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

An IT manager is concerned about the cost of implementing a web filtering solution in an effort to mitigate the risks associated with malware and resulting data leakage. Given that the ARO is twice per year, the ALE resulting from a data leak is $25,000 and the ALE after implementing the web filter is $15,000. The web filtering solution will cost the organization $10,000 per year. Which of the following values is the single loss expectancy of a data leakage event after implementing the web filtering solution?

A. $0

B. $7,500

C. $10,000

D. $12,500

E. $15,000

Correct Answer: B

The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as: ALE = ARO x SLE

Single Loss Expectancy (SLE) is mathematically expressed as: Asset value (AV) x Exposure Factor (EF)

SLE = AV x EF - Thus the Single Loss Expectancy (SLE) = ALE/ARO = $15,000 / 2 = $ 7,500

References:

http://www.financeformulas.net/Return_on_Investment.html https://en.wikipedia.org/wiki/Risk_assessment

QUESTION 2

A company is facing penalties for failing to effectively comply with e-discovery requests. Which of the following could reduce the overall risk to the company from this issue?

A. Establish a policy that only allows filesystem encryption and disallows the use of individual file encryption.

B. Require each user to log passwords used for file encryption to a decentralized repository.

C. Permit users to only encrypt individual files using their domain password and archive all old user passwords.

D. Allow encryption only by tools that use public keys from the existing escrowed corporate PKI.

Correct Answer: D

Electronic discovery (also called e-discovery) refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case. E-discovery can be carried out offline

on a particular computer or it can be done in a network.

An e-discovery policy would define how data is archived and encrypted. If the data is archived in an insecure manor, a

user could be able to delete data that the user does not want to be searched. Therefore, we need to find a way of securing

the data in a way that only authorized people can access the data.

A public key infrastructure (PKI) supports the distribution and identification of public encryption keys for the encryption of data. The data can only be decrypted by the private key.

In this question, we have an escrowed corporate PKI. Escrow is an independent and licensed third party that holds something (money, sensitive data etc.) and releases it only when predefined conditions have been met. In this case, Escrow is

holding the private key of the PKI.

By encrypting the e-discovery data by using the PKI public key, we can ensure that the data can only be decrypted by the private key held in Escrow and this will only happen when the predefined conditions are met.

QUESTION 3

The risk manager is reviewing a report which identifies a requirement to keep a business critical legacy system operational for the next two years. The legacy system is out of support because the vendor and security patches are no longer released. Additionally, this is a proprietary embedded system and little is documented and known about it. Which of the following should the Information Technology department implement to reduce the security risk from a compromise of this system?

A. Virtualize the system and migrate it to a cloud provider.

B. Segment the device on its own secure network.

C. Install an antivirus and HIDS on the system.

D. Hire developers to reduce vulnerabilities in the code.

Correct Answer: B

The question states that the application is a proprietary embedded system and little is documented and known about it. If we don\\'t know much about the application or system, we should not make any changes to the system. The best solution would be to isolate the system by segmenting the device on its own secure network. This will reduce the risk of a compromise of the system without making changes to the system itself.

QUESTION 4

A critical system audit shows that the payroll system is not meeting security policy due to missing OS security patches. Upon further review, it appears that the system is not being patched at all. The vendor states that the system is only supported on the current OS patch level. Which of the following compensating controls should be used to mitigate the vulnerability of missing OS patches on this system?

A. Isolate the system on a secure network to limit its contact with other systems

B. Implement an application layer firewall to protect the payroll system interface

C. Monitor the system\\'s security log for unauthorized access to the payroll application

D. Perform reconciliation of all payroll transactions on a daily basis

Correct Answer: A

The payroll system is not meeting security policy due to missing OS security patches. We cannot apply the patches to the system because the vendor states that the system is only supported on the current OS patch level. Therefore, we need

another way of securing the system.

We can improve the security of the system and the other systems on the network by isolating the payroll system on a secure network to limit its contact with other systems. This will reduce the likelihood of a malicious user accessing the

payroll system and limit any damage to other systems if the payroll system is attacked.

QUESTION 5

Which of the following activities is commonly deemed "OUT OF SCOPE" when undertaking a penetration test?

A. Test password complexity of all login fields and input validation of form fields

B. Reverse engineering any thick client software that has been provided for the test

C. Undertaking network-based denial of service attacks in production environment

D. Attempting to perform blind SQL injection and reflected cross-site scripting attacks

E. Running a vulnerability scanning tool to assess network and host weaknesses

Correct Answer: C

Penetration testing is done to look at a network in an adversarial fashion with the aim of looking at what an attacker will use. Penetration testing is done without malice and undertaking a network-based denial of service attack in the production environment is as such `OUT OF SCOPE\\'.