[Lead2pass New Lead2pass SY0-401 Exam Dumps New Updated By CompTIA Official Exam Center (501-525)

Lead2pass 2017 October New CompTIA SY0-401 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! In recent years, many people choose to take CompTIA SY0-401 certification exam which can make you get the CompTIA certificate and that is the passport to get a better job and get promotions. How to prepare for CompTIA SY0-401 exam and get the certificate? Please refer to CompTIA SY0-401 exam questions and answers on Lead2pass. Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 501Which of the following is a common coding error in which boundary checking is not performed? A. Input validationB. FuzzingC. Secure codingD. Cross-site scriptingAnswer: AExplanation:Input validation is a defensive technique intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain. QUESTION 502One of the most consistently reported software security vulnerabilities that leads to major exploitsis: A. Lack of malware detection.B. Attack surface decrease.C. Inadequate network hardening.D. Poor input validation. Answer: DExplanation:D: With coding there are standards that should be observed. Of these standards the most fundamental is input validation. Attacks such as SQL injection depend on unfiltered input being sent through a web application. This makes for a software vulnerability that can be exploited. There are two primary ways to do input validation: client-side validation and server-side validation. Thus with poor input validation you increase your risk with regard to exposure to major software exploits. QUESTION 503Without validating user input, an application becomes vulnerable to all of the following EXCEPT: A. Buffer overflow.B. Command injection.C. Spear phishing.D. SQL injection. Answer: CExplanation:Input validation is a defensive technique intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain. QUESTION 504Which of the following can BEST help prevent cross-site scripting attacks and buffer overflows on a production system? A. Input validationB. Network intrusion detection systemC. Anomaly-based HIDSD. Peer review Answer: AExplanation:Input validation is a defensive technique intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain. QUESTION 505The BEST methods for a web developer to prevent the website application code from being vulnerable to cross-site request forgery (XSRF) are to: (Select TWO). A. Permit redirection to Internet-facing web URLs.B. Ensure all HTML tags are enclosed in angle brackets, e.g., "<" and ">".C. Validate and filter input on the server side and client side.D. Use a web proxy to pass website requests between the user and the application.E. Restrict and sanitize use of special characters in input and URLs. Answer: CEExplanation:XSRF or cross-site request forgery applies to web applications and is an attack that exploits the web application's trust of a user who known or is supposed to have been authenticated. This is often accomplished without the user's knowledge.XSRF can be prevented by adding a randomization string (called a nonce) to each URL request and session establishment and checking the client HTTP request header referrer for spoofing. QUESTION 506After visiting a website, a user receives an email thanking them for a purchase which they did not request. Upon investigation the security administrator sees the following source code in a pop-up window: <HTML><body onload="document.getElementByID(`badForm').submit()"><form id="badForm" action="shoppingsite.company.com/purchase.php" method="post" ><input name="Perform Purchase" value="Perform Purchase"/></form></body></HTML> Which of the following has MOST likely occurred? A. SQL injectionB. Cookie stealingC. XSRFD. XSS Answer: CExplanation:XSRF or cross-site request forgery applies to web applications and is an attack that exploits the web application's trust of a user who known or is supposed to have been authenticated. This is often accomplished without the user's knowledge. QUESTION 507Which of the following is the BEST way to prevent Cross-Site Request Forgery (XSRF) attacks? A. Check the referrer field in the HTTP headerB. Disable Flash contentC. Use only cookies for authenticationD. Use only HTTPS URLs Answer: AExplanation:XSRF or cross-site request forgery applies to web applications and is an attack that exploits the web application's trust of a user who known or is supposed to have been authenticated. This is accomplished by changing values in the HTTP header and even in the user's cookie to falsify access. It can be prevented by embedding additional authentication data into requests that allows the web application to detect requests from unauthorized locations. Examples are synchronizer token patterns, cookie-to-header tokens, and checking the HTTP Referrer header and the HTTP Origin header. QUESTION 508The process of making certain that an entity (operating system, application, etc.) is as secure as it can be is known as: A. StabilizingB. ReinforcingC. HardeningD. Toughening Answer: CExplanation:Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes

removing unnecessary functions and features, removing unnecessary usernames or logins and disabling unnecessary services. QUESTION 509Vendors typically ship software applications with security settings disabled by default to ensure a wide range of interoperability with other applications and devices. A security administrator should perform which of the following before deploying new software? A. Application white listingB. Network penetration testingC. Application hardeningD. Input fuzzing testing Answer: CExplanation:Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing unnecessary functions and features, removing unnecessary usernames or logins and disabling unnecessary services. QUESTION 510Which of the following describes the process of removing unnecessary accounts and services from an application to reduce risk exposure? A. Error and exception handlingB. Application hardeningC. Application patch managementD. Cross-site script prevention Answer: BExplanation:Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing unnecessary functions and features, removing unnecessary usernames or logins and disabling unnecessary services. QUESTION 511A network administrator is responsible for securing applications against external attacks. Every month, the underlying operating system is updated. There is no process in place for other software updates.Which of the following processes could MOST effectively mitigate these risks? A. Application hardeningB. Application change managementC. Application patch managementD. Application firewall review Answer: CExplanation:The question states that operating system updates are applied but not other software updates. The `other software' in this case would be applications. Software updates includes functionality updates and more importantly security updates. The process of applying software updates or `patches' to applications is known as `application patch management'. Application patch management is an effective way of mitigating security risks associated with software applications. QUESTION 512A recently installed application update caused a vital application to crash during the middle of the workday. The application remained down until a previous version could be reinstalled on the server, and this resulted in a significant loss of data and revenue. Which of the following could BEST prevent this issue from occurring again? A. Application configuration baselinesB. Application hardeningC. Application access controlsD. Application patch management Answer: DExplanation:Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a systems from newly discovered attacks and vulnerabilities. A part of patch management is testing the effects of vendor updates on a test system first to ensure that the updates do not have detrimental effects on the system, and, should the updates have no detrimental effects on the test systems, backing up the production systems before applying the updates on a production system. QUESTION 513An administrator finds that non-production servers are being frequently compromised, production servers are rebooting at unplanned times and kernel versions are several releases behind the version with all current security fixes.Which of the following should the administrator implement? A. SnapshotsB. SandboxingC. Patch managementD. Intrusion detection system Answer: CExplanation:Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a systems from newly discovered attacks and vulnerabilities. QUESTION 514Which of the following is the term for a fix for a known software problem? A. SkiffB. PatchC. SlipstreamD. Upgrade Answer: BExplanation:Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a systems from newly discovered attacks and vulnerabilities. QUESTION 515Which of the following practices is used to mitigate a known security vulnerability? A. Application fuzzingB. Patch managementC. Password crackingD. Auditing security logs Answer: BExplanation:Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a systems from new attacks and vulnerabilities that have recently become known. QUESTION 516Which of the following can a security administrator implement on mobile devices that will help prevent unwanted people from viewing the data if the device is left unattended? A. Screen lockB. Voice encryptionC. GPS trackingD. Device encryption Answer: AExplanation:Screen-lock is a security feature that requires the user to enter a PIN or a password after a short period of inactivity before they can access the system again. This feature ensures that if your device is left unattended or is lost or stolen, it will be difficult for anyone else to access your data or applications. QUESTION 517Which of the following can be used on a smartphone to BEST protect against sensitive data loss if the device is stolen? (Select TWO). A. TetheringB. Screen lock PINC. Remote wipeD. Email passwordE. GPS trackingF. Device encryption Answer: CFExplanation:C: Remote wipe is the process of deleting data on a device in the event that the device is stolen. This is performed over remote connections such as the mobile phone service or the internet connection and helps ensure that sensitive data is not accessed by unauthorized people.F: 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 518Which of the following controls can be implemented together to prevent data loss in the event of theft of a mobile device storing sensitive information? (Select TWO). A. Full device encryptionB. Screen locksC.

GPSD. Asset trackingE. Inventory control Answer: ABExplanation:A: 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.B: Screen locks are a security feature that requires the user to enter a PIN or a password after a short period of inactivity before they can access the system again. This feature ensures that if your device is left unattended or is lost or stolen, it will be difficult for anyone else to access your data or applications. QUESTION 519A way to assure data at-rest is secure even in the event of loss or theft is to use: A. Full device encryption.B. Special permissions on the file system.C. Trusted Platform Module integration.D. Access Control Lists. Answer: AExplanation: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 520Which of the following should Matt, a security administrator, include when encrypting smartphones? (Select TWO). A. Steganography imagesB. Internal memoryC. Master boot recordsD. Removable memory cardsE. Public keys Answer: BDExplanation:All useable data on the device should be encrypted. This data can be located on the hard drive, or removable drives, such as USB devices and memory cards, and on internal memory. QUESTION 521A bank has recently deployed mobile tablets to all loan officers for use at customer sites. Which of the following would BEST prevent the disclosure of customer data in the event that a tablet is lost or stolen? A. Application controlB. Remote wipingC. GPSD. Screen-locks Answer: BExplanation:Remote wipe is the process of deleting data on a device in the event that the device is stolen. This is performed over remote connections such as the mobile phone service or the internet connection and helps ensure that sensitive data is not accessed by unauthorized people. QUESTION 522A small company has recently purchased cell phones for managers to use while working outside if the office.The company does not currently have a budget for mobile device management and is primarily concerned with deterring leaks if sensitive information obtained by unauthorized access to unattended phones. Which of the following would provide the solution BEST meets the company's requirements? A. Screen-lockB. Disable removable storageC. Full device encryptionD. Remote wiping Answer: AExplanation:Screen-lock is a security feature that requires the user to enter a password after a short period of inactivity before they can access the system again. This feature ensures that if your device is left unattended or is lost or stolen, it will be difficult for anyone else to access your data or applications. QUESTION 523Pete, the system administrator, has concerns regarding users losing their company provided smartphones. Pete's focus is on equipment recovery. Which of the following BEST addresses his concerns? A. Enforce device passwords.B. Use remote sanitation.C. Enable GPS tracking.D. Encrypt stored data. Answer: CExplanation:Global Positioning System (GPS) tracking can be used to identify its location of a stolen device and can allow authorities to recover the device. However, for GPS tracking to work, the device must have an Internet connection or a wireless phone service over which to send its location information. QUESTION 524After a security incident involving a physical asset, which of the following should be done at the beginning? A. Record every person who was in possession of assets, continuing post-incident.B. Create working images of data in the following order: hard drive then RAM.C. Back up storage devices so work can be performed on the devices immediately.D. Write a report detailing the incident and mitigation suggestions. Answer: AExplanation:Asset tracking is the process of maintaining oversight over inventory, and ensuring that a device is still in the possession of the assigned authorized user. QUESTION 525The chief Risk officer is concerned about the new employee BYOD device policy and has requested the security department implement mobile security controls to protect corporate data in the event that a device is lost or stolen. The level of protection must not be compromised even if the communication SIM is removed from the device. Which of the following BEST meets the requirements? (Select TWO) A. Asset trackingB. Screen-locksC. GEO-TrackingD. Device encryption Answer: ADExplanation:A: Asset tracking is the process of maintaining oversight over inventory, and ensuring that a device is still in the possession of the assigned authorized user.D: 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.