[Lead2pass New Lead2pass SY0-401 Exam Dumps New Updated By CompTIA Official Exam Center (551-575)

Lead2pass 2017 October New CompTIA SY0-401 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! Test your preparation for CompTIA SY0-401 with these actual SY0-401 new questions below. Exam questions are a sure method to validate one's preparation for actual certification exam. Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 551Which of the following can be used to maintain a higher level of security in a SAN by allowing isolation of mis-configurations or faults? A. VLANB. Protocol securityC. Port securityD. VSANAnswer: DExplanation:A storage area network (SAN) is a secondary network that offers storage isolation by consolidating storage devices such as hard drives, drive arrays, optical jukeboxes, and tape libraries. Virtualization can be used to further enhance the security of a SAN by using switches to create a VSAN. These switches act as routers controlling and filtering traffic into and out of the VSAN while allowing unrestricted traffic within the VSAN. QUESTION 552A company needs to receive data that contains personally identifiable information. The company requires both the transmission and data at rest to be encrypted. Which of the following achieves this goal? (Select TWO). A. SSHB. TFTPC. NTLMD. TKIPE. SMTPF. PGP/GPG Answer: AFExplanation:We can use SSH to encrypt the transmission and PGP/GPG to encrypt the data at rest (on disk).A: Secure Shell (SSH) is a cryptographic protocol that can be used to secure network communication. It establishes a secure tunnel over an insecure network.F: Pretty Good Privacy (PGP) is a data encryption and decryption solution that can be used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. QUESTION 553Which of the following does full disk encryption prevent? A. Client side attacksB. Clear text accessC. Database theftD. Network-based attacks Answer: BExplanation:Full-disk encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen. QUESTION 554Full disk encryption is MOST effective against which of the following threats? A. Denial of service by data destructionB. Eavesdropping emanationsC. Malicious codeD. Theft of hardware Answer: DExplanation:Full-disk encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen. However, it does not prevent the theft of hardware it only protects data should the device be stolen. QUESTION 555Which of the following is the BEST method for ensuring all files and folders are encrypted on all corporate laptops where the file structures are unknown? A. Folder encryptionB. File encryptionC. Whole disk encryptionD. Steganography Answer: CExplanation:Full-disk encryption encrypts the data on the hard drive of the device or on a removable drive. This feature ensures that the data on the device or removable drive cannot be accessed in a useable form should it be stolen. Furthermore, full-disk encryption is not dependant on knowledge of the file structure. QUESTION 556To protect corporate data on removable media, a security policy should mandate that all removable devices use which of the following? A. Full disk encryptionB. Application isolationC. Digital rights managementD. Data execution prevention Answer: AExplanation:Full-disk encryption encrypts the data on the hard drive of the device or on a removable drive. This feature ensures that the data on the device or removable drive cannot be accessed in a useable form should it be stolen. QUESTION 557A merchant acquirer has the need to store credit card numbers in a transactional database in a high performance environment. Which of the following BEST protects the credit card data? A. Database field encryptionB. File-level encryptionC. Data loss prevention systemD. Full disk encryption Answer: AExplanation:Database encryption makes use of cryptography functions that are built into the database software to encrypt the data stored in the data base. This often offers granular encryption options which allows for the encryptions of the entire database, specific database tables, or specific database fields, such as a credit card number field. QUESTION 558Which of the following types of data encryption would Matt, a security administrator, use to encrypt a specific table? A. Full diskB. Individual filesC. DatabaseD. Removable media Answer: CExplanation:A table is stored in a database. Database encryption makes use of cryptography functions that are built into the database software to encrypt the data stored in the database. This often offers granular encryption options which allows for the encryptions of the entire database, specific database tables, or specific database fields, such as a credit card number field. QUESTION 559A database administrator would like to start encrypting database exports stored on the SAN, but the storage administrator warns that this may drastically increase the amount of disk space used by the exports. Which of the following explains the reason for the increase in disk space usage? A. Deduplication is not compatible with encryptionB. The exports are being stored on smaller SAS drivesC. Encrypted files are much larger than unencrypted filesD. The SAN already uses encryption at rest Answer: CExplanation:Encryption adds overhead to the data which results in and increase in file size. This overhead is attached to each file and could include the encryption/decryption key, data recovery files and data decryption field in file header. As a result, requires increased storage space. QUESTION 560Which of the following is an advantage of implementing individual file encryption

on a hard drive which already deploys full disk encryption? A. Reduces processing overhead required to access the encrypted filesB. Double encryption causes the individually encrypted files to partially lose their propertiesC. Individually encrypted files will remain encrypted when copied to external mediaD. File level access control only apply to individually encrypted files in a fully encrypted drive Answer: CExplanation:With full disk encryption a file is encrypted as long as it remains on the disk. This is because the data on the disk is decrypted when the user logs on, thus the data is in a decrypted form when it is copied to another disk. Individually encrypted files on the other hand remain encrypted. QUESTION 561A team of firewall administrators have access to a `master password list' containing service account passwords. Which of the following BEST protects the master password list? A. File encryptionB. Password hashingC. USB encryptionD. Full disk encryption Answer: AExplanation:File encryption can be used to protect the contents of individual files. It uses randomly generated symmetric encryption keys for the file and stores the key in an encrypted form using the user's public key on the encrypted file. QUESTION 562A security administrator has concerns regarding employees saving data on company provided mobile devices. Which of the following would BEST address the administrator's concerns? A. Install a mobile application that tracks read and write functions on the device.B. Create a company policy prohibiting the use of mobile devices for personal use.C. Enable GPS functionality to track the location of the mobile devices.D. Configure the devices so that removable media use is disabled. Answer: DExplanation:Mobile devices can be plugged into computers where they appear as an additional disk in the same way as a USB drive. This is known as removable media. This would enable users to copy company data onto the mobile devices. By disabling removable media use, the users will not be able to copy data onto the mobile devices. QUESTION 563Which of the following can be used to mitigate risk if a mobile device is lost? A. Cable lockB. Transport encryptionC. Voice encryptionD. Strong passwords Answer: DExplanation:Passwords are the most likely mechanism that can be used to mitigate risk when a mobile device is lost. A strong password would be more difficult to crack. QUESTION 564Which of the following types of encryption will help in protecting files on a PED? A. Mobile device encryptionB. Transport layer encryptionC. Encrypted hidden containerD. Database encryption Answer: AExplanation:Device encryption encrypts the data on a Personal Electronic Device (PED). This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen. QUESTION 565Which of the following is a way to implement a technical control to mitigate data loss in case of a mobile device theft? A. Disk encryptionB. Encryption policyC. Solid state driveD. Mobile device policy Answer: AExplanation:Disk and device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen. QUESTION 566An SSL/TLS private key is installed on a corporate web proxy in order to inspect HTTPS requests. Which of the following describes how this private key should be stored so that it is protected from theft? A. Implement full disk encryptionB. Store on encrypted removable mediaC. Utilize a hardware security moduleD. Store on web proxy file system Answer: CExplanation:Hardware Security Module (HSM) hardware-based encryption solution that is usually used in conjunction with PKI to enhance security with certification authorities (CAs). It is available as an expansion card and can cryptographic keys, passwords, or certificates. QUESTION 567Which of the following has a storage root key? A. HSMB. EFSC. TPMD. TKIP Answer: CExplanation:Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disable in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates on non-volatile (NV) memory. Data stored on NV memory is retained unaltered when the device has no power. The storage root key is embedded in the TPM to protect TPM keys created by applications, so that these keys cannot be used without the TPM. QUESTION 568Which of the following would be used when a higher level of security is desired for encryption key storage? A. TACACS+B. L2TPC. LDAPD. TPM Answer: DExplanation:Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disable in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates. QUESTION 569Which of the following is a hardware based encryption device? A. EFSB. TrueCryptC. TPMD. SLE Answer: CExplanation:Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disable in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates. QUESTION 570A company wants to ensure that all aspects if data are protected when sending to other sites within the enterprise. Which of the following would ensure some type of encryption is performed while data is in transit? A. SSHB. SHA1C. TPMD. MD5 Answer: A QUESTION 571Which of the following should be enabled in a laptop's BIOS prior to full disk encryption? A. USBB. HSMC. RAIDD. TPM Answer: DExplanation:Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disable in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates. QUESTION 572Which of the following is a hardware-based security technology included in a computer? A. Symmetric keyB. Asymmetric keyC. Whole disk encryptionD. Trusted platform module Answer: DExplanation:Trusted Platform Module (TPM) is a hardware-based encryption solution that is

embedded in the system's motherboard and is enabled or disable in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates. QUESTION 573Which of the following provides dedicated hardware-based cryptographic functions to an operating system and its applications running on laptops and desktops? A. TPMB. HSMC. CPUD. FPU Answer: AExplanation:Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disable in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates. QUESTION 574Which of the following is built into the hardware of most laptops but is not setup for centralized management by default? A. Whole disk encryptionB. TPM encryptionC. USB encryptionD. Individual file encryption Answer: BExplanation:Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disable in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates. QUESTION 575A hospital IT department wanted to secure its doctor's tablets. The IT department wants operating system level security and the ability to secure the data from alteration. Which of the following methods would MOST likely work? A. Cloud storageB. Removal MediaC. TPMD. Wiping Answer: CExplanation:Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disable in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.More free Lead2pass SY0-401 exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDLXZsWm9MWmh0a0E These CompTIA SY0-401 exam questions are all a small selection of questions. If you want to practice more questions for actual SY0-401 exam, use the links at the end of this document. Also you can find links for SY0-401 VCE software that is great for preparation and self-assessment for CompTIA SY0-401 exam. 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]