D. Logical controls

Correct Answer: C

Explanation:

Administrative, technical and physical controls are categories of access control mechanisms.

Logical and Technical controls are synonymous. So both of them could be eliminated as possible choices.

Physical Controls: These are controls to protect the organization's people and physical environment, such as locks, gates, and guards. Physical controls may be called "operational controls" in some contexts.

Physical security covers a broad spectrum of controls to protect the physical assets (primarily the people) in an organization. Physical Controls are sometimes referred to as "operational" controls in some risk management frameworks. These controls range from doors, locks, and windows to environment controls, construction standards, and guards. Typically, physical security is based on the notion of establishing security zones or concentric areas within a facility that require increased security as you get closer to the valuable assets inside the facility. Security zones are the physical representation of the defense-in-depth principle discussed earlier in this chapter. Typically, security zones are associated with rooms, offices, floors, or smaller elements, such as a cabinet or storage locker. The design of the physical security controls within the facility must take into account the protection of the asset as well as the individuals working in that area.

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 1301-1303). Auerbach Publications. Kindle Edition. Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1312-1318). Auerbach Publications. Kindle Edition.

QUESTION 176

Why do buffer overflows happen? What is the main cause?

- A. Because buffers can only hold so much data
- B. Because of improper parameter checking within the application
- C. Because they are an easy weakness to exploit
- D. Because of insufficient system memory

Correct Answer: B

Explanation:

Buffer Overflow attack takes advantage of improper parameter checking within the application. This is the classic form of buffer overflow and occurs because the programmer accepts whatever input the user supplies without checking to make sure that the length of the input is less than the size of the buffer in the program.

The buffer overflow problem is one of the oldest and most common problems in software development and programming, dating back to the introduction of interactive computing. It can result when a program fills up the assigned buffer of memory with more data than its buffer can hold. When the program begins to write beyond the end of the buffer, the program's execution path can be changed, or data can be written into areas used by the operating system itself. This can lead to the insertion of malicious code that can be used to gain administrative privileges on the program or system.

SSCP Exam Dumps SSCP PDF Dumps SSCP VCE Dumps SSCP Q&As https://www.ensurepass.com/SSCP.html

As explained by Gaurab, it can become very complex. At the time of input even if you are checking the length of the input, it has to be check against the buffer size. Consider a case where entry point of data is stored in Buffer1 of Application1 and then you copy it to Buffer2 within Application2 later on, if you are just checking the length of data against Buffer1, it will not ensure that it will not cause a buffer overflow in Buffer2 of Application2.

A bit of reassurance from the ISC2 book about level of Coding Knowledge needed for the exam: It should be noted that the CISSP is not required to be an expert programmer or know the inner workings of developing application software code, like the FORTRAN programming language, or how to develop Web applet code using Java. It is not even necessary that the CISSP know detailed security-specific coding practices such as the major divisions of buffer overflow exploits or the reason for preferring str(n)cpy to strcpy in the C language (although all such knowledge is, of course, helpful). Because the CISSP may be the person responsible for ensuring that security is included in such developments, the CISSP should know the basic procedures and concepts involved during the design and development of software programming. That is, in order for the CISSP must understand the fundamental concepts of programming developments and the security strengths and weaknesses of various application development processes.

The following are incorrect answers:

"Because buffers can only hold so much data" is incorrect. This is certainly true but is not the best answer because the finite size of the buffer is not the problem -- the problem is that the programmer did not check the size of the input before moving it into the buffer.

"Because they are an easy weakness to exploit" is incorrect. This answer is sometimes true but is not the best answer because the root cause of the buffer overflow is that the programmer did not check the size of the user input.

"Because of insufficient system memory" is incorrect. This is irrelevant to the occurrence of a buffer overflow.

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 13319-13323). Auerbach Publications. Kindle Edition.

QUESTION 177

Smart cards are an example of which type of control?

- A. Detective control
- B. Administrative control
- C. Technical control
- D. Physical control

Correct Answer: C

Explanation:

Logical or technical controls involve the restriction of access to systems and the protection of information. Smart cards and encryption are examples of these types of control.

Controls are put into place to reduce the risk an organization faces, and they come in three main flavors: administrative, technical, and physical. Administrative controls are commonly referred to as "soft controls" because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Technical controls (also called logical controls) are software or hardware components, as in firewalls, IDS, encryption, identification and authentication mechanisms. And physical controls are

SSCP Exam Dumps SSCP PDF Dumps SSCP VCE Dumps SSCP Q&As https://www.ensurepass.com/SSCP.html

items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.

Many types of technical controls enable a user to access a system and the resources within that system. A technical control may be a username and password combination, a Kerberos implementation, biometrics, public key infrastructure (PKI), RADIUS, TACACS +, or authentication using a smart card through a reader connected to a system. These technologies verify the user is who he says he is by using different types of authentication methods. Once a user is properly authenticated, he can be authorized and allowed access to network resources.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 245). McGraw- Hill. Kindle Edition.

KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 32).

QUESTION 178

Which of the following is NOT true of the Kerberos protocol?

- A. Only a single login is required per session.
- B. The initial authentication steps are done using public key algorithm.
- C. The KDC is aware of all systems in the network and is trusted by all of them
- D. It performs mutual authentication

Correct Answer: B

Explanation:

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. It has the following characteristics:

It is secure: it never sends a password unless it is encrypted. Only a single login is required per session. Credentials defined at login are then passed between resources without the need for additional logins. The concept depends on a trusted third party - a Key Distribution Center (KDC). The KDC is aware of all systems in the network and is trusted by all of them. It performs mutual authentication, where a client proves its identity to a server and a server proves its identity to the client.

Kerberos introduces the concept of a Ticket-Granting Server/Service (TGS). A client that wishes to use a service has to receive a ticket from the TGS - a ticket is a time-limited cryptographic message - giving it access to the server. Kerberos also requires an Authentication Server (AS) to verify clients. The two servers combined make up a KDC.

Within the Windows environment, Active Directory performs the functions of the KDC. The following figure shows the sequence of events required for a client to gain access to a service using Kerberos authentication. Each step is shown with the Kerberos message associated with it, as defined in RFC 4120 "The Kerberos Network Authorization Service (V5)".



Kerberos Authentication Step by Step

Step 1: The user logs on to the workstation and requests service on the host. The workstation sends a message to the Authorization Server requesting a ticket granting ticket (TGT).

Step 2: The Authorization Server verifies the user's access rights in the user database and creates a TGT and session key. The Authorization Sever encrypts the results using a key derived from the user's password and sends a message back to the user workstation.

The workstation prompts the user for a password and uses the password to decrypt the incoming message. When decryption succeeds, the user will be able to use the TGT to request a service ticket.

Step 3: When the user wants access to a service, the workstation client application sends a request to the Ticket Granting Service containing the client name, realm name and a timestamp. The user proves his identity by sending an authenticator encrypted with the session key received in Step 2.

Step 4: The TGS decrypts the ticket and authenticator, verifies the request, and creates a ticket for the requested server. The ticket contains the client name and optionally the client IP address. It also contains the realm name and ticket lifespan. The TGS returns the ticket to the user workstation. The returned message contains two copies of a server session key ?one encrypted with the client password, and one encrypted by the service password.

Step 5: The client application now sends a service request to the server containing the ticket received in Step 4 and an authenticator. The service authenticates the request by decrypting the session key. The server verifies that the ticket and authenticator match, and then grants access

SSCP Exam Dumps SSCP PDF Dumps SSCP VCE Dumps SSCP Q&As https://www.ensurepass.com/SSCP.html

to the service. This step as described does not include the authorization performed by the Intel AMT device, as described later.

Step 6: If mutual authentication is required, then the server will reply with a server authentication message.

The Kerberos server knows "secrets" (encrypted passwords) for all clients and servers under its control, or it is in contact with other secure servers that have this information. These "secrets" are used to encrypt all of the messages shown in the figure above. To prevent "replay attacks," Kerberos uses timestamps as part of its protocol definition. For timestamps to work properly, the clocks of the client and the server need to be in synch as much as possible. In other words, both computers need to be set to the same time and date. Since the clocks of two computers are often out of synch, administrators can establish a policy to establish the maximum acceptable difference to Kerberos between a client's clock and server's clock. If the difference between a client's clock and the server's clock is less than the maximum time difference specified in this policy, any timestamp used in a session between the two computers will be considered authentic. The maximum difference is usually set to five minutes.

Note that if a client application wishes to use a service that is "Kerberized" (the service is configured to perform Kerberos authentication), the client must also be Kerberized so that it expects to support the necessary message responses. For more information about Kerberos, see http://web.mit.edu/kerberos/www/.

References:

Introduction to Kerberos Authentication from Intel http://www.zeroshell.net/eng/kerberos/Kerberos-definitions/#1.3.5.3 http://www.ietf.org/rfc/rfc4120.txt

QUESTION 179

Which access control model would a lattice-based access control model be an example of?

- A. Mandatory access control.
- B. Discretionary access control.
- C. Non-discretionary access control.
- D. Rule-based access control.

Correct Answer: A

Explanation:

In a lattice model, there are pairs of elements that have the least upper bound of values and greatest lower bound of values. In a Mandatory Access Control (MAC) model, users and data owners do not have as much freedom to determine who can access files.

TIPS FROM CLEMENT

Mandatory Access Control is in place whenever you have permissions that are being imposed on the subject and the subject cannot arbitrarily change them. When the subject/owner of the file can change permissions at will, it is discretionary access control.

Here is a breakdown largely based on explanations provided by Doug Landoll. I am reproducing below using my own word and not exactly how Doug explained it:

FIRST: The Lattice

A lattice is simply an access control tool usually used to implement Mandatory Access Control (MAC) and it could also be used to implement RBAC but this is not as common. The lattice model can be used for Integrity level or file permissions as well. The lattice has a least upper bound and

SSCP Exam Dumps SSCP PDF Dumps SSCP VCE Dumps SSCP Q&As https://www.ensurepass.com/SSCP.html