Latest ISC SSCP Practice test Material in Three Different Formats

P.S. Free & New SSCP dumps are available on Google Drive shared by itPass4sure: https://drive.google.com/open?id=1iQ5V5pGZP7LIuISlrdHfTzz0oEw2u8H-

itPass4sure never sells the useless SSCP certification SSCP exam dumps out. You will receive our SSCP exam dumps in time and get ISC Certification Certified easily. Try SSCP Exam free demo before you decide to buy it in itPass4sure. After you buy itPass4sure certification SSCP exam dumps, you will get free update for ONE YEAR!

To save you from loss of money and time, itPass4sure is offering a product that is specially designed to help you pass the System Security Certified Practitioner (SSCP) (SSCP) exam on the first try. The ISC SSCP Exam Dumps is easy to use and very easy to understand, ensuring that it is student-oriented. You can choose from 3 different formats available according to your needs. The 3 formats are desktop SSCP Practice Test software, web-based System Security Certified Practitioner (SSCP) (SSCP) practice exam, and SSCP dumps PDF format.

>> New SSCP Exam Dumps <<

Reliable SSCP Exam Prep - Exam SSCP Overview

Pass rate is 98.65% for SSCP exam cram, and we can help you pass the exam just one time. SSCP training materials cover most of knowledge points for the exam, and you can have a good command of these knowledge points through practicing, and you can also improve your professional ability in the process of learning. In addition, SSCP Exam Dumps have free demo for you to have a try, so that you can know what the complete version is like. We offer you free update for one year, and the update version will be sent to your mail automatically.

ISC System Security Certified Practitioner (SSCP) Sample Questions (Q98-Q103):

NEW QUESTION # 98
What are called user interfaces that limit the functions that can be selected by a user?

- A. Constrained user interfaces
- B. Limited user interfaces
- C. Unlimited user interfaces
- D. Mini user interfaces

Answer: A

Explanation:
Constrained user interfaces limit the functions that can be selected by a user.
Another method for controlling access is by restricting users to specific functions based on their role in the system. This is typically implemented by limiting available menus, data
views, encryption, or by physically constraining the user interfaces.
This is common on devices such as an automated teller machine (ATM). The advantage of a constrained user interface is that it limits potential avenues of attack and system failure by restricting the processing options that are available to the user.
On an ATM machine, if a user does not have a checking account with the bank he or she will not be shown the "Withdraw money from checking" option. Likewise, an information system might have an "Add/Remove Users" menu option for administrators, but if a normal, non-administrative user logs in he or she will not even see that menu option. By not even identifying potential options for non-qualifying users, the system limits the potentially harmful execution of unauthorized system or application commands.
Many database management systems have the concept of "views." A database view is an extract of the data stored in the database that is filtered based on predefined user or system criteria. This permits multiple users to access the same database while only having the ability to access data they need (or are allowed to have) and not data for another user.
The use of database views is another example of a constrained user interface.
The following were incorrect answers:
All of the other choices presented were bogus answers.
The following reference(s) were 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 1989-2002). Auerbach Publications. Kindle Edition.

NEW QUESTION # 99
During the salvage of the Local Area Network and Servers, which of the following steps would normally be performed first?

- A. Damage mitigation
- B. Recover equipment
- C. Install LAN communications network and servers
- D. Assess damage to LAN and servers

Answer: D

Explanation:
The first activity in every recovery plan is damage assessment, immediately followed by damage mitigation.
This first activity would typically include assessing the damage to all network and server components (including cables, boards, file servers, workstations, printers, network equipment), making a list of all items to be repaired or replaced, selecting appropriate vendors and relaying findings to Emergency Management Team.
Following damage mitigation, equipment can be recovered and LAN communications network and servers can be reinstalled.
Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 135).

NEW QUESTION # 100
Which of the following attacks could capture network user passwords?

- A. Sniffing
- B. IP Spoofing
- C. Smurfing
- D. Data diddling

Answer: A

Explanation:
A network sniffer captures a copy every packet that traverses the network segment the sniffer is connect to.

Sniffers are typically devices that can collect information from a communication medium, such as a network. These devices can range from specialized equipment to basic workstations with customized software.
A sniffer can collect information about most, if not all, attributes of the communication. The most common method of sniffing is to plug a sniffer into an existing network device like a hub or switch.
A hub (which is designed to relay all traffic passing through it to all of its ports) will automatically begin sending all the traffic on that network segment to the sniffing device. On the other hand, a switch (which is designed to limit what traffic gets sent to which port) will have to be specially configured to send all traffic to the port where the sniffer is plugged in.
Another method for sniffing is to use a network tap--a device that literally splits a network transmission into two identical streams; one going to the original network destination and the other going to the sniffing device. Each of these methods has its advantages and disadvantages, including cost, feasibility, and the desire to maintain the secrecy of the sniffing activity.
The packets captured by sniffer are decoded and then displayed by the sniffer. Therfore, if the username/password are contained in a packet or packets traversing the segment the sniffer is connected to, it will capture and display that information (and any other information on that segment it can see).
Of course, if the information is encrypted via a VPN, SSL, TLS, or similar technology, the information is still captured and displayed, but it is in an unreadable format.
The following answers are incorrect:
Data diddling involves changing data before, as it is enterred into a computer, or after it is extracted.
Spoofing is forging an address and inserting it into a packet to disguise the origin of the communication - or causing a system to respond to the wrong address.
Smurfing would refer to the smurf attack, where an attacker sends spoofed packets to the broadcast address on a gateway in order to cause a denial of service.

NEW QUESTION # 101
What is the name of the protocol use to set up and manage Security Associations (SA) for
IP Security (IPSec)?

- A. Oakley
- B. Internet Security Association and Key Management Protocol
- C. Internet Key Exchange (IKE)
- D. Secure Key Exchange Mechanism

Answer: C

Explanation:
The Key management for IPSec is called the Internet Key Exchange (IKE)
Note: IKE underwent a series of improvements establishing IKEv2 with RFC 4306. The basis of this answer is IKEv2.
The IKE protocol is a hybrid of three other protocols: ISAKMP (Internet Security Association and Key Management Protocol), Oakley and SKEME. ISAKMP provides a framework for authentication and key exchange, but does not define them (neither authentication nor key exchange). The Oakley protocol describes a series of modes for key exchange and the SKEME protocol defines key exchange techniques.
IKE-Internet Key Exchange. A hybrid protocol that implements Oakley and Skeme key exchanges inside the ISAKMP framework. IKE can be used with other protocols, but its initial implementation is with the IPSec protocol. IKE provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations. IKE is implemented in accordance with RFC 2409, The Internet Key Exchange.
The Internet Key Exchange (IKE) security protocol is a key management protocol standard that is used in conjunction with the IPSec standard. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. IKE is a hybrid protocol that implements the Oakley key exchange and the SKEME key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and SKEME are security protocols implemented by IKE.)
IKE automatically negotiates IPSec security associations (SAs) and enables IPSec secure communications without costly manual preconfiguration. Specifically, IKE provides these benefits:
Eliminates the need to manually specify all the IPSec security parameters in the crypto maps at both peers.
Allows you to specify a lifetime for the IPSec security association.
Allows encryption keys to change during IPSec sessions.
Allows IPSec to provide anti-replay services.
Permits certification authority (CA) support for a manageable, scalable IPSec implementation.
Allows dynamic authentication of peers.
About ISAKMP The Internet Security Association and Key Management Protocol (ISAKMP) is a framework that defines the phases for establishing a secure relationship and support for negotiation of security attributes, it does not establish sessions keys by itself, it is used along with the Oakley session key establishment protocol. The Secure Key Exchange Mechanism (SKEME)

describes a secure exchange mechanism and Oakley defines the modes of operation needed to establish a secure connection. ISAKMP provides a framework for Internet key management and provides the specific protocol support for negotiation of security attributes. Alone, it does not establish session keys. However it can be used with various session key establishment protocols, such as Oakley, to provide a complete solution to Internet key management. About Oakley The Oakley protocol uses a hybrid Diffie-Hellman technique to establish session keys on Internet hosts and routers. Oakley provides the important security property of Perfect Forward Secrecy (PFS) and is based on cryptographic techniques that have survived substantial public scrutiny. Oakley can be used by itself, if no attribute negotiation is needed, or Oakley can be used in conjunction with ISAKMP. When ISAKMP is used with Oakley, key escrow is not feasible.

The ISAKMP and Oakley protocols have been combined into a hybrid protocol. The resolution of ISAKMP with Oakley uses the framework of ISAKMP to support a subset of Oakley key exchange modes. This new key exchange protocol provides optional PFS, full security association attribute negotiation, and authentication methods that provide both repudiation and non-repudiation. Implementations of this protocol can be used to establish VPNs and also allow for users from remote sites (who may have a dynamically allocated IP address) access to a secure network.

About IPSec The IETF's IPSec Working Group develops standards for IP-layer security mechanisms for both IPv4 and IPv6. The group also is developing generic key management protocols for use on the Internet. For more information, refer to the IP Security and Encryption Overview.

IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides security for transmission of sensitive information over unprotected networks such as the Internet. It acts at the network level and implements the following standards:

IPSec

Internet Key Exchange (IKE)

Data Encryption Standard (DES)

MD5 (HMAC variant)

SHA (HMAC variant)

Authentication Header (AH)

Encapsulating Security Payload (ESP)

IPSec services provide a robust security solution that is standards-based. IPSec also provides data authentication and anti-replay services in addition to data confidentiality services.

For more information regarding IPSec, refer to the chapter "Configuring IPSec Network Security."

About SKEME

SKEME constitutes a compact protocol that supports a variety of realistic scenarios and security models over Internet. It provides clear tradeoffs between security and performance as required by the different scenarios without incurring in unnecessary system complexity. The protocol supports key exchange based on public key, key distribution centers, or manual installation, and provides for fast and secure key refreshment. In addition, SKEME selectively provides perfect forward secrecy, allows for replaceability and negotiation of the underlying cryptographic primitives, and addresses privacy issues as anonymity and repudiatability

SKEME's basic mode is based on the use of public keys and a Diffie-Hellman shared secret generation.

However, SKEME is not restricted to the use of public keys, but also allows the use of a pre-shared key. This key can be obtained by manual distribution or by the intermediary of a key distribution center (KDC) such as Kerberos.

In short, SKEME contains four distinct modes:

Basic mode, which provides a key exchange based on public keys and ensures PFS thanks to Diffie-Hellman.

A key exchange based on the use of public keys, but without Diffie-Hellman.

A key exchange based on the use of a pre-shared key and on Diffie-Hellman.

A mechanism of fast rekeying based only on symmetrical algorithms.

In addition, SKEME is composed of three phases: SHARE, EXCH and AUTH.

During the SHARE phase, the peers exchange half-keys, encrypted with their respective public keys. These two half-keys are used to compute a secret key K. If anonymity is wanted, the identities of the two peers are also encrypted. If a shared secret already exists, this phase is skipped.

The exchange phase (EXCH) is used, depending on the selected mode, to exchange either Diffie-Hellman public values or nonces. The Diffie-Hellman shared secret will only be computed after the end of the exchanges.

The public values or nonces are authenticated during the authentication phase (AUTH),

using the secret key established during the SHARE phase.
The messages from these three phases do not necessarily follow the order described above; in actual practice they are combined to minimize the number of exchanged messages.
References used for this question:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 172).
http://tools.ietf.org/html/rfc4306
http://tools.ietf.org/html/rfc4301
http://en.wikipedia.org/wiki/Internet_Key_Exchange
CISCO ISAKMP and OAKLEY information
CISCO Configuring Internet Key Exchange Protocol
http://www.hsc.fr/ressources/articles/ipsec-tech/index.html.en

NEW QUESTION # 102
Which of the following is the simplest type of firewall ?

- A. Dual-homed host firewall
- B. Packet filtering firewall
- C. Stateful packet filtering firewall
- D. Application gateway

Answer: B

Explanation:
Explanation/Reference:
A static packet filtering firewall is the simplest and least expensive type of firewalls, offering minimum security provisions to a low-risk computing environment.
A static packet filter firewall examines both the source and destination addresses of the incoming data packet and applies ACL's to them. They operates at either the Network or Transport layer. They are known as the First generation of firewall.
Older firewalls that were only packet filters were essentially routing devices that provided access control functionality for host addresses and communication sessions. These devices, also known as stateless inspection firewalls, do not keep track of the state of each flow of traffic that passes though the firewall; this means, for example, that they cannot associate multiple requests within a single session to each other.
Packet filtering is at the core of most modern firewalls, but there are few firewalls sold today that only do stateless packet filtering. Unlike more advanced filters, packet filters are not concerned about the content of packets. Their access control functionality is governed by a set of directives referred to as a ruleset.
Packet filtering capabilities are built into most operating systems and devices capable of routing; the most common example of a pure packet filtering device is a network router that employs access control lists.
There are many types of Firewall:
Application Level Firewalls - Often called a Proxy Server. It works by transferring a copy of each accepted data packet from one network to another. They are known as the Second generation of firewalls.
An application-proxy gateway is a feature of advanced firewalls that combines lower-layer access control with upper-layer functionality. These firewalls contain a proxy agent that acts as an intermediary between two hosts that wish to communicate with each other, and never allows a direct connection between them.
Each successful connection attempt actually results in the creation of two separate connections-one between the client and the proxy server, and another between the proxy server and the true destination.
The proxy is meant to be transparent to the two hosts-from their perspectives there is a direct connection.
Because external hosts only communicate with the proxy agent, internal IP addresses are not visible to the outside world. The proxy agent interfaces directly with the firewall ruleset to determine whether a given instance of network traffic should be allowed to transit the firewall.
Stateful Inspection Firewall - Packets are captured by the inspection engine operating at the network layer and then analyzed at all layers. They are known as the Third generation of firewalls.
Stateful inspection improves on the functions of packet filters by tracking the state of connections and blocking packets that deviate from the expected state. This is accomplished by incorporating greater awareness of the transport layer. As with packet filtering, stateful inspection intercepts packets at the network layer and inspects them to see if they are permitted by an existing firewall rule, but unlike packet filtering, stateful inspection keeps track of each connection in a state table. While the details of state table entries vary by firewall product, they typically include source IP address, destination IP address, port numbers, and connection state information.

Web Application Firewalls - The HTTP protocol used in web servers has been exploited by attackers in many ways, such as to place malicious software on the computer of someone browsing the web, or to fool a person into revealing private information that they might not have otherwise. Many of these exploits can be detected by specialized application firewalls called web application firewalls that reside in front of the web server.
Web application firewalls are a relatively new technology, as compared to other firewall technologies, and the type of threats that they mitigate are still changing frequently. Because they are put in front of web servers to prevent attacks on the server, they are often considered to be very different than traditional firewalls.
Host-Based Firewalls and Personal Firewalls - Host-based firewalls for servers and personal firewalls for desktop and laptop personal computers (PC) provide an additional layer of security against network-based attacks. These firewalls are software-based, residing on the hosts they are protecting-each monitors and controls the incoming and outgoing network traffic for a single host. They can provide more granular protection than network firewalls to meet the needs of specific hosts.
Host-based firewalls are available as part of server operating systems such as Linux, Windows, Solaris, BSD, and Mac OS X Server, and they can also be installed as third-party add-ons. Configuring a host- based firewall to allow only necessary traffic to the server provides protection against malicious activity from all hosts, including those on the same subnet or on other internal subnets not separated by a network firewall. Limiting outgoing traffic from a server may also be helpful in preventing certain malware that infects a host from spreading to other hosts.11 Host-based firewalls usually perform logging, and can often be configured to perform address-based and application-based access controls Dynamic Packet Filtering - Makes informed decisions on the ACL's to apply. They are known as the Fourth generation of firewalls.
Kernel Proxy - Very specialized architecture that provides modular kernel-based, multi-layer evaluation and runs in the NT executive space. They are known as the Fifth generation of firewalls.
The following were incorrect answers:
All of the other types of firewalls listed are more complex than the Packet Filtering Firewall.
Reference(s) used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 6th Edition, Telecommunications and Network Security, Page 630.
and
NIST Guidelines on Firewalls and Firewalls policies, Special Publication 800-4 Revision 1

NEW QUESTION # 103
.....

Our SSCP practice questions enjoy great popularity in this line. We provide our SSCP exam braindumps on the superior quality and being confident that they will help you expand your horizon of knowledge of the exam. They are time-tested SSCP Learning Materials, so they are classic. As well as our after-sales services. And we can always give you the most professional services on our SSCP training guide.

Reliable SSCP Exam Prep: https://www.itpass4sure.com/SSCP-practice-exam.html

ISC New SSCP Exam Dumps So our practice materials are triumph of their endeavor, Gone are the days when SSCP hadn't their place in the corporate world, Reliable SSCP Exam Prep Virtual Networks, Reliable SSCP Exam Prep Virtual Machines, Reliable SSCP Exam Prep Storage, Reliable SSCP Exam Prep Identity, Reliable SSCP Exam Prep App Service, Reliable SSCP Exam Prep Databases, and Reliable SSCP Exam Prep Workloads Automation, That is the reason why our ISC SSCP pass-for-sure materials can still occupy so much market share.

When you select SSCP latest pdf vce, you are sure to 100% pass your first time to participate in the difficult and critical SSCP Actual Test, Facebook Is Like a Conference: How Do You.

SSCP sure pass torrent & SSCP training questions & SSCP valid practice

So our practice materials are triumph of their endeavor, Gone are the days when SSCP hadn't their place in the corporate world, ISC Certification Virtual Networks, ISC Certification Virtual Machines, ISC Certification Storage, SSCP ISC Certification Identity, ISC Certification App Service, ISC Certification Databases, and ISC Certification Workloads Automation.

That is the reason why our ISC SSCP pass-for-sure materials can still occupy so much market share, Even you have finished buying our SSCP study guide with us, we still be around you with considerate services.

- SSCP Valid Test Blueprint □ SSCP Valid Test Blueprint □ New SSCP Test Vce □ Download □ SSCP □ for free by simply entering ▸ www.troytecdumps.com ◂ website □SSCP Valid Test Blueprint
- SSCP Valid Test Blueprint □ SSCP Free Practice Exams □ Latest SSCP Exam Papers □ Immediately open ☀ www.pdfvce.com □☀□ and search for ☀ SSCP □☀□ to obtain a free download □SSCP Exam Learning
- SSCP Guide □ Test SSCP Lab Questions □ SSCP Exam Learning □ Search for 【 SSCP 】 and obtain a free

download on ➤ www.validtorrent.com □ □Exam SSCP Details

- Trustworthy SSCP Source □ New SSCP Test Vce □ SSCP Study Guide □ Search on ➠ www.pdfvce.com □ for " SSCP " to obtain exam materials for free download □Learning SSCP Mode
- Verified ISC New SSCP Exam Dumps - Authorized www.pdfdumps.com - Leading Provider in Qualification Exams □ ➤ www.pdfdumps.com □ is best website to obtain ✔ SSCP □✔□ for free download □New SSCP Exam Question
- New SSCP Test Vce □ Latest SSCP Exam Papers □ SSCP Study Guide □ Search on ➠ www.pdfvce.com □ for 「 SSCP 」 to obtain exam materials for free download □SSCP Guide
- Free PDF Quiz Valid SSCP - New System Security Certified Practitioner (SSCP) Exam Dumps □ Easily obtain ▸ SSCP ◂ for free download through ☀ www.exam4labs.com □☀□ □Test SSCP Engine
- The latest ISC SSCP Exam free download □ Immediately open ⇛ www.pdfvce.com ⇚ and search for ➤ SSCP □ to obtain a free download □Exam SSCP Details
- Free PDF 2026 ISC Trustable SSCP: New System Security Certified Practitioner (SSCP) Exam Dumps □ Download ▸ SSCP ◂ for free by simply entering ➥ www.vce4dumps.com □ website □Trustworthy SSCP Source
- 2026 ISC Trustable SSCP: New System Security Certified Practitioner (SSCP) Exam Dumps □ Enter ▸ www.pdfvce.com ◂ and search for □ SSCP □ to download for free □SSCP Current Exam Content
- SSCP Reliable Test Duration □ SSCP Valid Test Tips □ Trustworthy SSCP Source □ Search for 【 SSCP 】 and download exam materials for free through ➤ www.prepawayete.com □ □Exam SSCP Details
- myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, bbs.t-firefly.com, Disposable vapes

P.S. Free & New SSCP dumps are available on Google Drive shared by itPass4sure: https://drive.google.com/open?id=1iQ5V5pGZP7LIuISlrdHfTzz0oEw2u8H-