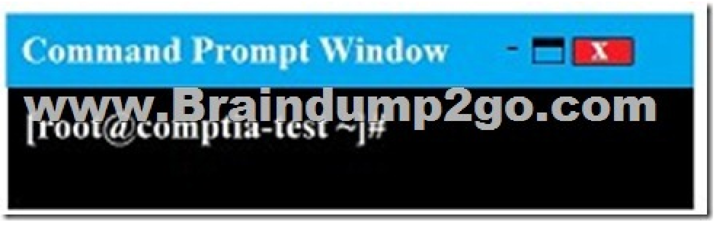
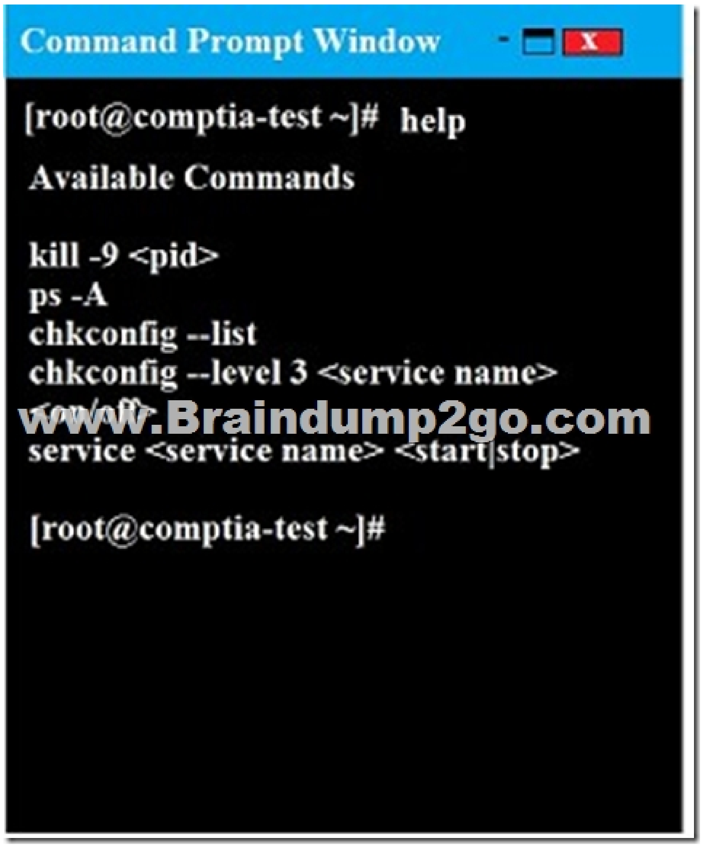
[Updated CAS-003 DumpsDownload Braindump2go CAS-003 Brain Dumps VCE for Free[Q306-Q316

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 306Legal counsel has notified the information security manager of a legal matter that will require the preservation of electronic records for 2000 sales force employees. Source records will be email, PC, network shares, and applications.After all restrictions have been lifted, which of the following should the information manager review?A.   Data retention policyB.   Legal holdC.   Chain of custodyD.   Scope statement**Answer: B**QUESTION 307SIMULATIONAs a security administrator, you are asked to harden a server running Red Hat Enterprise Server 5.5 64- bit.This server is being used as a DNS and time server. It is not used as a database, web server, or print server. There are no wireless connections to the server, and it does not need to print. The command window will be provided along with root access. You are connected via a secure shell with root access.You may query help for a list of commands.Instructions:You need to disable and turn off unrelated services and processes. It is possible to simulate a crash of your server session. The simulation can be reset, but the server cannot be rebooted. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



```
[root@comptia-test ~]#
```



```
[root@comptia-test ~]#  help
 Available Commands

 kill -9 <pid>
 ps -A
 chkconfig --list
 chkconfig --level 3 <service name>
 <on/off>
 service <service name> <start|stop>

 [root@comptia-test ~]#
```

As a security administrator, you are asked to harden a server running Red Hat Enterprise Server 5.5 64-bit. This server is being used as a DNS and time server. It is not used as a database, web server, or print server. There are no wireless connections to the server, and it does not need to print. The command window will be provided along with root access. You are connected via a secure shell with root access. You may query help for a list of commands. Instructions: You need to disable and turn off unrelated services and processes. It is possible to simulate a crash of your server session. The simulation can be reset, but the server cannot be rebooted. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button. Answer: In Order to deactivate web services, database services and print service, we can do following things1) deactivate its services/etc/init.d/apache2 stop/etc/init.d/mysqld stop2) close ports for these servicesWeb Serveriptables -I INPUT -p tcp -m tcp --dport 443 -j REJECTservice iptables savePrint Serveriptables -I INPUT -p tcp -m tcp --dport 631 -j REJECTservice iptables saveDatabase Serveriptables -I INPUT -p tcp -m tcp --dport <<port umber>> -j REJECTservice iptables save3) Kill the process any running for the sameps -aef|grep mysqlkill -9 <<process id>>QUESTION 308The legal department has required that all traffic to and from a company's cloud-based word processing and email system is logged. To meet this requirement, the Chief Information Security Officer (CISO) has implemented a next-generation firewall to perform inspection of the secure traffic and has decided to use a cloud-based log aggregation solution for all traffic that is logged.Which of the following presents a long-term risk to user privacy in this scenario?A. Confidential or sensitive documents are inspected by the firewall before being logged.B. Latency when viewing videos and other online content may increase.C. Reports generated from the firewall will take longer to produce due to more information from inspected traffic.D. Stored logs may contain non-encrypted usernames and passwords for personal websites.**Answer: A** QUESTION 309A consultant is hired to perform a passive vulnerability assessment of a company to determine what information might be collected about the company and its employees. The assessment will be considered successful if the consultant can discover the name of one of the IT administrators.Which of the following is MOST likely to produce the needed information?A. WhoisB. DNS enumerationC. Vulnerability scannerD. Fingerprinting**Answer: A**QUESTION 310A breach was caused by an insider threat in which customer PII was compromised. Following the breach, a lead security analyst is asked to determine which vulnerabilities the attacker used to access company resources.Which of the following should the analyst use to remediate the vulnerabilities?A. Protocol analyzerB. Root cause analyzerC. Behavioral analyticsD. Data leak prevention**Answer: D** QUESTION 311A security analyst has requested network engineers integrate sFlow into the SOC's overall monitoring picture. For this to be a useful addition to the monitoring capabilities, which of the following must be considered by the engineering team?A. Effective deployment of network tapsB. Overall bandwidth available at Internet PoPC. Optimal placement of log aggregatorsD. Availability of application layer visualizers**Answer: D**QUESTION 312Ann, a member of the finance department at a large corporation, has submitted a suspicious email she received to the information security team. The team was not expecting an email from Ann, and it contains a PDF file inside a ZIP compressed archive. The information security learn is not sure which files were opened. A security team member uses an air-gapped PC to open the ZIP and PDF, and it appears to be a social engineering attempt to deliver an exploit.Which of the following would provide greater insight on the potential impact of this attempted attack?A. Run an antivirus scan on the finance PC.B. Use a protocol analyzer on the air-gapped PC.C. Perform reverse engineering on the document.D. Analyze network logs for unusual traffic.E. Run a baseline analyzer against the user's computer.**Answer: B** QUESTION 313A new cluster of virtual servers has been set up in a lab environment and must be audited before being allowed on the production network. The security manager needs to ensure unnecessary services are disabled and all system accounts are using strong credentials.Which of the following tools should be used? (Choose two.)A. FuzzerB. SCAP scannerC. Packet analyzerD. Password crackerE. Network enumeratorF. SIEM**Answer: BF**QUESTION 314A security engineer is embedded with a development team to ensure security is built into products being developed. The security engineer wants to ensure developers are not blocked by a large number of security requirements applied at specific schedule points.Which of the following solutions BEST meets the engineer's goal?A. Schedule weekly reviews of al unit test results with the entire development team and follow up between meetings with surprise code inspections.B. Develop and implement a set of automated security tests to be installed on each development team leader's workstation.C. Enforce code quality and reuse standards into the requirements definition phase of the waterfall development process.D. Deploy an integrated software tool that builds and tests each portion of code committed by developers and provides feedback.**Answer: C**QUESTION 315A security engineer is working with a software development team. The engineer is tasked with ensuring all security requirements are adhered to by the developers.Which of the following BEST describes the contents of the supporting document the engineer is creating?A. A series of ad-hoc tests that each verify security control functionality of the entire system at once.B. A series of discrete tasks that, when viewed in total, can be used to verify and document each individual constraint from the SRTM.C. A set of formal methods that apply to one or more of the programing languages used on the development project.D. A methodology to verify each security control in each unit of developed code prior to committing the code.**Answer: D**QUESTION 316A security technician is incorporating the following requirements in an RFP for a new SIEM:- New security notifications must be dynamically implemented by the SIEM engine- The SIEM must be able to identify traffic baseline anomalies- Anonymous attack data from all customers must augment attack detection and risk scoringBased on the above requirements, which of the following should the SIEM support? (Choose two.)A.   Autoscaling search capabilityB.   Machine learningC.   Multisensor deploymentD.   Big Data analyticsE.   Cloud-based managementF.   Centralized log aggregation **Answer: BD**!!!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