[October-2020SY0-501 Exam Dumps VCE Free Download in Braindump2go[Q1204-Q1235

2020/October Latest Braindump2go SY0-501 Exam Dumps with PDF and VCE Free Updated Today! Following are some new SY0-501 Real Exam Questions!QUESTION 1204A university is opening a facility in a location where there is an elevated risk of theft. The university wants to protect the desktops in its classrooms and labs. Which of the following should the university use to BEST protect these assets deployed in the facility?A. Visitor logsB. Cable locksC. GuardsD. Disk encryptionE. Motion detectionAnswer: BQUESTION 1205Which of the following is the primary reason for implementing layered security measures in a cybersecurity architecture?A. It increases the number of controls required to subvert a systemB. It decreases the time a CERT has to respond to a security incident.C. It alleviates problems associated with EOL equipment replacement.D. It allows for bandwidth upgrades to be made without user disruption.Answer: AQUESTION 1206Which of the following attacks can be used to exploit a vulnerability that was created by untrained users?A. A spear-phishing email with a file attachment.B. A DoS using IoT devicesC. An evil twin wireless access pointD. A domain hijacking of a bank websiteAnswer: AQUESTION 1207A company uses an enterprise desktop imaging solution to manage deployment of its desktop computers. Desktop computer users are only permitted to use software that is part of the baseline image. Which of the following technical solutions was MOST likely deployed by the company to ensure only known-good software can be installed on corporate desktops?A. Network access controlB. Configuration managerC. Application whitelistingD. File integrity checksAnswer: CQUESTION 1208A company recently experienced a security incident in which its domain controllers were the target of a DoS attack. In which of the following steps should technicians connect domain controllers to the network and begin authenticating users again?A. PreparationB. IdentificationC. ContainmentD. EradicationE. RecoveryF. Lessons learnedAnswer: EQUESTION 1209Which of the following explains why a vulnerability scan might return a false positive?A. The scan is performed at a time of day when the vulnerability does not exist.B. The test is performed against the wrong host.C. The signature matches the product but not the version information.D. The hosts are evaluated based on an OS-specific profile.Answer: AQUESTION 1210An organization has implemented a two-step verification process to protect user access to data that is stored in the cloud. Each employee now uses an email address or mobile number to receive a code to access the data. Which of the following authentication methods did the organization implement?A. Token keyB. Static codeC. Push notificationD. HOTPAnswer: DQUESTION 1211Which of the following policies would help an organization identify and mitigate potential single points of failure in the company's IT/security operations?A. Least privilegeB. Awareness trainingC. Separation of dutiesD. Mandatory vacationAnswer: CQUESTION 1212Which of the following may indicate a configuration item has reached end-of-life?A. The device will no longer turn on and indicated an error.B. The vendor has not published security patches recently.C. The object has been removed from the Active Directory.D. Logs show a performance degradation of the component.Answer: BQUESTION 1213Using an ROT13 cipher to protect confidential information for unauthorized access is known as:A. steganography.B. obfuscation.C. non-repudiation.D. diffusion.Answer: BQUESTION 1214A company is implementing a tool to mask all PII when moving data from a production server to a testing server. Which of the following security techniques is the company applying?A. Data wipingB. SteganographyC. Data obfuscationD. Data sanitizationAnswer: CQUESTION 1215A security analyst has received several reports of an issue on an internal web application. Users state they are having to provide their credentials twice to log in. The analyst checks with the application team and notes this is not an expected behavior. After looking at several logs, the analyst decides to run some commands on the gateway and obtains the following output: Which of the following BEST describes the attack the company is experiencing?A. MAC floodingB. URL redirectionC. ARP poisoningD. DNS hijackingAnswer: CQUESTION 1216A technician needs to document which application versions are listening on open ports. Which of the following is MOST likely to return the information the technician needs?A. Banner grabbingB. Steganography toolsC. Protocol analyzerD. Wireless scannerAnswer: AQUESTION 1217A government contracting company issues smartphones to employees to enable access to corporate resources. Several employees will need to travel to a foreign country for business purposes and will require access to their phones. However, the company recently received intelligence that its intellectual property is highly desired by the same country's government. Which of the following MDM configurations would BEST reduce the disk of compromise while on foreign soil?A. Disable firmware OTA updates.B. Disable location services.C. Disable push notification services.D. Disable wipe.Answer: BQUESTION 1218A security analyst is performing a manual audit of captured data from a packet analyzer. The analyst looks for Base64 encoded strings and applies the filter http.authbasic. Which of the following BEST describes what the analyst is looking for?A. Unauthorized softwareB. Unencrypted credentialsC. SSL certificate issuesD. Authentication tokensAnswer: BQUESTION 1219Which of the following impacts are associated with vulnerabilities in embedded systems? (Choose two.)A.

Repeated exploitation due to unpatchable firmwareB. Denial of service due to an integrated legacy operating system.C. Loss of inventory accountability due to device deploymentD. Key reuse and collision issues due to decentralized management.E. Exhaustion of network resources resulting from poor NIC management.Answer: ADQUESTION 1220Given the output: Which of the following account management practices should the security engineer use to mitigate the identified risk?A. Implement least privilegeB. Eliminate shared accounts.C. Eliminate password reuse.D. Implement two-factor authenticationAnswer: BQUESTION 1221An organization wants to separate permissions for individuals who perform system changes from individuals who perform auditing of those system changes. Which of the following access control approaches is BEST suited for this?A. Assign administrators and auditors to different groups and restrict permissions on system log files to read-only for the auditor group. B. Assign administrators and auditors to the same group, but ensure they have different permissions based on the function they perform.C. Create two groups and ensure each group has representation from both the auditors and the administrators so they can verify any changes that were made.D. Assign file and folder permissions on an individual user basis and avoid group assignment altogether.Answer: AQUESTION 1222Which of the following concepts ensure ACL rules on a directory are functioning as expected? (Choose two.)A. AccountingB. AuthenticationC. AuditingD. AuthorizationE. Non-repudiationAnswer: ACQUESTION 1223A datacenter engineer wants to ensure an organization's servers have high speed and high redundancy and can sustain the loss of two physical disks in an array. Which of the following RAID configurations should the engineer implement to deliver this functionality?A. RAID 0B. RAID 1C. RAID 5D. RAID 10E. RAID 50Answer: DQUESTION 1224An organization requires secure configuration baselines for all platforms and technologies that are used. If any system cannot conform to the secure baseline, the organization must process a risk acceptance and receive approval before the system is placed into production. It may have non-conforming systems in its lower environments (development and staging) without risk acceptance, but must receive risk approval before the system is placed in production. Weekly scan reports identify systems that do not conform to any secure baseline.The application team receives a report with the following results:

Host	Environment	Baseline deviation ID
NYAccountingDev	Development	2633 (low), 3124 (high)
NYAccountingStg	Staging	2633 (low), 3124 (high)
NYAccountingProd	Production	2633 (low), 3124 (high)

There are currently no risk acceptances for baseline deviations. This is a mission-critical application, and the organization cannot operate if the application is not running. The application fully functions in the development and staging environments. Which of the following actions should the application team take?A. Remediate 2633 and 3124 immediately.B. Process a risk acceptance for 2633 and 3124.C. Process a risk acceptance for 2633 and remediate 3124.D. Shut down NYAccountingProd and investigate the reason for the different scan results.Answer: CQUESTION 1225A company is having issues with intellectual property being sent to a competitor from its system. The information being sent is not random but has an identifiable pattern. Which of the following should be implemented in the system to stop the content from being sent?A. EncryptionB. HashingC. IPSD. DLPAnswer: DQUESTION 1226A network technician needs to monitor and view the websites that are visited by an employee. The employee is connected to a network switch. Which of the following would allow the technician to monitor the employee's web traffic?A. Implement promiscuous mode on the NIC of the employee's computer.B. Install and configured a transparent proxy server.C. Run a vulnerability scanner to capture DNS packets on the router.D. Configure a VPN to forward packets to the technician's computer.Answer: BQUESTION 1227A security administrator is adding a NAC requirement for all VPN users to ensure the connecting devices are compliant with company policy. Which of the following items provides the HIGHEST assurance to meet this requirement?A. Implement a permanent agent.B. Install antivirus software.C. Use an agentless implementation.D. Implement PKI.Answer: AQUESTION 1228A company wants to configure its wireless network to require username and password authentication. Which of the following should the systems administrator implement?A. WPSB. PEAPC. TKIPD. PKIAnswer: AQUESTION 1229An organization is struggling to differentiate threats from normal traffic and access to systems. A security engineer has been asked to recommend a system that will aggregate data and provide metrics that will assist in identifying malicious actors or other anomalous activity throughout the environment. Which of the following solutions should the engineer recommend?A. Web application firewallB. SIEMC. IPSD. UTME. File integrity monitorAnswer: BQUESTION 1230The concept of connecting a user account across the systems of multiple enterprises is BEST known as:A. federation.B. a remote access policy.C. multifactor authentication.D. single sign-on.Answer: AQUESTION 1231A junior systems administrator noticed that one of two hard drives in a server room had a red error notification. The administrator removed the hard drive to replace it but was unaware that the server was configured in an array. Which of the following configurations would ensure no data is lost?A. RAID 0B. RAID 1C. RAID 2D. RAID 3Answer: BQUESTION 1232Joe, a user at a company, clicked an email link that led to a website that infected his workstation. Joe was connected to the network, and the virus spread to the network shares. The protective

measures failed to stop this virus, and it has continued to evade detection. Which of the following should a security administrator implement to protect the environment from this malware?A. Install a definition-based antivirus.B. Implement an IDS/IPS.C. Implement a heuristic behavior-detection solution.D. Implement CASB to protect the network shares.Answer: BQUESTION 1233 A systems administrator wants to implement a secure wireless network requiring wireless clients to pre- register with the company and install a PKI client certificate prior to being able to connect to the wireless network. Which of the following should the systems administrator configure?A. EAP-TTLSB. EAP-TLSC. EAP-FASTD. EAP with PEAPE. EAP with MSCHAPv2Answer: BQUESTION 1234A systems administrator wants to replace the process of using a CRL to verify certificate validity. Which of the following would BEST suit the administrator's needs?A. OCSPB. CSRC. Key escrowD. CAAnswer: AQUESTION 1235 Which of the following attacks can be mitigated by proper data retention policies?A. Dumpster divingB. Man-in-the-browserC. Spear phishingD. Watering holeAnswer: AResources From:1.2020 Latest Braindump2go SY0-501 Exam Dumps (PDF & VCE) Free Share:https://www.braindump2go.com/sy0-501.html2.2020 Latest Braindump2go SY0-501 PDF and SY0-501 VCE Dumps Free Share:https://drive.google.com/drive/folders/1Mto9aYkbmrvlHB5IFqCx-MuIqEVJQ9Yu?usp=sharing3.2020 Free Braindump2go SY0-501 PDF Download:https://www.braindump2go.com/free-online-pdf/SY0-501-PDF-Dumps(1204-1214).pdf https://www.braindump2go.com/free-online-pdf/SY0-501-VCE-Dumps(1215-1235).pdfFree Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!