Free Questions for ISSEP by certscare

Shared by Fernandez on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A security policy is an overall general statement produced by senior management that dictates what role security plays within the organization. Which of the following are required to be addressed in a well designed policy? Each correct answer represents a part of the solution. Choose all that apply.

Options:

A- What is being secured?

B- Who is expected to comply with the policy?

C- Where is the vulnerability, threat, or risk?

D- Who is expected to exploit the vulnerability?

Answer:

A, B, C

Explanation:

A security policy is an overall general statement produced by senior management (or a selected policy board or committee) that dictates what role security plays within the organization.

A well designed policy addresses the following:

What is being secured? - Typically an asset.

Who is expected to comply with the policy? - Typically employees.

Where is the vulnerability, threat, or risk? - Typically an issue of integrity or responsibility.

Question 2

Question Type: **MultipleChoice**

Which of the following security controls works as the totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy?

Options:

A- Trusted computing base (TCB)

B- Common data security architecture (CDSA)

C- Internet Protocol Security (IPSec)

D- Application program interface (API)

Answer:

A

Explanation:

Trusted computing base (TCB) refers to hardware, software, controls, and processes that cause a computer system or network to be devoid of malicious software or hardware. Maintaining the trusted computing base (TCB) is essential for security policy to be implemented successfully.

Answer option C is incorrect. Internet Protocol Security (IPSec) is a standard-based protocol that provides the highest level of VPN security. IPSec can encrypt virtually everything above the networking layer. It is used for VPN connections that use the L2TP protocol. It secures both

data and password. IPSec cannot be used with Point-to-Point Tunneling Protocol (PPTP).

Answer option B is incorrect. The Common data security architecture (CDSA) is a set of layered security services and cryptographic framework.

It deals with the communications and data security problems in the emerging Internet and intranet application space. It presents an

infrastructure for building cross-platform, interoperable, security-enabled applications for client-server environments.

Answer option D is incorrect. An application programming interface (API) is an interface implemented by a software program which enables it

to interact with other software. It facilitates interaction between different software programs similar to the way the user interface facilitates

interaction between humans and computers. An API is implemented by applications, libraries, and operating systems to determine their

vocabularies and calling conventions, and is used to access their services. It may include specifications for routines, data structures, object

classes, and protocols used to communicate between the consumer and the implementer of the API.

Question 3

Question Type: MultipleChoice

You have been tasked with finding an encryption methodology that will encrypt most types of email attachments. The requirements are that your solution must use the RSA algorithm. Which of the following is your best choice?

Options:

A- PGP

B- S/MIME

C- DES

D- Blowfish

Answer:

B

Explanation:

Secure/MIME, a version of the MIME protocol that supports encryption of messages and is based on

RSA's public-key encryption. Multipurpose

Internet Mail Extensions (MIME) is an Internet standard for email attachments.

Answer options D and C are incorrect. Blowfish and DES are both symmetric key algorithms and they

are not used with email attachments.

Answer option A is incorrect. PGP (Pretty Good Privacy) is used to secure email, but not email

attachments, and it is not based on RSA.

Question 4

Question Type: MultipleChoice

Which of the following categories of system specification describes the technical, performance,

operational, maintenance, and support characteristics for the entire system?

Options:

A- Process specification

B- Product specification

C- Development specification

D- System specification

Answer:

D

Explanation:

The various system specification categories are as follows:

Question 5

Question Type: MultipleChoice

Which of the following memorandums directs the Departments and Agencies to post clear privacy

policies on World Wide Web sites, and provides guidance for doing it?

Options:

A- OMB M-99-18

B- OMB M-00-13

C- OMB M-03-19

D- OMB M-00-07

Answer:

A

Explanation:

The OMB M-99-18 memorandum instructs Federal departments and agencies to post clear privacy

policies on World Wide Web (WWW) sites. It

also provides the assistance on posting the privacy policies. The policy states that the agencies should clearly and concisely inform visitors accessing their Web sites what information the agency collects about individuals, why the agency collects it, and how the agency will use it.

The privacy policies should be clearly labeled and easily accessed when someone visits a Web site.

Answer option D is incorrect. The OMB M-00-07 memorandum emphasizes that security should be built into and funded as part of the system architecture.

Answer option B is incorrect. The OMB M-00-13 memorandum reminds the Federal agencies that it is required by law and policy to establish clear privacy policies for Web activities and to comply with those policies.

Answer option C is incorrect. The OMB M-03-19 memorandum reports the instructions for the Federal Information Security Management Act and Updated Guidance on quarterly IT security reporting.

Question 6

Question Type: MultipleChoice

Which of the following are the ways of sending secure e-mail messages over the Internet?

Each correct answer represents a complete solution. Choose two.

Options:

A- PGP

B- S/MIME

C- TLS

D- IPSec

Answer:

A, B

Explanation:

Pretty Good Privacy (PGP) and Secure Multipurpose Internet Mail Extensions (S/MIME) are two ways

of sending secure e-mail messages over the

Internet. Both use public key cryptography, where users each possess two keys, a public key for

encrypting, and a private key for decrypting

messages. Because PGP has evolved from a free distribution, it is more popular than S/MIME.

Answer option C is incorrect. Transport Layer Security (TLS) is an application layer protocol that uses

a combination of public and symmetric

key processing to encrypt data.

Answer option D is incorrect. Internet Protocol Security (IPSec) is a standard-based protocol that

provides the highest level of VPN security.

IPSec can encrypt virtually everything above the networking layer. It is used for VPN connections

that use the L2TP protocol. It secures both

data and password.

IPSec cannot be used with Point-to-Point Tunneling Protocol (PPTP).

Question 7

Question Type: MultipleChoice

Which of the following DITSCAP/NIACAP model phases is used to confirm that the evolving system development and integration complies with the agreements between role players documented in the first phase?

Options:

A- Verification

B- Validation

C- Post accreditation

D- Definition

Answer:

A