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.geekcert.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 is not a form of passive attack?

A. Scavenging

B. Data diddling

C. Shoulder surfing

D. Sniffing

Correct Answer: B

Data diddling involves alteration of existing data and is extremely common. It is one of the easiest types of crimes to prevent by using access and accounting controls, supervision, auditing, separation of duties, and authorization limits. It is a form of active attack. All other choices are examples of passive attacks, only affecting confidentiality.

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

10: Law, Investigation, and Ethics (page 645).

QUESTION 2

Which of the following teams should NOT be included in an organization\\'s contingency plan?

A. Damage assessment team

B. Hardware salvage team

C. Tiger team

D. Legal affairs team

Correct Answer: C

According to NIST\\'s Special publication 800-34, a capable recovery strategy will require some or all of the following functional groups: Senior management official, management team, damage assessment team, operating system administration team, systems software team, server recovery team, LAN/WAN recovery team, database recovery team, network operations recovery team, telecommunications team, hardware salvage team, alternate site recovery coordination team, original site restoration/salvage coordination team, test team, administrative support team, transportation and relocation team, media relations team, legal affairs team, physical/personal security team, procurements team. Ideally, these teams would be staffed with the personnel responsible for the same or similar operation under normal conditions. A tiger team, originally a U.S. military jargon term, defines a team (of sneakers) whose purpose is to penetrate security, and thus test security measures. Used today for teams performing ethical hacking.

Source: SWANSON, Marianne, and al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 23).

QUESTION 3

How are memory cards and smart cards different?

A. Memory cards normally hold more memory than smart cards

B. Smart cards provide a two-factor authentication whereas memory cards don\\'t

C. Memory cards have no processing power

D. Only smart cards can be used for ATM cards

Correct Answer: C

The main difference between memory cards and smart cards is their capacity to process information. A memory card holds information but cannot process information. A smart card holds information and has the necessary hardware and software to actually process that information.

A memory card holds a user\\'s authentication information, so that this user needs only type in a user ID or PIN and presents the memory card to the system. If the entered information and the stored information match and are approved by an authentication service, the user is successfully authenticated.

A common example of a memory card is a swipe card used to provide entry to a building. The user enters a PIN and swipes the memory card through a card reader. If this is the correct combination, the reader flashes green and the individual can open the door and enter the building.

Memory cards can also be used with computers, but they require a reader to process the information. The reader adds cost to the process, especially when one is needed for every computer. Additionally, the overhead of PIN and card generation adds additional overhead and complexity to the whole authentication process. However, a memory card provides a more secure authentication method than using only a password because the attacker would need to obtain the card and know the correct PIN.

Administrators and management need to weigh the costs and benefits of a memory card implementation as well as the security needs of the organization to determine if it is the right authentication mechanism for their environment.

One of the most prevalent weaknesses of memory cards is that data stored on the card are not protected. Unencrypted data on the card (or stored on the magnetic strip) can be extracted or copied. Unlike a smart card, where security controls and logic are embedded in the integrated circuit, memory cards do not employ an inherent mechanism to protect the data from exposure.

Very little trust can be associated with confidentiality and integrity of information on the memory cards.

The following answers are incorrect:

"Smart cards provide two-factor authentication whereas memory cards don\\'t" is incorrect. This is not necessarily true. A memory card can be combined with a pin or password to offer two factors authentication where something you have and something you know are used for factors.

"Memory cards normally hold more memory than smart cards" is incorrect. While a memory card may or may not have more memory than a smart card, this is certainly not the best answer to the question.

"Only smart cards can be used for ATM cards" is incorrect. This depends on the decisions made by the particular institution and is not the best answer to the question.

Reference(s) used for this question:

Shon Harris, CISSP All In One, 6th edition , Access Control, Page 199 and also for people using the Kindle edition of the book you can look at Locations 4647-4650. Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition :

Access Control ((ISC)2 Press) (Kindle Locations 2124-2139). Auerbach Publications. Kindle Edition.

QUESTION 4

Which of the following steps should be one of the first step performed in a Business Impact Analysis (BIA)?

A. Identify all CRITICAL business units within the organization.

B. Evaluate the impact of disruptive events.

C. Estimate the Recovery Time Objectives (RTO).

D. Identify and Prioritize Critical Organization Functions

Correct Answer: D

Project Initiation and Management

This is the first step in building the Business Continuity program is project initiation and management. During this phase, the following activities will occur:

Obtain senior management support to go forward with the project

Define a project scope, the objectives to be achieved, and the planning assumptions

Estimate the project resources needed to be successful, both human resources and financial resources

Define a timeline and major deliverables of the project In this phase, the program will be managed like a project, and a project manager should be assigned to the BC and DR domain.

The next step in the planning process is to have the planning team perform a BIA. The BIA will help the company decide what needs to be recovered, and how quickly. Mission functions are typically designated with terms such as critical, essential, supporting and nonessential to help determine the appropriate prioritization.

One of the first steps of a BIA is to Identify and Prioritize Critical Organization Functions. All organizational functions and the technology that supports them need to be classified based on their recovery priority. Recovery time frames for organization operations are driven by the consequences of not performing the function. The consequences may be the result of organization lost during the down period; contractual commitments not met resulting in fines or lawsuits, lost goodwill with customers.

All other answers are incorrect.

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 21073-21075). Auerbach Publications. Kindle Edition.

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20697-20710). Auerbach Publications. Kindle Edition.

QUESTION 5

Which one of the following statements about the advantages and disadvantages of network-based Intrusion detection systems is true

A. Network-based IDSs are not vulnerable to attacks.

B. Network-based IDSs are well suited for modern switch-based networks.

C. Most network-based IDSs can automatically indicate whether or not an attack was successful.

D. The deployment of network-based IDSs has little impact upon an existing network.

Correct Answer: D

Network-based IDSs are usually passive devices that listen on a network wire without interfering with the normal operation of a network. Thus, it is usually easy to retrofit a network to include network-based IDSs with minimal effort.

Network-based IDSs are not vulnerable to attacks is not true, even thou network-based IDSs can be made very secure against attack and even made invisible to many attackers they still have to read the packets and sometimes a well crafted packet might exploit or kill your capture engine.

Network-based IDSs are well suited for modern switch-based networks is not true as most switches do not provide universal monitoring ports and this limits the monitoring range of a network-based IDS sensor to a single host. Even when switches provide such monitoring ports, often the single port cannot mirror all traffic traversing the switch.

Most network-based IDSs can automatically indicate whether or not an attack was successful is not true as most network-based IDSs cannot tell whether or not an attack was successful; they can only discern that an attack was initiated. This means that after a network-based IDS detects an attack, administrators must manually investigate each attacked host to determine whether it was indeed penetrated.

Reference:

NIST special publication 800-31 Intrusion Detection System pages 15-16

Official guide to the CISSP CBK. Pages 196 to 197