[Lead2pass New Lead2pass 2017 New SY0-401 Exam PDF Ensure SY0-401 Certification Exam Pass Successfully (526-550)

Lead2pass 2017 October New CompTIA SY0-401 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! Lead2pass is constantly updating SY0-401 exam dumps. We will provide our customers with the latest and the most accurate exam questions and answers that cover a comprehensive knowledge point, which will help you easily prepare for SY0-401 exam and successfully pass your exam. You just need to spend 20-30 hours on studying the exam dumps. Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 526Which of the following technical controls helps to prevent Smartphones from connecting to a corporate network? A. Application white listingB. Remote wipingC. Acceptable use policyD. Mobile device managementAnswer: DExplanation:Mobile device management (MDM) is allows for managing the mobile devices that employees use to access company resources. MDM is intended to improve security, provide monitoring, enable remote management, and support troubleshooting. It can be used to push or remove applications, manage data, and enforce configuration settings on these devices. QUESTION 527A network administrator noticed various chain messages have been received by the company.Which of the following security controls would need to be implemented to mitigate this issue? A. Anti-spamB. AntivirusC. Host-based firewallsD. Anti-spyware Answer: AExplanation: A spam filter is a software or hardware solution used to identify and block, filter, or remove unwanted messages sent via email or instant messaging (IM). QUESTION 528Which of the following will allow Pete, a security analyst, to trigger a security alert because of a tracking cookie? A. Network based firewallB. Anti-spam softwareC. Host based firewallD. Anti-spyware software Answer: DExplanation: Spyware monitors a user's activity and uses network protocols to reports it to a third party without the user's knowledge. This is usually accomplished using a tracking cookie. QUESTION 529A security administrator wants to deploy security controls to mitigate the threat of company employees' personal information being captured online. Which of the following would BEST serve this purpose? A. Anti-spywareB. AntivirusC. Host-based firewallD. Web content filter Answer: AExplanation:Spyware monitors a user's activity and uses network protocols to reports it to a third party without the user's knowledge. This is usually accomplished using a tracking cookie. QUESTION 530A user has several random browser windows opening on their computer. Which of the following programs can be installed on his machine to help prevent this from happening? A. AntivirusB. Pop-up blockerC. Spyware blockerD. Anti-spam Answer: BExplanation:Pop-up blockers prevent websites from opening new browser windows without the users consent. These are often used for advertisements but can also be used to distribute malicious code. QUESTION 531Which of the following is a vulnerability associated with disabling pop-up blockers? A. An alert message from the administrator may not be visibleB. A form submitted by the user may not openC. The help window may not be displayedD. Another browser instance may execute malicious code Answer: DExplanation: Pop-up blockers prevent websites from opening new browser windows without the users consent. These are often used for advertisements but can also be used to distribute malicious code. QUESTION 532Which of the following encompasses application patch management? A. Configuration managementB. Policy managementC. Cross-site request forgeryD. Fuzzing Answer: AExplanation: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 its configuration, 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 533A periodic update that corrects problems in one version of a product is called a A. HotfixB. OverhaulC. Service packD. Security update Answer: CExplanation:A service pack is a collection of updates and hotfixes that address a number of software issues, as well as new software features. It is released periodically by the vendor. QUESTION 534A technician has implemented a system in which all workstations on the network will receive security updates on the same schedule. Which of the following concepts does this illustrate? A. Patch managementB. Application hardeningC. White box testingD. Black box testing Answer: AExplanation: 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 before applying the updates on a production system, and scheduling updates. QUESTION 535Pete, the compliance manager, wants to meet regulations. Pete would like certain ports blocked only on all computers that do credit card transactions. Which of the following should Pete implement to BEST achieve this goal? A. A host-based intrusion prevention systemB. A host-based firewallC. Antivirus update systemD. A network-based intrusion detection system Answer: BExplanation:A host-based firewall is installed on a client system and is used to protect the client system from the activities of the user as well as from communication from the network or Internet. QUESTION

536Each server on a subnet is configured to only allow SSH access from the administrator's workstation. Which of the following BEST describes this implementation? A. Host-based firewallsB. Network firewallsC. Network proxyD. Host intrusion prevention Answer: AExplanation:A host-based firewall is installed on a client system and is used to protect the client system from the activities of the user as well as from communication from the network or Internet. These firewalls manage network traffic using filters to block certain ports and protocols while allowing others to pass through the system. QUESTION 537Which of the following is an important step in the initial stages of deploying a host-based firewall? A. Selecting identification versus authenticationB. Determining the list of exceptionsC. Choosing an encryption algorithmD. Setting time of day restrictions Answer: BExplanation: A host-based firewall is installed on a client system and is used to protect the client system from the activities of the user as well as from communication from the network or Internet. These firewalls manage network traffic using filters to block certain ports and protocols while allowing others to pass through the system. QUESTION 538Which of the following MOST interferes with network-based detection techniques? A. Mime-encodingB. SSLC. FTPD. Anonymous email accounts Answer: B Explanation:Secure Sockets Layer (SSL) is used to establish secure TCP communication between two machines by encrypting the communication. Encrypted communications cannot easily be inspected for anomalies by network-based intrusion detection systems (NIDS). QUESTION 539Joe, a network security engineer, has visibility to network traffic through network monitoring tools. However, he's concerned that a disgruntled employee may be targeting a server containing the company's financial records. Which of the following security mechanism would be MOST appropriate to confirm Joe's suspicion? A. HIDSB. HIPSC. NIPSD. NIDS Answer: AExplanation:A host-based IDS (HIDS) is an intrusion detection system that runs as a service on a host computer system. It is used to monitor the machine logs, system events, and application activity for signs of intrusion. It is useful for detecting attacks that originate outside the organization as well as attacks by internal users logged on to the system. QUESTION 540Which of the following devices will help prevent a laptop from being removed from a certain location? A. Device encryptionB. Cable locksC. GPS trackingD. Remote data wipes Answer: BExplanation:Cable locks are theft deterrent devices that can be used to tether a device to a fixed point keep smaller devices from being easy to steal. QUESTION 541Which of the following can be used as an equipment theft deterrent? A. Screen locksB. GPS trackingC. Cable locksD. Whole disk encryption Answer: C Explanation:Cable locks are theft deterrent devices that can be used to tether a device to a fixed point keep smaller devices from being easy to steal. QUESTION 542The librarian wants to secure the public Internet kiosk PCs at the back of the library. Which of the following would be the MOST appropriate? (Select TWO). A. Device encryptionB. AntivirusC. Privacy screenD. Cable locksE. Remote wipe Answer: BDExplanation:B: Antivirus software is used to protect systems against viruses, which are a form of malicious code designed to spread from one system to another, consuming network resources. Public systems are particularly prone to viruses.D: Cable locks are theft deterrent devices that can be used to tether a device to a fixed point keep devices from being easy to steal. QUESTION 543A computer is suspected of being compromised by malware. The security analyst examines the computer and finds that a service called Telnet is running and connecting to an external website over port 443. This Telnet service was found by comparing the system's services to the list of standard services on the company's system image. This review process depends on: A. MAC filtering.B. System hardening.C. Rogue machine detection.D. Baselining. Answer: DExplanation: Application baseline defines the level or standard of security that will be implemented and maintained for the application. It may include requirements of hardware components, operating system versions, patch levels, installed applications and their configurations, and available ports and services. Systems can be compared to the baseline to ensure that the required level of security is being maintained. QUESTION 544Identifying a list of all approved software on a system is a step in which of the following practices? A. Passively testing security controlsB. Application hardeningC. Host software baseliningD. Client-side targeting Answer: CExplanation:Application baseline defines the level or standard of security that will be implemented and maintained for the application. It may include requirements of hardware components, operating system versions, patch levels, installed applications and their configurations, and available ports and services. Systems can be compared to the baseline to ensure that the required level of security is being maintained. QUESTION 545A new application needs to be deployed on a virtual server. The virtual server hosts a SQL server that is used by several employees.Which of the following is the BEST approach for implementation of the new application on the virtual server? A. Take a snapshot of the virtual server after installing the new application and store the snapshot in a secure location.B. Generate a baseline report detailing all installed applications on the virtualized server after installing the new application.C. Take a snapshot of the virtual server before installing the new application and store the snapshot in a secure location.D. Create an exact copy of the virtual server and store the copy on an external hard drive after installing the new application. Answer: CExplanation:Snapshots are backups of virtual machines that can be used to quickly recover from poor updates, and errors arising from newly installed applications. However, the snapshot should be taken before the application or update is installed. QUESTION 546The information security technician wants to ensure security controls are deployed and

functioning as intended to be able to maintain an appropriate security posture. Which of the following security techniques is MOST appropriate to do this? A. Log auditsB. System hardeningC. Use IPS/IDSD. Continuous security monitoring Answer: D Explanation:A security baseline is the security setting of a system that is known to be secure. This is the initial security setting of a system. Once the baseline has been applied, it must be maintained or improved. Maintaining the security baseline requires continuous monitoring. QUESTION 547Which of the following solutions provides the most flexibility when testing new security controls prior to implementation? A. Trusted OSB. Host software baseliningC. OS hardeningD. Virtualization Answer: D Explanation:Virtualization is used to host one or more operating systems in the memory of a single host computer and allows multiple operating systems to run simultaneously on the same hardware. Virtualization offers the flexibility of quickly and easily making backups of entire virtual systems, and quickly recovering the virtual system when errors occur. Furthermore, malicious code compromises of virtual systems rarely affect the host system, which allows for safer testing and experimentation. QUESTION 548A company is about to release a very large patch to its customers. An administrator is required to test patch installations several times prior to distributing them to customer PCs.Which of the following should the administrator use to test the patching process quickly and often? A. Create an incremental backup of an unpatched PCB. Create an image of a patched PC and replicate it to serversC. Create a full disk image to restore after each installationD. Create a virtualized sandbox and utilize snapshots Answer: D Explanation:Sandboxing is the process of isolating a system before installing new applications or patches on it so as to restrict the software from being able to cause harm to production systems. Before the patch is installed, a snapshot of the system should be taken. Snapshots are backups that can be used to quickly recover from poor updates, and errors arising from newly installed applications. QUESTION 549An administrator is building a development environment and requests that three virtual servers are cloned and placed in a new virtual network isolated from the production network. Which of the following describes the environment the administrator is building? A. CloudB. TrustedC. SandboxD. Snapshot Answer: CExplanation:Sandboxing is the process of isolating a system before installing new applications on it so as to restrict any potential malware that may be embedded in the new application from being able to cause harm to production systems. QUESTION 550Which of the following techniques describes the use of application isolation during execution to prevent system compromise if the application is compromised? A. Least privilege B. SandboxingC. Black boxD. Application hardening Answer: BExplanation:Sandboxing is the process of isolating a system before installing new applications on it so as to restrict any potential malware that may be embedded in the new application from being able to cause harm to production systems. More free Lead2pass SY0-401 exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDLXZsWm9MWmh0a0E Lead2pass is no doubt your best choice. Using the CompTIA SY0-401 exam dumps can let you improve the efficiency of your studying so that it can help you save much more time. 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]