[Lead2pass New Lead2pass 100% Valid SY0-401 Exam Questions PDF Free Download (651-675)

Lead2pass 2017 October New CompTIA SY0-401 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! Lead2pass has updated the latest version of CompTIA SY0-401 exam, which is a hot exam of CompTIA certification. It is Lead2pass CompTIA SY0-401 exam dumps that give you confidence to pass this certification exam in first attempt and with maximized score. Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 651A security administrator wants to check user password complexity. Which of the following is the BEST tool to use? A. Password historyB. Password loggingC. Password crackerD. Password hashingAnswer: CExplanation:The most important countermeasure against password crackers is to use long, complex passwords, which are changed regularly. Password-cracking tools compare hashes from potential passwords with the hashes stored in the accounts database. Each potential password is hashed, and that hash value is compared with the accounts database. If a match is found, the password- cracker tool has discovered a password for a user account. QUESTION 652When Ann an employee returns to work and logs into her workstation she notices that, several desktop configuration settings have changed. Upon a review of the CCTV logs, it is determined that someone logged into Ann's workstation. Which of the following could have prevented this from happening? A. Password complexity policy B. User access reviewsC. Shared account prohibition policyD. User assigned permissions policy Answer: AExplanation:The most important countermeasure against password crackers is to use long, complex passwords, which are changed regularly. Since changes were made to Ann's desktop configuration settings while she was not at work, means that her password was compromised. QUESTION 653After a recent internal audit, the security administrator was tasked to ensure that all credentials must be changed within 90 days, cannot be repeated, and cannot contain any dictionary words or patterns. All credentials will remain enabled regardless of the number of attempts made. Which of the following types of user account options were enforced? (Select TWO). A. RecoveryB. User assigned privilegesC. LockoutD. DisablementE. Group based privilegesF. Password expirationG. Password complexity Answer: FGExplanation:Password complexity often requires the use of a minimum of three out of four standard character types for a password. The more characters in a password that includes some character type complexity, the more resistant it is to password-cracking techniques. In most cases, passwords are set to expire every 90 days. QUESTION 654An internal auditing team would like to strengthen the password policy to support special characters. Which of the following types of password controls would achieve this goal? A. Add reverse encryptionB. Password complexityC. Increase password lengthD. Allow single sign on Answer: BExplanation:Generally, the minimum password length is considered to be 8 upper and lowercase characters. The use of at least one non-alpha character like punctuation, special characters, or numbers, combined with the password length produces strong passwords. Strong passwords are produced by the combination of a password's length and complexity. QUESTION 655The systems administrator notices that many employees are using passwords that can be easily guessed or are susceptible to brute force attacks. Which of the following would BEST mitigate this risk? A. Enforce password rules requiring complexity.B. Shorten the maximum life of account passwords.C. Increase the minimum password length.D. Enforce account lockout policies. Answer: AExplanation:Password complexity often requires the use of a minimum of three out of four standard character types for a password. The more characters in a password that includes some character complexity, the more resistant it is to brute force attacks. QUESTION 656Sara, a security manager, has decided to force expiration of all company passwords by the close of business day. Which of the following BEST supports this reasoning? A. A recent security breach in which passwords were cracked.B. Implementation of configuration management processes.C. Enforcement of password complexity requirements.D. Implementation of account lockout procedures. Answer: AExplanation:A password only needs to be changed if it doesn't meet the compliance requirements of the company's password policy, or is evidently insecure. It will also need to be changed if it has been reused, or due to possible compromise as a result of a system intrusion. QUESTION 657A security administrator is concerned about the strength of user's passwords. The company does not want to implement a password complexity policy. Which of the following can the security Administrator implement to mitigate the risk of an online password attack against users with weak passwords? A. Increase the password length requirementsB. Increase the password historyC. Shorten the password expiration periodD. Decrease the account lockout time Answer: CExplanation:Reducing the password expiration period will require passwords to be changed at the end of that period. A password needs to be changed if it doesn't meet the compliance requirements of the company's password policy, or is evidently insecure. It will also need to be changed if it has been reused, or due to possible compromise as a result of a system intrusion. This will give online password attackers less time to crack the weak passwords. QUESTION 658Which of the following should be done before resetting a user's password due to expiration? A. Verify the user's domain membership.B. Verify the user's identity.C. Advise the user of new policies.D. Verify the proper group membership. Answer: BExplanation:

When resetting a password, users have to establish their identity by answering a series of personal questions, using a hardware authentication token, or responding to a password notification e-mail. Users can then either specify a new, unlocked password, or ask that a randomly generated one be provided. This can be done from their workstation login prompt, or through a telephone call. QUESTION 659The IT department has setup a website with a series of questions to allow end users to reset their own accounts. Which of the following account management practices does this help? A. Account DisablementsB. Password ExpirationC. Password ComplexityD. Password Recovery Answer: DExplanation:People tend to forget their own passwords and because a user's password in not stored on the operating system, only a hash value is kept and most operating systems allows the administrator to change the value meaning that the password can then be recovered. If you allow end users to reset their own accounts then the password recovery process is helped along. QUESTION 660An insurance company requires an account recovery process so that information created by an employee can be accessed after that employee is no longer with the firm. Which of the following is the BEST approach to implement this process? A. Employee is required to share their password with authorized staff prior to leaving the firmB. Passwords are stored in a reversible form so that they can be recovered when neededC. Authorized employees have the ability to reset passwords so that the data is accessibleD. All employee data is exported and imported by the employee prior to them leaving the firm Answer: CExplanation:Since a user's password isn't stored on most operating systems (only a hash value is kept), most operating systems allow the administrator (or authorized person in this case) to change the value then the information/files/documents can be accessed. This is the safest way of recovery by an authorized person and is not dependent on those who leave the firm. QUESTION 661A small company has a website that provides online customer support. The company requires an account recovery process so that customers who forget their passwords can regain access.Which of the following is the BEST approach to implement this process? A. Replace passwords with hardware tokens which provide two-factor authentication to the online customer support site.B. Require the customer to physically come into the company's main office so that the customer can be authenticated prior to their password being reset.C. Web-based form that identifies customer by another mechanism and then emails the customer their forgotten password.D. Web-based form that identifies customer by another mechanism, sets a temporary password and forces a password change upon first login. Answer: DExplanation:People tend to forget their passwords, thus you should have a password recovery system for them that will not increase risk exposure. Setting a temporary password will restrict the time that the password is valid and thus decrease risk; and in addition forcing the customer to change it upon first login will make the password more secure for the customer. QUESTION 662A user has forgotten their account password. Which of the following is the BEST recovery strategy? A. Upgrade the authentication system to use biometrics instead.B. Temporarily disable password complexity requirements.C. Set a temporary password that expires upon first use.D. Retrieve the user password from the credentials database. Answer: CExplanation:Since a user's password isn't stored on most operating systems (only a hash value is kept), most operating systems allow the administrator to change the value for a user who has forgotten theirs. This new value allows the user to log in and then immediately change it to another value that they can (ideally) remember. Also setting a temporary password to expire upon first use will not allow a hacker the opportunity or time to use it. QUESTION 663Which of the following is a BEST practice when dealing with user accounts that will only need to be active for a limited time period? A. When creating the account, set the account to not remember password history.B. When creating the account, set an expiration date on the account.C. When creating the account, set a password expiration date on the account.D. When creating the account, set the account to have time of day restrictions. Answer: BExplanation:Disablement is a secure feature to employ on user accounts for temporary workers, interns, or consultants. It automatically disables a user account or causes the account to expire at a specific time and on a specific day. QUESTION 664ABC company has a lot of contractors working for them. The provisioning team does not always get notified that a contractor has left the company. Which of the following policies would prevent contractors from having access to systems in the event a contractor has left? A. Annual account reviewB. Account expiration policyC. Account lockout policyD. Account disablement Answer: BExplanation:Account expiration is a secure feature to employ on user accounts for temporary workers, interns, or consultants. It automatically disables a user account or causes the account to expire at a specific time and on a specific day. QUESTION 665Which of the following controls mitigates the risk of Matt, an attacker, gaining access to a company network by using a former employee's credential? A. Account expirationB. Password complexityC. Account lockoutD. Dual factor authentication Answer: AExplanation:Account expiration is a secure feature to employ on user accounts for temporary workers, interns, or consultants. It automatically disables a user account or causes the account to expire at a specific time and on a specific day. QUESTION 666Which of the following security benefits would be gained by disabling a terminated user account rather than deleting it? A. Retention of user keysB. Increased logging on access attemptsC. Retention of user directories and filesD. Access to quarantined files Answer: AExplanation:Account Disablement should be implemented when a user will be gone from a company whether they leave temporary or permanently. In the case of permanently leaving the company the account should be

disabled. Disablement means that the account will no longer be an active account and that the user keys for that account are retained which would not be the case if the account was deleted from the system. QUESTION 667During an audit, the security administrator discovers that there are several users that are no longer employed with the company but still have active user accounts. Which of the following should be performed? A. Account recoveryB. Account disablementC. Account lockoutsD. Account expiration Answer: BExplanation:Account Disablement should be implemented when a user will be gone from a company whether they leave temporary or permanently. In the case of permanently leaving the company the account should be disabled. Disablement means that the account will no longer be an active account. QUESTION 668A hacker has discovered a simple way to disrupt business for the day in a small company which relies on staff working remotely. In a matter of minutes the hacker was able to deny remotely working staff access to company systems with a script. Which of the following security controls is the hacker exploiting? A. DoS B. Account lockoutC. Password recoveryD. Password complexity Answer: BExplanation:B: Account lockout automatically disables an account due to repeated failed log on attempts. The hacker must have executed a script to repeatedly try logging on to the remote accounts, forcing the account lockout policy to activate. QUESTION 669Account lockout is a mitigation strategy used by Jane, the administrator, to combat which of the following attacks? (Select TWO). A. SpoofingB. Man-in-the-middleC. DictionaryD. Brute forceE. Privilege escalation Answer: CDExplanation:Account lockout is a useful method for slowing down online password-guessing attacks. A dictionary attack performs password guessing by making use of a pre-existing list of likely passwords. A brute-force attack is intended to try every possible valid combination of characters to create possible passwords in the attempt to discover the specific passwords used by user accounts. QUESTION 670A recent audit has discovered that at the time of password expiration clients are able to recycle the previous credentials for authentication. Which of the following controls should be used together to prevent this from occurring? (Select TWO). A. Password ageB. Password hashingC. Password complexityD. Password historyE. Password length Answer: ADExplanation:D: Password history determines the number of previous passwords that cannot be used when a user changes his password. For example, a password history value of 5 would disallow a user from changing his password to any of his previous 5 passwords.A: When a user is forced to change his password due to a maximum password age period expiring, he could change his password to a previously used password. Or if a password history value of 5 is configured, the user could change his password six times to cycle back round to his original password. This is where the minimum password age comes in. This is the period that a password must be used for. For example, a minimum password age of 30 would determine that when a user changes his password, he must continue to use the same password for at least 30 days. QUESTION 671A password history value of three means which of the following? A. Three different passwords are used before one can be reused.B. A password cannot be reused once changed for three years.C. After three hours a password must be re-entered to continue.D. The server stores passwords in the database for three days. Answer: AExplanation:Password History defines the number of unique new passwords a user must use before an old password can be reused. QUESTION 672An administrator discovers that many users have used their same passwords for years even though the network requires that the passwords be changed every six weeks. Which of the following, when used together, would BEST prevent users from reusing their existing password? (Select TWO). A. Length of passwordB. Password historyC. Minimum password ageD. Password expirationE. Password complexityF. Non-dictionary words Answer: BCExplanation:In this question, users are forced to change their passwords every six weeks. However, they are able to change their password and enter the same password as the new password. Password history determines the number of previous passwords that cannot be used when a user changes his password. For example, a password history value of 5 would disallow a user from changing his password to any of his previous 5 passwords. When a user is forced to change his password due to a maximum password age period expiring, (the question states that the network requires that the passwords be changed every six weeks) he could change his password to a previously used password. Or if a password history value of 5 is configured, the user could change his password six times to cycle back round to his original password. This is where the minimum password age comes in. This is the period that a password must be used for. For example, a minimum password age of 30 would determine that when a user changes his password, he must continue to use the same password for at least 30 days. QUESTION 673A system administrator has noticed that users change their password many times to cycle back to the original password when their passwords expire. Which of the following would BEST prevent this behavior? A. Assign users passwords based upon job role.B. Enforce a minimum password age policy.C. Prevent users from choosing their own passwords.D. Increase the password expiration time frame. Answer: BExplanation:A minimum password age policy defines the period that a password must be used for before it can be changed. QUESTION 674Which of the following is an important implementation consideration when deploying a wireless network that uses a shared password? A. Authentication serverB. Server certificateC. Key lengthD. EAP method Answer: C Explanation:Key length is the main issue of concern since the wireless network uses a shared password. With risks of shared passwords makes the length of the password a crucial factor to risk mitigation. QUESTION 675A security administrator is

reviewing the below output from a password auditing tool: P@ss.@pW1.S3cU4 Which of the following additional policies should be implemented based on the tool's output? A. Password ageB. Password historyC. Password lengthD. Password complexity Answer: CExplanation:The output shows that all the passwords are either 4 or 5 characters long. This is way too short, 8 characters are shown to be the minimum for password length. More free Lead2pass SY0-401 exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDLXZsWm9MWmh0a0E Lead2pass offers you all the SY0-401 exam questions which are the same as your real test with 100% correct and coverage rate. We provide the latest full version of SY0-401 PDF and VCE dumps to ensure your SY0-401 exam 100% pass. 2017 CompTIA SY0-401 (All 1868 Q&As) exam dumps (PDF&VCE) from Lead2pass: https://www.lead2pass.com/sy0-401.html [100% Exam Pass Guaranteed]