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.leads4pass.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

In what way can violation clipping levels assist in violation tracking and analysis?

A. Clipping levels set a baseline for acceptable normal user errors, and violations exceeding that threshold will be recorded for analysis of why the violations occurred.

B. Clipping levels enable a security administrator to customize the audit trail to record only those violations which are deemed to be security relevant.

C. Clipping levels enable the security administrator to customize the audit trail to record only actions for users with access to user accounts with a privileged status.

D. Clipping levels enable a security administrator to view all reductions in security levels which have been made to user accounts which have incurred violations.

Correct Answer: A

Companies can set predefined thresholds for the number of certain types of errors that will be allowed before the activity is considered suspicious. The threshold is a baseline for violation activities that may be normal for a user to commit before alarms are raised. This baseline is referred to as a clipping level.

The following are incorrect answers:

Clipping levels enable a security administrator to customize the audit trail to record only those violations which are deemed to be security relevant. This is not the best answer, you would not record ONLY security relevant violations, all violations would be recorded as well as all actions performed by authorized users which may not trigger a violation. This could allow you to indentify abnormal activities or fraud after the fact.

Clipping levels enable the security administrator to customize the audit trail to record only actions for users with access to user accounts with a privileged status. It could record all security violations whether the user is a normal user or a privileged user.

Clipping levels enable a security administrator to view all reductions in security levels which have been made to user accounts which have incurred violations. The keyword "ALL" makes this question wrong. It may detect SOME but not all of violations. For example, application level attacks may not be detected.

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One uide, 6th Edition (p. 1239). McGraw-Hill. Kindle Edition.

and

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

QUESTION 2

Which of the following was designed to support multiple network types over the same serial link?

A. Ethernet

B. SLIP

C. PPP

D. PPTP

Correct Answer: C

The Point-to-Point Protocol (PPP) was designed to support multiple network types over the same serial

link, just as Ethernet supports multiple network types over the same LAN. PPP replaces the earlier Serial

Line Internet Protocol (SLIP) that only supports IP over a serial link. PPTP is a tunneling protocol.

Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 3:

TCP/IP from a Security Viewpoint.

QUESTION 3

Which of the following is immune to the effects of electromagnetic interference (EMI) and therefore has a much longer effective usable length?

A. Fiber Optic cable

B. Coaxial cable

C. Twisted Pair cable

D. Axial cable

Correct Answer: A

Fiber Optic cable is immune to the effects of electromagnetic interference (EMI) and therefore has a much longer effective usable length (up to two kilometers in some cases).

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 72.

QUESTION 4

Which of the following best describes signature-based detection?

A. Compare source code, looking for events or sets of events that could cause damage to a system or network.

B. Compare system activity for the behaviour patterns of new attacks.

C. Compare system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack.

D. Compare network nodes looking for objects or sets of objects that match a predefined pattern of objects that may describe a known attack.

Correct Answer: C

Misuse detectors compare system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack. As the patterns corresponding to known attacks are called signatures, misuse detection is sometimes called "signature-based detection."

The most common form of misuse detection used in commercial products specifies each pattern of events corresponding to an attack as a separate signature. However, there are more sophisticated approaches to doing misuse detection (called "state-based" analysis techniques) that can leverage a single signature to detect groups of attacks.

Reference: Old Document: BACE, Rebecca and MELL, Peter, NIST Special Publication 800-31 on Intrusion Detection Systems, Page

16.

The publication above has been replaced by 800-94 on page 2-4

The Updated URL is: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

QUESTION 5

What is the PRIMARY use of a password?

A. Allow access to files.

B. Identify the user.

C. Authenticate the user.

D. Segregate various user\\'s accesses.

Correct Answer: C

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