[June-2022Real SY0-601 Exam PDF and VCE Free Download from Braindump2go[Q656-Q671

June/2022 Latest Braindump2go SY0-601 Exam Dumps with PDF and VCE Free Updated Today! Following are some new Braindump2go SY0-601 Real Exam Questions!QUESTION 656A DBA reports that several production server hard drives were wipes over the weekend. The DBA also reports that several Linux servers were unavailable due to system files being deleted unexpectedly. A security analyst verified that software was configured to delete data deliberately from those servers. No backdoors to any servers were found. Which of the following attacks was MOST likely used to cause the data loss?A. Logic BombB. RansomwareC. Fileless virusD. Remote access TrojansE. RootkitAnswer: AQUESTION 657Digital signatures use asymmetric encryption. This means the message is encrypted with:A. the senders private key and decrypted with the senders' public keyB. the senders public key and decrypted with the senders' private keyC. the senders private key and decrypted with the recipient's public keyD. the senders public key and decrypted with the recipient's private keyAnswer: AQUESTION 658A help desk technician receives a phone call from someone claiming to be a part of the organizations cybersecurity incident response team. The caller asks the technician to verify networks internal firewall IP address. Which of the following is the technicians BEST course of action?A. direct the caller to stop by the help desk in person and hang up declining any further requests from the caller.B. ask for the callers name, verify the persons identity in the email directory, and provide the requested information over the phone.C. write down the phone number of the caller if possible, the name of the person requesting the information. Hang-up, and notify the organizations cybersecurity officerD. request the caller send an email for identity verification and provide the requested information via email to the caller.Answer: CQUESTION 659An employee received a word processing file that was delivered as an email attachment. The subject line and email content enticed the employee to open the attachment.Which of the following attack vectors BEST matches this malware?A. embedded Python codeB. Macro-enabled fileC. Bash scriptingD. Credential-harvesting websiteAnswer: BQUESTION 660Which of the following is the BEST example of a cost-effective physical control to enforce a USB removable media retention policy?A. putting security/antitamper tape over USB ports. Keylogging the port numbers and regularly inspecting the ports.B. implementing a GPO that will restrict access to authorized USB removable media and regularly verifying that it is enforcedC. placing systems into locked key-controlled containers with no access to the USB ports.D. installing an endpoint agent to detect connectivity of USB and removable mediaAnswer: BQUESTION 661The SOC for a large MSSP in a meeting to discuss the lessons learned from a recent incident that took much too long to resolve. This type of incident has become more common over weeks and is consuming large amounts of the analysts time due to manual tasks being performed. Which of the following solutions should the SOC consider to BEST improve its response time?A. configure a NIDS appliance using a Switched Port AnalyzerB. collect OSINT and catalog the artifacts in a central repositoryC. implement a SOAR with customizable playbooksD. install a SIEM with community-driven threat intelligenceAnswer: CQUESTION 662A security analyst is investigating suspicious traffic on the web server located at IP address 10.10.1.1. a search of the WAF logs reveals the following output:172.16.1.3/ 10.10.1.1/ web/ permit and logA. XSS attackB. SQLi attackC. Replay attackD. XSRF attackAnswer: AQUESTION 663Which of the following is an example of transference of risk?A. purchasing insuranceB. patching vulnerable serversC. retiring outdated applicationsD. Application owner risk sign-offAnswer: AQUESTION 664A security engineer was assigned to implement a solution to prevent attackers from gaining access by pretending to be authorized users. Which of the following technologies meets the requirement?A. SSOB. IDSC. MFAD. TPMAnswer: CQUESTION 665A tax organization is working on a solution to validate the online submission of documents. The solution should be carried on a portable USB device that should be inserted on any computer that is transmitting a transaction securely. Which of the following is the BEST certificate for these requirements?A. user certificateB. self-signed certificateC. computer certificateD. root certificateAnswer: CQUESTION 666During a trial, a judge determined evidence gathered from a hard drive was not admissible. Which of the following BEST explains this reasoning?A. the forensic investigator forgot to run a checksum on the disk image after creationB. the chain of custody form did not note time zone offsets between transportation regionsC. the computer was turned off, and a RAM image could not be taken at the same timeD. the hard drive was not properly kept in an antistatic bag when it was moved.Answer: DQUESTION 667A security analyst needs to be able to search and correlate logs from multiple sources in a single tool. Which of the following would BEST allow a security analyst to have this ability?A. SOARB. SIEMC. Log collectorsD. Network-attached storageAnswer: CQUESTION 668The chief information security officer (CISO) has requested that a third-party vendor provide supporting documents that show proper controls are in place to protect customer data which of the following would be BEST for the third-party vendor to provide the CISO?A. GDPR compliance attestationB. cloud security alliance materialsC. SOC 2 type 2 reportD. NIST RMP workbooksAnswer: CQUESTION 669A company labeled some documents with the public

sensitivity classification. This means the documents can be accessed by:A. employees of other companies and the pressB. all members of the department that created the documentsC. only the company's employees and those listed in the documentD. only the individuals listed in the documentsAnswer: CQUESTION 670Which of the following explains why RTO is included in a BIA?A. it identifies the amount of allowable downtime for an application or systemB. it prioritizes risks so the organization can allocate resources appropriately.C. it monetizes the loss of an asset and determines a break even point for risk mitigationD. it informs the backup approach so that the organization can recover data to a known timeAnswer: CQUESTION 671A security analyst is receiving numerous alerts reporting that the response time of an internet-facing application has been degraded. However, the internal network performance has degraded. Which of the following MOST likely explains this behavior?A. DNS poisoningB. MAC floodingC. DDoS attackD. ARP poisoningAnswer: CResources From:1.2022 Latest Braindump2go SY0-601 Exam Dumps (PDF & VCE) Free Share:https://www.braindump2go.com/sy0-601.html2.2022 Latest Braindump2go SY0-601 PDF and SY0-601 VCE Dumps Free Share:
https://drive.google.com/drive/folders/1VvH3gDuiIKHw7Kx_vZmMM4mpCRWbTVq4?usp=sharing3.2021 Free Braindump2go SY0-601 Exam Questions Download:https://www.braindump2go.com/free-online-pdf/SY0-601-PDF-Dumps(656-671).pdfFree Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!