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.certbus.com/sscp.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by ISC Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following is the FIRST step in protecting data\\'s confidentiality?

A. Install a firewall

B. Implement encryption

C. Identify which information is sensitive

D. Review all user access rights

Correct Answer: C

In order to protect the confidentiality of the data.

The following answers are incorrect because :

Install a firewall is incorrect as this would come after the information has been identified for sensitivity levels.

Implement encryption is also incorrect as this is one of the mechanisms to protect the data once it has been identified.

Review all user access rights is also incorrect as this is also a protection mechanism for the identified information.

Reference : Shon Harris AIO v3 , Chapter-4 : Access Control , Page : 126

QUESTION 2

What is called the type of access control where there are pairs of elements that have the least upper bound of values and greatest lower bound of values?

A. Mandatory model

B. Discretionary model

C. Lattice model

D. Rule model

Correct Answer: C

In a lattice model, there are pairs of elements that have the least upper bound of values and greatest lower bound of values.

Reference(s) 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 34.

QUESTION 3

Which type of attack would a competitive intelligence attack best classify as?

A. Business attack

B. Intelligence attack

C. Financial attack

D. Grudge attack

Correct Answer: A

Business attacks concern information loss through competitive intelligence gathering and computer-related attacks. These attacks can be very costly due the loss of trade secrets and reputation.

Intelligence attacks are aimed at sensitive military and law enforcement files containing military data and investigation reports.

Financial attacks are concerned with frauds to banks and large corporations.

Grudge attacks are targeted at individuals and companies who have done something that the attacker doesn\\'t like.

The CISSP for Dummies book has nice coverage of the different types of attacks, here is an extract: Terrorism Attacks

Terrorism exists at many levels on the Internet. In April 2001, during a period of tense relations between China and the U.S. (resulting from the crash landing of a U.S. Navy reconnaissance plane on Hainan Island), Chinese hackers (cyberterrorists) launched a major effort to disrupt critical U.S. infrastructure, which included U.S. government and military systems.

Following the terrorist attacks against the U.S. on September 11, 2001, the general public became painfully aware of the extent of terrorism on the Internet. Terrorist organizations and cells are using online capabilities to coordinate attacks, transfer funds, harm international commerce, disrupt critical systems, disseminate propaganda, and gain useful information about developing techniques and instruments of terror, including nuclear , biological, and chemical weapons.

Military and intelligence attacks

Military and intelligence attacks are perpetrated by criminals, traitors, or foreign intelligence agents seeking classified law enforcement or military information. Such attacks may also be carried out by governments during times of war and conflict.

Financial attacks

Banks, large corporations, and e-commerce sites are the targets of financial attacks, all of which are motivated by greed. Financial attacks may seek to steal or embezzle funds, gain access to online financial information, extort individuals or businesses, or obtain the personal credit card numbers of customers.

Business attacks

Businesses are becoming the targets of more and more computer and Internet attacks. These attacks include competitive intelligence gathering, denial of service, and other computer- related attacks. Businesses are often targeted for several reasons including Lack of expertise: Despite heightened security awareness, a shortage of qualified security professionals still exists, particularly in private enterprise.

Lack of resources: Businesses often lack the resources to prevent, or even detect, attacks against their systems.

Lack of reporting or prosecution : Because of public relations concerns and the inability to prosecute computer criminals

due to either a lack of evidence or a lack of properly handled evidence, the majority of business attacks still go unreported.

The cost to businesses can be significant, including loss of trade secrets or proprietary information, loss of revenue, and loss of reputation.

Grudge attacks

Grudge attacks are targeted at individuals or businesses and are motivated by a desire to take revenge against a person or organization. A disgruntled employee, for example, may steal trade secrets, delete valuable data, or plant a logic bomb in a critical system or application.

Fortunately, these attacks (at least in the case of a disgruntled employee) can be easier to prevent or prosecute than many other types of attacks because:

The attacker is often known to the victim.

The attack has a visible impact that produces a viable evidence trail.

Most businesses (already sensitive to the possibility of wrongful termination suits) have well- established termination procedures

"Fun" attacks

"Fun" attacks are perpetrated by thrill seekers and script kiddies who are motivated by curiosity or excitement. Although these attackers may not intend to do any harm or use any of the information that they access, they\\'re still dangerous and their activities are still illegal. These attacks can also be relatively easy to detect and prosecute. Because the perpetrators are often script kiddies or otherwise inexperienced hackers, they may not know how to cover their tracks effectively.

Also, because no real harm is normally done nor intended against the system, it may be tempting (although ill advised) for a business to prosecute the individual and put a positive public relations spin on the incident. You\\'ve seen the film at 11: "We quickly detected the attack, prevented any harm to our network, and prosecuted the responsible individual; our security is unbreakable !" Such action, however, will likely motivate others to launch a more serious and concerted grudge attack against the business.

Many computer criminals in this category only seek notoriety. Although it\\'s one thing to brag to a small circle of friends about defacing a public Web site, the wily hacker who appears on CNN reaches the next level of hacker celebrity-dom. These twisted individuals want to be caught to revel in their 15 minutes of fame.

References:

ANDRESS, Mandy, ram CISSP, Coriolis, 2001, Chapter 10: Law, Investigation, and Ethics (page 187)

and

CISSP Professional Study Guide by James Michael Stewart, Ed Tittel, Mike Chapple, page 607- and

CISSP for Dummies, Miller L. H. and Gregory P. H. ISBN: 0470537914, page 309-311

QUESTION 4

What enables users to validate each other\\'s certificate when they are certified under different certification hierarchies?

A. Cross-certification

B. Multiple certificates

C. Redundant certification authorities

D. Root certification authorities

Correct Answer: A

Cross-certification is the act or process by which two CAs each certifiy a public key of the other, issuing a public-key certificate to that other CA, enabling users that are certified under different certification hierarchies to validate each other\\'s certificate.

Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 5

Which of the following is NOT part of the Kerberos authentication protocol?

A. Symmetric key cryptography

B. Authentication service (AS)

C. Principals

D. Public Key

Correct Answer: D

There is no such component within kerberos environment. Kerberos uses only symmetric encryption and does not make use of any public key component.

The other answers are incorrect because :

Symmetric key cryptography is a part of Kerberos as the KDC holds all the users\\' and services\\' secret keys.

Authentication service (AS) : KDC (Key Distribution Center) provides an authentication service

Principals : Key Distribution Center provides services to principals , which can be users , applications or network services.

References: Shon Harris , AIO v3 , Chapter - 4: Access Control , Pages : 152-155.

QUESTION 6

In response to Access-request from a client such as a Network Access Server (NAS), which of the following is not one of the response from a RADIUS Server?

A. Access-Accept

B. Access-Reject

C. Access-Granted

D. Access-Challenge

Correct Answer: C

In response to an access-request from a client, a RADIUS server returns one of three authentication responses: access-accept, access-reject, or access-challenge, the latter being a request for additional authentication information such as a one-time password from a token or a callback identifier.

Source: TIPTON, Harold F. and KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, page 36.

QUESTION 7

Which of the following computer crime is MORE often associated with INSIDERS?

A. IP spoofing

B. Password sniffing

C. Data diddling

D. Denial of service (DOS)

Correct Answer: C

It refers to the alteration of the existing data , most often seen before it is entered into an application.This type of crime is extremely common and can be prevented by using appropriate access controls and proper segregation of duties. It will more likely be perpetrated by insiders, who have access to data before it is processed. The other answers are incorrect because : IP Spoofing is not correct as the questions asks about the crime associated with the insiders. Spoofing is generally accomplished from the outside. Password sniffing is also not the BEST answer as it requires a lot of technical knowledge in understanding the encryption and decryption process. Denial of service (DOS) is also incorrect as most Denial of service attacks occur over the internet. Reference : Shon Harris , AIO v3 , Chapter-10 : Law , Investigation and Ethics , Page : 758-760.

QUESTION 8

Which of the following would be MOST important to guarantee that the computer evidence will be admissible in court?

A. It must prove a fact that is immaterial to the case.

B. Its reliability must be proven.

C. The process for producing it must be documented and repeatable.

D. The chain of custody of the evidence must show who collected, secured, controlled, handled, transported the evidence, and that it was not tampered with.

Correct Answer: D

It has to be material, relevant and reliable, and the chain of custody must be maintained, it is unlikely that it will be admissible in court if it has been tampered with.

The following answers are incorrect:

It must prove a fact that is immaterial to the case. Is incorrect because evidence must be relevant. If it is immaterial then it is not relevant.

Its reliability must be proven. Is incorrect because it is not the best answer. While evidence must be relevant if the chain of custody cannot be verified, then the evidence could lose it\\'s credibility because there is no proof that the evidence was not tampered with. So, the correct answer above is the BEST answer.

The process for producing it must be documented and repeatable. Is incorrect because just because the process is documented and repeatable does not mean that it will be the same. This amounts to Corroborative Evidence that may help to support a case.

QUESTION 9

In the process of gathering evidence from a computer attack, a system administrator took a series of actions which are listed below. Can you identify which one of these actions has compromised the whole evidence collection process?

A. Using a write blocker

B. Made a full-disk image

C. Created a message digest for log files

D. Displayed the contents of a folder

Correct Answer: D

Displaying the directory contents of a folder can alter the last access time on each listed file. Using a write blocker is wrong because using a write blocker ensure that you cannot modify the data on the host and it prevent the host from writing to its hard drives.

Made a full-disk image is wrong because making a full-disk image can preserve all data on a hard disk, including deleted files and file fragments.

Created a message digest for log files is wrong because creating a message digest for log files. A message digest is a cryptographic checksum that can demonstrate that the integrity of a file has not been compromised (e.g. changes to the content of a log file)

Domain: LEGAL, REGULATIONS, COMPLIANCE AND INVESTIGATIONS

References:

AIO 3rd Edition, page 783-784

NIST 800-61 Computer Security Incident Handling guide page 3-18 to 3-20

QUESTION 10

The Diffie-Hellman algorithm is used for:

A. Encryption

B. Digital signature

C. Key agreement

D. Non-repudiation

Correct Answer: C

The Diffie-Hellman algorithm is used for Key agreement (key distribution) and cannot be used to encrypt

and decrypt messages.

Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 4).

Note: key agreement, is different from key exchange, the functionality used by the other asymmetric

algorithms.

References:

AIO, third edition Cryptography (Page 632) AIO, fourth edition Cryptography (Page 709)

QUESTION 11

How long are IPv4 addresses?

A. 32 bits long.

B. 64 bits long.

C. 128 bits long.

D. 16 bits long.

Correct Answer: A

IPv4 addresses are currently 32 bits long. IPv6 addresses are 128 bits long.

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 87.

QUESTION 12

Because ordinary cable introduces a toxic hazard in the event of fire, special cabling is required in a separate area provided for air circulation for heating, ventilation, and air-conditioning (sometimes referred to as HVAC) and typically provided in the space between the structural ceiling and a drop-down ceiling. This area is referred to as the:

A. smoke boundry area

B. fire detection area

C. Plenum area

D. Intergen area

Correct Answer: C

In building construction, a plenum (pronounced PLEH-nuhm, from Latin meaning full) is a separate space provided for air circulation for heating, ventilation, and air-conditioning (sometimes referred to as HVAC) and typically provided in the space between the structural ceiling and a drop-down ceiling. A plenum may also be under a raised floor. In buildings with computer installations, the plenum space is often used to house connecting communication cables. Because ordinary cable introduces a toxic hazard in the event of fire, special plenum cabling is required in plenum areas.

Source: http://searchdatacenter.techtarget.com/sDefinition/0,,sid80_gci213716,00.html

QUESTION 13

Considerations of privacy, invasiveness, and psychological and physical comfort when using the system are important elements for which of the following?

A. Accountability of biometrics systems

B. Acceptability of biometrics systems

C. Availability of biometrics systems

D. Adaptability of biometrics systems

Correct Answer: B

Acceptability refers to considerations of privacy, invasiveness, and psychological and physical comfort when using the system.

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 39.

QUESTION 14

Which of the following phases of a system development life-cycle is most concerned with maintaining proper authentication of users and processes to ensure appropriate access control decisions?

A. Development/acquisition

B. Implementation

C. Operation/Maintenance

D. Initiation

Correct Answer: C

The operation phase of an IT system is concerned with user authentication.

Authentication is the process where a system establishes the validity of a transmission, message, or a means of verifying the eligibility of an individual, process, or machine to carry out a desired action, thereby ensuring that security is not compromised by an untrusted source.

It is essential that adequate authentication be achieved in order to implement security policies and achieve security

goals. Additionally, level of trust is always an issue when dealing with cross-domain interactions. The solution is to establish an authentication policy and apply it to cross-domain interactions as required.

Source: STONEBURNER, Gary and 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 (page 15).

QUESTION 15

Which of the following is not appropriate in addressing object reuse?

A. Degaussing magnetic tapes when they\\'re no longer needed.

B. Deleting files on disk before reusing the space.

C. Clearing memory blocks before they are allocated to a program or data.

D. Clearing buffered pages, documents, or screens from the local memory of a terminal or printer.

Correct Answer: B

Object reuse requirements, applying to systems rated TCSEC C2 and above, are used to protect files, memory, and other objects in a trusted system from being accidentally accessed by users who are not authorized to access them. Deleting files on disk merely erases file headers in a directory structure. It does not clear data from the disk surface, thus making files still recoverable. All other options involve clearing used space, preventing any unauthorized access.

Source: RUSSEL, Deborah and GANGEMI, G.T. Sr., Computer Security Basics, O\\'Reilly, July 1992 (page 119).