[Lead2pass New Lead2pass SY0-401 Exam Questions Guarantee SY0-401 Certification Exam 100% Success (626-650)

Lead2pass 2017 October New CompTIA SY0-401 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! How to 100% pass SY0-401 exam? Lead2pass SY0-401 dump is unparalleled in quality and is 100% guaranteed to make you pass SY0-401 exam. All the SY0-401 exam questions are the latest. Here are some free share of CompTIA SY0-401 dumps. Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 626The company's sales team plans to work late to provide the Chief Executive Officer (CEO) with a special report of sales before the quarter ends. After working for several hours, the team finds they cannot save or print the reports.Which of the following controls is preventing them from completing their work? A. Discretionary access controlB. Role-based access controlC. Time of Day access controlD. Mandatory access controlAnswer: CExplanation:Time of day restrictions limit when users can access specific systems based on the time of day or week. It can limit access to sensitive environments to normal business hours when oversight and monitoring can be performed to prevent fraud, abuse, or intrusion. In this case, the sales team is prevented from saving or printing reports after a certain time. QUESTION 627Which of the following security concepts can prevent a user from logging on from home during the weekends? A. Time of day restrictionsB. Multifactor authenticationC. Implicit denyD. Common access card Answer: AExplanation:Time of day restrictions limit when users can access specific systems based on the time of day or week. It can limit access to sensitive environments to normal business hours when oversight and monitoring can be performed to prevent fraud, abuse, or intrusion. QUESTION 628A technician is reviewing the logical access control method an organization uses. One of the senior managers requests that the technician prevent staff members from logging on during nonworking days. Which of the following should the technician implement to meet managements request? A. Enforce KerberosB. Deploy smart cardsC. Time of day restrictionsD. Access control lists Answer: CExplanation:Time of day restrictions limit when users can access specific systems based on the time of day or week. It can limit access to sensitive environments to normal business hours. QUESTION 629 Ann, the security administrator, wishes to implement multifactor security. Which of the following should be implemented in order to compliment password usage and smart cards? A. Hard tokensB. Fingerprint readersC. Swipe badge readersD. Passphrases Answer: BExplanation:A multifactor authentication method uses two or more processes for logon. A twofactor method might use smart cards and biometrics for logon. For obvious reasons, the two or more factors employed should not be from the same category. QUESTION 630Hotspot QuestionFor each of the given items, select the appropriate authentication category from the dropdown choices.Instructions: When you have completed the simulation, please select the Done button to submit. Answer: Explanation: Something you are includes fingerprints, retina scans, or voice recognition.Something you have includes smart cards, token devices, or keys.Something you know includes a passwords, codes, PINs, combinations, or secret phrases.Somewhere you are includes a physical location s or logical addresses, such as domain name, an IP address, or a MAC address.Something you do includes your typing rhythm, a secret handshake, or a private knock
http://en.wikipedia.org/wiki/Password_authentication_protocol#Working_cycle http://en.wikipedia.org/wiki/Smart_card#Security QUESTION 631A network administrator uses an RFID card to enter the datacenter, a key to open the server rack, and a username and password to logon to a server. These are examples of which of the following? A. Multifactor authenticationB. Single factor authenticationC. Separation of dutiesD. Identification Answer: BExplanation:Single-factor authentication (SFA) is a process for securing access to a given system by identifying the party requesting access via a single category of credentials. In this case, the network administrator makes use of an RFID card to access the datacenter, a key to access the server rack, and a username and password to access a server. QUESTION 632Use of a smart card to authenticate remote servers remains MOST susceptible to which of the following attacks? A. Malicious code on the local systemB. Shoulder surfingC. Brute force certificate crackingD. Distributed dictionary attacks Answer: AExplanation:Once a user authenticates to a remote server, malicious code on the user's workstation could then infect the server. QUESTION 633Employee badges are encoded with a private encryption key and specific personal information.The encoding is then used to provide access to the network. Which of the following describes this access control type? A. SmartcardB. TokenC. Discretionary access controlD. Mandatory access control Answer: AExplanation: Smart cards are credit-card-sized IDs, badges, or security passes with an embedded integrated circuit chip that can include data regarding the authorized bearer. This data can then be used for identification and/or authentication purposes. QUESTION 634LDAP and Kerberos are commonly used for which of the following? A. To perform queries on a directory serviceB. To store usernames and passwords for Federated IdentityC. To sign SSL wildcard certificates for subdomainsD. To utilize single sign-on capabilities Answer: DExplanation:Single sign-on is usually achieved via the Lightweight Directory Access Protocol (LDAP), although Kerberos can also be used. QUESTION 635After Ann, a user, logs into her banking websites she has access to her financial

institution mortgage, credit card, and brokerage websites as well. Which of the following is being described? A. Trusted OSB. Mandatory access controlC. Separation of dutiesD. Single sign-on Answer: DExplanation:Single sign-on means that once a user (or other subject) is authenticated into a realm, re- authentication is not required for access to resources on any realm entity. The question states that when Ann logs into her banking websites she has access to her financial institution mortgage, credit card, and brokerage websites as well. This describes an SSO scenario. QUESTION 636A company wants to ensure that all credentials for various systems are saved within a central database so that users only have to login once for access to all systems. Which of the following would accomplish this? A. Multi-factor authenticationB. Smart card accessC. Same Sign-OnD. Single Sign-On Answer: DExplanation:Single sign-on means that once a user (or other subject) is authenticated into a realm, re- authentication is not required for access to resources on any realm entity. Single sign-on is able to internally translate and store credentials for the various mechanisms, from the credential used for original authentication. QUESTION 637A user attempting to log on to a workstation for the first time is prompted for the following information before being granted access: username, password, and a four-digit security pin that was mailed to him during account registration. This is an example of which of the following? A. Dual-factor authenticationB. Multifactor authenticationC. Single factor authenticationD. Biometric authentication Answer: CExplanation: Multi-factor authentication (MFA) is a method of computer access control which a user can pass by successfully presenting authentication factors from at least two of the three categories:knowledge factors ("things only the user knows"), such as passwords possession factors ("things only the user has"), such as ATM cards inherence factors ("things only the user is"), such as biometricsIn this question a username, password, and a four-digit security pin knowledge are all knowledge factors (something the user knows). Therefore, this is single-factor authentication. QUESTION 638Which of the following allows a network administrator to implement an access control policy based on individual user characteristics and NOT on job function? A. Attributes basedB. Implicit deny C. Role basedD. Rule based Answer: AExplanation:Attribute-based access control allows access rights to be granted to users via policies, which combine attributes together. The policies can make use of any type of attributes, which includes user attributes, resource attributes and environment attributes. QUESTION 639Which of the following is best practice to put at the end of an ACL? A. Implicit denyB. Time of day restrictionsC. Implicit allowD. SNMP string Answer: AExplanation:An implicit deny clause is implied at the end of each ACL. This implies that if you aren't specifically granted access or privileges for a resource, you're denied access by default. The implicit deny clause is set by the system. QUESTION 640Users report that they are unable to access network printing services. The security technician checks the router access list and sees that web, email, and secure shell are allowed. Which of the following is blocking network printing? A. Port securityB. Flood guardsC. Loop protectionD. Implicit deny Answer: DExplanation:Implicit deny says that if you aren't explicitly granted access or privileges for a resource, you're denied access by default. The scenario does not state that network printing is allowed in the router access list, therefore, it must be denied by default. QUESTION 641Failure to validate the size of a variable before writing it to memory could result in which of the following application attacks? A. Malicious logicB. Cross-site scriptingC. SQL injectionD. Buffer overflow Answer: D QUESTION 642In order for Sara, a client, to logon to her desktop computer, she must provide her username, password, and a four digit PIN. Which of the following authentication methods is Sara using? A. Three factorB. Single factorC. Two factorD. Four factor Answer: BExplanation:Single-factor authentication is when only one authentication factor is used. In this case, Something you know is being used as an authentication factor. Username, password, and PIN form part of Something you know. QUESTION 643The security department has implemented a new laptop encryption product in the environment. The product requires one user name and password at the time of boot up and also another password after the operating system has finished loading. This setup is using which of the following authentication types? A. Two-factor authenticationB. Single sign-onC. Multifactor authenticationD. Single factor authentication Answer: DExplanation:Single-factor authentication is when only one authentication factor is used. In this case, Something you know is being used as an authentication factor. Username, password, and PIN form part of Something you know. QUESTION 644Which of the following is a measure of biometrics performance which rates the ability of a system to correctly authenticate an authorized user? A. Failure to captureB. Type IIC. Mean time to registerD. Template capacity Answer: BExplanation:Type II, or false acceptance rate (FAR), is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. QUESTION 645Use of group accounts should be minimized to ensure which of the following? A. Password securityB. Regular auditingC. Baseline managementD. Individual accountability Answer: DExplanation:Holding users accountable for their actions is part of security, and can only be achieved by users having their own user accounts. To adequately provide accountability, the use of shared or group accounts should be discouraged. QUESTION 646The system administrator is tasked with changing the administrator password across all 2000 computers in the organization. Which of the following should the system administrator implement to accomplish this task? A. A security groupB. A group policyC. Key escrowD. Certificate revocation Answer: BExplanation:Group policy is used to

manage Windows systems in a Windows network domain environment by means of a Group Policy Object (GPO). GPO's include a number of settings related to credentials, such as password complexity requirements, password history, password length, account lockout settings. QUESTION 647A network inventory discovery application requires non-privileged access to all hosts on a network for inventory of installed applications. A service account is created by the network inventory discovery application for accessing all hosts. Which of the following is the MOST efficient method for granting the account non-privileged access to the hosts? A. Implement Group Policy to add the account to the users group on the hostsB. Add the account to the Domain Administrator group C. Add the account to the Users group on the hostsD. Implement Group Policy to add the account to the Power Users group on the hosts. Answer: AExplanation:Group Policy is an infrastructure that allows you to implement specific configurations for users and computers. Group Policy settings are contained in Group Policy objects (GPOs), which are linked to the following Active Directory directory service containers: sites, domains, or organizational units (OUs). This means that if the GPO is linked to the domain, all Users groups in the domain will include the service account. QUESTION 648A group policy requires users in an organization to use strong passwords that must be changed every 15 days. Joe and Ann were hired 16 days ago. When Joe logs into the network, he is prompted to change his password; when Ann logs into the network, she is not prompted to change her password. Which of the following BEST explains why Ann is not required to change her password? A. Ann's user account has administrator privileges.B. Joe's user account was not added to the group policy.C. Ann's user account was not added to the group policy.D. Joe's user account was inadvertently disabled and must be re-created. Answer: CExplanation:Group policy is used to manage Windows systems in a Windows network domain environment by means of a Group Policy Object (GPO). GPO's include a number of settings related to credentials, which includes password expiration. Because Anne was not prompted to change her password, it could only mean that her user account was not added to the group policy. QUESTION 649An auditing team has found that passwords do not meet best business practices. Which of the following will MOST increase the security of the passwords? (Select TWO). A. Password ComplexityB. Password ExpirationC. Password AgeD. Password LengthE. Password History Answer: ADExplanation:Passwords should have the strength to avoid discovery through attack, but it should also be easy enough for the user to remember. The length and complexity of a password combined are vital factors in defining a password's strength. QUESTION 650Which of the following passwords is the LEAST complex? A. MyTrain!45B. Mytr@in!!C. MyTr@in12D. MyTr@in#8 Answer: BExplanation:Password policies often enforce a minimum of three out of four standard character types, which includes uppercase and lowercase letters, numbers, and symbols. Although this option includes three of the four character types, it does not include numbers, which makes it less complex than the other options. More free Lead2pass SY0-401 exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDLXZsWm9MWmh0a0E Always up-to-date Lead2pass SY0-401 VCE - everything you need for your CompTIA SY0-401 exam to pass. Our CompTIA SY0-401 software allows you to practise exam dumps in real SY0-401 exam environment. Welcome to choose. 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]