[Nov-2017 Dumps Passing SY0-501 Exam By Learning PassLeader Free SY0-501 Exam Dumps (Section C)

New Updated SY0-501 Exam Questions from PassLeader SY0-501 PDF dumps! Welcome to download the newest PassLeader SY0-501 VCE dumps: https://www.passleader.com/sy0-501.html (166 Q&As) Keywords: SY0-501 exam dumps, SY0-501 exam questions, SY0-501 VCE dumps, SY0-501 PDF dumps, SY0-501 practice tests, SY0-501 study guide, SY0-501 braindumps, CompTIA Security+ Exam P.S. New SY0-501 dumps PDF: https://drive.google.com/open?id=1Ei1CtZKTLawI_2jpkecHaVbM_kXPMZAu >> New SY0-401 dumps PDF: https://drive.google.com/open?id=0B-ob6L_QjGLpcG9CWHp3bXlNTTg QUESTION 61 The Chief Security Officer (CSO) at a multinational banking corporation is reviewing a plan to upgrade the entire corporate IT infrastructure. The architecture consists of a centralized cloud environment hosting the majority of data, small server clusters at each corporate location to handle the majority of customer transaction processing, ATMs, and a new mobile banking application accessible from smartphones, tablets, and the Internet via HTTP. The corporation does business having varying data retention and privacy laws. Which of the following technical modifications to the architecture and corresponding security controls should be implemented to provide the MOST complete protection of data? A.   Revoke exiting root certificates, re-issue new customer certificates, and ensure all transactions are digitally signed to minimize fraud, implement encryption for data in-transit between data centers. B.   Ensure all data is encryption according to the most stringent regulatory guidance applicable, implement encryption for data in-transit between data centers, increase data availability by replicating all data, transaction data, logs between each corporate location. C.   Store customer data based on national borders, ensure end-to end encryption between ATMs, end users, and servers, test redundancy and COOP plans to ensure data is not inadvertently shifted from one legal jurisdiction to another with more stringent regulations. D.   Install redundant servers to handle corporate customer processing, encrypt all customer data to ease the transfer from one country to another, implement end-to-end encryption between mobile applications and the cloud. Answer: C QUESTION 62 While reviewing the monthly internet usage it is noted that there is a large spike in traffic classified as "unknown" and does not appear to be within the bounds of the organizations Acceptable Use Policy. Which of the following tool or technology would work BEST for obtaining more information on this traffic? A.   Firewall logs B.   IDS logs C.   Increased spam filtering D.   Protocol analyzer Answer: B QUESTION 63 A network administrator wants to ensure that users do not connect any unauthorized devices to the company network. Each desk needs to connect a VoIP phone and computer. Which of the following is the BEST way to accomplish this? A.   Enforce authentication for network devices B.   Configure the phones on one VLAN, and computers on another C.   Enable and configure port channels D.   Make users sign an Acceptable use Agreement Answer: A QUESTION 64 An administrator has concerns regarding the traveling sales team who works primarily from smart phones. Given the sensitive nature of their work, which of the following would BEST prevent access to the data in case of loss or theft? A.   Enable screensaver locks when the phones are not in use to prevent unauthorized access. B.   Configure the smart phones so that the stored data can be destroyed from a centralized location. C.   Configure the smart phones so that all data is saved to removable media and kept separate from the device. D.   Enable GPS tracking on all smart phones so that they can be quickly located and recovered. Answer: B QUESTION 65 A user of the wireless network is unable to gain access to the network. The symptoms are: * Unable to connect to both internal and Internet resources. * The wireless icon shows connectivity but has no network access. The wireless network is WPA2 Enterprise and users must be a member of the wireless security group to authenticate. Which of the following is the MOST likely cause of the connectivity issues? A.   The wireless signal is not strong enough B.   A remote DDoS attack against the RADIUS server is taking place C.   The user's laptop only supports WPA and WEP D.   The DHCP scope is full E.   The dynamic encryption key did not update while the user was offline Answer: A QUESTION 66 A Chief Financial Officer (CFO) has asked the Chief Information Officer (CIO) to provide responses to a recent audit report detailing deficiencies in the organization security controls. The CFO would like to know ways in which the organization can improve its authorization controls. Given the request by the CFO, which of the following controls should the CIO focus on in the report? (Select THREE.) A.   Password complexity policies B.   Hardware tokens C.   Biometric systems D.   Role-based permissions E.   One time passwords F.   Separation of duties G.   Multifactor authentication H.   Single sign-on I.   Lease

privilege Answer: DFI QUESTION 67 A mobile device user is concerned about geographic positioning information being included in messages sent between users on a popular social network platform. The user turns off the functionality in the application, but wants to ensure the application cannot re-enable the setting without the knowledge of the user. Which of the following mobile device capabilities should the user disable to achieve the stated goal? A.   Device access control B.   Location based services C.   Application control D.   GEO-Tagging Answer: D QUESTION 68 A member of a digital forensics team, Joe arrives at a crime scene and is preparing to collect system data. Before powering the system off, Joe knows that he must collect the most volatile date first. Which of the following is the correct order in which Joe should collect the data? A.   CPU cache, paging/swap files, RAM, remote logging data B.   RAM, CPU cache, Remote logging data, paging/swap files C.   Paging/swap files, CPU cache, RAM, remote logging data D.   CPU cache, RAM, paging/swap files, remote logging data Answer: D QUESTION 69 An organization has hired a penetration tester to test the security of its ten web servers. The penetration tester is able to gain root/administrative access in several servers by exploiting vulnerabilities associated with the implementation of SMTP, POP, DNS, FTP, Telnet, and IMAP. Which of the following recommendations should the penetration tester provide to the organization to better protect their web servers in the future? A.   Use a honeypot B.   Disable unnecessary services C.   Implement transport layer security D.   Increase application event logging Answer: B QUESTION 70 A security engineer is faced with competing requirements from the networking group and database administrators. The database administrators would like ten application servers on the same subnet for ease of administration, whereas the networking group would like to segment all applications from one another. Which of the following should the security administrator do to rectify this issue? A.   Recommend performing a security assessment on each application, and only segment the applications with the most vulnerability. B.   Recommend classifying each application into like security groups and segmenting the groups from one another. C.   Recommend segmenting each application, as it is the most secure approach. D.   Recommend that only applications with minimal security features should be segmented to protect them. Answer: B QUESTION 71 A security analyst has been asked to perform a review of an organization's software development lifecycle. The analyst reports that the lifecycle does not contain a phase in which team members evaluate and provide critical feedback of another developer's code. Which of the following assessment techniques is BEST described in the analyst's report? A.   Architecture evaluation B.   Baseline reporting C.   Whitebox testing D.   Peer review Answer: D QUESTION 72 An attacker wearing a building maintenance uniform approached a company's receptionist asking for access to a secure area. The receptionist asks for identification, a building access badge and checks the company's list approved maintenance personnel prior to granting physical access to the secure are. The controls used by the receptionist are in place to prevent which of the following types of attacks? A.   Tailgating B.   Shoulder surfing C.   Impersonation D.   Hoax Answer: C QUESTION 73 A security administrator is tasked with conducting an assessment made to establish the baseline security posture of the corporate IT infrastructure. The assessment must report actual flaws and weaknesses in the infrastructure. Due to the expense of hiring outside consultants, the testing must be performed using in-house or cheaply available resource. There cannot be a possibility of any requirement being damaged in the test. Which of the following has the administrator been tasked to perform? A.   Risk transference B.   Penetration test C.   Threat assessment D.   Vulnerability assessment Answer: D QUESTION 74 A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website. During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine. Which of the following describes the type of attack the proxy has been legitimately programmed to perform? A.   Transitive access B.   Spoofing C.   Man-in-the-middle D.   Replay Answer: C QUESTION 75 Which of the following use the SSH protocol? A.   Stelnet B.   SCP C.   SNMP D.   FTPS E.   SSL F.   SFTP Answer: BF QUESTION 76 Which of the following is the GREATEST risk to a company by allowing employees to physically bring their personal smartphones to work? A.   Taking pictures of proprietary information and equipment in restricted areas. B.   Installing soft token software to connect to the company's wireless network. C.   Company cannot automate patch management on personally-owned devices. D.   Increases the attack surface by having more target devices on the company's campus. Answer: A QUESTION 77 Which of the following is the summary of loss for a given year? A.   MTBF

B.   ALE C.   SLA D.   ARO Answer: B QUESTION 78 A Security Officer on a military base needs to encrypt several smart phones that will be going into the field. Which of the following encryption solutions should be deployed in this situation? A.   Elliptic curve B.   One-time pad C.   3DES D.   AES-256 Answer: D QUESTION 79 An organization relies heavily on an application that has a high frequency of security updates. At present, the security team only updates the application on the first Monday of each month, even though the security updates are released as often as twice a week. Which of the following would be the BEST method of updating this application? A.   Configure testing and automate patch management for the application. B.   Configure security control testing for the application. C.   Manually apply updates for the application when they are released. D.   Configure a sandbox for testing patches before the scheduled monthly update. Answer: A QUESTION 80 A technician must configure a firewall to block external DNS traffic from entering a network. Which of the following ports should they block on the firewall? A.   53 B.   110 C.   143 D.   443 Answer: A QUESTION 81 A software development company needs to share information between two remote servers, using encryption to protect it. A programmer suggests developing a new encryption protocol, arguing that using an unknown protocol with secure, existing cryptographic algorithm libraries will provide strong encryption without being susceptible to attacks on other known protocols. Which of the following summarizes the BEST response to the programmer's proposal? A.   The newly developed protocol will only be as secure as the underlying cryptographic algorithms used. B.   New protocols often introduce unexpected vulnerabilities, even when developed with otherwise secure and tested algorithm libraries. C.   A programmer should have specialized training in protocol development before attempting to design a new encryption protocol. D.   The obscurity value of unproven protocols against attacks often outweighs the potential for introducing new vulnerabilities. Answer: B QUESTION 82 A security technician would like to obscure sensitive data within a file so that it can be transferred without causing suspicion. Which of the following technologies would BEST be suited to accomplish this? A.   Transport Encryption B.   Stream Encryption C.   Digital Signature D.   Steganography Answer: D Explanation: Steganography is the process of hiding a message in another message so as to obfuscate its importance. It is also the process of hiding a message in a medium such as a digital image, audio file, or other file. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or message and use that file to hide your message. References: https://en.wikipedia.org/wiki/Steganography QUESTION 83 A supervisor in your organization was demoted on Friday afternoon. The supervisor had the ability to modify the contents of a confidential database, as well as other managerial permissions. On Monday morning, the database administrator reported that log files indicated that several records were missing from the database Which of the following risk mitigation strategies should have been implemented when the supervisor was demoted? A.   Incident management B.   Routine auditing C.   IT governance D.   Monthly user rights reviews Answer: D QUESTION 84 Which of the following attack types is being carried out where a target is being sent unsolicited messages via Bluetooth? A.   War chalking B.   Bluejacking C.   Bluesnarfing D.   Rogue tethering Answer: B Explanation: Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol. References: https://en.wikipedia.org/wiki/Bluejacking QUESTION 85 Joe is exchanging encrypted email with another party. Joe encrypts the initial email with a key. When Joe receives a response, he is unable to decrypt the response with the same key he used initially. Which of the following would explain the situation? A.   An ephemeral key was used for one of the messages. B.   A stream cipher was used for the initial email; a block cipher was used for the reply. C.   Out-of-band key exchange has taken place. D.   Asymmetric encryption is being used. Answer: D Explanation: Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes. References: https://www.digicert.com/ssl-cryptography.htm https://en.wikipedia.org/wiki/Public-key_cryptography QUESTION 86 Recently several employees were victims of a phishing email that appeared to originate from the company president. The email claimed the employees would be disciplined if they did not click on a malicious link in the message. Which of the following principles of social engineering made this attack successful? A.   Authority B.   Spamming

C.   Social proof D.   Scarcity Answer: A QUESTION 87 Which of the following is the LEAST secure hashing algorithm? A.   SHA1 B.   RIPEMD C.   MD5 D.   DES Answer: C QUESTION 88 An employee uses RDP to connect back to the office network. If RDP is misconfigured, which of the following security exposures would this lead to? A.   A virus on the administrator's desktop would be able to sniff the administrator's username and password. B.   Result in an attacker being able to phish the employee's username and password. C.   A social engineering attack could occur, resulting in the employee's password being extracted. D.   A man in the middle attack could occur, resulting the employee's username and password being captured. Answer: D QUESTION 89 Joe, the security administrator, sees this in a vulnerability scan report: "The server 10.1.2.232 is running Apache 2.2.20 which may be vulnerable to a mod_cgi exploit." Joe verifies that the mod_cgi module is not enabled on 10.1.2.232. This message is an example of what? A.   a threat. B.   a risk. C.   a false negative. D.   a false positive. Answer: D QUESTION 90 A security analyst wishes to increase the security of an FTP server. Currently, all trails to the FTP server is unencrypted. Users connecting to the FTP server use a variety of modem FTP client software. The security analyst wants to keep the same port and protocol, while also still allowing unencrypted connections. Which of the following would BEST accomplish these goals? A.   Require the SFTP protocol to connect to the file server. B.   Use implicit TLS on the FTP server. C.   Use explicit FTPS for the connections. D.   Use SSH tunneling to encrypt the FTP traffic. Answer: B Download the newest PassLeader SY0-501 dumps from passleader.com now! 100% Pass Guarantee! SY0-501 PDF dumps & SY0-501 VCE dumps: https://www.passleader.com/sy0-501.html (166 Q&As) (New Questions Are 100% Available and Wrong Answers Have Been Corrected! Free VCE simulator!) P.S. New SY0-501 dumps PDF: https://drive.google.com/open?id=1Ei1CtZKTLawI_2jpkecHaVbM_kXPMZAu >> New SY0-401 dumps PDF: https://drive.google.com/open?id=0B-ob6L_QjGLpcG9CWHp3bXlNTTg