[March-2019-NewExam Pass 100%!Braindump2go CAS-003 Dumps in PDF and VCE 401Q Instant Download

2019/March Braindump2go CAS-003 Exam Dumps with PDF and VCE New Updated Today! Following are some new CAS-003 Exam Questions:1.|2019 Latest Braindump2go CAS-003 Exam Dumps (PDF & VCE) Instant Download:https://www.braindump2go.com/cas-003.html2.|2019 Latest Braindump2go CAS-003 Exam Questions & Answers Instant Download:https://drive.google.com/drive/folders/11eVcvdRTGUBlESzBX9a6YlPUYiZ4xoHE?usp=sharingNew Question There have been some failures of the company's internal facing website. A security engineer has found the WAF to be the root cause of the failures. System logs show that the WAF has been unavailable for 14 hours over the past month, in four separate situations. One of these situations was a two hour scheduled maintenance time, aimed at improving the stability of the WAF. Using the MTTR based on the last month's performance figures, which of the following calculations is the percentage of uptime assuming there were 722 hours in the month?A. 92.24 percentB. 98.06 percentC. 98.34 percentD. 99.72 percentAnswer: BExplanation:A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked.14h of down time in a period of 772 supposed uptime = 14/772 x 100 = 1.939 % Thus the % of uptime = 100% - 1.939% = 98.06%New QuestionA security consultant is conducting a network assessment and wishes to discover any legacy backup Internet connections the network may have. Where would the consultant find this information and why would it be valuable?A. This information can be found in global routing tables, and is valuable because backup connections typically do not have perimeter protection as strong as the primary connection.B. This information can be found by calling the regional Internet registry, and is valuable because backup connections typically do not require VPN access to the network.C. This information can be found by accessing telecom billing records, and is valuable because backup connections typically have much lower latency than primary connections.D. This information can be found by querying the network's DNS servers, and is valuable because backup DNS servers typically allow recursive queries from Internet hosts.Answer: AExplanation:A routing table is a set of rules, often viewed in table format that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. All IP- enabled devices, including routers and switches, use routing tables. Each packet contains information about its origin and destination. When a packet is received, a network device examines the packet and matches it to the routing table entry providing the best match for its destination. The table then provides the device with instructions for sending the packet to the next hop on its route across the network. Thus the security consultant can use the global routing table to get the appropriate information.New QuestionA Chief Information Security Officer (CISO) has requested that a SIEM solution be implemented. The CISO wants to know upfront what the projected TCO would be before looking further into this concern. Two vendor proposals have been received:Vendor A: product-based solution which can be purchased by the pharmaceutical company. Capital expenses to cover central log collectors, correlators, storage and management consoles expected to be $150,000. Operational expenses are expected to be a 0.5 full time employee (FTE) to manage the solution, and 1 full time employee to respond to incidents per year.Vendor B: managed service-based solution which can be the outsourcer for the pharmaceutical company's needs.Bundled offering expected to be $100,000 per year.Operational expenses for the pharmaceutical company to partner with the vendor are expected to be a 0.5 FTE per year.Internal employee costs are averaged to be $80,000 per year per FTE. Based on calculating TCO of the two vendor proposals over a 5 year period, which of the following options is MOST accurate?A. Based on cost alone, having an outsourced solution appears cheaper.B. Based on cost alone, having an outsourced solution appears to be more expensive.C. Based on cost alone, both outsourced an in-sourced solutions appear to be the same.D. Based on cost alone, having a purchased product solution appears cheaper.Answer: AExplanation:The costs of making use of an outsources solution will actually be a savings for the company thus the outsourced solution is a cheaper option over a 5 year period because it amounts to 0,5 FTE per year for the company and at present the company expense if $80,000 per year per FTE.For the company to go alone it will cost $80,000 per annum per FTE = $400,000 over 5 years.With Vendor a $150,000 + $200,000 (?FTE) = $350,000 With Vendor B = $100,000 it will be more expensive.New QuestionA pentester must attempt to crack passwords on a windows domain that enforces strong complex passwords. Which of the following would crack the MOST passwords in the shortest time period?A. Online password testingB. Rainbow tables attackC. Dictionary attackD. Brute force attackAnswer: BExplanation:The passwords in a Windows (Active Directory) domain are encrypted. When a password is "tried" against a system it is "hashed" using encryption so that the actual password is never sent in clear text across the communications line. This prevents eavesdroppers from intercepting the password. The hash of a password usually looks like a bunch of garbage and is typically a different length than the original password. Your password might be "shitzu" but the hash of your password would look something like

"7378347eedbfdd761619451949225ec1".To verify a user, a system takes the hash value created by the password hashing function on the client computer and compares it to the hash value stored in a table on the server. If the hashes match, then the user is authenticated and granted access. Password cracking programs work in a similar way to the login process. The cracking program starts by taking plaintext passwords, running them through a hash algorithm, such as MD5, and then compares the hash output with the hashes in the stolen password file. If it finds a match then the program has cracked the password. Rainbow Tables are basically huge sets of precomputed tables filled with hash values that are pre-matched to possible plaintext passwords. The Rainbow Tables essentially allow hackers to reverse the hashing function to determine what the plaintext password might be. The use of Rainbow Tables allow for passwords to be cracked in a very short amount of time compared with brute-force methods, however, the trade-off is that it takes a lot of storage (sometimes Terabytes) to hold the Rainbow Tables themselves.New QuestionA security engineer on a large enterprise network needs to schedule maintenance within a fixed window of time. A total outage period of four hours is permitted for servers. Workstations can undergo maintenance from 8:00 pm to 6:00 am daily. Which of the following can specify parameters for the maintenance work? (Select TWO).A. Managed security serviceB. Memorandum of understandingC. Quality of serviceD. Network service providerE. Operating level agreementAnswer: BEExplanation:B: A memorandum of understanding (MOU) documents conditions and applied terms for outsourcing partner organizations that must share data and information resources. It must be signed by a re presentative from each organization that has the legal authority to sign and are typically secured, as they are considered confidential.E: An operating level agreement (O LA) defines the responsibilities of each partner's internal support group and what group and resources are used to meet the specified goal. It is used in conjunction with service level agreements (SLAs).New QuestionThe source workstation image for new accounting PCs has begun blue-screening. A technician notices that the date/time stamp of the image source appears to have changed. The desktop support director has asked the Information Security department to determine if any changes were made to the source image. Which of the following methods would BEST help with this process? (Select TWO).A. Retrieve source system image from backup and run file comparison analysis on the two images.B. Parse all images to determine if extra data is hidden using steganography.C. Calculate a new hash and compare it with the previously captured image hash.D. Ask desktop support if any changes to the images were made.E. Check key system files to see if date/time stamp is in the past six months.Answer: ACExplanation:Running a file comparison analysis on the two images will determine whether files have been changed, as well as what files were changed.Hashing can be used to meet the goals of integrity and non-repudiation. One of its advantages of hashing is its ability to verify that information has remained unchanged. If the hash values are the same, then the images are the same. If the hash values differ, there is a difference between the two images.New QuestionWhich of the following activities is commonly deemed "OUT OF SCOPE" when undertaking a penetration test?A. Test password complexity of all login fields and input validation of form fieldsB. Reverse engineering any thick client software that has been provided for the testC. Undertaking network-based denial of service attacks in production environmentD. Attempting to perform blind SQL injection and reflected cross-site scripting attacksE. Running a vulnerability scanning tool to assess network and host weaknessesAnswer: CExplanation:Penetration testing is done to look at a network in an adversarial fashion with the aim of looking at what an attacker will use. Penetration testing is done without malice and undertaking a network-based denial of service attack in the production environment is as such `OUT OF SCOPE'.New QuestionThe Information Security Officer (ISO) is reviewing new policies that have been recently made effective and now apply to the company. Upon review, the ISO identifies a new requirement to implement two-factor authentication on the company's wireless system. Due to budget constraints, the company will be unable to implement the requirement for the next two years. The ISO is required to submit a policy exception form to the Chief Information Officer (CIO). Which of the following are MOST important to include when submitting the exception form? (Select THREE).A. Business or technical justification for not implementing the requirements.B. Risks associated with the inability to implement the requirements.C. Industry best practices with respect to the technical implementation of the current controls.D. All sections of the policy that may justify non-implementation of the requirements.E. A revised DRP and COOP plan to the exception form.F. Internal procedures that may justify a budget submission to implement the new requirement.G. Current and planned controls to mitigate the risks.Answer: ABGExplanation:The Exception Request must include:A description of the non-compliance.The anticipated length of non-compliance (2-year maximum). The proposed assessment of risk associated with non-compliance. The proposed plan for managing the risk associated with non-compliance. The proposed metrics for evaluating the success of risk management (if risk is significant). The proposed review date to evaluate progress toward compliance. An endorsement of the request by the appropriate Information Trustee (VP or Dean).New QuestionA security administrator was doing a packet capture and noticed a system communicating with an unauthorized address within the 2001::/32 prefix. The network administrator confirms there is no IPv6 routing into or out of the network.Which of the following is the BEST course of action?A. Investigate the network traffic and block UDP port 3544 at the firewallB. Remove the system

from the network and disable IPv6 at the routerC. Locate and remove the unauthorized 6to4 relay from the networkD. Disable the switch port and block the 2001::/32 traffic at the firewallAnswer: AExplanation:The 2001::/32 prefix is used for Teredo tunneling. Teredo is a transition technology that gives full IPv6 connectivity for IPv6-capable hosts that are on the IPv4 Internet but have no native connection to an IPv6 network. Unlike similar protocols, it can perform its function even from behind network address translation (NAT) devices such as home routers.Teredo provides IPv6 (Internet Protocol version 6) connectivity by encapsulating IPv6 datagram packets within IPv4 User Datagram Protocol (UDP) packets. Teredo routes these datagrams on the IPv4 Internet and through NAT devices. Teredo nodes elsewhere on the IPv6 network (called Teredo relays) receive the packets, decapsulate them, and pass them on. The Teredo server listens on UDP port 3544.Teredo clients are assigned an IPv6 address that starts with the Teredo prefix (2001::/32). In this question, the BEST course of action would be to block UDP port 3544 at the firewall. This will block the unauthorized communication. You can then investigate the traffic within the network.New QuestionAn organization uses IP address block 203.0.113.0/24 on its internal network. At the border router, the network administrator sets up rules to deny packets with a source address in this subnet from entering the network, and to deny packets with a destination address in this subnet from leaving the network. Which of the following is the administrator attempting to prevent?A. BGP route hijacking attacksB. Bogon IP network trafficC. IP spoofing attacksD. Man-in-the-middle attacksE. Amplified DDoS attacksAnswer: C Explanation:The IP address block 203.0.113.0/24 is used on the internal network. Therefore, there should be no traffic coming into the network claiming to be from an address in the 203.0.113.0/24 range. Similarly, there should be no outbound traffic destined for an address in the 203.0.113.0/24 range. So this has been blocked at the firewall. This is to protect against IP spoofing attacks where an attacker external to the network sends data claiming to be from an internal computer with an address in the 203.0.113.0/24 range. IP spoofing, also known as IP address forgery or a host file hijack, is a hijacking technique in which a cracker masquerades as a trusted host to conceal his identity, spoof a Web site, hijack browsers, or gain access to a network. Here's how it works: The hijacker obtains the IP address of a legitimate host and alters packet headers so that the legitimate host appears to be the source.When IP spoofing is used to hijack a browser, a visitor who types in the URL (Uniform Resource Locator) of a legitimate site is taken to a fraudulent Web page created by the hijacker. For example, if the hijacker spoofed the Library of Congress Web site, then any Internet user who typed in the URL www.loc.gov would see spoofed content created by the hijacker.If a user interacts with dynamic content on a spoofed page, the hijacker can gain access to sensitive information or computer or network resources. He could steal or alter sensitive data, such as a credit card number or password, or install malware. The hijacker would also be able to take control of a compromised computer to use it as part of a zombie army in order to send out spam.New QuestionThe Information Security Officer (ISO) believes that the company has been targeted by cybercriminals and it is under a cyber attack. Internal services that are normally available to the public via the Internet are inaccessible, and employees in the office are unable to browse the Internet. The senior security engineer starts by reviewing the bandwidth at the border router, and notices that the incoming bandwidth on the router's external interface is maxed out. The security engineer then inspects the following piece of log to try and determine the reason for the downtime, focusing on the company's external router's IP which is 128.20.176.19:11:16:22.110343 IP 90.237.31.27.19 > 128.20.176.19.19: UDP, length 140011:16:22.110351 IP 23.27.112.200.19 > 128.20.176.19.19: UDP, length 140011:16:22.110358 IP 192.200.132.213.19 > 128.20.176.19.19: UDP, length 140011:16:22.110402 IP 70.192.2.55.19 > 128.20.176.19.19: UDP, length 140011:16:22.110406 IP 112.201.7.39.19 > 128.20.176.19.19: UDP, length 1400Which of the following describes the findings the senior security engineer should report to the ISO and the BEST solution for service restoration?A. After the senior engineer used a network analyzer to identify an active Fraggle attack, the company's ISP should be contacted and instructed to block the malicious packets.B. After the senior engineer used the above IPS logs to detect the ongoing DDOS attack, an IPS filter should be enabled to block the attack and restore communication.C. After the senior engineer used a mirror port to capture the ongoing amplification attack, a BGP sinkhole should be configured to drop traffic at the source networks. D. After the senior engineer used a packet capture to identify an active Smurf attack, an ACL should be placed on the company's external router to block incoming UDP port 19 traffic.Answer: AExplanation:The exhibit displays logs that are indicative of an active fraggle attack. A Fraggle attack is similar to a smurf attack in that it is a denial of service attack, but the difference is that a fraggle attack makes use of ICMP and UDP ports 7 and 19. Thus when the senior engineer uses a network analyzer to identify the attack he should contact the company's ISP to block those malicious packets.!!!RECOMMEND!!!1.|2019 Latest Braindump2go CAS-003 Exam Dumps (PDF & VCE) Instant Download:https://www.braindump2go.com/cas-003.html2.|2019 Latest Braindump2go CAS-003 Study Guide Video Instant Download: YouTube Video: YouTube.com/watch?v=WCO0vTnXfrk