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

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

QUESTION 1

When an outgoing request is made on a port number greater than 1023, this type of firewall creates an ACL to allow the incoming reply on that port to pass:

A. packet filtering

B. CIrcuit level proxy

C. Dynamic packet filtering

D. Application level proxy

Correct Answer: C

The dynamic packet filtering firewall is able to create ACL\\'s on the fly to allow replies on dynamic ports (higher than 1023).

Packet filtering is incorrect. The packet filtering firewall usually requires that the dynamic ports be left open as a group in order to handle this situiation.

Circuit level proxy is incorrect. The circuit level proxy builds a conduit between the trusted and untrusted hosts and does not work by dynamically creating ACL\\'s.

Application level proxy is incorrect. The application level proxy "proxies" for the trusted host in its communications with the untrusted host. It does not dynamically create ACL\\'s to control traffic.

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

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 4

What are the three most important functions that Digital Signatures perform?

A. Integrity, Confidentiality and Authorization

B. Integrity, Authentication and Nonrepudiation

C. Authorization, Authentication and Nonrepudiation

D. Authorization, Detection and Accountability

Correct Answer: B

Reference: TIPTON, Harold F. and KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2.

QUESTION 5

What would BEST define a covert channel?

A. An undocumented backdoor that has been left by a programmer in an operating system

B. An open system port that should be closed.

C. A communication channel that allows transfer of information in a manner that violates the system\\'s security policy.

D. A trojan horse.

Correct Answer: C

The Answer: A communication channel that allows transfer of information in a manner that violates the system\\'s security policy. A covert channel is a way for an entity to receive information in an unauthorized manner. It is an information flow that is not controlled by a security mechanism. This type of information path was not developed for communication; thus, the system does not properly protect this path, because the developers never envisioned information being passed in this way. Receiving information in this manner clearly violates the system\\'s security policy. The channel to transfer this unauthorized data is the result of one of the following conditions:· Oversight in the development of the product

Improper implementation of access controls

Existence of a shared resource between the two entities

Installation of a Trojan horse The following answers are incorrect: An undocumented backdoor that has been left by a programmer in an operating system is incorrect because it is not a means by which unauthorized transfer of information takes place. Such backdoor is usually referred to as a Maintenance Hook. An open system port that should be closed is incorrect as it does not define a covert channel.

A trojan horse is incorrect because it is a program that looks like a useful program but when you install it it would include a bonus such as a Worm, Backdoor, or some other malware without the installer knowing about it.

Reference(s) used for this question:

Shon Harris AIO v3 , Chapter-5 : Security Models and Architecture

AIOv4 Security Architecture and Design (pages 343 - 344)

AIOv5 Security Architecture and Design (pages 345 - 346)