RC0-C02$^{\text{Q\&As}}$

CompTIA Advanced Security Practitioner (CASP) Recertification Exam for Continuing Education

QUESTION 1

In an effort to reduce internal email administration costs, a company is determining whether to outsource its email to a managed service provider that provides email, spam, and malware protection. The security manager is asked to provide input regarding any security implications of this change. Which of the following BEST addresses risks associated with disclosure of intellectual property?

A. Require the managed service provider to implement additional data separation.

B. Require encrypted communications when accessing email.

C. Enable data loss protection to minimize emailing PII and confidential data.

D. Establish an acceptable use policy and incident response policy.

Correct Answer: C

QUESTION 2

The helpdesk department desires to roll out a remote support application for internal use on all company computers. This tool should allow remote desktop sharing, system log gathering, chat, hardware logging, inventory management, and remote registry access. The risk management team has been asked to review vendor responses to the RFQ. Which of the following questions is the MOST important?

A. What are the protections against MITM?

B. What accountability is built into the remote support application?

C. What encryption standards are used in tracking database?

D. What snapshot or "undo" features are present in the application?

E. What encryption standards are used in remote desktop and file transfer functionality?

Correct Answer: B

QUESTION 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 CIOs 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.

Correct Answer: D

QUESTION 4

A Security Administrator has some concerns about the confidentiality of data when using SOAP. Which of the following BEST describes the Security Administrator\\'s concerns?

A. The SOAP header is not encrypted and allows intermediaries to view the header data. The body can be partially or completely encrypted.

B. The SOAP protocol supports weak hashing of header information. As a result the header and body can easily be deciphered by brute force tools.

C. The SOAP protocol can be easily tampered with, even though the header is encrypted.

D. The SOAP protocol does not support body or header encryption which allows assertions to be viewed in clear text by intermediaries.

Correct Answer: A

QUESTION 5

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

Correct Answer: AB

In cryptography, a salt is random data that is used as an additional input to a one-way function that hashes a password or passphrase. In this question, enabling salting for users\\' passwords means to store the passwords in an encrypted format.

Traditional Unix systems keep user account information, including one-way encrypted passwords, in a text file called ``/etc/passwd\\'\\'. As this file is used by many tools (such as ``ls\\'\\') to display file ownerships, etc. by matching user id #\\'s with the user\\'s names, the file needs to be world-readable. Consequentially, this can be somewhat of a security risk. Another method of storing account information is with the shadow password format. As with the traditional method, this method stores account information in the /etc/passwd file in a compatible format. However, the password is stored as a single "x" character (ie. not actually stored in this file). A second file, called ``/etc/shadow\\'\\', contains encrypted password as well as other information such as account or password expiration values, etc.