[Nov-2018Full Version CAS-003 Dumps VCE 374Q for Free Download[Q133-143

2018/November 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) 374Q&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=sharingQUESTION 133A vulnerability scanner report shows that a client-server host monitoring solution operating in the credit card corporate environment is managing SSL sessions with a weak algorithm which does not meet corporate policy. Which of the following are true statements? (Select TWO).A. The X509 V3 certificate was issued by a non trusted public CA.B. The client-server handshake could not negotiate strong ciphers.C. The client-server handshake is configured with a wrong priority.D. The client-server handshake is based on TLS authentication.E. The X509 V3 certificate is expired.F. The client-server implements client-server mutual authentication with different certificates.Answer: BCExplanation:The client-server handshake could not negotiate strong ciphers. This means that the system is not configured to support the strong ciphers provided by later versions of the SSL protocol. For example, if the system is configured to support only SSL version 1.1, then only a weak cipher will be supported.The client-server handshake is configured with a wrong priority. The client sends a list of SSL versions it supports and priority should be given to the highest version it supports. For example, if the client supports SSL versions 1.1, 2 and 3, then the server should use version 3. If the priority is not configured correctly (if it uses the lowest version) then version 1.1 with its weak algorithm will be used.QUESTION 134Which of the following provides the BEST risk calculation methodology?A. Annual Loss Expectancy (ALE) x Value of Asset B. Potential Loss x Event Probability x Control Failure ProbabilityC. Impact x Threat x VulnerabilityD. Risk Likelihood x Annual Loss Expectancy (ALE)Answer: BExplanation:Of the options given, the BEST risk calculation methodology would be Potential Loss x Event Probability x Control Failure Probability. This exam is about computer and data security so `loss' caused by risk is not necessarily a monetary value.For example:Potential Loss could refer to the data lost in the event of a data storage failure. Event probability could be the risk a disk drive or drives failing. Control Failure Probability could be the risk of the storage RAID not being able to handle the number of failed hard drives without losing data.QUESTION 135Company XYZ finds itself using more cloud-based business tools, and password management is becoming onerous. Security is important to the company; as a result, password replication and shared accounts are not acceptable. Which of the following implementations addresses the distributed login with centralized authentication and has wide compatibility among SaaS vendors?A. Establish a cloud-based authentication service that supports SAML.B. Implement a new Diameter authentication server with read-only attestation.C. Install a read-only Active Directory server in the corporate DMZ for federation.D. Allow external connections to the existing corporate RADIUS server.Answer: AExplanation:There is widespread adoption of SAML standards by SaaS vendors for single sign-on identity management, in response to customer demands for fast, simple and secure employee, customer and partner access to applications in their environments. By eliminating all passwords and instead using digital signatures for authentication and authorization of data access, SAML has become the Gold Standard for single sign-on into cloud applications. SAML-enabled SaaS applications are easier and quicker to user provision in complex enterprise environments, are more secure and help simplify identity management across large and diverse user communities.Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. The SAML specification defines three roles: the principal (typically a user), the Identity provider (IdP), and the service provider (SP). In the use case addressed by SAML, the principal requests a service from the service provider. The service provider requests and obtains an identity assertion from the identity provider. On the basis of this assertion, the service provider can make an access control decision ?in other words it can decide whether to perform some service for the connected principal.QUESTION 136A government agency considers confidentiality to be of utmost importance and availability issues to be of least importance. Knowing this, which of the following correctly orders various vulnerabilities in the order of MOST important to LEAST important?A. Insecure direct object references, CSRF, SmurfB. Privilege escalation, Application DoS, Buffer overflowC. SQL injection, Resource exhaustion, Privilege escalationD. CSRF, Fault injection, Memory leaksAnswer: AExplanation:Insecure direct object references are used to access data. CSRF attacks the functions of a web site which could access data. A Smurf attack is used to take down a system.A direct object reference is likely to occur when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key without any validation mechanism which will allow attackers to manipulate these references to access unauthorized data.Cross-Site Request Forgery (CSRF) is a type of attack that occurs when a malicious Web site, email, blog, instant message, or program causes a user's Web browser to perform an unwanted action on a trusted site for which the

user is currently authenticated. The impact of a successful cross-site request forgery attack is limited to the capabilities exposed by the vulnerable application. For example, this attack could result in a transfer of funds, changing a password, or purchasing an item in the user's context. In effect, CSRF attacks are used by an attacker to make a target system perform a function (funds Transfer, form submission etc.) via the target's browser without knowledge of the target user, at least until the unauthorized function has been committed.A smurf attack is a type of network security breach in which a network connected to the Internet is swamped with replies to ICMP echo (PING) requests. A smurf attacker sends PING requests to an Internet broadcast address. These are special addresses that broadcast all received messages to the hosts connected to the subnet. Each broadcast address can support up to 255 hosts, so a single PING request can be multiplied 255 times. The return address of the request itself is spoofed to be the address of the attacker's victim. All the hosts receiving the PING request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's T-1 (or even T-3) line with ping replies, bring the entire Internet service to its knees.Smurfing falls under the general category of Denial of Service attacks -- security attacks that don't try to steal information, but instead attempt to disable a computer or network.QUESTION 137Joe, a hacker, has discovered he can specifically craft a webpage that when viewed in a browser crashes the browser and then allows him to gain remote code execution in the context of the victim's privilege level. The browser crashes due to an exception error when a heap memory that is unused is accessed. Which of the following BEST describes the application issue?A. Integer overflowB. Click-jackingC. Race conditionD. SQL injectionE. Use after freeF. Input validationAnswer: EExplanation:Use-After-Free vulnerabilities are a type of memory corruption flaw that can be leveraged by hackers to execute arbitrary code.Use After Free specifically refers to the attempt to access memory after it has been freed, which can cause a program to crash or, in the case of a Use-After-Free flaw, can potentially result in the execution of arbitrary code or even enable full remote code execution capabilities. According to the Use After Free definition on the Common Weakness Enumeration (CWE) website, a Use After Free scenario can occur when "the memory in question is allocated to another pointer validly at some point after it has been freed. The original pointer to the freed memory is used again and points to somewhere within the new allocation. As the data is changed, it corrupts the validly used memory; this induces undefined behavior in the process."QUESTION 138A large enterprise acquires another company which uses antivirus from a different vendor. The CISO has requested that data feeds from the two different antivirus platforms be combined in a way that allows management to assess and rate the overall effectiveness of antivirus across the entire organization. Which of the following tools can BEST meet the CISO's requirement?A. GRCB. IPSC. CMDBD. Syslog-ngE. IDSAnswer: AExplanation:GRC is a discipline that aims to coordinate information and activity across governance, risk management and compliance with the purpose of operating more efficiently, enabling effective information sharing, more effectively reporting activities and avoiding wasteful overlaps. An integrated GRC (iGRC) takes data feeds from one or more sources that detect or sense abnormalities, faults or other patterns from security or business applications.QUESTION 139A risk manager has decided to use likelihood and consequence to determine the risk of an event occurring to a company asset. Which of the following is a limitation of this approach to risk management?A. Subjective and based on an individual's experience.B. Requires a high degree of upfront work to gather environment details.C. Difficult to differentiate between high, medium, and low risks.D. Allows for cost and benefit analysis.E. Calculations can be extremely complex to manage.Answer: AExplanation:Using likelihood and consequence to determine risk is known as qualitative risk analysis. With qualitative risk analysis, the risk would be evaluated for its probability and impact using a numbered ranking system such as low, medium, and high or perhaps using a 1 to 10 scoring system.After qualitative analysis has been performed, you can then perform quantitative risk analysis. A Quantitative risk analysis is a further analysis of the highest priority risks during which a numerical or quantitative rating is assigned to the risk. Qualitative risk analysis is usually quick to perform and no special tools or software is required. However, qualitative risk analysis is subjective and based on the user's experience.QUESTION 140Joe, a penetration tester, is tasked with testing the security robustness of the protocol between a mobile web application and a RESTful application server. Which of the following security tools would be required to assess the security between the mobile web application and the RESTful application server? (Select TWO).A. Jailbroken mobile deviceB. Reconnaissance toolsC. Network enumeratorD. HTTP interceptorE. Vulnerability scannerF. Password crackerAnswer: DE Explanation:Communications between a mobile web application and a RESTful application server will use the HTTP protocol. To capture the HTTP communications for analysis, you should use an HTTP Interceptor.To assess the security of the application server itself, you should use a vulnerability scanner.A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an

individual or an enterprise can use to tighten the network's security. Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.QUESTION 141A security manager for a service provider has approved two vendors for connections to the service provider backbone. One vendor will be providing authentication services for its payment card service, and the other vendor will be providing maintenance to the service provider infrastructure sites. Which of the following business agreements is MOST relevant to the vendors and service provider's relationship?A. Memorandum of AgreementB. Interconnection Security AgreementC. Non-Disclosure AgreementD. Operating Level AgreementAnswer: BExplanation:The Interconnection Security Agreement (ISA) is a document that identifies the requirements for connecting systems and networks and details what security controls are to be used to protect the systems and sensitive data.QUESTION 142A well-known retailer has experienced a massive credit card breach. The retailer had gone through an audit and had been presented with a potential problem on their network. Vendors were authenticating directly to the retailer's AD servers, and an improper firewall rule allowed pivoting from the AD server to the DMZ where credit card servers were kept. The firewall rule was needed for an internal application that was developed, which presents risk. The retailer determined that because the vendors were required to have site to site VPN's no other security action was taken.To prove to the retailer the monetary value of this risk, which of the following type of calculations is needed?A. Residual Risk calculationB. A cost/benefit analysisC. Quantitative Risk AnalysisD. Qualitative Risk AnalysisAnswer: CExplanation:Performing quantitative risk analysis focuses on assessing the probability of risk with a metric measurement which is usually a numerical value based on money or time.QUESTION 143The security administrator finds unauthorized tables and records, which were not present before, on a Linux database server. The database server communicates only with one web server, which connects to the database server via an account with SELECT only privileges.Web server logs show the following:90.76.165.40 ? - [08/Mar/2014:10:54:04] ?GET calendar.php?create%20table%20hiddenHTTP/1.1? 200 572490.76.165.40 ? - [08/Mar/2014:10:54:05] ?GET ../../../root/.bash_history HTTP/1.1? 200572490.76.165.40 ? - [08/Mar/2014:10:54:04] ?GET index.php?user=<script>Create</script>HTTP/1.1? 200 5724The security administrator also inspects the following file system locations on the database server using the command ?ls -al /root'drwxrwxrwx 11 root root 4096 Sep 28 22:45 .drwxr-xr-x 25 root root 4096 Mar 8 09:30 ..-rws------ 25 root root 4096 Mar 8 09:30 .bash_history-rw------- 25 root root 4096 Mar 8 09:30 .bash_history-rw------- 25 root root 4096 Mar 8 09:30 .profile-rw------- 25 root root 4096 Mar 8 09:30 .sshWhich of the following attacks was used to compromise the database server and what can the security administrator implement to detect such attacks in the future? (Select TWO).A. Privilege escalationB. Brute force attackC. SQL injectionD. Cross-site scriptingE. Using input validation, ensure the following characters are sanitized: <>F. Update crontab with: find / (-perm -4000) ?type f ?print0 | xargs -0 ls ?l | email.shG. Implement the following PHP directive: $clean_user_input = addslashes($user_input)H. Set an account lockout policyAnswer: AFExplanation:This is an example of privilege escalation.Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.The question states that the web server communicates with the database server via an account with SELECT only privileges. However, the privileges listed include read, write and execute (rwx). This suggests the privileges have been `escalated'.Now that we know the system has been attacked, we should investigate what was done to the system.The command "Update crontab with: find / (-perm -4000) ?ype f ?rint0 | xargs -0 ls ? | email.sh" is used to find all the files that are setuid enabled. Setuid means set user ID upon execution. If the setuid bit is turned on for a file, the user executing that executable file gets the permissions of the individual or group that owns the file.!!!RECOMMEND!!!1.|2018 Latest CAS-003 Exam Dumps (PDF & VCE) 374Q&As Download:https://www.braindump2go.com/cas-003.html2.|2018 Latest CAS-003 Study Guide Video: YouTube Video: YouTube.com/watch?v=ZdQwbjNbjb0