Free SSCP Exam Braindumps certification guide Q&A [Q49-Q69

Free SSCP Exam Braindumps certification guide Q&A
SSCP Certification Overview Latest SSCP PDF Dumps

Conclusion

Becoming an (ISC)2 Systems Security Certified Practitioner is a matter of checking the exam blueprint carefully and understanding what's expected from you. Passing the certification exam from the first attempt is achievable as long as the candidates enroll in (ISC)2 official training sessions and check the study guides available on Amazon along with other reliable sources.

The common mistakes made on the SSCP exam by candidates would be:

Not knowing how to respond to certain questions and guessing their responses. Guessing and guessing until it's too late, and guessing all the way up to the point where they know they are incorrect. Dressing inappropriately for the experience. The common mistakes here can be made by bringing inappropriate materials like cheat sheets and books during the exam. However, it's safe to take a copy of the syllabus and other documents that you can look at anytime you want during your exam. You can keep these in a folder and bring it with you using an organizer to avoid any trouble. Not knowing what to expect. Having anxiety and fear that they wouldn't pass because of their background especially if they've only been in IT for less than two years. Not preparing themselves physically and emotionally. By leaving the test center early before others, thus giving them less time to review their answers. Skipping questions. Not having the right training.
On the other hand, people who pass the exam by preparing themselves with **SSCP Dumps** would be able to answer questions

confidently. Rather than having doubts about their answers; they could feel that they are right about their responses because of what they learned during training. They know what to expect and understand how difficult it is to pass these exams because of all the things they learned from their teachers who are ISC certified security professionals.

QUESTION 49

What is called the use of technologies such as fingerprint, retina, and iris scans to authenticate the individuals requesting access to resources?
* Micrometrics
* Macrometrics
* Biometrics
* MicroBiometrics

Explanation/Reference:

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 35.

QUESTION 50

Which of the following can prevent hijacking of a web session?
* RSA
* SET
* SSL
* PPP

The Secure Socket Layer (SSL) protocol is used between a web server and client and provides entire session encryption, thus preventing from session hijacking. RSA is asymmetric encryption algorithm that can be used in setting up a SSL session. SET is the Secure Electronic Transaction protocol that was introduced by Visa and Mastercard to allow for more credit card transaction possibilities. PPP is a point-to-point protocol. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 89).

QUESTION 51

The typical computer fraudsters are usually persons with which of the following characteristics?
* They have had previous contact with law enforcement
* They conspire with others
* They hold a position of trust
* They deviate from the accepted norms of society

Explanation/Reference:

These people, as employees, are trusted to perform their duties honestly and not take advantage of the trust placed in them.

The following answers are incorrect:

They have had previous contact with law enforcement. Is incorrect because most often it is a person that holds a position of trust and this answer implies they have a criminal background. This type of individual is typically not in a position of trust within an organization.

They conspire with others. Is incorrect because they typically work alone, often as a form of retribution over a percieved injustice done to them.

They deviate from the accepted norms of society. Is incorrect because while the nature of fraudsters deviate from the norm, the fraudsters often hold a position of trust within the organization.

QUESTION 52

_____, _____, and _____ are required to successfully complete a crime.
(Choose three)
* Root kit
* Motive
* Buffer Overflow
* Means
* Opportunity
* Advantage

Means, motive, and opportunity are the three items needed to commit a crime.

QUESTION 53

Which of the following best allows risk management results to be used knowledgeably?
* A vulnerability analysis
* A likelihood assessment
* An uncertainty analysis
* A threat identification

Explanation/Reference:

Risk management consists of two primary and one underlying activity; risk assessment and risk mitigation are the primary activities and uncertainty analysis is the underlying one. After having performed risk assessment and mitigation, an uncertainty analysis should be performed. Risk management must often rely on speculation, best guesses, incomplete data, and many unproven assumptions. A documented uncertainty analysis allows the risk management results to be used knowledgeably. A vulnerability analysis, likelihood assessment and threat identification are all parts of the collection and analysis of data part of the risk assessment, one of the primary activities of risk management.

Source: SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (pages 19-21).

QUESTION 54

IT security measures should:
* Be complex
* Be tailored to meet organizational security goals.
* Make sure that every asset of the organization is well protected.
* Not be developed in a layered fashion.

Section: Security Operation Adimnistration

Explanation/Reference:

In general, IT security measures are tailored according to an organization’s unique needs. While numerous factors, such as the overriding mission requirements, and guidance, are to be considered, the fundamental issue is the protection of the mission or business from IT security-related, negative impacts. Because IT security needs are not uniform, system designers and security practitioners should consider the level of trust when connecting to other external networks and internal sub-domains. Recognizing

the uniqueness of each system allows a layered security strategy to be used – implementing lower assurance solutions with lower costs to protect less critical systems and higher assurance solutions only at the most critical areas.

The more complex the mechanism, the more likely it may possess exploitable flaws. Simple mechanisms tend to have fewer exploitable flaws and require less maintenance. Further, because configuration management issues are simplified, updating or replacing a simple mechanism becomes a less intensive process.

Security designs should consider a layered approach to address or protect against a specific threat or to reduce a vulnerability. For example, the use of a packet-filtering router in conjunction with an application gateway and an intrusion detection system combine to increase the work-factor an attacker must expend to successfully attack the system. Adding good password controls and adequate user training improves the system’s security posture even more.

The need for layered protections is especially important when commercial-off-the-shelf (COTS) products are used. Practical experience has shown that the current state-of-the-art for security quality in COTS products does not provide a high degree of protection against sophisticated attacks. It is possible to help mitigate this situation by placing several controls in series, requiring additional work by attackers to accomplish their goals.

Source: STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (pages 9-10).

QUESTION 55

Which of the following rules pertaining to a Business Continuity Plan/Disaster Recovery Plan is incorrect?
* In order to facilitate recovery, a single plan should cover all locations.
* There should be requirements to form a committee to decide a course of action. These decisions should be made ahead of time and incorporated into the plan.
* In its procedures and tasks, the plan should refer to functions, not specific individuals.
* Critical vendors should be contacted ahead of time to validate equipment can be obtained in a timely manner.

Explanation/Reference:

The first documentation rule when it comes to a BCP/DRP is “one plan, one building”. Much of the plan revolves around reconstructing a facility and replenishing it with production contents. If more than one facility is involved, then the reader of the plan will find it difficult to identify quantities and specifications of replacement resource items. It is possible to have multiple plans for a single building, but those plans must be linked so that the identification and ordering of resource items is centralized. All other statements are correct.

Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 162).

QUESTION 56

What can be described as an imaginary line that separates the trusted components of the TCB from those elements that are NOT trusted?
* The security kernel
* The reference monitor
* The security perimeter
* The reference perimeter

Explanation/Reference:

The security perimeter is the imaginary line that separates the trusted components of the kernel and the Trusted Computing Base

(TCB) from those elements that are not trusted. The reference monitor is an abstract machine that mediates all accesses to objects by subjects. The security kernel can be software, firmware or hardware components in a trusted system and is the actual instantiation of the reference monitor. The reference perimeter is not defined and is a distracter.

Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

QUESTION 57

:Which of the following is considered the LEAST secure?
* Confidential
* Public
* Private
* Sensitive

The order of classification from highest to lowest is: Sensitive, Confidential, Private, and Public. Review NIST Special Publication 800-26 for more details about information classifications.

QUESTION 58

Why should batch files and scripts be stored in a protected area?
* Because of the least privilege concept.
* Because they cannot be accessed by operators.
* Because they may contain credentials.
* Because of the need-to-know concept.

Section: Access Control

Explanation/Reference:

Because scripts contain credentials, they must be stored in a protected area and the transmission of the scripts must be dealt with carefully. Operators might need access to batch files and scripts. The least privilege concept requires that each subject in a system be granted the most restrictive set of privileges needed for the performance of authorized tasks. The need-to-know principle requires a user having necessity for access to, knowledge of, or possession of specific information required to perform official tasks or services.

Source: WALLHOFF, John, CISSP Summary 2002, April 2002, CBK#1 Access Control System & Methodology (page 3)

QUESTION 59

The Information Technology Security Evaluation Criteria (ITSEC) was written to address which of the following that the Orange Book did not address?
* integrity and confidentiality.
* confidentiality and availability.
* integrity and availability.
* none of the above.

TCSEC focused on confidentiality while ITSEC added integrity and availability as security goals.

The following answers are incorrect:

integrity and confidentiality. Is incorrect because TCSEC addressed confidentiality. confidentiality and availability. Is incorrect because TCSEC addressed confidentiality. none of the above. Is incorrect because ITSEC added integrity and availability as security goals.

QUESTION 60

Which of the following is less likely to be included in the change control sub-phase of the maintenance phase of a software product?
* Estimating the cost of the changes requested
* Recreating and analyzing the problem
* Determining the interface that is presented to the user
* Establishing the priorities of requests

Explanation/Reference:

Change control sub-phase includes Recreating and analyzing the problem, Determining the interface that is presented to the user, and Establishing the priorities of requests.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page

252).

QUESTION 61

A momentary low voltage, from 1 cycle to a few seconds, is a:
* spike
* blackout
* sag
* fault

Explanation/Reference:

A momentary low voltage is a sag. A synonym would be a dip.

Risks to electrical power supply:

POWER FAILURE

Blackout: complete loss of electrical power

Fault: momentary power outage

POWER DEGRADATION

Brownout: an intentional reduction of voltage by the power company.

Sag/dip: a short period of low voltage

POWER EXCESS

Surge: Prolonged rise in voltage

Spike: Momentary High Voltage

In-rush current: the initial surge of current required by a load before it reaches normal operation.

– Transient: line noise or disturbance is superimposed on the supply circuit and can cause fluctuations in electrical power

Refence(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 462). McGraw-Hill. Kindle Edition.

QUESTION 62

The three classic ways of authenticating yourself to the computer security software are: something you know, something you have, and something:
* you need.
* you read.
* you are.
* you do.
Section: Access Control

Explanation/Reference:

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

QUESTION 63

The DES algorithm is an example of what type of cryptography?
* Secret Key
* Two-key
* Asymmetric Key
* Public Key
Explanation/Reference:

DES is also known as a Symmetric Key or Secret Key algorithm.

DES is a Symmetric Key algorithm, meaning the same key is used for encryption and decryption.

For the exam remember that:

DES key Sequence is 8 Bytes or 64 bits (8 x 8 = 64 bits)

DES has an Effective key length of only 56 Bits. 8 of the Bits are used for parity purpose only.

DES has a total key length of 64 Bits.

The following answers are incorrect:

Two-key This is incorrect because DES uses the same key for encryption and decryption.

Asymmetric Key This is incorrect because DES is a Symmetric Key algorithm using the same key for encryption and decryption and an Asymmetric Key algorithm uses both a Public Key and a Private Key.

Public Key. This is incorrect because Public Key or algorithm Asymmetric Key does not use the same key is used for encryption and

decryption.

References used for this question:

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

QUESTION 64

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?
* Validation
* Verification
* Assessment
* Accuracy

Explanation/Reference:

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 C&A 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 Exam Guide, 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 65

Which type of attack is based on the probability of two different messages using the same hash function producing a common message digest?
* Differential cryptanalysis
* Differential linear cryptanalysis
* Birthday attack
* Statistical attack

Section: Cryptography

Explanation/Reference:

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. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 163).

and

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

QUESTION 66

The scope and focus of the Business continuity plan development depends most on:
* Directives of Senior Management
* Business Impact Analysis (BIA)
* Scope and Plan Initiation
* Skills of BCP committee
Section: Risk, Response and Recovery

Explanation/Reference:

SearchStorage.com Definitions mentions “As part of a disaster recovery plan, BIA is likely to identify costs linked to failures, such as loss of cash flow, replacement of equipment, salaries paid to catch up with a backlog of work, loss of profits, and so on.

A BIA report quantifies the importance of business components and suggests appropriate fund allocation for measures to protect them. The possibilities of failures are likely to be assessed in terms of their impacts on safety, finances, marketing, legal compliance, and quality assurance.

Where possible, impact is expressed monetarily for purposes of comparison. For example, a business may spend three times as much on marketing in the wake of a disaster to rebuild customer confidence.” Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 278.

QUESTION 67

Which of the following statements is true about data encryption as a method of protecting data?
* It should sometimes be used for password files
* It is usually easily administered
* It makes few demands on system resources
* It requires careful key management
In cryptography, you always assume the “bad guy” has the encryption algorithm (indeed, many algorithms such as DES, Triple DES, AES, etc. are public domain). What the bad guy lacks is the key used to complete that algorithm and encrypt/decrypt information. Therefore, protection of the key, controlled distribution, scheduled key change, timely destruction, and several other factors require careful consideration. All of these factors are covered under the umbrella term of “key management”.

Another significant consideration is the case of “data encryption as a method of protecting data” as the question states. If that data is to be stored over a long period of time (such as on backup), you must ensure that your key management scheme stores old keys for as long as they will be needed to decrypt the information they encrypted.

The other answers are not correct because:

“It should sometimes be used for password files.” – Encryption is often used to encrypt passwords stored within password files, but it is not typically effective for the password file itself. On most systems, if a user cannot access the contents of a password file, they cannot authenticate. Encrypting the entire file prevents that access.

“It is usually easily administered.” – Developments over the last several years have made cryptography

significantly easier to manage and administer. But it remains a significant challenge. This is not a good answer.

“It makes few demands on system resources.” – Cryptography is, essentially, a large complex mathematical algorithm. In order to encrypt and decrypt information, the system must perform this algorithm hundreds, thousands, or even millions/billions/trillions of times. This becomes system resource intensive, making this a very bad answer.

Reference:

Official ISC2 Guide page: 266 (poor explanation)

All in One Third Edition page: 657 (excellent explanation)

Key Management – Page 732, All in One Fourth Edition

QUESTION 68

Related to information security, integrity is the opposite of which of the following?
* abstraction
* alteration
* accreditation
* application
Explanation/Reference:

Integrity is the opposite of “alteration.”

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

QUESTION 69

Which of the following statements pertaining to stream ciphers is correct?
* A stream cipher is a type of asymmetric encryption algorithm.
* A stream cipher generates what is called a keystream.
* A stream cipher is slower than a block cipher.
* A stream cipher is not appropriate for hardware-based encryption.
A stream cipher is a type of symmetric encryption algorithm that operates on continuous streams of plain text and is appropriate for hardware-based encryption.

Stream ciphers can be designed to be exceptionally fast, much faster than any block cipher. A stream cipher generates what is called a keystream (a sequence of bits used as a key).

Stream ciphers can be viewed as approximating the action of a proven unbreakable cipher, the one-time pad (OTP), sometimes known as the Vernam cipher. A one-time pad uses a keystream of completely random digits. The keystream is combined with the plaintext digits one at a time to form the ciphertext. This system was proved to be secure by Claude Shannon in 1949. However, the keystream must be (at least) the same length as the plaintext, and generated completely at random. This makes the system very cumbersome to implement in practice, and as a result the one-time pad has not been widely used, except for the most critical applications.

A stream cipher makes use of a much smaller and more convenient key – 128 bits, for

example. Based on this key, it generates a pseudorandom keystream which can be combined with the plaintext digits in a similar fashion to the one-time pad. However, this comes at a cost: because the keystream is now pseudorandom, and not truly random, the proof of security associated with the one-time pad no longer holds: it is quite possible for a stream cipher to be completely insecure if it is not implemented properly as we have seen with the Wired Equivalent Privacy (WEP) protocol.

Encryption is accomplished by combining the keystream with the plaintext, usually with the bitwise XOR operation.

Source: DUPUIS, Clement, CISSP Open Study Guide on domain 5, cryptography, April 1999.

More details can be obtained on Stream Ciphers in RSA Security’s FAQ on Stream Ciphers.