[Lead2pass New Lead2pass SY0-401 Exam Dumps New Updated By CompTIA Official Exam Center (576-600)

Lead2pass 2017 October New CompTIA SY0-401 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! How to 100% pass SY0-401 exam? Lead2pass provides the guaranteed SY0-401 exam dumps to boost up your confidence in SY0-401 exam. Successful candidates have provided their reviews about our SY0-401 dumps. Now Lead2pass supplying the new version of SY0-401 VCE and PDF dumps. We ensure our SY0-401 exam questions are the most complete and authoritative compared with others', which will ensure your SY0-401 exam pass. Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 576Which of the following hardware based encryption devices is used as a part of multi-factor authentication to access a secured computing system? A. Database encryptionB. USB encryptionC. Whole disk encryptionD. TPMAnswer: 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 577The systems administrator wishes to implement a hardware-based encryption method that could also be used to sign code. They can achieve this by: A. Utilizing the already present TPM.B. Configuring secure application sandboxes.C. Enforcing whole disk encryption.D. Moving data and applications into the cloud. 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 578Which of the following BEST explains the use of an HSM within the company servers? A. Thumb drives present a significant threat which is mitigated by HSM.B. Software encryption can perform multiple functions required by HSM.C. Data loss by removable media can be prevented with DLP.D. Hardware encryption is faster than software encryption. Answer: DExplanation:Hardware Security Module (HSM) is a cryptoprocessor that can be used to enhance security. It provides a fast solution for the for large asymmetrical encryption calculations and is much faster than software-based cryptographic solutions. QUESTION 579Access mechanisms to data on encrypted USB hard drives must be implemented correctly otherwise: A. user accounts may be inadvertently locked out.B. data on the USB drive could be corrupted.C. data on the hard drive will be vulnerable to log analysis.D. the security controls on the USB drive can be bypassed. Answer: DExplanation:A common access mechanism to data on encrypted USB hard drives is a password. If a weak password is used, someone could guess the password and bypass the security controls on the USB drive to access the data. QUESTION 580A security administrator has implemented a policy to prevent data loss. Which of the following is the BEST method of enforcement? A. Internet networks can be accessed via personally-owned computers.B. Data can only be stored on local workstations.C. Wi-Fi networks should use WEP encryption by default.D. Only USB devices supporting encryption are to be used. Answer: DExplanation:The concern for preventing data loss is the concern for maintaining data confidentiality. This can be accomplished through encryption, access controls, and steganography. USB encryption is usually provided by the vendor of the USB device. It is not included on all USB devices. QUESTION 581Which of the following data security techniques will allow Matt, an IT security technician, to encrypt a system with speed as its primary consideration? A. Hard drive encryptionB. Infrastructure as a serviceC. Software based encryptionD. Data loss prevention 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. It should be implemented using a hardware-based solution for greater speed. QUESTION 582A large corporation has data centers geographically distributed across multiple continents. The company needs to securely transfer large amounts of data between the data center. The data transfer can be accomplished physically or electronically, but must prevent eavesdropping while the data is on transit. Which of the following represents the BEST cryptographic solution? A. Driving a van full of Micro SD cards from data center to data center to transfer dataB. Exchanging VPN keys between each data center via an SSL connection and transferring the data in the VPNC. Using a courier to deliver symmetric VPN keys to each data center and transferring data in the VPND. Using PKI to encrypt each file and transferring them via an Internet based FTP or cloud server Answer: BExplanation:A virtual private network (VPN) is an encrypted communication tunnel that connects two systems over an untrusted network, such as the Internet. They provide security for both authentication and data transmission through a process called encapsulation. Secure Sockets Layer (SSL) can be used to exchange the VPN keys securely. SSL is used to establish secure TCP communication between two machines by encrypting the communication. QUESTION 583A security administrator wants to ensure that the message the administrator sends out to their Chief Financial Officer (CFO) does not get changed in route. Which of the following is the administrator MOST concerned with? A. Data confidentialityB. High availabilityC. Data integrityD. Business continuity Answer: CExplanation:Integrity is the process of ensuring that the information has not been altered during transmission.This can be accomplished by means of hashing.

QUESTION 584An administrator wants to ensure that the reclaimed space of a hard drive has been sanitized while the computer is in use. Which of the following can be implemented? A. Cluster tip wipingB. Individual file encryptionC. Full disk encryptionD. Storage retention Answer: AExplanation:A computer hard disk is divided into small segments called clusters. A file usually spans several clusters but rarely fills the last cluster, which is called cluster tip. This cluster tip area may contain file data because the size of the file you are working with may grow or shrink and needs to be securely deleted. QUESTION 585The act of magnetically erasing all of the data on a disk is known as: A. WipingB. DissolutionC. ScrubbingD. Degaussing Answer: DExplanation:Degaussing is a form a data wiping that entails the use of magnets to alter the magnetic structure of the storage medium. QUESTION 586Company XYZ recently salvaged company laptops and removed all hard drives, but the Chief Information Officer (CIO) is concerned about disclosure of confidential information. Which of the following is the MOST secure method to dispose of these hard drives? A. DegaussingB. Physical DestructionC. Lock up hard drives in a secure safeD. Wipe Answer: BExplanation:The physical description of hard drives is the only secure means of disposing hard drives. This can include incineration, an acid bath, and crushing. QUESTION 587During a recent investigation, an auditor discovered that an engineer's compromised workstation was being used to connect to SCADA systems while the engineer was not logged in. The engineer is responsible for administering the SCADA systems and cannot be blocked from connecting to them. The SCADA systems cannot be modified without vendor approval which requires months of testing.Which of the following is MOST likely to protect the SCADA systems from misuse? A. Update anti-virus definitions on SCADA systemsB. Audit accounts on the SCADA systemsC. Install a firewall on the SCADA networkD. Deploy NIPS at the edge of the SCADA network Answer: DExplanation:A supervisory control and data acquisition (SCADA) system is an industrial control system (ICS) that is used to control infrastructure processes, facility-based processes, or industrial processes. A network-based IPS (NIPS) is an intrusion detection and prevention system that scans network traffic in real time against a database of attack signatures. It is useful for detecting and responding to network-based attacks originating from outside the organization. QUESTION 588Which of the following are examples of network segmentation? (Select TWO). A. IDSB. IaaSC. DMZD. SubnetE. IPS Answer: CDExplanation:C: A demilitarized zone (DMZ) is a part of the network that is separated of segmented from the rest of the network by means of firewalls and acts as a buffer between the untrusted public Internet and the trusted local area network (LAN).D. IP subnets can be used to separate or segment networks while allowing communication between the network segments via routers. QUESTION 589Which of the following can be implemented in hardware or software to protect a web server from cross-site scripting attacks? A. Intrusion Detection SystemB. Flood Guard ProtectionC. Web Application FirewallD. URL Content Filter Answer: CExplanation:Cross-site scripting (XSS) is a form of malicious code-injection attack on a web server in which an attacker injects code into the content sent to website visitors. XSS can be mitigated by implementing patch management on the web server, using firewalls, and auditing for suspicious activity. QUESTION 590When considering a vendor-specific vulnerability in critical industrial control systems which of the following techniques supports availability? A. Deploying identical application firewalls at the borderB. Incorporating diversity into redundant designC. Enforcing application white lists on the support workstationsD. Ensuring the systems' anti-virus definitions are up-to-date Answer: BExplanation:If you know there is a vulnerability that is specific to one vendor, you can improve availability by implementing multiple systems that include at least one system from a different vendor and so is not affected by the vulnerability. QUESTION 591Jane, a security administrator, needs to implement a secure wireless authentication method that uses a remote RADIUS server for authentication.Which of the following is an authentication method Jane should use? A. WPA2-PSKB. WEP-PSKC. CCMPD. LEAP Answer: DExplanation:A RADIUS server is a server with a database of user accounts and passwords used as a central authentication database for users requiring network access. The Lightweight Extensible Authentication Protocol (LEAP) is a proprietary wireless LAN authentication method developed by Cisco Systems. Important features of LEAP are dynamic WEP keys and mutual authentication (between a wireless client and a RADIUS server). LEAP allows for clients to reauthenticate frequently; upon each successful authentication, the clients acquire a new WEP key (with the hope that the WEP keys don't live long enough to be cracked). LEAP may be configured to use TKIP instead of dynamic WEP. QUESTION 592Ann, a security administrator, wishes to replace their RADIUS authentication with a more secure protocol, which can utilize EAP. Which of the following would BEST fit her objective? A. CHAPB. SAMLC. KerberosD. Diameter Answer: DExplanation:Diameter is an authentication, authorization, and accounting protocol that replaces the RADIUS protocol. Diameter Applications extend the base protocol by including new commands and/or attributes, such as those for use of the Extensible Authentication Protocol (EAP). QUESTION 593Which of the following is an authentication service that uses UDP as a transport medium? A. TACACS+B. LDAPC. KerberosD. RADIUS Answer: DExplanation: RADIUS runs in the application layer and makes use of UDP as transport. QUESTION 594Pete, a security auditor, has detected clear text passwords between the RADIUS server and the authenticator. Which of the following is configured in the RADIUS server and what technologies should the authentication protocol

be changed to? A. PAP, MSCHAPv2B. CHAP, PAPC. MSCHAPv2, NTLMv2D. NTLM, NTLMv2 Answer: AExplanation:PAP transmits the username and password to the authentication server in plain text. MSCHAPv2 is utilized as an authentication option for RADIUS servers that are used for Wi-Fi security using the WPA-Enterprise protocol. QUESTION 595RADIUS provides which of the following? A. Authentication, Authorization, AvailabilityB. Authentication, Authorization, AuditingC. Authentication, Accounting, AuditingD. Authentication, Authorization, Accounting Answer: DExplanation:The Remote Authentication Dial In User Service (RADIUS) networking protocol offers centralized Authentication, Authorization, and Accounting (AAA) management for users who make use of a network service. It is for this reason that A, B, and C: are incorrect. http://en.wikipedia.org/wiki/RADIUS QUESTION 596Which of the following types of security services are used to support authentication for remote users and devices? A. BiometricsB. HSMC. RADIUSD. TACACS Answer: CExplanation:RADIUS authentication phase takes place when a network client connects to a network access server (NAS) and provides authentication credentials. The NAS will then make use of the authentication credentials to issue a RADIUS authentication request to the RADIUS server, which will then exchange RADIUS authentication messages with the NAS. QUESTION 597Which of the following relies on the use of shared secrets to protect communication? A. RADIUSB. KerberosC. PKID. LDAP Answer: AExplanation:Obfuscated passwords are transmitted by the RADIUS protocol via a shared secret and the MD5 hashing algorithm. QUESTION 598Ann has taken over as the new head of the IT department. One of her first assignments was to implement AAA in preparation for the company's new telecommuting policy. When she takes inventory of the organizations existing network infrastructure, she makes note that it is a mix of several different vendors. Ann knows she needs a method of secure centralized access to the company's network resources. Which of the following is the BEST service for Ann to implement? A. RADIUSB. LDAPC. SAMLD. TACACS+ Answer: AExplanation:The Remote Authentication Dial In User Service (RADIUS) networking protocol offers centralized Authentication, Authorization, and Accounting (AAA) management for users who make use of a network service. QUESTION 599Which of the following is mainly used for remote access into the network? A. XTACACSB. TACACS+C. KerberosD. RADIUS Answer: DExplanation:Most gateways that control access to the network have a RADIUS client component that communicates with the RADIUS server. Therefore, it can be inferred that RADIUS is primarily used for remote access. QUESTION 600A system administrator is using a packet sniffer to troubleshoot remote authentication. The administrator detects a device trying to communicate to TCP port 49. Which of the following authentication methods is MOST likely being attempted? A. RADIUSB. TACACS+C. KerberosD. LDAP Answer: BExplanation:TACACS makes use of TCP port 49 by default. More free Lead2pass SY0-401 exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDLXZsWm9MWmh0a0E All the SY0-401 braindumps are updated. Get a complete hold of SY0-401 PDF dumps and SY0-401 practice test with free VCE player through Lead2pass and boost up your skills. 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]