

[Updated CAS-003 Dumps] 100% Real CAS-003 Exam PDF Free Download in Braindump2go [Q317-Q327]

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.html> 2. | 2018 Latest CAS-003 Exam Questions & Answers Download:

<https://drive.google.com/drive/folders/11eVcvdRTGUBIESzBX9a6YIPUYiZ4xoHE?usp=sharing> QUESTION 317 An

organization enables BYOD but wants to allow users to access the corporate email, calendar, and contacts from their devices. The data associated with the user's accounts is sensitive, and therefore, the organization wants to comply with the following

requirements: Active full-device encryption Enabled remote-device wipe Blocking unsigned applications Containerization of email,

calendar, and contacts Which of the following technical controls would BEST protect the data from attack or loss and meet the above requirements? A. Require frequent password changes and disable NFC. B. Enforce device encryption and activate MAM. C.

Install a mobile antivirus application. D. Configure and monitor devices with an MDM. **Answer: B** QUESTION 318 Given the

following information about a company's internal network: User IP space: 192.168.1.0/24 Server IP space: 192.168.192.0/25 A

security engineer has been told that there are rogue websites hosted outside of the proper server space, and those websites need to be identified. Which of the following should the engineer do? A. Use a protocol analyzer on 192.168.1.0/24 B. Use a port scanner on

192.168.1.0/24 C. Use an HTTP interceptor on 192.168.1.0/24 D. Use a port scanner on 192.168.192.0/25 E. Use a protocol

analyzer on 192.168.192.0/25 F. Use an HTTP interceptor on 192.168.192.0/25 **Answer: B** QUESTION 319 The Chief Information

Officer (CIO) wants to increase security and accessibility among the organization's cloud SaaS applications. The applications are configured to use passwords, and two-factor authentication is not provided natively. Which of the following would BEST address the

CIO's concerns? A. Procure a password manager for the employees to use with the cloud applications. B. Create a VPN tunnel

between the on-premises environment and the cloud providers. C. Deploy applications internally and migrate away from SaaS

applications. D. Implement an IdP that supports SAML and time-based, one-time passwords. **Answer: B** QUESTION 320 During a

security assessment, activities were divided into two phases; internal and external exploitation. The security assessment team set a

hard time limit on external activities before moving to a compromised box within the enterprise perimeter. Which of the following

methods is the assessment team most likely to employ NEXT? A. Pivoting from the compromised, moving laterally through the

enterprise, and trying to exfiltrate data and compromise devices. B. Conducting a social engineering attack attempt with the goal of accessing the compromised box physically. C. Exfiltrating network scans from the compromised box as a precursor to social media

reconnaissance D. Open-source intelligence gathering to identify the network perimeter and scope to enable further system

compromises. **Answer: A** QUESTION 321 An organization's network engineering team recently deployed a new software encryption

solution to ensure the confidentiality of data at rest, which was found to add 300ms of latency to data read-write requests in storage, impacting business operations. Which of the following alternative approaches would BEST address performance requirements while

meeting the intended security objective? A. Employ hardware FDE or SED solutions. B. Utilize a more efficient cryptographic

hash function. C. Replace HDDs with SSD arrays. D. Use a FIFO pipe a multithreaded software solution. **Answer: A** QUESTION

322 While attending a meeting with the human resources department, an organization's information security officer sees an employee

using a username and password written on a memo pad to log into a specific service. When the information security officer inquires

further as to why passwords are being written down, the response is that there are too many passwords to remember for all the

different services the human resources department is required to use. Additionally, each password has specific complexity

requirements and different expiration time frames. Which of the following would be the BEST solution for the information security

officer to recommend? A. Utilizing MFAB. B. Implementing SSOC. C. Deploying 802.1XD. D. Pushing SAML adoption E.

Implementing TACACS **Answer: B** QUESTION 323 Which of the following is the GREATEST security concern with respect to

BYOD? A. The filtering of sensitive data out of data flows at geographic boundaries. B. Removing potential bottlenecks in data

transmission paths. C. The transfer of corporate data onto mobile corporate devices. D. The migration of data into and out of the

network in an uncontrolled manner. **Answer: D** QUESTION 324 Given the following code snippet:

```
SecCond = "1SS"
SecStatus = false
try (
    if (SecStatus)
        SecCond = "2SS"
        console.log("ship to ship")
    else
        console.log("nothing to see here")
} catch (e) {
    SecCond = "normal operations"
    console.log(e)
    console.log("Exception logged")
}
```

Which of the following failure modes would the code exhibit? A. Open B. Secure C. Halt D. Exception **Answer: D** QUESTION 325 A medical facility wants to purchase mobile devices for doctors and nurses. To ensure accountability, each individual will be assigned a separate mobile device. Additionally, to protect patients' health information, management has identified the following requirements:- Data must be encrypted at rest.- The device must be disabled if it leaves the facility.- The device must be disabled when tampered with. Which of the following technologies would BEST support these requirements? (Select two.) A. eFuse B. NFCC. GPSD. Biometric E. USB 4.1 F. MicroSD **Answer: CD** QUESTION 326 A security administrator wants to implement two-factor authentication for network switches and routers. The solution should integrate with the company's RADIUS server, which is used for authentication to the network infrastructure devices. The security administrator implements the following:- An HOTP service is installed on the RADIUS server.- The RADIUS server is configured to require the HOTP service for authentication. The configuration is successfully tested using a software supplicant and enforced across all network devices. Network administrators report they are unable to log onto the network devices because they are not being prompted for the second factor. Which of the following should be implemented to BEST resolve the issue? A. Replace the password requirement with the second factor. Network administrators will enter their username and then enter the token in place of their password in the password field. B. Configure the RADIUS server to accept the second factor appended to the password. Network administrators will enter a password followed by their token in the password field. C. Reconfigure network devices to prompt for username, password, and a token. Network administrators will enter their username and password, and then they will enter the token. D. Install a TOTP service on the RADIUS server in addition to the HOTP service. Use the HOTP on older devices that do not support two-factor authentication. Network administrators will use a web portal to log onto these devices. **Answer: B** QUESTION 327 Following a merger, the number of remote sites for a company has doubled to 52. The company has decided to secure each remote site with an NGFW to provide web filtering, NIDS/NIPS, and network antivirus. The Chief Information Officer (CIO) has requested that the security engineer provide recommendations on sizing for the firewall with the requirements that it be easy to manage and provide capacity for growth. The tables below provide information on a subset of remote sites and the firewall options:

Location	# of Users	Connectivity	Bandwidth
St. Louis	18	50 Mbps	20 Mbps
De Moines	12	25 Mbps	10 Mbps
Chicago	27	100 Mbps	41 Mbps
Rapid City	6	10 Mbps	8 Mbps
Indianapolis	7	12 Mbps	8 Mbps

Vendor	Maximum Recommended Devices	Firewall Throughput	Full UTM?	Centralized Management Available?
A	40	400 Mbps	Y	Y
B	60	400 Mbps	N	Y
C	25	200 Mbps	N	N
D	25	100 Mbps	Y	Y

Which of the following would be the BEST option to recommend to the CIO? A. Vendor C for small remote sites, and Vendor B for large sites. B. Vendor B for all remote sites C. Vendor C for all remote sites D. Vendor A for all remote sites E. Vendor D for all remote sites **Answer: D!!!RECOMMEND!!!**1. |2018 Latest CAS-003 Exam Dumps (PDF & VCE) 368Q&As
Download: <https://www.braindump2go.com/cas-003.html> 2. |2018 Latest CAS-003 Study Guide Video: YouTube Video:
[YouTube.com/watch?v= ZKiZ45b-b8](https://www.youtube.com/watch?v=ZKiZ45b-b8)