[2017 New Exam Collection SY0-401 Dumps And SY0-401 New Questions (176-200)

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

The CompTIA SY0-401 exam is a very hard exam to successfully pass. Here you will find free Lead2pass CompTIA practice sample exam test questions that will help you prepare in passing the SY0-401 exam. Lead2pass Guarantees you 100% pass exam SY0-401. Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 176After a number of highly publicized and embarrassing customer data leaks as a result of social engineering attacks by phone, the Chief Information Officer (CIO) has decided user training will reduce the risk of another data leak. Which of the following would be MOST effective in reducing data leaks in this situation? A. Information Security AwarenessB. Social Media and BYODC. Data Handling and DisposalD. Acceptable Use of IT SystemsAnswer: AExplanation:Education and training with regard to Information Security Awareness will reduce the risk of data leaks and as such forms an integral part of Security Awareness. By employing social engineering data can be leaked by employees and only when company users are made aware of the methods of social engineering via Information Security Awareness Training, you can reduce the risk of data leaks. QUESTION 177Sara, a company's security officer, often receives reports of unauthorized personnel having access codes to the cipher locks of secure areas in the building. Sara should immediately implement which of the following? A. Acceptable Use PolicyB. Physical security controlsC. Technical controlsD. Security awareness training Answer: DExplanation:Security awareness and training include explaining policies, procedures, and current threats to both users and management. A security awareness and training program can do much to assist in your efforts to improve and maintain security. A good security awareness training program for the entire organization should cover the following areas: Importance of security; Responsibilities of people in the organization; Policies and procedures; Usage policies; Account and password- selection criteria as well as Social engineering prevention. QUESTION 178Human Resources (HR) would like executives to undergo only two specific security training programs a year. Which of the following provides the BEST level of security training for the executives? (Select TWO). A. Acceptable use of social mediaB. Data handling and disposalC. Zero day exploits and virusesD. Phishing threats and attacksE. Clean desk and BYODF. Information security awareness Answer: DFExplanation:Managers/ i.e. executives in the company are concerned with more global issues in the organization, including enforcing security policies and procedures. Managers should receive additional training or exposure that explains the issues, threats, and methods of dealing with threats. Management will also be concerned about productivity impacts and enforcement and how the various departments are affected by security policies. Phishing is a form of social engineering in which you ask someone for a piece of information that you are missing by making it look as if it is a legitimate request. An email might look as if it is from a bank and contain some basic information, such as the user's name. Executives an easily fall prey to phishing if they are not trained to lookout for these attacks. QUESTION 179The method to provide end users of IT systems and applications with requirements related to acceptable use, privacy, new threats and trends, and use of social networking is: A. Security awareness training.B. BYOD security training.C. Role-based security training.D. Legal compliance training. Answer: AExplanation:Security awareness and training are critical to the success of a security effort. They include explaining policies, procedures, and current threats to both users and management. QUESTION 180 Sara, an employee, tethers her smartphone to her work PC to bypass the corporate web security gateway while connected to the LAN. While Sara is out at lunch her PC is compromised via the tethered connection and corporate data is stolen. Which of the following would BEST prevent this from occurring again? A. Disable the wireless access and implement strict router ACLs.B. Reduce restrictions on the corporate web security gateway.C. Security policy and threat awareness training.D. Perform user rights and permissions reviews. Answer: CExplanation:BYOD (In this case Sara's smart phone) involves the possibility of a personal device that is infected with malware introducing that malware to the network and security awareness training will address the issue of the company's security policy with regard to BYOD. QUESTION 181Which of the following is the BEST reason to provide user awareness and training programs for organizational staff? A. To ensure proper use of social mediaB. To reduce organizational IT riskC. To detail business impact analysesD. To train staff on zero-days Answer: BExplanation:Ideally, a security awareness training program for the entire organization should cover the following areas:Importance of securityResponsibilities of people in the organizationPolicies and proceduresUsage policiesAccount and password-selection criteriaSocial engineering preventionYou can accomplish this training either by using internal staff or by hiring outside trainers. This type of training will significantly reduce the organizational IT risk. QUESTION 182Ann would like to forward some Personal Identifiable Information to her HR department by email, but she is worried about the confidentiality of the information. Which of the following will accomplish this task securely? A. Digital SignaturesB. HashingC. Secret KeyD. Encryption Answer: DExplanation:Encryption is used to prevent unauthorized

users from accessing data. Data encryption will support the confidentiality of the email. QUESTION 183Ann a technician received a spear-phishing email asking her to update her personal information by clicking the link within the body of the email. Which of the following type of training would prevent Ann and other employees from becoming victims to such attacks? A. User AwarenessB. Acceptable Use PolicyC. Personal Identifiable InformationD. Information Sharing Answer: CExplanation:Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person's name to a fingerprint (think biometrics), credit card number, or patient record. Employees should be made aware of this type of attack by means of training. QUESTION 184End-user awareness training for handling sensitive personally identifiable information would include secure storage and transmission of customer: A. Date of birth.B. First and last name.C. Phone number.D. Employer name. Answer: AExplanation:Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person's name to a fingerprint (think biometrics), credit card number, or patient record. Date of birth is personally identifiable information. QUESTION 185Which of the following concepts is a term that directly relates to customer privacy considerations? A. Data handling policiesB. Personally identifiable informationC. Information classificationD. Clean desk policies Answer: BExplanation:Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person's name to a fingerprint (think biometrics), credit card number, or patient record. This has a direct relation to customer privacy considerations. QUESTION 186Which of the following policies is implemented in order to minimize data loss or theft? A. PII handlingB. Password policyC. Chain of custodyD. Zero day exploits Answer: AExplanation:Although the concept of PII is old, it has become much more important as information technology and the Internet have made it easier to collect PII through breaches of internet security, network security and web browser security, leading to a profitable market in collecting and reselling PII. PII can also be exploited by criminals to stalk or steal the identity of a person, or to aid in the planning of criminal acts.Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person's name to a fingerprint (think biometrics), credit card number, or patient record.Thus a PII handling policy can be used to protect data. QUESTION 187Used in conjunction, which of the following are PII? (Select TWO). A. Marital statusB. Favorite movieC. Pet's nameD. BirthdayE. Full name Answer: DEExplanation:Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person's name to a fingerprint (think biometrics), credit card number, or patient record. A birthday together with a full name makes it personally identifiable information. QUESTION 188Which of the following helps to apply the proper security controls to information? A. Data classificationB. DeduplicationC. Clean desk policyD. Encryption Answer: AExplanation:Information classification is done by confidentiality and comprises of three categories, namely:public use, internal use and restricted use. These categories make applying the appropriate policies and security controls practical. QUESTION 189Which of the following security awareness training is BEST suited for data owners who are concerned with protecting the confidentiality of their data? A. Social networking use trainingB. Personally owned device policy trainingC. Tailgating awareness policy trainingD. Information classification training Answer: DExplanation:Information classification is done by confidentiality and comprises of three categories, namely:public use, internal use and restricted use. Knowing these categories and how to handle data according to its category is essential in protecting the confidentiality of the data. QUESTION 190An organization is recovering data following a datacenter outage and determines that backup copies of files containing personal information were stored in an unsecure location, because the sensitivity was unknown. Which of the following activities should occur to prevent this in the future? A. Business continuity planningB. Quantitative assessmentC. Data classificationD. Qualitative assessment Answer: CExplanation:Information classification is done by confidentiality and comprises of three categories, namely:public use, internal use and restricted use. Knowing how to apply these categories and matching it up with the appropriate data handling will address the situation of the data `unknown sensitivity' QUESTION 191What is the term for the process of luring someone in (usually done by an enforcement officer or a government agent)? A. EnticementB. EntrapmentC. DeceitD. Sting Answer: AExplanation:Enticement is the process of luring someone into your plan or trap. QUESTION 192In which of the following categories would creating a corporate privacy policy, drafting acceptable use policies, and group based access control be classified? A. Security control frameworksB. Best practiceC. Access control methodologiesD. Compliance activity Answer: BExplanation:Best practices are based on what is known in the industry and those methods that have consistently shown superior results over those achieved by other means. Furthermore best practices are applied to all aspects in the work environment. QUESTION 193Which of the following is the process in which a law enforcement officer or a government agent encourages or induces a person to commit a crime when the potential criminal expresses a desire not to go ahead? A. EnticementB. EntrapmentC. DeceitD. Sting Answer: BExplanation:Entrapment is the process in which a law enforcement officer or a government agent encourages or induces a person to commit a crime when the potential

criminal expresses a desire not to go ahead. Entrapment is a valid legal defense in a criminal prosecution. QUESTION 194Results from a vulnerability analysis indicate that all enabled virtual terminals on a router can be accessed using the same password. The company's network device security policy mandates that at least one virtual terminal have a different password than the other virtual terminals. Which of the following sets of commands would meet this requirement? A. line vty 0 6 P@s5W0Rd password line vty 7 Qwer++!Y passwordB. line console 0 password password line vty 0 4 password P@s5W0RdC. line vty 0 3 password Qwer++!Y line vty 4 password P@s5W0RdD. line vty 0 3 password Qwer++!Y line console 0 password P@s5W0Rd Answer: CExplanation: The VTY lines are the Virtual Terminal lines of the router, used solely to control inbound Telnet connections. They are virtual, in the sense that they are a function of software - there is no hardware associated with them.Two numbers follow the keyword VTY because there is more than one VTY line for router access. The default number of lines is five on many Cisco routers. Here, I'm configuring one password for all terminal (VTY) lines. I can specify the actual terminal or VTY line numbers as a range. The syntax that you'll see most often, vty 0 4, covers all five terminal access lines. QUESTION 195Why would a technician use a password cracker? A. To look for weak passwords on the networkB. To change a user's passwords when they leave the companyC. To enforce password complexity requirementsD. To change users passwords if they have forgotten them Answer: AExplanation:A password cracker will be able to expose weak passwords on a network. QUESTION 196Which of the following security concepts would Sara, the security administrator, use to mitigate the risk of data loss? A. Record time offsetB. Clean desk policyC. Cloud computingD. Routine log review Answer: BExplanation:Clean Desk Policy Information on a desk--in terms of printouts, pads of note paper, sticky notes, and the like--can be easily seen by prying eyes and taken by thieving hands. To protect data and your business, encourage employees to maintain clean desks and to leave out only those papers that are relevant to the project they are working on at that moment. All sensitive information should be put away when the employee is away from their desk. This will mitigate the risk of data loss when applied. QUESTION 197The manager has a need to secure physical documents every night, since the company began enforcing the clean desk policy. The BEST solution would include: (Select TWO). A. Fire- or water-proof safe.B. Department door locks.C. Proximity card.D. 24-hour security guard.E. Locking cabinets and drawers. Answer: AE Explanation:Using a safe and locking cabinets to protect backup media, documentation, and any other physical artifacts that could do harm if they fell into the wrong hands would form part of keeping employees desks clean as in a clean desk policy. QUESTION 198XYZ Corporation is about to purchase another company to expand its operations. The CEO is concerned about information leaking out, especially with the cleaning crew that comes in at night.The CEO would like to ensure no paper files are leaked. Which of the following is the BEST policy to implement? A. Social media policyB. Data retention policyC. CCTV policyD. Clean desk policy Answer: DExplanation:Clean Desk Policy Information on a desk--in terms of printouts, pads of note paper, sticky notes, and the like--can be easily seen by prying eyes and taken by thieving hands. To protect data and your business, encourage employees to maintain clean desks and to leave out only those papers that are relevant to the project they are working on at that moment. All sensitive information should be put away when the employee is away from their desk. QUESTION 199Which of the following could a security administrator implement to mitigate the risk of tailgating for a large organization? A. Train employees on correct data disposal techniques and enforce policies.B. Only allow employees to enter or leave through one door at specified times of the day. C. Only allow employees to go on break one at a time and post security guards 24/7 at each entrance.D. Train employees on risks associated with social engineering attacks and enforce policies. 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. Many social engineering intruders needing physical access to a site will use this method of gaining entry. Educate users to beware of this and other social engineering ploys and prevent them from happening. QUESTION 200Which of the following is a security concern regarding users bringing personally-owned devices that they connect to the corporate network? A. Cross-platform compatibility issues between personal devices and server-based applicationsB. Lack of controls in place to ensure that the devices have the latest system patches and signature filesC. Non-corporate devices are more difficult to locate when a user is terminatedD. Non-purchased or leased equipment may cause failure during the audits of company-owned assets Answer: BExplanation:With employees who want to bring their own devices you will have to make them understand why they cannot. You do not want them plugging in a flash drive, let alone a camera, smartphone, tablet computer, or other device, on which company fi les could get intermingled with personal files. Allowing this to happen can create situations where data can leave the building that shouldn't as well as introduce malware to the system. Employees should not sync unauthorized smartphones to their work systems. Some smartphones use multiple wireless spectrums and unwittingly open up the possibility for an attacker in the parking lot to gain access through the phone to the internal network. Thus if you do not have controls in place then your network is definitely at risk. Lead2pass new released premium SY0-401 exam dumps guarantee you a 100% exam success or we promise full money back! Download CompTIA SY0-401 exam dumps full version from Lead2pass instantly! 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]