RC0-C02 Q&As

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

Pass CompTIA RC0-C02 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/rc0-c02.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A company is deploying a new iSCSI-based SAN. The requirements are as follows:

SAN nodes must authenticate each other.

Shared keys must NOT be used.

Do NOT use encryption in order to gain performance.

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

Correct Answer: BD

CHAP (Challenge Handshake Authentication Protocol) is commonly used for iSCSI authentication.

Initiators and targets both using CHAP authentication is known as mutual CHAP authentication.

Another option is to use IPSec using AH with PKI certificates for authentication. One of the two core security protocols in IPSec is the Authentication Header (AH). This is another protocol whose name has been well chosen: AH is a protocol

that provides authentication of either all or part of the contents of a datagram through the addition of a header that is calculated based on the values in the datagram. We can use PKI certificates for authentication rather than shared keys.

QUESTION 2

A company that must comply with regulations is searching for a laptop encryption product to use for its 40,000 end points. The product must meet regulations but also be flexible enough to minimize overhead and support in regards to password resets and lockouts. Which of the following implementations would BEST meet the needs?

A. A partition-based software encryption product with a low-level boot protection and authentication

B. A container-based encryption product that allows the end users to select which files to encrypt

C. A full-disk hardware-based encryption product with a low-level boot protection and authentication

D. A file-based encryption product using profiles to target areas on the file system to encrypt

Correct Answer: D

The question is asking for a solution that will minimize overhead and support in regards to password resets and lockouts.

File based encryption products operate under the context of the computer user\\'s user account. This means that the user does not need to remember a separate password for the encryption software. If the user forgets his user account

password or is locked out due to failed login attempts, the support department can reset his password from a central database of user accounts (such as Active Directory) without the need to visit the user\\'s computer.

Profiles can be used to determine areas on the file system to encrypt such as Document folders.

QUESTION 3

A company receives an e-discovery request for the Chief Information Officer\\'s (CIO\\'s) email data. The storage administrator reports that the data retention policy relevant to their industry only requires one year of email data. However the storage administrator also reports that there are three years of email data on the server and five years of email data on backup tapes. How many years of data MUST the company legally provide?

A. 1

B. 2

C. 3

D. 5

Correct Answer: D

QUESTION 4

Due to a new regulatory requirement, ABC Company must now encrypt all WAN transmissions. When speaking with the network administrator, the security administrator learns that the existing routers have the minimum processing power to do the required level of encryption. Which of the following solutions minimizes the performance impact on the router?

A. Deploy inline network encryption devices

B. Install an SSL acceleration appliance

C. Require all core business applications to use encryption

D. Add an encryption module to the router and configure IPSec

Correct Answer: A

All WAN transmissions must be encrypted. Encryption uses a lot of processing power on a router to encrypt the outgoing data and decrypt the incoming data. In this question, the routers do not have much processing power. We can minimize the performance impact on the router by offloading the encryption function to another device: an inline network encryption device. This is a hardware device specifically designed to perform the function of data encryption and decryption.

QUESTION 5

During an incident involving the company main database, a team of forensics experts is hired to respond to the breach. The team is in charge of collecting forensics evidence from the company\\'s database server. Which of the following is the correct order in which the forensics team should engage?

A. Notify senior management, secure the scene, capture volatile storage, capture non- volatile storage, implement chain of custody, and analyze original media.

B. Take inventory, secure the scene, capture RAM, capture hard drive, implement chain of custody, document, and analyze the data.

C. Implement chain of custody, take inventory, secure the scene, capture volatile and non- volatile storage, and document the findings.

D. Secure the scene, take inventory, capture volatile storage, capture non-volatile storage, document, and implement chain of custody.

Correct Answer: D

The scene has to be secured first to prevent contamination. Once a forensic copy has been created, an analyst will begin the process of moving from most volatile to least volatile information. The chain of custody helps to protect the integrity and reliability of the evidence by keeping an evidence log that shows all access to evidence, from collection to appearance in court.