

100% Money Back
Guarantee

Vendor:ISC

Exam Code:SSCP

Exam Name:System Security Certified Practitioner
(SSCP)

Version:Demo

QUESTION 1

Which of the following will a Business Impact Analysis NOT identify?

- A. Areas that would suffer the greatest financial or operational loss in the event of a disaster.
- B. Systems critical to the survival of the enterprise.
- C. The names of individuals to be contacted during a disaster.
- D. The outage time that can be tolerated by the enterprise as a result of a disaster.

Correct Answer: C

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

QUESTION 2

Which of the following is the most important consideration in locating an alternate computing facility during the development of a disaster recovery plan?

- A. It is unlikely to be affected by the same disaster.
- B. It is close enough to become operational quickly.
- C. It is close enough to serve its users.
- D. It is convenient to airports and hotels.

Correct Answer: A

You do not want the alternate or recovery site located in close proximity to the original site because the same event that create the situation in the first place might very well impact that site also.

From NIST: "The fixed site should be in a geographic area that is unlikely to be negatively affected by the same disaster event (e.g., weather-related impacts or power grid failure) as the organization's primary site.

The following answers are incorrect:

It is close enough to become operational quickly. Is incorrect because it is not the best answer. You'd want the alternate site to be close but if it is too close the same event could impact that site as well.

It is close enough to serve its users. Is incorrect because it is not the best answer. You'd want the alternate site to be close to users if applicable, but if it is too close the same event could impact that site as well It is convenient to airports and hotels. Is incorrect because it is not the best answer, it is more important that the same event does not impact the alternate site then convenience.

References:

OIG CBK Business Continuity and Disaster Recovery Planning (pages 368 - 369)

QUESTION 3

What is called an event or activity that has the potential to cause harm to the information systems or networks?

- A. Vulnerability
- B. Threat agent
- C. Weakness D. Threat

Correct Answer: D

Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley and Sons, Pages 16, 32.

QUESTION 4

One of the following assertions is NOT a characteristic of Internet Protocol Security (IPsec)

- A. Data cannot be read by unauthorized parties
- B. The identity of all IPsec endpoints are confirmed by other endpoints
- C. Data is delivered in the exact order in which it is sent
- D. The number of packets being exchanged can be counted.

Correct Answer: C

IPSec provide replay protection that ensures data is not delivered multiple times, however IPSec does not ensure that data is delivered in the exact order in which it is sent. IPSEC uses TCP and packets may be delivered out of order to the receiving side depending which route was taken by the packet.

Internet Protocol Security (IPsec) has emerged as the most commonly used network layer security control for protecting communications. IPsec is a framework of open standards for ensuring private communications over IP networks. Depending on how IPsec is implemented and configured, it can provide any combination of the following types of protection:

Confidentiality. IPsec can ensure that data cannot be read by unauthorized parties. This is accomplished by encrypting data using a cryptographic algorithm and a secret key a value known only to the two parties exchanging data. The data can only be decrypted by someone who has the secret key.

Integrity. IPsec can determine if data has been changed (intentionally or unintentionally) during transit. The integrity of data can be assured by generating a message authentication code (MAC) value, which is a cryptographic checksum of the data. If the data is altered and the MAC is recalculated, the old and new MACs will differ.

Peer Authentication. Each IPsec endpoint confirms the identity of the other IPsec endpoint with which it wishes to communicate, ensuring that the network traffic and data is being sent from the expected host.

Replay Protection. The same data is not delivered multiple times, and data is not delivered grossly out of order. However, IPsec does not ensure that data is delivered in the exact order in which it is sent.

Traffic Analysis Protection. A person monitoring network traffic does not know which parties are communicating, how often communications are occurring, or how much data is being exchanged. However, the number of packets being exchanged can be counted.

Access Control. IPsec endpoints can perform filtering to ensure that only authorized IPsec users can access particular network resources. IPsec endpoints can also allow or block certain types of network traffic, such as allowing Web server access but denying file sharing.

The following are incorrect answers because they are all features provided by IPSEC: "Data cannot be read by unauthorized parties" is wrong because IPsec provides confidentiality through the usage of the Encapsulating Security Protocol (ESP), once encrypted the data cannot be read by unauthorized parties because they have access only to the ciphertext. This is accomplished by encrypting data using a cryptographic algorithm and a session key, a value known only to the two parties exchanging data. The data can only be decrypted by someone who has a copy of the session key.

"The identity of all IPsec endpoints are confirmed by other endpoints" is wrong because IPsec provides peer authentication: Each IPsec endpoint confirms the identity of the other IPsec endpoint with which it wishes to communicate, ensuring that the network traffic and data is being sent from the expected host.

"The number of packets being exchanged can be counted" is wrong because although IPsec provides traffic protection where a person monitoring network traffic does not know which parties are communicating, how often communications are occurring, or how much data is being exchanged, the number of packets being exchanged still can be counted.

Reference(s) used for this question:

NIST 800-77 Guide to IPsec VPNs . Pages 2-3 to 2-4

QUESTION 5

In order to enable users to perform tasks and duties without having to go through extra steps it is important that the security controls and mechanisms that are in place have a degree of?

- A. Complexity
- B. Non-transparency
- C. Transparency
- D. Simplicity

Correct Answer: C

The security controls and mechanisms that are in place must have a degree of transparency.

This enables the user to perform tasks and duties without having to go through extra steps because of the presence of the security controls. Transparency also does not let the user know too much about the controls, which helps prevent him from figuring out how to circumvent them. If the controls are too obvious, an attacker can figure out how to compromise them more easily.

Security (more specifically, the implementation of most security controls) has long been a sore point with users who are subject to security controls. Historically, security controls have been very intrusive to users,

forcing them to interrupt their work flow and remember arcane codes or processes (like long passwords or access codes), and have generally been seen as an obstacle to getting work done. In recent years, much work has been done to remove that stigma of security controls as a detractor from the work process adding nothing but time and money. When developing access control, the system must be as transparent as possible to the end user. The users should be required to interact with the system as little as possible, and the process around using the control should be engineered so as to involve little effort on the part of the user.

For example, requiring a user to swipe an access card through a reader is an effective way to ensure a person is authorized to enter a room. However, implementing a technology (such as RFID) that will automatically scan the badge as the user approaches the door is more transparent to the user and will do less to impede the movement of personnel in a busy area.

In another example, asking a user to understand what applications and data sets will be required when requesting a system ID and then specifically requesting access to those resources may allow for a great deal of granularity when provisioning access, but it can hardly be seen as transparent. A more transparent process would be for the access provisioning system to have a role-based structure, where the user would simply specify the role he or she has in the organization and the system would know the specific resources that user needs to access based on that role. This requires less work and interaction on the part of the user and will lead to more accurate and secure access control decisions because access will be based on predefined need, not user preference.

When developing and implementing an access control system special care should be taken to ensure that the control is as transparent to the end user as possible and interrupts his work flow as little as possible.

The following answers were incorrect:

All of the other detractors were incorrect.

Reference(s) used for this question:

HARRIS, Shon, All-In-One CISSP Certification uide, 6th edition. Operations Security, Page 1239

Harris, Shon (2012-10-25). CISSP All-in-One uide, 6th Edition (Kindle Locations 25278-25281).

McGraw-Hill. Kindle Edition.

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition :

Access Control ((ISC)2 Press) (Kindle Locations 713-729). Auerbach Publications. Kindle Edition.

QUESTION 6

Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It does not permit management to:

- A. specify what users can do
- B. specify which resources they can access
- C. specify how to restrain hackers
- D. specify what operations they can perform on a system.

Correct Answer: C

Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It permits management to specify what users can do, which resources they can access, and what operations they can perform on a system. Specifying HOW to restrain hackers is not directly linked to access control.

Source: DUPUIS, Clement, Access Control Systems and Methodology, Version 1, May 2002, CISSP Open Study Group Study Guide for Domain 1, Page 12.

QUESTION 7

Which of the following is NOT a transaction redundancy implementation?

- A. on-site mirroring
- B. Electronic Vaulting
- C. Remote Journaling
- D. Database Shadowing

Correct Answer: A

Three concepts are used to create a level of fault tolerance and redundancy in transaction processing.

They are Electronic vaulting, remote journaling and database shadowing provide redundancy at the transaction level. Electronic vaulting is accomplished by backing up system data over a network. The backup location is usually at a separate geographical location known as the vault site. Vaulting can be used as a mirror or a backup mechanism using the standard incremental or differential backup cycle. Changes to the host system are sent to the vault server in real-time when the backup method is implemented as a mirror. If vaulting updates are recorded in real-time, then it will be necessary to perform regular backups at the off-site location to provide recovery services due to inadvertent or malicious alterations to user or system data.

Journaling or Remote Journaling is another technique used by database management systems to provide redundancy for their transactions. When a transaction is completed, the database management system duplicates the journal entry at a remote location. The journal provides sufficient detail for the transaction to be replayed on the remote system. This provides for database recovery in the event that the database becomes corrupted or unavailable.

There are also additional redundancy options available within application and database software platforms. For

example, database shadowing may be used where a database management system updates records in multiple locations. This technique updates an entire copy of the database at a remote location.

Reference 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 20403-20407). 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 20375-20377). Auerbach Publications. Kindle Edition.

QUESTION 8

Which of the following is NOT a symmetric key algorithm?

- A. Blowfish
- B. Digital Signature Standard (DSS)
- C. Triple DES (3DES)
- D. RC5

Correct Answer: B

Digital Signature Standard (DSS) specifies a Digital Signature Algorithm (DSA) appropriate for applications requiring a digital signature, providing the capability to generate signatures (with the use of a private key) and verify them (with the use of the corresponding public key).

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

8: Cryptography (page 550).

Reference: DSS: <http://www.itl.nist.gov/fipspubs/fip186.htm>.

QUESTION 9

Which of the following statements pertaining to biometrics is FALSE?

- A. User can be authenticated based on behavior.
- B. User can be authenticated based on unique physical attributes.
- C. User can be authenticated by what he knows.
- D. A biometric system's accuracy is determined by its crossover error rate (CER).

Correct Answer: C

As this is not a characteristic of Biometrics this is the right choice for this question. This is one of the three basic way authentication can be performed and it is not related to Biometrics. Example of something you know would be a

password or PIN for example.

Please make a note of the negative 'FALSE' within the question. This question may seem tricky to some of you but you would be amazed at how many people cannot deal with negative questions. There will be a few negative questions within the real exam, just like this one the keyword NOT or FALSE will be in Uppercase to clearly indicate that it is negative.

Biometrics verifies an individual's identity by analyzing a unique personal attribute or behavior, which is one of the most effective and accurate methods of performing authentication (one to one matching) or identification (a one to many matching).

A biometric system scans an attribute or behavior of a person and compares it to a template store within an authentication server database, such template would be created in an earlier enrollment process.

Because this system inspects the grooves of a person's fingerprint, the pattern of someone's retina, or the pitches of someone's voice, it has to be extremely sensitive.

The system must perform accurate and repeatable measurements of anatomical or physiological characteristics. This type of sensitivity can easily cause false positives or false negatives. The system must be calibrated so that these false positives and false negatives occur infrequently and the results are as accurate as possible.

There are two types of failures in biometric identification:

False Rejection also called False Rejection Rate (FRR) -- The system fail to recognize a legitimate user.

While it could be argued that this has the effect of keeping the protected area extra secure, it is an intolerable frustration to legitimate users who are refused access because the scanner does not recognize them.

False Acceptance or False Acceptance Rate (FAR) -- This is an erroneous recognition, either by confusing one user with another or by accepting an imposter as a legitimate user.

Physiological Examples:

Unique Physical Attributes:

Fingerprint (Most commonly accepted)

Hand Geometry

Retina Scan (Most accurate but most intrusive)

Iris Scan

Vascular Scan

Behavioral Examples:

Repeated Actions

Keystroke Dynamics

(Dwell time (the time a key is pressed) and Flight time (the time between "key up" and the next "key down").

Signature Dynamics

(Stroke and pressure points)

EXAM TIP:

Retina scan devices are the most accurate but also the most invasive biometrics system available today.

The continuity of the retinal pattern throughout life and the difficulty in fooling such a device also make it a great long-term, high-security option. Unfortunately, the cost of the proprietary hardware as well the stigma of users thinking it is potentially harmful to the eye makes retinal scanning a bad fit for most situations.

Remember for the exam that fingerprints are the most commonly accepted type of biometrics system.

The other answers are incorrect:

'Users can be authenticated based on behavior.' is incorrect as this choice is TRUE as it pertains to BIOMETRICS.

Biometrics systems makes use of unique physical characteristics or behavior of users.

'User can be authenticated based on unique physical attributes.' is also incorrect as this choice is also TRUE as it pertains to BIOMETRICS. Biometrics systems makes use of unique physical characteristics or behavior of users.

'A biometric system's accuracy is determined by its crossover error rate (CER)' is also incorrect as this is TRUE as it also pertains to BIOMETRICS. The CER is the point at which the false rejection rates and the false acceptance rates are equal. The smaller the value of the CER, the more accurate the system.

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 25353-25356). 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 25297-25303). Auerbach Publications. Kindle Edition.

QUESTION 10

The fact that a network-based IDS reviews packets payload and headers enable which of the following?

- A. Detection of denial of service
- B. Detection of all viruses

- C. Detection of data corruption
- D. Detection of all password guessing attacks

Correct Answer: A

Because a network-based IDS reviews packets and headers, denial of service attacks can also be detected.

This question is an easy question if you go through the process of elimination. When you see an answer containing the keyword: ALL It is something a give away that it is not the proper answer. On the real exam you may encounter a few question where the use of the work ALL renders the choice invalid. Pay close attention to such keyword.

The following are incorrect answers:

Even though most IDSs can detect some viruses and some password guessing attacks, they cannot detect ALL viruses or ALL password guessing attacks. Therefore these two answers are only detractors.

Unless the IDS knows the valid values for a certain dataset, it can NOT detect data corruption.

Reference used for this question:

KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley and Sons, Page 48.

QUESTION 11

Which of the following encryption algorithms does not deal with discrete logarithms?

- A. El Gamal
- B. Diffie-Hellman
- C. RSA
- D. Elliptic Curve

Correct Answer: C

The security of the RSA system is based on the assumption that factoring the product into two original large prime numbers is difficult

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 159).

Shon Harris, CISSP All-in-One Examine Guide, Third Edition, McGraw-Hill Companies, August 2005, Chapter 8: Cryptography, Page 636 - 639

QUESTION 12

PGP uses which of the following to encrypt data?

- A. An asymmetric encryption algorithm
- B. A symmetric encryption algorithm
- C. A symmetric key distribution system
- D. An X.509 digital certificate

Correct Answer: B

Notice that the question specifically asks what PGP uses to encrypt. For this, PGP uses a symmetric key algorithm. PGP then uses an asymmetric key algorithm to encrypt the session key and then send it securely to the receiver. It is a hybrid system where both types of ciphers are being used for different purposes.

Whenever a question talks about the bulk of the data to be sent, Symmetric is always the best choice to use because of the inherent speed within Symmetric Ciphers. Asymmetric ciphers are 100 to 1000 times slower than Symmetric Ciphers.

The other answers are not correct because:

"An asymmetric encryption algorithm" is incorrect because PGP uses a symmetric algorithm to encrypt data.

"A symmetric key distribution system" is incorrect because PGP uses an asymmetric algorithm for the distribution of the session keys used for the bulk of the data.

"An X.509 digital certificate" is incorrect because PGP does not use X.509 digital certificates to encrypt the data, it uses a session key to encrypt the data.

References:

Official ISC2 Guide page: 275

All in One Third Edition page: 664 - 665