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

Two universities are making their 802.11n wireless networks available to the other university\\'s students. The infrastructure will pass the student\\'s credentials back to the home school for authentication via the Internet.

The requirements are:

Mutual authentication of clients and authentication server

The design should not limit connection speeds

Authentication must be delegated to the home school No passwords should be sent unencrypted

The following design was implemented:

WPA2 Enterprise using EAP-PEAP-MSCHAPv2 will be used for wireless security

RADIUS proxy servers will be used to forward authentication requests to the home school

The RADIUS servers will have certificates from a common public certificate authority

A strong shared secret will be used for RADIUS server authentication

Which of the following security considerations should be added to the design?

A. The transport layer between the RADIUS servers should be secured

B. WPA Enterprise should be used to decrease the network overhead

C. The RADIUS servers should have local accounts for the visiting students

D. Students should be given certificates to use for authentication to the network

Correct Answer: A

One of the requirements in this question states, "No passwords should be sent unencrypted". The design that was implemented makes no provision for the encryption of passwords as they are sent between RADIUS servers. The local RADIUS servers will pass the student\\'s credentials back to the home school RADIUS servers for authentication via the Internet. When passing sensitive data such as usernames and passwords over the internet, the data should be sent over a secure connection. We can secure the transport layer between the RADIUS servers by implementing TLS (Transport Layer Security). Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

QUESTION 2

An administrator is implementing a new network-based storage device. In selecting a storage protocol, the administrator would like the data in transit\\'s integrity to be the most important concern. Which of the following protocols meets these needs by implementing either AES-CMAC or HMAC-SHA256 to sign data?

A. SMB

B. NFS

C. FCoE

D. iSCSI

Correct Answer: A

Server Message Block (SMB) is a protocol that has long been used by Windows computers for sharing files, printers and other resources among computers on the network. The server message blocks are the requests that an SMB client

sends to a server and the responses that the server sends back to the client.

Microsoft has improved the SMB protocol over the years. In 2006, they came out with a new version, SMB 2.0, in conjunction with Vista, and SMB 2.1 with Windows 7. Version 2 was a major revision with significant changes, including a

completely different packet format. Windows 8 introduces another new version, SMB 3.0. Microsoft has made a number of security improvements in SMB 3.0, which will be introduced in the Windows 8 client and Windows Server 2012. A new

algorithm is used for SMB signing. SMB 2.x uses HMAC-SHA256. SMB 3.0 uses AES-CMAC. CMAC is based on a symmetric key block cipher (AES), whereas HMAC is based on a hash function (SHA). AES (Advanced Encryption Standard)

is the specification adopted by the U.S. government in 2002 and was approved by the National Security Agency (NSA) for encryption of top secret information.

QUESTION 3

A user is suspected of engaging in potentially illegal activities. Law enforcement has requested that the user continue to operate on the network as normal. However, they would like to have a copy of any communications from the user involving certain key terms. Additionally, the law enforcement agency has requested that the user\\'s ongoing communication be retained in the user\\'s account for future investigations. Which of the following will BEST meet the goals of law enforcement?

A. Begin a chain-of-custody on for the user\\'s communication. Next, place a legal hold on the user\\'s email account.

B. Perform an e-discover using the applicable search terms. Next, back up the user\\'s email for a future investigation.

C. Place a legal hold on the user\\'s email account. Next, perform e-discovery searches to collect applicable emails.

D. Perform a back up of the user\\'s email account. Next, export the applicable emails that match the search terms.

Correct Answer: C

A legal hold is a process that an organization uses to maintain all forms of pertinent information when legal action is reasonably expected. E-discovery refers to discovery in litigation or government investigations that manages the exchange of electronically stored information (ESI). ESI includes email and office documents, photos, video, databases, and other filetypes.

QUESTION 4

Joe is a security architect who is tasked with choosing a new NIPS platform that has the ability to perform SSL inspection, analyze up to 10Gbps of traffic, can be centrally managed and only reveals inspected application payload

data to specified internal security employees. Which of the following steps should Joe take to reach the desired outcome?

A. Research new technology vendors to look for potential products. Contribute to an RFP and then evaluate RFP responses to ensure that the vendor product meets all mandatory requirements. Test the product and make a product recommendation.

B. Evaluate relevant RFC and ISO standards to choose an appropriate vendor product. Research industry surveys, interview existing customers of the product and then recommend that the product be purchased.

C. Consider outsourcing the product evaluation and ongoing management to an outsourced provider on the basis that each of the requirements are met and a lower total cost of ownership (TCO) is achieved.

D. Choose a popular NIPS product and then consider outsourcing the ongoing device management to a cloud provider. Give access to internal security employees so that they can inspect the application payload data.

E. Ensure that the NIPS platform can also deal with recent technological advancements, such as threats emerging from social media, BYOD and cloud storage prior to purchasing the product.

Correct Answer: A

A request for a Proposal (RFP) is in essence an invitation that you present to vendors asking them to submit proposals on a specific commodity or service. This should be evaluated, then the product should be tested and then a product recommendation can be made to achieve the desired outcome.

QUESTION 5

After being notified of an issue with the online shopping cart, where customers are able to arbitrarily change the price of listed items, a programmer analyzes the following piece of code used by a web based shopping cart.

SELECT ITEM FROM CART WHERE ITEM=ADDSLASHES($USERINPUT);

The programmer found that every time a user adds an item to the cart, a temporary file is created on the web server /tmp directory. The temporary file has a name which is generated by concatenating the content of the $USERINPUT variable

and a timestamp in the form of MM-DD-YYYY, (e.g. smartphone-12-25-2013.tmp) containing the price of the item being purchased. Which of the following is MOST likely being exploited to manipulate the price of a shopping cart\\'s items?

A. Input validation

B. SQL injection

C. TOCTOU

D. Session hijacking

Correct Answer: C

In this question, TOCTOU is being exploited to allow the user to modify the temp file that contains the price of the item. In software development, time of check to time of use (TOCTOU) is a class of software bug caused by changes in a system between the checking of a condition (such as a security credential) and the use of the results of that check. This is one example of a race condition. A simple example is as follows: Consider a Web application that allows a user to edit pages, and also allows administrators to lock pages to prevent editing. A user requests to edit a page, getting a form which can be used to alter its content. Before the user submits the form, an administrator locks the page, which should

prevent editing. However, since editing has already begun, when the user submits the form, those edits (which have already been made) are accepted. When the user began editing, the appropriate authorization was checked, and the user was indeed allowed to edit. However, the authorization was used later, at a time when edits should no longer have been allowed. TOCTOU race conditions are most common in Unix between operations on the file system, but can occur in other contexts, including local sockets and improper use of database transactions.