Vendor:ISC

Exam Code:SSCP

Exam Name: System Security Certified Practitioner (SSCP)

Version: Demo

QUESTION 1

What does the simple integrity axiom mean in the Biba model?

A. No write down

B. No read down

C. No read up

D. No write up

Correct Answer: B

The simple integrity axiom of the Biba access control model states that a subject at one level of integrity is not permitted to observe an object of a lower integrity (no read down).

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 Architectures and Models (page 205).

QUESTION 2

Which of the following issues is not addressed by digital signatures?

A. nonrepudiation

B. authentication

C. data integrity

D. denial-of-service

Correct Answer: D

A digital signature directly addresses both confidentiality and integrity of the CIA triad. It does not directly address availability, which is what denial-of-service attacks.

The other answers are not correct because:

"nonrepudiation" is not correct because a digital signature can provide for nonrepudiation.

"authentication" is not correct because a digital signature can be used as an authentication mechanism

"data integrity" is not correct because a digital signature does verify data integrity (as part of nonrepudiation)

References:

Official ISC2 Guide page: 227 and 265

All in One Third Edition page: 648

QUESTION 3

What does "residual risk" mean?

A. The security risk that remains after controls have been implemented

B. Weakness of an assets which can be exploited by a threat

C. Risk that remains after risk assessment has has been performed

D. A security risk intrinsic to an asset being audited, where no mitigation has taken place.

Correct Answer: A

Residual risk is "The security risk that remains after controls have been implemented" ISO/IEC TR 13335-1 Guidelines for the Management of IT Security (GMITS), Part 1: Concepts and Models for IT Security, 1996. "Weakness of an assets which can be exploited by a threat" is vulnerability. "The result of unwanted incident" is impact. Risk that remains after risk analysis has been performed is a distracter.

Risk can never be eliminated nor avoided, but it can be mitigated, transferred or accpeted. Even after applying a countermeasure like for example putiing up an Antivirus. But still it is not 100% that systems will be protected by antivirus.

QUESTION 4

As per RFC 1122, which of the following is not a defined layer in the DoD TCP/IP protocol model?

A. Application layer

B. Session layer

C. Internet layer

D. Link/Network Access Layer

Correct Answer: B

As per RFC, The DoD TCP/IP protocol model defines four layers, with the layers having names, not

numbers, as follows:

Application (process-to-process) Layer:

This is the scope within which applications create user data and communicate this data to other processes

or applications on another or the same host. The communications partners are often called peers. This is

where the "higher level" protocols such as SMTP, FTP, SSH, HTTP, etc.

operate.

Transport (host-to-host) Layer:

The Transport Layer constitutes the networking regime between two network hosts, either on the local

network or on remote networks separated by routers. The Transport Layer provides a uniform networking interface that hides the actual topology (layout) of the underlying network connections. This is where flow-control, error-correction, and connection protocols exist, such as TCP. This layer deals with opening and maintaining connections between internet hosts.

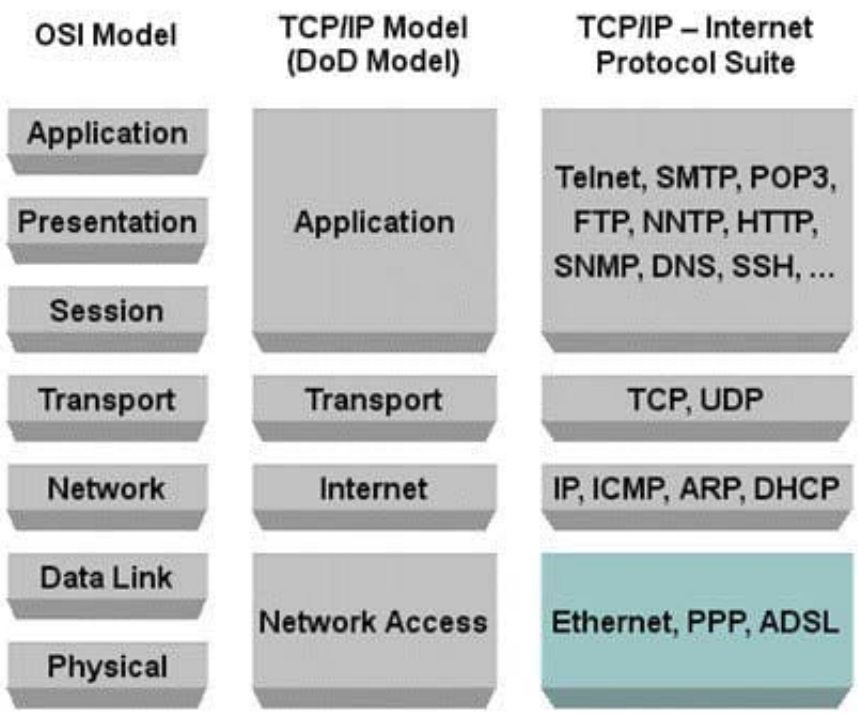
Internet (internetworking) Layer:

The Internet Layer has the task of exchanging datagrams across network boundaries. It is therefore also referred to as the layer that establishes internetworking; indeed, it defines and establishes the Internet. This layer defines the addressing and routing structures used for the TCP/IP protocol suite. The primary protocol in this scope is the Internet Protocol, which defines IP addresses. Its function in routing is to transport datagrams to the next IP router that has the connectivity to a network closer to the final data destination.

Link (network access) Layer:

This layer defines the networking methods with the scope of the local network link on which hosts communicate without intervening routers. This layer describes the protocols used to describe the local network topology and the interfaces needed to affect transmission of Internet Layer datagrams to next-neighbor hosts.

The DoD tcp/ip model DoD model Osi Model



Graphic above from: http://bit.kuas.edu.tw/

REALITY VERSUS THE STANDARD

In real life today, this is getting very confusing. Many books and references will not use exactly the same names as the initial RFC that was published. For example, the Link layer is often times called Network Access. The same applies with Transport which is often times called Host-to- Host and vice versa.

The following answer is incorrect:

The session layer is defined within the OSI/ISO model but not within the DOD model. Being incorrect it made it the best answer according to the question. It does not belong to the DoD TCP/IP Model.

Reference(s) Used for this question:

http://www.freesoft.org/CIE/RFC/1122/

http://bit.kuas.edu.tw/~csshieh/teach/np/tcpip/

QUESTION 5

Which of the following teams should NOT be included in an organization\\'s contingency plan?

A. Damage assessment team

B. Hardware salvage team

C. Tiger team

D. Legal affairs team

Correct Answer: C

According to NIST\\'s Special publication 800-34, a capable recovery strategy will require some or all of the following functional groups: Senior management official, management team, damage assessment team, operating system administration team, systems software team, server recovery team, LAN/WAN recovery team, database recovery team, network operations recovery team, telecommunications team, hardware salvage team, alternate site recovery coordination team, original site restoration/salvage coordination team, test team, administrative support team, transportation and relocation team, media relations team, legal affairs team, physical/personal security team, procurements team. Ideally, these teams would be staffed with the personnel responsible for the same or similar operation under normal conditions. A tiger team, originally a U.S. military jargon term, defines a team (of sneakers) whose purpose is to penetrate security, and thus test security measures. Used today for teams performing ethical hacking.

Source: SWANSON, Marianne, and al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 23).

QUESTION 6

After a company is out of an emergency state, what should be moved back to the original site first?

A. Executives

B. Least critical components

C. IT support staff

D. Most critical components

Correct Answer: B

This will expose any weaknesses in the plan and ensure the primary site has been properly repaired before moving back. Moving critical assets first may induce a second disaster if the primary site has not been repaired properly.

The first group to go back would test items such as connectivity, HVAC, power, water, improper procedures, and/or steps that has been overlooked or not done properly. By moving these first, and fixing any problems identified, the critical operations of the company are not negatively affected.

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

9: Disaster Recovery and Business continuity (page 621).

QUESTION 7

Which of the following is the act of performing tests and evaluations to test a system\\'s security level to see if it complies with the design specifications and security requirements?

A. Validation

B. Verification

C. Assessment

D. Accuracy

Correct Answer: B

Verification vs. Validation:

Verification determines if the product accurately represents and meets the specifications. A product can be developed that does not match the original specifications. This step ensures that the specifications are properly met.

Validation determines if the product provides the necessary solution intended real-world problem. In large projects, it is easy to lose sight of overall goal. This exercise ensures that the main goal of the project is met.

From DITSCAP:

6.3.2. Phase 2, Verification. The Verification phase shall include activities to verify compliance of the system with previously agreed security requirements. For each life-cycle development activity, DoD Directive 5000.1 (reference (i)), there is a corresponding set of security activities, enclosure 3, that shall verify compliance with the security requirements and evaluate vulnerabilities.

6.3.3. Phase 3, Validation. The Validation phase shall include activities to evaluate the fully integrated system to validate system operation in a specified computing environment with an acceptable level of residual risk. Validation shall culminate in an approval to operate.

You must also be familiar with Verification and Validation for the purpose of the exam. A simple definition for Verification would be whether or not the developers followed the design specifications along with the security requirements. A simple definition for Validation would be whether or not the final product meets the end user needs and can be use for a specific purpose.

Wikipedia has an informal description that is currently written as: Validation can be expressed by the query "Are you building the right thing?" and Verification by "Are you building it right? NOTE:

DITSCAP was replaced by DIACAP some time ago (2007). While DITSCAP had defined both a verification and a validation phase, the DIACAP only has a validation phase. It may not make a difference in the answer for the exam; however, DIACAP is the cornerstone policy of DOD CandA and IA efforts today. Be familiar with both terms just in case all of a sudden the exam becomes updated with the new term.

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One uide, 6th Edition (p. 1106). McGraw-Hill. Kindle Edition.

http://iase.disa.mil/ditscap/DITSCAP.html

https://en.wikipedia.org/wiki/Verification_and_validation

For the definition of "validation" in DIACAP, Click Here

Further sources for the phases in DIACAP, Click Here

QUESTION 8

Which conceptual approach to intrusion detection system is the most common?

A. Behavior-based intrusion detection

B. Knowledge-based intrusion detection

C. Statistical anomaly-based intrusion detection

D. Host-based intrusion detection

Correct Answer: B

There are two conceptual approaches to intrusion detection. Knowledge-based intrusion detection uses a database of known vulnerabilities to look for current attempts to exploit them on a system and trigger an alarm if an attempt is found. The other approach, not as common, is called behaviour-based or statistical analysis-based. A host-based intrusion detection system is a common implementation of intrusion detection, not a conceptual approach.

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 3: Telecommunications and Network Security (page 63).

Also: HARRIS, Shon, All-In-One CISSP Certification uide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 193-194).

QUESTION 9

Which access control model would a lattice-based access control model be an example of?

A. Mandatory access control.

B. Discretionary access control.

C. Non-discretionary access control.

D. Rule-based access control.

Correct Answer: A

In a lattice model, there are pairs of elements that have the least upper bound of values and greatest lower bound of values. In a Mandatory Access Control (MAC) model, users and data owners do not have as much freedom to determine who can access files.

TIPS FROM CLEMENT

Mandatory Access Control is in place whenever you have permissions that are being imposed on the subject and the subject cannot arbitrarily change them. When the subject/owner of the file can change permissions at will, it is discretionary access control. Here is a breakdown largely based on explanations provided by Doug Landoll. I am reproducing below using my own word and not exactly how Doug explained it:

FIRST: The Lattice

A lattice is simply an access control tool usually used to implement Mandatory Access Control (MAC) and it could also be used to implement RBAC but this is not as common. The lattice model can be used for Integrity level or file permissions as well. The lattice has a least upper bound and greatest lower bound. It makes use of pair of elements such as the subject security clearance pairing with the object sensitivity label.

SECOND: DAC (Discretionary Access Control)

Let\\'s get into Discretionary Access Control: It is an access control method where the owner (read the creator of the object) will decide who has access at his own discretion. As we all know, users are sometimes insane. They will share their files with other users based on their identity but nothing prevent the user from further sharing it with other users on the network. Very quickly you loose control on the flow of information and who has access to what. It is used in small and friendly environment where a low level of security is all that is required.

THIRD: MAC (Mandatory Access Control)

All of the following are forms of Mandatory Access Control:

Mandatory Access control (MAC) (Implemented using the lattice)

You must remember that MAC makes use of Security Clearance for the subject and also Labels will be assigned to the objects. The clearance of the Subject must dominate (be equal or higher) the clearance of the Object being accessed. The label attached to the object will indicate the sensitivity leval and the categories the object belongs to. The categories are used to implement the Need to Know. All of the following are forms of Non Discretionary Access Control:

Role Based Access Control (RBAC)

Rule Based Access Control (Think Firewall in this case)

The official ISC2 book says that RBAC (synonymous with Non Discretionary Access Control) is a form of DAC but they are simply wrong. RBAC is a form of Non Discretionary Access Control. Non Discretionary DOES NOT equal mandatory access control as there is no labels and clearance involved.

I hope this clarifies the whole drama related to what is what in the world of access control.

In the same line of taught, you should be familiar with the difference between Explicit permission (the user has his own profile) versus Implicit (the user inherit permissions by being a member of a role for example).

The following answers are incorrect:

Discretionary access control. Is incorrect because in a Discretionary Access Control (DAC) model, access is restricted based on the authorization granted to the users. It is identity based access control only. It does not make use of a lattice.

Non-discretionary access control. Is incorrect because Non-discretionary Access Control (NDAC) uses the role-based access control method to determine access rights and permissions. It is often times used as a synonym to RBAC which is Role Based Access Control. The user inherit permission from the role when they are assigned into the role. This type of access could make use of a lattice but could also be implemented without the use of a lattice in some case. Mandatory Access Control was a better choice than this one, but RBAC could also make use of a lattice. The BEST answer was MAC. Rule-based access control. Is incorrect because it is an example of a Non-discretionary Access Control (NDAC) access control mode. You have rules that are globally applied to all users. There is no such thing as a lattice being use in Rule-Based Access Control.

References:

AIOv3 Access Control (pages 161 - 168)

AIOv3 Security Models and Architecture (pages 291 - 293)

QUESTION 10

Which of the following is NOT a compensating measure for access violations?

A. Backups

B. Business continuity planning

C. Insurance

D. Security awareness

Correct Answer: D

Security awareness is a preventive measure, not a compensating measure for access violations.

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 2: Access control systems (page 50).

QUESTION 11

The Orange Book states that "Hardware and software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB [Trusted Computing Base]." This statement is the formal requirement for:

A. Security Testing.

B. Design Verification.

C. System Integrity.

D. System Architecture Specification.

Correct Answer: C

This is a requirement starting as low as C1 within the TCSEC rating.

The Orange book requires the following for System Integrity Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

NOTE FROM CLEMENT:

This is a question that confuses a lot of people because most people take for granted that the orange book with its associated Bell LaPadula model has nothing to do with integrity. However you have to be careful about the context in which the word integrity is being used. You can have Data Integrity and you can have System Integrity which are two completely different things.

Yes, the Orange Book does not specifically address the Integrity requirements, however it has to run on top of systems that must meet some integrity requirements.

This is part of what they call operational assurance which is defined as a level of confidence of a trusted system\\'s architecture and implementation that enforces the system\\'s security policy. It includes:

System architecture

Covert channel analysis

System integrity Trusted recovery DATA INTEGRITY Data Integrity is very different from System Integrity. When you have integrity of the data, there are three goals:

1.

Prevent authorized users from making unauthorized modifications

2.

Preven unauthorized users from making modifications

3.

Maintaining internal and external consistancy of the data Bell LaPadula which is based on the Orange Book address does not address Integrity, it addresses only

Confidentiality.

Biba address only the first goal of integrity.

Clark-Wilson addresses the three goals of integrity.

In the case of this question, there is a system integrity requirement within the TCB. As mentioned above

here is an extract of the requirements: Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

The following answers are incorrect:

Security Testing. Is incorrect because Security Testing has no set of requirements in the Orange book.

Design Verification. Is incorrect because the Orange book\\'s requirements for Design Verification include: A

formal model of the security policy must be clearly identified and documented, including a mathematical

proof that the model is consistent with its axioms and is sufficient to support the security policy. System Architecture Specification. Is incorrect because there are no requirements for System Architecture Specification in the Orange book.

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

Trusted Computer Security Evaluation Criteria (TCSEC), DoD 5200.28-STD, page 15, 18, 25, 31, 40, 50.

Harris, Shon (2012-10-25). CISSP All-in-One uide, 6th Edition, Security Architecture and Design,

Page 392-397, for users with the Kindle Version see Kindle Locations 28504- 28505. and DOD TCSEC - http://www.cerberussystems.com/INFOSEC/stds/d520028.htm

---

QUESTION 12

Which of the following is not a security goal for remote access?

A. Reliable authentication of users and systems

B. Protection of confidential data

C. Easy to manage access control to systems and network resources

D. Automated login for remote users

Correct Answer: D

An automated login function for remote users would imply a weak authentication, thus certainly not a security goal.

Source: TIPTON, Harold F. and KRAUSE, Micki, Information Security Management Handbook, 4th edition, volume 2, 2001, CRC Press, Chapter 5: An Introduction to Secure Remote Access (page 100).