Exam Questions CAS-002

CompTIA Advanced Security Practitioner (CASP)
NEW QUESTION 1
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 from running on mobile devices?

A. Single sign-on
B. Identity propagation
C. Remote attestation
D. Secure code review

Answer: C

NEW QUESTION 2
An organization is selecting a SaaS provider to replace its legacy, in house Customer Resource Management (CRM) application. Which of the following ensures the organization mitigates the risk of managing separate user credentials?

A. Ensure the SaaS provider supports dual factor authentication.
B. Ensure the SaaS provider supports encrypted password transmission and storage.
C. Ensure the SaaS provider supports secure hash file exchange.
D. Ensure the SaaS provider supports role-based access control.
E. Ensure the SaaS provider supports directory services federation.

Answer: E

NEW QUESTION 3
A security administrator is tasked with increasing the availability of the storage networks while enhancing the performance of existing applications. Which of the following technologies should the administrator implement to meet these goals? (Select TWO).

A. LUN masking
B. Snapshots
C. vSAN
D. Dynamic disk pools
E. Multipath
F. Deduplication

Answer: DE

NEW QUESTION 4
A company has a difficult time communicating between the security engineers, application developers, and sales staff. The sales staff tends to overpromise the application deliverables. The security engineers and application developers are falling behind schedule. Which of the following should be done to solve this?

A. Allow the sales staff to shadow the developers and engineers to see how their sales impact the deliverables.
B. Allow the security engineering team to do application development so they understand why it takes so long.
C. Allow the application developers to attend a sales conference so they understand how business is done.
D. Allow the sales staff to learn application programming and security engineering so they understand the whole lifecycle.

Answer: A

NEW QUESTION 5
A security analyst, Ann, states that she believes Internet facing file transfer servers are being attacked. Which of the following figures is evidence that would aid Ann in making a case to management that action needs to be taken to safeguard these servers?

A. Provide a report of all the IP addresses that are connecting to the systems and their locations
B. Establish alerts at a certain threshold to notify the analyst of high activity
C. Provide a report showing the file transfer logs of the servers
D. Compare the current activity to the baseline of normal activity

Answer: D

NEW QUESTION 6
The risk manager at a small bank wants to use quantitative analysis to determine the ALE of running a business system at a location which is subject to fires during the year. A risk analyst reports to the risk manager that the asset value of the business system is $120,000 and, based on industry data, the exposure factor to fires is only 20% due to the fire suppression system installed at the site. Fires occur in the area on average every four years. Which of the following is the ALE?

A. $6,000
B. $24,000
C. $30,000
D. $96,000

Answer: A

NEW QUESTION 7
A system worth $100,000 has an exposure factor of eight percent and an ARO of four. Which of the following figures is the system’s SLE?

A. $2,000
NEW QUESTION 8
An administrator has enabled salting for users' passwords on a UNIX box. A penetration tester must attempt to retrieve password hashes. Which of the following files must the penetration tester use to eventually obtain passwords on the system? (Select TWO).

A. /etc/passwd
B. /etc/shadow
C. /etc/security
D. /etc/password
E. /sbin/logon
F. /bin/bash

Answer: AB

NEW QUESTION 9
An administrator believes that the web servers are being flooded with excessive traffic from time to time. The administrator suspects that these traffic floods correspond to when a competitor makes major announcements. Which of the following should the administrator do to prove this theory?

A. Implement data analytics to try and correlate the occurrence times.
B. Implement a honey pot to capture traffic during the next attack.
C. Configure the servers for high availability to handle the additional bandwidth.
D. Log all traffic coming from the competitor's public IP addresses.

Answer: A

NEW QUESTION 10
A software developer and IT administrator are focused on implementing security in the organization to protect OSI layer 7. Which of the following security technologies would BEST meet their requirements? (Select TWO).

A. NIPS
B. HSM
C. HIPS
D. NIDS
E. WAF

Answer: CE

NEW QUESTION 11
A network engineer wants to deploy user-based authentication across the company's wired and wireless infrastructure at layer 2 of the OSI model. Company policies require that users be centrally managed and authenticated and that each user's network access be controlled based on the user's role within the company. Additionally, the central authentication system must support hierarchical trust and the ability to natively authenticate mobile devices and workstations. Which of the following are needed to implement these requirements? (Select TWO).

A. SAML
B. WAYF
C. LDAP
D. RADIUS
E. Shibboleth
F. PKI

Answer: CD

NEW QUESTION 12
A newly-appointed risk management director for the IT department at Company XYZ, a major pharmaceutical manufacturer, needs to conduct a risk analysis regarding a new system which the developers plan to bring on-line in three weeks. The director begins by reviewing the thorough and well-written report from the independent contractor who performed a security assessment of the system. The report details what seem to be a manageable volume of infrequently exploited security vulnerabilities. The director decides to implement continuous monitoring and other security controls to mitigate the impact of the vulnerabilities. Which of the following should the director require from the developers before agreeing to deploy the system?

A. An incident response plan which guarantees response by tier two support within 15 minutes of an incident.
B. A definitive plan of action and milestones which lays out resolutions to all vulnerabilities within six months.
C. Business insurance to transfer all risk from the company shareholders to the insurance company.
D. A prudent plan of action which details how to decommission the system within 90 days of becoming operational.

Answer: B

NEW QUESTION 13
A hosting company provides inexpensive guest virtual machines to low-margin customers. Customers manage their own guest virtual machines. Some customers want basic guarantees of logical separation from other customers and it has been indicated that some customers would like to have configuration control of this separation; whereas others want this provided as a value-added service by the hosting company. Which of the following BEST meets these requirements?

A. The hosting company should install a hypervisor-based firewall and allow customers to manage this on an as-needed basis.
B. The hosting company should manage the hypervisor-based firewall; while allowing customers to configure their own host-based firewall.
C. Customers should purchase physical firewalls to protect their guest hosts and have the hosting company manage these if requested.
D. The hosting company should install a host-based firewall on customer guest hosts and offer to administer host firewalls for customers if requested.

Answer: B

NEW QUESTION 14
A database administrator comes across the below records in one of the databases during an internal audit of the payment system:
UserID | Address | Credit Card No. | Password
--- | --- | --- | ---
jsmith123 | fake street55XX-XXX-XXXX-1397 | Password100 | jqdoe234 | fake street42XX-XXX-XXXX-202717DEC12

From a security perspective, which of the following should be the administrator’s GREATEST concern, and what will correct the concern?
A. Concern: Passwords are stored in plain text
B. Correction: Require a minimum of 8 alphanumeric characters and hash the password.
C. Concern: User IDs are also usernames, and could be enumerated, thereby disclosing sensitive account information
D. Correction: Require user IDs to be more complex by using alphanumeric characters and hash the UserIDs.
E. Concern: User IDs are confidential private information
F. Correction: Require encryption of user IDs.
G. Concern: More than four digits within a credit card number are stored
H. Correction: Only store the last four digits of a credit card to protect sensitive financial information.

Answer: A

NEW QUESTION 15
A team is established to create a secure connection between software packages in order to list employee’s remaining or unused benefits on their paycheck stubs. Which of the following business roles would be MOST effective on this team?
A. Network Administrator, Database Administrator, Programmers
B. Network Administrator, Emergency Response Team, Human Resources
C. Finance Officer, Human Resources, Security Administrator
D. Database Administrator, Facilities Manager, Physical Security Manager

Answer: C

NEW QUESTION 16
A system administrator has installed a new Internet facing secure web application that consists of a Linux web server and Windows SQL server into a new corporate site. The administrator wants to place the servers in the most logical network security zones and implement the appropriate security controls. Which of the following scenarios BEST accomplishes this goal?
A. Create an Internet zone, DMZ, and Internal zone on the firewall
B. Place the web server in the DMZ
C. Configure IPtables to allow TCP 80 and 443. Set SELinux to permissive
D. Place the SQL server in the internal zone
E. Configure the Windows firewall to allow TCP 80 and 443. Configure the Internet zone with ACLs of allow 80 and 443 destination DMZ.
F. Create an Internet zone, DMZ, and Internal zone on the firewall
G. Place the web server in the DMZ
H. Configure IPtables to allow TCP 443. Set enforcement threshold on SELinux to on
I. Place the SQL server in the internal zone
J. Configure the Windows firewall to allow TCP 1433 and 1443. Configure the Internet zone with ACLs of allow 443 destination DMZ.
K. Create an Internet zone and two DMZ zones on the firewall
L. Place the web server in DMZ on
M. Set the enforcement threshold on SELinux to 100, and configure IPtables to allow TCP 80 and 443. Place the SQL server in DMZ tw
N. Configure the Windows firewall to allow TCP 80 and 443. Configure the Internet zone with an ACL of allow 443 destination ANY.
O. Create an Internet zone and two DMZ zones on the firewall
P. Place the web server in DMZ on
Q. Set enforcement threshold on SELinux to zero, and configure IPtables to allow TCP 80 and 443. Place the SQL server in DMZ tw
R. Configure the Internet zone ACLs with allow 80, 443, 1433, and 1443 destination ANY.

Answer: B

NEW QUESTION 17
The Chief Information Security Officer (CISO) at a software development company is concerned about the lack of introspection during a testing cycle of the company’s flagship product. Testing was conducted by a small offshore consulting firm and the report by the consulting firm clearly indicates that limited test cases were used and many of the code paths remained untested.
The CISO raised concerns about the testing results at the monthly risk committee meeting, highlighting the need to get to the bottom of the product behaving unexpectedly in only some large enterprise deployments.
The Security Assurance and Development teams highlighted their availability to redo the testing if required.
Which of the following will provide the MOST thorough testing?
A. Have the small consulting firm redo the Black box testing.
B. Use the internal teams to perform Grey box testing.
C. Use the internal team to perform Black box testing.
D. Use the internal teams to perform White box testing.
E. Use a larger consulting firm to perform Black box testing.

Answer: D

NEW QUESTION 18
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 19
An organization would like to allow employees to use their network username and password to access a third-party service. The company is using Active Directory Federated Services for their directory service. Which of the following should the company ensure is supported by the third-party? (Select TWO).

A. LDAP/S
B. SAML
C. NTLM
D. OAuth
E. Kerberos

Answer: BE

NEW QUESTION 20
A security analyst is tasked to create an executive briefing, which explains the activity and motivation of a cyber adversary. Which of the following is the MOST important content for the brief for management personnel to understand?

A. Threat actor types, threat actor motivation, and attack tools
B. Unsophisticated agents, organized groups, and nation states
C. Threat actor types, attack sophistication, and the anatomy of an attack
D. Threat actor types, threat actor motivation, and the attack impact

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