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.pass2lead.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 of the following would MOST likely ensure that a system development project meets business objectives?

A. Development and tests are run by different individuals

B. User involvement in system specification and acceptance

C. Development of a project plan identifying all development activities

D. Strict deadlines and budgets

Correct Answer: B

Effective user involvement is the most critical factor in ensuring that the application meets business objectives.

A great way of getting early input from the user community is by using Prototyping. The prototyping method was formally introduced in the early 1980s to combat the perceived weaknesses of the waterfall model with

regard to the speed of development. The objective is to build a simplified version (prototype) of the

application, release it for review, and use the feedback from the users\\' review to build a second, better

version.

This is repeated until the users are satisfied with the product. t is a four-step process:

initial concept,

design and implement initial prototype,

refine prototype until acceptable, and

complete and release final version.

There is also the Modified Prototype Model (MPM. This is a form of prototyping that is ideal for Web

application development. It allows for the basic functionality of a desired system or component to be

formally deployed in a quick time frame. The maintenance phase is set to begin after the deployment. The

goal is to have the process be flexible enough so the application is not based on the state of the

organization at any given time. As the organization grows and the environment changes, the application

evolves with it, rather than being frozen in time.

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 Locations 12101-12108 and 12099-12101). Auerbach Publications.

Kindle Edition.

and

Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review

manual, chapter 6: Business Application System Development, Acquisition, Implementation and

Maintenance (page 296).

QUESTION 2

In the UTP category rating, the tighter the wind:

A. the higher the rating and its resistance against interference and crosstalk.

B. the slower the rating and its resistance against interference and attenuation.

C. the shorter the rating and its resistance against interference and attenuation.

D. the longer the rating and its resistance against interference and attenuation.

Correct Answer: A

The category rating is based on how tightly the copper cable is wound within the shielding: The tighter the wind, the higher the rating and its resistance against interference and crosstalk. Twisted pair copper cabling is a form of wiring in which two conductors are wound together for the purposes of canceling out electromagnetic interference (EMI) from external sources and crosstalk from neighboring wires. Twisting wires decreases interference because the loop area between the wires (which determines the magnetic coupling into the signal) is reduced. In balanced pair operation, the two wires typically carry equal and opposite signals (differential mode) which are combined by subtraction at the destination. The noise from the two wires cancel each other in this subtraction because the two wires have been exposed to similar EMI.

The twist rate (usually defined in twists per metre) makes up part of the specification for a given type of cable. The greater the number of twists, the greater the attenuation of crosstalk. Where pairs are not twisted, as in most residential interior telephone wiring, one member of the pair may be closer to the source than the other, and thus exposed to slightly different induced EMF.

Reference:

KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley and Sons, Page 101.

and

http://www.consultants-online.co.za/pub/itap_101/html/ch04s05.html

QUESTION 3

Which of the following is used by RADIUS for communication between clients and servers?

A. TCP

B. SSL

C. UDP

D. SSH

Correct Answer: C

Source: TIPTON, Harold F. and KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Page 33.

QUESTION 4

Which of the following refers to the data left on the media after the media has been erased?

A. remanence

B. recovery

C. sticky bits

D. semi-hidden

Correct Answer: A

Actually the term "remanence" comes from electromagnetism, the study of the electromagnetics. Originally referred to (and still does in that field of study) the magnetic flux that remains in a magnetic circuit after an applied magnetomotive force has been removed. Absolutely no way a candidate will see anywhere near that much detail on any similar CISSP question, but having read this, a candidate won\\'t be likely to forget it either.

It is becoming increasingly commonplace for people to buy used computer equipment, such as a hard drive, or router, and find information on the device left there by the previous owner; information they thought had been deleted. This is a classic example of data remanence: the remains of partial or even the entire data set of digital information. Normally, this refers to the data that remain on media after they are written over or degaussed. Data remanence is most common in storage systems but can also occur in memory.

Specialized hardware devices known as degaussers can be used to erase data saved to magnetic media. The measure of the amount of energy needed to reduce the magnetic field on the media to zero is known as coercivity.

It is important to make sure that the coercivity of the degausser is of sufficient strength to meet object reuse requirements when erasing data. If a degausser is used with insufficient coercivity, then a remanence of the data will exist. Remanence is the measure of the existing magnetic field on the media; it is the residue that remains after an object is degaussed or written over.

Data is still recoverable even when the remanence is small. While data remanence exists, there is no assurance of safe object reuse.

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 Locations 4207-4210). Auerbach Publications. Kindle Edition.

and Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 19694-19699). Auerbach Publications. Kindle Edition.

QUESTION 5

If an operating system permits shared resources such as memory to be used sequentially by multiple users/application or subjects without a refresh of the objects/memory area, what security problem is MOST likely to exist?

A. Disclosure of residual data.

B. Unauthorized obtaining of a privileged execution state.

C. Data leakage through covert channels.

D. Denial of service through a deadly embrace.

Correct Answer: A

Allowing objects to be used sequentially by multiple users without a refresh of the objects can lead to disclosure of residual data. It is important that steps be taken to eliminate the chance for the disclosure of residual data.

Object reuse refers to the allocation or reallocation of system resources to a user or, more appropriately, to an application or process. Applications and services on a computer system may create or use objects in memory and in storage to perform programmatic functions. In some cases, it is necessary to share these resources between various system applications. However, some objects may be employed by an application to perform privileged tasks on behalf of an authorized user or upstream application. If object usage is not controlled or the data in those objects is not erased after use, they may become available to unauthorized users or processes. Disclosure of residual data and Unauthorized obtaining of a privileged execution state are both a problem with shared memory and resources. Not clearing the heap/stack can result in residual data and may also allow the user to step on somebody\\'s session if the security token/ identify was maintained in that space. This is generally more malicious and intentional than accidental though. The MOST common issue would be Disclosure of residual data.

The following answers are incorrect: Unauthorized obtaining of a privileged execution state. Is incorrect because this is not a problem with Object Reuse.

Data leakage through covert channels. Is incorrect because it is not the best answer. A covert channel is a communication path. Data leakage would not be a problem created by Object Reuse. In computer security, a covert channel is a type of computer security attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy. The term, originated in 1973 by Lampson is defined as "(channels) not intended for information transfer at all, such as the service program\\'s effect on system load." to distinguish it from Legitimate channels that are subjected to access controls by COMPUSEC.

Denial of service through a deadly embrace. Is incorrect because it is only a detractor.

References:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 4174-4179). Auerbach Publications. Kindle Edition.

and

https://www.fas.org/irp/nsa/rainbow/tg018.htm

and

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

QUESTION 6

Which of the following is NOT an advantage that TACACS+ has over TACACS?

A. Event logging

B. Use of two-factor password authentication

C. User has the ability to change his password

D. Ability for security tokens to be resynchronized

Correct Answer: A

Although TACACS+ provides better audit trails, event logging is a service that is provided with TACACS. 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 121).

QUESTION 7

Which of the following would be the best criterion to consider in determining the classification of an information asset?

A. Value

B. Age

C. Useful life

D. Personal association

Correct Answer: A

Information classification should be based on the value of the information to the organization and its sensitivity (reflection of how much damage would accrue due to disclosure).

Age is incorrect. While age might be a consideration in some cases, the guiding principles should be value and sensitivity.

Useful life. While useful lifetime is relevant to how long data protections should be applied, the classification is based on information value and sensitivity.

Personal association is incorrect. Information classification decisions should be based on value of the information and its sensitiviry.

References

CBK, pp. 101 - 102.

QUESTION 8

Which of the following is the LEAST user accepted biometric device?

A. Fingerprint

B. Iris scan

C. Retina scan

D. Voice verification

Correct Answer: C

The biometric device that is least user accepted is the retina scan, where a system scans the blood-vessel pattern on the backside of the eyeball. When using this device, an individual has to place their eye up to a device, and may require a puff of air to be blown into the eye. The iris scan only needs for an individual to glance at a camera that could be placed above a door.

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

4: Access Control (page 131).

QUESTION 9

What is the primary role of smartcards in a PKI?

A. Transparent renewal of user keys

B. Easy distribution of the certificates between the users

C. Fast hardware encryption of the raw data

D. Tamper resistant, mobile storage and application of private keys of the users

Correct Answer: D

Reference: HARRIS, Shon, All-In-One CISSP Certification uide, 2001, McGraw- Hill/Osborne, page 139;

SNYDER, J., What is a SMART CARD?.

Wikipedia has a nice definition at: http://en.wikipedia.org/wiki/Tamper_resistance

Security

Tamper-resistant microprocessors are used to store and process private or sensitive information, such as private keys or electronic money credit. To prevent an attacker from retrieving or modifying the information, the chips are designed so that the information is not accessible through external means and can be accessed only by the embedded software, which should contain the appropriate security measures. Examples of tamper-resistant chips include all secure cryptoprocessors, such as the IBM 4758 and chips used in smartcards, as well as the Clipper chip.

It has been argued that it is very difficult to make simple electronic devices secure against tampering, because numerous attacks are possible, including:

physical attack of various forms (microprobing, drills, files, solvents, etc.)

freezing the device

applying out-of-spec voltages or power surges

applying unusual clock signals

inducing software errors using radiation measuring the precise time and power requirements of certain operations (see power analysis)

Tamper-resistant chips may be designed to zeroise their sensitive data (especially cryptographic keys) if they detect penetration of their security encapsulation or out-of-specification environmental parameters. A chip may even be rated for "cold zeroisation", the ability to zeroise itself even after its power supply has been crippled.

Nevertheless, the fact that an attacker may have the device in his possession for as long as he likes, and perhaps obtain numerous other samples for testing and practice, means that it is practically impossible to totally eliminate tampering by a sufficiently motivated opponent. Because of this, one of the most important elements in protecting a system is overall system design. In particular, tamper-resistant systems should "fail gracefully" by ensuring that compromise of one device does not compromise the entire system. In this manner, the attacker can be practically restricted to attacks that cost less than the expected return from compromising a single device (plus, perhaps, a little more for kudos). Since the most sophisticated attacks have been estimated to cost several hundred thousand dollars to carry out, carefully designed systems may be invulnerable in practice.

QUESTION 10

What physical characteristic does a retinal scan biometric device measure?

A. The amount of light reaching the retina

B. The amount of light reflected by the retina

C. The pattern of light receptors at the back of the eye

D. The pattern of blood vessels at the back of the eye

Correct Answer: D

The retina, a thin nerve (1/50th of an inch) on the back of the eye, is the part of the eye which senses light

and transmits impulses through the optic nerve to the brain - the equivalent of film in a camera. Blood

vessels used for biometric identification are located along the neural retina, the outermost of retina\\'s four

cell layers.

The following answers are incorrect:

The amount of light reaching the retina The amount of light reaching the retina is not used in the biometric

scan of the retina.

The amount of light reflected by the retina The amount of light reflected by the retina is not used in the

biometric scan of the retina.

The pattern of light receptors at the back of the eye This is a distractor

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

Reference: Retina Scan Technology.

ISC2 Official Guide to the CBK, 2007 (Page 161)

QUESTION 11

Which of the following best describes remote journaling?

A. Send hourly tapes containing transactions off-site.

B. Send daily tapes containing transactions off-site.

C. Real-time capture of transactions to multiple storage devices.

D. Real time transmission of copies of the entries in the journal of transactions to an alternate site.

Correct Answer: D

Remote Journaling is a technology to facilitate sending copies of the journal of transaction entries from a production system to a secondary system in realtime. The remote nature of such a connection is predicated upon having local journaling already established. Local journaling on the production side allows each change that ensues for a journal-eligible object e.g., database physical file, SQL table, data area, data queue, byte stream file residing within the IFS) to be recorded and logged. It\\'s these local images that flow to the remote system. Once there, the journal entries serve a variety of purposes, from feeding a high availability software replay program or data warehouse to offering an offline, realtime vault of the most recent database changes.

Reference(s) used for this question:

The Essential Guide to Remote Journaling by IBM

and

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

and KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley and Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 286).

QUESTION 12

Which of the following is not a property of the Rijndael block cipher algorithm?

A. It employs a round transformation that is comprised of three layers of distinct and invertible transformations.

B. It is suited for high speed chips with no area restrictions.

C. It operates on 64-bit plaintext blocks and uses a 128 bit key.

D. It could be used on a smart card.

Correct Answer: C

All other properties above apply to the Rijndael algorithm, chosen as the AES standard to replace DES.

The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt

data in blocks of 128 bits. Rijndael was designed to handle additional block sizes and key lengths, however they are not adopted in the AES standard.

IDEA cipher algorithm operates on 64-bit plaintext blocks and uses a 128 bit key.

Reference(s) used for this question:

http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

and

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

QUESTION 13

What does the (star) integrity axiom mean in the Biba model?

A. No read up

B. No write down

C. No read down D. No write up

Correct Answer: D

The (star) integrity axiom of the Biba access control model states that an object at one level of integrity is not permitted to modify an object of a higher level of integrity (no write up). 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 14

Which of the following services is NOT provided by the digital signature standard (DSS)?

A. Encryption

B. Integrity

C. Digital signature

D. Authentication

Correct Answer: A

DSS provides Integrity, digital signature and Authentication, but does not provide Encryption.

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 160).

QUESTION 15

Secure Electronic Transaction (SET) and Secure HTTP (S-HTTP) operate at which layer of the OSI model?

A. Application Layer.

B. Transport Layer.

C. Session Layer.

D. Network Layer.

Correct Answer: A

The Secure Electronic Transaction (SET) and Secure HTTP (S-HTTP) operate at the Application Layer of the Open Systems Interconnect (OSI) model.

Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley and Sons, Page 89.