[Lead2pass Professional Best Lead2pass CompTIA SY0-401 PDF Dumps With New Update Exam Questions (426-450)

Lead2pass 2017 September New CompTIA SY0-401 Exam Dumps! 100% Free Download! 100% Pass Guaranteed! Lead2pass provides 100% pass SY0-401 exam questions and answers for your CompTIA SY0-401 exam. We provide CompTIA SY0-401 exam questions from Lead2pass dumps and answers for the training of SY0-401 practice test. Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 426A vulnerability assessment indicates that a router can be accessed from default port 80 and default port 22. Which of the following should be executed on the router to prevent access via these ports? (Select TWO). A. FTP service should be disabledB. HTTPS service should be disabledC. SSH service should be disabledD. HTTP service should disabledE. Telnet service should be disabledAnswer: CDExplanation:Port 80 is used by HTTP. Port 22 is used by SSH. By disabling the HTTP and Telnet services, you will prevent access to the router on ports 80 and 22. QUESTION 427During a routine audit a web server is flagged for allowing the use of weak ciphers. Which of the following should be disabled to mitigate this risk? (Select TWO). A. SSL 1.0B. RC4C. SSL 3.0D. AESE. DESF. TLS 1.0 Answer: AEExplanation:TLS 1.0 and SSL 1.0 both have known vulnerabilities and have been replaced by later versions. Any systems running these ciphers should have them disabled. Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network. They use X.509 certificates and hence asymmetric cryptography to authenticate the counterparty with whom they are communicating, and to exchange a symmetric key. This session key is then used to encrypt data flowing between the parties. This allows for data/message confidentiality, and message authentication codes for message integrity and as a by-product, message authentication Netscape developed the original SSL protocol. Version 1.0 was never publicly released because of serious security flaws in the protocol; version 2.0, released in February 1995, "contained a number of security flaws which ultimately led to the design of SSL version 3.0". TLS 1.0 was first defined in RFC 2246 in January 1999 as an upgrade of SSL Version 3.0. As stated in the RFC, "the differences between this protocol and SSL 3.0 are not dramatic, but they are significant enough to preclude interoperability between TLS 1.0 and SSL 3.0". TLS 1.0 does include a means by which a TLS implementation can downgrade the connection to SSL 3.0, thus weakening security.TLS 1.1 and then TLS 1.2 were created to replace TLS 1.0. QUESTION 428A new web server has been provisioned at a third party hosting provider for processing credit card transactions. The security administrator runs the netstat command on the server and notices that ports 80, 443, and 3389 are in a `listening' state. No other ports are open. Which of the following services should be disabled to ensure secure communications? A. HTTPSB. HTTPC. RDPD. TELNET Answer: BExplanation:HTTP uses port 80. HTTP does not provide encrypted communications. Port 443 is used by HTTPS which provides secure encrypted communications. Port 3389 is used by RDP (Remote Desktop Protocol) which does provide encrypted communications. QUESTION 429Joe analyzed the following log and determined the security team should implement which of the following as a mitigation method against further attempts? Host 192.168.1.123[00: 00: 01]Successful Login: 015 192.168.1.123 : local[00: 00: 03]Unsuccessful Login: 022 214.34.56.006 : RDP 192.168.1.124[00: 00: 04]UnSuccessful Login: 010 214.34.56.006 : RDP 192.168.1.124[00: 00: 07]UnSuccessful Login: 007 214.34.56.006 : RDP 192.168.1.124[00: 00: 08]UnSuccessful Login: 003 214.34.56.006 : RDP 192.168.1.124 A. ReportingB. IDSC. Monitor system logsD. Hardening Answer: DExplanation:We can see a number of unsuccessful login attempts using a Remote Desktop Connection (using the RDP protocol) from a computer with the IP address 192.168.1.124. Someone successfully logged in locally. This is probably an authorized login (for example, Joe logging in).Hardening is the process of securing a system. We can harden (secure) the system by either disallowing remote desktop connections altogether or by restricting which IPs are allowed to initiate remote desktop connections. QUESTION 430The Chief Technology Officer (CTO) wants to improve security surrounding storage of customer passwords.The company currently stores passwords as SHA hashes. Which of the following can the CTO implement requiring the LEAST change to existing systems? A. Smart cardsB. TOTPC. Key stretchingD. Asymmetric keys Answer: AExplanation: Smart cards usually come in two forms. The most common takes the form of a rectangular piece of plastic with an embedded microchip. The second is as a USB token. It contains a built in processor and has the ability to securely store and process information. A "contact" smart card communicates with a PC using a smart card reader whereas a "contactless" card sends encrypted information via radio waves to the PC.Typical scenarios in which smart cards are used include interactive logon, e-mail signing, e-mail decryption and remote access authentication. However, smart cards are programmable and can contain programs and data for many different applications. For example smart cards may be used to store medical histories for use in emergencies, to make electronic cash payments or to verify the identity of a customer to an e-retailer.Microsoft provides two device independent APIs to insulate application developers from differences between current and future implementations: CryptoAPI and Microsoft

Win32?SCard APIs.The Cryptography API contains functions that allow applications to encrypt or digitally sign data in a flexible manner, while providing protection for the user's sensitive private key data. All cryptographic operations are performed by independent modules known as cryptographic service providers (CSPs).There are many different cryptographic algorithms and even when implementing the same algorithm there are many choices to make about key sizes and padding for example. For this reason, CSPs are grouped into types, in which each supported CryptoAPI function, by default, performs in a way particular to that type. For example, CSPs in the PROV_DSS provider type support DSS Signatures and MD5 and SHA hashing. QUESTION 431An auditor's report discovered several accounts with no activity for over 60 days. The accounts were later identified as contractors' accounts who would be returning in three months and would need to resume the activities. Which of the following would mitigate and secure the auditors finding? A. Disable unnecessary contractor accounts and inform the auditor of the update.B. Reset contractor accounts and inform the auditor of the update.C. Inform the auditor that the accounts belong to the contractors.D. Delete contractor accounts and inform the auditor of the update. Answer: AExplanation:A disabled account cannot be used. It is `disabled'. Whenever an employee leaves a company, the employee's user account should be disabled. The question states that the accounts are contractors' accounts who would be returning in three months. Therefore, it would be easier to keep the accounts rather than deleting them which would require that the accounts are recreated in three months time. By disabling the accounts, we can ensure that the accounts cannot be used; in three months when the contractors are back, we can simply re-enable the accounts. QUESTION 432An administrator notices that former temporary employees' accounts are still active on a domain.Which of the following can be implemented to increase security and prevent this from happening? A. Implement a password expiration policy.B. Implement an account expiration date for permanent employees.C. Implement time of day restrictions for all temporary employees.D. Run a last logon script to look for inactive accounts. Answer: DExplanation:You can run a script to return a list of all accounts that haven't been used for a number of days, for example 30 days. If an account hasn't been logged into for 30 days, it's a safe bet that the user the account belonged to is no longer with the company. You can then disable all the accounts that the script returns. A disabled account cannot be used to log in to a system. This is a good security measure. As soon as an employee leaves the company, the employees account should always be disabled. QUESTION 433How must user accounts for exiting employees be handled? A. Disabled, regardless of the circumstancesB. Disabled if the employee has been terminatedC. Deleted, regardless of the circumstancesD. Deleted if the employee has been terminated Answer: AExplanation:You should always disable an employee's account as soon as they leave. The employee knows the username and password of the account and could continue to log in for potentially malicious purposes. Disabling the account will ensure that no one can log in using that account. QUESTION 434An administrator has a network subnet dedicated to a group of users. Due to concerns regarding data and network security, the administrator desires to provide network access for this group only. Which of the following would BEST address this desire? A. Install a proxy server between the users' computers and the switch to filter inbound network traffic.B. Block commonly used ports and forward them to higher and unused port numbers.C. Configure the switch to allow only traffic from computers based upon their physical address.D. Install host-based intrusion detection software to monitor incoming DHCP Discover requests. Answer: C Explanation:Configuring the switch to allow only traffic from computers based upon their physical address is known as MAC filtering. The physical address is known as the MAC address. Every network adapter has a unique MAC address hardcoded into the adapter. You can configure the ports of a switch to allow connections from computers with specific MAC addresses only and block all other MAC addresses.MAC filtering is commonly used in wireless networks but is considered insecure because a MAC address can be spoofed. However, in a wired network, it is more secure because it would be more difficult for a rogue computer to sniff a MAC address. QUESTION 435A new virtual server was created for the marketing department. The server was installed on an existing host machine. Users in the marketing department report that they are unable to connect to the server. Technicians verify that the server has an IP address in the same VLAN as the marketing department users. Which of the following is the MOST likely reason the users are unable to connect to the server? A. The new virtual server's MAC address was not added to the ACL on the switchB. The new virtual server's MAC address triggered a port security violation on the switchC. The new virtual server's MAC address triggered an implicit deny in the switchD. The new virtual server's MAC address was not added to the firewall rules on the switch Answer: AExplanation:Configuring the switch to allow only traffic from computers based upon their physical address is known as MAC filtering. The physical address is known as the MAC address. Every network adapter has a unique MAC address hardcoded into the adapter. You can configure the ports of a switch to allow connections from computers with specific MAC addresses only and block all other MAC addresses.In computer networking, MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network.MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists. While the restriction of network access through the

use of lists is straightforward, an individual person is not identified by a MAC address, rather a device only, so an authorized person will need to have a whitelist entry for each device that he or she would use to access the network. QUESTION 436Which of the following can be implemented if a security administrator wants only certain devices connecting to the wireless network? A. Disable SSID broadcastB. Install a RADIUS serverC. Enable MAC filteringD. Lowering power levels on the AP Answer: C Explanation:MAC filtering is commonly used in wireless networks. In computer networking, MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network. MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists. While the restriction of network access through the use of lists is straightforward, an individual person is not identified by a MAC address, rather a device only, so an authorized person will need to have a whitelist entry for each device that he or she would use to access the network. QUESTION 437Which of the following implementation steps would be appropriate for a public wireless hot-spot? A. Reduce power levelB. Disable SSID broadcastC. Open system authenticationD. MAC filter Answer: CExplanation:For a public wireless hot-spot, you want members of the public to be able to access the wireless network without having to provide them with a password. Therefore, Open System Authentication is the best solution.Open System Authentication (OSA) is a process by which a computer can gain access to a wireless network that uses the Wired Equivalent Privacy (WEP) protocol. With OSA, a computer equipped with a wireless modem can access any WEP network and receive files that are not encrypted.For OSA to work, the service set identifier (SSID) of the computer should match the SSID of the wireless access point. The SSID is a sequence of characters that uniquely names a wireless local area network (WLAN). The process occurs in three steps. First, the computer sends a request for authentication to the access point. Then the access point generates an authentication code, usually at random, intended for use only during that session. Finally, the computer accepts the authentication code and becomes part of the network as long as the session continues and the computer remains within range of the original access point. If it is necessary to exchange encrypted data between a WEP network access point and a wireless-equipped computer, a stronger authentication process called Shared Key Authentication (SKA) is required. QUESTION 438Which of the following controls would allow a company to reduce the exposure of sensitive systems from unmanaged devices on internal networks? A. 802.1xB. Data encryptionC. Password strengthD. BGP Answer: AExplanation:IEEE 802.1X (also known as Dot1x) is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN- though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols. The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. An analogy to this is providing a valid visa at the airport's arrival immigration before being allowed to enter the country. With 802.1X port- based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network. QUESTION 439A system security analyst using an enterprise monitoring tool notices an unknown internal host exfiltrating files to several foreign IP addresses. Which of the following would be an appropriate mitigation technique? A. Disabling unnecessary accountsB. Rogue machine detectionC. Encrypting sensitive filesD. Implementing antivirus Answer: BExplanation:Rogue machine detection is the process of detecting devices on the network that should not be there. If a user brings in a laptop and plugs it into the network, the laptop is a "rogue machine". The laptop could cause problems on the network. Any device on the network that should not be there is classed as rogue. QUESTION 440Matt, a developer, recently attended a workshop on a new application. The developer installs the new application on a production system to test the functionality. Which of the following is MOST likely affected? A. Application designB. Application securityC. Initial baseline configurationD. Management of interfaces Answer: CExplanation:The initial baseline configuration of a computer system is an agreed configuration for the computer. For example, the initial baseline configuration will list what operating system he computer will run, what software applications and patches will be installed and what configuration settings should be applied to the system.In this question, we are installing a new software application on a server. After the installation of the software, the "configuration" of the server (installed software, settings etc) is now different from the initial baseline configuration. QUESTION 441In order to maintain oversight of a third party service provider, the company is going to implement a Governance, Risk, and Compliance (GRC) system. This system is

promising to provide overall security posture coverage. Which of the following is the MOST important activity that should be considered? A. Continuous security monitoringB. Baseline configuration and host hardeningC. Service Level Agreement (SLA) monitoringD. Security alerting and trending Answer: AExplanation:The company is investing in a Governance, Risk, and Compliance (GRC) system to provide overall security posture coverage. This is great for testing the security posture. However, to be effective and ensure the company always has a good security posture, you need to monitor the security continuously.Once a baseline security configuration is documented, it is critical to monitor it to see that this baseline is maintained or exceeded. A popular phrase among personal trainers is "that which gets measured gets improved." Well, in network security, "that which gets monitored gets secure." Continuous monitoring means exactly that: ongoing monitoring. This may involve regular measurements of network traffic levels, routine evaluations for regulatory compliance, and checks of network security device configurations. QUESTION 442A security analyst performs the following activities: monitors security logs, installs surveillance cameras and analyzes trend reports. Which of the following job responsibilities is the analyst performing? (Select TWO). A. Detect security incidentsB. Reduce attack surface of systemsC. Implement monitoring controlsD. Hardening network devicesE. Prevent unauthorized access Answer: ACExplanation:By monitoring security logs, installing security cameras and analyzing trend reports, the security analyst is implementing monitoring controls.With the monitoring controls in place, by monitoring the security logs, reviewing the footage from the security cameras and analyzing trend reports, the security analyst is able to detect security incidents. QUESTION 443 Which of the following is an indication of an ongoing current problem? A. AlertB. TrendC. AlarmD. Trap Answer: C Explanation:An alarm indicates that something is wrong and needs to be resolved as soon as possible. Alarms usually continue to sound until the problem is resolved or the alarm is manually silenced. QUESTION 444Which of the following is a notification that an unusual condition exists and should be investigated? A. AlertB. TrendC. AlarmD. Trap Answer: AExplanation:We need to look carefully at the wording of the question to determine the answer. This question is asking about an "unusual condition" that should be investigated. There are different levels of alerts from Critical to Warning to Information only.An Alarm would be triggered by a serious definite problem that needs resolving urgently. An "unusual condition" probably wouldn't trigger an alarm; it is more likely to trigger an Alert. QUESTION 445A security manager must remain aware of the security posture of each system. Which of the following supports this requirement? A. Training staff on security policiesB. Establishing baseline reportingC. Installing anti-malware softwareD. Disabling unnecessary accounts/services Answer: BExplanation:The IT baseline protection approach is a methodology to identify and implement computer security measures in an organization. The aim is the achievement of an adequate and appropriate level of security for IT systems. This is known as a baseline.A baseline report compares the current status of network systems in terms of security updates, performance or other metrics to a predefined set of standards (the baseline). QUESTION 446Suspicious traffic without a specific signature was detected. Under further investigation, it was determined that these were false indicators. Which of the following security devices needs to be configured to disable future false alarms? A. Signature based IPSB. Signature based IDSC. Application based IPSD. Anomaly based IDS Answer: DExplanation:Most intrusion detection systems (IDS) are what is known as signature-based. This means that they operate in much the same way as a virus scanner, by searching for a known identity - or signature - for each specific intrusion event. And, while signature-based IDS is very efficient at sniffing out known s of attack, it does, like anti-virus software, depend on receiving regular signature updates, to keep in touch with variations in hacker technique. In other words, signature- based IDS is only as good as its database of stored signatures. Any organization wanting to implement a more thorough - and hence safer - solution, should consider what we call anomaly-based IDS. By its nature, anomaly-based IDS is a rather more complex creature. In network traffic terms, it captures all the headers of the IP packets running towards the network. From this, it filters out all known and legal traffic, including web traffic to the organization's web server, mail traffic to and from its mail server, outgoing web traffic from company employees and DNS traffic to and from its DNS server.There are other equally obvious advantages to using anomaly-based IDS. For example, because it detects any traffic that is new or unusual, the anomaly method is particularly good at identifying sweeps and probes towards network hardware. It can, therefore, give early warnings of potential intrusions, because probes and scans are the predecessors of all attacks. And this applies equally to any new service installed on any item of hardware - for example, Telnet deployed on a network router for maintenance purposes and forgotten about when the maintenance was finished. This makes anomaly-based IDS perfect for detecting anything from port anomalies and web anomalies to mis-formed attacks, where the URL is deliberately mis-typed. QUESTION 447 Jane, a security administrator, has observed repeated attempts to break into a server. Which of the following is designed to stop an intrusion on a specific server? A. HIPSB. NIDSC. HIDSD. NIPS Answer: AExplanation:This question is asking which of the following is designed to stop an intrusion on a specific server. To stop an intrusion on a specific server, you would use a HIPS (Host Intrusion Prevention System). The difference between a HIPS and other intrusion prevention systems is that a HIPS is a software intrusion prevention systems that is installed on a `specific server'. Intrusion prevention systems (IPS), also known as intrusion

detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it. A HIPS (Host Intrusion Prevention System) is software installed on a host which monitors the host for suspicious activity by analyzing events occurring within that host with the aim of detecting and preventing intrusion. QUESTION 448Which of the following tools will allow a technician to detect security-related TCP connection anomalies? A. Logical tokenB. Performance monitorC. Public key infrastructureD. Trusted platform module Answer: B Explanation:Performance Monitor in a Windows system can monitor many different `counters'. For TCP network connections, you can monitor specific TCP related counters including the following:Connection FailuresConnections ActiveConnections Established Connections PassiveConnections ResetSegments Received/secSegments Retransmitted/secSegments Sent/secTotal Segments/sec By monitoring the counters listed above, you will be able to detect security-related TCP connection anomalies. QUESTION 449Which of the following would a security administrator implement in order to identify a problem between two systems that are not communicating properly? A. Protocol analyzerB. Baseline reportC. Risk assessmentD. Vulnerability scan Answer: A Explanation:A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. Capturing and analyzing the packets sent from two systems that are not communicating properly could help determine the cause of the issue.Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal). QUESTION 450Which of the following is BEST used to capture and analyze network traffic between hosts on the same network segment? A. Protocol analyzerB. Router C. FirewallD. HIPS Answer: AExplanation:A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. Capturing and analyzing the packets sent from two systems that are not communicating properly could help determine the cause of the issue.Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal). More free Lead2pass SY0-401 exam new questions on Google Drive:
https://drive.google.com/open?id=0B3Syig5i8gpDLXZsWm9MWmh0a0E Lead2pass is the leader in SY0-401 certification test questions with training materials for CompTIA SY0-401 exam dumps. Lead2pass CompTIA training tools are constantly being revised and updated. We 100% guarantee CompTIA SY0-401 exam questions with quality and reliability which will help you pass CompTIA SY0-401 exam. 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]