

SSCP Exam Discount, SSCP Reliable Test Labs



ISC2 SSCP SSCP SSCP Exam Practice Test

ISC2 IT Fundamentals SSCP SSCP Practice exam, a way to boost your performance and acquiring 100% success in your final ISC2 IT Fundamentals SSCP SSCP exam. Such ISC2 IT Fundamentals SSCP exam gives you confidence to pass the ISC2 IT Fundamentals SSCP SSCP exam with only a single attempt. ISC2 IT Fundamentals SSCP Microsoft Azure Practice exams offer you a 100% of guaranteed success and gives you the confidence to be a ISC2 IT Fundamentals SSCP Microsoft Azure certified professional and have the credentials you need to be the outstanding ISC2 IT Fundamentals SSCP SSCP expert with mega skills. The one more plus point of these tests is of full syllabus coverage with hands-on-practice of different questions consist different scenarios.

Vendor	ISC2
Exam Code	SSCP
Exam Name	Systems Security Certified Practitioner
Related Certification	Systems Security Certified Practitioner
Related Technology	IT Fundamentals
Test Format	MCQ
Product Questions	1074 Questions
Exam Language	English
Questions Format	PDF + Online Practice Test Format
Price (Bundle)	\$92

Use authentic preparation material – Pass4Leads SSCP Practice Questions

You can easily pass your ISC2 SSCP SSCP exam if you prepare for your ISC2 SSCP Systems Security Certified Practitioner exam from an authentic source. Pass4Leads are highly reputed and can provide you with an authentic and real study material through which you can get success in Systems Security Certified Practitioner certification exam. You just need to get ISC2 SSCP IT Fundamentals study material from Pass4Leads who are known in the market. Not only focus on study material you also need to prepare through SSCP SSCP practice exam, which can increase your performance in the real ISC2 SSCP exam.

Sample output to test PDF Combine only

DOWNLOAD the newest It-Tests SSCP PDF dumps from Cloud Storage for free: <https://drive.google.com/open?id=1CBcDc1F0kuqGsXeoUMQJY9la6RtmglGp>

Our SSCP practice prep boosts varied functions to be convenient for you to master the SSCP training materials and get a good preparation for the exam and they include the self-learning function, the self-assessment function, the function to stimulate the exam and the timing function. We provide 24-hours online on SSCP Guide prep customer service and the long-distance professional personnel assistance to for the client. If clients have any problems about our study materials and we will solve the client's SSCP problems as quickly as we can.

Language of questions of SSCP Exam:

The ISC SSCP certification exam is administered separately in three languages. These languages are English, Japanese, and Brazilian Portuguese

What are the language, duration, and format of the ISC SSCP Certification Exam?

Details related to language, Duration, and format of the exam is as follows:

>> SSCP Exam Discount <<

Free PDF SSCP - The Best System Security Certified Practitioner (SSCP)

Exam Discount

You must want to receive our SSCP practice materials at the first time after payment. Don't worry. As long as you finish your payment, our online workers will handle your orders of the study materials quickly. The whole payment process lasts a few seconds. Besides that, you can ask what you want to know about our SSCP Study Guide. Once you submit your questions, we will soon give you detailed explanations. Even you come across troubles during practice the SSCP study materials; we will also help you solve the problems. We are willing to deal with your problems on SSCP learning guide.

ISC System Security Certified Practitioner (SSCP) Sample Questions (Q122-Q127):

NEW QUESTION # 122

When two or more separate entities (usually persons) operating in concert to protect sensitive functions or information must combine their knowledge to gain access to an asset, this is known as?

- A. Dual Control
- B. Segregation of duties
- C. Separation of duties
- D. Need to know

Answer: A

Explanation:

Section: Security Operation Administration

Explanation/Reference:

The question mentions clearly "operating together". Which means the BEST answer is Dual Control.

Two mechanisms necessary to implement high integrity environments where separation of duties is paramount are dual control or split knowledge.

Dual control enforces the concept of keeping a duo responsible for an activity. It requires more than one employee available to perform a task. It utilizes two or more separate entities (usually persons), operating together, to protect sensitive functions or information.

Whenever the dual control feature is limited to something you know, it is often called split knowledge (such as part of the password, cryptographic keys etc.) Split knowledge is the unique "what each must bring" and joined together when implementing dual control. To illustrate, let say you have a box containing petty cash is secured by one combination lock and one keyed lock. One employee is given the combination to the combo lock and another employee has possession of the correct key to the keyed lock. In order to get the cash out of the box both employees must be present at the cash box at the same time. One cannot open the box without the other. This is the aspect of dual control.

On the other hand, split knowledge is exemplified here by the different objects (the combination to the combo lock and the correct physical key), both of which are unique and necessary, that each brings to the meeting.

This is typically used in high value transactions / activities (as per the organizations risk appetite) such as:

Approving a high value transaction using a special user account, where the password of this user account is split into two and managed by two different staff. Both staff should be present to enter the password for a high value transaction. This is often combined with the separation of duties principle. In this case, the posting of the transaction would have been performed by another staff. This leads to a situation where collusion of at least 3 people are required to make a fraud transaction which is of high value. Payment Card and PIN printing is separated by SOD principles. Now the organization can even enhance the control mechanism by implementing dual control / split knowledge. The card printing activity can be modified to require two staff to key in the passwords for initiating the printing process. Similarly, PIN printing authentication can also be made to be implemented with dual control. Many Host Security modules (HSM) comes with built in controls for dual controls where physical keys are required to initiate the PIN printing process.

Managing encryption keys is another key area where dual control / split knowledge to be implemented.

PCI DSS defines Dual Control as below. This is more from a cryptographic perspective, still useful:

Dual Control: Process of using two or more separate entities (usually persons) operating in concert to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person is permitted to access or use the materials (for example, the cryptographic key). For manual key generation, conveyance, loading, storage, and retrieval, dual control requires dividing knowledge of the key among the entities. (See also Split Knowledge).

Split knowledge: Condition in which two or more entities separately have key components that individually convey no knowledge of the resultant cryptographic key.

It is key for information security professionals to understand the differences between Dual Control and Separation of Duties. Both complement each other, but are not the same.

The following were incorrect answers:

Segregation of Duties address the splitting of various functions within a process to different users so that it will not create an opportunity for a single user to perform conflicting tasks.

For example, the participation of two or more persons in a transaction creates a system of checks and balances and reduces the possibility of fraud considerably. So it is important for an organization to ensure that all tasks within a process has adequate separation.

Let us look at some use cases of segregation of duties

A person handling cash should not post to the accounting records

A loan officer should not disburse loan proceeds for loans they approved Those who have authority to sign cheques should not reconcile the bank accounts The credit card printing personal should not print the credit card PINs Customer address changes must be verified by a second employee before the change can be activated.

In situations where the separation of duties are not possible, because of lack of staff, the senior management should set up additional measure to offset the lack of adequate controls.

To summarise, Segregation of Duties is about Separating the conflicting duties to reduce fraud in an end to end function.

Need To Know (NTK):

The term "need to know", when used by government and other organizations (particularly those related to the military), describes the restriction of data which is considered very sensitive. Under need-to-know restrictions, even if one has all the necessary official approvals (such as a security clearance) to access certain information, one would not be given access to such information, unless one has a specific need to know; that is, access to the information must be necessary for the conduct of one's official duties. As with most security mechanisms, the aim is to make it difficult for unauthorized access to occur, without inconveniencing legitimate access. Need-to-know also aims to discourage "browsing" of sensitive material by limiting access to the smallest possible number of people.

EXAM TIP: HOW TO DECIPHER THIS QUESTION

First, you probably noticed that both Separation of Duties and Segregation of Duties are synonymous with each others. This means they are not the BEST answers for sure. That was an easy first step.

For the exam remember:

Separation of Duties is synonymous with Segregation of Duties

Dual Control is synonymous with Split Knowledge

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 16048-16078). Auerbach Publications. Kindle Edition.

and

<http://www.ciso.in/dual-control-or-segregation-of-duties/>

NEW QUESTION # 123

Which of the following security controls might force an operator into collusion with personnel assigned organizationally within a different function in order to gain access to unauthorized data?

- A. Job rotation of operations personnel
- B. Management monitoring of audit logs
- C. Limiting the local access of operations personnel
- D. Enforcing regular password changes

Answer: C

Explanation:

The questions specifically said: "within a different function" which eliminate Job Rotation as a choice.

Management monitoring of audit logs is a detective control and it would not prevent collusion.

Changing passwords regularly would not prevent such attack.

This question validates if you understand the concept of separation of duties and least privilege.

By having operators that have only the minimum access level they need and only what they need to do their duties within a company, the operations personnel would be force to use collusion to defeat those security mechanism.

NEW QUESTION # 124

A DMZ is located:

- A. right in front of your first Internet facing firewall
- B. right behind your first network passive Internet http firewall
- C. right behind your first Internet facing firewall

- D. right behind your first network active firewall

Answer: C

Explanation:

Explanation/Reference:

While the purpose of systems in the DMZ is to allow public access to certain internal network resources (EMAIL, DNS, Web), it is a good practice to restrict that access to the minimum necessary to provide those services through use of a firewall.

In computer security, a DMZ or Demilitarized Zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external attacker only has direct access to equipment in the DMZ, rather than any other part of the network. The name is derived from the term

"demilitarized zone", an area between nation states in which military operation is not permitted.

The following are incorrect answers:

"Right in front of your first Internet facing firewall" While the purpose of systems in the DMZ is to allow public access to certain internal network resources (EMAIL, DNS, Web), it is a good practice to restrict that access to the minimum necessary to provide those services through use of a firewall.

"Right behind your first network active firewall" This is an almost-right-sounding answer meant to distract the unwary.

"Right behind your first network passive Internet http firewall" This is an almost-right-sounding answer meant to distract the unwary.

References:

CBK, p. 434

and

AIO3, p. 483

and

http://en.wikipedia.org/wiki/DMZ_%28computing%29

NEW QUESTION # 125

Secure Shell (SSH-2) provides all the following services except:

- A. command execution
- **B. user authentication**
- C. secure remote login
- D. port forwarding

Answer: B

Explanation:

This is one of the tricky negative question. You have to pay close attention to the word EXCEPT within the question.

The SSH transport layer is a secure, low level transport protocol. It provides strong encryption, cryptographic host authentication, and integrity protection.

Authentication in this protocol level is host-based; this protocol does not perform user authentication. A higher level protocol for user authentication can be designed on top of this protocol.

The protocol has been designed to be simple and flexible to allow parameter negotiation, and to minimize the number of round-trips.

The key exchange method, public key algorithm, symmetric encryption algorithm, message authentication algorithm, and hash algorithm are all negotiated. It is expected that in most environments, only 2 round-trips will be needed for full key exchange, server authentication, service request, and acceptance notification of service request. The worst case is 3 round-trips.

The following are incorrect answers:

"Remote log-on" is incorrect. SSH does provide remote log-on. "Command execution" is incorrect. SSH does provide command execution.

"Port forwarding" is incorrect. SSH does provide port forwarding. SSH also has a wonderful feature called SSH Port Forwarding, sometimes called SSH Tunneling, which allows you to establish a secure SSH session and then tunnel arbitrary TCP connections through it. Tunnels can be created at any time, with almost no effort and no programming, which makes them very appealing. See the article below in the reference to take a look at SSH Port Forwarding in detail, as it is a very useful but often misunderstood technology. SSH Port Forwarding can be used for secure communications in a myriad of different ways.

You can see a nice tutorial on the PUTTY web site on how to use PUTTY to do port forwarding at:

<http://www.cs.uu.nl/technical/services/ssh/putty/puttyfw.html>

NEW QUESTION # 126

Which of the following outlined how senior management are responsible for the computer and information security decisions that they make and what actually took place within their organizations?

- A. The Computer Security Act of 1987.
- B. The Economic Espionage Act of 1996.
- C. The Computer Fraud and Abuse Act of 1986.
- **D. The Federal Sentencing Guidelines of 1991.**

Answer: D

Explanation:

Section: Risk, Response and Recovery

Explanation/Reference:

In 1991, U.S. Federal Sentencing Guidelines were developed to provide judges with courses of action in dealing with white collar crimes. These guidelines provided ways that companies and law enforcement should prevent, detect and report computer crimes. It also outlined how senior management are responsible for the computer and information security decisions that they make and what actually took place within their organizations.

NEW QUESTION # 127

• • • • •

The SSCP torrent prep contains the real questions and simulation questions of various qualifying examinations. It is very worthy of study efficiently. Time is constant development, and proposition experts will set questions of real SSCP exam continuously according to the progress of the society change tendency of proposition, and consciously highlight the hot issues and policy changes. In order to be able to better grasp the proposition thesis direction, the System Security Certified Practitioner (SSCP) study question focus on proposition which one recent theory and published, in all kinds of academic report even if update to find effective thesis points, according to the proposition of preferences and habits, ponder proposition style of topic selection, to update our SSCP Exam Question, to facilitate users of online learning, better fit time development hot spot.

SSCP Reliable Test Labs: <https://www.it-tests.com/SSCP.html>

- [illegible]

BONUS!!! Download part of It-Tests SSCP dumps for free: <https://drive.google.com/open?>

id=1CBcDc1F0kuqGsXeoUMQJY9la6RtmgIGp