SSCP Q&As

System Security Certified Practitioner (SSCP)

Pass ISC SSCP Exam with 100% Guarantee

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

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

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which division of the Orange Book deals with discretionary protection (need-to-know)?

A. D

B. C

C. B

D. A

Correct Answer: B

C deals with discretionary protection. See matric below:

TNI/TCSEC MATRIX

	A1	B3	B2	B1	C2	C1
DISCRETIONARY ACCESS						
Discretionary Access Control						
Identification and Authentication						
System Integrity						
System Architecture						
Security Testing						
Security Features User's Guide Trusted Facility Manual Design Documentation Test Documentation						
CONTROLLED ACCESS						
Protect Audit Trails						
Object Reuse						
MANDATORY ACCESS CONTROL						
Labels						
Mandatory Access Control						
Process isolation in system architecture						
Design Specification & Verification						
Device labels						
Subject Sensitivity Labels						
Trusted Path						
Separation of Administrator and User functions						
Covert Channel Analysis (Only Covert Storage Channel at B2)						
Trusted Facility Management						
Configuration Management						
Trusted Recovery						
Covert Channel Analysis (Both Timing and Covert Channel analysis at B3)						
Security Administrator Role Defined						
Monitor events and notify security personnel						
Trusted Distribution						
Formal Methods						
	A1	B3	B2	B1	C2	C1

TCSEC Matric

The following are incorrect answers:

D is incorrect. D deals with minimal security.

B is incorrect. B deals with mandatory protection.

A is incorrect. A deals with verified protection.

Reference(s) used for this question:

CBK, p. 329 330

and

Shon Harris, CISSP All In One (AIO), 6th Edition , page 392-393

QUESTION 2

Controls to keep password sniffing attacks from compromising computer systems include which of the following?

A. static and recurring passwords.

B. encryption and recurring passwords.

C. one-time passwords and encryption.

D. static and one-time passwords.

Correct Answer: C

To minimize the chance of passwords being captured one-time passwords would prevent a password sniffing attack because once used it is no longer valid. Encryption will also minimize these types of attacks.

The following answers are correct:

static and recurring passwords. This is incorrect because if there is no encryption then someone password sniffing would be able to capture the password much easier if it never changed.

encryption and recurring passwords. This is incorrect because while encryption helps, recurring passwords do nothing to minimize the risk of passwords being captured.

static and one-time passwords. This is incorrect because while one-time passwords will prevent these types of attacks, static passwords do nothing to minimize the risk of passwords being captured.

QUESTION 3

Which of the following is the core of fiber optic cables made of?

A. PVC

B. Glass fibers

C. Kevlar

D. Teflon

Correct Answer: B

Fiber optic cables have an outer insulating jacket made of Teflon or PVC, Kevlar fiber, which helps to strengthen the cable and prevent breakage, plastic coatings, used to cushion the fiber center. The center (core) of the cable is made of glass or plastic fibers. Source: ANDRESS, Mandy, ram CISSP, Coriolis, 2001, Chapter 3: Telecommunications and Network Security (page 31).

QUESTION 4

Which of the following is not one of the three goals of Integrity addressed by the Clark-Wilson model?

A. Prevention of the modification of information by unauthorized users.

B. Prevention of the unauthorized or unintentional modification of information by authorized users.

C. Preservation of the internal and external consistency.

D. Prevention of the modification of information by authorized users.

Correct Answer: A

There is no need to prevent modification from authorized users. They are authorized and allowed to make the changes. On top of this, it is also NOT one of the goal of Integrity within Clark-Wilson.

As it turns out, the Biba model addresses only the first of the three integrity goals which is Prevention of the modification of information by unauthorized users. Clark-Wilson addresses all three goals of integrity.

The ClarkWilson model improves on Biba by focusing on integrity at the transaction level and addressing three major goals of integrity in a commercial environment. In addition to preventing changes by unauthorized subjects, Clark and Wilson realized that high-integrity systems would also have to prevent undesirable changes by authorized subjects and to ensure that the system continued to behave consistently. It also recognized that it would need to ensure that there is constant mediation between every subject and every object if such integrity was going to be maintained.

Integrity is addressed through the following three goals:

1.

Prevention of the modification of information by unauthorized users.

2.

Prevention of the unauthorized or unintentional modification of information by authorized users.

3.

Preservation of the internal and external consistency.

The following reference(s) were used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17689-17694). Auerbach Publications. Kindle Edition.

and KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley and Sons, Page 31.

QUESTION 5

In what way can violation clipping levels assist in violation tracking and analysis?

A. Clipping levels set a baseline for acceptable normal user errors, and violations exceeding that threshold will be recorded for analysis of why the violations occurred.

B. Clipping levels enable a security administrator to customize the audit trail to record only those violations which are deemed to be security relevant.

C. Clipping levels enable the security administrator to customize the audit trail to record only actions for users with access to user accounts with a privileged status.

D. Clipping levels enable a security administrator to view all reductions in security levels which have been made to user accounts which have incurred violations.

Correct Answer: A

Companies can set predefined thresholds for the number of certain types of errors that will be allowed before the activity is considered suspicious. The threshold is a baseline for violation activities that may be normal for a user to commit before alarms are raised. This baseline is referred to as a clipping level.

The following are incorrect answers:

Clipping levels enable a security administrator to customize the audit trail to record only those violations which are deemed to be security relevant. This is not the best answer, you would not record ONLY security relevant violations, all violations would be recorded as well as all actions performed by authorized users which may not trigger a violation. This could allow you to indentify abnormal activities or fraud after the fact.

Clipping levels enable the security administrator to customize the audit trail to record only actions for users with access to user accounts with a privileged status. It could record all security violations whether the user is a normal user or a privileged user.

Clipping levels enable a security administrator to view all reductions in security levels which have been made to user accounts which have incurred violations. The keyword "ALL" makes this question wrong. It may detect SOME but not all of violations. For example, application level attacks may not be detected.

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One uide, 6th Edition (p. 1239). McGraw-Hill. Kindle Edition.

and

TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.