SSCP$^{Q\&As}$

System Security Certified Practitioner (SSCP)

Pass ISC SSCP Exam with 100% Guarantee

Following Questions and Answers are all new published by ISC Official Exam Center

QUESTION 1

The following is NOT a security characteristic we need to consider while choosing a biometric identification systems:

A. data acquisition process

B. cost

C. enrollment process

D. speed and user interface

Correct Answer: B

Cost is a factor when considering Biometrics but it is not a security characteristic.

All the other answers are incorrect because they are security characteristics related to Biometrics.

data acquisition process can cause a security concern because if the process is not fast and efficient it can discourage individuals from using the process.

enrollment process can cause a security concern because the enrollment process has to be quick and efficient. This process captures data for authentication.

speed and user interface can cause a security concern because this also impacts the users acceptance rate of biometrics. If they are not comfortable with the interface and speed they might sabotage the devices or otherwise attempt to circumvent them.

References:

OIG Access Control (Biometrics) (pgs 165-167)

From: TIPTON, Harold F. and KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Pages 5-6.

in process of correction

QUESTION 2

In SSL/TLS protocol, what kind of authentication is supported when you establish a secure session between a client and a server?

A. Peer-to-peer authentication

B. Only server authentication (optional)

C. Server authentication (mandatory) and client authentication (optional)

D. Role based authentication scheme

Correct Answer: C

RESCORLA, Eric, SSL and TLS: Designing and Building Secure Systems, 2000, Addison Wesley Professional; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

QUESTION 3

What is the name of the first mathematical model of a multi-level security policy used to define the concept of a secure state, the modes of access, and rules for granting access?

A. Clark and Wilson Model

B. Harrison-Ruzzo-Ullman Model

C. Rivest and Shamir Model

D. Bell-LaPadula Model

Correct Answer: D

Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 4

Which of the following is the simplest type of firewall ?

A. Stateful packet filtering firewall

B. Packet filtering firewall

C. Dual-homed host firewall

D. Application gateway

Correct Answer: B

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 uide, 6th Edition, Telecommunications and Network Security, Page 630. and NIST Guidelines on Firewalls and Firewalls policies, Special Publication 800-4 Revision 1

QUESTION 5

A public key algorithm that does both encryption and digital signature is which of the following?

A. RSA

B. DES

C. IDEA

D. Diffie-Hellman

Correct Answer: A

RSA can be used for encryption, key exchange, and digital signatures.

Key Exchange versus key Agreement

KEY EXCHANGE Key exchange (also known as "key establishment") is any method in cryptography by which cryptographic keys are exchanged between users, allowing use of a cryptographic algorithm.

If sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received. The nature of the equipping they require depends on the encryption technique they might use. If they use a code, both will require a copy of the same codebook. If they use a cipher, they will need appropriate keys. If the cipher is a symmetric key cipher, both will need a copy of the same key. If an asymmetric key cipher with the public/private key property, both will need the other\\'s public key.

KEY AGREEMENT

Diffie-Hellman is a key agreement algorithm used by two parties to agree on a shared secret. The Diffie Hellman (DH) key agreement algorithm describes a means for two parties to agree upon a shared secret over a public network in such a way that the secret will be unavailable to eavesdroppers. The DH algorithm converts the shared secret into an arbitrary amount of keying material. The resulting keying material is used as a symmetric encryption key.

The other answers are not correct because:

DES and IDEA are both symmetric algorithms.

Diffie-Hellman is a common asymmetric algorithm, but is used only for key agreement. It is not typically

used for data encryption and does not have digital signature capability.

References:

http://tools.ietf.org/html/rfc2631

For Diffie-Hellman information: http://www.netip.com/articles/keith/diffie-helman.htm

SSCP Study Guide SSCP Exam Questions SSCP Braindumps