[November-2018SY0-501 Dumps 566Q Instant Download in Braindump2go[Q168-Q178

2018/November Braindump2go SY0-501 Exam Dumps with PDF and VCE New Updated Today! Following are some new SY0-501 Real Exam Questions:1.|2018 Latest SY0-501 Exam Dumps (PDF & VCE) 566Q&As Download:https://www.braindump2go.com/sy0-501.html2.|2018 Latest SY0-501 Exam Questions & Answers Download:https://drive.google.com/drive/folders/1Mto9aYkbmrvlHB5IFqCx-MuIqEVJQ9Yu?usp=sharingQUESTION 168An attacker uses a network sniffer to capture the packets of a transaction that adds $20 to a gift card. The attacker then user a function of the sniffer to push those packets back onto the network again, adding another $20 to the gift card. This can be done many times. Which of the following describes this type of attack?A. Integer overflow attackB. Smurf attackC. Replay attackD. Buffer overflow attackE. Cross-site scripting attack**Answer: C**QUESTION 169An organization is moving its human resources system to a cloud services provider. The company plans to continue using internal usernames and passwords with the service provider, but the security manager does not want the service provider to have a company of the passwords. Which of the following options meets all of these requirements?A. Two-factor authenticationB. Account and password synchronizationC. Smartcards with PINSD. Federated authentication**Answer: D**QUESTION 170The data backup window has expanded into the morning hours and has begun to affect production users. The main bottleneck in the process is the time it takes to replicate the backups to separate severs at the offsite data center. Which of the following uses of deduplication could be implemented to reduce the backup window?A. Implement deduplication at the network level between the two locationsB. Implement deduplication on the storage array to reduce the amount of drive space neededC. Implement deduplication on the server storage to reduce the data backed upD. Implement deduplication on both the local and remote servers**Answer: B**QUESTION 171A penetration testing is preparing for a client engagement in which the tester must provide data that proves and validates the scanning tools' results. Which of the following is the best method for collecting this information?A. Set up the scanning system's firewall to permit and log all outbound connectionsB. Use a protocol analyzer to log all pertinent network trafficC. Configure network flow data logging on all scanning systemD. Enable debug level logging on the scanning system and all scanning tools used.**Answer: B**QUESTION 172Which of the following best describes the initial processing phase used in mobile device forensics?A. The phone should be powered down and the battery removed to preserve the state of data on any internal or removable storage utilized by the mobile deviceB. The removable data storage cards should be processed first to prevent data alteration when examining the mobile deviceC. The mobile device should be examined first, then removable storage and lastly the phone without removable storage should be examined againD. The phone and storage cards should be examined as a complete unit after examining the removable storage cards separately.**Answer: D** QUESTION 173Ann a security analyst is monitoring the IDS console and noticed multiple connections from an internal host to a suspicious call back domain. Which of the following tools would aid her to decipher the network traffic?A. Vulnerability Scanner B. NMAPC. NETSTATD. Packet Analyzer**Answer: D**QUESTION 174An administrator is testing the collision resistance of different hashing algorithms. Which of the following is the strongest collision resistance test?A. Find two identical messages with different hashesB. Find two identical messages with the same hashC. Find a common has between two specific messagesD. Find a common hash between a specific message and a random message**Answer: A**QUESTION 175The SSID broadcast for a wireless router has been disabled but a network administrator notices that unauthorized users are accessing the wireless network. The administor has determined that attackers are still able to detect the presence of the wireless network despite the fact the SSID has been disabled. Which of the following would further obscure the presence of the wireless network?A. Upgrade the encryption to WPA or WPA2B. Create a non-zero length SSID for the wireless routerC. Reroute wireless users to a honeypotD. Disable responses to a broadcast probe requestAnswer: DExplanation:When ?SSID broadcast? is disabled you can:1) Completely disable the sending of beacons2) Disable probe responses except in cases where the probe request was explicitly addressed to the correct SSID (ignore broadcast probe requests to the wildcardSSID) and was from an authorized client (apply MAC Address filtering), and even send a null SSID in the probe responses to those.QUESTION 176Which of the following should be used to implement voice encryption?A. SSLv3B. VDSLC. SRTPD. VoIP**Answer: C**QUESTION 177During an application design, the development team specifics a LDAP module for single sign-on communication with the company's access control database. This is an example of which of the following?A. Application controlB. Data in-transitC. IdentificationD. Authentication**Answer: D**QUESTION 178After a merger, it was determined that several individuals could perform the tasks of a network administrator in the merged organization. Which of the following should have been performed to ensure that employees have proper access?A. Time-of-day restrictionsB. Change managementC. Periodic auditing of user credentialsD. User rights and permission review**Answer: D** !!!RECOMMEND!!!1.|2018 Latest SY0-501 Exam Dumps (PDF & VCE) 566Q&As

Download:https://www.braindump2go.com/sy0-501.html2.|2018 Latest SY0-501 Study Guide Video: YouTube Video: YouTube.com/watch?v=J3AL-94tVwI