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.pass4itsure.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

In the statement below, fill in the blank:

Law enforcement agencies must get a warrant to search and seize an individual\\'s property, as stated in the _____ Amendment.

A. First.

B. Second.

C. Third.

D. Fourth.

Correct Answer: D

The Fourth Amendment does not apply to a seizure or an arrest by private citizens.

Search and seizure activities can get tricky depending on what is being searched for and where.

For example, American citizens are protected by the Fourth Amendment against unlawful search and seizure, so law enforcement agencies must have probable cause and request a search warrant from a judge or court before conducting such a search.

The actual search can only take place in the areas outlined by the warrant. The Fourth Amendment does not apply to actions by private citizens unless they are acting as police agents. So, for example, if Kristy\\'s boss warned all employees that the management could remove files from their computers at any time, and

her boss was not a police officer or acting as a police agent, she could not successfully claim that her

Fourth Amendment rights were violated. Kristy\\'s boss may have violated some specific privacy laws, but he

did not violate Kristy\\'s Fourth Amendment rights.

In some circumstances, a law enforcement agent may seize evidence that is not included in the warrant,

such as if the suspect tries to destroy the evidence. In other words, if there is an impending possibility that

evidence might be destroyed, law enforcement may quickly seize the evidence to prevent its destruction.

This is referred to as exigent circumstances, and a judge will later decide whether the seizure was proper

and legal before allowing the evidence to be admitted. For example, if a police officer had a search warrant

that allowed him to search a suspect\\'s living room but no other rooms, and then he saw the suspect

dumping cocaine down the toilet, the police officer could seize the cocaine even though it was in a room

not covered under his search warrant. After evidence is gathered, the chain of custody needs to be

enacted and enforced to make sure the evidence\\'s integrity is not compromised.

All other choices were only detractors.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One uide, 6th Edition (p. 1057). McGraw-Hill.

Kindle Edition.

QUESTION 2

What setup should an administrator use for regularly testing the strength of user passwords?

A. A networked workstation so that the live password database can easily be accessed by the cracking program.

B. A networked workstation so the password database can easily be copied locally and processed by the cracking program.

C. A standalone workstation on which the password database is copied and processed by the cracking program.

D. A password-cracking program is unethical; therefore it should not be used.

Correct Answer: C

Poor password selection is frequently a major security problem for any system\\'s security. Administrators should obtain and use password-guessing programs frequently to identify those users having easily guessed passwords.

Because password-cracking programs are very CPU intensive and can slow the system on which it is running, it is a good idea to transfer the encrypted passwords to a standalone (not networked) workstation. Also, by doing the work on a non-networked machine, any results found will not be accessible by anyone unless they have physical access to that system.

Out of the four choice presented above this is the best choice.

However, in real life you would have strong password policies that enforce complexity requirements and does not let the user choose a simple or short password that can be easily cracked or guessed. That would be the best choice if it was one of the choice presented.

Another issue with password cracking is one of privacy. Many password cracking tools can avoid this by only showing the password was cracked and not showing what the password actually is. It is masking the password being used from the person doing the cracking.

Source: National Security Agency, Systems and Network Attack Center (SNAC), The 60 Minute Network Security Guide, February 2002, page 8.

QUESTION 3

Which of the following are the two MOST common implementations of Intrusion Detection Systems?

A. Server-based and Host-based.

B. Network-based and Guest-based.

C. Network-based and Client-based.

D. Network-based and Host-based.

Correct Answer: D

The two most common implementations of Intrusion Detection are Network-based and Host- based.

IDS can be implemented as a network device, such as a router, switch, firewall, or dedicated device monitoring traffic, typically referred to as network IDS (NIDS).

The" (IDS) "technology can also be incorporated into a host system (HIDS) to monitor a single system for undesirable activities. " A network intrusion detection system (NIDS) is a network device .... that monitors traffic traversing the network segment for which it is integrated." Remember that NIDS are usually passive in nature.

HIDS is the implementation of IDS capabilities at the host level. Its most significant difference from NIDS is that related processes are limited to the boundaries of a single-host system. However, this presents advantages in effectively detecting objectionable activities because the IDS process is running directly on the host system, not just observing it from the network.

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 3649-3652). Auerbach Publications. Kindle Edition.

QUESTION 4

Which of the following embodies all the detailed actions that personnel are required to follow?

A. Standards

B. Guidelines

C. Procedures

D. Baselines

Correct Answer: C

Procedures are step-by-step instructions in support of of the policies, standards, guidelines and baselines.

The procedure indicates how the policy will be implemented and who does what to accomplish the tasks."

Standards is incorrect. Standards are a "Mandatory statement of minimum requirements that support some

part of a policy, the standards in this case is your own company standards and not standards such as the

ISO standards"

Guidelines is incorrect. "Guidelines are discretionary or optional controls used to enable individuals to

make judgments with respect to security actions."

Baselines is incorrect. Baselines "are a minimum acceptable level of security. This minimum is

implemented using specific rules necessary to implement the security controls in support of the policy and

standards." For example, requiring a password of at leat 8 character would be an example. Requiring all users to have a minimun of an antivirus, a personal firewall, and an anti spyware tool could be another example.

References:

CBK, pp. 12 - 16. Note especially the discussion of the "hammer policy" on pp. 16-17 for the differences between policy, standard, guideline and procedure.

AIO3, pp. 88-93.

QUESTION 5

Which of the following results in the most devastating business interruptions?

A. Loss of Hardware/Software

B. Loss of Data

C. Loss of Communication Links

D. Loss of Applications

Correct Answer: B

Source: Veritas eLearning CD - Introducing Disaster Recovery Planning, Chapter 1.

All of the others can be replaced or repaired. Data that is lost and was not backed up, cannot be restored.