Vendor:ISC

Exam Code:CISSP

Exam Name: Certified Information Systems Security Professional

Version: Demo

QUESTION 1

Which of the following answers BEST describes the Bell La-Padula model of storage and access control of classified information?

A. No read up and No write down

B. No write up, no read down

C. No read over and no write up

D. No reading from higher classification levels

Correct Answer: A

Explanation: The Bell?aPadula model is perhaps the most well-known and significant security model, in addition to being one of the oldest models used in the creation of modern secure computing systems. Like the Trusted Computer System Evaluation Criteria (or TCSEC), it was inspired by early U.S. Department of Defense security policies and the need to prove that confidentiality could be maintained. In other words, its primary goal is to prevent disclosure as the model system moves from one state (one point in time) to another.

In the world of Information Access Controls, there are multipl models, see some of them below:

- Bell La-Padula Model: Works to restrict users from reading data from a higher classification to protect that data. This model is concerned with information security.

- Biba Model: This model means that a user can\\'t write information TO a higher level

- Clark-Wilson Model: This model requires that all data access occur through controlled access programs.

- Information Flow Model: This is concerned with the properties of information flow in both directions, not only in one direction. It requires that each piece of information has unique properties.

- Noninterference Model: This model is intended to ensure that higher-level security functions don\\'t interfere with lower-level operations in an attempt to isolate one from the other. Each are different and suited for different information processing environments.

The following answers are incorrect:

- No write up, no read down: Sorry but this is defines the Biba model of information integrity.

- No read over, no write up: This is an incorrect answer.

- No Reading from higher classification levels: This is incorrect but it is half correct in that data may not be written DOWN to a lower level of classification because it would create something called a spillage where data is leaked out of a more secure area into a less secure one.

The following reference(s) was used to create this question:

2013. Official Security+ Curriculum.

and

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17597-17600). Auerbach Publications. Kindle Edition.

QUESTION 2

A circuit level proxy is _____ when compared to an application level proxy.

A. lower in processing overhead.

B. more difficult to maintain.

C. more secure.

D. slower.

Correct Answer: A

Explanation: Since the circuit level proxy does not anayze the application content of the packet in making its decisions, it has lower overhead than an application level proxy.

"More difficult to maintain" is incorrect. Circuit level proxies are typicall easier to configure and simpler to maintain that an application level proxy.

"More secure" is incorrect. A circuit level proxy is not necessarily more secure than an application layer proxy.

"Slower" is incorrect. Because it is lower in overhead, a circuit level proxy is typically faster than an application level proxy. CBK,pp. 466 - 467 AIO3, pp.488 - 490

QUESTION 3

Why is security an issue when a system is booted into single-user mode?

A. The operating system is started without the security front-end loaded.

B. The users cannot log in to the system, and they will complain.

C. Backup tapes cannot be restored while in single-user mode.

D. Proper forensics cannot be executed while in single-user mode.

Correct Answer: A

The correct answer is "The operating system is started without the security front-end loaded". When the operator boots the system in single-user mode, the user front-end security controls are not loaded. This mode should be used for recovery and maintenance procedures only, and all operations should be logged and audited.

QUESTION 4

Which of the following MUST system and database administrators be aware of and apply when configuring systems used for storing personal employee data?

A. Secondary use of the data by business users

B. The organization\\'s security policies and standards

C. The business purpose for which the data is to be used

D. The overall protection of corporate resources and data

Correct Answer: B

QUESTION 5

Which integrity model defines a constrained data item, an integrity verification procedure and a transformation procedure?

A. The Take-Grant model

B. The Biba integrity model

C. The Clark Wilson integrity model

D. The Bell-LaPadula integrity model

Correct Answer: C

Explanation: The Clark-Wilson model was developed to address security issues in commercial environments. The model uses two categories of mechanisms to realize integrity: well-formed transactions and separation of duty. It defines a constraint data item, a integrity verification and a transformation of that object. A possible way to represent a constraint that only certain trusted programs can modify objects is using application:checksum condition, where the checksum ensures authenticity of the application. Another way is using application:endorser condition, which indicates that a valid certificate, stating that the application has been endorsed by the specified endorser, must be presented. Static separation of duty is enforced by the security administrator when assigning group membership. Dynamic separation of duty enforces control over how permissions are used at the access time

---

QUESTION 6

In an online transaction processing system (OLTP), which of the following actions should be taken when erroneous or invalid transactions are detected?

A. The transactions should be dropped from processing.

B. The transactions should be processed after the program makes adjustments.

C. The transactions should be written to a report and reviewed.

D. The transactions should be corrected and reprocessed.

Correct Answer: C

Explanation: In an online transaction processing system (OLTP) all transactions are recorded as they occur. When erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.

As explained in the ISC2 OIG:

OLTP is designed to record all of the business transactions of an organization as they occur. It is a data processing system facilitating and managing transaction-oriented applications. These are characterized as a system used by many

concurrent users who are actively adding and modifying data to effectively change real-time data.

OLTP environments are frequently found in the finance, telecommunications, insurance, retail, transportation, and travel industries. For example, airline ticket agents enter data in the database in real-time by creating and modifying travel

reservations, and these are increasingly joined by users directly making their own reservations and purchasing tickets through airline company Web sites as well as discount travel Web site portals. Therefore, millions of people may be

accessing the same flight database every day, and dozens of people may be looking at a specific flight at the same time.

The security concerns for OLTP systems are concurrency and atomicity.

Concurrency controls ensure that two users cannot simultaneously change the same data, or that one user cannot make changes before another user is finished with it. In an airline ticket system, it is critical for an agent processing a

reservation to complete the transaction, especially if it is the last seat available on the plane.

Atomicity ensures that all of the steps involved in the transaction complete successfully. If one step should fail, then the other steps should not be able to complete. Again, in an airline ticketing system, if the agent does not enter a name into

the name data field correctly, the transaction should not be able to complete.

OLTP systems should act as a monitoring system and detect when individual processes abort, automatically restart an aborted process, back out of a transaction if necessary, allow distribution of multiple copies of application servers across

machines, and perform dynamic load balancing.

A security feature uses transaction logs to record information on a transaction before it is processed, and then mark it as processed after it is done. If the system fails during the transaction, the transaction can be recovered by reviewing the

transaction logs. Checkpoint restart is the process of using the transaction logs to restart the machine by running through the log to the last checkpoint or good transaction. All transactions following the last checkpoint are applied before

allowing users to access the data again.

Wikipedia has nice coverage on what is OLTP:

Online transaction processing, or OLTP, refers to a class of systems that facilitate and manage transaction-oriented applications, typically for data entry and retrieval transaction processing. The term is somewhat ambiguous; some understand

a "transaction" in the context of computer or database transactions, while others (such as the Transaction Processing Performance Council) define it in terms of business or commercial transactions.

OLTP has also been used to refer to processing in which the system responds immediately to user requests. An automatic teller machine (ATM) for a bank is an example of a commercial transaction processing application.

The technology is used in a number of industries, including banking, airlines, mailorder, supermarkets, and manufacturing. Applications include electronic banking, order processing, employee time clock systems, e-commerce, and eTrading.

There are two security concerns for OLTP system: Concurrency and Atomicity

ATOMICITY

In database systems, atomicity (or atomicness) is one of the ACID transaction properties. In an atomic transaction, a series of database operations either all occur, or nothing occurs. A guarantee of atomicity prevents updates to the database

occurring only partially, which can cause greater problems than rejecting the whole series outright. The etymology of the phrase originates in the Classical Greek concept of a fundamental and indivisible component; see atom.

An example of atomicity is ordering an airline ticket where two actions are required: payment, and a seat reservation. The potential passenger must either:

both pay for and reserve a seat; OR neither pay for nor reserve a seat.

The booking system does not consider it acceptable for a customer to pay for a ticket without securing the seat, nor to reserve the seat without payment succeeding.

CONCURRENCY Database concurrency controls ensure that transactions occur in an ordered fashion. The main job of these controls is to protect transactions issued by different users/applications from the effects of each other. They must preserve the four characteristics of database transactions ACID test: Atomicity, Consistency, Isolation, and Durability. Read http://en.wikipedia.org/wiki/ACID for more details on the ACID test. Thus concurrency control is an essential element for correctness in any system where two database transactions or more, executed with time overlap, can access the same data, e.g., virtually in any general-purpose database system. A well established concurrency control theory exists for database systems: serializability theory, which allows to effectively design and analyze concurrency control methods and mechanisms. Concurrency is not an issue in itself, it is the lack of proper concurrency controls that makes it a serious issue.

The following answers are incorrect:

The transactions should be dropped from processing. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs. The transactions should be processed after the program makes adjustments. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs. The transactions should be corrected and reprocessed. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs. Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 12749-12768). Auerbach Publications. Kindle Edition. and http://en.wikipedia.org/wiki/Online_transaction_processing and http://databases.about.com/od/administration/g/concurrency.htm

---

QUESTION 7

What is the term commonly used to refer to a technique of authenticating one machine to another by forging packets from a trusted source?

A. Man-in-the-Middle (MITM) attack

B. Smurfing

C. Session redirect

D. Spoofing

Correct Answer: D

QUESTION 8

What is the highest amount a company should spend annually on countermeasures for protecting an asset valued at $1,000,000 from a threat that has an annualized rate of occurrence (ARO) of once every five years and an exposure factor (EF) of 30%?

A. $300,000

B. $150,000

C. $60,000

D. $1,500

Correct Answer: C

Explanation: The cost of a countermeasure should not be greater in cost than the risk it mitigates (ALE). For a quantitative risk assessment, the equation is ALE = ARO x SLE where the SLE is calculated as the product of asset value x exposure factor. An event that happen once every five years would have an ARO of .2 (1 divided by 5).

SLE = Asset Value (AV) x Exposure Fact (EF) SLE = 1,000,000 x .30 = 300,000

ALE = SLE x Annualized Rate of Occurance (ARO) ALE = 300,000 x .2 = 60,000

Know your acronyms: ALE -- Annual loss expectancy ARO -- Annual rate of occurrence SLE -- Single loss expectancy

The following are incorrect answers:

$300,000 is incorrect. See the explanation of the correct answer for the correct calculation. $150,000 is incorrect. See the explanation of the correct answer for the correct calculation. $1,500 is incorrect. See the explanation of the correct answer for the correct calculation.

Reference(s) used for this question: Mc Graw Hill, Shon Harris, CISSP All In One (AIO) book, Sixth Edition , Pages 87-88 and Official ISC2 Guide to the CISSP Exam, (OIG), Pages 60-61

QUESTION 9

Which integrity model defines a constrained data item, an integrity verification procedure and a transformation procedure?

A. The Take-Grant model

B. The Biba integrity model

C. The Clark Wilson integrity model

D. The Bell-LaPadula integrity model

Correct Answer: C

Explanation: The Clark Wilson integrity model addresses the three following integrity goals: 1) data is protected from modification by unauthorized users; 2) data is protected from unauthorized modification by authorized users; and 3) data is internally and externally consistent. It also defines a Constrained Data Item (CDI), an Integrity Verification Procedure (IVP), a Transformation Procedure (TP) and an Unconstrained Data item. The Bell-LaPadula and Take-Grant models are not integrity models. 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 5: Security Architecture and Models (page 205).

QUESTION 10

Which authentication technique best protects against hijacking?

A. Static authentication

B. Continuous authentication

C. Robust authentication

D. Strong authentication

Correct Answer: B

Explanation: A continuous authentication provides protection against impostors who can see, alter, and insert information passed between the claimant and verifier even after the claimant/verifier authentication is complete. This is the best protection against hijacking. Static authentication is the type of authentication provided by traditional password schemes and the strength of the authentication is highly dependent on the difficulty of guessing passwords. The robust authentication mechanism relies on dynamic authentication data that changes with each authenticated session between a claimant and a verifier, and it does not protect against hijacking. Strong authentication refers to a two-factor authentication (like something a user knows and something a user is). Source: TIPTON, Harold F. and KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 3: Secured Connections to External Networks (page 51).

QUESTION 11

Whose role is it to assign classification level to information?

A. Security Administrator

B. User

C. Owner

D. Auditor

Correct Answer: C

The Data/Information Owner is ultimately responsible for the protection of the data. It is the Data/Information Owner that decides upon the classifications of that data they are responsible for.

The data owner decides upon the classification of the data he is responsible for and alters that classification if the business need arises.

The following answers are incorrect:

Security Administrator. Is incorrect because this individual is responsible for ensuring that the access right granted are correct and support the polices and directives that the Data/Information Owner defines.

User. Is Incorrect because the user uses/access the data according to how the Data/Information Owner defined their access.

Auditor. Is incorrect because the Auditor is responsible for ensuring that the access levels are appropriate. The Auditor

would verify that the Owner classified the data properly. CISSP All In One Third Edition, Shon Harris, Page 121

QUESTION 12

With RAID Level 5 the spare drives that replace the failed drives are usually hot swappable, meaning the can be replaced on the server while the?

A. System is up and running.

B. System is down and running.

C. System is in-between and running.

D. System is centre and running.

Correct Answer: A

Explanation: This is true, since RAID 5 uses parity to provide fault tolerance through the array, once of the disk in it can become corrupted, and you usually can just take it out without turning off the system (Hot SWAP) and plug a spare disk on the bay. Then the array will automatically begin to reconstruct the information in the new disk with the parity contained through the other disks in the array. This Hot Swap capability is usually present in enterprise servers that require high availability.

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: