[June-2018-NewFree Braindump2go New SY0-501 Dumps 563Q[374-384

2018 June Latest CompTIA SY0-501 Exam Dumps with PDF and VCE Just Updated Today! Following are some new SY0-501 Real Exam Questions: 1.|2018 Latest SY0-501 Exam Dumps (PDF & VCE) 563Q 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=sharing**QUESTION 374Which of the following BEST describes an important security advantage yielded by implementing vendor diversity?**A. SustainabilityB. HomogeneityC. ResiliencyD. Configurability**Answer: C**QUESTION 375A dumpster diver recovers several hard drives from a company and is able to obtain confidential data from one of the hard drives. The company then discovers its information is posted online. Which of the following methods would have MOST likely prevented the data from being exposed?A. Removing the hard drive from its enclosureB. Using software to repeatedly rewrite over the disk spaceC. Using Blowfish encryption on the hard drivesD. Using magnetic fields to erase the data**Answer: D**QUESTION 376A manager wants to distribute a report to several other managers with the company. Some of them reside in remote locations that are not connected to the domain but have a local server. Because there is sensitive data within the report and the size of the report is beyond the limit of the email attachment size, emailing the report is not an option. Which of the following protocols should be implemented to distribute the report securely? (Select THREE)A. S/MIMEB. SSHC. SNMPv3D. FTPSE. SRTPF. HTTPSG. LDAPS**Answer: BDF** QUESTION 377A vice president at a manufacturing organization is concerned about desktops being connected to the network. Employees need to log onto the desktops' local account to verify that a product is being created within specifications; otherwise, the desktops should be as isolated as possible. Which of the following is the BEST way to accomplish this?A. Put the desktops in the DMZ.B. Create a separate VLAN for the desktops.C. Air gap the desktops.D. Join the desktops to an ad-hoc network.**Answer: C**QUESTION 378An in-house penetration tester has been asked to evade a new DLP system. The tester plans to exfiltrate data through steganography. Discovery of which of the following would help catch the tester in the act?A. Abnormally high numbers of outgoing instant messages that contain obfuscated textB. Large-capacity USB drives on the tester's desk with encrypted zip filesC. Outgoing emails containing unusually large image filesD. Unusual SFTP connections to a consumer IP address**Answer: C** QUESTION 379A member of the admins group reports being unable to modify the "changes" file on a server. The permissions on the file are as follows:Permissions User Group File-rwxrw-r--+ Admins Admins changesBased on the output above, which of the following BEST explains why the user is unable to modify the "changes" file?A. The SELinux mode on the server is set to "enforcing."B. The SELinux mode on the server is set to "permissive."C. An FACL has been added to the permissions for the file.D. The admins group does not have adequate permissions to access the file.**Answer: C**QUESTION 380A penetration tester is conducting an assessment on Comptia.org and runs the following command from a coffee shop while connected to the public Internet:c:nslookup -querytype=MX comptia.orgServer: UnknownAddress: 198.51.100.45comptia.org MX preference=10, mail exchanger = 92.68.102.33comptia.org MX preference=20, mail exchanger = exchg1.comptia.org exchg1.comptia.org internet address = 192.168.102.67Which of the following should the penetration tester conclude about the command output?A. The public/private views on the Comptia.org DNS servers are misconfigured.B. Comptia.org is running an older mail server, which may be vulnerable to exploits.C. The DNS SPF records have not been updated for Comptia.org.D. 192.168.102.67 is a backup mail server that may be more vulnerable to attack.**Answer: D**QUESTION 381A security analyst is inspecting the results of a recent internal vulnerability scan that was performed against intranet services. The scan reports include the following critical-rated vulnerability:Title: Remote Command Execution vulnerability in web serverRating: Critical (CVSS 10.0)Threat actor: any remote user of the web serverConfidence: certainRecommendation: apply vendor patchesWhich of the following actions should the security analyst perform FIRST?A. Escalate the issue to senior management.B. Apply organizational context to the risk rating.C. Organize for urgent out-of-cycle patching.D. Exploit the server to check whether it is a false positive.**Answer: B**QUESTION 382 Company A agrees to provide perimeter protection, power, and environmental support with measurable goals for Company B, but will not be responsible for user authentication or patching of operating systems within the perimeter. Which of the following is being described?A. Service level agreementB. Memorandum of understandingC. Business partner agreementD. Interoperability agreement**Answer: A**QUESTION 383A company is deploying smartphones for its mobile salesforce. These devices are for personal and business use but are owned by the company. Sales personnel will save new customer data via a custom application developed for the company. This application will integrate with the contact information stored in the smartphones and will populate new customer records onto it. The customer application's data is encrypted at rest, and the application's connection to the back office system is considered secure. The Chief Information Security Officer (CISO) has concerns that customer contact information may be accidentally leaked due to the limited security capabilities of the devices and the planned controls. Which of the following will be

the MOST efficient security control to implement to lower this risk?A. Implement a mobile data loss agent on the devices to prevent any user manipulation with the contact information.B. Restrict screen capture features on the devices when using the custom application and the contact information.C. Restrict contact information storage dataflow so it is only shared with the customer application.D. Require complex passwords for authentication when accessing the contact information.**Answer: C**
QUESTION 384The Chief Information Security Officer (CISO) is asking for ways to protect against zero-day exploits. The CISO is concerned that an unrecognized threat could compromise corporate data and result in regulatory fines as well as poor corporate publicity. The network is mostly flat, with split staff/guest wireless functionality. Which of the following equipment MUST be deployed to guard against unknown threats?A. Cloud-based antivirus solution, running as local admin, with push technology for definition updatesB. Implementation of an off-site datacenter hosting all company data, as well as deployment of VDI for all client computing needsC. Host-based heuristic IPS, segregated on a management VLAN, with direct control of the perimeter firewall ACLsD. Behavior-based IPS with a communication link to a cloud-based vulnerability and threat feed**Answer: D**
!!!RECOMMEND!!!1.|2018 Latest SY0-501 Exam Dumps (PDF & VCE) 563Q Download:https://www.braindump2go.com/sy0-501.html2.|2018 Latest SY0-501 Study Guide Video: YouTube Video: YouTube.com/watch?v=NVxs6ev6Ww0