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.passapply.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

Which of the following would be LESS likely to prevent an employee from reporting an incident?

A. They are afraid of being pulled into something they don\\'t want to be involved with.

B. The process of reporting incidents is centralized.

C. They are afraid of being accused of something they didn\\'t do.

D. They are unaware of the company\\'s security policies and procedures.

Correct Answer: B

The reporting process should be centralized else employees won\\'t bother.

The other answers are incorrect because :

They are afraid of being pulled into something they don\\'t want to be involved with is incorrect as most of

the employees fear of this and this would prevent them to report an incident. They are afraid of being

accused of something they didn\\'t do is also incorrect as this also prevents them to report an incident.

They are unaware of the company\\'s security policies and procedures is also incorrect as mentioned above.

Reference : Shon Harris AIO v3 , Ch-10 : Laws , Investigatio and Ethics , Page : 675.

QUESTION 2

What is NOT an authentication method within IKE and IPsec?

A. CHAP

B. Pre shared key

C. certificate based authentication

D. Public key authentication

Correct Answer: A

CHAP is not used within IPSEC or IKE. CHAP is an authentication scheme used by Point to Point Protocol (PPP) servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three-way handshake. This happens at the time of establishing the initial link (LCP), and may happen again at any time afterwards. The verification is based on a shared secret (such as the client user\\'s password).

After the completion of the link establishment phase, the authenticator sends a "challenge" message to the peer.

The peer responds with a value calculated using a one-way hash function on the challenge and the secret combined.

The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authenticator acknowledges the authentication; otherwise it should terminate the connection.

At random intervals the authenticator sends a new challenge to the peer and repeats steps 1 through 3.

The following were incorrect answers:

Pre Shared Keys

In cryptography, a pre-shared key or PSK is a shared secret which was previously shared between the two parties using some secure channel before it needs to be used. To build a key from shared secret, the key derivation function should be used. Such systems almost always use symmetric key cryptographic algorithms. The term PSK is used in WiFi encryption such as WEP or WPA, where both the wireless access points (AP) and all clients share the same key.

The characteristics of this secret or key are determined by the system which uses it; some system designs require that such keys be in a particular format. It can be a password like \\'bret13i\\', a passphrase like \\'Idaho hung gear id gene\\', or a hexadecimal string like \\'65E4 E556 8622 EEE1\\'. The secret is used by all systems involved in the cryptographic processes used to secure the traffic between the systems. Certificat Based Authentication

The most common form of trusted authentication between parties in the wide world of Web commerce is the exchange of certificates. A certificate is a digital document that at a minimum includes a Distinguished Name (DN) and an associated public key.

The certificate is digitally signed by a trusted third party known as the Certificate Authority (CA). The CA vouches for the authenticity of the certificate holder. Each principal in the transaction presents certificate as its credentials. The recipient then validates the certificate\\'s signature against its cache of known and trusted CA certificates. A "personal

certificate" identifies an end user in a transaction; a "server certificate" identifies the service provider.

Generally, certificate formats follow the X.509 Version 3 standard. X.509 is part of the Open Systems Interconnect

(OSI) X.500 specification.

Public Key Authentication

Public key authentication is an alternative means of identifying yourself to a login server, instead of typing a password. It is more secure and more flexible, but more difficult to set up.

In conventional password authentication, you prove you are who you claim to be by proving that you know the correct password. The only way to prove you know the password is to tell the server what you think the password is. This means that if the server has been hacked, or spoofed an attacker can learn your password.

Public key authentication solves this problem. You generate a key pair, consisting of a public key (which everybody is allowed to know) and a private key (which you keep secret and do not give to anybody). The private key is able to generate signatures. A signature created using your private key cannot be forged by anybody who does not have a copy of that private key; but anybody who has your public key can verify that a particular signature is genuine. So you generate a key pair on your own computer, and you copy the public key to the server. Then, when the server asks you to prove who you are, you can generate a signature using your private key. The server can verify that signature (since it has your public key) and allow you to log in. Now if the server is hacked or spoofed, the attacker does not gain your private key or password; they only gain one signature. And signatures cannot be re-used, so they have gained nothing.

There is a problem with this: if your private key is stored unprotected on your own computer, then anybody who gains access to your computer will be able to generate signatures as if they were you. So they will be able to log in to your server under your account. For this reason, your private key is usually encrypted when it is stored on your local machine, using a passphrase of your choice. In order to generate a signature, you must decrypt the key, so you have to type your passphrase.

References:

RFC 2409: The Internet Key Exchange (IKE); DORASWAMY, Naganand and HARKINS, Dan

Ipsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks, 1999, Prentice Hall PTR; SMITH, Richard E.

Internet Cryptography, 1997, Addison-Wesley Pub Co.; HARRIS, Shon, All-In-One CISSP Certification uide, 2001, McGraw-Hill/Osborne, page 467.

http://en.wikipedia.org/wiki/Pre-shared_key

http://www.home.umk.pl/~mgw/LDAP/RS.C4.JUN.97.pdf

http://the.earth.li/~sgtatham/putty/0.55/htmldoc/Chapter8.html#S8.1

QUESTION 3

An Architecture where there are more than two execution domains or privilege levels is called:

A. Ring Architecture.

B. Ring Layering

C. Network Environment.

D. Security Models

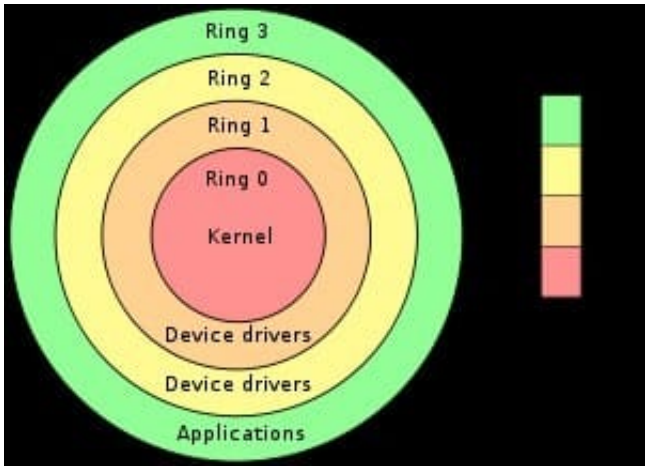
Correct Answer: A

In computer science, hierarchical protection domains, often called protection rings, are a mechanism to protect data and functionality from faults (fault tolerance) and malicious behavior (computer security). This approach is diametrically opposite to that of capability-based security.

Computer operating systems provide different levels of access to resources. A protection ring is one of two or more hierarchical levels or layers of privilege within the architecture of a computer system. This is generally hardware-enforced by some CPU architectures that provide different CPU modes at the hardware or microcode level. Rings are arranged in a hierarchy from most privileged (most trusted, usually numbered zero) to least privileged (least trusted, usually with the highest ring number). On most operating systems, Ring 0 is the level with the most privileges and interacts most directly with the physical hardware such as the CPU and memory.

Special gates between rings are provided to allow an outer ring to access an inner ring\\'s resources in a predefined manner, as opposed to allowing arbitrary usage. Correctly gating access between rings can improve security by preventing programs from one ring or privilege level from misusing resources intended for programs in another. For example, spyware running as a user program in Ring 3 should be prevented from turning on a web camera without informing the user, since hardware access should be a Ring 1 function reserved for device drivers. Programs such as web browsers running in higher numbered rings must request access to the network, a resource restricted to a lower numbered ring.

Ring Architecture



All of the other answers are incorrect because they are detractors.

References:

OIG CBK Security Architecture and Models (page 311)

and

https://en.wikipedia.org/wiki/Ring_%28computer_security%29

QUESTION 4

Which of the following is best defined as a mode of system termination that automatically leaves system processes and components in a secure state when a failure occurs or is detected in a system?

A. Fail proof

B. Fail soft

C. Fail safe

D. Fail Over

Correct Answer: C

NOTE: This question is referring to a system which is Logical/Technical, so it is in the context of a system

that you must choose the right answer. This is very important to read the question carefully and to identify

the context whether it is in the Physical world or in the Technical/Logical world.

RFC 2828 (Internet Security Glossary) defines fail safe as a mode of system termination that automatically

leaves system processes and components in a secure state when a failure occurs or is detected in the

system.

A secure state means in the Logical/Technical world that no access would be granted or no packets would

be allowed to flow through the system inspecting the packets such as a firewall for example.

If the question would have made reference to a building or something specific to the Physical world then

the answer would have been different. In the Physical World everything becomes open and full access

would be granted. See the valid choices below for the Physical context.

Fail-safe in the physical security world is when doors are unlocked automatically in case of emergency.

Used in environment where humans work around. As human safety is prime concern during Fire or other

hazards.

The following were all wrong choices:

Fail-secure in the physical security world is when doors are locked automatically in case of emergency.

Can be in an area like Cash Locker Room provided there should be alternative manually operated exit

door in case of emergency.

Fail soft is selective termination of affected non-essential system functions and processes when a failure

occurs or is detected in the system.

Fail Over is a redundancy mechanism and does not apply to this question.

There is a great post within the CCCure Forums on this specific

QUESTION 5

A department manager has read access to the salaries of the employees in his/her department but not to the salaries of employees in other departments. A database security mechanism that enforces this policy would typically be said to provide which of the following?

A. Content-dependent access control

B. Context-dependent access control

C. Least privileges access control

D. Ownership-based access control

Correct Answer: A

When access control is based on the content of an object, it is considered to be content dependent access control.

Content-dependent access control is based on the content itself.

The following answers are incorrect:

context-dependent access control. Is incorrect because this type of control is based on what the context is, facts about the data rather than what the object contains. least privileges access control. Is incorrect because this is based on the least amount of rights needed to perform their jobs and not based on what is contained in the database. ownership-

based access control. Is incorrect because this is based on the owner of the data and and not based on what is contained in the database.

References:

OIG CBK Access Control (page 191)