log on again instead of going to his supervisor.**

# <H1>Lab 11.5 Restricting Access to Programs

**<H2>Objectives**

<TX1>Some group policies are very effective at controlling access to network resources, system configuration parameters, and programs. Others are not foolproof. For example, a group policy that prevents users from “seeing” the C: drive when opening My Computer does not prevent them from creating a desktop shortcut that links to the C: drive. Although the specific policy was enforced, the presumed objective of rendering users unable to access the C: drive was not achieved.

<TX2>On the other hand, some policies are so foolproof that they interfere with IT business processes. Although an administrator may not want regular users to access a program on their workstations, the administrator may not be able to remove the program without causing a lot of inconvenience for network staff. The command prompt (cmd.exe) is a good example. Most business users do not need to use this program, but it can be very useful for network technicians when troubleshooting workstation connectivity. In this case, a software restriction policy associated with the User Configuration portion of the GPO and linked to an OU that contained general user accounts but not network technician accounts could meet the goal.

<TX2>Although this approach sounds sensible, how would you identify the restricted program? If the policy were based on the location of the file, users might not be able to run the program in its default directory, but they could copy it to another directory and run it there. Windows Server 2016 supports this kind of policy, but also supports a policy that identifies the program by its specific characteristics (using a hash value) rather than its location. Thus, no matter where the program resided, users would be prevented from using it.

<TX2>In this lab, you configure such a policy and apply it to an OU that contains user accounts. This means that the policy will take effect when the user logs in, regardless of what computer is being used.

<TX2>After completing this lab, you will be able to:

* <BL>Create an organizational unit
* Move Active Directory objects
* Create, implement, and test a software restriction group policy
* Use the Runas command to elevate user credentials to administrative credentials

**<H2>Materials Required**

<TX1>This lab requires the following:

* <BL>Windows Server 2016
* Windows 10 VM

**<H2>Activity**

<FE1TX1>Estimated completion time: **20–30 minutes**

1. <NL\_FIRST>Log on to Windows Server as Administrator.
2. <NL\_MID>Launch Active Directory Users and Computers. Create an organizational unit under the domain: right-click the domain name, click New, and click Organizational Unit. In the Name box, type Interns, uncheck the box to the left of Protect container from accidental deletion, and click OK. Note how the organizational units (Interns and Domain Controllers) have different icons than the container folders.
3. Right-click the Interns OU, click New, and click User. Create a user named Juntu S. Bach with a user logon name of jbach. Set Juntu Bach’s password to Pa$$word and uncheck the User must change password at next logon option. Now you are going to create a group policy that will apply to all users in the Interns OU.
4. Launch the Group Policy Management console. Right-click the Interns OU and click Create a GPO in this domain, and Link it here. In the New GPO window, type Command Prompt Restriction and click OK.
5. In the left pane, click the S to the left of the Interns OU. You will see your new GPO, Command Prompt Restriction. Click the Command Prompt Restriction GPO, if necessary place a check mark in the box to the left of Do not show this message again, and click OK.
6. In the right pane, click the Settings tab. (If the Internet Explorer window appears, click Add, click Add, and click Close.) Note that neither computer nor user configurations have been entered. In the left pane, right-click the Command Prompt Restriction GPO and click Edit. Expand the Policies folder under User Configuration. Expand Windows Settings, expand Security Settings, expand and then right-click Software Restriction Policies, and select New Software Restriction Policies.
7. Right-click the Additional Rules folder and select New Hash Rule. Verify that the Security level box is set to Disallowed. Click the Browse button and navigate to C:\Windows\System32, click cmd.exe, click Open, and notice that Cmd.exe is added in the File information box. Click OK. Close the Group Policy Management Editor window. In the Group Policy Management console, click the green Refresh icon in the toolbar and notice that the Settings tab now shows a setting in the User Configuration section. Click show to the right of Security Settings, click show to the right of Software Restriction Policies/Additional Rules, and then click show to the right of Hash Rules to verify that the software restriction for Cmd.exe is listed. Run gpupdate /force from a command prompt.
8. Restart Windows 10 VM. The software restriction policy is a user policy, so when a user in the Interns OU, to which the Command Prompt Restriction GPO is linked, logs in, the policy will be enforced. Log on to Windows 10 VM as jbach with the password Pa$$word. Click Start, type cmd in the Search programs and files box, and press Enter. It looks as if your policy failed. Juntu Bach is able to open a command.
9. The problem is, the file Cmd.exe on Windows Server 2016 is different from the Cmd.exe on Windows 10 VM. You are using a hash function to identify the file, so if there’s any difference whatsoever between the two files, the hash you made on the server’s version of Cmd.exe will be totally different from the hash of Windows 10 VM’s Cmd.exe. It would seem that using the path to identify the file would be easier (C:\Windows\System32\cmd.exe), but (as stated earlier) users could work around that. So, we need to take an extra step. At the command prompt in Windows 10 VM, enter the following command: **net use \* \\Server\C$ /user:administrator.** Press Enter. If you are prompted for the administrator’s password, type Pa$$word and press Enter. You have mapped a drive to the hidden administrative share of the C: drive on Windows Server.
10. Use Windows Explorer on Windows 10 VM to navigate to C:\Windows\System32\cmd.exe on the local Windows 10 VM machine. Copy cmd.exe and paste it into the mapped drive in the root directory. You can find that mapped drive in Computer. Log out of Windows 10 VM.
11. Return to Windows Server and access the Group Policy Management console. Return to the Group Policy Management Editor and the Command Prompt Restriction GPO linked to the Interns OU. In the User Configuration, access the Software Restriction Policies and open the Additional Rules folder. Notice the version of Cmd.exe you hashed [Cmd .Exe (6.3.9600.16384)]. Delete this policy. Right-click the Additional Rules folder in the left pane and create another Hash Rule, as you did in Step 7, except this time, instead of browsing to the System32 directory, browse to C:\cmd.exe—that is, the version you copied from Windows 10 VM. Notice that this is not the same version of Cmd.exe that you identified on Windows Server’s System32 directory. Run gpupdate /force from a command prompt.
12. Return to Windows 10 VM and log in as jbach. Click Start, type cmd in the Search programs and files box, and press Enter. Now you should see an alert, as shown in Figure 11-5.

**[Insert Figure 11-5 Here]**

1. Log off Windows 10 VM and log on as pjones. Can you access a command prompt? Why?
2. Close all windows and log off both systems.

**<H2>Certification Objectives**

<TX1>Objectives for CompTIA Security+ Exam:

* <BL>2.3 Given a scenario, troubleshoot common security issues.
* 4.1 Compare and contrast identity and access management concepts.
* 4.3 Given a scenario, implement identity and access management controls.
* 4.4 Given a scenario, differentiate common account management practices.
* 6.1 Compare and contrast basic concepts of cryptography.

**<H2>Review Questions**

1. <TF>In this lab, instead of deleting the Command Prompt Restriction GPO linked to the Interns OU, we could simply have disabled it in the Group Policy Management console in the right-pane Scope tab. True or **False**?
2. <FIB>The GPO created in this lab was inefficient because, although it had only a User Configuration section policy, each computer in the Interns OU would have to process the Computer Configuration section as well, even though there are no settings there to process. A more efficient method of implementation would have been to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
3. <FIBA>configure WMI filtering in the Group Policy Management console in the right-pane Scope tab
4. configure Security Filtering in the Group Policy Management console in the right-pane Scope tab
5. **configure the GPO Status in the Group Policy Management console in the right-pane Details tab**
6. hide User Configuration in the Group Policy Management console in the right-pane Settings tab
7. <MULT>Which of the following settings can be “pushed out” to Windows 10 VM or Windows Server 2016 computers using settings in the Computer Configuration/Policies/Windows Settings/Security Settings of a GPO? (Choose all that apply.)
8. **Outbound Windows Firewall rules**
9. Folder redirection
10. **Network Access Protection client configuration**
11. **802.1x authentication protocol for use by Windows 10 VM clients on a wired network**
12. <MULT>Which of the following statements regarding Software Restriction policies is correct? (Choose all that apply.)
13. <MULTA>By default, Software Restriction policies are configured to allow domain administrators to manage trusted publishers.
14. By default, Software Restriction policies are configured to allow enterprise administrators to manage trusted publishers.
15. **Software Restriction policies allow an administrator to determine what websites are trusted for software downloads.**
16. **By default, Software Restriction policies have the security level set to unrestricted**.
17. <MULT>In this lab, jbach could not run Cmd.exe on Windows 10 VM. What could the administrator have done so that the Cmd.exe program could be run on Windows 10 VM for jbach? (Choose all that apply.)
18. **<MULTA>Move jbach’s user account out of the Interns OU.**
19. Move the Interns OU into the domain container.
20. **Configure the GPO Status in the Group Policy Management console in the right-pane Details tab.**
21. Assign full control permissions to jbach for the Interns OU.