SSCP Valid Vce Dumps | Detailed SSCP Study Plan

ISC SSCP System Security Certified Practitioner (SSCP) 2

>> Latest SSCP Test Questions <<

SSCP Test Dumps & SSCP Valid Exam Book

We provide up-to-date System Security Certified Practitioner (SSCP) (SSCP) exam questions and study materials in three different formats. We have developed three variations of authentic ISC SSCP exam questions to cater to different learning preferences, ensuring that all candidates can effectively prepare for the SSCP Practice Test. Prep4cram offers System Security Certified Practitioner (SSCP) (SSCP) practice questions in PDF format, browser-based practice exams, and desktop practice test software.

ISC System Security Certified Practitioner (SSCP) Sample Questions (Q376-Q381):

NEW QUESTION # 376
What attack involves the perpetrator sending spoofed packet(s) wich contains the same destination and source IP address as the remote host, the same port for the source and destination, having the SYN flag, and targeting any open ports that are open on the remote host?

- A. Land attack
- B. Teardrop attack
- C. Boink attack
- D. Smurf attack

Answer: A

Explanation:
Explanation/Reference:
The Land attack involves the perpetrator sending spoofed packet(s) with the SYN flag set to the victim's machine on any open port that is listening. The packet(s) contain the same destination and source IP address as the host, causing the victim's machine to reply to itself repeatedly. In addition, most systems experience a total freeze up, where as CTRL-ALT-DELETE fails to work, the mouse and keyboard become non operational and the only method of correction is to reboot via a reset button on the system or by turning the machine off.
The Boink attack, a modified version of the original Teardrop and Bonk exploit programs, is very similar to the Bonk attack, in that it involves the perpetrator sending corrupt UDP packets to the host. It however allows the attacker to attack multiple ports where Bonk was mainly directed to port 53 (DNS).
The Teardrop attack involves the perpetrator sending overlapping packets to the victim, when their machine attempts to re-construct the packets the victim's machine hangs.
A Smurf attack is a network-level attack against hosts where a perpetrator sends a large amount of ICMP echo (ping) traffic at broadcast addresses, all of it having a spoofed source address of a victim. If the routing device delivering traffic to those broadcast addresses performs the IP broadcast to layer 2 broadcast function, most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply each, multiplying the traffic by the number of hosts responding. On a multi-access broadcast network, there could potentially be hundreds of machines to reply to each packet.
Resources:
http://en.wikipedia.org/wiki/Denial-of-service_attack
http://en.wikipedia.org/wiki/LAND

Latest SSCP Test Questions & SSCP Test Dumps

BTW, DOWNLOAD part of TestPassed SSCP dumps from Cloud Storage: https://drive.google.com/open?id=1FXj5HqhuJeYYqg-4D9fPkTl3qkeAbV1M

We are dedicated to providing an updated SSCP practice test material with these three formats: PDF, Web-Based practice exam, and Desktop practice test software. With our SSCP practice exam (desktop and web-based), you can evaluate and enhance your knowledge essential to crack the test. This step is critical to the success of your ISC SSCP Exam Preparation, as these practice tests help you identify your strengths and weaknesses.

ISC SSCP (System Security Certified Practitioner) certification exam is a globally recognized certification that validates the skills and knowledge of professionals in the field of system security. System Security Certified Practitioner (SSCP) certification is designed for those who wish to demonstrate their expertise in implementing, monitoring, and administering IT infrastructure in accordance with established security policies and procedures. System Security Certified Practitioner (SSCP) certification exam covers a wide range of topics, including access controls, cryptography, network and communications security, risk management, and security operations and administration.

Risk Identification, Analysis, & Monitoring (15%):

- Understanding the Process of Risk Management – It includes risk visibility & reporting, risk treatment, risk management frameworks, and risk management concepts;
- Performing Various Security Evaluation Activities – This objective covers audit finding remediation, remediation validation, interpreting & reporting testing and scanning results, as well as participating in security testing;
- Operating & Maintaining Monitoring Systems – This area includes the information about logging, events of interest, source

systems, as well as regulatory and legal concerns;
- Analyzing Monitoring Results – As for this domain, it requires the students' skills in performing event data analysis, finding security anomalies and baselines, as well as your knowledge about the visualization, trends, and metrics. It also covers their expertise in documenting and communicating findings.

>> SSCP Valid Vce Dumps <<

HOT SSCP Valid Vce Dumps - The Best ISC System Security Certified Practitioner (SSCP) - Detailed SSCP Study Plan

Our services before, during and after the clients use our SSCP certification material are considerate. Before the purchase, the clients can download and try out our SSCP learning file freely. During the clients use our products they can contact our online customer service staff to consult the problems about our products. Our company gives priority to the satisfaction degree of the clients on our SSCP Exam Questions and puts the quality of the service in the first place. We also have free demo of our SSCP learning guide for you to check the quality before your payment.

The SSCP exam covers seven domains, including access controls, security operations and administration, risk identification, monitoring and analysis, cryptography, network and communications security, and systems and application security. SSCP Exam consists of 125 multiple-choice questions and lasts for three hours. Candidates must score at least 700 out of 1000 points to pass the exam.

ISC System Security Certified Practitioner (SSCP) Sample Questions (Q893-Q898):

NEW QUESTION # 893
A periodic review of user account management should not determine:

- A. Whether active accounts are still being used.
- B. Strength of user-chosen passwords.
- C. Whether management authorizations are up-to-date.
- D. Conformity with the concept of least privilege.

Answer: B

Explanation:
Organizations should have a process for (1) requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.
Reviews should examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth.
These reviews can be conducted on at least two levels: (1) on an application-by-application basis, or (2) on a system wide basis.
The strength of user passwords is beyond the scope of a simple user account management review, since it requires specific tools to try and crack the password file/database through either a dictionary or brute-force attack in order to check the strength of passwords.
Reference(s) used for this question:
SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and
Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and
Practices for Securing Information Technology Systems, September 1996 (page 28).

NEW QUESTION # 894
Controlling access to information systems and associated networks is necessary for the preservation of their:

- A. authenticity,confidentiality, integrity and availability.
- B. integrity and availability.
- C. Confidentiality, integrity, and availability.
- D. Authenticity, confidentiality and availability

Answer: C

Explanation:
Section: Access Control
Explanation/Reference:
Controlling access to information systems and associated networks is necessary for the preservation of their confidentiality, integrity and availability.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 31.

NEW QUESTION # 895
A contingency plan should address:

- A. Identified risks.
- B. Potential risks.
- C. Residual risks.
- D. All answers are correct.

Answer: D

Explanation:
Section: Risk, Response and Recovery
Explanation/Reference:
Because it is rarely possible or cost effective to eliminate all risks, an attempt is made to reduce risks to an acceptable level through the risk assessment process. This process allows, from a set of potential risks (whether likely or not), to come up with a set of identified, possible risks.
The implementation of security controls allows reducing the identified risks to a smaller set of residual risks.
Because these residual risks represent the complete set of situations that could affect system performance, the scope of the contingency plan may be reduced to address only this decreased risk set.
As a result, the contingency plan can be narrowly focused, conserving resources while ensuring an effective system recovery capability.
Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page
7).

NEW QUESTION # 896
The Information Technology Security Evaluation Criteria (ITSEC) was written to address which of the following that the Orange Book did not address?

- A. integrity and availability.
- B. confidentiality and availability.
- C. integrity and confidentiality.
- D. none of the above.

Answer: A

Explanation:
TCSEC focused on confidentiality while ITSEC added integrity and availability as security goals.
The following answers are incorrect:
integrity and confidentiality. Is incorrect because TCSEC addressed confidentiality. confidentiality and availability. Is incorrect because TCSEC addressed confidentiality.
none of the above. Is incorrect because ITSEC added integrity and availability as security goals.

NEW QUESTION # 897
Which of the following can be best defined as computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data and for detecting or extracting the marks later?

- A. Digital enveloping
- B. Digital signature

- C. Steganography
- D. Digital watermarking

Answer: D

Explanation:
RFC 2828 (Internet Security Glossary) defines digital watermarking as computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data-text, graphics, images, video, or audio#and for detecting or extracting the marks later. The set of embedded bits (the digital watermark) is sometimes hidden, usually imperceptible, and always intended to be unobtrusive. It is used as a measure to protect intellectual property rights. Steganography involves hiding the very existence of a message. A digital signature is a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity. A digital envelope is a combination of encrypted data and its encryption key in an encrypted form that has been prepared for use of the recipient.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION # 898
.....