[2017 New Lead2pass Latest CompTIA SY0-401 Exam Questions Free Download (201-225)

2017 August CompTIA Official New Released SY0-401 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed!

Are you interested in successfully completing the CompTIA SY0-401 Certification Then start to earning Salary? Lead2pass has leading edge developed CompTIA exam questions that will ensure you pass this SY0-401 exam! Lead2pass delivers you the most accurate, current and latest updated SY0-401 Certification exam questions and available with a 100% money back guarantee promise! Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 201Several employees submit the same phishing email to the administrator. The administrator finds that the links in the email are not being blocked by the company's security device. Which of the following might the administrator do in the short term to prevent the emails from being received? A. Configure an ACLB. Implement a URL filterC. Add the domain to a block listD. Enable TLS on the mail serverAnswer: CExplanation:Blocking e-mail is the same as preventing the receipt of those e-mails and this is done by applying a filter. But the filter must be configured to block it. Thus you should add that specific domain from where the e-mails are being sent to the list of addresses that is to be blocked. QUESTION 202 A security researcher wants to reverse engineer an executable file to determine if it is malicious. The file was found on an underused server and appears to contain a zero-day exploit. Which of the following can the researcher do to determine if the file is malicious in nature? A. TCP/IP socket design reviewB. Executable code reviewC. OS Baseline comparisonD. Software architecture review Answer: CExplanation:Zero-Day Exploits begin exploiting holes in any software the very day it is discovered. It is very difficult to respond to a zero-day exploit. Often, the only thing that you as a security administrator can do is to turn off the service. Although this can be a costly undertaking in terms of productivity, it is the only way to keep the network safe. In this case you want to check if the executable file is malicious. Since a baseline represents a secure state is would be possible to check the nature of the executable file in an isolated environment against the OS baseline. QUESTION 203A security administrator has concerns about new types of media which allow for the mass distribution of personal comments to a select group of people. To mitigate the risks involved with this media, employees should receive training on which of the following? A. Peer to PeerB. Mobile devicesC. Social networkingD. Personally owned devices Answer: CExplanation:There many companies that allow full use of social media in the workplace, believing that the marketing opportunities it holds outweigh any loss in productivity. What they are unknowingly minimizing are the threats that exist. Rather than being all new threats, the social networking/media threats tend to fall in the categories of the same old tricks used elsewhere but in a new format. A tweet can be sent with a shortened URL so that it does not exceed the 140- character limit set by Twitter; unfortunately, the user has no idea what the shortened URL leads to. This makes training your employees regarding the risks social networking entails essential. QUESTION 204The information security team does a presentation on social media and advises the participants not to provide too much personal information on social media web sites. This advice would BEST protect people from which of the following? A. Rainbow tables attacksB. Brute force attacksC. Birthday attacksD. Cognitive passwords attacks Answer: DExplanation:Social Networking Dangers are `amplified' in that social media networks are designed to mass distribute personal messages. If an employee reveals too much personal information it would be easy for miscreants to use the messages containing the personal information to work out possible passwords. QUESTION 205 Pete, the system administrator, has blocked users from accessing social media web sites. In addition to protecting company information from being accidentally leaked, which additional security benefit does this provide? A. No competition with the company's official social presence B. Protection against malware introduced by banner adsC. Increased user productivity based upon fewer distractionsD. Elimination of risks caused by unauthorized P2P file sharing Answer: BExplanation:Banner, or header information messages sent with data to find out about the system(s) does happen. Banners often identify the host, the operating system running on it, and other information that can be useful if you are going to attempt to later breach the security of it. QUESTION 206Which of the following is a security risk regarding the use of public P2P as a method of collaboration? A. Data integrity is susceptible to being compromised.B. Monitoring data changes induces a higher cost.C. Users are not responsible for data usage tracking.D. Limiting the amount of necessary space for data storage. Answer: AExplanation:Peer-to-peer (P2P) networking is commonly used to share files such as movies and music, but you must not allow users to bring in devices and create their own little networks. All networking must be done through administrators and not on a P2P basis. Data integrity can easily be compromised when using public P2P networking. QUESTION 207Which of the following has serious security implications for large organizations and can potentially allow an attacker to capture conversations? A. SubnettingB. NATC. JabberD. DMZ Answer: CExplanation:Jabber is a new unified communications application and could possible expose you to attackers that want to capture conversations because Jabber provides a single interface across presence, instant messaging, voice, video messaging,

desktop sharing and conferencing. QUESTION 208The use of social networking sites introduces the risk of: A. Disclosure of proprietary informationB. Data classification issuesC. Data availability issuesD. Broken chain of custody Answer: A Explanation:People and processes must be in place to prevent the unauthorized disclosure or proprietary information and sensitive information s these pose a security risk to companies. With social networking your company can be exposed to as many threats as the amount of users that make use of social networking and are not advised on security policy regarding the use of social networking. QUESTION 209Which of the following statements is MOST likely to be included in the security awareness training about P2P? A. P2P is always used to download copyrighted material.B. P2P can be used to improve computer system response. C. P2P may prevent viruses from entering the network.D. P2P may cause excessive network bandwidth. Answer: DExplanation: P2P networking by definition involves networking which will reduce available bandwidth for the rest of the users on the network. QUESTION 210A security team has established a security awareness program. Which of the following would BEST prove the success of the program? A. PoliciesB. ProceduresC. MetricsD. Standards Answer: CExplanation:All types of training should be followed up- be tested to see if it worked and how much was learned in the training process. You must follow up and gather training metrics to validate compliance and security posture. By training metrics, we mean some quantifiable method for determining the efficacy of training. QUESTION 211Which of the following is an attack vector that can cause extensive physical damage to a datacenter without physical access? A. CCTV system accessB. Dial-up accessC. Changing environmental controls D. Ping of death Answer: CExplanation:Environmental systems include heating, air conditioning, humidity control, fire suppression, and power systems. All of these functions are critical to a well-designed physical plant. A computer room will typically require full-time environmental control. Changing any of these controls (when it was set to its optimum values) will result in damage. QUESTION 212A company that purchased an HVAC system for the datacenter is MOST concerned with which of the following? A. AvailabilityB. IntegrityC. ConfidentialityD. Fire suppression Answer: AExplanation:Availability means simply to make sure that the data and systems are available for authorized users. Data backups, redundant systems, and disaster recovery plans all support availability; as does environmental support by means of HVAC. QUESTION 213Which of the following should be connected to the fire alarm system in order to help prevent the spread of a fire in a server room without data loss to assist in an FM-200 deployment? A. Water base sprinkler systemB. ElectricalC. HVACD. Video surveillance Answer: C Explanation:HVAC refers to heating, ventilation and air-conditioning to allow for a zone-based environmental control measure. The fire-alarm system should ideally also be hooked up to the HVAC so that the HVAC can monitor the changes in heating and ventilation. QUESTION 214Which of the following is a security benefit of providing additional HVAC capacity or increased tonnage in a datacenter? A. Increased availability of network services due to higher throughputB. Longer MTBF of hardware due to lower operating temperaturesC. Higher data integrity due to more efficient SSD coolingD. Longer UPS run time due to increased airflow Answer: BExplanation:The mean time between failures (MTBF) is the measure of the anticipated incidence of failure for a system or component. This measurement determines the component's anticipated lifetime. If the MTBF of a cooling system is one year, you can anticipate that the system will last for a one-year period; this means that you should be prepared to replace or rebuild the system once a year. If the system lasts longer than the MTBF, your organization receives a bonus. MTBF is helpful in evaluating a system's reliability and life expectancy. Thus longer MTBF due to lower operating temperatures is a definite advantage QUESTION 215Which of the following fire suppression systems is MOST likely used in a datacenter? A. FM-200B. Dry-pipeC. Wet-pipeD. Vacuum Answer: AExplanation:FM200 is a gas and the principle of a gas system is that it displaces the oxygen in the room, thereby removing this essential component of a fi re. in a data center is is the preferred choice of fire suppressant. QUESTION 216When implementing fire suppression controls in a datacenter it is important to: A. Select a fire suppression system which protects equipment but may harm technicians.B. Ensure proper placement of sprinkler lines to avoid accidental leakage onto servers.C. Integrate maintenance procedures to include regularly discharging the system.D. Use a system with audible alarms to ensure technicians have 20 minutes to evacuate. Answer: BExplanation:Water-based systems can cause serious damage to all electrical equipment and the sprinkler lines in a fire suppression control system should be placed in such a way so as not to leak onto computers when it do get activated because it works with overhead nozzles. QUESTION 217Which of the following should be considered to mitigate data theft when using CAT5 wiring? A. CCTVB. Environmental monitoringC. Multimode fiberD. EMI shielding Answer: DExplanation:EMI Shielding refers to the process of preventing electronic emissions from your computer systems from being used to gather intelligence and preventing outside electronic emissions from disrupting your information-processing abilities. Thus all wiring should be shielded to mitigate data theft. QUESTION 218Environmental control measures include which of the following? A. Access listB. LightingC. Motion detectionD. EMI shielding Answer: D Explanation:Environmental controls include HVAC, Fire Suppression, EMI Shielding, Hot and Cold Aisles, Environmental monitoring as well as Temperature and Humidity controls. QUESTION 219When a new network drop was installed, the cable was

run across several fluorescent lights. The users of the new network drop experience intermittent connectivity. Which of the following environmental controls was MOST likely overlooked during installation? A. Humidity sensorsB. EMI shieldingC. Channel interferenceD. Cable kinking Answer: BExplanation:Shielding refers to the process of preventing electronic emissions from your computer systems from being used to gather intelligence and preventing outside electronic emissions from disrupting your information-processing abilities. In this case you are experiencing intermittent connectivity since Electro Magnetic Interference (EMI) was not taken into account when running the cables over fluorescent lighting. QUESTION 220The datacenter design team is implementing a system, which requires all servers installed in racks to face in a predetermined direction. AN infrared camera will be used to verify that servers are properly racked. Which of the following datacenter elements is being designed? A. Hot and cold aislesB. Humidity controlC. HVAC systemD. EMI shielding Answer: AExplanation:There are often multiple rows of servers located in racks in server rooms. The rows of servers are known as aisles, and they can be cooled as hot aisles and cold aisles. With a hot aisle, hot air outlets are used to cool the equipment, whereas with cold aisles, cold air intake is used to cool the equipment. Combining the two, you have cold air intake from below the aisle and hot air outtake above it, providing constant circulation. Infrared cameras are heat detection measures thus it is hot and cold aisle design elements. QUESTION 221A company is installing a new security measure that would allow one person at a time to be authenticated to an area without human interaction. Which of the following does this describe? A. FencingB. MantrapC. A guardD. Video surveillance Answer: BExplanation:Mantraps make use of electronic locks and are designed to allow you to limit the amount of individual allowed access to an area at any one time. QUESTION 222Key cards at a bank are not tied to individuals, but rather to organizational roles. After a break in, it becomes apparent that extra efforts must be taken to successfully pinpoint who exactly enters secure areas. Which of the following security measures can be put in place to mitigate the issue until a new key card system can be installed? A. BollardsB. Video surveillance C. Proximity readersD. Fencing Answer: BExplanation:Video surveillance is making use of a camera, or CCTV that is able to record everything it sees and is always running. This way you will be able to check exactly who enters secure areas. QUESTION 223A datacenter requires that staff be able to identify whether or not items have been removed from the facility. Which of the following controls will allow the organization to provide automated notification of item removal? A. CCTVB. Environmental monitoringC. RFIDD. EMI shielding Answer: CExplanation:RFID is radio frequency identification that works with readers that work with 13.56 MHz smart cards and 125 kHz proximity cards and can open turnstiles, gates, and any other physical security safeguards once the signal is read. Fitting out the equipment with RFID will allow you to provide automated notification of item removal in the event of any of the equipped items is taken off the premises. QUESTION 224Datacenter access is controlled with proximity badges that record all entries and exits from the datacenter. The access records are used to identify which staff members accessed the data center in the event of equipment theft. Which of the following MUST be prevented in order for this policy to be effective? A. Password reuseB. PhishingC. Social engineeringD. Tailgating Answer: DExplanation:Tailgating is the term used for someone being so close to you when you enter a building that they are able to come in right behind you without needing to use a key, a card, or any other security device. This should be prevented in this case. QUESTION 225Due to issues with building keys being duplicated and distributed, a security administrator wishes to change to a different security control regarding a restricted area. The goal is to provide access based upon facial recognition. Which of the following will address this requirement? A. Set up mantraps to avoid tailgating of approved users.B. Place a guard at the entrance to approve access.C. Install a fingerprint scanner at the entrance.D. Implement proximity readers to scan users' badges. Answer: BExplanation:A guard can be instructed to deny access until authentication has occurred will address the situation adequately. All CompTIA SY0-401 exam questions are the new checked and updated! In recent years, the SY0-401 certification has become a global standard for many successful IT companies. Want to become a certified CompTIA professional? Download Lead2pass 2017 latest released SY0-401 exam dumps full version and pass SY0-401 100%! SY0-401 new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDVzFZWExUbFM0YU0 2017 CompTIA **SY0-401** exam dumps (All 1868 Q&As) from Lead2pass: https://www.lead2pass.com/sy0-401.html [100% Exam Pass Guaranteed]