SSCP$^{\text{Q\&As}}$

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

Which of the following is NOT a part of a risk analysis?

A. Identify risks

B. Quantify the impact of potential threats

C. Provide an economic balance between the impact of the risk and the cost of the associated countermeasure

D. Choose the best countermeasure

Correct Answer: D

This step is not a part of RISK ANALYSIS.

A risk analysis has three main goals: identify risks, quantify the impact of potential threats, and provide an economic balance between the impact of the risk and the cost of the associated countermeasure. Choosing the best countermeasure is not part of the risk analysis.

Source: HARRIS, Shon, All-In-One CISSP Certification uide, McGraw-Hill/Osborne, 2002, chapter

3: Security Management Practices (page 73).

HARRIS, Shon, Mike Meyers\\' CISSP(R) Certification Passport, 2002, McGraw-Hill, page 12.

QUESTION 2

Which access model is most appropriate for companies with a high employee turnover?

A. Role-based access control

B. Mandatory access control

C. Lattice-based access control

D. Discretionary access control

Correct Answer: A

The underlying problem for a company with a lot of turnover is assuring that new employees are assigned the correct access permissions and that those permissions are removed when they leave the company. Selecting the best answer requires one to think about the access control options in the context of a company with a lot of flux in the employee population. RBAC simplifies the task of assigning permissions because the permissions are assigned to roles which do not change based on who belongs to them. As employees join the company, it is simply a matter of assigning them to the appropriate roles and their permissions derive from their assigned role. They will implicitely inherit the permissions of the role or roles they have been assigned to. When they leave the company or change jobs, their role assignment is revoked/changed appropriately.

Mandatory access control is incorrect. While controlling access based on the clearence level of employees and the sensitivity of obects is a better choice than some of the other incorrect answers, it is not the best choice when RBAC is an option and you are looking for the best solution for a high number of employees constantly leaving or joining the company.

Lattice-based access control is incorrect. The lattice is really a mathematical concept that is used in formally modeling information flow (Bell-Lapadula, Biba, etc). In the context of the question, an abstract model of information flow is not an appropriate choice. CBK, pp. 324-325.

Discretionary access control is incorrect. When an employee joins or leaves the company, the object owner must grant or revoke access for that employee on all the objects they own. Problems would also arise when the owner of an object leaves the company. The complexity of assuring that the permissions are added and removed correctly makes this the least desirable solution in this situation.

References

Alll in One, third edition page 165

RBAC is discussed on pp. 189 through 191 of the ISC(2) guide.

QUESTION 3

It is a violation of the "separation of duties" principle when which of the following individuals access the software on systems implementing security?

A. security administrator

B. security analyst

C. systems auditor

D. systems programmer

Correct Answer: D

Reason: The security administrator, security analysis, and the system auditor need access to portions of the security systems to accomplish their jobs. The system programmer does not need access to the working (AKA: Production) security systems.

Programmers should not be allowed to have ongoing direct access to computers running production systems (systems used by the organization to operate its business). To maintain system integrity, any changes they make to production systems should be tracked by the organization\\'s change management

control system.

Because the security administrator\\'s job is to perform security functions, the performance of non-security

tasks must be strictly limited. This separation of duties reduces the likelihood of loss that results from users

abusing their authority by taking actions outside of their assigned functional responsibilities.

References:

OFFICIAL (ISC)2® GUIDE TO THE CISSP® EXAM (2003), Hansche, S., Berti, J., Hare, H., Auerbach

Publication, FL, Chapter 5 - Operations Security, section 5.3,"Security Technology and Tools," Personnel

section (page 32).

KRUTZ, R. and VINES, R. The CISSP Prep Guide: Gold Edition (2003), Wiley Publishing Inc., Chapter 6:

Operations Security, Separations of Duties (page 303).

QUESTION 4

What enables users to validate each other\\'s certificate when they are certified under different certification hierarchies?

A. Cross-certification

B. Multiple certificates

C. Redundant certification authorities

D. Root certification authorities

Correct Answer: A

Cross-certification is the act or process by which two CAs each certifiy a public key of the other, issuing a public-key certificate to that other CA, enabling users that are certified under different certification hierarchies to validate each other\\'s certificate.

Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 5

Which type of attack is based on the probability of two different messages using the same hash function producing a common message digest?

A. Differential cryptanalysis

B. Differential linear cryptanalysis

C. Birthday attack

D. Statistical attack

Correct Answer: C

A Birthday attack is usually applied to the probability of two different messages using the same hash function producing a common message digest.

The term "birthday" comes from the fact that in a room with 23 people, the probability of two of more people having the same birthday is greater than 50%.

Linear cryptanalysis is a general form of cryptanalysis based on finding affine approximations to the action of a cipher. Attacks have been developed for block ciphers and stream ciphers. Linear cryptanalysis is one of the two most widely used attacks on block ciphers; the other being differential cryptanalysis.

Differential Cryptanalysis is a potent cryptanalytic technique introduced by Biham and Shamir. Differential cryptanalysis is designed for the study and attack of DES-like cryptosystems. A DES-like cryptosystem is an iterated cryptosystem which relies on conventional cryptographic techniques such as substitution and diffusion. Differential cryptanalysis is a general form of cryptanalysis applicable primarily to block ciphers, but also to stream ciphers and cryptographic hash functions. In the broadest sense, it is the study of how differences in an input can affect the resultant difference at the output. In the case of a block cipher, it refers to a set of techniques for tracing differences through the network of transformations, discovering where the cipher exhibits non-random behaviour, and exploiting such properties to recover the secret key.

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 163).

and

http://en.wikipedia.org/wiki/Differential_cryptanalysis