[Updated CAS-003 DumpsInstant Download Braindump2go CAS-003 PDF Dumps and CAS-003 VCE Dumps 242Q[Q328-Q341

2018-10-26 Braindump2go CAS-003 Exam Dumps with PDF and VCE New Updated Today! Following are some new CAS-003 Real Exam Questions:1.|2018 Latest CAS-003 Exam Dumps (PDF & VCE) 368Q&As Download:https://www.braindump2go.com/cas-003.html2.|2018 Latest CAS-003 Exam Questions & Answers Download: **https://drive.google.com/drive/folders/11eVcvdRTGUBlESzBX9a6YlPUYiZ4xoHE?usp=sharing**QUESTION 328Given the following output from a security tool in Kali:

```
[12:17:41] dumping options:

filename: </usr/share/sectools/scans>
state: <8>
lineo: <56>
literals: <74>
sequences: [3]
symbols: [0]
req_del: <200>
mseq_len: <1024>
plugin: <none>
s_syms: <0>
literal [1] = [jf2d43kaj4i9eahfh8fbiud8sd8sdhfdfhj9]
```


A. Log reductionB. Network enumeratorC. FuzzerD. SCAP scanner**Answer: D**QUESTION 329Due to a recent breach, the Chief Executive Officer (CEO) has requested the following activities be conducted during incident response planning:- Involve business owners and stakeholders- Create an applicable scenario- Conduct a biannual verbal review of the incident response plan- Report on the lessons learned and gaps identifiedWhich of the following exercises has the CEO requested?A. Parallel operationsB. Full transitionC. Internal reviewD. TabletopE. Partial simulation**Answer: C**QUESTION 330A government organization operates and maintains several ICS environments. The categorization of one of the ICS environments led to a moderate baseline. The organization has complied a set of applicable security controls based on this categorization.Given that this is a unique environment, which of the following should the organization do NEXT to determine if other security controls should be considered?A. Check for any relevant or required overlays.B. Review enhancements within the current control set.C. Modify to a high-baseline set of controls.D. Perform continuous monitoring.**Answer: C**QUESTION 331A security researches is gathering information about a recent spoke in the number of targeted attacks against multinational banks. The spike is on top of already sustained attacks against the banks. Some of the previous attacks have resulted in the loss of sensitive data, but as of yet the attackers have not successfully stolen any funds.Based on the information available to the researcher, which of the following is the MOST likely threat profile?A. Nation-state-sponsored attackers conducting espionage for strategic gain.B. Insiders seeking to gain access to funds for illicit purposes.C. Opportunists seeking notoriety and fame for personal gain.D. Hackvisits seeking to make a political statement because of socio-economic factors.**Answer: D**QUESTION 332A security analyst is inspecting pseudocode of the following multithreaded application:1. perform daily ETL of data1.1 validate that yesterday's data model file exists1.2 validate that today's data model file does not exist 1.2 extract yesterday's data model1.3 transform the format1.4 load the transformed data into today's data model file 1.5 exitWhich of the following security concerns is evident in the above pseudocode?A. Time of check/time of useB. Resource exhaustionC. Improper storage of sensitive dataD. Privilege escalation**Answer: A**QUESTION 333An organization is considering the use of a thin client architecture as it moves to a cloud-hosted environment. A security analyst

is asked to provide thoughts on the security advantages of using thin clients and virtual workstations.Which of the following are security advantages of the use of this combination of thin clients and virtual workstations?A. Malicious insiders will not have the opportunity to tamper with data at rest and affect the integrity of the system.B. Thin client workstations require much less security because they lack storage and peripherals that can be easily compromised, and the virtual workstations are protected in the cloud where security is outsourced.C. All thin clients use TPM for core protection, and virtual workstations use vTPM for core protection with both equally ensuring a greater security advantage for a cloud-hosted environment.D. Malicious users will have reduced opportunities for data extractions from their physical thin client workstations, this reducing the effectiveness of local attacks.**Answer: B**QUESTION 334A security analyst is attempting to break into a client's secure network. The analyst was not given prior information about the client, except for a block of public IP addresses that are currently in use.After network enumeration, the analyst's NEXT step is to perform:A. a gray-box penetration testB. a risk analysisC. a vulnerability assessmentD. an external security auditE. a red team exercise**Answer: A**QUESTION 335A security architect is determining the best solution for a new project. The project is developing a new intranet with advanced authentication capabilities, SSO for users, and automated provisioning to streamline Day 1 access to systems. The security architect has identified the following requirements:1. Information should be sourced from the trusted master data source.2. There must be future requirements for identity proofing of devices and users.3. A generic identity connector that can be reused must be developed.4. The current project scope is for internally hosted applications only.Which of the following solution building blocks should the security architect use to BEST meet the requirements?A. LDAP, multifactor authentication, oAuth, XACMLB. AD, certificate-based authentication, Kerberos, SPMLC. SAML, context-aware authentication, oAuth, WAYFD. NAC, radius, 802.1x, centralized active directory**Answer: A**QUESTION 336Which of the following is an external pressure that causes companies to hire security assessors and penetration testers?A. Lack of adequate in-house testing skills.B. Requirements for geographically based assessmentsC. Cost reduction measuresD. Regulatory insistence on independent reviews.**Answer: D**QUESTION 337Engineers at a company believe a certain type of data should be protected from competitors, but the data owner insists the information is not sensitive. An information security engineer is implementing controls to secure the corporate SAN. The controls require dividing data into four groups: non-sensitive, sensitive but accessible, sensitive but export-controlled, and extremely sensitive.Which of the following actions should the engineer take regarding the data?A. Label the data as extremely sensitive.B. Label the data as sensitive but accessible.C. Label the data as non-sensitive.D. Label the data as sensitive but export-controlled.**Answer: C**QUESTION 338A security engineer is performing an assessment again for a company. The security engineer examines the following output from the review:Which of the following tools is the engineer utilizing to perform this assessment?

A. Vulnerability scannerB. SCAP scannerC. Port scannerD. Interception proxy**Answer: B**QUESTION 339The marketing department has developed a new marketing campaign involving significant social media outreach. The campaign includes allowing employees and customers to submit blog posts and pictures of their day-to-day experiences at the company. The information security manager has been asked to provide an informative letter to all participants regarding the security risks and how to avoid privacy and operational security issues.Which of the following is the MOST important information to reference in the letter?A. After-action reports from prior incidents.B. Social engineering techniquesC. Company policies and employee NDAsD. Data classification processes**Answer: C**QUESTION 340A database administrator is required to adhere to and implement privacy principles when executing daily tasks. A manager directs the administrator to reduce the number of unique instances of PII stored within an organization's systems to the greatest extent possible.Which of the following principles is being demonstrated?A. Administrator accountabilityB. PII securityC. Record transparencyD. Data minimization**Answer: D**QUESTION 341A newly hired security analyst has joined an established SOC team. Not long after going through corporate orientation, a new attack method on web-based applications was publicly revealed. The security analyst immediately brings this new information to the team lead, but the team lead is not concerned about it.Which of the following is the MOST likely reason for the team lead's position?A. The organization has accepted the risks associated with web-based threats.B. The attack type does not meet the organization's threat model.C. Web-based applications are on isolated network segments.D. Corporate policy states that NIPS signatures must be updated every hour.**Answer: A**!!!RECOMMEND!!!1.|2018 Latest CAS-003 Exam Dumps (PDF & VCE) 368Q&As Download:https://www.braindump2go.com/cas-003.html2.|2018 Latest CAS-003 Study Guide Video: YouTube Video: YouTube.com/watch?v=_ZKiZ45b-b8