[June-2018-NewBraindump2go SY0-501 Exam VCE and PDF Dumps 563Q for 100% Passing SY0-501 Exam[330-340

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=sharingQUESTION 330A security analyst has received the following alert snippet from the HIDS appliance: Given the above logs, which of the following is the cause of the attack?A. The TCP ports on destination are all openB. FIN, URG, and PSH flags are set in the packet headerC. TCP MSS is configured improperlyD. There is improper Layer 2 segmentation**Answer: B**QUESTION 331A security analyst reviews the following output: The analyst loads the hash into the SIEM to discover if this hash is seen in other parts of the network. After inspecting a large number of files, the security analyst reports the following: Which of the following is the MOST likely cause of the hash being found in other areas?A. Jan Smith is an insider threatB. There are MD5 hash collisionsC. The file is encryptedD. Shadow copies are present**Answer: B**QUESTION 332A company's AUP requires:- Passwords must meet complexity requirements.- Passwords are changed at least once every six months.- Passwords must be at least eight characters long.An auditor is reviewing the following report: Which of the following controls should the auditor recommend to enforce the AUP?A. Account lockout thresholdsB. Account recoveryC. Password expirationD. Prohibit password reuse**Answer: C**QUESTION 333An organization's primary datacenter is experiencing a two-day outage due to an HVAC malfunction. The node located in the datacenter has lost power and is no longer operational, impacting the ability of all users to connect to the alternate datacenter. Which of the following BIA concepts BEST represents the risk described in this scenario?A. SPoFB. RTOC. MTBFD. MTTR**Answer: A** QUESTION 334A security analyst notices anomalous activity coming from several workstations in the organizations. Upon identifying and containing the issue, which of the following should the security analyst do NEXT?A. Document and lock the workstations in a secure area to establish chain of custodyB. Notify the IT department that the workstations are to be reimaged and the data restored for reuseC. Notify the IT department that the workstations may be reconnected to the network for the users to continue workingD. Document findings and processes in the after-action and lessons learned report**Answer: D**QUESTION 335An employee receives an email, which appears to be from the Chief Executive Officer (CEO), asking for a report of security credentials for all users.Which of the following types of attack is MOST likely occurring?A. Policy violationB. Social engineeringC. WhalingD. Spear phishing**Answer: D**QUESTION 336An information security analyst needs to work with an employee who can answer questions about how data for a specific system is used in the business. The analyst should seek out an employee who has the role of:A. stewardB. ownerC. privacy officerD. systems administrator**Answer: B**QUESTION 337A group of non-profit agencies wants to implement a cloud service to share resources with each other and minimize costs. Which of the following cloud deployment models BEST describes this type of effort?A. PublicB. HybridC. CommunityD. Private**Answer: C**QUESTION 338A director of IR is reviewing a report regarding several recent breaches. The director complies the following statistics:- Initial IR engagement time frame- Length of time before an executive management notice went out- Average IR phase completionThe director wants to use data to shorten the response time. Which of the following would accomplish this?A. CSIRTB. Containment phaseC. Escalation notificationsD. Tabletop exercise**Answer: D**QUESTION 339A copy of a highly confidential salary report was recently found on a printer in the IT department. The human resources department does not have this specific printer mapped to its devices, and it is suspected that an employee in the IT department browsed to the share where the report was located and printed it without authorization. Which of the following technical controls would be the BEST choice to immediately prevent this from happening again?A. Implement a DLP solution and classify the report as confidential, restricting access only to human resources staffB. Restrict access to the share where the report resides to only human resources employees and enable auditingC. Have all members of the IT department review and sign the AUP and disciplinary policiesD. Place the human resources computers on a restricted VLAN and configure the ACL to prevent access from the IT department**Answer: B**QUESTION 340A company is developing a new system that will unlock a computer automatically when an authorized user sits in front of it, and then lock the computer when the user leaves. The user does not have to perform any action for this process to occur. Which of the following technologies provides this capability?A. Facial recognitionB. Fingerprint scannerC. Motion detectorD. Smart cards**Answer: A**!!!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