RC0-C02 Q&As

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

Pass CompTIA RC0-C02 Exam with 100% Guarantee

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

QUESTION 1

A Security Manager is part of a team selecting web conferencing systems for internal use. The system will only be used for internal employee collaboration. Which of the following are the MAIN concerns of the security manager? (Select THREE).

A. Security of data storage

B. The cost of the solution

C. System availability

D. User authentication strategy

E. PBX integration of the service

F. Operating system compatibility

Correct Answer: ACD

QUESTION 2

ABC Corporation has introduced token-based authentication to system administrators due to the risk of password compromise. The tokens have a set of HMAC counter-based codes and are valid until they are used. Which of the following types of authentication mechanisms does this statement describe?

A. TOTP

B. PAP

C. CHAP

D. HOTP

Correct Answer: D

The question states that the HMAC counter-based codes and are valid until they are used.

These are "one-time" use codes.

HOTP is an HMAC-based one-time password (OTP) algorithm. HOTP can be used to authenticate a user in a system via an authentication server. Also, if some more steps are carried out (the server calculates subsequent OTP value and

sends/displays it to the user who checks it against subsequent OTP value calculated by his token), the user can also authenticate the validation server. Both hardware and software tokens are available from various vendors. Hardware tokens

implementing OATH HOTP tend to be significantly cheaper than their competitors based on proprietary algorithms. Some products can be used for strong passwords as well as OATH HOTP.

Software tokens are available for (nearly) all major mobile/smartphone platforms.

QUESTION 3

A risk manager has decided to use likelihood and consequence to determine the risk of an event occurring to a company asset. Which of the following is a limitation of this approach to risk management?

A. Subjective and based on an individual\\'s experience.

B. Requires a high degree of upfront work to gather environment details.

C. Difficult to differentiate between high, medium, and low risks.

D. Allows for cost and benefit analysis.

E. Calculations can be extremely complex to manage.

Correct Answer: A

Using likelihood and consequence to determine risk is known as qualitative risk analysis. With qualitative risk analysis, the risk would be evaluated for its probability and impact using a numbered ranking system such as low, medium, and high

or perhaps using a 1 to 10 scoring system.

After qualitative analysis has been performed, you can then perform quantitative risk analysis. A Quantitative risk analysis is a further analysis of the highest priority risks during which a numerical or quantitative rating is assigned to the risk.

Qualitative risk analysis is usually quick to perform and no special tools or software is required. However, qualitative risk analysis is subjective and based on the user\\'s experience.

QUESTION 4

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 5

The Chief Information Security Officer (CISO) at a company knows that many users store business documents on public cloud-based storage, and realizes this is a risk to the company. In response, the CISO implements a mandatory training course in which all employees are instructed on the proper use of cloud-based storage. Which of the following risk strategies did the CISO implement?

A. Avoid

B. Accept

C. Mitigate

D. Transfer

Correct Answer: C

Mitigation means that a control is used to reduce the risk. In this case, the control is training.