CSSLP[Q&As]

Certified Secure Software Lifecycle Professional Practice Test

Pass ISC CSSLP Exam with 100% Guarantee

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

https://www.geekcert.com/csslp.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which of the following statements describe the main purposes of a Regulatory policy? Each correct answer represents a complete solution. Choose all that apply.

A. It acknowledges the importance of the computing resources to the business model

B. It provides a statement of support for information security throughout the enterprise

C. It ensures that an organization is following the standard procedures or base practices of operation in its specific industry.

D. It gives an organization the confidence that it is following the standard and accepted industry policy.

Correct Answer: CD

The main purposes of a Regulatory policy are as follows: It ensures that an organization is following the standard procedures or base practices of operation in its specific industry. It gives an organization the confidence that it is following the standard and accepted industry policy. Answer: B and A are incorrect. These are the policy elements of Senior Management Statement of Policy.

QUESTION 2

Which of the following is an attack with IP fragments that cannot be reassembled?

A. Password guessing attack

B. Teardrop attack

C. Dictionary attack

D. Smurf attack

Correct Answer: B

Teardrop is an attack with IP fragments that cannot be reassembled. In this attack, corrupt packets are sent to the victim\\'s computer by using IP\\'s packet fragmentation algorithm. As a result of this attack, the victim\\'s computer might hang. Answer: D is incorrect. Smurf is an ICMP attack that involves spoofing and flooding. Answer: C is incorrect. Dictionary attack is a type of password guessing attack. This type of attack uses a dictionary of common words to find out the password of a user. It can also use common words in either upper or lower case to find a password. There are many programs available on the Internet to automate and execute dictionary attacks. Answer: A is incorrect. A password guessing attack occurs when an unauthorized user tries to log on repeatedly to a computer or network by guessing usernames and passwords. Many password guessing programs that attempt to break passwords are available on the Internet. Following are the types of password guessing attacks: Brute force attack Dictionary attack

QUESTION 3

You are responsible for network and information security at a metropolitan police station. The most important concern is that unauthorized parties are not able to access data. What is this called?

A. Confidentiality

B. Availability

C. Integrity

D. Encryption

Correct Answer: A

The CIA (Confidentiality, Integrity, and Availability) triangle is concerned with three facets of security. Confidentiality is the concern that data be secure from unauthorized access. Answer: B and C are incorrect. The CIA (Confidentiality, Integrity, and Availability) triangle is concerned with three facets of security. Integrity is the concern that data not be altered without it being traceable. Availability is the concern that the data, while being secured, is readily accessible. Answer: D is incorrect. Confidentiality may be implemented with encryption but encryption is just a technique to obtain confidentiality.

QUESTION 4

Which of the following security design patterns provides an alternative by requiring that a user\\'s authentication credentials be verified by the database before providing access to that user\\'s data?

A. Secure assertion

B. Authenticated session

C. Password propagation

D. Account lockout

Correct Answer: C

Password propagation provides an alternative by requiring that a user\\'s authentication credentials be verified by the database before providing access to that user\\'s data. Answer: D is incorrect. Account lockout implements a limit on the incorrect password attempts to protect an account from automated password-guessing attacks. Answer: B is incorrect. Authenticated session allows a user to access more than one access-restricted Web page without re-authenticating every page. It also integrates user authentication into the basic session model. Answer: A is incorrect. Secure assertion distributes application-specific sanity checks throughout the system.

QUESTION 5

How can you calculate the Annualized Loss Expectancy (ALE) that may occur due to a threat?

A. Single Loss Expectancy (SLE) X Annualized Rate of Occurrence (ARO)

B. Single Loss Expectancy (SLE)/ Exposure Factor (EF)

C. Asset Value X Exposure Factor (EF)

D. Exposure Factor (EF)/Single Loss Expectancy (SLE)

Correct Answer: A

The Annualized Loss Expectancy (ALE) that occurs due to a threat can be calculated by multiplying the Single Loss Expectancy (SLE) with the Annualized Rate of Occurrence (ARO). Annualized Loss Expectancy (ALE) = Single Loss

Expectancy (SLE) X Annualized Rate of Occurrence (ARO) Annualized Rate of Occurrence (ARO) is a number that represents the estimated frequency in which a threat is expected to occur. It is calculated based upon the probability of the event occurring and the number of employees that could make that event occur. Single Loss Expectancy (SLE) is the value in dollars that is assigned to a single event. SLE can be calculated by the following formula: SLE = Asset Value ($) X Exposure Factor (EF) The Exposure Factor (EF) represents the % of assets loss caused by a threat. The EF is required to calculate Single Loss Expectancy (SLE).