Certshared now are offering 100% pass ensure CAS-002 dumps!
https://www.certshared.com/exam/CAS-002/ (450 Q&As)

CompTIA

Exam Questions CAS-002
CompTIA Advanced Security Practitioner (CASP)
NEW QUESTION 1
- (Topic 1)
An external penetration tester compromised one of the client organization’s authentication servers and retrieved the password database. Which of the following methods allows the penetration tester to MOST efficiently use any obtained administrative credentials on the client organization’s other systems, without impacting the integrity of any of the systems?

A. Use the pass the hash technique
B. Use rainbow tables to crack the passwords
C. Use the existing access to change the password
D. Use social engineering to obtain the actual password

Answer: A

NEW QUESTION 2
- (Topic 1)
The Chief Executive Officer (CEO) of a large prestigious enterprise has decided to reduce business costs by outsourcing to a third party company in another country. Functions to be outsourced include: business analysts, testing, software development and back office functions that deal with the processing of customer data. The Chief Risk Officer (CRO) is concerned about the outsourcing plans. Which of the following risks are MOST likely to occur if adequate controls are not implemented?

A. Geographical regulation issues, loss of intellectual property and interoperability agreement issues
B. Improper handling of client data, interoperability agreement issues and regulatory issues
C. Cultural differences, increased cost of doing business and divestiture issues
D. Improper handling of customer data, loss of intellectual property and reputation damage

Answer: D

NEW QUESTION 3
- (Topic 1)
The 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:

Which 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: A

NEW QUESTION 4
- (Topic 1)
A company is deploying a new iSCSI-based SAN. The requirements are as follows: Which of the following design specifications meet all the requirements? (Select TWO).

A. Targets use CHAP authentication
B. IPSec using AH with PKI certificates for authentication
C. Fiber channel should be used with AES
D. Initiators and targets use CHAP authentication
E. Fiber channel over Ethernet should be used
F. IPSec using AH with PSK authentication and 3DES
G. Targets have SCSI IDs for authentication

Answer: BD

NEW QUESTION 5
- (Topic 2)
Customers are receiving emails containing a link to malicious software. These emails are subverting spam filters. The email reads as follows:

Delivered-To: customer@example.com
Received: by 10.14.120.205
Mon, 01 Nov 2010 11:15:24 -0700 (PDT)

Received: by 10.231.31.193
Mon, 01 Nov 2010 11:15:23 -0700 (PDT)

Return-Path: <IT@company.com>
Received: from 127.0.0.1 for <customer@example.com>; Mon, 01 Nov 2010 13:15:14 -0500 (envelope-from <IT@company.com>)
Received: from smtpex.example.com (SMTP READY)
with ESMTP (AIO); Mon, 01 Nov 2010 13:15:14 -0500

Guaranteed success with Our exam guides
visit - https://www.certshared.com
NEW QUESTION 6  
- (Topic 2)  
A port in a fibre channel switch failed, causing a costly downtime on the company's primary website. Which of the following is the MOST likely cause of the downtime?  
A. The web server iSCSI initiator was down.  
B. The web server was not multipathed.  
C. The SAN snapshots were not up-to-date.  
D. The SAN replication to the backup site failed.  

Answer: B

NEW QUESTION 7  
- (Topic 2)  
It has come to the IT administrator's attention that the "post your comment" field on the company blog page has been exploited, resulting in cross-site scripting attacks against customers reading the blog. Which of the following would be the MOST effective at preventing the "post your comment" field from being exploited?  
A. Update the blog page to HTTPS  
B. Filter metacharacters  
C. Install HIDS on the server  
D. Patch the web application  
E. Perform client side input validation  

Answer: B

NEW QUESTION 8  
- (Topic 2)  
A company with 2000 workstations is considering purchasing a HIPS to minimize the impact of a system compromise from malware. Currently, the company projects a total cost of $50,000 for the next three years responding to and eradicating workstation malware. The Information Security Officer (ISO) has received three quotes from different companies that provide HIPS.  
Which solution should the company select if the contract is only valid for three years?  
A. First quote  
B. Second quote  
C. Third quote  
D. Accept the risk  

Answer: B

NEW QUESTION 9  
- (Topic 2)  
Which of the following would be used in forensic analysis of a compromised Linux system? (Select THREE).  
A. Check log files for logins from unauthorized IPs.  
B. Check /proc/kmem for fragmented memory segments.  
C. Check for unencrypted passwords in /etc/shadow.  
D. Check timestamps for files modified around time of compromise.  
E. Use lsif to determine files with future timestamps.  
F. Use gpg to encrypt compromised data files.  
G. Verify the MD5 checksum of system binaries.  
H. Use vmstat to look for excessive disk I/O.  

Answer: ADG

NEW QUESTION 10  
- (Topic 3)  
A company receives a subpoena for email that is four years old. Which of the following should the company consult to determine if it can provide the email in question?  
A. Data retention policy
NEW QUESTION 11
- (Topic 3)
A data breach has occurred at Company A and as a result, the Chief Information Officer (CIO) has resigned. The CIO's laptop, cell phone and PC were all wiped of data per company policy. A month later, prosecutors in litigation with Company A suspect the CIO knew about the data breach long before it was discovered and have issued a subpoena requesting all the CIO's email from the last 12 months. The corporate retention policy recommends keeping data for no longer than 90 days. Which of the following should occur?

A. Restore the CIO's email from an email server backup and provide the last 90 days from the date of the subpoena request.
B. Inform the litigators that the CIO's information has been deleted as per corporate policy.
C. Restore the CIO's email from an email server backup and provide the last 90 days from the date of the CIO resignation.
D. Restore the CIO's email from an email server backup and provide whatever is available up to the last 12 months from the subpoena date.

Answer: D

NEW QUESTION 12
- (Topic 3)
An organization determined that each of its remote sales representatives must use a smartphone for email access. The organization provides the same centrally manageable model to each person. Which of the following mechanisms BEST protects the confidentiality of the resident data?

A. Require dual factor authentication when connecting to the organization’s email server.
B. Require each sales representative to establish a PIN to access the smartphone and limit email storage to two weeks.
C. Require encrypted communications when connecting to the organization’s email server.
D. Require a PIN and automatic wiping of the smartphone if someone enters a specific number of incorrect PINs.

Answer: D

NEW QUESTION 13
- (Topic 4)
Three companies want to allow their employees to seamlessly connect to each other’s wireless corporate networks while keeping one consistent wireless client configuration. Each company wants to maintain its own authentication infrastructure and wants to ensure that an employee who is visiting the other two companies is authenticated by the home office when connecting to the other companies’ wireless network. All three companies have agreed to standardize on 802.1x EAP-PEAP-MSCHAPv2 for client configuration. Which of the following should the three companies implement?

A. The three companies should agree on a single SSID and configure a hierarchical RADIUS system which implements trust delegation.
B. The three companies should implement federated authentication through Shibboleth connected to an LDAP backend and agree on a single SSID.
C. The three companies should implement a central portal-based single sign-on and agree to use the same CA when issuing client certificates.
D. All three companies should use the same wireless vendor to facilitate the use of a shared cloud based wireless controller.

Answer: A

NEW QUESTION 14
- (Topic 4)
Which of the following does SAML uses to prevent government auditors or law enforcement from identifying specific entities as having already connected to a service provider through an SSO operation?

A. Transient identifiers
B. Directory services
C. Restful interfaces
D. Security bindings

Answer: A

NEW QUESTION 15
- (Topic 4)
During a new desktop refresh, all hosts are hardened at the OS level before deployment to comply with policy. Six months later, the company is audited for compliance to regulations. The audit discovers that 40% of the desktops do not meet requirements. Which of the following is the cause of the noncompliance?

A. The devices are being modified and settings are being overridden in production.
B. The patch management system is causing the devices to be noncompliant after issuing the latest patches.
C. The desktop applications were configured with the default username and password.
D. 40% of the devices have been compromised.

Answer: A

NEW QUESTION 16
- (Topic 4)
Ann, a software developer, wants to publish her newly developed software to an online store. Ann wants to ensure that the software will not be modified by a third party or end users before being installed on mobile devices. Which of the following should Ann implement to stop modified copies of her software form running on mobile devices?
A. Single sign-on
B. Identity propagation
C. Remote attestation
D. Secure code review

Answer: C

NEW QUESTION 17
- (Topic 5)
An IT administrator has been tasked by the Chief Executive Officer with implementing security using a single device based on the following requirements:
1. Selective sandboxing of suspicious code to determine malicious intent.
2. VoIP handling for SIP and H.323 connections.
3. Block potentially unwanted applications.
1. Which of the following devices would BEST meet all of these requirements?
A. UTM
B. HIDS
C. NIDS
D. WAF
E. HSM

Answer: A

NEW QUESTION 18
- (Topic 5)
A security officer is leading a lessons learned meeting. Which of the following should be components of that meeting? (Select TWO).
A. Demonstration of IPS system
B. Review vendor selection process
C. Calculate the ALE for the event
D. Discussion of event timeline
E. Assigning of follow up items

Answer: DE

NEW QUESTION 19
- (Topic 5)
A software development manager is taking over an existing software development project. The team currently suffers from poor communication due to a long delay between requirements documentation and feature delivery. This gap is resulting in an above average number of security-related bugs making it into production. Which of the following development methodologies is the team MOST likely using now?
A. Agile
B. Waterfall
C. Scrum
D. Spiral

Answer: B

NEW QUESTION 20
- (Topic 5)
A security administrator needs to deploy a remote access solution for both staff and contractors. Management favors remote desktop due to ease of use. The current risk assessment suggests protecting Windows as much as possible from direct ingress traffic exposure. Which of the following solutions should be selected?
A. Deploy a remote desktop server on your internal LAN, and require an active directory integrated SSL connection for access.
B. Change remote desktop to a non-standard port, and implement password complexity for the entire active directory domain.
C. Distribute new IPSec VPN client software to applicable partie
D. Virtualize remote desktop services functionality.
E. Place the remote desktop server(s) on a screened subnet, and implement two-factor authentication.

Answer: D

NEW QUESTION 21
......
Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

CAS-002 Practice Exam Features:

* CAS-002 Questions and Answers Updated Frequently
* CAS-002 Practice Questions Verified by Expert Senior Certified Staff
* CAS-002 Most Realistic Questions that Guarantee you a Pass on Your First Try
* CAS-002 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click 
Order The CAS-002 Practice Test Here