This page was exported from - New Braindump2go Exam Dumps
Export date: Thu Feb 13 1:56:04 2025 / +0000 GMT

[2018-NEW-ExamsBraindump2go Valid SY0-501 VCE Dumps for 100% Passing Exam SY0-501[Q1-Q11

2018 New CompTIA SY0-501 Exam Dumps with PDF and VCE Free Updated Today! Following are some new SY0-501 Exam Questions:1.2018 New SY0-501 Exam Dumps (PDF and VCE)Share:https://www.braindump2go.com/sy0-501.html2.2018 New SY0-501 Exam Questions & Answers:
https://drive.google.com/drive/folders/1QYBwvoau8PlTQ3bugQuy0pES-zrLrRB1?usp=sharingQUESTION 111Anne, the Chief Executive Officer (CEO), has reported that she is getting multiple telephone calls from someone claiming to be from the helpdesk. The caller is asking to verify her network authentication credentials because her computer is broadcasting across the network. This is MOST likely which of the following types of attacks?A. VishingB. ImpersonationC. SpimD. ScarewareAnswer: AQUESTION 112An administrator discovers the following log entry on a server:Nov 12 2013 00:23:45 httpd[2342]: GET/app2/prod/proc/process.php?input=change;cd%20../../../etc;cat%20shadowWhich of the following attacks is being attempted?A. Command injectionB. Password attackC. Buffer overflowD. Cross-site scriptingAnswer: BQUESTION 113A security team wants to establish an Incident Response plan. The team has never experienced an incident. Which of the following would BEST help them establish plans and procedures?A. Table top exercisesB. Lessons learnedC. Escalation proceduresD. Recovery proceduresAnswer: DQUESTION 114Which of the following would verify that a threat does exist and security controls can easily be bypassed without actively testing an application?A. Protocol analyzerB. Vulnerability scanC. Penetration testD. Port scannerAnswer: BExplanation:A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.QUESTION 1A high-security defense installation recently began utilizing large guard dogs that bark very loudly and excitedly at the slightest provocation.Which of the following types of controls does this BEST describe?A. DeterrentB. PreventiveC. DetectiveD. CompensatingAnswer: AQUESTION 2 An incident responder receives a call from a user who reports a computer is exhibiting symptoms consistent with a malware infection. Which of the following steps should the responder perform NEXT?A. Capture and document necessary information to assist in the response.B. Request the user capture and provide a screenshot or recording of the symptomsC. Use a remote desktop client to collect and analyze the malware m real timeD. Ask the user to back up files for later recoveryAnswer: CQUESTION 3 Multiple organizations operating in the same vertical want to provide seamless wireless access for their employees as they visit the other organizations. Which of the following should be implemented if all the organizations use the native 802.1x client on their mobile devices?A. ShibbolethB. RADIUS federationC. SAMLD. OAuthE. OpenlD connectAnswer: BQUESTION 4An analyst wants to implement a more secure wifeless authentication for office access points. Which of the following technologies allows for encrypted authentication of wireless clients over TLS?A. PEAPB. EAPC. WPA2D. RADIUSAnswer: CQUESTION 5A security analyst is hardening an authentication server. One of the primary requirements is to ensure there is mutual authentication and delegation. Given these requirements, which of the following technologies should the analyst recommend and configure?A. LDAP servicesB. Kerberos servicesC. NTLM servicesD. CHAP servicesAnswer: CQUESTION 6An organization wishes to provide better security for its name resolution services.Which of the following technologies BEST supports the deployment DNSSEC at the organization?A. LDAPB. TPMC. TLSD. SSLE. PWAnswer: CQUESTION 7Ann, an employee in the payroll department, has contacted the help desk citing multiple issues with her device, including: Slow performance Word documents, PDFs, and images no longer opening A pop-upAnn states the issues began after she opened an invoice that a vendor emailed to her.Upon opening the invoice, she had to click several security warnings to view it in her word processor. With which of the following is the device MOST likely infected?A. SpywareB. Crypto-malwareC. RootkitD. BackdoorAnswer: DQUESTION 8A department head at a university resigned on the first day of the spring semester. It was subsequently determined that the department head deleted numerous files and directories from the server-based home directory while the campus was closed. Which of the following policies or procedures co have prevented this from occurring?A. Time-of-day restrictionsB. Permission auditing and reviewC. OffboardingD. Account expirationAnswer: dQUESTION 9A company is using a mobile device deployment model in which employees use their personal devices for work at their own discretion. Some of the problems the

company is encountering include the following:* There is no standardization.* Employees ask for reimbursement for their devices.* Employees do not replace their devices often enough to keep them running efficiently.* The company does not have enough control over the devices.Which of the following is a deployment model that would help the company overcome these problems?A. BYOD B. VDIC. COPED. CYODAnswer: DQUESTION 10A security administrator is developing controls for creating audit trails and tracking if a PHI data breach is to occur. The administrator has been given the following requirements:* All access must be correlated to a user account.* All user accounts must be assigned to a single individual.* User access to the PHI data must be recorded.* Anomalies in PHI data access must be reported.* Logs and records cannot be deleted or modified.Which of the following should the administrator implement to meet the above requirements? (Select THREE).A. Eliminate shared accounts.B. Create a standard naming convention for accounts.C. Implement usage auditing and review.D. Enable account lockout thresholds.E. Copy logs in real time to a secured WORM drive.F. Implement time-of-day restrictions.G. Perform regular permission audits and reviews.Answer: ACGQUESTION 11Which of the following can be provided to an AAA system for the identification phase?A. UsernameB. PermissionsC. One-time tokenD. Private certificateAnswer: A!!!RECOMMEND!!!1.2018 New SY0-501 Exam Dumps (PDF and VCE)Share:https://www.braindump2go.com/sy0-501.html**2.2018 New SY0-501 Study Guide Video:** YouTube Video: YouTube.com/watch?v=iqQ_uBVOfZw