[2018-3-19 Lead2pass 100% Valid SY0-501 Exam Questions PDF Free Download (201-210)

Free Share SY0-501 PDF Dumps With Lead2pass Updated Exam Questions.v.2018-3-19.250q: https://www.lead2pass.com/sy0-501.html QUESTION 201Which of the following must be intact for evidence to be admissible in court? A. Chain of custodyB. Order of violationC. Legal holdD. PreservationAnswer: A QUESTION 202A vulnerability scanner that uses its running service's access level to better assess vulnerabilities across multiple assets within an organization is performing a: A. Credentialed scan.B. Non-intrusive scan.C. Privilege escalation test.D. Passive scan. Answer: A QUESTION 203Which of the following cryptography algorithms will produce a fixed-length, irreversible output? A. AESB. 3DESC. RSAD. MD5 Answer: D QUESTION 204A technician suspects that a system has been compromised. The technician reviews the following log entry: WARNING- hash mismatch: C:WindowSysWOW64user32.dllWARNING- hash mismatch: C:WindowSysWOW64kernel32.dll Based solely ono the above information, which of the following types of malware is MOST likely installed on the system? A. RootkitB. RansomwareC. TrojanD. Backdoor Answer: A QUESTION 205A new firewall has been places into service at an organization. However, a configuration has not been entered on the firewall. Employees on the network segment covered by the new firewall report they are unable to access the network. Which of the following steps should be completed to BEST resolve the issue? A. The firewall should be configured to prevent user traffic form matching the implicit deny rule.B. The firewall should be configured with access lists to allow inbound and outbound traffic.C. The firewall should be configured with port security to allow traffic.D. The firewall should be configured to include an explicit deny rule. Answer: A QUESTION 206A security analyst is testing both Windows and Linux systems for unauthorized DNS zone transfers within a LAN on comptia.org from example.org. Which of the following commands should the security analyst use? (Select two.) A. nslookupcomptia.orgset type=ANYls-d example.orgB. nslookupcomptia.orgset type=MXexample.orgC. dig -axfr comptia.org@example.orgD. ipconfig/flushDNSE. ifconfig eth0 downifconfig eth0 updhclient renewF. dig@example.org comptia.org Answer: AC QUESTION 207Which of the following are the MAIN reasons why a systems administrator would install security patches in a staging environment before the patches are applied to the production server? (Select two.) A. To prevent server availability issuesB. To verify the appropriate patch is being installedC. To generate a new baseline hash after patchingD. To allow users to test functionalityE. To ensure users are trained on new functionality Answer: AD QUESTION 208A Chief Information Officer (CIO) drafts an agreement between the organization and its employees. The agreement outlines ramifications for releasing information without consent and/for approvals. Which of the following BEST describes this type of agreement? A. ISAB. NDAC. MOUD. SLA Answer: B QUESTION 209Which of the following would meet the requirements for multifactor authentication? A. Username, PIN, and employee ID numberB. Fingerprint and passwordC. Smart card and hardware tokenD. Voice recognition and retina scan Answer: B QUESTION 210A manager suspects that an IT employee with elevated database access may be knowingly modifying financial transactions for the benefit of a competitor. Which of the following practices should the manager implement to validate the concern? A. Separation of dutiesB. Mandatory vacationsC. Background checksD. Security awareness training Answer: A **SY0-501 dumps full version (PDF&VCE):** https://www.lead2pass.com/sy0-501.html **Large amount of free SY0-501 exam questions on Google Drive:** https://drive.google.com/open?id=1Hm6GQHDVOsEnyhNf3EHqIGEtor5IUsfu] You may also need: SY0-401 exam dumps: https://drive.google.com/open?id=0B3Syig5i8gpDLXZsWm9MWmh0a0E