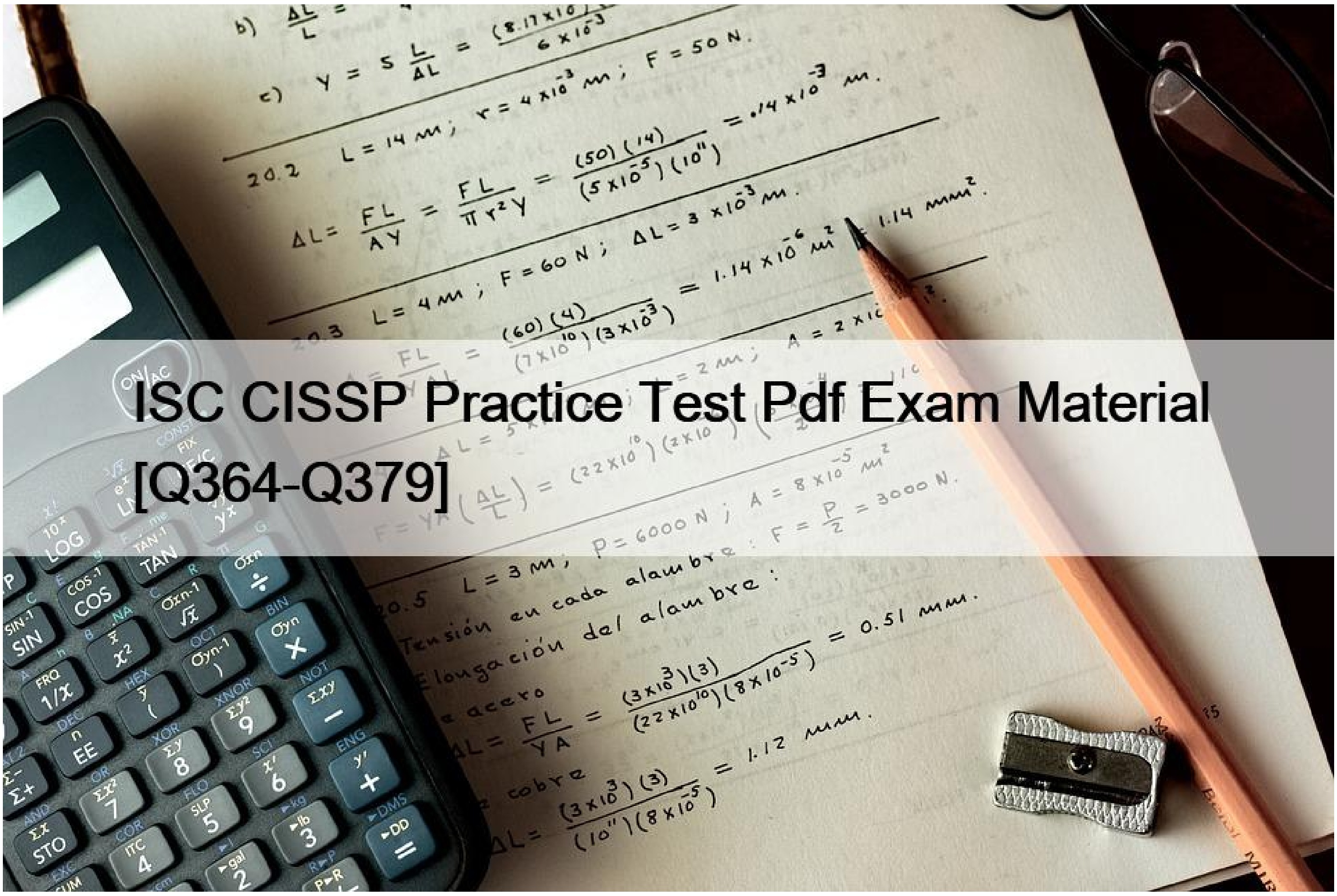
ISC CISSP Practice Test Pdf Exam Material [Q364-Q379



ISC CISSP Practice Test Pdf Exam Material
CISSP Answers CISSP Free Demo Are Based On The Real Exam

Exam Prerequisites

To be CISSP certified, you must have at least five years of industrial experience in IT and security in a combination with two or more of the eight domains of the CISSP objectives. One year of required experience can be fulfilled by receiving a four-year university degree or an additional certification from the approved (ISC)2 list.

NEW QUESTION 364

Which of the following measures would be the BEST deterrent to the theft of corporate information from a laptop which was left in a hotel room?
* Store all data on disks and lock them in an in-room safe
* Remove the batteries and power supply from the laptop and store them separately from the computer
* Install a cable lock on the laptop when it is unattended
* Encrypt the data on the hard drive
To encrypt the data on the hard drive is the best deterrent for information theft (not however the best for physical theft).

NEW QUESTION 365

Which RAID Level often implements a one-for-one disk to disk ratio?
* RAID Level 1
* RAID Level 0
* RAID Level 2
* RAID Level 5
RAID Level 1 often implemented by a one-for-one disk to disk ratio.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten

Domains of Computer Security, 2001, John Wiley & Sons, Page 65.

See Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne,

2002, chapter 7: Telecommunications and Network Security (page 480).

See also: &#8220;This level duplicates all disk writes from one disk to another to create two identical

drives. This technique is also known as data mirroring. Redundancy is provided at this level&#8221;

Source: Official ISC2 Guide to the CISSP CBK. p. 657

=============================

RAID Level 0 &#8211; &#8220;Writes files in stripes across multiple disks without the use of parity informaiton.

This technique allows for fast reading and writing to disk. However, without parity information, it is

not possible to recover from a hard drive failure.&#8221; Source: Official ISC2 Guide to the CISSP CBK.

p. 657 =============================

RAID Level 2 &#8211; &#8220;Data is spread across multiple disks at the bit level using this technique. Redundancy information is computed using a Hammering error correction code, which is the same technique used within hard drives and error-correcting memory modules.&#8221; Source: Official ISC2 guide to the CISSP CBK p.657-658 ============================= RAID Level 5 &#8211; &#8220;This level requires three or more drives to implement. Data and parity information is striped together across all drives. This level is the most popular and can tolerate the loss of any one drive.&#8221; Source: Official ISC2 Guide to the CISSP CBK p. 658

NEW QUESTION 366

Which of the following is a security feature of Global Systems for Mobile Communications (GSM)?
* It uses a Subscriber Identity Module (SIM) for authentication.
* It uses encrypting techniques for all communications.
* The radio spectrum is divided with multiple frequency carriers.
* The signal is difficult to read as it provides end-to-end encryption.

NEW QUESTION 367

Which RAID Level often implements a one-for-one disk to disk ratio?
* RAID Level 1
* RAID Level 0
* RAID Level 2
* RAID Level 5
Explanation/Reference:

Explanation:

RAID Level 1, disk mirroring, uses a one-for-one setup, where data are written to two drives at once. If one drive fails, the other drive has the exact same data available.

Incorrect Answers:

B: RAID Level 0 uses data striped over several drives, not just two drives. There is not one-to-one disk ratio.

C: RAID Level 2 uses data striped over several drives, not just two drives. There is not one-to-one disk ratio.

D: RAID Level 5 does not use a one-to-one disk ratio.

References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 1270

NEW QUESTION 368

Which of the following cryptographic attacks describes when the attacker has a copy of the plaintext and the corresponding ciphertext?
* known plaintext
* brute force
* ciphertext only
* chosen plaintext
The goal to this type of attack is to find the cryptographic key that was used to encrypt the message. Once the key has been found, the attacker would then be able to decrypt all messages that had been encrypted using that key.

The known-plaintext attack (KPA) or crib is an attack model for cryptanalysis where the attacker has samples of both the plaintext and its encrypted version (ciphertext), and is at liberty to make use of them to reveal further secret information such as secret keys and code books. The term &#8220;crib&#8221; originated at Bletchley Park, the British World War II decryption operation

In cryptography, a brute force attack or exhaustive key search is a strategy that can in theory be used against any encrypted data by an attacker who is unable to take advantage of any weakness in an encryption system that would otherwise make his task easier. It involves systematically checking all possible keys until the correct key is found. In the worst case, this would involve traversing the entire key space, also called search space.

In cryptography, a ciphertext-only attack (COA) or known ciphertext attack is an attack model for cryptanalysis where the attacker is assumed to have access only to a set of ciphertexts.

The attack is completely successful if the corresponding plaintexts can be deduced, or even better, the key. The ability to obtain any information at all about the underlying plaintext is still considered a success. For example, if an adversary is sending ciphertext continuously to maintain traffic-flow security, it would be very useful to be able to distinguish real messages from nulls. Even making an informed guess of the existence of real messages would facilitate traffic analysis.

In the history of cryptography, early ciphers, implemented using pen-and-paper, were routinely broken using ciphertexts alone. Cryptographers developed statistical techniques for attacking ciphertext, such as frequency analysis. Mechanical encryption devices such as Enigma made these attacks much more difficult (although, historically, Polish cryptographers were able to mount a successful ciphertext-only cryptanalysis of the

Enigma by exploiting an insecure protocol for indicating the message settings).

Every modern cipher attempts to provide protection against ciphertext-only attacks. The vetting process for a new cipher design standard usually takes many years and includes exhaustive testing of large quantities of ciphertext for any statistical departure from random noise. See: Advanced Encryption Standard process. Also, the field of steganography evolved, in part, to develop methods like mimic functions that allow one piece of data to adopt the statistical profile of another. Nonetheless poor cipher usage or reliance on home- grown proprietary algorithms that have not been subject to thorough scrutiny has resulted in many computer-age encryption systems that are still subject to ciphertext-only attack.

Examples include:

Early versions of Microsoft&#8217;s PPTP virtual private network software used the same RC4 key for the sender and the receiver (later versions had other problems). In any case where a stream cipher like RC4 is used twice with the same key it is open to ciphertext-only attack.

See: stream cipher attack

Wired Equivalent Privacy (WEP), the first security protocol for Wi-Fi, proved vulnerable to several attacks, most of them ciphertext-only.

A chosen-plaintext attack (CPA) is an attack model for cryptanalysis which presumes that the attacker has the capability to choose arbitrary plaintexts to be encrypted and obtain the corresponding ciphertexts. The goal of the attack is to gain some further information which reduces the security of the encryption scheme. In the worst case, a chosen-plaintext attack could reveal the scheme&#8217;s secret key.

This appears, at first glance, to be an unrealistic model; it would certainly be unlikely that an attacker could persuade a human cryptographer to encrypt large amounts of plaintexts of the attacker&#8217;s choosing. Modern cryptography, on the other hand, is implemented in software or hardware and is used for a diverse range of applications; for many cases, a chosen-plaintext attack is often very feasible. Chosen-plaintext attacks become extremely important in the context of public key cryptography, where the encryption key is public and attackers can encrypt any plaintext they choose.

Any cipher that can prevent chosen-plaintext attacks is then also guaranteed to be secure against known-plaintext and ciphertext-only attacks; this is a conservative approach to security.

Two forms of chosen-plaintext attack can be distinguished:

Batch chosen-plaintext attack, where the cryptanalyst chooses all plaintexts before any of them are encrypted. This is often the meaning of an unqualified use of &#8220;chosen-plaintext attack&#8221;.

Adaptive chosen-plaintext attack, where the cryptanalyst makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions.

References:

Source: TIPTON, Harold, Official (ISC)2 Guide to the CISSP CBK (2007), page 271.

and

Wikipedia at the following links:

http://en.wikipedia.org/wiki/Chosen-plaintext_attack

http://en.wikipedia.org/wiki/Known-plaintext_attack

http://en.wikipedia.org/wiki/Ciphertext-only_attac

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

NEW QUESTION 369

Good security is built on which of the following concept?

* The concept of a pass-through device that only allows certain traffic in and out
* The Concept of defense in depth
* The Concept of Preventative controls
* The Concept of Defensive Controls

This the best of the four answers as a defense that depends on multiple layers is superior to one where all protection is embedded in a single layer (e.g., a firewall).

Defense in depth would include all categories of controls.

The Following answers are incorrect:

&#8220;Concept of a pass through device that only allows certain traffic in and out&#8221; is incorrect.

This is one definition of a firewall which can be a component of a defense in depth strategy in combination with other measures.

&#8220;Concept of preventative controls&#8221; is incorrect. This is a component of a defense in depth strategy but the core concept is that there must be multiple layers of defenses.

&#8220;Concept of defensive controls&#8221; is incorrect. This is a component of a defense in depth strategy but the core concept is that there must be multiple layers of defenses.

References:

http://en.wikipedia.org/wiki/Defense_in_depth_(computing)

http://www.nsa.gov/snac/support/defenseindepth.pdf

NEW QUESTION 370

What is the main problem of the renewal of a root CA certificate?

* It requires key recovery of all end user keys

* It requires the authentic distribution of the new root CA certificate to all PKI participants
* It requires the collection of the old root CA certificates from all the users
* It requires issuance of the new root CA certificate
The main task here is the authentic distribution of the new root CA certificate as new trust anchor to all the PKI participants (e.g. the users).

In some of the rollover-scenarios there is no automatic way, often explicit assignment of trust from each user is needed, which could be very costly.

Other methods make use of the old root CA certificate for automatic trust establishment

(see PKIX-reference), but these solutions works only well for scenarios with currently valid root CA certificates (and not for emergency cases e.g. compromise of the current root CA certificate).

The rollover of the root CA certificate is a specific and delicate problem and therefore are often ignored during PKI deployment.

Reference: Camphausen, I.; Petersen, H.; Stark, C.: Konzepte zum Root CA

Zertifikatswechsel, conference Enterprise Security 2002, March 26-27, 2002, Paderborn;

RFC 2459 : Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

NEW QUESTION 371

Which choice is NOT a good criterion for selecting a safeguard?
* The ability to recover from a reset without damaging the asset
* Accountability features for tracking and identifying operators
* The ability to recover from a reset with the permissions set to allow all
* Comparing the potential dollar loss of an asset to the cost of a safeguard
The correct answer is &#8220;The ability to recover from a reset with the permissions set to cllow all&#8221;.

Permissions should be set to deny all

during reset.

NEW QUESTION 372

An international medical organization with headquarters in the United States (US) and branches in France wants to test a drug in both countries. What is the organization allowed to do with the test subject&#8217;s data?
* Aggregate it into one database in the US
* Process it in the US, but store the information in France
* Share it with a third party
* Anonymize it and process it in the US
Explanation

Section: Security Assessment and Testing

NEW QUESTION 373

What does CSMA stand for?

* Common Systems Methodology Applications
* Carrier Sense Multiple Access
* Carrier Sense Multiple Attenuation
* Carrier Station Multi-port Actuator

The correct answer is &#8220;Carrier Sense Multiple Access&#8221;. The other acronyms do not exist.

NEW QUESTION 374

What mechanism does a system use to compare the security labels of a subject and an object?

* Validation Module.
* Reference Monitor.
* Clearance Check.
* Security Module.

Because the Reference Monitor is responsible for access control to the objects by the subjects it compares the security labels of a subject and an object.

According to the OIG: The reference monitor is an access control concept referring to an abstract machine that mediates all accesses to objects by subjects based on information in an access control database. The reference monitor must mediate all access, be protected from modification, be verifiable as correct, and must always be invoked. The reference monitor, in accordance with the security policy, controls the checks that are made in the access control database.

The following are incorrect:

Validation Module. A Validation Module is typically found in application source code and is used to

validate data being inputted.

Clearance Check. Is a distractor, there is no such thing other than what someone would do when

checking if someone is authorized to access a secure facility.

Security Module. Is typically a general purpose module that prerforms a variety of security related

functions.

References:

OIG CBK, Security Architecture and Design (page 324)

AIO, 4th Edition, Security Architecture and Design, pp 328-328.

Wikipedia &#8211; http://en.wikipedia.org/wiki/Reference_monitor

NEW QUESTION 375

A controlled light fixture mounted on a 5-meter pole can illuminate an area 30 meter in diameter.

For security lighting purposes, what would be the proper distance between fixtures?

* 25 meters
* 30 meters

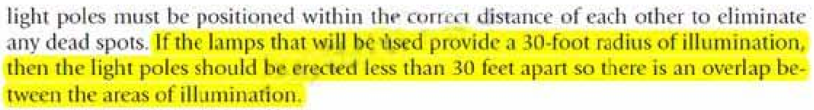
* 35 meters
* 40 meters
The answer should be 25 meters:

If a lamp provides a 30 foot illumination, the lamps should be placed less than 30 feet apart to

provide an overlap. A 30 meter coverage area mean the next light should be less than 30 meters

away, and the only answer that fits is 25 meters.

Chapter 6, page 459 of Shon Harris CISSP 5th edition book.



light poles must be positioned within the correct distance of each other to eliminate any dead spots. If the lamps that will be used provide a 30-foot radius of illumination, then the light poles should be erected less than 30 feet apart so there is an overlap between the areas of illumination.

NEW QUESTION 376

What does the simple security (ss) property mean in the Bell-LaPadula model?
* No read up
* No write down
* No read down
* No write up
Explanation/Reference:

Explanation:

Three main rules are used and enforced in the Bell-LaPadula model:

The simple security (SS) rule, the *-property (star property) rule, and the strong star property rule. The simple security rule states that a subject at a given security level cannot read data that reside at a higher security level.

The *-property rule (star property rule) states that a subject in a given security level cannot write information to a lower security level. The simple security rule is referred to as the &#8220;no read up&#8221; rule, and the

*-property rule is referred to as the &#8220;no write down&#8221; rule.

The third rule, the strong star property rule, states that a subject that has read and write capabilities can only perform those functions at the same security level; nothing higher and nothing lower. So, for a subject to be able to read and write to an object, the clearance and classification must be equal.

Incorrect Answers:

B: The simple security rule is referred to as the &#8220;no read up&#8221; rule, not the &#8220;no write down&#8221; rule. The *- property rule is referred to as the &#8220;no write down&#8221; rule.

C: The simple security rule is referred to as the &#8220;no read up&#8221; rule, not the &#8220;no read down&#8221; rule.

D: The simple security rule is referred to as the &#8220;no read up&#8221; rule, not the &#8220;no write up&#8221; rule.

References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, pp. 369-370

NEW QUESTION 377

What attack takes advantage of operating system buffer overflows?

* Spoofing
* Brute force
* DoS
* Exhaustive

Denial of Service is an attack on the operating system or software using buffer overflows. The result is that the target is unable to reply to service requests. This is too a large an area of information to try to cover here, so I will limit my discussion to the types of denial of service (DoS) attacks:

NEW QUESTION 378

Which of the following is the MOST effective attack against cryptographic hardware modules?

* Plaintext
* Brute force
* Power analysis
* Man-in-the-middle (MITM)

NEW QUESTION 379

Which of the following can be best defined as computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data and for detecting or extracting the marks later?

* Steganography
* Digital watermarking
* Digital enveloping
* Digital signature

RFC 2828 (Internet Security Glossary) defines digital watermarking as computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data-text, graphics, images, video, or audio#and for detecting or extracting the marks later. The set of embedded bits (the digital watermark) is sometimes hidden, usually imperceptible, and always intended to be unobtrusive. It is used as a measure to protect intellectual property rights. Steganography involves hiding the very existence of a message. A digital signature is a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data&#8217;s origin and integrity. A digital envelope is a combination of encrypted data and its encryption key in an encrypted form that has been prepared for use of the recipient. Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

How to earn CISSP Credential?

The candidate must earn 120 continuing education units (CEUs) for the CISSP certification. The CEUs may be earned through participation in the ISSA-certified training course, obtaining CEUs from any other Information Systems Security Association (ISSA) member, obtaining certification credits for passing the exam, or through participating in many other online sites.

CISSP [Jul-2022 Newly Released Exam Questions For You To Pass:
https://www.topexamcollection.com/CISSP-vce-collection.html]