SSCP$^{Q\&As}$

System Security Certified Practitioner (SSCP)

Pass ISC SSCP Exam with 100% Guarantee

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

QUESTION 1

What can be defined as secret communications where the very existence of the message is hidden?

A. Clustering

B. Steganography

C. Cryptology

D. Vernam cipher

Correct Answer: B

Steganography is a secret communication where the very existence of the message is hidden. For example, in a digital image, the least significant bit of each word can be used to comprise a message without causing any significant change in the image. Key clustering is a situation in which a plaintext message generates identical ciphertext messages using the same transformation algorithm but with different keys. Cryptology encompasses cryptography and cryptanalysis. The Vernam Cipher, also called a one-time pad, is an encryption scheme using a random key of the same size as the message and is used only once. It is said to be unbreakable, even with infinite resources.

Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley and Sons, 2001, Chapter 4: Cryptography (page 134).

QUESTION 2

When it comes to magnetic media sanitization, what difference can be made between clearing and purging information?

A. Clearing completely erases the media whereas purging only removes file headers, allowing the recovery of files.

B. Clearing renders information unrecoverable by a keyboard attack and purging renders information unrecoverable against laboratory attack.

C. They both involve rewriting the media.

D. Clearing renders information unrecoverable against a laboratory attack and purging renders information unrecoverable to a keyboard attack.

Correct Answer: B

The removal of information from a storage medium is called sanitization. Different kinds of sanitization provide different levels of protection. A distinction can be made between clearing information (rendering it unrecoverable by a keyboard attack) and purging (rendering it unrecoverable against laboratory attack).

There are three general methods of purging media: overwriting, degaussing, and destruction.

There should be continuous assurance that sensitive information is protected and not allowed to be placed in a circumstance wherein a possible compromise can occur. There are two primary levels of threat that the protector of information must guard against: keyboard attack (information scavenging through system software capabilities) and laboratory attack (information scavenging through laboratory means). Procedures should be implemented to address these threats before the Automated Information System (AIS) is procured, and the procedures should be continued throughout the life cycle of the AIS.

Reference(s) use for this question:

SWANSON, Marianne and GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (page 26).

and

A guide to understanding Data Remanence in Automated Information Systems

QUESTION 3

Which of the following tasks is NOT usually part of a Business Impact Analysis (BIA)?

A. Calculate the risk for each different business function.

B. Identify the company\\'s critical business functions.

C. Calculate how long these functions can survive without these resources.

D. Develop a mission statement.

Correct Answer: D

The Business Impact Analysis is critical for the development of a business continuity plan (BCP). It identifies risks, critical processes and resources needed in case of recovery and quantifies the impact a disaster will have upon the organization. The development of a mission statement is normally performed before the BIA.

A BIA (business impact analysis) is considered a functional analysis, in which a team collects data through interviews and documentary sources; documents business functions, activities, and transactions ; develops a hierarchy of business functions; and finally applies a classification scheme to indicate each individual function\\'s criticality level.

BIA Steps

The more detailed and granular steps of a BIA are outlined here:

1.

Select individuals to interview for data gathering.

2.

Create data-gathering techniques (surveys, questionnaires, qualitative and quantitative approaches).

3.

Identify the company\\'s critical business functions.

4.

Identify the resources these functions depend upon.

5.

Calculate how long these functions can survive without these resources.

6.

Identify vulnerabilities and threats to these functions.

7.

Calculate the risk for each different business function.

8.

Document findings and report them to management. Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Location 21076). Auerbach Publications. Kindle Edition.

and

Harris, Shon (2012-10-18). CISSP All-in-One uide, 6th Edition (p. 905-910). McGraw- Hill. Kindle Edition.

QUESTION 4

Which of the following is true of network security?

A. A firewall is a not a necessity in today\\'s connected world.

B. A firewall is a necessity in today\\'s connected world.

C. A whitewall is a necessity in today\\'s connected world.

D. A black firewall is a necessity in today\\'s connected world.

Correct Answer: B

Commercial firewalls are a dime-a-dozen in todays world. Black firewall and whitewall are just distracters.

QUESTION 5

What is the appropriate role of the security analyst in the application system development or acquisition project?

A. policeman

B. control evaluator and consultant

C. data owner

D. application user

Correct Answer: B

The correct answer is "control evaluator and consultant". During any system development or acquisition, the security staff should evaluate security controls and advise (or consult) on the strengths and weaknesses with those responsible for making the final decisions on the project.

The other answers are not correct because:

policeman - It is never a good idea for the security staff to be placed into this type of role (though it is sometimes unavoidable). During system development or acquisition, there should be no need of anyone filling the role of policeman.

data owner - In this case, the data owner would be the person asking for the new system to manage, control, and secure information they are responsible for. While it is possible the security staff could also be the data owner for such a project if they happen to have responsibility for the information, it is also possible someone else would fill this role. Therefore, the best answer remains "control evaluator and consultant".

application user - Again, it is possible this could be the security staff, but it could also be many other people or groups. So this is not the best answer.

Reference:

Official ISC2 Guide page: 555 - 560

All in One Third Edition page: 832 - 846