Domain 3: Security Architecture and Engineering

Test ID: 175720902

Pregunta #1 de 193

Id. de pregunta: 1105091

Su organización está considerando si construir o comprar una nueva instalación. ¿Qué factor de accesibilidad debe tenerse en cuenta durante la fase de construcción o adquisición de una infraestructura de instalación?

- ✗ **A)** población de la zona
- ✓ **B)** tráfico
- ✗ **C)** terreno peligroso
- ✗ **D)** tasa de criminalidad

explicación

La densidad del tráfico debe tenerse en cuenta durante la fase de adquisición de la instalación. La ubicación de la instalación debe proporcionar un fácil acceso a los servicios de transporte con fines de desplazamiento y para responder a situaciones de emergencia.

La tasa de criminalidad es una consideración de seguridad importante al decidir la ubicación de la instalación de procesamiento de información, pero no es una consideración de accesibilidad.

El terreno peligroso es una consideración importante en el marco de los desastres naturales y no es una consideración de accesibilidad. No debe elegir un lugar donde las inundaciones, terremotos, tornados, huracanes, deslizamientos de tierra, caída de rocas de las montañas o nevadas excesivas puedan interrumpir las operaciones de las instalaciones.

La población de la zona se incluye en consideraciones de visibilidad y no en consideraciones de accesibilidad.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar principios de seguridad al diseño de sitios e instalaciones

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Accesibilidad

Pregunta #2 de 193

Id. de pregunta: 1114698

¿Cuál de las siguientes afirmaciones con respecto a la computación en la nube y la computación en red son ciertas?

un. Tanto la computación en la nube como la computación en red son escalables.

B. La computación en red es adecuada para almacenar objetos tan pequeños como 1 byte.

c. La computación en la nube puede ser más respetuosa con el medio ambiente que la computación en red.

d. La computación en la nube se compone de clientes ligeros, computación en red y computación de utilidades.

- ✗ **A)** opciones A y B
- ✗ **B)** Opción d
- ✓ **C)** opciones a, c y d
- ✗ **D)** opción c
- ✗ **E)** todas las opciones
- ✗ **F)** opciones a, b y c
- ✗ **G)** opción b
- ✗ **H)** opción A

explicación

Tanto la computación en la nube como la computación en red son escalables. La computación en la nube se compone de clientes ligeros, computación en red y computación de utilidad. La computación en la nube puede ser más respetuosa con el medio ambiente que la computación en red.

La computación en red NO es adecuada para almacenar objetos tan pequeños como 1 byte.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
evaluar y mitigar las vulnerabilidades de las arquitecturas de seguridad, los diseños y los elementos de la solución

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Grid Computing

Computación en la nube frente a computación en red, http://www.ibm.com/developerworks/web/library/wa-cloudgrid/

Question #3 of 193

Question ID: 1111720

¿En qué modo 3DES NO funciona?

✗ **A)** DES-EEE2

✗ **B)** DES-EEE3

✗ **C)** DES-EDE3

✓ **D)** DES-DDD2

explicación

DES-DDD2 NO es un modo de una operación 3DES.

Triple Data Encryption Standard (3DES) presenta una alta resistencia al criptoanálisis diferencial porque utiliza 48 rondas de cálculo en comparación con DES que utiliza 16 rondas de cálculo. Triple DES es la nueva y mejorada versión de DES con una clave de 168 bits. El cifrado y descifrado por 3DES tarda más tiempo debido a la mayor longitud de la clave y la mayor potencia de procesamiento necesaria para derivar la clave secreta. Una operación 3DES puede funcionar en los modos siguientes:

- DES-EEE3 que utiliza tres claves diferentes para el cifrado.
- DES-EDE3 que utiliza tres claves diferentes para cifrar, descifrar y, a continuación, volver a cifrar los datos, respectivamente. Este proceso lo convierte en la forma más segura de cifrado 3DES.
- DES-EEE2 y DES-EDE2 funcionan de forma similar a DES-EDE3. Sin embargo, utilizan sólo dos claves. El primer y tercer proceso de cifrado utilizan la misma clave.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, modos DES

Question #4 of 193

Question ID: 1192937

Haga clic en cada uno de los encabezados del escenario para expandir o contraer su contenido. Debe leer todo el escenario para responder a la pregunta.

fondo

Usted es un profesional de la seguridad contratado recientemente por una institución financiera que cotiza en bolsa para ayudar a administrar la seguridad de la organización. La oficina principal de la compañía está en Nueva York, NY, y tiene sucursales adicionales en todo Estados Unidos.

Temas actuales

La infraestructura actual incluye servidores Windows, servidores UNIX, clientes Windows, clientes Mac, dispositivos móviles Windows y dispositivos móviles Mac implementados en todas las oficinas. El departamento de TI de la compañía tiene un gran personal ubicado en la oficina de Nueva York. Cada sucursal tiene unos pocos miembros del personal de TI local que solo se encargan de los problemas de esa sucursal.

Ha identificado varias instancias en las que los ataques contra los sistemas cliente no se impidieron ni detectaron en el nivel de cliente porque no se implementó ningún control para evitar el ataque. Los datos fueron robados de algunos dispositivos. Toda una sucursal estaba infectada con malware y virus y requería varios días de tiempo de recuperación, lo que significaba la pérdida de ingresos. Por último, recientemente descubrió que varios sistemas cliente tienen instaladas versiones sin licencia de sistemas operativos. Debe asegurarse de que se implementan los controles adecuados para mitigar estos riesgos.

En una auditoría reciente, descubrió que varios dispositivos móviles carecían de las actualizaciones adecuadas para sus sistemas operativos o aplicaciones. Además, los usuarios habían desactivado las funciones de limpieza remota y localización GPS en estos dispositivos y habían instalado varias aplicaciones no autorizadas. Necesita una solución para mitigar estos riesgos y controlar la configuración y las aplicaciones de los dispositivos móviles cuando esos dispositivos están conectados a la empresa.

Debido a varios contratos entre su empresa y terceros, debe asegurarse de que ciertos sistemas dentro de su infraestructura logren EAL7 en el modelo de evaluación de criterios comunes.

Recientemente, uno de los servidores de la intranet fue víctima de un ataque de denegación de servicio (DoS). El departamento de TI tardó más de 24 horas en devolver el servidor al estado operativo. Durante ese tiempo, el personal de la oficina principal no pudo acceder a la información importante de recursos humanos almacenada en el servidor afectado.

Se espera que los usuarios utilicen el cifrado simétrico y asimétrico para garantizar la confidencialidad de los datos. Debe implementar un sistema adecuado para administrar las claves de cifrado, los valores hash y los certificados digitales en todos los equipos cliente. También debe proteger las contraseñas, cifrar unidades y administrar los derechos digitales de estos mismos equipos.

La integridad de los datos se ha convertido en una preocupación cada vez más seria para los archivos creados y mantenidos por el departamento de investigación. Debe implementar la solución adecuada para estos archivos. Todos los archivos se encuentran en un único servidor que es accesible sólo por los usuarios en el departamento de investigación.

Nunca se completó formalmente un análisis de riesgos exhaustivo para toda la organización. Se le ha pedido que encabece este proyecto. Como parte de este proceso, debe identificar las amenazas geográficas para cada oficina individual.

Su organización desplegará dos oficinas internacionales a finales de este año. Se le ha invitado a participar en la selección de instalaciones y en el proceso de seguridad interna del edificio para proporcionar información de seguridad concreta.

Una de las oficinas internacionales previstas desempeñará tareas muy delicadas para una entidad gubernamental. Por este motivo, debe asegurarse de que la empresa selecciona una ubicación donde se puede mantener un perfil bajo. ¿En cuál de los siguientes criterios basa su selección de instalaciones?

- ✗ **A)** Alrededores
- ✗ **B)** construcción
- ✗ **C)** accesibilidad
- ✓ **D)** visibilidad

explicación

Le preocupa la visibilidad. La cantidad de visibilidad depende de la organización y de los procesos que se lleven a cabo en la instalación. En el caso de esta oficina, debe asegurarse de que la empresa selecciona una ubicación donde se puede mantener un perfil bajo.

La accesibilidad es la facilidad con la que los empleados y los funcionarios pueden acceder a las instalaciones. La construcción es el material utilizado para construir la instalación. El área circundante es el entorno en el que se encuentra la instalación, y se refiere principalmente a la tasa de delincuencia local y la distancia a los servicios de emergencia. Ninguno de estos factores es relevante para mantener un perfil bajo.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar principios de seguridad al diseño de sitios e instalaciones

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, diseño de sitios e instalaciones

---

Question #5 of 193

Question ID: 1105079

En PKI, ¿cuál es la entidad que firma un certificado?

- ✗ **A)** un principal
- ✗ **B)** un tema
- ✓ **C)** un emisor
- ✗ **D)** un verificador

explicación

En una infraestructura de clave pública (PKI), un emisor es la entidad que firma un certificado. La firma de un certificado comprueba que el nombre y la clave del certificado son válidos. PKI es un sistema diseñado para distribuir de forma segura las claves públicas. Una PKI normalmente consta de los siguientes componentes: certificados, un repositorio de claves, un método para revocar certificados y un método para evaluar una cadena de certificados, que los profesionales de seguridad pueden usar para seguir la posesión de claves. Cadena de custodia podría ser utilizado en la prueba de casos legales contra los piratas informáticos.

Una entidad de seguridad es cualquier entidad que posee una clave pública. Un comprobador es una entidad que comprueba una cadena de claves pública. Un sujeto es una entidad que busca que se valide un certificado.

Una PKI proporciona certificación digital. Incluye una entidad de certificación (CA) y marca de tiempo. Un servidor de Protocolo ligero de acceso a directorios (LDAP) se utiliza en una PKI para proporcionar la estructura de directorios. Una PKI proporciona compatibilidad sin repudio.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 3: Arquitectura de seguridad y certificados de ingeniería

---

Question #6 of 193

Question ID: 1105027

Se le ha pedido específicamente que implemente un cifrado de secuencias. ¿Qué algoritmo criptográfico podría utilizar?

- ✗ **A)** RC6
- ✓ **B)** RC4
- ✗ **C)** MD5
- ✗ **D)** RC5

explicación

RC4 es un cifrado de flujo.

Los cifrados de flujo y de bloques son dos tipos principales de algoritmos simétricos. Los cifrados de bloque procesan un bloque de bits y los cifrados de flujo de un bit a la vez. RC4, RC5 y RC6 no proporcionan hash unidireccional.

RC5 y RC6 son cifrados por bloques.

MD5 es un algoritmo hash unidireccional. El hash unidireccional hace referencia a insertar una cadena de longitud variable en un algoritmo hash y producir un valor hash de longitud fija. Este valor hash se anexa al final del mensaje que se envía. Este valor hash se vuelve a calcular en el extremo de los receptores de la misma manera en que se creó utilizando la misma lógica de cálculo. Si el valor hash vuelto a calcular es el mismo que el valor hash generado, el mensaje no se modificó durante el curso de la transmisión. MD2, MD4 y MD5 toman un mensaje de longitud arbitraria y producen un resumen del mensaje de 128 bits.

Los algoritmos hash incluyen MD2, MD4, MD5, HAVAL y todas las variantes del algoritmo hash seguro (SHA).

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 3: Arquitectura e ingeniería de seguridad, RC4/RC5/RC6/RC7

Question #7 of 193

Question ID: 1105106

¿Qué descripción se aplica a una oleada?

- ✗ **A)** una fuente de alimentación prolongada por debajo del voltaje normal
- ✗ **B)** un bajo voltaje momentánea
- ✗ **C)** un corte de energía momentánea
- ✓ **D)** un alto voltaje prolongado
- ✗ **E)** un corte de energía prolongado

explicación

Una sobretensión se refiere a un voltaje por encima del nivel normal durante un período prolongado. Los protectores contra sobretensiones evitan que los componentes eléctricos se dañen por un suministro de voltaje excesivo por encima del nivel normal.

El término para un bajo voltaje momentánea es un hundimiento. Un corte de energía prolongado es un apagón. Un corte de energía momentánea es una falla. Una fuente de alimentación prolongada por debajo del voltaje normal es un pardo.

Los picos se refieren a niveles de voltaje por encima del nivel normal. A diferencia de las oleadas, los picos son momentáneas y duran solo una fracción de segundo.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Tipos de interrupciones

---

Question #8 of 193

Question ID: 1105095

Durante una auditoría de seguridad reciente, un contratista de seguridad externo ha sugerido que recortar el paisaje alrededor de las entradas. Además, se ha sugerido que instale CCTV en todas las entradas. ¿Qué faceta del enfoque de prevención del delito mediante el diseño ambiental (CPTED) se está abordando?

- ✓ **A)** vigilancia natural
- ✗ **B)** control de acceso natural
- ✗ **C)** refuerzo territorial
- ✗ **D)** endurecimiento de objetivos

explicación

La vigilancia natural es la faceta del enfoque cpted que se está abordando. La vigilancia natural en el enfoque CPTED incluye guardias de seguridad, circuito cerrado de televisión (CCTV), línea de visión, paisajismo de bajo nivel y entradas elevadas. La principal preocupación de esta faceta es garantizar que los delincuentes se sientan incómodos haciendo un ataque.

El control de acceso natural en el enfoque CPTED incluye la colocación de puertas, cercas, iluminación y paisajismo. Esta faceta garantiza que el acceso a las entradas de los edificios esté controlado.

El refuerzo territorial en el enfoque CPTED incluye muros, cercas, paisajismo, iluminación, banderas y aceras que enfatizan o amplían el área de influencia de la compañía para que los usuarios sientan que son dueños del área.

El endurecimiento del objetivo no forma parte de CPTED. Es otro enfoque de la seguridad física, que hace hincapié en negar el acceso a través de barreras físicas y artificiales. El mejor enfoque es crear un entorno utilizando el enfoque CPTED y luego aplicar el endurecimiento del objetivo sobre el diseño CPTED.

La vigilancia informática o de red es otro tipo de vigilancia, pero no forma parte del enfoque CPTED. La vigilancia informática o de red incluye registros de auditoría, rastreadores de red y supervisión de teclado.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar principios de seguridad al diseño de sitios e instalaciones

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, CPTED

Question #9 of 193

Question ID: 1111719

Ha creado una clave criptográfica en el controlador de dominio de su organización. ¿Qué debes hacer a continuación?

- ✓ **A)** Inicialice la clave.
- ✗ **B)** Termine la clave.
- ✗ **C)** Active la clave.
- ✗ **D)** Distribuya la clave.

explicación

Después de crear una clave criptográfica, debe inicializar la clave estableciendo todos sus atributos principales.

Las cuatro fases del ciclo de vida de la clave criptográfica son las siguientes:

- Pre-operacional
- operacional
- Post-operacional
- destruido

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 3: Arquitectura e ingeniería de seguridad, Gestión de claves

Administración de claves en sistemas distribuidos,
http://research.microsoft.com/pubs/132506/distributed%20key%20lifecycle%20management.pdf

---

Question #10 of 193

Question ID: 1111713

Su organización ha decidido implementar un sitio web para que los clientes compren los productos de su organización. El sitio Web utilizará el protocolo SET. ¿Qué afirmación es cierta de este protocolo?

- ✓ **A)** SET utiliza firmas digitales y certificados digitales para realizar y verificar una transacción electrónica.
- ✗ **B)** SET transmite automáticamente la información de la tarjeta de crédito de un usuario a una CA cuando se realiza una compra en línea.
- ✗ **C)** SET funciona en la capa de red del modelo OSI.
- ✗ **D)** SET utiliza 3DES para el intercambio de claves simétricas.

explicación

La transacción electrónica segura (SET) utiliza firmas digitales y certificados digitales para realizar y verificar una transacción electrónica.

SET utiliza el estándar de cifrado de datos (DES) para cifrar las transacciones en línea. No utiliza 3DES para el intercambio de claves simétricas.

SET funciona en la capa de aplicación y no en la capa de red del modelo de interconexiones de sistemas abiertos (OSI).

SET no transmite automáticamente la información de la tarjeta de crédito de un usuario a una CA tan pronto como se realiza una compra en línea. Los certificados digitales y las firmas digitales del usuario, el banco y el comerciante están involucrados en la transacción.

SET es un estándar de protocolo abierto, propuesto por Visa y MasterCard para transmitir información de tarjetas de crédito a través de Internet, que utiliza criptografía para preservar el secreto de las transacciones electrónicas. Las siguientes entidades están implicadas en una transacción SET:

- El emisor, es decir, el banco o la institución financiera que proporciona una tarjeta de crédito al individuo (emisor)
- La persona autorizada que utiliza la tarjeta de crédito
- El comerciante que proporciona la mercancía al titular de la tarjeta
- El adquirente, es decir, el banco o la institución financiera que procesa las tarjetas de pago

El titular de la tarjeta de crédito, el comerciante y el banco emisor garantizan la confidencialidad y privacidad de una transacción SET mediante el uso de certificados digitales y firmas digitales. Los pasos siguientes describen brevemente el funcionamiento de SET:

- El emisor proporciona el software de billetera electrónica que almacena la información de la tarjeta de crédito para las transacciones en línea. La billetera electrónica genera las claves públicas y privadas.
- Los comerciantes reciben un certificado digital junto con dos claves públicas, una para el banco y la otra para el comerciante.

- El certificado del comerciante se valida al usuario durante una transacción en línea.
- La información de la orden de pago, que es específica del pedido del usuario, se cifra mediante el uso de la clave pública del comerciante. Los datos de pago se cifran mediante el uso de la clave pública del banco.
- El comerciante verifica la firma digital en el certificado digital que es utilizado por el individuo para la transacción.
- El mensaje de pedido que viaja del comerciante al banco incluye la clave pública del banco, la información de pago del cliente y el certificado digital del comerciante.
- Después de recibir una verificación firmada digitalmente del banco, el comerciante llena el pedido para el cliente.

En resumen, la transacción en línea que implica SET se facilita a través de dos pares de claves asimétricas y dos certificados digitales. Set implicaría el uso de dos certificados digitales para la pasarela y dos para los adquirentes.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
evaluar y mitigar las vulnerabilidades de las arquitecturas de seguridad, los diseños y los elementos de la solución

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, SET

Question #11 of 193

Question ID: 1111704

¿Qué componente NO está asociado con los criterios comunes?

✗ **A)** objetivo de seguridad
✗ **B)** objetivo de la evaluación
✗ **C)** perfil de protección
✓ **D)** acreditación

explicación

La acreditación no es un componente asociado de los Criterios Comunes. La acreditación es el proceso en el que la dirección acepta la funcionalidad y la garantía del sistema. La acreditación representa la satisfacción de la dirección con respecto a la funcionalidad y la garantía del producto.

Los criterios comunes están asociados con los atributos de funcionalidad y garantía de un producto. Los Criterios Comunes se iniciaron en 1993 con el objetivo de combinar criterios de evaluación, como TCSEC e ITSEC, en un estándar global para la evaluación de productos de infraestructura, su funcionalidad de seguridad y su garantía. Los Criterios Comunes son un estándar mundialmente reconocido y aceptado para la evaluación de productos de infraestructura. Este criterio de evaluación reduce la complejidad de las calificaciones y garantiza que los proveedores

fabriquen productos para los mercados internacionales. Por lo tanto, los criterios comunes abordan la funcionalidad en términos de lo que hace un producto y garantiza que el producto funcionará de manera coherente y predecible.

Los criterios comunes asignan un nivel de garantía de evaluación. A diferencia del Libro Naranja, que asigna una calificación a un producto en función de los métodos que utilizan para relacionarse con el modelo Bell-LaPadula, los Criterios Comunes asignan una calificación basada en un perfil de protección. Un perfil de protección contiene un conjunto de requisitos de seguridad para un producto y la justificación detrás de dichos requisitos.

En la Parte 3 de los Criterios comunes, Requisitos de garantía de seguridad, siete paquetes predefinidos de componentes de garantía que componen la escala CC para calificar la confianza en la seguridad de los productos y sistemas de TI se denominan nivel de garantía de evaluación (EAL). Un perfil de protección puede ser documentado y presentado por proveedores y clientes que demandan una solución de seguridad. Los siete niveles de EAL son los siguientes:

- EAL1: El producto está probado funcionalmente.
- EAL2: El producto está probado estructuralmente.
- EAL3: El producto se prueba y comprueba metódicamente.
- EAL4: El producto se diseña, prueba y revisa metódicamente.
- EAL5: El producto está semi-formalmente diseñado y probado.
- EAL6: El producto tiene un diseño semi-formalmente verificado y está probado.
- EAL7: El producto tiene un diseño formalmente verificado y está probado.

La minuciosidad de las pruebas aumenta y las pruebas se vuelven más detalladas con cada nivel.

El objetivo de evaluación (TOE) define el producto que se va a evaluar para la calificación. El TOE es una parte de los criterios comunes.

El objetivo de seguridad del proveedor define la funcionalidad y los mecanismos de garantía que cumplen con la solución de seguridad.

El EAL o paquete describe los requisitos que debe cumplir la solución de seguridad propuesta para lograr una calificación EAL específica para el producto.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender los conceptos fundamentales de los modelos de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Operaciones de seguridad, criterios comunes

Question #12 of 193

Question ID: 1105039

¿Qué algoritmo de cifrado se basa en el acuerdo de claves Diffie-Hellman?

✗ **A)** HAVAL

✗ **B)** mochila

✗ **C)** Algoritmo internacional de cifrado de datos

✓ **D)** El Gamal

explicación

El Gamal es un algoritmo de cifrado de clave pública asimétrica basado en el acuerdo de claves Diffie-Hellman. Se utiliza para firmas digitales, cifrado de datos e intercambio de claves. Las funciones matemáticas del algoritmo de El Gamal calculan logaritmos discretos en un cuerpo finito.

HAVAL es un algoritmo hash y no un algoritmo de cifrado. Procesa tamaños de bloque de 1024 bits de información. HAVAL crea resúmenes de mensajes de tamaños variables en lugar de un valor de salida fijo. HAVAL produce hashes en longitudes de 128, 160, 192, 224 y 256 bits.

Knapsack es un algoritmo de cifrado asimétrico. No se basa en el acuerdo de claves Diffie-Hellman.

El algoritmo internacional de cifrado de datos (IDEA) es un cifrado de bloques que opera en bloques de datos de 64 bits, requiere una clave de 128 bits y realiza ocho rondas de cálculo. El software de cifrado Pretty Good Privacy (PGP) utiliza IDEA.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, El Gamal

Problema de la mochila, http://en.wikipedia.org/wiki/Knapsack_problem

---

Question #13 of 193

Question ID: 1105069

Su administrador le ha pedido que se asegure de que los archivos de contraseñas que se almacenan en los servidores no son vulnerables a los ataques. ¿A qué tipo de ataque serían vulnerables estos archivos?

✗ **A)** un ataque de inundación SYN

✓ **B)** un ataque de diccionario

✗ **C)** un ataque de canal lateral

✗ **D)** un ataque de denegación de servicio (DoS)

explicación

Los archivos de contraseñas son vulnerables a ataques de diccionario y ataques de fuerza bruta. Un ataque de diccionario se basa en los esfuerzos del atacante para determinar la clave de descifrado para derrotar a un cifrado. Este ataque utiliza palabras del diccionario y normalmente tiene éxito porque con frecuencia los usuarios eligen contraseñas de un diccionario que son fáciles de recordar. Por lo tanto, el ataque de diccionario es una parte del criptoanálisis. El cifrado unidireccional o el hash unidireccional protege contra la lectura o modificación del archivo de contraseñas, pero un intruso puede iniciar un ataque de diccionario después de capturar el archivo de contraseña.

Un ataque de inundación SYN es una técnica de denegación de servicio (DoS). El atacante envía varios paquetes SYN a un equipo de destino desde una dirección IP de origen falsificada. El equipo víctima responde a las solicitudes de servicio respondiendo con una confirmación (SYN-ACK) y asignando recursos a la dirección IP de origen falsificada. El equipo de destino se queda sin recursos y se deniegan las solicitudes de los usuarios legítimos.

En un ataque de canal lateral, el atacante obtiene información sobre los algoritmos de cifrado que se ejecutan en el criptosistema que se implementa en la red. El atacante puede utilizar información, como el consumo de energía, las radiaciones electromagnéticas y el sonido, para entrar en un sistema. El ataque de canal lateral también se puede basar en el tiempo necesario para realizar un cálculo.

Un ataque DoS explota las limitaciones del protocolo TCP/IP inundando la red con un gran número de solicitudes de recursos falsos o consumiendo el ancho de banda completo de la red. Para satisfacer las solicitudes de recursos creadas falsamente por el atacante, la red agota sus recursos. Por lo tanto, a los usuarios legítimos y autorizados se les niegan los servicios sobre la base de una crisis de recursos en la red.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Ataque de diccionario

---

Question #14 of 193

Question ID: 1105050

¿Qué es una función de trampilla?

- ✗ **A)** Un ataque en el que se interceptan mensajes entre dos entidades para que un atacante pueda hacerse pasar por una de las entidades
- ✓ **B)** Un mecanismo que permite la implementación de la función inversa en una función unidireccional
- ✗ **C)** Un ataque que intenta repetidamente valores diferentes para determinar la clave utilizada
- ✗ **D)** Un mecanismo integrado en un algoritmo que permite a un individuo omitir o subvertir la seguridad de alguna manera

explicación

Una función de trampilla es un mecanismo que permite la implementación de la función inversa en una función unidireccional.

Una puerta trasera es un mecanismo integrado en un algoritmo que permite a un individuo eludir o subvertir la seguridad de alguna manera.

Un ataque de fuerza bruta es un ataque que intenta repetidamente diferentes valores para determinar la clave utilizada.

Un ataque de estado en el medio es un ataque en el que se interceptan mensajes entre dos entidades para que un atacante pueda descubrir las claves de las entidades legítimas. El resultado final es que el atacante puede leer todos los mensajes transmitidos entre las dos entidades legítimas.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e Ingeniería de Seguridad, RSA

Question #15 of 193

Question ID: 1114714

¿Qué se consideraría un error medioambiental?

a. Sobrecalentamiento

b. Electricidad estática

c. Problemas de autenticación

d. Configuración de dispositivo no válida

- ✗ **A)** Opciones C y D
- ✗ **B)** opción b
- ✗ **C)** Opciones B y C
- ✗ **D)** Opción d
- ✓ **E)** opciones A y B
- ✗ **F)** opción A
- ✗ **G)** opción c

explicación

El sobrecalentamiento y la electricidad estática se consideran errores ambientales. Un error de entorno es un error que provoca una vulnerabilidad del sistema debido al entorno de instalación.

El sobrecalentamiento es un error ambiental porque generalmente es causado por un flujo de aire insuficiente dentro del sistema. Simplemente mover el sistema a una mejor posición o eliminar algunas de las cosas alrededor del sistema puede evitar el sobrecalentamiento. La electricidad estática es un error ambiental porque generalmente es causada por condiciones ambientales, especialmente baja humedad. La electricidad estática se puede reducir aumentando la humedad, usando el suelo antiestático, usando la puesta a tierra apropiada, y así sucesivamente.

Los problemas de autenticación son errores de validación de acceso, no errores de medio ambiente.

La configuración de dispositivo no válida es un error de configuración, no un error de medio ambiente.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Seguridad Ambiental

---

Question #16 of 193

Question ID: 1104995

¿Qué ataque se considera un ataque pasivo?

✓ **A)** Escuchas telefónicas

✗ **B)** ataque de penetración

✗ **C)** ataque de denegación de servicio (DoS)

✗ **D)** diddling de datos

explicación

Las escuchas telefónicas se consideran un ataque pasivo porque no son intrusivas y generalmente solo capturan lo que está ocurriendo. Las escuchas también se consideran un ataque pasivo.

Un ataque DoS, un ataque de penetración y la diddling de datos se consideran ataques activos porque son intrusivos por naturaleza y en realidad intentan causar una determinada condición, afectar el rendimiento o alterar algo.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
evaluar y mitigar las vulnerabilidades de las arquitecturas de seguridad, los diseños y los elementos de la solución

Referencias:

CISSP Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Escuchas

---

Question #17 of 193

Question ID: 1105053

Durante una operación XOR, se combinan dos bits. Ambos valores son iguales. ¿Cuál será el resultado de esta combinación?

✓ **A)** 0

✗ **B)** o

✗ **C)** 1

✗ **D)** éxtasis

explicación

Si se combinan dos bits en una operación XOR y ambos valores de bits son iguales, el resultado de la combinación es 0.

Si se combinan dos bits en una operación XOR y ambos valores de bits son diferentes, el resultado de la combinación es 1.

Las otras dos opciones no son válidas.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Operaciones lógicas

---

Question #18 of 193

Question ID: 1105077

Ha implementado una infraestructura de clave pública (PKI) para emitir certificados a los equipos de la red de su organización. Debe asegurarse de que los certificados que se han validado están protegidos. ¿Qué se debe proteger en una PKI para hacer esto?

- ✗ **A)** La clave pública del certificado de un usuario
- ✗ **B)** La clave privada del certificado de un usuario
- ✗ **C)** la clave pública de la CA raíz
- ✓ **D)** la clave privada de la CA raíz

explicación

La clave privada de la entidad de certificación (CA) raíz debe protegerse para asegurarse de que los certificados que se han validado en una infraestructura de clave pública (PKI) están protegidos. Si la clave privada de la CA raíz se ha visto comprometida, se debe crear un nuevo certificado raíz y se debe volver a generar la PKI.

Si la clave privada del certificado de un usuario se ha visto comprometida, se debe crear un nuevo certificado para ese usuario y se debe revocar el certificado comprometido del usuario. El compromiso del certificado de un usuario no pondrá en peligro otros certificados de una PKI. Una clave pública, como su nombre lo indica, es pública y no es necesario mantener en secreto.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Question #19 of 193

Question ID: 1104935

¿Qué afirmación es cierta para las estaciones de trabajo en modo compartimentado (CMW)?

- ✗ **A)** El Comité de Protección de los Derechos de Todos los Estados Miembros se basa en el
- ✗ **B)** CMW funciona en un modo de seguridad dedicado.
- ✗ **C)** Cmw, de forma predeterminada, concede acceso relacionado con la información a todos los usuarios que tienen autorización de seguridad.
- ✓ **D)** El CMW requiere el uso de etiquetas informativas.

explicación

El uso de etiquetas de información como medida de seguridad es exclusivo de las estaciones de trabajo en modo compartimentado (CMW). CMW implementa etiquetas de información y etiquetas de confidencialidad. Las etiquetas de información definen el nivel de protección de seguridad de los objetos y las etiquetas de confidencialidad definen los permisos.

CMW funciona en el modo de seguridad compartimentado. En el modo de seguridad compartimentado, los usuarios tienen acceso a toda la información, pero es posible que no tengan la necesidad de conocer el acceso a los datos o la aprobación formal requerida para el acceso a los datos. Este proceso garantiza que un usuario sólo tiene los privilegios de acceso necesarios para la información específica del trabajo del usuario. Por ejemplo, un usuario del departamento de pruebas de software no debe requerir acceso a los datos financieros internos de la organización. Por lo tanto, el usuario no necesita conocer los métodos utilizados para acceder a la información. Al usuario se le concede acceso de acuerdo con el principio de necesidad de conocer y mediante un proceso de aprobación formal.

Como mínimo, se permite el acceso a los datos a los usuarios de cada nivel en función de su respectivo segmento o compartimento. Por lo tanto, el CMW no trabaja en el concepto de privilegio máximo, sino en el concepto de privilegio mínimo.

El modo de seguridad dedicado es otra categoría de modos de operación de seguridad. El modo dedicado administra una única clasificación de la información a diferencia del modo de seguridad compartimentado donde los usuarios pueden procesar simultáneamente múltiples compartimentos de información.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobjetiva:

Implementar y gestionar procesos de ingeniería utilizando principios de diseño seguro

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Operaciones de seguridad, modo de seguridad compartimentado

---

Question #20 of 193

Question ID: 1111724

¿Cuál de estos ataques es un ataque al criptosistema de una organización?

- ✗ **A)** Denegación de servicio (DoS)
- ✗ **B)** ataque de fuerza bruta
- ✗ **C)** desbordamiento de búfer
- ✓ **D)** ataque de texto sin formato conocido

explicación

De los ataques dados, solo un ataque de texto plano conocido es un ataque al criptosistema de una organización. En este tipo de ataque, el atacante tiene el texto no cifrado y el texto cifrado para un mensaje. Los atacantes quieren descubrir la clave utilizada para cifrar el mensaje para que se puedan leer otros mensajes.

Los ataques contra criptosistemas incluyen los siguientes:

- ataques de solo cifrado: este ataque se produce cuando un atacante tiene varios mensajes que se han cifrado con el mismo algoritmo. El objetivo del ataque es descubrir la clave utilizada en el cifrado. Una vez que se descubre la clave, se pueden descifrar todos los mensajes enviados con esa clave. Este es el tipo más común de ataque, pero es el más difícil de lograr.
- ataques de texto no cifrado conocidos: este ataque se produce cuando un atacante tiene la versión de texto no cifrado y texto cifrado de un mensaje. El objetivo del ataque es descubrir la clave utilizada en el cifrado.
- ataques de texto no cifrado elegidos: este ataque se produce cuando un atacante tiene el texto no cifrado y el texto cifrado y puede seleccionar el texto sin formato que se cifra para ver el texto cifrado correspondiente. El objetivo del ataque es descubrir la clave utilizada en el cifrado.
- ataques de texto cifrado elegidos: este ataque se produce cuando un atacante elige el texto cifrado que se va a descifrar y tiene acceso al texto no cifrado resultante. El objetivo del ataque es descubrir la clave utilizada en el cifrado.
- criptoanálisis diferencial - Este ataque mira pares de texto cifrado y analiza el resultado de las diferencias en los pares de texto plano correspondientes. El objetivo del ataque es descubrir la clave utilizada en el cifrado.
- criptoanálisis lineal : este ataque se produce cuando un atacante lleva a cabo un ataque de texto sin formato conocido en varios mensajes cifrados cifrados con la misma clave. Cuantos más mensajes se utilicen, mayor será la probabilidad de que se detecte la clave correcta.

- ataques de canal lateral: este ataque utiliza la inferencia para determinar el valor de la clave de cifrado. Este método aplica ingeniería inversa en lugar de técnicas matemáticas.
- ataques de reproducción: este ataque se produce cuando un atacante captura algunos mensajes y los reenvia, con la esperanza de engañar al receptor haciándolo pensando que el atacante es una entidad legítima. Por lo general, esta información implicaba información de autenticación.
- ataques algebraicos - Este ataque analiza las vulnerabilidades de las matemáticas utilizadas en el algoritmo e intenta explotar la estructura algebraica.
- ataques analíticos : este ataque identifica debilidades estructurales en el diseño de un algoritmo.
- ataques estadísticos : este ataque identifica la debilidad estadística en el diseño de un algoritmo.

Tenga en cuenta que muchos países restringen el uso o la exportación de sistemas criptográficos. Los delincuentes podrían utilizar el cifrado para evitar la detección y el enjuiciamiento. El gobierno de los Estados Unidos ha reducido en gran medida sus restricciones a la exportación de criptografía, pero todavía hay algunas restricciones en vigor. Los productos que utilizan cifrado no se pueden vender a ningún país que Estados Unidos haya declarado que apoya el terrorismo. El temor es que los enemigos del país usarían el cifrado para ocultar su comunicación, y el gobierno sería incapaz de romper este cifrado y espiar sus transferencias de datos.

Los ataques de fuerza bruta, los ataques de denegación de servicio (DoS) y los ataques de desbordamiento de búfer se consideran ataques contra operaciones. Los ataques de fuerza bruta son ataques que intentan diferentes entradas para lograr un objetivo en particular, a menudo utilizados para obtener credenciales de usuario para el acceso no autorizado. Los ataques DoS son acciones que impiden que un sistema o sus recursos funcionen según lo planeado. Los ataques de desbordamiento de búfer se producen cuando se aceptan demasiados datos como entrada para una aplicación o sistema operativo.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, ataque de texto plano conocido

---

Question #21 of 193

Question ID: 1105057

Recientemente ha detectado una carpeta en el equipo que contiene una copia segura de la clave privada para todos los usuarios de la organización. Mantenga esta copia para asegurarse de que puede recuperar las claves perdidas. ¿De qué práctica de seguridad es este un ejemplo?

✗ **A)** Crl

✗ **B)** criptografía cuántica

✓ **C)** depósito de garantía de claves

✗ **D)** esteganografía

explicación

El depósito de garantía de claves es cuando se mantiene una copia segura de la clave privada de un usuario para asegurarse de que puede recuperar la clave si se pierde. En algunos casos, se puede seleccionar un tercero para proporcionar el servicio de depósito de garantía de claves cuando la clave es propiedad de una organización pero la usa otra. Si un tercero proporciona este servicio, garantiza que la organización que usa la clave todavía puede recuperar datos si la organización propietaria de la clave sale de la ciudad. El depósito de garantía de claves es una preocupación principal en criptografía y en una infraestructura de clave pública (PKI). El servicio de depósito de garantía de claves es necesario al implementar una PKI si la pérdida de datos es inaceptable.

La criptografía cuántica es un método relativamente nuevo de cifrado. La criptografía cuántica se diferencia de las tecnologías probadas en que se basa más en la física, en lugar de las matemáticas, como un aspecto clave de su modelo de seguridad. Si bien la mayoría de las organizaciones utilizan tecnologías probadas, el uso de criptografía cuántica aumentará porque es más seguro. Teóricamente, la computación cuántica ofrece la posibilidad de factorizar los productos de grandes números primos y calcular logaritmos discretos en tiempo polinómico. Estos cálculos se pueden lograr en un período de tiempo tan comprimido porque un bit cuántico en una computadora cuántica es en realidad una superposición lineal de los estados uno y cero y, por lo tanto, teóricamente puede representar ambos valores en paralelo. Esto permite que el cálculo que generalmente toma tiempo exponencial se realice en tiempo polinómico, ya que se pueden calcular simultáneamente diferentes valores del patrón binario de la solución.

Una lista de revocación de certificados (CRL) es una lista de certificados que se han revocado, ya no son válidos y no se deben usar.

La esteganografía es la ciencia de ocultar mensajes dentro de otro medio. Un uso común de la esteganografía implica ocultar un mensaje dentro de una imagen o gráfico de aspecto normal.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

¿Qué es el depósito de garantía de claves?, http://www.webopedia.com/TERM/K/key_escrow.html

---

Question #22 of 193

Question ID: 1105071

¿Qué se refiere al tipo de modelo de confianza utilizado por las CA?

- ✗ **A)** anillo
- ✓ **B)** jerarquía
- ✗ **C)** autobús
- ✗ **D)** malla

explicación

Las entidades de certificación (CA) se organizan en una jerarquía de confianza. Una CA raíz está en la parte superior de una jerarquía de confianza de CA y contiene un certificado raíz, que se usa para firmar certificados para CA en el nivel inmediatamente inferior a la CA raíz. El modelo centralizado usa una CA para emitir y revocar certificados.

Los términos bus, anillo y malla se refieren a los tipos de topología de red. Por ejemplo, las redes Ethernet a menudo se configuran en una topología de bus. Las redes Token Ring se organizan en una topología en anillo. Cada nodo de una topología de malla tiene una conexión física con todos los demás nodos de la topología de malla.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Autoridad de certificación (CA) y Autoridad de registro (RA)

Question #23 of 193

Question ID: 1132508

¿Qué clasificación de seguridad TCSEC aborda el uso del análisis de canal encubierto?

- ✗ **A)** D
- ✗ **B)** B1
- ✓ **C)** B2
- ✗ **D)** A1

explicación

La clasificación de seguridad B2 aborda el uso del análisis de canal encubierto en un sistema. El análisis de canal encubierto es un requisito de garantía operativa que se especifica en el Libro Naranja. Es necesario que los sistemas de clase B2 protejan contra los canales de almacenamiento encubierto. Es necesario que los sistemas de clase B3 protejan contra el almacenamiento encubierto y los canales de temporización encubiertos.

Los criterios de evaluación de sistemas informáticos de confianza (TCSEC) clasifican los sistemas en divisiones jerárquicas de niveles de seguridad que van desde la protección verificada hasta la seguridad mínima.

Los niveles definidos por TCSEC y los subniveles de seguridad son los siguientes:

- R: Protección verificada que ofrece el más alto nivel de seguridad
  - Una calificación A1 implica que la garantía de seguridad, el diseño, el desarrollo, la implementación, la evaluación y la documentación de un equipo se realizan de una manera muy formal y detallada. Una infraestructura que contiene sistemas con clasificación A1 es el entorno más seguro y normalmente se utiliza para almacenar información altamente confidencial y confidencial. Este nivel especifica los controles de distribución de confianza.
- B: Protección obligatoria basada en el modelo de seguridad bell-lapadula y aplicada mediante el uso de etiquetas de seguridad.
  - Una clasificación B1 se refiere a la seguridad etiquetada, donde cada objeto tiene una etiqueta de clasificación y cada sujeto tiene un nivel de autorización de seguridad. Para acceder al contenido del objeto, el sujeto debe tener un nivel igual o mayor de autorización de seguridad que el objeto. Un sistema compara el nivel de autorización de seguridad de un sujeto con la clasificación del objeto para permitir o denegar el acceso al objeto. La categoría B1 ofrece aislamiento de procesos, el uso de etiquetas de dispositivos, el uso de especificaciones y verificaciones de diseño y controles de acceso obligatorios. Los sistemas B1 se utilizan para manejar información clasificada.
  - Una clasificación B2 se refiere a la protección estructurada. Se debe utilizar un procedimiento de autenticación estricto en los sistemas con clasificación B2 para permitir que un sujeto acceda a los objetos mediante la ruta de acceso de confianza sin puertas traseras. Este nivel es el nivel más bajo para implementar la administración de instalaciones de confianza; los niveles B3 y A1 también lo implementan. Los requisitos adicionales de una calificación B2 incluyen la separación de las funciones de operador y administrador, las etiquetas de sensibilidad y el análisis del canal de almacenamiento encubierto (pero NO el análisis de temporización encubierto). Un sistema B2 se utiliza en entornos que contienen información altamente confidencial. Por lo tanto, un sistema B2 debe ser resistente a los intentos de penetración.
  - Una clasificación B3 se refiere a los dominios de seguridad. Los sistemas B3 deben ser capaces de realizar una recuperación de confianza. Un sistema evaluado con una clasificación B3 debe tener el rol del administrador de seguridad totalmente definido. Un sistema B3 debe proporcionar la funcionalidad de supervisión y auditoría. Un sistema B3 se utiliza en entornos que contienen información altamente sensible y debe ser resistente a los intentos de penetración. Otra característica de la clasificación B3 es el análisis de canal de temporización encubierto.
- C: Protección discrecional basada en el acceso discrecional de sujetos, objetos, individuos y grupos.

- Una clasificación C1 se refiere a la protección de seguridad discrecional. Para habilitar el proceso de calificación, los sujetos y los objetos deben separarse de la instalación de auditoría mediante un proceso de identificación y autenticación claro. Un sistema de clasificación C1 es adecuado para entornos en los que los usuarios procesan la información en el mismo nivel de sensibilidad. Un sistema de clasificación C1 es adecuado para entornos con problemas de seguridad baja.
- Una clasificación C2 se refiere a la protección de acceso controlado. La funcionalidad de autenticación y auditoría en los sistemas debe estar habilitada para que se produzca el proceso de clasificación. Un sistema con una clasificación C2 proporciona protección de recursos y no permite la reutilización de objetos. La reutilización de objetos implica que un objeto no debe tener datos remanentes que puedan ser utilizados por un sujeto más adelante. Un sistema C2 proporciona un control de acceso granular y establece un nivel de responsabilidad cuando los sujetos acceden a objetos. Un sistema con clasificación C2 es adecuado para un entorno comercial.

- D: Clasificación de protección mínima que se ofrece a los sistemas que no cumplen los criterios de evaluación

Una calificación más alta implica un mayor grado de confianza y seguridad. Por ejemplo, una clasificación B2 proporciona más seguridad que una clasificación C2. Una calificación más alta incluye los requisitos de una calificación más baja. Por ejemplo, una clasificación B2 incluye las características y especificaciones de una clasificación C2.

Por lo tanto, todas las demás opciones son incorrectas.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender los conceptos fundamentales de los modelos de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Operaciones de seguridad, Orange Book

---

Question #24 of 193

Question ID: 1105070

El jefe del departamento de TI le informa de que la red de su organización ha sido víctima de un ataque de solo texto cifrado. ¿Qué afirmación es cierta con respecto a este tipo de ataque?

✗ **A)** Es muy difícil para un atacante recopilar el texto cifrado en una red.

✗ **B)** Un ataque de sólo texto cifrado es considerado por los hackers como el ataque más fácil.

✓ **C)** Un ataque de solo texto cifrado se centra en descubrir la clave de cifrado.

✗ **D)** Un ataque de cumpleaños es un ejemplo de un ataque de sólo texto cifrado.

explicación

Un ataque de solo texto cifrado se centra principalmente en descubrir la clave de cifrado mediante la recopilación de varios mensajes cifrados y, a continuación, intentar deducir un patrón de los mensajes cifrados.

Un ataque de cumpleaños no es un ejemplo de un ataque de sólo texto cifrado. Un ataque de cumpleaños se basa en la probabilidad de que dos mensajes tengan el mismo valor hash. Llevar a cabo un ataque de cumpleaños implica encontrar dos mensajes con el mismo valor hash. Este proceso es similar a encontrar dos personas con las mismas fechas de cumpleaños entre un grupo de personas. Si una función hash genera el mismo valor hash para dos mensajes diferentes, es mucho más fácil para un atacante detectar el valor de texto no cifrado correspondiente mediante ataques de fuerza bruta. La frecuencia de los ataques de fuerza bruta ha aumentado porque la velocidad y la potencia del procesador han aumentado. Los valores grandes de las funciones hash son una contramedida a los ataques de cumpleaños. Cuanto mayor sea el valor de la salida de la función hash, menores serán las posibilidades de colisiones de valores hash. Esto hace que sea más difícil para un atacante romper la salida del valor hash. Por ejemplo, SHA-1 que produce una salida hash de 160 bits es más resistente a los ataques de cumpleaños en comparación con MD5 que produce una salida hash de 128 bits. Un ataque de cumpleaños en la función hash intenta lograr una colisión después de 2m / 2 posibles valores de entrada de prueba si la aplicación de una función hash da como resultado una salida de longitud fija de m bits.

Los ataques de solo texto cifrado son más comunes porque es muy fácil para un atacante obtener el texto cifrado mediante el uso de software de rastreador de paquetes en la red. El desafío para el atacante es encontrar la clave de cifrado que le permite descifrar toda la información de texto cifrado y convertirla en información de texto no cifrado.

Un ataque de solo texto cifrado se considera un ataque común pero desafiante para obtener acceso a información confidencial.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, ataque solo de texto cifrado

---

Question #25 of 193

Question ID: 1114705

¿Qué afirmación es cierta del algoritmo de Rijndael?

✗ **A)** Rijndael utiliza longitudes de bloque fijas y longitudes de clave fijas.

✓ **B)** Rijndael utiliza longitudes de bloque variables y longitudes de clave variables.

✗ **C)** Rijndael utiliza longitudes de bloque fijas y longitudes de clave variables.

✗ **D)** Rijndael utiliza longitudes de bloque variables y longitudes de clave fijas.

explicación

Rijndael es un algoritmo de cifrado de bloques que utiliza longitudes de bloque variables y longitudes de clave variables. El tamaño de bloque y clave que admiten los algoritmos de Rijndael son 128, 192 y 256 bits. El número de rondas de cifrado depende del tamaño de la clave y el bloque. Rijndael es un algoritmo de clave simétrica.

Estos son algunos ejemplos de longitudes de clave variables y longitudes de bloque variables que Rijndael puede utilizar:

Clave = 128 - Tamaño del bloque = 128 - rondas = 10

Clave = 192 - Tamaño del bloque = 192 - rondas = 12

Clave = 256 - Tamaño del bloque = 256 - rondas = 14

Rijndael opera en las capas no lineal, de adición de claves y de mezcla lineal. Rijndael requiere poca memoria y proporciona resistencia contra todos los ataques conocidos y ha sido elegido para proteger la información gubernamental sensible pero no clasificada. El estándar de encripción avanzada (AES) NIST utiliza el algoritmo de Rijndael. AES y Rijndael se conocen a menudo como cifrados de bloques iterados.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Estándar de cifrado avanzado (AES)

Question #26 of 193

Question ID: 1105040

¿Qué es un algoritmo que se utiliza para crear un resumen de mensaje para un archivo para garantizar la integridad?

✓ **A)** picadillo

✗ **B)** Texto cifrado

✗ **C)** Plaintext

✗ **D)** clave pública

explicación

Un hash es un algoritmo que se utiliza para crear un resumen de mensaje, o una huella digital, para un archivo. Un hash es un valor de longitud fija. Si se cambia un archivo y, a continuación, se utiliza un algoritmo hash en el archivo, el segundo resumen del mensaje será diferente del primero. En consecuencia, el resumen del mensaje se puede utilizar para determinar si se ha modificado un archivo determinado. Los algoritmos hash no protegen los archivos de la visualización no autorizada; sólo se utilizan para validar la integridad del archivo.

El texto sin formato se refiere a archivos que no se han cifrado. Texto cifrado se refiere a los archivos que se han cifrado. Una clave pública se utiliza en el cifrado asimétrico para cifrar mensajes. El cifrado asimétrico se basa en dos claves: una pública y otra privada. Un usuario puede distribuir la clave pública a otras personas para permitir que esas personas cifren la información para su transmisión al usuario; a continuación, el usuario puede utilizar la clave privada para descifrar la información. Sólo la clave privada se puede utilizar para descifrar la información.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Hashing

¿Qué es el hashing, http://searchsqlserver.techtarget.com/definition/hashing

---

Question #27 of 193

Question ID: 1105016

¿Qué mecanismo conserva la información HTTP de la conexión anterior?

✗ **A)** HTTPS (en)

✗ **B)** IPSec

✓ **C)** Galletas

✗ **D)** SSH

explicación

Las cookies conservan la información HTTP de la conexión anterior. Las cookies son archivos de texto que contienen información sobre los parámetros de la conexión. Este archivo se almacena por el servidor Web en el disco duro del equipo del cliente cada vez que una conexión HTTP se establece inicialmente por el explorador, para ser reutilizado posteriormente cuando se reinicia la conexión. Las cookies pueden ser mal utilizadas aprovechando la información sensible almacenada en el archivo. Las cookies también se pueden utilizar para rastrear los hábitos de navegación de los usuarios.

Secure shell (SSH) crea una conexión segura entre dos equipos o dispositivos de red a través de una conexión WAN mediante el mecanismo de túnel y el intercambio de claves Diffie-Hellman. SSH se utiliza normalmente para iniciar sesión de forma remota en otras máquinas a través de WAN. SSH también se conoce como un telnet cifrado. Telnet establece las sesiones de administración en un texto claro sobre una WAN insegura, tal como Internet. Por lo tanto, SSH está desarrollado para proporcionar la función de cifrado mientras se administran las estaciones de forma remota o se accede a los datos.

El protocolo de seguridad de Internet (IPSec) es un conjunto de protocolos que permiten a los usuarios establecer un canal de intercambio de datos seguro entre un cliente y un servidor. IPSec es utilizado por redes privadas virtuales (VPN). IPSec consta de métodos seguros de cifrado y autenticación para proporcionar seguridad de datos. IPSec es básicamente un marco que consta de los protocolos de cifrado y autenticación.

El Protocolo seguro de transporte de hipertexto (HTTPS) se utiliza para proteger la comunicación entre dos equipos mediante la seguridad de capa de sockets seguros (SSL). HTTPS protege todo el canal entre dos estaciones en lugar de cada paquete. HTTPS también se conoce como SSL sobre HTTP.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Cookies

---

Question #28 of 193

Question ID: 1105063

Desea enviar un archivo a un compañero de trabajo llamado María. No desea proteger el contenido del archivo de la vista; sin embargo, cuando María recibe el archivo, desea que pueda determinar si el contenido del archivo se modificó durante el tránsito.

¿Qué medida de protección debe usar?

✗ **A)** cifrado simétrico

✗ **B)** cifrado asimétrico

✗ **C)** un certificado digital

✓ **D)** una firma digital

explicación

Debe utilizar una firma digital para permitir a María determinar si el contenido del archivo se ha modificado durante el tránsito. Una firma digital contiene una suma de comprobación cifrada para un archivo. María puede crear una suma de comprobación a partir del archivo que recibe y compararla con la suma de comprobación de la firma digital para asegurarse de que el archivo no se ha modificado durante el tránsito. El uso de una firma digital es un método para proporcionar seguridad de integridad.

El cifrado simétrico y asimétrico se puede utilizar para cifrar archivos, pero ninguno de estos métodos se puede utilizar para determinar si un archivo se ha cambiado durante el tránsito. Un certificado digital es una clave pública con la identificación que lo acompaña y que permite a un usuario estar razonablemente seguro de la identidad del propietario de una clave pública para que la información no se envíe por error a un impostor. Un certificado digital no se puede utilizar para determinar si el contenido de un archivo se ha cambiado durante el tránsito.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Firmas Digitales

---

Question #29 of 193

Question ID: 1111725

Su organización ha implementado una infraestructura de clave pública (PKI) para emitir certificados. Recientemente, su organización emitió varios certificados a una organización asociada. Ha revocado los certificados hoy. Sin embargo, a la administración le preocupa que el período de gracia de la solicitud de revocación impida que los certificados se revoquen de manera oportuna. ¿Qué afirmación es cierta de este período?

✓ **A)** Se relaciona con el tiempo de respuesta máximo que tarda la CA para una revocación.

✗ **B)** Se refiere al período de gracia para que un servidor de CA de reserva se actualice a sí mismo.

✗ **C)** Se refiere a la validez de una firma digital.

✗ **D)** Se refiere al tiempo que tarda una autoridad de registro (RA) en registrar un usuario.

explicación

El período de gracia de la solicitud de revocación hace referencia al tiempo de respuesta máximo que tarda el servidor de la entidad de certificación (CA) para realizar una revocación. Un certificado se revoca cuando la información contenida en el certificado está supuestamente en peligro o cuando el certificado expira. La solicitud de revocación puede ser iniciada por las siguientes entidades:

- el titular del certificado
- la propia CA
- otra CA que emite certificados
- un RA asociado

La CA que entretiene la solicitud de revocación realizada por una entidad decide la cantidad de tiempo necesario para procesar la solicitud. La cantidad de tiempo se conoce como período de gracia de solicitud de revocación.

Durante el proceso de revocación, la entidad solicitante debe estar debidamente autenticada de forma similar a una transacción regular. El procedimiento utilizado para autenticar la entidad durante la revocación sigue siendo el mismo que el utilizado para emitir el certificado. La solicitud de revocación lleva una firma digital con un certificado digital válido.

El período de gracia de la solicitud de revocación no hace referencia a la validez de una firma digital.

El período de gracia de la solicitud de revocación no hace referencia al tiempo que tarda una entidad de registro (RA) en registrar un usuario. Durante el proceso de registro e inscripción, la RA inicia el proceso de certificación con la CA en nombre del usuario solicitante. El proceso se inicia solo después de establecer y confirmar la identidad de un usuario solicitante. Por lo tanto, RA actúa entre la CA y la entidad solicitante.

El servidor de CA de reserva no requiere un período de gracia para actualizarse. Por lo tanto, el período de gracia de la solicitud de revocación no está relacionado con el servidor de CA de copia de seguridad.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Autoridad de certificación (CA) y Autoridad de registro (RA)

Requisitos operacionales,http://www.cesnet.cz/pki/CP/Basic/2.0/html/ch04.html

Question #30 of 193

Question ID: 1113941

¿Qué tipo de sistema de rociadores de agua NO es apropiado para un entorno de procesamiento de datos?

- ✗ **A)** sistema de rociadores de agua de tubería seca
- ✓ **B)** sistema de rociadores de agua diluyda
- ✗ **C)** sistema de rociadores de agua de tubería húmeda
- ✗ **D)** sistema de rociadores de agua pre-acción

explicación

El sistema de rociadores de agua diluye no se recomienda para entornos de procesamiento de datos porque cuando se activa, descarga un gran volumen de agua en un corto espacio de tiempo y puede dañar los sistemas informáticos y otros equipos de procesamiento de datos. Un sistema de agua de rociadores de diluvio es similar a un sistema de rociadores de agua de tubería seca, pero el cabezal de rociadores está abierto para permitir la liberación de un gran volumen de agua en un período relativamente corto.

El sistema de rociadores de agua de tubería seca no contiene agua en las tuberías. Contiene presión de aire. El agua se retene mediante válvulas. Esto induce un retraso entre la activación del aspersor al alcanzar un umbral de temperatura y la descarga real de agua. Este retraso permite apagar los sistemas informáticos y la unidad de energía eléctrica en caso de falsa alarma.

El sistema de rociadores de agua de tubería húmeda siempre contiene agua en las tuberías, y el agua se descarga cada vez que se activa el aspersor. Los sistemas de rociadores de tuberías húmedas son los más adecuados para extinguir incendios que requieren un tiempo de reacción mínimo. La desventaja de este tipo de sistema es que una rotura en la tubería puede causar daños extensos por agua a los equipos críticos. A diferencia de los rociadores de pre-acción, los sistemas de rociadores de tuberías húmedas no proporcionan tiempo suficiente para apagar los sistemas informáticos y la unidad de energía eléctrica en caso de una falsa alarma.

Se recomienda un sistema de rociadores de agua antes de la acción para las instalaciones de procesamiento de datos. Combina sistemas de tubería seca y rociadores de tubería húmeda. El agua se libera en las tuberías solo cuando la temperatura alcanza un umbral predefinido. El cabezal del aspersor no libera el agua inmediatamente, sino que espera a que un contacto se derrita. En caso de una falsa alarma, este mecanismo proporciona tiempo suficiente para cerrar el suministro de agua o para utilizar un extintor de incendios si el fuego es controlable y limitado a un área pequeña.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, extinción de incendios

---

Question #31 of 193

Question ID: 1105045

Debe descifrar un archivo que se cifra mediante cifrado asimétrico. ¿Qué se debe utilizar para descifrar el archivo?

✗ **A)** Plaintext
✓ **B)** clave privada
✗ **C)** clave pública
✗ **D)** resumen del mensaje

explicación

Se debe utilizar una clave privada para descifrar un archivo que utiliza cifrado asimétrico. En el cifrado asimétrico, que a veces se conoce como cifrado de clave pública, un usuario crea una clave pública y un par de claves privadas. El usuario distribuye la clave pública y conserva la clave privada. A continuación, otro usuario puede utilizar la clave pública distribuida para cifrar un archivo antes de enviarlo al propietario de la clave privada. A continuación, el propietario utiliza la clave privada para descifrar el archivo recibido. Si un hacker quiere descifrar un archivo que fue cifrado con la clave pública de un usuario, entonces el hacker debe obtener acceso o fabricar un reemplazo para la clave privada.

Un resumen del mensaje, creado por un algoritmo hash, se puede utilizar para determinar si un archivo se ha modificado después de la creación del resumen del mensaje del archivo. El texto sin formato hace referencia a archivos sin cifrar.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, algoritmos asimétricos

---

Question #32 of 193

Question ID: 1192923

¿Qué modelo de control de acceso utiliza el axioma de integridad estrella (*) y el axioma de integridad simple?

- ✓ **A)** Modelo biba
- ✗ **B)** Modelo de muro chino
- ✗ **C)** Modelo de Clark-Wilson
- ✗ **D)** Modelo Bell-LaPadula

explicación

El modelo de control de acceso Biba, un modelo de seguridad formal para la integridad de objetos y sujetos en un sistema, utiliza el axioma de integridad de estrella (*) y el axioma de integridad simple. El axioma de integridad *, a veces denominado "sin escritura", se utiliza para garantizar que un sujeto no escriba en un objeto con un nivel de integridad superior. El axioma de integridad simple, a veces denominado "sin lectura hacia abajo", se utiliza para garantizar que un sujeto no lea datos de un nivel de integridad inferior.

Ninguno de los otros modelos utiliza estos axiomas.

El énfasis principal del modelo Biba es la integridad. Aborda la modificación no autorizada de datos. El modelo biba utiliza una relación sujeto-objeto. Garantiza que se mantiene la integridad evitando que los datos fluyan entre los niveles de integridad. El objetivo de la integridad es prevenir la modificación de la información por parte de usuarios no autorizados, prevenir la modificación no autorizada o involuntaria de la información por parte de usuarios autorizados y preservar la consistencia interna y externa de la información. A los sujetos se les asignan clases de acuerdo con su confiabilidad; a los objetos se les asignan etiquetas de integridad de acuerdo con el daño que se haría si los datos se modificaran incorrectamente.

Los dos modelos de control de acceso más conocidos son el modelo Bell-LaPadula y el modelo Biba.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobjetiva:
Implementar y gestionar procesos de ingeniería utilizando principios de diseño seguro

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Operaciones de seguridad, Modelo Biba

---

Question #33 of 193

Question ID: 1104946

¿Qué modelo de seguridad ilustra el modo de seguridad multinivel?

✓ **A)** Modelo Bell-LaPadula

✗ **B)** modelo de transacción finita

✗ **C)** modelo de acceso

✗ **D)** Modelo de Brewer y Nash

explicación

El modelo Bell-LaPadula ilustra el modo de seguridad multinivel porque permite el procesamiento simultáneo de información clasificada a través de los niveles de seguridad. Este modelo aborda el flujo de información de niveles más altos a bajos. La ventaja clave del modo de seguridad multinivel es la capacidad de procesar información de diferentes categorías y permitir el acceso a una base de usuarios seleccionada. Este modelo formaliza la política de seguridad multinivel del Departamento de Defensa de los Estados Unidos.

El modelo de transacción finita y el modelo de acceso no son categorías válidas de modelos de flujo de información que implementan el modo de seguridad multinivel.

El modelo de Brewer y Nash, también conocido como el modelo de la Muralla China, establece que los controles de acceso para un sistema cambiarán dinámicamente en función de las actividades de un usuario y las solicitudes de acceso anteriores. Las solicitudes de los usuarios para acceder a la información pueden ser denegadas si la solicitud presenta un conflicto de intereses. Por ejemplo, es posible que un usuario del departamento de cuentas no pueda ver los informes financieros de una empresa hermana de la misma organización. Esto garantiza que el usuario no introduzca ningún conflicto de intereses.

El modo de seguridad multinivel asigna etiquetas de confidencialidad a sujetos y objetos. Un sujeto puede acceder al objeto si la etiqueta de sensibilidad del sujeto es mayor o igual que la etiqueta de sensibilidad del objeto. Si la etiqueta de sensibilidad del sujeto es inferior a la etiqueta de sensibilidad del objeto, se deniega al sujeto el acceso al objeto.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender los conceptos fundamentales de los modelos de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Operaciones de seguridad, Modelo Bell-LaPadula

---

Question #34 of 193

Question ID: 1192926

Haga clic en cada uno de los encabezados del escenario para expandir o contraer su contenido. Debe leer todo el escenario para responder a la pregunta.

fondo

Usted es un profesional de la seguridad contratado recientemente por una institución financiera que cotiza en bolsa para ayudar a administrar la seguridad de la organización. La oficina principal de la compañía está en Nueva York, NY, y tiene sucursales adicionales en todo Estados Unidos.

Temas actuales

La infraestructura actual incluye servidores Windows, servidores UNIX, clientes Windows, clientes Mac, dispositivos móviles Windows y dispositivos móviles Mac implementados en todas las oficinas. El departamento de TI de la compañía tiene un gran personal ubicado en la oficina de Nueva York. Cada sucursal tiene unos pocos miembros del personal de TI local que solo se encargan de los problemas de esa sucursal.

Ha identificado varias instancias en las que los ataques contra los sistemas cliente no se impidieron ni detectaron en el nivel de cliente porque no se implementó ningún control para evitar el ataque. Los datos fueron robados de algunos dispositivos. Toda una sucursal estaba infectada con malware y virus y requería varios días de tiempo de recuperación, lo que significaba la pérdida de ingresos. Por último, recientemente descubrió que varios sistemas cliente tienen instaladas versiones sin licencia de sistemas operativos. Debe asegurarse de que se implementan los controles adecuados para mitigar estos riesgos.

En una auditoría reciente, descubrió que varios dispositivos móviles carecían de las actualizaciones adecuadas para sus sistemas operativos o aplicaciones. Además, los usuarios habían desactivado las funciones de limpieza remota y localización GPS en estos dispositivos y habían instalado varias aplicaciones no autorizadas. Necesita una solución para mitigar estos riesgos y controlar la configuración y las aplicaciones de los dispositivos móviles cuando esos dispositivos están conectados a la empresa.

Debido a varios contratos entre su empresa y terceros, debe asegurarse de que ciertos sistemas dentro de su infraestructura logren EAL7 en el modelo de evaluación de criterios comunes.

Recientemente, uno de los servidores de la intranet fue víctima de un ataque de denegación de servicio (DoS). El departamento de TI tardó más de 24 horas en devolver el servidor al estado operativo. Durante ese tiempo, el personal de la oficina principal no pudo acceder a la información importante de recursos humanos almacenada en el servidor afectado.

Se espera que los usuarios utilicen el cifrado simétrico y asimétrico para garantizar la confidencialidad de los datos. Debe implementar un sistema adecuado para administrar las claves de cifrado, los valores hash y los certificados digitales en todos los equipos cliente. También debe proteger las contraseñas, cifrar unidades y administrar los derechos digitales de estos mismos equipos.

La integridad de los datos se ha convertido en una preocupación cada vez más seria para los archivos creados y mantenidos por el departamento de investigación. Debe implementar la solución adecuada para estos archivos. Todos los archivos se encuentran en un único servidor que es accesible sólo por los usuarios en el departamento de investigación.

Nunca se completó formalmente un análisis de riesgos exhaustivo para toda la organización. Se le ha pedido que encabece este proyecto. Como parte de este proceso, debe identificar las amenazas geográficas para cada oficina

individual.

Su organización desplegará dos oficinas internacionales a finales de este año. Se le ha invitado a participar en la selección de instalaciones y en el proceso de seguridad interna del edificio para proporcionar información de seguridad concreta.

¿Qué debe implementar en los equipos cliente para administrar mejor las claves de cifrado, las contraseñas, el cifrado de unidad y los derechos digitales para los usuarios?

- ✓ **A)** Tpm
- ✗ **B)** PKI
- ✗ **C)** Vm
- ✗ **D)** DNS

explicación

Debe implementar el Módulo de plataforma segura (TPM) en los equipos cliente para administrar mejor las claves de cifrado, las contraseñas, el cifrado de unidad y los derechos digitales de los usuarios.

Una infraestructura de clave pública (PKI) se usa para administrar de forma centralizada los certificados digitales. Un Sistema de nombres de dominio (DNS) se utiliza para resolver nombres de dominio completos (FQDN) en direcciones IP. Una máquina virtual (VM) es un equipo de software que, al igual que un equipo físico, ejecuta un sistema operativo y aplicaciones. Las máquinas virtuales comparten recursos con el equipo host.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender las capacidades de seguridad de los sistemas de información (por ejemplo, protección de memoria, Módulo de plataforma segura (TPM), cifrado/descifrado)

Referencias:

Módulo de plataforma segura (TPM), http://whatis.techtarget.com/definition/trusted-platform-module-TPM

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Capacidades de seguridad de los sistemas de información

---

Question #35 of 193

Question ID: 1192929

Se le ha pedido que implemente software antivirus para su entorno de virtualización. ¿Dónde debe instalar el software antivirus?

- ✗ **A)** Sólo en cada equipo virtual
- ✗ **B)** Sólo en el equipo host
- ✗ **C)** Sólo en el equipo físico
- ✓ **D)** Tanto en el equipo host como en todos los equipos virtuales

explicación

Debe instalar el software antivirus tanto en el equipo host como en todos los equipos virtuales. Las máquinas virtuales pueden verse comprometidas con virus al igual que un equipo físico.

La virtualización le permite implementar equipos virtuales en la red sin necesidad de adquirir el hardware físico para implementar el servidor. La virtualización le permite aislar las máquinas virtuales individuales de la manera que necesite. Sin embargo, todas las máquinas virtuales ubicadas en un host virtual se ven comprometidas si el host virtual está en peligro. Por lo tanto, es importante no limitar la implementación de las medidas de seguridad adecuadas al host virtual. También debe implementar las medidas de seguridad adecuadas en cada máquina virtual, incluida la implementación de software antivirus y el uso del principio de privilegios mínimos.

No debe instalar el software antivirus sólo en el equipo host, en cada equipo virtual o sólo en el equipo físico. Dado que las máquinas virtuales pueden verse comprometidas con virus al igual que un equipo físico, debe asegurarse de que el software antivirus está instalado en el equipo host y en cada equipo virtual.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
evaluar y mitigar las vulnerabilidades de las arquitecturas de seguridad, los diseños y los elementos de la solución

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, virtualización

Seguridad y Virtualización, HYPERLINK "http://techgenix.com/security-virtualization/" \t "sean" http://www.windowsecurity.com/articles/Security-Virtualization.html

---

Question #36 of 193

Question ID: 1105044

¿Qué tipo de cifrado reemplaza el texto original de un mensaje con un texto diferente?

- ✓ **A)** cifrado de sustitución
- ✗ **B)** cifrado de transposición
- ✗ **C)** cifrado de secuencias
- ✗ **D)** cifrado de bloques

explicación

Un cifrado de sustitución es un método de cifrado en el que los bloques de caracteres del texto original se sustituyen por diferentes caracteres o bloques de caracteres. El receptor descifra el mensaje a su forma original invirtiendo el proceso de sustitución. Una clave secreta decide la secuencia y el orden de las funciones que debe realizar el receptor para volver a convertir el texto cifrado en texto sin formato.

Un cifrado de bloques divide el mensaje en bloques de bits y, a continuación, cifra cada bloque. Un cifrado de bloques funciona en una secuencia de bloques de texto sin formato de tamaño fijo y se puede operar como una secuencia. El cifrado es más adecuado en la implementación de software en lugar de hardware. Las funciones de cifrado de sustitución y transposición se llevan a cabo bloque a bloque. En un cifrado por bloques, la difusión propaga la influencia de un carácter de texto plano sobre muchos caracteres de texto cifrado. La difusión se logra a través de la permutación. La técnica de confusión se utiliza en cifrados por bloques para ocultar la conexión estadística entre el texto cifrado y el texto plano. La técnica de difusión se utiliza para difundir la influencia de un carácter de texto plano sobre muchos caracteres de texto cifrado.

Un cifrado de secuencia trata el mensaje como una secuencia de bits. Las funciones matemáticas se realizan en los bits individuales. Este método de funcionamiento hace que el cifrado de secuencias sea más adecuado para implementaciones de hardware. Con un cifrado de flujo, el mismo equipo se puede utilizar para el cifrado y descifrado. Un cifrado de flujo es susceptible a implementaciones de hardware que dan como resultado velocidades más altas. Dado que el cifrado tiene lugar poco a poco, no hay propagación de errores.

Un cifrado de transposición dispersa el texto original en el mensaje en lugar de sustituirlo por otro texto. Las permutaciones y combinaciones se utilizan para revolver las letras en un cifrado de transposición. Una clave determina la posición de las letras movidas en el texto original.

Hay dos tipos de cifrados de sustitución: simples y poligráficos. Un cifrado de sustitución simple opera en letras individuales, mientras que un cifrado de sustitución poligráfica opera en grupos más grandes de letras. Un cifrado mono-alfabético en sustitución simple implementa la sustitución fija sobre el mensaje completo, mientras que un cifrado polialfabético, como un cifrado polialfabético Vigenere, en sustitución poligráfica despliega múltiples sustituciones en diferentes momentos del mensaje.

Un ejemplo del cifrado de sustitución es el cifrado César, que es un cifrado mono-alfabético. En el cifrado César, cada letra del texto original se sustituye por el alfabeto tres lugares más allá de ella en la secuencia del alfabeto.

Un algoritmo criptográfico también se conoce como cifrado.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Conceptos de criptografía

---

Question #37 of 193

Question ID: 1104936

¿Qué afirmación es cierta del modelo de flujo de información?

- ✗ **A)** El modelo de flujo de información no permite el flujo de información de un nivel de seguridad inferior a un nivel de seguridad superior.
- ✓ **B)** El modelo de flujo de información permite el flujo de información dentro del mismo nivel de seguridad.
- ✗ **C)** El modelo de Biba no se basa en el modelo de flujo de información.
- ✗ **D)** El modelo de flujo de información solo se ocupa de la dirección del flujo.

explicación

El modelo de flujo de información permite el flujo de información entre los diferentes niveles de seguridad y los objetos dentro del mismo nivel de seguridad basado en una matriz de control de acceso. Un flujo actúa como un tipo de dependencia al relacionar dos versiones del mismo objeto. El flujo asigna la transformación del objeto de una versión a otra.

El modelo Biba y el modelo Ball-LaPadula se basan tanto en el modelo de flujo de información como en el modelo de máquina de estado.

El modelo de flujo de información permite cada tipo de flujo de información y no se limita a la dirección del flujo. Se permite que la información fluya entre diferentes niveles de seguridad o dentro del mismo nivel de seguridad si no hay ninguna restricción en la operación. Si un usuario intenta una operación restringida, el sistema utiliza la matriz de control de acceso para verificar si el usuario tiene permiso para realizar la acción o no.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobjetiva:
Implementar y gestionar procesos de ingeniería utilizando principios de diseño seguro

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 3: Operaciones de seguridad, modelos de flujo de información

---

Question #38 of 193

Question ID: 1113924

¿Cuál es el propósito de un dispositivo que utiliza el acceso directo a memoria (DMA)?

- ✗ **A)** Se comunica mediante una dirección lógica.
- ✓ **B)** Implementa la transferencia de datos de alta velocidad entre el dispositivo y la memoria.
- ✗ **C)** Proporciona multiprocesamiento mediante una entrada/salida (E/S) controlada por interrupciones.
- ✗ **D)** Implementa la transferencia de datos de alta velocidad entre el dispositivo y la CPU.

explicación

El propósito de un dispositivo que utiliza DMA es la transferencia de datos de alta velocidad entre el dispositivo y la memoria. Esto se conoce a menudo como E/S mediante DMA.

La E/S controlada por interrupciones proporciona multiprocesamiento mediante interrupciones. En este entorno, un dispositivo envía una interrupción a la CPU mientras está ocupada para que la CPU pueda continuar con otros procesos.

La E/S totalmente asignada garantiza que un dispositivo se comunique mediante direcciones lógicas. El sistema operativo confía en el dispositivo.

La E/S preasignada garantiza que un dispositivo se comunique mediante una dirección física. El sistema operativo no confía en el dispositivo.

La E/S programable permite a la CPU consultar el dispositivo para ver si aceptará más datos. En este tipo de administración de dispositivos, la CPU puede perder mucho tiempo esperando en un dispositivo para estar listo.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender las capacidades de seguridad de los sistemas de información (por ejemplo, protección de memoria, Módulo de plataforma segura (TPM), cifrado/descifrado)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura de seguridad e ingeniería, memoria y almacenamiento,

---

Question #39 of 193

Question ID: 1105074

¿Qué es una lista de números de serie de certificados digitales que no han caducado, pero que deben considerarse no válidos?

✗ **A)** UDP

✗ **B)** Ca

✓ **C)** Crl

✗ **D)** KDC

explicación

Una lista de revocación de certificados (CRL) contiene una lista de números de serie de certificados digitales que no han caducado pero que una entidad de certificación (CA) ha especificado que no son válidos. Normalmente, el número de serie de un certificado digital se coloca en una CRL porque el certificado digital se ha visto comprometido de alguna manera.

Una CA genera y valida certificados digitales. Un centro de distribución de claves (KDC) se utiliza en la autenticación de red Kerberos para distribuir las claves de acceso a recursos. Protocolo de datagramas de usuario (UDP) proporciona comunicaciones sin conexión en la red TCP/IP

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Lista de revocación de certificados (CRL)

Question #40 of 193

Question ID: 1111710

Un servidor de archivos se ha reiniciado inesperadamente en modo de usuario único. No está seguro de qué causó el reinicio. ¿Qué debes hacer a continuación?

✓ **A)** Recuperar archivos dañados del sistema de archivos.

✗ **B)** Reinicie el servidor de archivos.

✗ **C)** Valide los archivos críticos de configuración y del sistema.

✗ **D)** Identifique la causa del reinicio inesperado.

explicación

Debe recuperar los archivos dañados del sistema de archivos a continuación.

Ninguna de las otras opciones es correcta. Cuando un sistema se bloquea, debe realizar los pasos siguientes en este orden:

- Entrar en modo de usuario único. (Es posible que el equipo ya esté en este modo).
- Recuperar archivos dañados del sistema de archivos.
- Identifique la causa del reinicio inesperado y repare el sistema según sea necesario.
- Valide la configuración crítica y los archivos del sistema y las operaciones del sistema.
- Reinicie el sistema con normalidad.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender las capacidades de seguridad de los sistemas de información (por ejemplo, protección de memoria, Módulo de plataforma segura (TPM), cifrado/descifrado)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 7: Operaciones de seguridad, recuperación de confianza

---

Question #41 of 193

Question ID: 1113918

¿Qué modelo de control de acceso utiliza estados y transiciones de estado en el diseño del sistema de protección?

✓ **A)** Modelo Take-Grant

✗ **B)** Modelo de flujo de información

✗ **C)** Modelo biba

✗ **D)** Modelo Bell-LaPadula

explicación

El modelo Take-Grant utiliza estados y transiciones de estado en el diseño del sistema de protección. El modelo Take-Grant fue creado para mostrar que es posible asegurar un sistema informático incluso cuando el número de sujetos y objetos es grande. Especifica los derechos que un sujeto puede transferir a un objeto.

Ninguno de los otros modelos utiliza estados y transiciones de estado.

Mediante el modelo Take-Grant, se crea un gráfico dirigido que especifica los derechos que un sujeto puede conceder a un objeto y recibir de otro sujeto.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobjetiva:
Implementar y gestionar procesos de ingeniería utilizando principios de diseño seguro

Referencias:

Cissp Cert Guide (3rd Edition), Chapter3: Security Operations, Take-Grant Model

Sistemas take-grant, http://ei.cs.vt.edu/~cs5204/sp99/distributedSys/groener/takegrnt.html

---

Question #42 of 193

Question ID: 1111709

¿Cuál es la mejor descripción de la memoria caché?

- ✗ **A)** memoria no volátil que mantiene su contenido incluso durante los cortes de energía
- ✗ **B)** Memoria especial utilizada en dispositivos portátiles
- ✗ **C)** memoria volátil que pierde su contenido durante los cortes de energía
- ✓ **D)** memoria utilizada para la transferencia de datos a alta velocidad

explicación

La memoria caché es la memoria que se utiliza para la transferencia de datos de alta velocidad. La CPU puede acceder a los datos de la memoria caché más rápidamente que los datos ubicados en la memoria de acceso aleatorio (RAM).

La memoria de sólo lectura (ROM) es una memoria no volátil que mantiene su contenido incluso durante los cortes de energía.

La memoria flash es una memoria especial que se utiliza en dispositivos portátiles.

La MEMORIA RAM es una memoria volátil que pierde su contenido durante los cortes de energía.

Para realizar pruebas, debe comprender la relación entre el bus del equipo, el almacenamiento primario, el almacenamiento secundario y la memoria. El bus de la computadora es un grupo de conductores para la dirección de datos y del control. La mayoría de los equipos contienen los tres tipos de buses siguientes:

- Bus de direcciones - una conexión cableada entre la CPU y los chips de RAM. Lleva información sobre qué dispositivo se está comunicando con la CPU.
- Bus de datos: el área en la que residen los datos que utiliza la CPU. Transporta los datos reales que se están procesando.
- Bus de control - la conexión entre la CPU y otros dispositivos. Lleva comandos de la CPU y devuelve señales de estado de los dispositivos.

El almacenamiento primario es la memoria direccionable directamente por la CPU, que es para el almacenamiento de instrucciones y datos asociados con el programa que se está ejecutando. El almacenamiento secundario es la memoria, como los discos magnéticos, que proporciona almacenamiento no volátil. La memoria virtual es la memoria de almacenamiento secundaria utilizada junto con la memoria real para presentar una CPU con un espacio de direcciones más grande y aparente.

La jerarquía de memoria en un equipo típico es la siguiente: CPU, caché, memoria principal y memoria secundaria.

El firmware es un tipo de software que se mantiene en un chip ROM o EROM. Permite que el ordenador se comunique con algún tipo de dispositivo periférico. Las instrucciones del BIOS del sistema también se mantienen en el firmware de la placa base. En la mayoría de las situaciones, el firmware no se puede modificar a menos que alguien tenga acceso físico al sistema. Esto es diferente de otros tipos de software que pueden ser modificados de forma remota o a través de medios lógicos.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender las capacidades de seguridad de los sistemas de información (por ejemplo, protección de memoria, Módulo de plataforma segura (TPM), cifrado/descifrado)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, CPU

Question #43 of 193

Question ID: 1113921

Está revisando los estándares de seguridad de Common Criteria. ¿Qué nivel de garantía de evaluación de criterios comunes (EAL) es el punto de referencia común para sistemas operativos y productos?

✓ **A)** EAL 4

✗ **B)** EAL 3

✗ **C)** EAL 5

✗ **D)** EAL 6

✗ **E)** EAL 7

explicación

EAL 4 es el punto de referencia común para sistemas operativos y productos. Common Criteria ha diseñado los criterios de evaluación en siete EES:

- EAL 1 - Un usuario desea que el sistema funcione, pero ignora las amenazas de seguridad.
- EAL 2 : los desarrolladores utilizan buenas prácticas de diseño, pero la seguridad no es una prioridad alta.
- EAL 3 : los desarrolladores proporcionan niveles moderados de seguridad.
- EAL 4 - La configuración de seguridad se basa en un buen desarrollo comercial. Este nivel es el punto de referencia común para los sistemas comerciales, incluidos los sistemas operativos y los productos.
- EAL 5 - La seguridad se implementa a partir del diseño temprano. Proporciona altos niveles de garantía de seguridad.
- EAL 6 - La ingeniería de seguridad especializada proporciona altos niveles de garantía. Este nivel será altamente seguro de los atacantes de penetración.
- EAL 7 - Se proporcionan niveles extremadamente altos de seguridad. Este nivel requiere pruebas exhaustivas, mediciones y pruebas independientes.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender los conceptos fundamentales de los modelos de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Operaciones de seguridad, criterios comunes

---

Question #44 of 193

Question ID: 1113933

¿Qué algoritmo hash utiliza un valor hash de 192 bits y se desarrolló para sistemas de 64 bits?

✗ **A)** MD5

✗ **B)** Sha

✓ **C)** tigre

✗ **D)** HAVAL

explicación

Tiger utiliza un valor hash de 192 bits y fue desarrollado para sistemas de 64 bits.

Ninguno de los otros algoritmos hash se desarrolló para sistemas de 64 bits.

HAVAL utiliza un hash de longitud variable. El algoritmo hash seguro (SHA) utiliza un valor hash de 160 bits. Message Digest 5 (MD5) utiliza un valor hash de 128 bits.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

CISSP Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Tiger

---

Question #45 of 193

Question ID: 1192928

Usted es responsable de administrar un equipo con Windows Server 2012 que hospeda varios equipos virtuales. Debe instalar los últimos parches para el sistema operativo. ¿Dónde debe instalar los parches?

- ✓ **A)** en el equipo host y en todos los equipos virtuales de Windows Server 2012
- ✗ **B)** solo en cada equipo virtual de Windows Server 2012
- ✗ **C)** Sólo en el equipo físico
- ✗ **D)** Sólo en el equipo host

explicación

Debe instalar las revisiones tanto en el equipo host como en todos los equipos virtuales de Windows Server 2008. Las máquinas virtuales pueden verse comprometidas al igual que un equipo físico.

No debe instalar las revisiones sólo en el equipo host, en cada equipo virtual de Windows Server 2008 únicamente o en el equipo físico. Dado que las máquinas virtuales pueden verse comprometidas al igual que un equipo físico, debe asegurarse de que las revisiones están instaladas tanto en el equipo host como en cada equipo virtual de Windows Server 2008.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
evaluar y mitigar las vulnerabilidades de las arquitecturas de seguridad, los diseños y los elementos de la solución

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, virtualización

Seguridad y Virtualización, HYPERLINK "http://techgenix.com/security-virtualization/" \t "sean" http://www.windowsecurity.com/articles/Security-Virtualization.html

---

Question #46 of 193

Question ID: 1105066

¿Qué servicio cumple la criptografía al garantizar que un remitente no puede denegar el envío de un mensaje una vez que se transmite?

- ✗ **A)** autenticidad
- ✓ **B)** no repudio
- ✗ **C)** integridad
- ✗ **D)** confidencialidad

explicación

El no repudio es el servicio que cumple la criptografía que garantiza que un remitente no puede denegar el envío de un mensaje una vez que se transmite.

La confidencialidad impide que los usuarios no autorizados accedan a los recursos y se puede proporcionar mediante cifrado. La autenticidad garantiza que un mensaje procede de un origen válido y que el remitente está identificado. La integridad garantiza que el mensaje no se edite de ninguna manera mientras se transmite.

La firma digital de mensajes de correo electrónico proporciona autenticación, no seguimiento e integridad. NO proporciona confidencialidad.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Firma Digital

---

Question #47 of 193

Question ID: 1132509

¿Qué característica identifica el nivel de seguridad TCSEC B2?

- ✓ **A)** protección estructurada
- ✗ **B)** protección de acceso controlada
- ✗ **C)** protección mínima
- ✗ **D)** seguridad etiquetada

explicación

El nivel de seguridad B2 se conoce como protección estructurada.

Los criterios de evaluación de sistemas informáticos de confianza (TCSEC) clasifican los sistemas en divisiones jerárquicas de niveles de seguridad que van desde la protección verificada hasta la seguridad mínima.

Los niveles definidos por TCSEC y los subniveles de seguridad son los siguientes:

- R: Protección verificada que ofrece el más alto nivel de seguridad
  - Una calificación A1 implica que la garantía de seguridad, el diseño, el desarrollo, la implementación, la evaluación y la documentación de un equipo se realizan de una manera muy formal y detallada. Una infraestructura que contiene sistemas con clasificación A1 es el entorno más seguro y normalmente se utiliza para almacenar información altamente confidencial y confidencial.
- B: Protección obligatoria basada en el modelo de seguridad bell-lapadula y aplicada mediante el uso de etiquetas de seguridad.
  - Una clasificación B1 se refiere a la seguridad etiquetada, donde cada objeto tiene una etiqueta de clasificación y cada sujeto tiene un nivel de autorización de seguridad. Para acceder al contenido del objeto, el sujeto debe tener un nivel igual o mayor de autorización de seguridad que el objeto. Un sistema compara el nivel de autorización de seguridad de un sujeto con la clasificación del objeto para permitir o denegar el acceso al objeto. La categoría B1 ofrece aislamiento de procesos, el uso de etiquetas de dispositivos, el uso de especificaciones y verificaciones de diseño y controles de acceso obligatorios. Los sistemas B1 se utilizan para manejar información clasificada.
  - Una clasificación B2 se refiere a la protección estructurada. Se debe utilizar un procedimiento de autenticación estricto en los sistemas con clasificación B2 para permitir que un sujeto acceda a los objetos mediante la ruta de acceso de confianza sin puertas traseras. Este nivel es el nivel más bajo para implementar la administración de instalaciones de confianza; los niveles B3 y A1 también lo implementan. Los requisitos adicionales de una clasificación B2 incluyen la separación de las funciones de operador y administrador, las etiquetas de sensibilidad y el análisis del canal de almacenamiento encubierto. Un sistema B2 se utiliza en entornos que contienen información altamente confidencial. Por lo tanto, un sistema B2 debe ser resistente a los intentos de penetración.
  - Una clasificación B3 se refiere a los dominios de seguridad. Los sistemas B3 deben ser capaces de realizar una recuperación de confianza. Un sistema evaluado con una clasificación B3 debe tener el rol del

administrador de seguridad totalmente definido. Un sistema B3 debe proporcionar la funcionalidad de supervisión y auditoría. Un sistema B3 se utiliza en entornos que contienen información altamente sensible y debe ser resistente a los intentos de penetración. Otra característica de la clasificación B3 es el análisis de canal de temporización encubierto.

- C: Protección discrecional basada en el acceso discrecional de sujetos, objetos, individuos y grupos.
  - Una clasificación C1 se refiere a la protección de seguridad discrecional. Para habilitar el proceso de calificación, los sujetos y los objetos deben separarse de la instalación de auditoría mediante un proceso de identificación y autenticación claro. Un sistema de clasificación C1 es adecuado para entornos en los que los usuarios procesan la información en el mismo nivel de sensibilidad. Un sistema de clasificación C1 es adecuado para entornos con problemas de seguridad baja.
  - Una clasificación C2 se refiere a la protección de acceso controlado. La funcionalidad de autenticación y auditoría en los sistemas debe estar habilitada para que se produzca el proceso de clasificación. Un sistema con una clasificación C2 proporciona protección de recursos y no permite la reutilización de objetos. La reutilización de objetos implica que un objeto no debe tener datos remanentes que puedan ser utilizados por un sujeto más adelante. Un sistema C2 proporciona un control de acceso granular y establece un nivel de responsabilidad cuando los sujetos acceden a objetos. Un sistema con clasificación C2 es adecuado para un entorno comercial.
- D: Clasificación de protección mínima que se ofrece a los sistemas que no cumplen los criterios de evaluación

Una calificación más alta implica un mayor grado de confianza y seguridad. Por ejemplo, una clasificación B2 proporciona más seguridad que una clasificación C2. Una calificación más alta incluye los requisitos de una calificación más baja. Por ejemplo, una clasificación B2 incluye las características y especificaciones de una clasificación C2.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender los conceptos fundamentales de los modelos de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Operaciones de seguridad, criterios comunes

---

Question #48 of 193

Question ID: 1111732

¿Qué tipo de sistema de rociadores de agua se utiliza mejor en climas más fríos?

✗ **A)** tubería húmeda

✗ **B)** diluvio

✓ **C)** tubería seca

✗ **D)** pre-acción

explicación

Un sistema de rociadores de agua de tubería seca se utiliza mejor en climas más fríos. Debido a que el agua no se mantiene en las tuberías del sistema, las tuberías no se congelarán. En un sistema de tuberías secas, los siguientes pasos se producen cuando se detecta un incendio:

- Se activa el sensor de calor o humo.
- El agua llena las tuberías que conducen a las cabezas de los aspersor.
- La alarma contra incendios suena.
- La energía eléctrica está desconectada.
- El agua fluye de los aspersores.

Los sistemas de tuberías húmedas retienen agua en las tuberías. Este sistema se suele implementar en todos los edificios en climas más cálidos.

Los sistemas de pre-acción son similares a los sistemas de tuberías secas. La principal diferencia es que los sistemas de pre-acción retienen el aire presurizado en las tuberías. Cuando se reduce el aire presurizado, las tuberías se llenan. Además, los cabezales de rociadores incluyen un enlace térmico-fusible que debe derretirse antes de que se libere el agua. Este tipo de sistema es más caro y, por lo tanto, solo se utiliza en entornos de procesamiento de datos.

Un sistema de diluvio libera una mayor cantidad de agua en un tiempo más corto.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, extinción de incendios

---

Question #49 of 193

Question ID: 1114715

La administración ha solicitado que se instalen detectores de agua para garantizar que el agua se detecte antes de que se realicen daños mayores. ¿En qué lugares deben instalarse detectores de agua?

a. Bajo pisos elevados

b. entre muros

c. bajo los cimientos del edificio

d. en los límites máximos caídos

- ✓ **A)** Opciones A y D
- ✗ **B)** Opción d
- ✗ **C)** opción c
- ✗ **D)** opción A
- ✗ **E)** opción b
- ✗ **F)** Opciones B y C

explicación

Los detectores de agua deben instalarse debajo de los pisos elevados y en los techos caídos. Los detectores de agua se utilizan para detectar agua antes de que se realicen daños importantes en el equipo, el suelo, las paredes y las computadoras. Los detectores de agua deben utilizarse como un control detective para garantizar que cualquier tipo de problema de agua se detecte lo antes posible.

No es necesario instalar detectores de agua entre las paredes y debajo de los cimientos del edificio.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, fugas de agua e inundaciones

---

Question #50 of 193

Question ID: 1105117

Los planes de diseño del centro de datos de su organización piden que se usen paneles de vidrio para una pared del centro de datos para garantizar que el personal del centro se pueda ver en todo momento. ¿Qué tipo de vidrio se debe utilizar?

- ✓ **A)** resistente a la rotura
- ✗ **B)** acrílico
- ✗ **C)** templado

✗ **D)** cableado

✗ **E)** estándar

explicación

El vidrio resistente a la rotura debe utilizarse en los paneles de vidrio utilizados para una pared del centro de datos. Esto se debe a que la pared actuará como una pared exterior.

Las ventanas estándar no proporcionan protección adicional.

Las ventanas templadas son aquellas en las que el vidrio se calienta y luego se enfría repentinamente para aumentar la integridad y la resistencia del vidrio.

El acrílico es un tipo de plástico en lugar de vidrio. Las ventanas acrílicas suelen ser más fuertes que las ventanas de vidrio. Los acrílicos de policarbonato son los acrílicos más fuertes.

Las ventanas cableadas tienen una malla de alambre incrustada entre dos hojas de vidrio. El cable ayuda a evitar la rotura.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

CISSP Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Entradas de Vidrio

---

Question #51 of 193

Question ID: 1105103

¿Qué control de seguridad física es EL MÁS apropiado cuando se requiere un juicio discriminatorio para mantener la seguridad física de una instalación?

✓ **A)** Guardias

✗ **B)** circuito cerrado de televisión (CCTV)

✗ **C)** Contraseñas

✗ **D)** Perros

explicación

Los guardias pueden servir como un control de seguridad física apropiado siempre que se requiera un juicio discriminatorio inmediato en respuesta a una amenaza de seguridad.

Los controles de acceso físico incluyen insignias, cerraduras, guardias de seguridad, perros, mantraps, torniquetes, cercas, dispositivos de vigilancia y sistemas de detección de intrusiones (IDS).

Los perros y los circuitos cerrados de televisión (CCTVs) son ejemplos de control de seguridad física, aunque requieren la intervención humana para tomar decisiones. Estos ejemplos no pueden usar el juicio discriminatorio para mantener la seguridad física sin la ayuda de otro control de seguridad física.

Una contraseña hace referencia a una cadena de caracteres que un usuario debe escribir para obtener acceso a un recurso protegido de otro modo. Si una persona conoce la contraseña, se concede acceso al sistema. No hay forma de utilizar el juicio discriminatorio en este caso.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Patrol Force

---

Question #52 of 193

Question ID: 1104975

¿Qué es un circuito integrado con lógica interna que es programable?

- ✗ **A)** caché
- ✗ **B)** ROM
- ✓ **C)** un PLD
- ✗ **D)** memoria flash

explicación

Un dispositivo lógico programable (PLD) es un circuito integrado con lógica interna que es programable.

La memoria flash es un tipo especial de memoria utilizada en dispositivos portátiles.

La memoria de sólo lectura es una memoria no volátil que conserva su contenido durante los cortes de energía.

La caché es un tipo de memoria utilizada para la comunicación de datos de alta velocidad. La CPU puede acceder a los datos en caché más rápidamente que los datos ubicados en ram.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender las capacidades de seguridad de los sistemas de información (por ejemplo, protección de memoria, Módulo de plataforma segura (TPM), cifrado/descifrado)

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, dispositivo lógico programable (PLD)

Guía para principiantes de dispositivos lógicos programables, http://www.instructables.com/id/A-Beginners-Guide-to-Programmable-Logic-Devices/

Question #53 of 193

Question ID: 1192925

Haga clic en cada uno de los encabezados del escenario para expandir o contraer su contenido. Debe leer todo el escenario para responder a la pregunta.

fondo

Usted es un profesional de la seguridad contratado recientemente por una institución financiera que cotiza en bolsa para ayudar a administrar la seguridad de la organización. La oficina principal de la compañía está en Nueva York, NY, y tiene sucursales adicionales en todo Estados Unidos.

Temas actuales

La infraestructura actual incluye servidores Windows, servidores UNIX, clientes Windows, clientes Mac, dispositivos móviles Windows y dispositivos móviles Mac implementados en todas las oficinas. El departamento de TI de la compañía tiene un gran personal ubicado en la oficina de Nueva York. Cada sucursal tiene unos pocos miembros del personal de TI local que solo se encargan de los problemas de esa sucursal.

Ha identificado varias instancias en las que los ataques contra los sistemas cliente no se impidieron ni detectaron en el nivel de cliente porque no se implementó ningún control para evitar el ataque. Los datos fueron robados de algunos dispositivos. Toda una sucursal estaba infectada con malware y virus y requería varios días de tiempo de recuperación, lo que significaba la pérdida de ingresos. Por último, recientemente descubrió que varios sistemas cliente tienen instaladas versiones sin licencia de sistemas operativos. Debe asegurarse de que se implementan los controles adecuados para mitigar estos riesgos.

En una auditoría reciente, descubrió que varios dispositivos móviles carecían de las actualizaciones adecuadas para sus sistemas operativos o aplicaciones. Además, los usuarios habían desactivado las funciones de limpieza remota y localización GPS en estos dispositivos y habían instalado varias aplicaciones no autorizadas. Necesita una solución

para mitigar estos riesgos y controlar la configuración y las aplicaciones de los dispositivos móviles cuando esos dispositivos están conectados a la empresa.

Debido a varios contratos entre su empresa y terceros, debe asegurarse de que ciertos sistemas dentro de su infraestructura logren EAL7 en el modelo de evaluación de criterios comunes.

Recientemente, uno de los servidores de la intranet fue víctima de un ataque de denegación de servicio (DoS). El departamento de TI tardó más de 24 horas en devolver el servidor al estado operativo. Durante ese tiempo, el personal de la oficina principal no pudo acceder a la información importante de recursos humanos almacenada en el servidor afectado.

Se espera que los usuarios utilicen el cifrado simétrico y asimétrico para garantizar la confidencialidad de los datos. Debe implementar un sistema adecuado para administrar las claves de cifrado, los valores hash y los certificados digitales en todos los equipos cliente. También debe proteger las contraseñas, cifrar unidades y administrar los derechos digitales de estos mismos equipos.

La integridad de los datos se ha convertido en una preocupación cada vez más seria para los archivos creados y mantenidos por el departamento de investigación. Debe implementar la solución adecuada para estos archivos. Todos los archivos se encuentran en un único servidor que es accesible sólo por los usuarios en el departamento de investigación.

Nunca se completó formalmente un análisis de riesgos exhaustivo para toda la organización. Se le ha pedido que encabece este proyecto. Como parte de este proceso, debe identificar las amenazas geográficas para cada oficina individual.

Su organización desplegará dos oficinas internacionales a finales de este año. Se le ha invitado a participar en la selección de instalaciones y en el proceso de seguridad interna del edificio para proporcionar información de seguridad concreta.

¿Cuál es la descripción correcta para el nivel de Criterios Comunes que ciertos sistemas deben alcanzar porque forman parte de contratos de terceros?

- ✗ **A)** metódicamente diseñado, probado y revisado
- ✗ **B)** semi-formalmente diseñado y probado
- ✗ **C)** diseño semi-formalmente verificado y probado
- ✓ **D)** diseño formalmente verificado y probado

explicación

EAL7 se define como un diseño formalmente verificado y probado. Los siguientes son los niveles de criterios comunes:

EAL1 - probado funcionalmente

EAL2 - probado estructuralmente

EAL3 - metódicamente probado y comprobado

EAL4 - metódicamente diseñado, probado y revisado

EAL5 - semi-formalmente diseñado y probado

EAL6 - diseño semi-formalmente verificado y probado

EAL7 - diseño formalmente verificado y probado

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender los conceptos fundamentales de los modelos de seguridad

Referencias:

Nivel de garantía de evaluación, http://searchdatacenter.techtarget.com/definition/Evaluation-Assurance-Level-EAL

Question #54 of 193

Question ID: 1105087

La administración decide utilizar el código de autenticación de mensajes (MAC) para proteger los mensajes de red. ¿Qué tipo de ataque previene esto?

- ✓ **A)** ataques de enmascaramiento
- ✗ **B)** ataques de denegación de servicio
- ✗ **C)** ataques con bombas lógicas
- ✗ **D)** Ataques de inundación SYN

explicación

El código de autenticación de mensajes (MAC) evita los ataques enmascarados. Enmascarar o suplantar es un truco popular en el que un atacante intercepta el paquete de red, reemplaza la dirección de origen del encabezado de los paquetes con la dirección del host autorizado y vuelve a insertar información falsa que se envía al receptor. Este tipo de ataque implica modificar el contenido de los paquetes. El MAC previene la modificación del paquete para asegurar la integridad de datos. MAC también puede factorizar ataques y problemas de notificación de envío.

Una bomba lógica implica un programa malicioso que permanece inactivo hasta que se activa después de una acción específica por parte del usuario, o después de un cierto intervalo de tiempo. MAC no puede prevenir un ataque de bomba lógica.

En un ataque de inundación SYN, el atacante inunda el objetivo con paquetes IP falsificados y hace que se congele o se bloquee. El MAC no previene un ataque de inundación SYN porque el ataque de inundación SYN es un ataque de denegación de servicio (DoS) que explota los buffers de un dispositivo que valide las conexiones entrantes.

Un ataque DoS inunda el sistema objetivo con solicitudes no deseadas, causando la pérdida de servicio a los usuarios. El MAC no previene los ataques Dos.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Hash unidireccional

---

Question #55 of 193

Question ID: 1105058

Dada la clave, ¿qué es un algoritmo que calcula las subclaves para cada ronda de cifrado?

- ✗ **A)** agrupación en clústeres de claves
- ✗ **B)** función unidireccional
- ✗ **C)** depósito de garantía de claves
- ✓ **D)** programación clave

explicación

Una programación de claves es un algoritmo que calcula las subclaves para cada ronda de cifrado.

El propósito del depósito de garantía de claves es garantizar que las claves de descifrado pueden ser recuperadas por un tercero.

Una función unidireccional es una función matemática que se utiliza para codificar datos en una dirección.

La agrupación en clústeres de claves es una instancia en la que dos claves diferentes generan el mismo texto cifrado que el texto no cifrado.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Horario clave, http://cryptodox.com/Key_schedule

Question #56 of 193

Question ID: 1105105

¿Qué característica de la instalación puede suponer la amenaza de seguridad más importante de una infraestructura de la instalación?

- ✗ **A)** mantraps
- ✗ **B)** alfombras y aerosoles antiestáticos
- ✗ **C)** pisos suspendidos
- ✓ **D)** techos de caída

explicación

Los techos de caída representan una amenaza significativa para la seguridad de una empresa. Una instalación se puede segregar en varias zonas mediante particiones internas. Si las particiones internas no se extienden por encima del techo, un intruso puede levantar el panel del techo y subir a través de las particiones, obteniendo acceso no autorizado a sistemas y recursos restringidos.

Los pisos suspendidos presentan una amenaza para la seguridad, pero no son la amenaza más importante para la seguridad de una instalación.

Las alfombras y aerosoles antiestáticos se utilizan para evitar la generación de electricidad estática en centros de datos ubicados en áreas secas o en áreas con una alta carga estática.

Las instalaciones con áreas altamente seguras despliegan mantraps para contener a un individuo en un área cerrada si surge la necesidad. El guardia de seguridad verifica las credenciales de una persona.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Centro de datos seguro

Question #57 of 193

Question ID: 1114699

¿Cuál de los siguientes representa problemas de seguridad en la computación en la nube?

a. Acceso de usuarios con privilegios

b. ubicación de los datos

c. Segregación de datos

d. recuperación de datos

- ✗ **A)** opción A
- ✗ **B)** Opción d
- ✗ **C)** Opciones C y D
- ✗ **D)** opción c
- ✓ **E)** todas las opciones
- ✗ **F)** opciones A y B
- ✗ **G)** opción b

explicación

Los siguientes son problemas de seguridad en la computación en la nube:

- Acceso de usuarios con privilegios
- Ubicación de los datos
- Segregación de datos
- Recuperación de datos

Otros problemas de seguridad en la computación en la nube son los siguientes:

- Apoyo a las investigaciones
- Viabilidad a largo plazo
- Cumplimiento de las regulaciones gubernamentales y de la industria

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
evaluar y mitigar las vulnerabilidades de las arquitecturas de seguridad, los diseños y los elementos de la solución

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, sistemas basados en la nube

Gartner: Siete riesgos de seguridad de computación en la nube, http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,0

Question #58 of 193

Question ID: 1104992

¿Qué es OVAL?

- ✗ **A)** Una aplicación que comprueba la red en busca de problemas de seguridad conocidos
- ✗ **B)** Una aplicación diseñada para infectar un sistema informático
- ✗ **C)** Una pieza de hardware que aísla una red de otra
- ✓ **D)** un estándar escrito en XML que proporciona contenido de seguridad abierto y disponible públicamente

explicación

Open Vulnerability and Assessment Language (OVAL) es un estándar escrito en XML que proporciona contenido de seguridad abierto y disponible públicamente. Su propósito es estandarizar la información entre diferentes herramientas de seguridad.

Un virus es una aplicación que está diseñada para infectar un sistema informático.

Un analizador de vulnerabilidades es una aplicación que comprueba la red en busca de problemas de seguridad conocidos.

Un firewall es una pieza de hardware que aísla una red de otra.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
evaluar y mitigar las vulnerabilidades de las arquitecturas de seguridad, los diseños y los elementos de la solución

Referencias:

OVAL, http://oval.mitre.org/

Question #59 of 193

Question ID: 1105119

Recientemente, su organización tenía un nuevo sistema de calefacción y aire acondicionado instalado para sus instalaciones. Ahora, cuando el calor o el aire se encienden, las luces de la instalación se atenúan durante un pequeño período de tiempo. ¿Qué está ocurriendo cuando las luces se atenúan?

- ✗ **A)** un pardo de energía
- ✗ **B)** un apagón eléctrico
- ✗ **C)** una subida de tensión
- ✓ **D)** un hundimiento de potencia

explicación

Cuando las luces se atenúan durante el encendido del sistema de calefacción y aire acondicionado, se está produciendo un hundimiento de energía.

Una subida de tensión es un problema momentánea de energía de alto voltaje. Por lo general, cuando se produce una subida de tensión, las luces en realidad pueden ser más brillantes. Las subidas de tensión pueden dañar los equipos electrónicos, incluidas las computadoras.

Un power brown-out es una degradación prolongada de la potencia.

Un apagón eléctrico es una pérdida prolongada y completa de poder.

Cuando se inicia un sistema de calefacción y aire acondicionado, se produce una corriente de precipitación donde se extrae una gran cantidad de corriente de la fuente de alimentación. Las corrientes de acometidas a menudo causan hundidos de energía.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Tipos de interrupciones

---

Question #60 of 193

Question ID: 1104941

¿Qué principio de seguridad utilizado en el modelo bell-lapadula impide que el nivel de seguridad de los sujetos y objetos se cambie una vez que se han creado?

- ✗ **A)** principio de dominación

✗ **B)** principio estático

✗ **C)** principio de privilegio mínimo

✓ **D)** principio de tranquilidad

explicación

El principio de tranquilidad utilizado en el modelo Bell-LaPadula evita que el nivel de seguridad de los sujetos y objetos se cambie una vez que se han creado. Por esta razón, el modelo Bell-LaPadula se considera de naturaleza muy estática. La propiedad de tranquilidad fuerte indica que los objetos nunca cambian su nivel de seguridad.

El principio estático y el principio de dominación no son principios de seguridad válidos.

El principio de privilegios mínimos garantiza que los usuarios reciban los permisos más restrictivos para ejecutar sus tareas de trabajo.

El modelo de Bell-LaPadula fue uno de los primeros modelos matemáticos de una política de seguridad multinivel utilizada para definir una máquina de estado segura. Aborda el flujo de control de la información, los niveles de seguridad y los modos de acceso. Los permisos de acceso se definen mediante una matriz de control de acceso que define el sistema de clasificación y la clase de sujetos y objetos. El flujo de información se produce cuando un sujeto accede, observa o altera un objeto.

Una limitación del modelo de Bell-LaPadula es que contiene canales encubiertos, que es una vía de comunicación que permite a un proceso transferir información de una manera que infringe el modelo de seguridad del sistema.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobjetiva:
Implementar y gestionar procesos de ingeniería utilizando principios de diseño seguro

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Operaciones de seguridad, Modelo Bell-LaPadula

---

Question #61 of 193

Question ID: 1114700

¿Qué medidas de seguridad debe emplear para proteger los teléfonos celulares propiedad de una organización?

un. Habilite las interfaces inalámbricas.

B. Mantener el control físico.

c. Habilitar la autenticación de usuario.

d. Deshabilite las características innecesarias.

- ✗ **A)** Opción d
- ✗ **B)** opción c
- ✗ **C)** opción A
- ✗ **D)** opción b
- ✓ **E)** opciones b, c y d
- ✗ **F)** opciones a, b y c

explicación

Debe emplear muchas medidas de seguridad para proteger los teléfonos celulares propiedad de una organización. Las salvaguardias incluyen:

- Mantener el control físico.
- Habilite la autenticación de usuario.
- Copia de seguridad de datos.
- Minimice la exposición de los datos y cifre los datos.
- Deshabilite las características innecesarias, incluidas las interfaces inalámbricas.
- Desactive los dispositivos comprometidos.

Cualquier dispositivo de mano debe tener estas medidas de seguridad en su lugar. Los teléfonos celulares, las tarjetas satelitales, las computadoras de mano y las PDA usan tecnología de tarjetas inteligentes, lo que significa que las tarjetas de datos pueden ser robadas.

No debe habilitar las interfaces inalámbricas. Las interfaces inalámbricas solo deben habilitarse cuando necesite utilizarlas y solo durante el tiempo que se necesiten.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Evaluar y mitigar las vulnerabilidades en los sistemas móviles

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Vulnerabilidades en sistemas móviles

Directrices sobre seguridad de teléfonos celulares y PDA (Borrador), http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf

---

Question #62 of 193

Question ID: 1192934

¿Qué es un ejemplo de un ataque de fuerza bruta?

- ✓ **A)** usar un programa para adivinar contraseñas de un archivo SAM
- ✗ **B)** buscar a través de la basura de una empresa
- ✗ **C)** recopilación de paquetes de una conexión de red
- ✗ **D)** enviar varios mensajes ICMP a un servidor Web

explicación

El uso de un programa para adivinar contraseñas de un archivo de administrador de cuentas de seguridad (SAM) es un ejemplo de un ataque de fuerza bruta. Un archivo SAM, que se utiliza en algunas redes de Windows, contiene contraseñas cifradas. Un hacker puede iniciar un ataque de fuerza bruta en un intento de descifrar las contraseñas almacenadas en un archivo SAM. Puede defenderse contra un ataque de red de fuerza bruta aumentando la complejidad y el espacio de claves de la contraseña.

El envío de varios mensajes ICMP (Protocolo de mensajes de control de Internet) a un servidor web es un tipo de ataque de denegación de servicio (DoS) que se conoce como ping de muerte. Buscar en la basura de una empresa para encontrar información confidencial es un tipo de ataque físico que a veces se conoce como buceo en contenedores de basura. El uso de un analizador de paquetes para recopilar paquetes de una conexión de red entre dos equipos es un método que se puede utilizar para iniciar un ataque man in the middle (MITM).

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Fuerza Bruta

---

Question #63 of 193

Question ID: 1105098

Debe almacenar algunos dispositivos de almacenamiento magnético en una instalación de almacenamiento temporal. ¿A qué temperatura podría comenzar a producirse el daño?

- ✗ **A)** 175 grados Fahrenheit
- ✓ **B)** 100 grados Fahrenheit

✗ **C)** 90 grados Fahrenheit

✗ **D)** 350 grados Fahrenheit

explicación

Para los dispositivos de almacenamiento magnético, el daño puede comenzar a ocurrir a 100 grados Fahrenheit. Los disquetes y las cintas son más sensibles a los daños causados por las altas temperaturas que otros equipos informáticos, papel y chapa.

Ninguna de las otras respuestas es correcta. Los daños a los sistemas informáticos y dispositivos periféricos pueden comenzar a ocurrir a 175 grados Fahrenheit. Los daños a los productos de papel pueden comenzar a ocurrir a 350 grados Fahrenheit.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

CISSP Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, HVAC

Question #64 of 193

Question ID: 1105109

¿Qué ubicación sería la más apropiada para el centro de datos de la instalación de procesamiento de información de una empresa?

✗ **A)** la planta superior de la instalación

✓ **B)** el núcleo de la instalación

✗ **C)** la planta baja de la instalación

✗ **D)** el sótano de la instalación

explicación

Los centros de datos deben estar ubicados en el núcleo de las instalaciones de procesamiento de información de la empresa y cerca de los puntos de distribución de cableado para proporcionar protección contra desastres naturales, garantizar un acceso más fácil a los servicios de emergencia y proporcionar la máxima protección de seguridad. Los centros de datos contienen equipos costosos y datos confidenciales relacionados con la empresa. Por lo tanto, la seguridad del centro de datos se planifica durante el diseño y la construcción de las instalaciones.

Los centros de datos no deben estar ubicados en el sótano o en la planta baja para protegerse contra inundaciones y facilitar el acceso a los intrusos.

Los centros de datos no deben estar ubicados en el último piso para protegerse contra los peligros de incendio.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Centro de datos seguro

---

Question #65 of 193

Question ID: 1105030

¿De qué tipo de algoritmo de cifrado es Diffie-Hellman un ejemplo?

- ✗ **A)** asimétrico con autorización
- ✓ **B)** asimétrico con autenticación
- ✗ **C)** simétrica con firma digital
- ✗ **D)** simétrico con autenticación

explicación

Diffie-Hellman es un ejemplo de criptografía asimétrica. Diffie-Hellman permite que dos computadoras reciban una clave simétrica de forma segura sin requerir una relación previa. Diffie-Hellman fue el primer algoritmo de clave pública.

Los algoritmos asimétricos incluyen Diffie-Hellman, RSA, ElGamal, Elliptic Curve Cryptosystem (ECC), LUC y Knapsack.

Los algoritmos simétricos incluyen data encryption standard (DES), triple DES (3DES), advanced encryption standard (AES), international data encryption algorithm (IDEA), blowfish, RC4, RC5 y RC6.

RSA se utiliza como el estándar mundial de facto para las firmas digitales. RSA es un algoritmo de clave pública que proporciona cifrado y autenticación. RSA no se ocupa de logaritmos discretos. La seguridad que proporciona RSA se basa en el uso de grandes números primos para el cifrado y descifrado. Es difícil factorizar números primos grandes. Por lo tanto, es difícil romper el cifrado. RSA puede evitar ataques de tipo "Man in the middle" al proporcionar autenticación antes del intercambio de claves públicas y privadas. La clave se pasa de forma segura a la máquina receptora. Por lo tanto, la criptografía de clave pública se utiliza preferiblemente para proteger los mensajes de fax.

RSA requiere una mayor potencia de procesamiento debido a la factorabilidad de los números, pero proporciona una administración eficiente de claves.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Diffie-Hellman

---

Question #66 of 193

Question ID: 1104972

¿Cuál es la mejor descripción de un sistema abierto?

- ✗ **A)** Un sistema que contiene un único punto de control
- ✓ **B)** un sistema que se basa en estándares y protocolos a partir de especificaciones publicadas
- ✗ **C)** un sistema que no sigue los estándares del sector
- ✗ **D)** Un sistema que contiene varios puntos de control

explicación

Un sistema abierto es un sistema que se basa en estándares y protocolos a partir de especificaciones publicadas. Los sistemas abiertos están sujetos a revisión y evaluación.

Un sistema distribuido es un sistema que contiene varios puntos de control. Los sistemas distribuidos pueden ser difíciles de administrar. En este entorno, los escritorios pueden contener información confidencial que puede estar en riesgo de quedar expuesta, los usuarios generalmente pueden carecer de conciencia de seguridad y puede existir falta de copia de seguridad adecuada.

Un sistema centralizado es un sistema que contiene un único punto de control. Sin embargo, este tipo de sistema también significa que tiene un único punto de error.

Un sistema cerrado es un sistema que no sigue los estándares de la industria.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender las capacidades de seguridad de los sistemas de información (por ejemplo, protección de memoria, Módulo de plataforma segura (TPM), cifrado/descifrado)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, sistemas cerrados frente a sistemas abiertos

---

Question #67 of 193

Question ID: 1105078

En PKI, ¿qué término hace referencia a una clave pública que se puede usar para comprobar el certificado utilizado en una firma digital?

- ✗ **A)** un objetivo
- ✗ **B)** un emisor
- ✗ **C)** un usuario de confianza
- ✓ **D)** un delimitador de confianza

explicación

En una infraestructura de clave pública (PKI), un anclaje de confianza es una clave pública que comprueba el certificado utilizado en una firma digital. PKI es un sistema para compartir claves públicas de forma segura.

Un emisor es una entidad PKI que firma certificados proporcionados por un sujeto. Una entidad PKI que comprueba una cadena de certificados se conoce como usuario de confianza o comprobador. En PKI, un destino es una ruta de acceso a una clave pública.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Firma Digital

---

Question #68 of 193

Question ID: 1113936

¿Qué afirmación es cierta de la criptografía simétrica?

- ✓ **A)** La criptografía simétrica es más rápida que la criptografía asimétrica.
- ✗ **B)** La criptografía simétrica proporciona una mejor seguridad en comparación con la criptografía asimétrica.
- ✗ **C)** La criptografía simétrica no requiere un mecanismo seguro para entregar correctamente las claves.
- ✗ **D)** La criptografía simétrica utiliza claves diferentes para cifrar y descifrar los mensajes.

explicación

La criptografía simétrica es más rápida que la criptografía asimétrica.

La criptografía simétrica utiliza claves simétricas o secretas para cifrar o descifrar mensajes. En criptografía simétrica, la misma clave que cifra los datos se utiliza para descifrar los datos. La criptografía asimétrica implica el uso de diferentes claves para cifrar y descifrar los datos. Estas claves se conocen como claves privadas y públicas, respectivamente.

Las claves simétricas no garantizan la seguridad y escalabilidad de la administración de claves porque se utiliza la misma clave para el cifrado y descifrado. Por lo tanto, la criptografía simétrica requiere un mecanismo seguro para entregar claves entre los hosts que se comunican.

La criptografía simétrica puede ser menos segura que la criptografía asimétrica debido a las mismas claves que se utilizan para el cifrado y descifrado. La distribución segura de la clave secreta es un problema con la criptografía de clave simétrica.

La criptografía simétrica es aproximadamente de 1.000 a 10.000 veces más rápida que la criptografía asimétrica.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, algoritmos simétricos

---

Question #69 of 193

Question ID: 1105014

Ha decidido adjuntar una marca de tiempo digital a un documento que se comparte en la red. ¿Qué ataque previene esto?

- ✗ **A)** un ataque de canal lateral
- ✗ **B)** un ataque de sólo texto cifrado
- ✓ **C)** un ataque de reproducción
- ✗ **D)** un ataque de texto no cifrado conocido

explicación

Las marcas de tiempo digitales resultan útiles para evitar ataques de reproducción. En un ataque de reproducción, el atacante supervisa el flujo de tráfico en una red. El atacante repite o retrasa maliciosamente la transmisión de datos válidos a través de la red. Establecer un valor de tiempo de umbral en cada sistema garantiza que el equipo sólo acepta paquetes dentro de un período de tiempo especificado. Un paquete recibido después de la hora especificada indicará las posibilidades de un ataque de reproducción. Las marcas de tiempo digitales se adjuntan a un documento en la creación del documento.

En un ataque de canal lateral, el atacante obtiene información sobre los algoritmos de cifrado del criptosistema que se implementa en la red. El atacante puede usar información, como el consumo de energía, las radiaciones electromagnéticas y el sonido para entrar en un sistema. El ataque de canal lateral también se puede basar en la medición del tiempo necesario para realizar un cálculo.

Un ataque de solo texto cifrado se centra principalmente en descubrir la clave de cifrado mediante la recopilación de varios mensajes cifrados y, a continuación, intentar deducir un patrón de los mensajes cifrados.

Un ataque de texto no cifrado conocido se centra principalmente en la detección de la clave utilizada para cifrar los mensajes. La clave se puede utilizar para descifrar y leer mensajes. El atacante tiene acceso a varias instancias de texto no cifrado y texto cifrado para varios mensajes.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Replay Attack

#74 de la parte superior del día, http://ittecture.wordpress.com/2008/12/27/tip-of-the-day-74/

Question #70 of 193

Question ID: 1113937

¿Qué factor NO afecta la fuerza relativa de un criptosistema?

- ✗ **A)** el secreto secreto de la clave secreta
- ✗ **B)** el algoritmo de cifrado
- ✗ **C)** la longitud de la clave secreta
- ✓ **D)** el valor de intercambio de claves

explicación

Los valores de intercambio de claves NO afectan a la fuerza relativa de un criptosistema.

La fuerza de un criptosistema, que también se conoce como factor de trabajo, se refiere a los esfuerzos requeridos por un atacante para romper el algoritmo de cifrado o la clave. La fuerza de un sistema criptográfico comercial se ve afectada por los siguientes factores:

- la fuerza del algoritmo utilizado por el estándar de cifrado
- la eficacia con la que se almacenan las claves secretas
- la longitud de la clave utilizada para cifrar y descifrar datos
- los vectores de inicialización
- la potencia de procesamiento computacional disponible del sistema
- El tiempo necesario para romper la clave de cifrado

Cuanto más sensibles sean los datos, más debe ser la fuerza del método de cifrado para resistir los ataques.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Características del criptosistema

---

Question #71 of 193

Question ID: 1105064

Debe determinar si la información de un archivo ha cambiado. ¿Qué debes usar?

- ✓ **A)** una firma digital
- ✗ **B)** un certificado digital
- ✗ **C)** cifrado de clave privada

✗ **D)** cifrado de clave pública

explicación

Las firmas digitales se utilizan para determinar si la información de un archivo ha cambiado. Una firma digital contiene una suma de comprobación cifrada para un archivo. Se envía un archivo firmado digitalmente a un destinatario. El destinatario puede crear una suma de comprobación a partir del archivo recibido, descifrar la suma de comprobación cifrada que la acompaña y comparar las dos sumas de comprobación. Si las sumas de comprobación coinciden, el destinatario sabe que el archivo no se ha cambiado en tránsito.

El cifrado de clave pública y privada se puede utilizar para cifrar un archivo, pero ninguno de estos métodos se puede utilizar para determinar que un archivo no se ha cambiado en tránsito. En la criptografía de clave pública, solo la clave privada puede descifrarse si la clave pública se cifra. Un certificado digital es una clave pública con la identificación que lo acompaña. Un certificado digital permite a un usuario estar razonablemente seguro de la identidad del propietario de una clave pública antes de utilizar la clave pública para cifrar la información que se enviará al propietario.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Firmas Digitales

---

Question #72 of 193

Question ID: 1104969

¿Cuál es la mejor descripción de las direcciones absolutas tal como se utilizan en la arquitectura de memoria?

✗ **A)** la memoria utilizada en búsquedas complejas
✗ **B)** Las direcciones de memoria que no son únicas
✗ **C)** Las direcciones de memoria indizada que utiliza el software
✓ **D)** las direcciones de memoria física que utiliza una CPU

explicación

Las direcciones absolutas en la arquitectura de memoria son las direcciones de memoria física que utiliza una CPU. También se conocen como direcciones explícitas.

Las direcciones relativas son las direcciones de memoria que no son únicas.

La memoria direccionable o asociativa por contenido es la memoria utilizada en búsquedas complejas. Este tipo de memoria busca un valor de datos específico en la memoria.

Las direcciones lógicas son direcciones de memoria indizadas que utiliza el software.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender las capacidades de seguridad de los sistemas de información (por ejemplo, protección de memoria, Módulo de plataforma segura (TPM), cifrado/descifrado)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, direccionamiento absoluto

---

Question #73 of 193

Question ID: 1104942

¿Qué procesos controlan el flujo de información en el modelo de control de acceso basado en celosía (LBAC)?

- ✗ **A)** estrella (*) integridad y axiomas de integridad simple
- ✗ **B)** regla triple de acceso
- ✗ **C)** seguridad simple, propiedad estrella y reglas de propiedad de estrella fuertes
- ✓ **D)** operadores de límite inferior menos alto y mayor

explicación

Los operadores de límite inferior mínimo y límite inferior más grandes controlan el flujo de información en el modelo de control de acceso basado en celosía (LBAC).

La regla triple de acceso se utiliza para controlar el flujo de información en el modelo de Clark-Wilson.

La integridad de la estrella (*) y los axiomas de integridad simple se utilizan para controlar el flujo de información en el modelo de Biba.

Las reglas de seguridad simple, propiedad de estrella y propiedad de estrella segura se utilizan para controlar el flujo de información en el modelo de Bell-LaPadula.

El énfasis principal del modelo LBAC es la confidencialidad. Fue desarrollado principalmente para hacer frente al flujo de información en las computadoras. El acceso se basa en clases de seguridad o etiquetas de seguridad. A cada sujeto se le concede acceso a un objeto o a un contenedor de información. La etiqueta del sujeto contiene la categoría a la que pertenecen los sujetos y los objetos. Los controles se aplican a los objetos para evitar el acceso no

autorizado. Un sujeto con una determinada clase de seguridad puede leer un objeto de una clase de seguridad inferior, pero no puede modificarlo. Un sujeto puede leer y escribir en un objeto que tiene la misma clase de seguridad. Un sujeto no puede tener acceso a un objeto que tiene una clase de seguridad superior.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobjetiva:
Implementar y gestionar procesos de ingeniería utilizando principios de diseño seguro

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Operaciones de seguridad, modelos de celosía multinivel

---

Question #74 of 193

Question ID: 1104938

¿Qué modelo de control de acceso garantiza la integridad mediante la implementación de reglas de supervisión de integridad y reglas de preservación de la integridad?

- ✗ **A)** Modelo de muro chino
- ✓ **B)** Modelo de Clark-Wilson
- ✗ **C)** Modelo Bell-LaPadula
- ✗ **D)** Modelo biba

explicación

El modelo de control de acceso de Clark-Wilson garantiza la integridad mediante la implementación de reglas de supervisión de integridad y reglas de preservación de la integridad. Las reglas de supervisión de integridad se conocen como reglas de certificación y las reglas de conservación de integridad se conocen como reglas de aplicación. Este modelo define un elemento de datos restringido, un procedimiento de comprobación de integridad y un procedimiento de transformación.

Ninguno de los otros modelos garantiza la integridad mediante el uso de este tipo de reglas.

El énfasis principal del modelo de Clark-Wilson es la integridad. Es mejor conocido por su uso en aplicaciones comerciales. El modelo de seguridad de Clark-Wilson proporciona integridad de los datos al evitar modificaciones no autorizadas por parte de usuarios no autorizados y modificaciones incorrectas por parte de usuarios autorizados. El modelo de Clark-Wilson mantiene la consistencia interna y externa. Se centra en la integridad, la separación de tareas, los elementos de datos restringidos, los procedimientos de transformación y las transacciones bien formadas.

La auditoría es necesaria en el modelo de Clark-Wilson. Este modelo debe auditarse y supervisarse para realizar un seguimiento del flujo de información de una transacción determinada.

El modelo de Clark-Wilson utiliza una relación de tres partes sujeto-programa-objeto conocida como triple. Los sujetos del modelo de Clark-Wilson acceden a los datos a través de un programa, que actúa como intermediario entre un sujeto y un objeto. Este proceso también se conoce como un triple de acceso. El sujeto sólo es capaz de acceder a un objeto a través de un programa de aplicación que forma la interfaz entre el sujeto y el objeto.

Los triples aseguran la separación de tareas porque a los sujetos no se les da acceso directo a los objetos. Sólo se puede acceder a los objetos mediante programas. La separación de funciones es vital en el modelo de Clark-Wilson. El modelo de Clark-Wilson impone la separación de tareas para una tarea determinada y garantiza que los sujetos separados realicen subtareas.

El modelo de Clark-Wilson NO aborda la confidencialidad de los datos.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobjetiva:
Implementar y gestionar procesos de ingeniería utilizando principios de diseño seguro

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Operaciones de seguridad, Modelo de integridad de Clark-Wilson

---

Question #75 of 193

Question ID: 1105032

¿Qué afirmación NO es cierta de los modos de operación del algoritmo estándar de cifrado de datos (DES)?

✗ **A)** El modo de encadenamiento de bloques de cifrado (CBC) y de retroalimentación de cifrado (CFB) se utilizan mejor para la autenticación.

✗ **B)** El funcionamiento en modo de libro de códigos electrónico (ECB) es el más adecuado para el cifrado de bases de datos.

✗ **C)** ECB es el modo DES más fácil y rápido que se puede utilizar.

✓ **D)** ECB utiliza repetidamente texto cifrado producido para cifrar un mensaje que consta de bloques.

explicación

Es cipher block chaining (CBC), no electronic code book (ECB), que utiliza repetidamente un algoritmo para cifrar un mensaje que consta de bloques. En CBC, la salida de texto cifrado se procesa como entrada en otro bloque para

evitar revelar un patrón. En ECB, un bloque determinado siempre produce el mismo texto cifrado para una entrada estándar de texto. El texto cifrado producido no se utiliza repetidamente, pero la salida de texto cifrado siempre es estándar.

La operación en modo ECB es la más adecuada para el cifrado de bases de datos y es el modo más fácil y rápido, aunque no el más seguro de usar. ECB es uno de los muchos modos de operación para DES y utiliza un bloque de datos de 64 bits para producir texto cifrado.

El modo CBC, la retroalimentación de salida y la retroalimentación de cifrado (CFB) son otros tres modos de operaciones de DES y se utilizan mejor para fines de autenticación. DESX es una variante de DES desarrollada para prevenir ataques de fuerza bruta. Con DESX, el texto sin formato de entrada es XORed bit a bit con 64 bits de datos de clave adicionales antes del cifrado con DES, y la salida de DES también es XORed bit a bit con otros 64 bits de datos clave.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e Ingeniería de Seguridad, CBC-MAC

Question #76 of 193

Question ID: 1114716

El plan de seguridad contra incendios de su empresa establece que el sistema de calefacción y aire acondicionado debe apagarse en caso de incendio. ¿Cuál de las siguientes NO representa razones para hacer esto?

un. Los sistemas de extinción de incendios no funcionarán si el sistema de calefacción y aire acondicionado está encendido.

B. Los sistemas de detección de incendios no funcionarán si el sistema de calefacción y aire acondicionado está encendido.

c. Se evitará la propagación de humo por todo el edificio.

d. Se evitará que el oxígeno llegue al fuego.

✗ **A)** opción c
✓ **B)** opciones A y B
✗ **C)** Opción d

✗ **D)** opción b

✗ **E)** opción A

✗ **F)** Opciones C y D

explicación

Los sistemas de extinción de incendios y los sistemas de detección de incendios funcionarán con normalidad si el sistema de calefacción y aire acondicionado está encendido. No es necesario que apague el sistema de calefacción y aire acondicionado para asegurarse de que los sistemas de extinción y detección de incendios funcionen.

Cuando apaga el sistema de calefacción y aire acondicionado en caso de incendio, se asegura de que el sistema de calefacción y aire acondicionado no envíe oxígeno para alimentar el fuego.

Cuando apaga el sistema de calefacción y aire acondicionado en caso de incendio, se asegura de que se evite la propagación de humo por todo el edificio.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, extinción de incendios

---

Question #77 of 193

Question ID: 1114703

¿Qué tipos de cifrado requieren que se compartan claves privadas?

a. Cifrado asimétrico

b. Cifrado de clave privada

c. Cifrado de clave pública

d. Cifrado simétrico

✗ **A)** opción A

✗ **B)** Opciones A y C

✗ **C)** opción c

✗ **D)** Opción d

✗ **E)** opción b

✓ **F)** Opciones B y D

explicación

El cifrado simétrico, que a veces se conoce como cifrado de clave privada, requiere que los usuarios compartan una clave privada. En el cifrado de clave privada, se utiliza una clave privada para cifrar un archivo y se utiliza la misma clave privada para descifrar el archivo. Los principales problemas de seguridad con el cifrado de claves privadas son la distribución y proliferación de claves privadas.

El cifrado asimétrico a veces se conoce como cifrado de clave pública. En el cifrado asimétrico, se utiliza una clave pública para cifrar un archivo y se utiliza una clave privada que corresponde a la clave pública para descifrar el archivo. La criptografía de clave pública se utiliza para crear firmas digitales.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, algoritmos simétricos

Cifrado, http://en.wikipedia.org/wiki/Encryption

Question #78 of 193

Question ID: 1105023

¿Qué servicio proporcionado por un criptosistema convierte la información en datos ininteligibles?

✗ **A)** autorización

✗ **B)** norepudiation

✗ **C)** integridad

✓ **D)** confidencialidad

explicación

El servicio proporcionado por un criptosistema que convierte la información en datos ininteligibles es la confidencialidad.

La no denuncia garantiza que el remitente de los datos no puede negar haber enviado los datos. La autorización permite a los usuarios tener acceso a un recurso una vez que se ha demostrado su identidad. La integridad garantiza

que los datos no hayan sido modificados por un usuario no autorizado desde que se crearon, transmitieron o almacenaron los datos.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Confidencialidad

---

Question #79 of 193

Question ID: 1113929

¿Qué tipo de ataque de contraseña se conoce a menudo como un ataque exhaustivo?

- ✗ **A)** ataque de phishing
- ✗ **B)** ataque de diccionario
- ✓ **C)** ataque de fuerza bruta
- ✗ **D)** ataque de suplantación de identidad

explicación

Una fuerza bruta es el ataque de contraseña que a menudo se conoce como un ataque exhaustivo. Un ataque de fuerza bruta es aquel en el que el atacante intenta todas las combinaciones de entrada posibles para obtener acceso a los recursos. Para protegerse contra este tipo de ataque, debe realizar periódicamente su propio ataque de fuerza bruta utilizando un cracker de contraseñas. También debe auditar dicha actividad y emplear un sistema de detección de intrusiones (IDS) para identificar actividades sospechosas. El uso de directivas de contraseñas, como una directiva de bloqueo de cuentas, también ayuda. Con una directiva de bloqueo de cuenta si la misma cuenta intenta iniciar sesión con una contraseña no válida, la cuenta se bloquea y no se puede desbloquear hasta que el usuario válido se ponga en contacto con el administrador del sistema.

Un ataque de diccionario es un método en el que el atacante intenta identificar las credenciales de usuario alimentando listas de palabras o frases de uso común. Debido a que utiliza un diccionario, un adjunto de diccionario no es tan exhaustivo como un ataque de fuerza bruta.

La suplantación de identidad se produce cuando un atacante implementa un programa falso que roba las credenciales de usuario. Esto se implementa mediante un caballo de Troya.

Un ataque de phishing es un ataque de correo electrónico en el que un hacker intenta obtener credenciales de usuario solicitándolas por correo electrónico. El correo electrónico de phishing se asemeja mucho a un correo electrónico oficial.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Fuerza Bruta

---

Question #80 of 193

Question ID: 1192931

Haga clic en cada uno de los encabezados del escenario para expandir o contraer su contenido. Debe leer todo el escenario para responder a la pregunta.

fondo

Usted es un profesional de la seguridad contratado recientemente por una institución financiera que cotiza en bolsa para ayudar a administrar la seguridad de la organización. La oficina principal de la compañía está en Nueva York, NY, y tiene sucursales adicionales en todo Estados Unidos.

Temas actuales

La infraestructura actual incluye servidores Windows, servidores UNIX, clientes Windows, clientes Mac, dispositivos móviles Windows y dispositivos móviles Mac implementados en todas las oficinas. El departamento de TI de la compañía tiene un gran personal ubicado en la oficina de Nueva York. Cada sucursal tiene unos pocos miembros del personal de TI local que solo se encargan de los problemas de esa sucursal.

Ha identificado varias instancias en las que los ataques contra los sistemas cliente no se impidieron ni detectaron en el nivel de cliente porque no se implementó ningún control para evitar el ataque. Los datos fueron robados de algunos dispositivos. Toda una sucursal estaba infectada con malware y virus y requería varios días de tiempo de recuperación, lo que significaba la pérdida de ingresos. Por último, recientemente descubrió que varios sistemas cliente tienen instaladas versiones sin licencia de sistemas operativos. Debe asegurarse de que se implementan los controles adecuados para mitigar estos riesgos.

En una auditoría reciente, descubrió que varios dispositivos móviles carecían de las actualizaciones adecuadas para sus sistemas operativos o aplicaciones. Además, los usuarios habían desactivado las funciones de limpieza remota y localización GPS en estos dispositivos y habían instalado varias aplicaciones no autorizadas. Necesita una solución

para mitigar estos riesgos y controlar la configuración y las aplicaciones de los dispositivos móviles cuando esos dispositivos están conectados a la empresa.

Debido a varios contratos entre su empresa y terceros, debe asegurarse de que ciertos sistemas dentro de su infraestructura logren EAL7 en el modelo de evaluación de criterios comunes.

Recientemente, uno de los servidores de la intranet fue víctima de un ataque de denegación de servicio (DoS). El departamento de TI tardó más de 24 horas en devolver el servidor al estado operativo. Durante ese tiempo, el personal de la oficina principal no pudo acceder a la información importante de recursos humanos almacenada en el servidor afectado.

Se espera que los usuarios utilicen el cifrado simétrico y asimétrico para garantizar la confidencialidad de los datos. Debe implementar un sistema adecuado para administrar las claves de cifrado, los valores hash y los certificados digitales en todos los equipos cliente. También debe proteger las contraseñas, cifrar unidades y administrar los derechos digitales de estos mismos equipos.

La integridad de los datos se ha convertido en una preocupación cada vez más seria para los archivos creados y mantenidos por el departamento de investigación. Debe implementar la solución adecuada para estos archivos. Todos los archivos se encuentran en un único servidor que es accesible sólo por los usuarios en el departamento de investigación.

Nunca se completó formalmente un análisis de riesgos exhaustivo para toda la organización. Se le ha pedido que encabece este proyecto. Como parte de este proceso, debe identificar las amenazas geográficas para cada oficina individual.

Su organización desplegará dos oficinas internacionales a finales de este año. Se le ha invitado a participar en la selección de instalaciones y en el proceso de seguridad interna del edificio para proporcionar información de seguridad concreta.

¿Cuál de las siguientes directivas y controles debe implementar para los sistemas cliente en función de sus riesgos identificados? (Elija todo lo que se aplique).)

- ✓ **A)** Utilice el cifrado de unidad en todas las unidades de disco duro del sistema cliente.
- ✓ **B)** Implemente software antimalware y antivirus en todos los sistemas cliente.
- ✓ **C)** Implemente solo sistemas operativos compatibles con licencia.
- ✓ **D)** Despliegue sistemas de detección de intrusiones basados en firewall y host en los sistemas cliente.

explicación

Debe implementar todas las directivas y controles enumerados para los sistemas cliente en función de sus riesgos identificados. Estos riesgos se identifican en el segundo párrafo del escenario.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
evaluar y mitigar las vulnerabilidades de las arquitecturas de seguridad, los diseños y los elementos de la solución

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, vulnerabilidades de arquitecturas de seguridad, diseños y elementos de solución

---

Question #81 of 193

Question ID: 1105083

Su organización ha implementado una infraestructura de clave pública (PKI). Debe asegurarse de que el explorador de cada usuario comprueba automáticamente el estado del certificado del usuario. ¿Qué deberías implementar?

✗ **A)** Crl
✓ **B)** OCSP
✗ **C)** mimo
✗ **D)** PGP

explicación

El Protocolo de estado de certificados en línea (OCSP) garantiza que el explorador de cada usuario compruebe automáticamente el estado del certificado del usuario.

Una lista de revocación de certificados (CRL) es una lista de todos los certificados que se han revocado.

Multipurpose Internet Mail Extension (MIME) es un estándar que controla cómo se transfieren los datos adjuntos de correo electrónico.

Pretty Good Privacy (PGP) es una aplicación gratuita de seguridad de correo electrónico.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e Ingeniería de Seguridad, OCSP

Question #82 of 193

Question ID: 1113931

¿Qué es un algoritmo de cifrado?

✗ **A)** una clave de cifrado

✓ **B)** una fórmula matemática

✗ **C)** datos antes del cifrado

✗ **D)** datos después del cifrado

explicación

En criptografía, un algoritmo de cifrado es una fórmula matemática utilizada para transformar texto plano en texto cifrado.

El texto sin formato, a veces denominado texto no cifrado, son datos antes del cifrado, y el texto cifrado son datos después del cifrado. Una clave de cifrado son datos que se pueden utilizar con un algoritmo de cifrado para cifrar o descifrar datos.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Matemáticas Criptográficas

Cifrado, http://searchsecurity.techtarget.com/definition/encryption

---

Question #83 of 193

Question ID: 1192936

Haga clic en cada uno de los encabezados del escenario para expandir o contraer su contenido. Debe leer todo el escenario para responder a la pregunta.

fondo

Usted es un profesional de la seguridad contratado recientemente por una institución financiera que cotiza en bolsa para ayudar a administrar la seguridad de la organización. La oficina principal de la compañía está en Nueva York, NY, y tiene sucursales adicionales en todo Estados Unidos.

Temas actuales

La infraestructura actual incluye servidores Windows, servidores UNIX, clientes Windows, clientes Mac, dispositivos móviles Windows y dispositivos móviles Mac implementados en todas las oficinas. El departamento de TI de la compañía tiene un gran personal ubicado en la oficina de Nueva York. Cada sucursal tiene unos pocos miembros del personal de TI local que solo se encargan de los problemas de esa sucursal.

Ha identificado varias instancias en las que los ataques contra los sistemas cliente no se impidieron ni detectaron en el nivel de cliente porque no se implementó ningún control para evitar el ataque. Los datos fueron robados de algunos dispositivos. Toda una sucursal estaba infectada con malware y virus y requería varios días de tiempo de recuperación, lo que significaba la pérdida de ingresos. Por último, recientemente descubrió que varios sistemas cliente tienen instaladas versiones sin licencia de sistemas operativos. Debe asegurarse de que se implementan los controles adecuados para mitigar estos riesgos.

En una auditoría reciente, descubrió que varios dispositivos móviles carecían de las actualizaciones adecuadas para sus sistemas operativos o aplicaciones. Además, los usuarios habían desactivado las funciones de limpieza remota y localización GPS en estos dispositivos y habían instalado varias aplicaciones no autorizadas. Necesita una solución para mitigar estos riesgos y controlar la configuración y las aplicaciones de los dispositivos móviles cuando esos dispositivos están conectados a la empresa.

Debido a varios contratos entre su empresa y terceros, debe asegurarse de que ciertos sistemas dentro de su infraestructura logren EAL7 en el modelo de evaluación de criterios comunes.

Recientemente, uno de los servidores de la intranet fue víctima de un ataque de denegación de servicio (DoS). El departamento de TI tardó más de 24 horas en devolver el servidor al estado operativo. Durante ese tiempo, el personal de la oficina principal no pudo acceder a la información importante de recursos humanos almacenada en el servidor afectado.

Se espera que los usuarios utilicen el cifrado simétrico y asimétrico para garantizar la confidencialidad de los datos. Debe implementar un sistema adecuado para administrar las claves de cifrado, los valores hash y los certificados digitales en todos los equipos cliente. También debe proteger las contraseñas, cifrar unidades y administrar los derechos digitales de estos mismos equipos.

La integridad de los datos se ha convertido en una preocupación cada vez más seria para los archivos creados y mantenidos por el departamento de investigación. Debe implementar la solución adecuada para estos archivos. Todos los archivos se encuentran en un único servidor que es accesible sólo por los usuarios en el departamento de investigación.

Nunca se completó formalmente un análisis de riesgos exhaustivo para toda la organización. Se le ha pedido que encabece este proyecto. Como parte de este proceso, debe identificar las amenazas geográficas para cada oficina individual.

Su organización desplegará dos oficinas internacionales a finales de este año. Se le ha invitado a participar en la selección de instalaciones y en el proceso de seguridad interna del edificio para proporcionar información de seguridad concreta.

¿Qué debe implementar para los archivos del departamento de investigación?

- ✗ **A)** RC6
- ✗ **B)** Diffie-Hellman
- ✓ **C)** SHA-3
- ✗ **D)** 3DES

explicación

Debe implementar SHA-3, un algoritmo hash, para los archivos del departamento de investigación. Garantizará la integridad de los datos.

3DES y RC6 son algoritmos simétricos. Diffie-Hellman es un algoritmo asimétrico. Los algoritmos simétricos y asimétricos no proporcionan integridad de datos.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Integridad de mensajes

---

Question #84 of 193

Question ID: 1104979

Se le ha pedido que se asegure de que los datos en reposo en los equipos de la organización permanecen confidenciales. ¿Qué control de seguridad debe implementar?

- ✗ **A)** cifrado de vínculos
- ✗ **B)** listas de control de acceso
- ✗ **C)** Instantáneas
- ✓ **D)** cifrado de unidades

explicación

Debe implementar el cifrado de unidad para asegurarse de que los datos en reposo en los equipos de la organización permanecen confidenciales.

El cifrado de vínculos garantiza que los datos en tránsito a través de la red estén protegidos. Las líneas de base proporcionan un nivel mínimo de seguridad o rendimiento para un sistema. Las listas de control de acceso (ACL) proporcionan integridad de datos para los datos en reposo y los datos en tránsito, pero no proporcionan confidencialidad.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
evaluar y mitigar las vulnerabilidades de las arquitecturas de seguridad, los diseños y los elementos de la solución

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, basado en el cliente

---

Question #85 of 193

Question ID: 1111718

¿Qué característica de PGP es diferente del uso de certificados de confianza formales?

- ✗ **A)** El uso de dominios de confianza por parte de los servidores y los clientes
- ✗ **B)** el uso de servidores de entidad emisora de certificados
- ✗ **C)** La implementación de claves privadas para la autenticación y el cifrado
- ✓ **D)** el establecimiento de una web de confianza entre los usuarios

explicación

Pretty Good Privacy (PGP) establece una red de confianza entre los usuarios. Una red de confianza implica que los usuarios generen y distribuyan sus claves públicas. Estas claves están firmadas por los usuarios entre sí, estableciendo una comunidad de usuarios que confían entre sí para la comunicación. Cada usuario tiene una colección de claves públicas firmadas almacenadas en un archivo conocido como conjunto de claves. Un nivel de confianza y validez están asociados a cada clave de esa lista. Por ejemplo, si A confía en B más que C, habrá un mayor nivel de confianza para B en comparación con C.

PGP es un estándar de cifrado de clave pública que se utiliza para proteger los correos electrónicos y los archivos que se transmiten a través de la red. PGP cifra los datos mediante un método de cifrado simétrico. PGP proporciona las siguientes funcionalidades:

- confidencialidad a través del Algoritmo Internacional de Cifrado de Datos (IDEA)
- integridad a través del algoritmo hash message digest 5 (MD5)
- autenticación a través de certificados de clave pública
- no enviar a través de mensajes firmados cifrados

PGP no utiliza servidores de entidad de certificación (CA) ni certificados de confianza formal. Los usuarios confían entre sí en lugar de confiar sólo en el servidor de CA antes de iniciar la comunicación.

El inconveniente de PGP es que, a diferencia del servidor de CA centralizado, es difícil lograr una funcionalidad estandarizada utilizando PGP. Después de la pérdida de una clave privada por parte de un usuario, el usuario debe informar a todos los demás usuarios en la web del usuario de confianza para evitar la comunicación no autorizada.

PGP implementa una red de confianza y no utiliza dominios de confianza entre los servidores y los clientes.

PGP no utiliza claves privadas para la autenticación y el cifrado, pero utiliza claves públicas y privadas para implementar la criptografía de clave pública para la autenticación y el cifrado.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, PGP

Question #86 of 193

Question ID: 1105072

¿Qué tarea realiza un sistema de revocación de claves?

- ✗ **A)** generación de claves
- ✓ **B)** invalidación de claves
- ✗ **C)** protección de clave privada
- ✗ **D)** validación de claves

explicación

Los sistemas de revocación de claves están diseñados para invalidar claves.

Las claves las generan los sistemas de generación de claves. El estándar de cifrado de datos (DES), por ejemplo, proporciona un sistema de generación de claves que produce claves de cifrado de 56 bits. Un receptor de una clave puede certificar la identidad del remitente de la clave mediante un sistema de certificación de claves. Los sistemas de cifrado suelen proporcionar protección con contraseña para proteger las claves privadas.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 3: Arquitectura e ingeniería de seguridad, Revocación

---

Question #87 of 193

Question ID: 1104954

¿A qué se refiere iso 15408?

- ✗ **A)** Itsec
- ✓ **B)** Criterios comunes
- ✗ **C)** TCSEC
- ✗ **D)** directiva de seguridad

explicación

ISO/IEC 15408 hace referencia a los criterios comunes (CC) que se utilizan para evaluar las propiedades de seguridad de los productos y sistemas de tecnología de la información (TI), como sistemas operativos, aplicaciones y otro hardware, firmware y software.

Los criterios de evaluación de seguridad de la tecnología de la información (ITSEC) evalúan los atributos de funcionalidad y garantía por separado. Este método de evaluación y calificación del sistema utilizado en Europa es diferente de los Criterios de evaluación de sistemas informáticos de confianza (TCSEC) en los que la funcionalidad y la garantía de un sistema se agrupan con fines de evaluación.

El Departamento de Defensa de los Estados Unidos (DoD, por sus, por sus, sus) desarrolló criterios de evaluación de sistemas informáticos de confianza (TCSEC, por sus, por sus) para evaluar y calificar la eficacia, la seguridad, la fiabilidad y la funcionalidad de los sistemas operativos, las aplicaciones y los productos de seguridad. Los criterios de evaluación se publicaron en un libro conocido como el Libro Naranja.

Una directiva de seguridad hace referencia a un grupo de reglas que definen el proceso de protección y administración de información confidencial. Una política de seguridad define los mecanismos de seguridad que se deben implementar para lograr el objetivo de seguridad.

Common Criteria es un estándar mundialmente reconocido y aceptado para la evaluación de productos de infraestructura. Este criterio de evaluación reduce la complejidad de las calificaciones y garantiza que los proveedores

fabriquen productos para los mercados internacionales. Por lo tanto, los criterios comunes abordan la funcionalidad en términos de lo que hace un producto y aseguran que el producto funcionará de manera predecible y consistente.

Los criterios comunes asignan un nivel de garantía de evaluación. A diferencia del Libro Naranja, que asigna una calificación a un producto en función de cómo se relacionan los productos con el modelo Bell-LaPadula, los Criterios Comunes asignan una calificación basada en un perfil de protección.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender los conceptos fundamentales de los modelos de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Operaciones de seguridad, criterios comunes

---

Question #88 of 193

Question ID: 1114709

Una nueva directiva de seguridad implementada por su organización establece que todos los mensajes de correo electrónico oficiales deben estar firmados con firmas digitales. ¿Qué elementos se proporcionan cuando se utilizan?

a. integridad

b. disponibilidad

c. cifrado

d. autenticación

e. No repudio

- ✗ **A)** opción c
- ✗ **B)** opciones c, d y e
- ✗ **C)** Opción d
- ✗ **D)** opción b
- ✓ **E)** opciones a, d y e
- ✗ **F)** opción A
- ✗ **G)** opción e
- ✗ **H)** opciones a, b y c

explicación

Una firma digital es un valor hash que se cifra con la clave privada del remitente. El mensaje está firmado digitalmente. Por lo tanto, proporciona autenticación, no repudio e integridad en el correo electrónico. En una transmisión de mensajes firmada digitalmente mediante una función hash, la síntesis del mensaje se cifra en la clave privada del remitente.

Las firmas digitales no proporcionan cifrado y no pueden garantizar la disponibilidad.

El estándar de firma digital (DSS) define las firmas digitales. Proporciona integridad y autenticación. No es un algoritmo de clave simétrica.

Una firma digital no se puede suplantar. Por lo tanto, los ataques, como los ataques de tipo "Man in the middle", no pueden dañar la integridad del mensaje.

Microsoft utiliza la firma digital para garantizar la integridad de los archivos de controlador.

Una forma de firma digital en la que el firmante no está al tanto del contenido del mensaje se denomina firma ciega.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Firmas Digitales

---

Question #89 of 193

Question ID: 1114691

¿Cuáles de las siguientes entidades NO son sujetos?

a. usuario

b. proceso

c. archivo

d. grupo

e. directorio

f. Equipo

- ✗ **A)** Opción d
- ✗ **B)** opción c

✗ **C)** todas las opciones

✗ **D)** opción f

✗ **E)** opción b

✗ **F)** opción A

✗ **G)** opción e

✓ **H)** opciones c, e y f solamente

✗ **I)** opciones a, b y d solamente

explicación

Un archivo, un directorio y un equipo NO son sujetos. Estas entidades son objetos. Un objeto es una entidad que contiene información. A los sujetos se les concede o deniega el acceso a los objetos.

Un usuario, un proceso y un grupo son sujetos. Los sujetos solicitan activamente acceso a los objetos. Todo lo que solicita acceso a un objeto es un asunto. Un programa puede ser un sujeto o un objeto, dependiendo de su uso actual. Un proceso es una instancia determinada de una aplicación que se está ejecutando. Un grupo de procesos que comparten el acceso a los mismos recursos se denomina dominio de protección.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender los conceptos fundamentales de los modelos de seguridad

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Objetos y Sujetos

---

Question #90 of 193

Question ID: 1192933

Haga clic en cada uno de los encabezados del escenario para expandir o contraer su contenido. Debe leer todo el escenario para responder a la pregunta.

fondo

Usted es un profesional de la seguridad contratado recientemente por una institución financiera que cotiza en bolsa para ayudar a administrar la seguridad de la organización. La oficina principal de la compañía está en Nueva York, NY, y tiene sucursales adicionales en todo Estados Unidos.

Temas actuales

La infraestructura actual incluye servidores Windows, servidores UNIX, clientes Windows, clientes Mac, dispositivos móviles Windows y dispositivos móviles Mac implementados en todas las oficinas. El departamento de TI de la compañía tiene un gran personal ubicado en la oficina de Nueva York. Cada sucursal tiene unos pocos miembros del personal de TI local que solo se encargan de los problemas de esa sucursal.

Ha identificado varias instancias en las que los ataques contra los sistemas cliente no se impidieron ni detectaron en el nivel de cliente porque no se implementó ningún control para evitar el ataque. Los datos fueron robados de algunos dispositivos. Toda una sucursal estaba infectada con malware y virus y requería varios días de tiempo de recuperación, lo que significaba la pérdida de ingresos. Por último, recientemente descubrió que varios sistemas cliente tienen instaladas versiones sin licencia de sistemas operativos. Debe asegurarse de que se implementan los controles adecuados para mitigar estos riesgos.

En una auditoría reciente, descubrió que varios dispositivos móviles carecían de las actualizaciones adecuadas para sus sistemas operativos o aplicaciones. Además, los usuarios habían desactivado las funciones de limpieza remota y localización GPS en estos dispositivos y habían instalado varias aplicaciones no autorizadas. Necesita una solución para mitigar estos riesgos y controlar la configuración y las aplicaciones de los dispositivos móviles cuando esos dispositivos están conectados a la empresa.

Debido a varios contratos entre su empresa y terceros, debe asegurarse de que ciertos sistemas dentro de su infraestructura logren EAL7 en el modelo de evaluación de criterios comunes.

Recientemente, uno de los servidores de la intranet fue víctima de un ataque de denegación de servicio (DoS). El departamento de TI tardó más de 24 horas en devolver el servidor al estado operativo. Durante ese tiempo, el personal de la oficina principal no pudo acceder a la información importante de recursos humanos almacenada en el servidor afectado.

Se espera que los usuarios utilicen el cifrado simétrico y asimétrico para garantizar la confidencialidad de los datos. Debe implementar un sistema adecuado para administrar las claves de cifrado, los valores hash y los certificados digitales en todos los equipos cliente. También debe proteger las contraseñas, cifrar unidades y administrar los derechos digitales de estos mismos equipos.

La integridad de los datos se ha convertido en una preocupación cada vez más seria para los archivos creados y mantenidos por el departamento de investigación. Debe implementar la solución adecuada para estos archivos. Todos los archivos se encuentran en un único servidor que es accesible sólo por los usuarios en el departamento de investigación.

Nunca se completó formalmente un análisis de riesgos exhaustivo para toda la organización. Se le ha pedido que encabece este proyecto. Como parte de este proceso, debe identificar las amenazas geográficas para cada oficina individual.

Su organización desplegará dos oficinas internacionales a finales de este año. Se le ha invitado a participar en la selección de instalaciones y en el proceso de seguridad interna del edificio para proporcionar información de seguridad concreta.

Se le ha pedido que identifique cualquier amenaza natural que pueda afectar a todas y cada una de las oficinas en los Estados Unidos. ¿Cuál de los siguientes debe incluir?

- ✗ **A)** interrupciones eléctricas, de comunicaciones y de servicios públicos
- ✗ **B)** huelgas, disturbios y actos terroristas
- ✗ **C)** explosiones, vandalismo y fraude
- ✓ **D)** tornados, inundaciones y terremotos

explicación

Las amenazas naturales incluyen huracanes/tormentas tropicales, tornados, terremotos e inundaciones.

Las amenazas del sistema incluyen interrupciones eléctricas, de comunicaciones y de servicios públicos. Las amenazas causadas por el ser humano incluyen explosiones, incendios, vandalismo, fraude, robo y colusión. Las amenazas por motivos políticos incluyen huelgas, disturbios, desobediencia civil, actos terroristas y atentados con bombas.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Evaluar y mitigar las vulnerabilidades en dispositivos integrados

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 1: Seguridad y Gestión de Riesgos, Amenazas Geográficas

---

Question #91 of 193

Question ID: 1192924

¿Qué modelo de control de acceso utiliza la regla de seguridad simple, la regla de propiedad de estrella y la regla de propiedad de estrella fuerte?

- ✗ **A)** Modelo biba
- ✓ **B)** Modelo Bell-LaPadula
- ✗ **C)** Modelo de Clark-Wilson
- ✗ **D)** Modelo de muro chino

explicación

El modelo bell-lapadula utiliza la regla de seguridad simple, la regla de propiedad de estrella y la regla de propiedad de estrella fuerte. La regla de seguridad simple, a veces denominada "sin lectura", garantiza que los sujetos de un determinado nivel de seguridad no puedan leer objetos de un nivel de seguridad superior. La regla de propiedad star (*), a veces denominada "no write down" o propiedad de confinamiento, garantiza que los sujetos en un determinado nivel de seguridad no puedan escribir objetos en un nivel de seguridad inferior. La regla de propiedad de estrella segura garantiza que un sujeto solo puede realizar funciones de lectura y escritura solo en objetos en el mismo nivel de seguridad. Bell-LaPadula solo se ocupa de la confidencialidad.

Ninguno de los otros modelos de control de acceso utiliza estas tres reglas de propiedad.

La principal preocupación del modelo Bell-LaPadula es la confidencialidad. Es un modelo de máquina de estado que captura los aspectos de confidencialidad del control de acceso. Las directivas de seguridad de este modelo impiden que los objetos fluyan a otros niveles de seguridad.

El modelo Bell-LaPadula permite que un sujeto de confianza infrinja la propiedad *, pero cumpla con la intención de la propiedad *. Por lo tanto, una persona que es un sujeto de confianza podría mover datos no clasificados de un documento clasificado a un documento sin clasificar sin infringir la intención de la propiedad *. Otro ejemplo sería que un sujeto de confianza degradaría la clasificación del material cuando se haya determinado que la degradación no dañaría la seguridad nacional u organizativa y no violaría la intención de la propiedad *.

El modelo Bell-LaPadula permite las siguientes acciones:

- Sujetos a leer desde un nivel inferior de seguridad en relación con su nivel de seguridad
- Sujetos a escribir a un nivel más alto de seguridad en relación con su nivel de seguridad
- Temas a leer en su mismo nivel de seguridad

En la parte discrecional del modo Bell-LaPadula que se basa en la matriz de acceso, la forma en que se definen y evalúan los derechos de acceso se denomina autorización.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobjetiva:
Implementar y gestionar procesos de ingeniería utilizando principios de diseño seguro

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Operaciones de seguridad, Modelo Bell-LaPadula

---

Question #92 of 193

Question ID: 1105101

Como parte del plan de seguridad de su organización, los guardias de seguridad están estacionados en cada entrada de acceso público a la instalación. En el contexto de la seguridad física, ¿qué declaración sobre el personal de los

guardias de seguridad es la más apropiada?

- ✗ **A)** El personal de guardia de seguridad es uno de los controles administrativos en una arquitectura de seguridad en capas.
- ✗ **B)** El personal de la guardia de seguridad actúa como la última línea de defensa en la seguridad de la infraestructura de la instalación.
- ✗ **C)** El personal de guardia de seguridad es una contramedida rentable para reducir el riesgo de seguridad física.
- ✓ **D)** El personal de guardia de seguridad es la contramedida más costosa para reducir el riesgo de seguridad física.

explicación

El personal de guardia de seguridad es la contramedida más costosa utilizada para reducir los riesgos de seguridad física. El costo de contratarlos, capacitarlos y mantenerlos puede superar fácilmente los beneficios. Cuando se utilizan guardias de seguridad, las compañías a menudo dirigen la luz hacia los puntos de entrada y lejos de un puesto de la fuerza de seguridad para proporcionar protección contra el resplandor.

El personal del protector de seguridad, conjuntamente con otros controles de seguridad físicos y controles técnicos tales como cercas, puertas, iluminación, perros, CCTVs, alarmas, y sistemas de la detección de la intrusión, actúa como la primera línea de defensa en mantener la seguridad de una infraestructura de la facilidad.

La última línea de defensa en una arquitectura de seguridad en capas es la fuerza de trabajo restante de la empresa, excluyendo a los guardias de seguridad.

El personal es un ejemplo de controles de seguridad física y no de controles administrativos. Las categorías de controles que deben componer cualquier programa de seguridad física son disuasión, retraso, detección, evaluación y respuesta. Las alarmas son controles de disuasión. Los bloqueos, las medidas de defensa en profundidad y los controles de acceso están retrasando los controles. Los sistemas de detección de intrusiones (IDS) son controles de detección. Los registros de auditoría son controles de evaluación.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Patrol Force

---

Question #93 of 193

Question ID: 1105084

Al desarrollar el sitio web de su organización, el desarrollador web debe asegurarse de que determinados mensajes se transmiten de forma segura. ¿Qué tecnología sería la mejor opción para este propósito?

- ✓ **A)** S-HTTP
- ✗ **B)** HTTP
- ✗ **C)** poner
- ✗ **D)** HTTPS (en)

explicación

HTTP seguro (S-HTTP) sería la mejor opción para asegurarse de que ciertos mensajes desde el servidor Web se transmiten de forma segura.

El Protocolo de transferencia de hipertexto (HTTP) es la tecnología que transmite mensajes desde Internet. No proporciona ninguna seguridad.

HTTP Seguro (HTTPS) es HTTP que se ejecuta a través de Capa de sockets seguros (SSL). Se utiliza para proteger partes enteras de un sitio Web. Mientras que HTTPS protegerá secciones enteras de un sitio Web, S-HTTP protege sólo ciertos mensajes.

Secure Electronic Transaction (SET) es una tecnología de seguridad que asegura las transacciones con tarjeta de crédito.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, HTTP, HTTPS y S-HTTP

Question #94 of 193

Question ID: 1105094

Su organización ha decidido construir una nueva instalación. Durante la fase de diseño, se le pide que considere la combustibilidad de los materiales de construcción. ¿Qué elementos NO debe considerar para este problema?

- ✗ **A)** techos
- ✗ **B)** puertas

✗ **C)** paredes

✓ **D)** Windows

explicación

Windows no tiene ninguna consideración con respecto a la combustibilidad del material. Los principales problemas con las ventanas son los requisitos de translucidez, la inastillación, las alarmas, la colocación y la accesibilidad a los intrusos.

Las paredes, puertas y techos deben considerarse en lo que respecta a la combustibilidad de sus materiales, incluida la madera, el acero y el hormigón.

Los principales problemas con las paredes son la combustibilidad del material, la calificación de incendios y el refuerzo para áreas seguras.

Los principales problemas con las puertas son la combustibilidad del material, la calificación contra incendios, la resistencia a la entrada forzada, las marcas de emergencia, la colocación, las entradas cerradas o controladas, las alarmas, las bisagras aseguradas, las cerraduras eléctricas de las puertas y el tipo de vidrio.

Los principales problemas con los techos son la combustibilidad del material, la calificación contra incendios, la clasificación de soporte de peso y las consideraciones de techo de caída.

Además, debe considerar la calefacción, la ventilación y el aire acondicionado, las fuentes de energía eléctrica, las líneas de agua y gas, y la detección y supresión de incendios.

Los principales problemas con la calefacción, la ventilación y el aire acondicionado incluyen presión de aire positiva, respiraderos de admisión protegidos, líneas eléctricas dedicadas, cierre de emergencia y colocación.

Los principales problemas con las fuentes de alimentación eléctrica incluyen fuentes de alimentación alternativas y de respaldo, fuente limpia y estable, alimentadores dedicados a las áreas requeridas y colocación y acceso a paneles de distribución y disyuntores.

Los principales problemas con las líneas de agua y gas incluyen válvulas de cierre, flujo positivo y colocación.

Los principales problemas con la detección y supresión de incendios incluyen la colocación de sensores y detectores, la colocación del sistema de supresión, los tipos de detectores y los tipos de agentes de supresión.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar principios de seguridad al diseño de sitios e instalaciones

Referencias:

CISSP Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Entradas de Vidrio

Question #95 of 193

Question ID: 1105075

¿Qué contiene una CRL X.509?

✗ **A)** claves privadas

✓ **B)** números de serie

✗ **C)** certificados digitales

✗ **D)** claves públicas

explicación

Una lista de revocación de certificados (CRL) X.509 contiene una lista de números de serie de certificados digitales sin expirar o revocados que deben considerarse no válidos. Las CRL las crean las entidades de certificación (CA).

Las claves públicas y privadas se utilizan en el cifrado, que se puede utilizar para proteger la confidencialidad del contenido del archivo. Un certificado digital es un documento electrónico que contiene credenciales de autenticación. Aunque una CRL contiene información acerca de los certificados digitales, una CRL no contiene certificados digitales.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Lista de revocación de certificados (CRL)

Question #96 of 193

Question ID: 1113943

Su organización protege su centro de datos mediante un bloqueo inteligente. Cada usuario tiene un código único para introducir en el candado inteligente para acceder al centro de datos. El código está configurado para permitir solo el acceso durante ciertas horas y días. ¿Qué tipo de bloqueo se implementa?

✗ **A)** cerradura de combinación

✓ **B)** bloqueo de cifrado

✗ **C)** cerradura del vaso

✗ **D)** bloqueo mecánico

explicación

Un bloqueo inteligente es un tipo de bloqueo de cifrado. Los bloqueos de cifrado son programables y utilizan teclados para controlar el acceso. Se debe introducir una combinación específica. El bloqueo inteligente le permite programar un código único para cada usuario. A continuación, el código se puede programar para permitir o denegar la conexión en función del día y la hora. Si una cerradura de cifrado tiene una opción de retraso de puerta, la alarma se activa después de que una puerta esté abierta durante un período específico.

Los dos tipos principales de cerraduras mecánicas son cerraduras de la salada y cerraduras del vaso.

Las cerraduras con warded son candados básicos. La cerradura tiene salas (proyecciones de metal alrededor del ojo de la cerradura), y sólo una llave en particular trabajará con las salas para desbloquear la cerradura.

Una cerradura de vaso tiene más piezas que una cerradura de caja. La llave cabe en el cilindro, elevando las piezas de la cerradura a la altura correcta. Hay tres tipos de cerraduras de vaso: cerraduras de vaso de pasador, cerraduras de vaso de oblea y cerraduras de vaso de palanca.

Los bloqueos combinados requieren la combinación correcta de números para desbloquear.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Tipos de cerraduras de puertas

---

Question #97 of 193

Question ID: 1113934

Su organización está trabajando con un socio internacional en un producto nuevo e innovador. Toda la comunicación relacionada con esto debe cifrarse mediante un algoritmo simétrico de dominio público. ¿Qué algoritmo debe utilizar?

✗ **A)** DES

✗ **B)** idea

✗ **C)** 3DES

✓ **D)** pez globo

explicación

Usted debe utilizar Blowfish. Blowfish es un algoritmo simétrico que se considera de dominio público. Puede ser utilizado libremente por cualquier persona.

El Estándar de cifrado digital (DES), el Triple DES (3DES) y el Algoritmo internacional de cifrado de datos (IDEA) no se consideran de dominio público.

Los algoritmos simétricos incluyen DES, 3DES, IDEA, Blowfish, Twofish, RC4, RC5, RC6, Advanced Encryption Standard (AES), SAFER y Serpent. Los algoritmos asimétricos incluyen Diffie-Hellman, RSA, ElGamal, Elliptic Curve Cryptosystem (ECC), LUC, Knapsack y Zero Knowledge Proof.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Blowfish

---

Question #98 of 193

Question ID: 1114712

¿Cuál es el primer paso en el diseño de un programa de seguridad física eficaz?

- ✗ **A)** Determinar las líneas de base de rendimiento a partir de niveles de riesgo aceptables.
- ✗ **B)** Realizar el análisis de riesgos de seguridad física.
- ✓ **C)** Identifique al equipo del programa de seguridad física.
- ✗ **D)** Defina un nivel de riesgo aceptable para cada amenaza de seguridad física.

explicación

Al diseñar un programa de seguridad física eficaz, el primer paso es identificar al equipo del programa de seguridad física.

Los pasos para diseñar un programa de seguridad física eficaz son los siguientes:

- Identifique al equipo del programa de seguridad física.
- Realizar el análisis de riesgos de seguridad física.
- Defina un nivel de riesgo aceptable para cada amenaza de seguridad.
- Determinar las líneas de base de rendimiento a partir de niveles de riesgo aceptables.
- Crear métricas de rendimiento de contramedidas.

A partir de los resultados del análisis, describa el nivel de protección y rendimiento requerido para las categorías de programas de disuasión, retraso, detección, evaluación y respuesta.

Identificar e implementar contramedidas para cada categoría de programa.

Evaluar las contramedidas periódicamente para asegurarse de que no se supera el nivel de riesgo aceptable.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Plan de Seguridad Física

---

Question #99 of 193

Question ID: 1104956

¿Qué libro de la serie Rainbow cubre los problemas de seguridad de las redes y los componentes de la red?

- ✓ **A)** el Libro Rojo
- ✗ **B)** el Libro Negro
- ✗ **C)** el Libro Naranja
- ✗ **D)** el Libro Verde

explicación

La evaluación de la seguridad de las redes, sus componentes y bases de datos se incluye en el Libro Rojo. El Libro Rojo asegura las diferentes redes proporcionando el marco para la seguridad. Aborda la interpretación de red de confianza (TNI).

El Libro Naranja se centra principalmente en la seguridad del sistema operativo. Los criterios de evaluación de los Criterios de Evaluación de Sistemas Informáticos confiables (TCSEC, por sus, por sus contramanos) desarrollados por el Departamento de Defensa de los Estados Unidos (DoD, por sus contramanos) se publican en el Libro Naranja. Estos criterios se utilizan para evaluar la garantía y la funcionalidad de un sistema. El énfasis del Libro Naranja está en controlar a los usuarios que pueden acceder al sistema. El Libro Naranja define las políticas de seguridad pertenecientes a las diferentes aplicaciones. Los usuarios y las aplicaciones pueden realizar las operaciones en función de estas directivas. El Libro Naranja incluye recomendaciones de reutilización de objetos que indican que un disco debe formateado siete veces para cumplir con los requisitos del Libro Naranja.

El Libro Verde proporciona directrices para la administración de contraseñas.

No existe tal entidad en seguridad como el Libro Negro.

El libro Forest Green define el manejo seguro de los medios de almacenamiento.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender los conceptos fundamentales de los modelos de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Operaciones de seguridad. Libro Verde

---

Question #100 of 193

Question ID: 1113940

Recientemente, la administración se ha preocupado de que RFI esté causando problemas en las instalaciones de su organización. ¿Qué puede causar este tipo de interferencia?

✗ **A)** motores eléctricos
✗ **B)** cableado eléctrico
✓ **C)** iluminación fluorescente
✗ **D)** relámpago

explicación

La iluminación fluorescente puede causar interferencias de radiofrecuencia (RFI).

Los rayos, los motores eléctricos y el cableado eléctrico pueden causar interferencias electromagnéticas (EMI).

EMI y RFI son términos utilizados para describir la interrupción o el ruido generado por las ondas electromagnéticas. RFI se refiere al ruido generado por las ondas de radio, y EMI es el término general para todas las interferencias electromagnéticas, incluidas las ondas de radio. EMI puede contener RFI. EMI y RFI a menudo se generan naturalmente, por ejemplo, manchas solares o el campo magnético de la Tierra. Las fuentes artificiales de EMI y RFI representan la mayor amenaza para los equipos electrónicos de fuentes como teléfonos celulares, computadoras portátiles y otras computadoras. Se deben adoptar directrices para prevenir la interferencia de EMI y RFI en la sala de computadoras, como limitar el uso y la colocación de imanes o teléfonos celulares alrededor de equipos sensibles. El gobierno de los Estados Unidos creó el estándar TEMPEST para evitar las escuchas de EMI mediante el empleo de blindaje de metales pesados.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Tipos de interrupciones

---

Question #101 of 193

Question ID: 1105031

Recientemente ha implementado una infraestructura de clave pública en una red de Windows Server 2008. Los certificados digitales se emitirán a todos los usuarios y equipos válidos. ¿Qué afirmación NO es cierta de los certificados digitales?

✗ **A)** La garantía de nivel 1 para un certificado digital solo requiere una dirección de correo electrónico.

✗ **B)** X.509 es un estándar de certificado digital.

✗ **C)** Los certificados digitales proporcionan autenticación antes de enviar información de forma segura a un servidor web.

✓ **D)** La garantía de nivel 2 para un certificado digital solo comprueba el nombre y la dirección de correo electrónico de un usuario.

explicación

El nivel 2 verifica el nombre, la dirección, el número de seguro social y otra información de un usuario en una base de datos de la oficina de crédito.

X.509 es un estándar de certificado digital. X.509 define la manera en que una entidad de certificación crea un certificado digital. X.509 define los distintos campos, como los nombres distintivos del sujeto, el número de serie, el número de versión, las fechas de duración y el identificador de firma digital, así como la firma de la autoridad emisora, presente en los certificados digitales. Hay varias versiones de X.509 desde su creación. La versión actual es X.509v4. El estándar X.509 se utiliza en muchos protocolos de seguridad, como el protocolo de capa de sockets seguros (SSL).

La garantía de nivel 1 para un certificado digital solo requiere una dirección de correo electrónico.

La certificación digital proporciona autenticación antes de enviar información de forma segura a un servidor web.

Los certificados actúan como medidas de seguridad para las transacciones de Internet en las que un usuario realiza una transacción en línea con un servidor web mediante la prestación de servicios, como la no denuncia, la autenticación y el cifrado y descifrado de datos.

Cuando se crea un certificado, la clave pública del usuario y el período de validez se combinan con el emisor del certificado y el identificador del algoritmo de firma digital antes de calcular la firma digital.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Certificados

---

Question #102 of 193

Question ID: 1113923

¿Qué afirmación es cierta para los equipos de conjuntos de instrucciones complejos (CISC)?

- ✓ **A)** Las llamadas de acceso a la memoria principal son menos en comparación con RISC.
- ✗ **B)** El programador debe llamar explícitamente a las funciones de carga y almacenamiento.
- ✗ **C)** Un conjunto de instrucciones ejecuta una única operación de bajo nivel.
- ✗ **D)** El conjunto de instrucciones es compatible con todos los lenguajes de programación de bajo nivel.

explicación

Las llamadas de acceso a la memoria principal en CISC son menos que el equipo de conjunto de instrucciones reducido (RISC).

Cada instrucción en CISC ejecuta varias operaciones de bajo nivel, como una operación aritmética, una carga de memoria o un almacén de memoria. Los conjuntos de instrucciones son complejos, lo que en efecto reduce el tamaño del programa. Las llamadas de acceso a la memoria también son menores que RISC porque un único conjunto de instrucciones ejecuta varias operaciones. Por lo tanto, tamaños de programa pequeños y menos llamadas de acceso a la memoria principal se atribuyen al tamaño compacto de la arquitectura de conjunto de instrucciones de microprocesador (ISA) en CISC. Los complejos conjuntos de instrucciones en CISC contribuyen a un efecto adverso en el rendimiento del procesador. La sobrecarga de descodificar las instrucciones también aumenta con la complejidad del conjunto de instrucciones.

CISC no es compatible con todos los lenguajes de programación de bajo nivel.

El programador en CISC no está obligado a llamar explícitamente a las funciones de carga y almacenamiento porque las instrucciones funcionan directamente en la memoria del procesador. Motorola 68000 y CDC 6600 son ejemplos de procesadores CISC.

Cuando los microordenadores se desarrollaron por primera vez, el tiempo de obtención de instrucciones era mucho más largo que el tiempo de ejecución de la instrucción debido a la velocidad relativamente lenta de los accesos a la memoria. Esta situación llevó al diseño de CISC.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender las capacidades de seguridad de los sistemas de información (por ejemplo, protección de memoria, Módulo de plataforma segura (TPM), cifrado/descifrado)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, CPU

Computación compleja del conjunto de instrucciones, http://whatis.techtarget.com/definition/CISC-complex-instruction-set-computer-or-computing

---

Question #103 of 193

Question ID: 1105054

¿Qué es la agrupación en clústeres de claves?

- ✗ **A)** el acto de transformar los datos en un formato legible
- ✗ **B)** la práctica de romper los sistemas criptográficos
- ✓ **C)** Cuando dos claves diferentes cifran un mensaje de texto no cifrado en el mismo texto cifrado
- ✗ **D)** el tiempo, el esfuerzo y los recursos estimados necesarios para romper un sistema criptográfico

explicación

La agrupación en clústeres de claves se produce cuando dos claves diferentes cifran un mensaje de texto no cifrado en el mismo texto cifrado.

La fuerza de trabajo es el tiempo, el esfuerzo y los recursos estimados necesarios para romper un sistema criptográfico.

Descifrar es el acto de transformar los datos en un formato legible.

La criptología es la práctica de romper los sistemas criptográficos.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Conceptos de criptografía

---

Question #104 of 193

Question ID: 1104993

¿En qué situación el scripting entre sitios (XSS) representa el mayor peligro?

- ✗ **A)** Un usuario tiene acceso a un sitio Web de contenido estático.
- ✗ **B)** Un usuario tiene acceso a un sitio Web de acceso público.
- ✓ **C)** Un usuario accede al sitio de una organización financiera con sus credenciales de inicio de sesión.
- ✗ **D)** Un usuario accede a un sitio basado en el conocimiento con sus credenciales de inicio de sesión.

explicación

Las secuencias de comandos entre sitios (XSS) representan el mayor peligro cuando un usuario accede al sitio de una organización financiera con sus credenciales de inicio de sesión. El problema no es que el hacker se hará cargo del servidor. Es más probable que el hacker se hará cargo de la sesión activa del usuario en el cliente. Esto permitirá al hacker obtener información sobre el usuario legítimo que no está disponible públicamente.

Mientras que las otras situaciones pueden resultar en un ataque XSS, estas situaciones no representan tanto peligro porque es poco probable que se obtenga información del mundo real.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
evaluar y mitigar las vulnerabilidades de las arquitecturas de seguridad, los diseños y los elementos de la solución

Referencias:

Información de secuencias de comandos entre sitios, https://httpd.apache.org/info/css-security/

Question #105 of 193

Question ID: 1192932

Haga clic en cada uno de los encabezados del escenario para expandir o contraer su contenido. Debe leer todo el escenario para responder a la pregunta.

fondo

Usted es un profesional de la seguridad contratado recientemente por una institución financiera que cotiza en bolsa para ayudar a administrar la seguridad de la organización. La oficina principal de la compañía está en Nueva York, NY, y tiene sucursales adicionales en todo Estados Unidos.

Temas actuales

La infraestructura actual incluye servidores Windows, servidores UNIX, clientes Windows, clientes Mac, dispositivos móviles Windows y dispositivos móviles Mac implementados en todas las oficinas. El departamento de TI de la compañía tiene un gran personal ubicado en la oficina de Nueva York. Cada sucursal tiene unos pocos miembros del personal de TI local que solo se encargan de los problemas de esa sucursal.

Ha identificado varias instancias en las que los ataques contra los sistemas cliente no se impidieron ni detectaron en el nivel de cliente porque no se implementó ningún control para evitar el ataque. Los datos fueron robados de algunos dispositivos. Toda una sucursal estaba infectada con malware y virus y requería varios días de tiempo de recuperación, lo que significaba la pérdida de ingresos. Por último, recientemente descubrió que varios sistemas cliente tienen instaladas versiones sin licencia de sistemas operativos. Debe asegurarse de que se implementan los controles adecuados para mitigar estos riesgos.

En una auditoría reciente, descubrió que varios dispositivos móviles carecían de las actualizaciones adecuadas para sus sistemas operativos o aplicaciones. Además, los usuarios habían desactivado las funciones de limpieza remota y localización GPS en estos dispositivos y habían instalado varias aplicaciones no autorizadas. Necesita una solución para mitigar estos riesgos y controlar la configuración y las aplicaciones de los dispositivos móviles cuando esos dispositivos están conectados a la empresa.

Debido a varios contratos entre su empresa y terceros, debe asegurarse de que ciertos sistemas dentro de su infraestructura logren EAL7 en el modelo de evaluación de criterios comunes.

Recientemente, uno de los servidores de la intranet fue víctima de un ataque de denegación de servicio (DoS). El departamento de TI tardó más de 24 horas en devolver el servidor al estado operativo. Durante ese tiempo, el personal de la oficina principal no pudo acceder a la información importante de recursos humanos almacenada en el servidor afectado.

Se espera que los usuarios utilicen el cifrado simétrico y asimétrico para garantizar la confidencialidad de los datos. Debe implementar un sistema adecuado para administrar las claves de cifrado, los valores hash y los certificados

digitales en todos los equipos cliente. También debe proteger las contraseñas, cifrar unidades y administrar los derechos digitales de estos mismos equipos.

La integridad de los datos se ha convertido en una preocupación cada vez más seria para los archivos creados y mantenidos por el departamento de investigación. Debe implementar la solución adecuada para estos archivos. Todos los archivos se encuentran en un único servidor que es accesible sólo por los usuarios en el departamento de investigación.

Nunca se completó formalmente un análisis de riesgos exhaustivo para toda la organización. Se le ha pedido que encabece este proyecto. Como parte de este proceso, debe identificar las amenazas geográficas para cada oficina individual.

Su organización desplegará dos oficinas internacionales a finales de este año. Se le ha invitado a participar en la selección de instalaciones y en el proceso de seguridad interna del edificio para proporcionar información de seguridad concreta.

¿Qué debe implementar para ayudar con los problemas del dispositivo móvil?

- ✗ **A)** directivas de grupo
- ✗ **B)** Kerberos
- ✓ **C)** Mdm
- ✗ **D)** Active Directory

explicación

Debe implementar la administración de dispositivos móviles (MDM) para ayudar con los problemas del dispositivo móvil.

Active Directory proporciona autenticación y realiza un seguimiento de los nombres de usuario, la contraseña y las directivas de grupo de una empresa. Kerberos proporciona autenticación. Ninguno de estos componentes se puede usar para administrar la configuración del dispositivo móvil.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Evaluar y mitigar las vulnerabilidades en los sistemas móviles

Referencias:

Proyecto de seguridad móvil de OWASP: ¿Qué es la tecnología MDM?,
https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=MDM_Technology

---

Question #106 of 193

Question ID: 1132519

¿Qué tecnología web proporciona el nivel más alto de seguridad?

✗ **A)** ActiveX

✗ **B)** JavaScript

✓ **C)** HTTPS (en)

✗ **D)** S-HTTP

explicación

De las opciones dadas, HTTPS proporciona el nivel más alto de seguridad. El protocolo HTTP Seguro (HTTPS) proporciona una conexión segura entre dos equipos. La conexión está protegida y todo el tráfico entre los dos equipos está cifrado. HTTPS utiliza capa de sockets seguros (SSL) o seguridad de la capa de transporte (TLS). Utiliza el cifrado de clave privada para cifrar todo el canal. SSL/TLS implementa la confidencialidad, la autenticación y la integridad por encima de la capa de transporte.

Http seguro (S-HTTP) es diferente de HTTPS. S-HTTP permite a los equipos negociar una conexión de cifrado y no es tan seguro como HTTPS. Utiliza el cifrado de documentos para proteger únicamente el contenido del documento HTTP.

ActiveX es muy vulnerable a los ataques porque los usuarios pueden configurar su equipo para tener acceso automáticamente a un componente o control ActiveX.

Los scripts de JavaScript se pueden descargar desde un sitio web y ejecutar, causando daños a los sistemas.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

CISSP Cert Guide (3rd Edition), Chapter 3: Security Architecture and Engineering, HTTP, HTTPS, and S-HTTP

HTTPS, http://searchsoftwarequality.techtarget.com/definition/HTTPS

Question #107 of 193

Question ID: 1105028

¿Cuál es el principal problema de la criptografía simétrica?

✗ **A)** implementación de hardware y software

✓ **B)** administración de claves

✗ **C)** diferentes claves para cifrado y descifrado

✗ **D)** alto procesamiento

explicación

La administración de claves es el principal problema con la criptografía simétrica. La criptografía simétrica utiliza una clave para cifrar y descifrar los datos, mientras que la criptografía asimétrica utiliza claves diferentes para cifrar y descifrar los datos. Las dos claves se conocen como privadas y las claves públicas. Los problemas de administración de claves incluyen la recuperación de claves, el almacenamiento de claves y el cambio de claves.

En realidad, la criptografía simétrica requiere mucho menos procesamiento que la criptografía asimétrica. La criptografía simétrica (clave privada) es más fácil de implementar y aproximadamente de 1000 a 10000 veces más rápida que la criptografía asimétrica (clave pública).

Cada persona autorizada que se comunique mediante el algoritmo simétrico debe tener una copia de la clave secreta. Si el número de usuarios se ejecuta en cientos, se requieren cientos de claves idénticas para ser manejado. Por lo tanto, se hace difícil administrar las claves. El cifrado simétrico requiere que cada nodo de comunicación tenga su propia clave.

La criptografía simétrica puede ser menos segura que la criptografía asimétrica debido a las mismas claves que se utilizan para el cifrado y descifrado.

La criptografía simétrica requiere un mecanismo seguro independiente para entregar claves a los nodos participantes en la comunicación.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, algoritmos simétricos

---

Question #108 of 193

Question ID: 1105059

Su organización ha decidido implementar el algoritmo asimétrico Diffie-Hellman. ¿Qué afirmación es cierta del intercambio de claves de este algoritmo?

✗ **A)** Los usuarios autorizados no necesitan intercambiar claves secretas.

✗ **B)** Los usuarios autorizados intercambian claves públicas a través de un medio seguro.

✗ **C)** Los usuarios no autorizados intercambian claves públicas a través de un medio no seguro.

✓ **D)** Los usuarios autorizados intercambian claves secretas a través de un medio no seguro.

explicación

En el intercambio de claves Diffie-Hellman, los usuarios autorizados intercambian claves secretas a través de un medio no seguro.

El algoritmo Diffie-Hellman es un protocolo criptográfico en el que las partes remitente y receptora establecen conjuntamente la clave secreta compartida para permitir su uso para todo el cifrado y descifrado futuro de datos masivos. Un algoritmo de intercambio de claves Diffie-Hellman no se utiliza normalmente para cifrar datos. Es un método utilizado para intercambiar claves de forma segura a través de un medio no seguro. Por lo tanto, Diffie-Hellman es un protocolo de intercambio de claves y se utiliza para la distribución segura de claves. Diffie-Hellman no ayuda en el cifrado y descifrado masivo.

En el intercambio de claves Diffie-Hellman, los usuarios autorizados no intercambian claves públicas sino una clave secreta compartida a través de un medio no seguro.

Los usuarios no autorizados no deben tener acceso a las claves secretas porque no son participantes autorizados de una comunicación segura.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Diffie-Hellman

---

Question #109 of 193

Question ID: 1105009

¿Qué son los servicios de confidencialidad?

✗ **A)** firmas digitales

✗ **B)** esquemas de autenticación

✗ **C)** Matrices RAID

✓ **D)** tecnologías de cifrado

explicación

Las tecnologías de cifrado, como Pretty Good Privacy (PGP), son servicios de confidencialidad, que se proporcionan para proteger el contenido de los archivos de los piratas informáticos.

Las firmas digitales se pueden utilizar para proteger la integridad de los archivos asegurándose de que los archivos no se cambian en tránsito. Una firma digital proporciona autenticación (saber quién envió realmente el mensaje), integridad (porque está implicado un algoritmo hash) y no devolución (el remitente no puede denegar el envío del mensaje).

La mayoría de los tipos de matrices de matriz redundante de discos independientes (RAID) son servicios de disponibilidad que están diseñados para garantizar que los datos permanezcan disponibles incluso en el caso de un error de hardware.

Los esquemas de autenticación son sistemas de rendición de cuentas, que están diseñados para identificar a los usuarios en una red informática.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, cifrado / descifrado

---

Question #110 of 193

Question ID: 1114708

Su organización implementa el cifrado híbrido para proporcionar un alto nivel de protección de los datos. ¿Qué afirmaciones son ciertas para este tipo de cifrado?

un. La clave secreta protege las claves de cifrado.

B. Las claves públicas descifran la clave secreta para su distribución.

c. La criptografía asimétrica se utiliza para la distribución segura de claves.

d. El algoritmo simétrico genera claves públicas y privadas.

E. La criptografía simétrica se utiliza para el cifrado y descifrado de datos.

- ✗ **A)** opción b
- ✗ **B)** Opción d
- ✗ **C)** opción e
- ✗ **D)** opción A
- ✗ **E)** Opciones C y D
- ✗ **F)** opciones A y B
- ✓ **G)** Opciones C y E
- ✗ **H)** opción c

explicación

Los métodos de cifrado híbridos utilizan algoritmos asimétricos y simétricos. Los algoritmos asimétricos son lentos, complejos, intensivos y requieren recursos adicionales del sistema y tiempo adicional para cifrar y descifrar los datos. Por lo tanto, los algoritmos asimétricos se utilizan para generar claves públicas y privadas que protegen las claves de cifrado, como las claves de sesión y las claves secretas, y son responsables de la distribución automatizada de claves.

Un algoritmo simétrico genera una clave secreta que se utiliza para el cifrado masivo y el descifrado de datos. Las siguientes características resumen el método de cifrado híbrido:

- Las claves públicas y privadas generadas por el algoritmo asimétrico protegen el proceso de intercambio de claves secretas o de sesión.
- Las claves públicas y privadas cifran y descifran la clave secreta entre dos puntos de comunicación.

Es importante tener en cuenta que las claves públicas y privadas se pueden utilizar para los procesos de cifrado y descifrado.

La clave secreta generada por el algoritmo simétrico se utiliza para el cifrado masivo y el descifrado de datos. La clave secreta cifra el mensaje real.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, cifrados híbridos

---

Question #111 of 193

Question ID: 1113944

Obtener acceso no autorizado al centro de datos mediante el uso de las credenciales de otro usuario al seguirlas en el edificio es un ejemplo de ¿qué opción?

✗ **A)** torniquete

✗ **B)** mantrap

✗ **C)** intrusión

✓ **D)** piggybacking

explicación

Piggybacking es el acto de obtener acceso no autorizado a una instalación mediante el uso de credenciales de acceso de otro usuario siguiéndolos en el edificio. Otro término común para piggybacking es tailgating.

Un mantrap se refiere a un conjunto de puertas dobles que generalmente son monitoreadas por un guardia de seguridad.

Un torniquete es un tipo de puerta que permite el movimiento en una sola dirección a la vez.

Mientras que piggybacking es una forma de intrusión, intrusión es un término genérico utilizado para cualquier tipo de violación de seguridad. Mantraps puede ayudar a prevenir el piggybacking.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

Piggybacking (seguridad), https://en.wikipedia.org/wiki/Piggybacking_%28security%29

Question #112 of 193

Question ID: 1114707

¿Qué opción es un algoritmo de cifrado de clave pública?

✗ **A)** idea

✗ **B)** listado

✓ **C)** RSA

✗ **D)** RC5

explicación

Rivest, Shamir, Adleman (RSA) es un algoritmo de cifrado de clave pública. RSA admite el cifrado y descifrado y protege los datos con un algoritmo que se basa en la dificultad de factorizar grandes números. RSA se basa en el hecho de que es difícil factorizar números grandes en dos números primos originales. La fuerza de RSA es la dificultad en encontrar los factores primos de números muy grandes.

Un algoritmo de cifrado de clave pública a veces se conoce como algoritmo de cifrado asimétrico. Con el cifrado asimétrico, la clave pública se comparte y se utiliza para cifrar la información, y la clave privada es secreta y se utiliza para descifrar los datos cifrados con la clave pública correspondiente. Si P representa la clave privada, Q representa la clave pública y M representa el mensaje de texto no cifrado, entonces lo siguiente es cierto con respecto a un criptosistema de clave pública:

Q[P(M)] = M

P[Q(M)] = M

Es computacionalmente inviable derivar P de Q.

El cifrado de clave privada a veces se conoce como cifrado simétrico. Con el cifrado de clave simétrica, la clave privada se utiliza para cifrar y descifrar datos. International Data Encryption Algorithm (IDEA), RC5 y Skipjack son algoritmos de cifrado de clave privada.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e Ingeniería de Seguridad, RSA

Question #113 of 193

Question ID: 1113939

¿Qué elemento puede ser una amenaza para los sistemas eléctricos en una instalación de procesamiento de información?

- ✓ **A)** un hundimiento
- ✗ **B)** un spike buster
- ✗ **C)** una fuente de alimentación ininterrumpida (UPS)
- ✗ **D)** un acondicionador de línea eléctrica

explicación

El hundimiento de voltaje se refiere a un bajo voltaje momentánea. El sistema eléctrico puede fallar en ausencia de suficiente suministro de voltaje requerido por el sistema eléctrico.

Una fuente de alimentación ininterrumpida (UPS) actúa como una fuente de respaldo para la energía limpia y constante necesaria para mantener las operaciones de datos cuando la unidad de alimentación primaria se apaga.

Un pico se refiere a un alto voltaje momentánea y puede ser una amenaza significativa para los componentes eléctricos. Los destructores de espigas suprimen el alto voltaje y evitan que los sistemas eléctricos se dañen.

Un acondicionador de línea eléctrica o un filtro de alimentación evitan fluctuaciones en la potencia y las interferencias, como el ruido. Debido a que factores como el ruido, la humedad, los apagones, etc., pueden dañar potencialmente los componentes eléctricos e interrumpir las operaciones comerciales, se deben tomar precauciones para protegerse contra las fluctuaciones de energía y las interferencias.

Los acondicionadores de líneas eléctricas no deben confundirse con los divisores de potencia. Los divisores de potencia proporcionan múltiples tomas de corriente para una sola entrada de alimentación. Las tomas de corriente transportan señales de potencia iguales en fase y amplitud a las señales de potencia de entrada. Los divisores de potencia se utilizan generalmente para apilar múltiples antenas para crear un sistema de antenas.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Tipos de interrupciones

---

Question #114 of 193

Question ID: 1105073

¿Qué entidad debe certificar el par de claves públicas de una CA raíz?

- ✗ **A)** una CA externa
- ✗ **B)** una CA subordinada
- ✗ **C)** un servidor Kerberos
- ✓ **D)** la CA raíz

explicación

Una entidad de certificación (CA) raíz debe certificar su propio par de claves públicas.

Es posible que una organización también desee que el par de claves públicas de una CA raíz esté certificado por una CA externa para mayor seguridad y confianza en el par de claves. Ni una CA subordinada ni un servidor Kerberos se utilizan para certificar el par de claves de una CA raíz.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Autoridad de certificación (CA) y Autoridad de registro (RA)

Question #115 of 193

Question ID: 1105038

¿Qué cifrado se basa en las pistas de los factores físicos en lugar del hardware o un criptosistema de software?

- ✗ **A)** un cifrado de transposición
- ✓ **B)** un cifrado de ocultación
- ✗ **C)** un cifrado DES
- ✗ **D)** un cifrado 3DES

explicación

El cifrado de ocultación se basa en las pistas de los factores físicos que afectan al emisor y al receptor. Se basa en el acuerdo entre las dos partes que se comunican en cuanto a qué patrón utilizar para determinar el mensaje real. Por ejemplo, dos usuarios pueden decidir utilizar cada cuatro palabras en un mensaje como clave. Por lo tanto, un mensaje "Por favor, eche un vistazo al exterior, el tiempo en la estación se retrasa" se decodificará como "Mirar retrasado".

Data Encryption Standard (DES) y Triple-DES (3DES) son algoritmos de cifrado simétricos basados en las funciones matemáticas de sustitución y transposición. Un algoritmo DES utiliza una única clave de 64 bits para el cifrado y descifrado de datos. Un algoritmo DES doble utiliza el mismo factor de trabajo que el algoritmo DES. Un algoritmo 3DES utiliza tres claves de 64 bits para el cifrado y descifrado. Un algoritmo 3DES utiliza 48 rondas de cálculo en comparación con un algoritmo DES que utiliza 16 rondas de cálculo. El factor de trabajo del DES triple es mayor que el del DES doble. Los algoritmos DES y 3DES no requieren un criptosistema de software y alteraciones de bits. El estándar ANSI X9.52 define 3DES.

Los cifrados de sustitución y transposición son dos tipos básicos de cifrado. Un cifrado de transposición dispersa el texto original en el mensaje en lugar de sustituirlo por otro texto. La permutación y las combinaciones se utilizan para codificar las letras en un cifrado de transposición. Una clave secreta determina la posición de las letras movidas en el texto original. El cifrado de transposición no requiere un criptosistema de software y alteraciones de bits.

Ninguna de las opciones requiere un criptosistema de software y alteraciones de bits.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

CISSP Cert Guide (3rd Edition),Chapter 3: Security Architecture and Engineering, Running Key and Concealment Ciphers

---

Question #116 of 193

Question ID: 1113919

¿Qué dos factores garantizan que la información esté compartimentada en el modelo de flujo de información?

- ✗ **A)** clasificación y flujo
- ✗ **B)** clasificación y función
- ✓ **C)** clasificación y necesidad de saber
- ✗ **D)** rol y necesidad de saber

explicación

La clasificación y la necesidad de saber garantizan que la información esté compartimentada en el modelo de flujo de información. La clasificación determina el nivel de seguridad necesario para ver el objeto. Need to know garantiza que el usuario que intenta ver el objeto necesita acceso a la información. Sin la necesidad de conocer la designación, un usuario con una autorización de alto secreto podría ver todos los objetos de alto secreto, no solo aquellos a los que el usuario necesita acceso.

Ninguno de los otros factores afecta a la compartimentación de la información en el modelo de flujo de información.

En el modelo de flujo de información, un flujo actúa como un tipo de dependencia al relacionar dos versiones del mismo objeto. El flujo asigna la transformación del objeto de una versión a otra.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender los conceptos fundamentales de los modelos de seguridad

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 3: Operaciones de seguridad, modelos de flujo de información

---

Question #117 of 193

Question ID: 1111705

¿Qué nivel de Orange Book se considera protecciones obligatorias y se basa en el modelo de seguridad de Bell-LaPadula?

✗ **A)** D
✓ **B)** B
✗ **C)** un
✗ **D)** C

explicación

Los Criterios de evaluación de sistemas informáticos de confianza (TCSEC) clasifican los sistemas en cuatro divisiones jerárquicas de niveles de seguridad: Nivel A (protección verificada y el nivel más alto de seguridad), Nivel B (protección obligatoria aplicada con etiquetas de seguridad), Nivel C (protección discrecional) y Nivel D (protección mínima). Los criterios de evaluación se publican en un libro conocido como el Libro Naranja.

Cada nivel puede tener subniveles numerados. Una calificación más alta implica un mayor grado de confianza y seguridad. Por ejemplo, una clasificación B2 proporciona más seguridad que una clasificación C2. Una calificación más alta incluye los requisitos de una calificación más baja. Por ejemplo, una clasificación B2 incluye las características y especificaciones de una clasificación C2.

El nivel A es una protección verificada, que ofrece el más alto nivel de seguridad. Una calificación A1 implica que la garantía de seguridad, el diseño, el desarrollo, la implementación, la evaluación y la documentación de un equipo se realizan de una manera muy formal y detallada. Una infraestructura que contiene sistemas con clasificación A1 es el entorno más seguro y normalmente se utiliza para almacenar información altamente confidencial y confidencial. Este nivel implementa la administración de instalaciones de confianza.

El nivel B es una protección obligatoria basada en el modelo de seguridad bell-lapadula y aplicada mediante el uso de etiquetas de seguridad.

- Una clasificación B1 hace referencia a la seguridad etiquetada, donde cada objeto tiene una etiqueta de clasificación y cada sujeto tiene un nivel de autorización de seguridad. Para acceder al contenido del objeto, el sujeto debe tener un nivel igual o mayor de autorización de seguridad que el objeto. Un sistema compara el nivel de autorización de seguridad de un sujeto con la clasificación del objeto para permitir o denegar el acceso al objeto. La categoría B1 ofrece aislamiento de procesos, el uso de etiquetas de dispositivos, el uso de especificaciones y verificaciones de diseño y controles de acceso obligatorios. Los sistemas B1 se utilizan para manejar información clasificada.
- Una clasificación B2 se refiere a la protección estructurada. Se debe utilizar un procedimiento de autenticación estricto en los sistemas con clasificación B2 para permitir que un sujeto acceda a los objetos mediante la ruta de acceso de confianza sin puertas traseras. Este nivel es el nivel más bajo para implementar la administración de instalaciones de confianza; los niveles B3 y A1 también lo implementan. Los requisitos adicionales de una clasificación B2 incluyen la separación de las funciones de operador y administrador, las etiquetas de sensibilidad y el análisis del canal de almacenamiento encubierto. Un sistema B2 se utiliza en entornos que contienen información altamente confidencial. Por lo tanto, un sistema B2 debe ser resistente a los intentos de penetración.
- Una clasificación B3 se refiere a los dominios de seguridad. Los sistemas B3 deben ser capaces de realizar una recuperación de confianza. Un sistema evaluado con una clasificación B3 debe tener el rol del administrador de seguridad totalmente definido. Un sistema B3 debe proporcionar la funcionalidad de supervisión y auditoría. Un sistema B3 se utiliza en entornos que contienen información altamente sensible y debe ser resistente a los intentos de penetración. Otra característica de la clasificación B3 es el análisis de canal de temporización encubierto. Esta categoría especifica controles de recuperación de confianza.

El nivel C es una protección discrecional basada en el acceso discrecional de sujetos, objetos, individuos y grupos.

- Una clasificación C1 se refiere a la protección de seguridad discrecional. Para habilitar el proceso de calificación, los sujetos y los objetos deben separarse de la instalación de auditoría mediante un proceso de identificación y autenticación claro. Un sistema de clasificación C1 es adecuado para entornos en los que los usuarios procesan la información en el mismo nivel de sensibilidad. Un sistema de clasificación C1 es adecuado para entornos con problemas de seguridad baja.
- Una clasificación C2 se refiere a la protección de acceso controlado. La funcionalidad de autenticación y auditoría en los sistemas debe estar habilitada para que se produzca el proceso de clasificación. Un sistema con una clasificación C2 proporciona protección de recursos y no permite la reutilización de objetos. La reutilización de objetos implica que un objeto no debe tener datos remanentes que puedan ser utilizados por un sujeto más adelante. Un sistema C2 proporciona un control de acceso granular y establece un nivel de responsabilidad cuando los sujetos acceden a objetos. Un sistema con clasificación C2 es adecuado para un entorno comercial.

El nivel D es una clasificación de protección mínima que se ofrece a los sistemas que no cumplen los criterios de evaluación de los niveles superiores.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender los conceptos fundamentales de los modelos de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Operaciones de seguridad. Libro naranja

---

Question #118 of 193

Question ID: 1104962

¿Qué sección del documento Requisitos mínimos de seguridad para el sistema operativo multiusuario (NISTIR 5153) aborda la responsabilidad del usuario de extremo a extremo?

✗ **A)** control de acceso

✗ **B)** integridad de los datos

✗ **C)** integridad del sistema

✓ **D)** auditoría

explicación

La sección de auditoría del documento Requisitos mínimos de seguridad para el sistema operativo multiusuario (NISTIR 5153) aborda la responsabilidad del usuario de extremo a extremo. En esta sección también se aborda la protección de la pista de auditoría contra el acceso no autorizado y, posiblemente, el uso del cifrado.

La sección de control de acceso define los usuarios y las condiciones en las que los usuarios pueden acceder al sistema. Estas condiciones pueden incluir controles basados en la identificación del usuario, la hora, la ubicación y el método de acceso.

La sección de integridad del sistema garantiza que las características de seguridad funcionen como se esperaba para proporcionar la integridad del sistema adecuada.

La sección de integridad de datos garantiza que las características de seguridad funcionen como se esperaba para proporcionar la integridad de datos adecuada.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Seleccione controles en función de los requisitos de seguridad de los sistemas

Referencias:

Requisitos mínimos de seguridad para el documento sistema operativo multiusuario (NISTIR 5153), http://csrc.nist.gov/publications/nistir/ir5153.txt

---

Question #119 of 193

Question ID: 1105127

Se le ha pedido que implemente un plan por el cual la sala de servidores de su empresa permanecerá en línea durante tres horas después de un corte de energía. Esto le dará a su departamento de TI tiempo suficiente para implementar el sitio alternativo. ¿Qué tecnología sería la mejor en este escenario?

- ✗ **A)** incursión
- ✓ **B)** generador de copia de seguridad
- ✗ **C)** SAI
- ✗ **D)** agrupamiento

explicación

Debe implementar un generador de copia de seguridad. Un generador de respaldo proporcionará energía por un tiempo limitado. Funciona con gasolina o diesel para generar electricidad. Los generadores de respaldo proporcionan energía redundante.

La matriz redundante de discos independientes (RAID) es una solución de disco mediante la cual los discos duros pueden proporcionar soluciones tolerantes a errores. No tiene nada que ver con la capacidad de potencia.

Una fuente de alimentación ininterrumpida (UPS) proporcionará energía por un corto tiempo, generalmente menos de una hora. Un UPS no proporcionará tiempo suficiente para implementar el sitio alternativo. Sin embargo, puede ser necesario implementar sistemas UPS para proporcionar energía hasta que el generador de respaldo se pueda poner en línea.

La agrupación en clústeres proporciona tolerancia a errores para los servidores. Los servidores que forman parte de un clúster proporcionan servicios en caso de que se produzca un error en otros servidores de los clústeres.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura de seguridad y fuente de alimentación de ingeniería

---

Question #120 of 193

Question ID: 1105025

Todo lo siguiente afecta a la intensidad del cifrado, EXCEPTO:

- ✓ **A)** la longitud de los datos que se están cifrando
- ✗ **B)** el secreto de la llave
- ✗ **C)** el algoritmo
- ✗ **D)** la longitud de la clave

explicación

La longitud de los datos que se cifran no afecta a la intensidad del cifrado.

La intensidad del cifrado se ve afectada por el algoritmo, la confidencialidad de la clave, la longitud de la clave y el vector de inicialización.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Características del criptosistema

---

Question #121 of 193

Question ID: 1105085

Debe asegurarse de que un único documento transmitido desde el servidor Web está cifrado. Debe implementar esta solución de la forma más sencilla posible.

¿Qué debes hacer?

- ✗ **A)** Usa JavaScript.
- ✗ **B)** Utilice HTTPS.
- ✗ **C)** Utilice ActiveX.
- ✓ **D)** Utilice S-HTTP.

explicación

Debe utilizar HTTP seguro (S-HTTP) para cifrar un único documento desde el servidor Web. Esto permitirá a los dos equipos negociar una conexión de cifrado si es necesario transmitir este documento.

No debe utilizar ActiveX. ActiveX personaliza controles, iconos y otros sistemas habilitados para Web para aumentar su facilidad de uso. Los componentes y controles ActiveX se descargan en el cliente.

JavaScript es un lenguaje de programación que permite el acceso a los recursos en el sistema que ejecuta el JavaScript. Los scripts de JavaScript se pueden descargar de un sitio web y ejecutar.

HTTP seguro (HTTPS) se utiliza para cifrar un canal completo mediante el cifrado de clave privada. Se utiliza para cifrar toda la información entre dos equipos.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, HTTP, HTTPS y S-HTTP

S-HTTP, http://searchsoftwarequality.techtarget.com/definition/S-HTTP

Question #122 of 193

Question ID: 1113935

¿Cuál es el propósito de la autenticación en un criptosistema?

- ✓ **A)** Comprobar la identidad del usuario o del sistema
- ✗ **B)** convertir la información en datos ininteligibles
- ✗ **C)** Asegurarse de que el remitente de los datos no puede negar haber enviado los datos
- ✗ **D)** asegurarse de que un usuario no autorizado no ha cambiado los datos

explicación

El propósito de la autenticación en un criptosistema es verificar la identidad del usuario o del sistema.

La integridad garantiza que los datos no hayan sido modificados por usuarios no autorizados desde que se crearon, transmitieron o almacenaron los datos. La no denuncia garantiza que el remitente de los datos no puede negar haber enviado los datos. El servicio proporcionado por un criptosistema que convierte la información en datos ininteligibles es la confidencialidad.

La autorización permite a los usuarios tener acceso a un recurso una vez que se ha demostrado su identidad.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, autenticación

---

Question #123 of 193

Question ID: 1113920

¿Qué modelo de seguridad garantiza que las actividades realizadas en un nivel de seguridad superior no afecten a las actividades en un nivel de seguridad inferior?

- ✗ **A)** Modelo de Brewer y Nash
- ✗ **B)** modelo de flujo de información
- ✗ **C)** Modelo biba
- ✓ **D)** modelo de no intervención

explicación

El modelo de no intervención proporciona seguridad multinivel y garantiza que los comandos y las actividades realizadas en un nivel de seguridad no afecten a las actividades en otro nivel de seguridad. Las actividades realizadas a un nivel de seguridad inferior no deben verse afectadas ni interferir con los sujetos u objetos de un nivel de seguridad superior. Este modelo proporciona protección contra la reutilización de objetos o la ejecución de programas malintencionados, que intentan obtener acceso a recursos restringidos. El modelo de no intervención aborda la situación en la que un grupo no se ve afectado por otro grupo mediante comandos específicos.

El modelo Biba se ocupa de la integridad de los datos y cumple con los siguientes requisitos:

- Un sujeto en un nivel de integridad inferior no debe ser capaz de escribir en un objeto en un nivel de integridad superior.
- Un sujeto no debe ser capaz de leer datos de un objeto en un nivel de integridad inferior.

El modelo de flujo de información se refiere al tipo de información, ya sea legal o ilegal, que fluye. Este modelo no se refiere a la dirección del flujo de información. El modelo establece que la información puede fluir de un nivel de seguridad a otro o entre los mismos niveles de seguridad a menos que se realice una operación restringida.

El modelo de Brewer y Nash, también conocido como el modelo de la Muralla China, establece que los controles de acceso para un sistema cambiarán dinámicamente según las actividades de un usuario y las solicitudes de acceso anteriores. Una solicitud del usuario para acceder a la información puede ser denegada si la solicitud presenta un conflicto de intereses. Por ejemplo, es posible que un usuario del departamento de cuentas no pueda ver los informes financieros de una empresa hermana de la misma organización. Esto garantiza que el usuario no introduzca ningún conflicto de intereses.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender los conceptos fundamentales de los modelos de seguridad

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Operaciones de Seguridad, Modelos de No Interferencia

---

Question #124 of 193

Question ID: 1105125

Se ha pedido a un usuario de TI que reemplace un disco duro en un servidor. Sin embargo, cuando el usuario abre la caja, se da cuenta de que el disco duro actual está conectado a la abertura del disco duro mediante un cable de acero. Indica que no sabe dónde está la clave. ¿Qué tipo de bloqueo se describe?

- ✗ **A)** trampa de cable
- ✓ **B)** bloqueo de ranura
- ✗ **C)** control del interruptor
- ✗ **D)** control portuario

explicación

Se está describiendo un bloqueo de ranura. Un cable de ranura conecta una unidad de disco duro interna a la ranura de la unidad de disco duro dentro de la computadora.

Un control de interruptor cubre el interruptor de encendido/apagado de un dispositivo.

Un control de puerto impide el acceso a discos duros o puertos de computadora no utilizados.

Una trampa de cable impide la extracción de un dispositivo que está conectado a un equipo pasando el cable del dispositivo a través de una unidad bloqueable. Una trampa de cable a veces se denomina bloqueo de cable.

Un control de interruptor periférico asegura un teclado colocando un interruptor de encendido/apagado entre el ordenador y el puerto del teclado.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Cerraduras

---

Question #125 of 193

Question ID: 1111723

Su organización ha decidido usar almohadillas de un solo uso para garantizar que ciertos datos confidenciales estén protegidos. Todas las siguientes afirmaciones son ciertas con respecto a este tipo de criptosistema, EXCEPTO:

✗ **A)** Cada almohadilla de una sola vez se puede utilizar sólo una vez.
✗ **B)** La almohadilla debe distribuirse y almacenarse de manera segura.
✗ **C)** El pad debe ser tan largo como el mensaje.
✓ **D)** El pad debe estar formado por valores secuenciales.

explicación

El pad NO debe estar formado por valores secuenciales. Debe estar formado por valores aleatorios.

Las siguientes afirmaciones con respecto a las almohadillas de un solo uso son verdaderas:

- Cada almohadilla se puede utilizar sólo una vez.
- El pad debe estar formado por valores aleatorios.
- El pad debe ser tan largo como el mensaje.
- La almohadilla debe distribuirse y almacenarse de manera segura.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, almohadillas de un solo uso

---

Question #126 of 193

Question ID: 1114702

¿Qué ataques se consideran ataques de control de acceso comunes?

a. suplantación de identidad

b. phreaking

c. Inundación SYN

d. ataques de diccionario

e. Ataques de fuerza bruta

- ✗ **A)** opción b
- ✗ **B)** todas las opciones
- ✗ **C)** opción A
- ✗ **D)** Opción d
- ✗ **E)** opción e
- ✓ **F)** opciones a, d y e solamente
- ✗ **G)** Sólo opciones B y C
- ✗ **H)** opción c

explicación

La suplantación de identidad, los ataques de diccionario y los ataques de fuerza bruta son ataques de control de acceso comunes. La suplantación de identidad se produce cuando un atacante implementa un programa falso que roba las credenciales de usuario. Un ataque de diccionario es un método en el que el atacante intenta identificar las credenciales de usuario alimentando listas de palabras o frases de uso común. Un ataque de fuerza bruta es aquel en el que el atacante intenta todas las combinaciones de entrada posibles para obtener acceso a los recursos.

Phreaking es un ataque realizado por un grupo de hackers que se especializan en el fraude telefónico. Se considera un ataque de telecomunicaciones y seguridad de red.

Una inundación SYN ocurre cuando una red se inunda con los paquetes síncronos (SYN). Como resultado, el sistema está sobrecargado y el rendimiento se ve afectado. Muchas veces, a los usuarios legítimos se les deniega el acceso. Una inundación SYN generalmente se considera un ataque de aplicación o sistema.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Ataque de diccionario

---

Question #127 of 193

Question ID: 1104944

¿Qué procesos definen el modo supervisor?

- ✗ **A)** procesos que se ejecutan en los anillos de protección externos
- ✗ **B)** procesos sin mecanismo de protección
- ✗ **C)** Procesos en el anillo de protección externo que tienen más privilegios
- ✓ **D)** procesos que se ejecutan en los anillos de protección internos

explicación

El modo supervisor se refiere a los procesos que se ejecutan en los anillos de protección internos. A los procesos de los anillos de protección internos se les conceden más privilegios que a los procesos del anillo de protección externo. Los procesos en el anillo interno se ejecutan en el modo privilegiado o supervisor, mientras que los procesos que trabajan en los anillos de protección externos se ejecutan en el modo de usuario. Estos procesos en el anillo interno incluyen el proceso del núcleo del sistema operativo y las instrucciones de entrada/salida (E/S). Los procesos se colocan en una estructura de anillo según el privilegio mínimo. Multiplexed Information and Computing Service (MULTICS) es un ejemplo de un sistema de protección en anillo.

Todas las demás opciones son incorrectas.

Cada sistema operativo tiene un mecanismo de protección, como segmentos de memoria y anillos de protección, para garantizar que las aplicaciones no afecten negativamente a los componentes críticos del sistema operativo. Los anillos de protección definen la directiva de seguridad para cada aplicación limitando las operaciones que puede realizar la aplicación. Ninguna aplicación en el sistema operativo funciona sin un mecanismo de protección. Los sistemas operativos son responsables de la asignación de memoria, las tareas de entrada y salida y la asignación de recursos. Si un sistema operativo permite el uso secuencial de un objeto sin actualizarlo, puede surgir la divulgación de datos residuales.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender los conceptos fundamentales de los modelos de seguridad

Referencias:

Question #128 of 193

Question ID: 1154292

¿Qué sentencias NO definen los requisitos de un núcleo de seguridad?

un. El monitor de referencia debe verificarse como correcto.

B. El monitor de referencia debe proporcionar aislamiento de procesos.

c. El núcleo de seguridad debe verificarse de manera exhaustiva.

d. El supervisor de referencia debe aplicar un método para eludir la garantía.

- ✗ **A)** opción c
- ✓ **B)** Opciones B y D
- ✗ **C)** opción A
- ✗ **D)** Opciones A y C
- ✗ **E)** opción b
- ✗ **F)** Opción d

explicación

El monitor de referencia no debe garantizar el aislamiento de los procesos. No debe haber ningún método para eludir la seguridad implementada por el monitor de referencia. Los registros base y de límite proporcionan aislamiento de procesos. Los procesos están contenidos dentro de sus propios dominios de seguridad, por lo que cada uno no realiza accesos no autorizados a otros procesos o sus recursos.

Los componentes de hardware, software y firmware que componen el núcleo de seguridad actúan como mediadores entre los sujetos y los objetos. El núcleo de seguridad proporciona una base para construir un sistema informático de confianza. Los cuatro requisitos del núcleo de seguridad son los siguientes:

- El núcleo de seguridad debe garantizar el aislamiento de los procesos.
- Cada intento de acceder al sistema debe invocar el monitor de referencia.
- Se debe verificar el monitor de referencia y registrar todas las decisiones.
- El núcleo de seguridad debe probarse de manera exhaustiva.

A diferencia del monitor de referencia que es un concepto de control de acceso, el núcleo de seguridad es un componente físico del sistema.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender las capacidades de seguridad de los sistemas de información (por ejemplo, protección de memoria, Módulo de plataforma segura (TPM), cifrado/descifrado)

Referencias:

Cissp Cert Guide (3rd Edition),, Capítulo 3: Arquitectura e ingeniería de seguridad, Mecanismos de protección de software

---

Question #129 of 193

Question ID: 1192930

Usted es responsable de administrar los equipos virtuales de la red. ¿Qué directriz es importante a la hora de administrar equipos virtuales?

- ✗ **A)** Implemente un firewall solo en el equipo host.
- ✓ **B)** Aísle el equipo host y cada equipo virtual entre sí.
- ✗ **C)** Actualice el sistema operativo y las aplicaciones sólo en el equipo host.
- ✗ **D)** Instale y actualice el programa antivirus sólo en el equipo host.

explicación

Debe aislar el equipo host y cada equipo virtual entre sí.

Ninguna de las otras instrucciones es correcta al administrar equipos virtuales. Debe actualizar el sistema operativo y la aplicación en el equipo host y en todos los equipos virtuales. Debe implementar un firewall en el equipo host y en todos los equipos virtuales. Debe instalar y actualizar el programa antivirus en el equipo host y en todos los equipos virtuales.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
evaluar y mitigar las vulnerabilidades de las arquitecturas de seguridad, los diseños y los elementos de la solución

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, virtualización

Seguridad y Virtualización, HYPERLINK "http://techgenix.com/security-virtualization/" \t "sean" http://www.windowsecurity.com/articles/Security-Virtualization.html

---

Question #130 of 193

Question ID: 1104945

¿Qué sucede cuando se produce un error de base de computación de confianza (TCB) como resultado de un proceso con menos privilegios que intenta acceder a segmentos de memoria restringida?

✗ **A)** Es necesario volver a instalar el sistema operativo.

✓ **B)** El sistema entra en modo de mantenimiento.

✗ **C)** Se requiere la intervención del administrador.

✗ **D)** El sistema se reinicia inmediatamente.

explicación

Si un proceso con privilegios más bajos intenta acceder a los segmentos de memoria restringida, el sistema transita al modo de mantenimiento, también denominado reinicio del sistema de emergencia. Se produce un reinicio del sistema de emergencia en respuesta a un error del sistema. Un reinicio del sistema de emergencia puede deberse a un error de base informática de confianza (TCB), un error de medios o un usuario que realiza una actividad insegura. Un proceso con menos privilegios que intenta tener acceso a segmentos de memoria restringidos es un ejemplo de una actividad no segura.

Un reinicio del sistema se produce en respuesta a otros errores de TCB. Se trata de un reinicio controlado del sistema. El propósito de realizar un reinicio del sistema es liberar recursos del sistema y realizar las actividades del sistema necesarias.

Se produce un arranque en frío del sistema si interviene un usuario o un administrador del sistema. Un arranque en frío del sistema se produce cuando los procedimientos de recuperación son inadecuados para recuperar el sistema de un TCB o un error de medios. El sistema permanece en un estado incoherente durante un intento del sistema de recuperación.

La reinstalación del sistema operativo no es una respuesta válida para la recuperación de confianza. La recuperación de confianza incluye un reinicio del sistema, un reinicio del sistema de emergencia y un inicio en frío del sistema.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender los conceptos fundamentales de los modelos de seguridad

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 8, Seguridad de desarrollo de software, Mecanismos de protección de software

Question #131 of 193

Question ID: 1105080

Su organización ha firmado recientemente un contrato con una agencia gubernamental. El contrato requiere que implemente el estándar X.509. ¿Qué rige esta norma?

✗ **A)** IPSec

✗ **B)** HTTP

✓ **C)** PKI

✗ **D)** Ike

explicación

X.509 es un estándar de certificados digitales y la infraestructura de clave pública (PKI) usa certificados digitales para publicar claves públicas. X.509 define la manera en que una entidad de certificación crea un certificado digital. X.509 define los distintos campos, como el nombre distintivo del sujeto, el número de serie, el número de versión, las fechas de duración y el identificador de firma digital y la firma de la autoridad emisora, presentes en los certificados digitales. La información mínima necesaria en un certificado digital es un nombre de usuario, una clave pública y la firma digital del certificador.

El estándar X.509 no rige el intercambio de claves de Internet (IKE), el protocolo de seguridad de Internet (IPSec) o el protocolo de transferencia de hipertexto (HTTP). Ninguno de ellos forma parte de una PKI.

Hay varias versiones de X.509 desde su creación. La versión actual es X.509v4. El estándar X.509 se utiliza en muchos protocolos de seguridad, como el protocolo SSL (Secure Socket Layer).

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 3: Arquitectura de seguridad y certificados de ingeniería

---

Question #132 of 193

Question ID: 1105033

¿Qué afirmación NO es cierta de un algoritmo RSA?

✗ **A)** RSA puede evitar ataques de "Man in the middle".

✗ **B)** RSA es un algoritmo de clave pública que realiza tanto el cifrado como la autenticación.

✓ **C)** Un algoritmo RSA es un ejemplo de criptografía simétrica.

✗ **D)** Los algoritmos de cifrado RSA no tratan con logaritmos discretos.

✗ **E)** RSA utiliza firmas de clave pública y privada para la verificación de integridad.

explicación

RSA es un ejemplo de criptografía asimétrica, no un método de criptografía simétrica.

RSA puede evitar ataques de tipo "Man in the middle" al proporcionar autenticación antes del intercambio de claves públicas y privadas. Un ataque de tipo "Man in the middle" es una amenaza para todas las comunicaciones de cifrado asimétricas.

RSA no se ocupa de logaritmos discretos. La seguridad proporcionada por RSA se basa en el uso de grandes números primos para el cifrado y descifrado. Es difícil factorizar números primos grandes. Por lo tanto, es difícil romper el cifrado. RSA requiere una mayor potencia de procesamiento debido a la factorabilidad de los números, pero garantiza una administración eficiente de las claves.

RSA se utiliza como el estándar mundial de facto para las firmas digitales. RSA es un algoritmo de clave pública que proporciona cifrado y autenticación.

RSA utiliza firmas de clave pública y privada para la verificación de integridad.

Con la criptografía de clave pública, la clave se pasa de forma segura al equipo receptor. Por lo tanto, se prefiere la criptografía de clave pública para proteger los mensajes de fax.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e Ingeniería de Seguridad, RSA

Question #133 of 193

Question ID: 1114701

La administración de su organización se ha dado cuenta recientemente de que el movimiento de Internet de las cosas (IoT) ha dado lugar a muchos problemas de seguridad. Le han pedido que identifique algunas de las vulnerabilidades presentadas por IoT de la siguiente lista:

A. Interfaz web de gestión insegura

B. Insuficiente o falta de autenticación

C. Falta de cifrado de transporte

D. Software/firmware inseguro

E. Insuficiente o falta de seguridad física

¿Cuál se aplicaría?

- ✗ **A)** A, B, C y D
- ✓ **B)** Todo lo anterior
- ✗ **C)** Sólo A y B
- ✗ **D)** Sólo C y D
- ✗ **E)** Sólo D y E
- ✗ **F)** Sólo B y C

explicación

Entre las vulnerabilidades presentadas por IoT se incluyen todas las siguientes:

Interfaz web de gestión insegura

- Falta de autenticación o falta de autenticación
- Falta de cifrado de transporte
- Software/firmware inseguro
- Falta o insuficiencia de seguridad física

Otras vulnerabilidades que pueden existir con IoT incluyen:

- Servicios de red inseguros
- Preocupaciones de privacidad
- Interfaz en la nube de administración insegura
- Interfaz móvil de administración insegura
- Falta o insuficiencia de configuraciones de seguridad

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Evaluar y mitigar las vulnerabilidades en dispositivos integrados

Referencias:

CISSP Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Internet de las Cosas

OWASP Internet of Things Top Ten Project,
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

---

Question #134 of 193

Question ID: 1111711

¿Qué término es una evaluación de los componentes de seguridad y su cumplimiento antes de la aceptación formal?

- ✗ **A)** control de seguridad
- ✗ **B)** acreditación
- ✓ **C)** certificación
- ✗ **D)** control del sistema de información

explicación

La certificación es una evaluación técnica detallada de los componentes de seguridad y su cumplimiento antes de la aceptación formal. Para la certificación se pueden utilizar los siguientes procesos:

- evaluación de salvaguardias
- análisis del riesgo
- verificación
- ensayo
- técnicas de auditoría

La certificación garantiza que un producto o un sistema está de acuerdo con las necesidades del cliente. Por ejemplo, un cliente confiará en el proceso de certificación para confirmar si un producto se adapta a las necesidades de su red.

La acreditación es la aprobación formal de la dirección de un producto. La acreditación valida que se ha verificado la seguridad y funcionalidad general del producto. La declaración de acreditación de la dirección viene después de revisar la información de certificación. Al emitir la acreditación, la dirección valida que los riesgos son conocidos y que el nivel de protección proporcionado por el producto es aceptable.

Las otras dos opciones son incorrectas. La necesidad de saber, la identificación y la autenticidad son la base de los controles de los sistemas de información.

Un control de seguridad no debe depender de la seguridad de su mecanismo.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
evaluar y mitigar las vulnerabilidades de las arquitecturas de seguridad, los diseños y los elementos de la solución

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Operaciones de Seguridad, Certificación y Acreditación

---

Question #135 of 193

Question ID: 1105128

Debe asegurarse de que los datos de los equipos de su organización no se pierdan cuando se produzca un corte de energía. Los usuarios deben tener tiempo suficiente para guardar sus datos si se produce un corte de energía. ¿Qué debes usar?

- ✗ **A)** un aspersor
- ✗ **B)** una cerradura de la puerta
- ✓ **C)** un UPS
- ✗ **D)** un aire acondicionado

explicación

Una fuente de alimentación ininterrumpida (UPS) protege los datos de los equipos de la pérdida debido a cortes de energía. Un UPS contiene una batería que mantiene una computadora en funcionamiento durante un corte de energía o de alimentación. Un UPS le da a un usuario tiempo para guardar cualquier dato no guardado cuando se produce un corte de energía. Un UPS es un control preventivo que se puede identificar durante el proceso de planificación de la continuidad del negocio. Siempre es más fácil prevenir una amenaza que recuperarse de una amenaza.

Las computadoras operan en un rango de temperatura relativamente estrecho, que requiere el acondicionamiento climático de los sistemas de calefacción y aire acondicionado.

Una cerradura de puerta es una medida de seguridad física que puede proteger un centro de datos y otros equipos informáticos de los piratas informáticos.

Un aspersor es un sistema de extinción de incendios que se requiere en la mayoría de los edificios de oficinas. Un aspersor rocía agua, lo que está dañando el equipo informático, por lo que las empresas deben considerar la instalación de sistemas de extinción de incendios que no sean de agua para proteger las computadoras en un centro de datos del fuego y el agua.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura de seguridad e ingeniería secure data center

---

Question #136 of 193

Question ID: 1105012

Mientras investiga el protocolo de seguridad de Internet (IPSec), descubre que utiliza el intercambio de claves de Internet (IKE). ¿Cuál es el propósito principal de IKE?

✗ **A)** Para cifrar los datos en toda la red
✓ **B)** para administrar las asociaciones de seguridad (HSA) a través de la red
✗ **C)** Para reproducir los datos a través de la red
✗ **D)** Para autenticar los datos a través de la red

explicación

El propósito principal del intercambio de claves de Internet (IKE) es administrar las asociaciones de seguridad en toda la red.

IPSec utiliza la carga de seguridad de encapsulación (ESP) y el encabezado de autenticación (AH) como protocolos de seguridad para el cifrado y la autenticación, respectivamente.

La reproducción de datos no es una opción válida porque la reproducción de datos es un ataque lanzado contra las transmisiones de red. El marco IPSec proporciona protección contra ataques de reproducción de datos.

IPSec es un marco en sí mismo y no especifica los algoritmos que se deben utilizar para el cifrado, la autenticación y la administración del proceso de intercambio de claves. IPSec realiza todas estas funciones mediante IKE.

IKE es una combinación de Internet Security Association y Key Management Protocol (ISAKMP) y OAKLEY. OAKLEY es el protocolo de establecimiento de claves que se basa en el algoritmo de intercambio de claves Diffie-Hellman y forma parte del marco IPSec. ISAKMP define los parámetros que se pueden negociar y los métodos de negociación que se utilizarán para asegurar un túnel VPN antes del intercambio de datos. Con la autenticación de clave previamente compartida utilizada por IPSec, solo se necesita una clave previamente compartida para todas las conexiones de red privada virtual (VPN). La autenticación de clave previamente compartida normalmente se basa en contraseñas simples y puede dar lugar a una costosa administración de claves en entornos grandes.

Una alternativa al presharing de la comunicación segura de claves es el uso de certificados digitales. Las partes pueden establecer la comunicación mediante la validación de los certificados digitales de la otra. Los certificados

digitales forman parte del marco de infraestructura de clave pública y garantizan una administración de claves eficaz en comparación con la clave previamente compartida que requiere una administración de claves cuidadosa.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition),Chapter 3: Security Architecture and Engineering, Internet Key Exchange (IKE), also sometimes referred to as IPsec Key Exchange

---

Question #137 of 193

Question ID: 1105107

Varias habitaciones de sus instalaciones tienen ruido en modo de travesía. ¿Qué factor influye en la generación de este ruido?

- ✗ **A)** presurización positiva
- ✗ **B)** diferencia entre los cables calientes y de tierra
- ✓ **C)** diferencia entre cables calientes y neutros
- ✗ **D)** fuente de alimentación ininterrumpida

explicación

La interferencia electromagnética (EMI) es una interferencia causada por la diferencia de carga entre tres tipos de cables eléctricos: caliente, neutro y a tierra. El ruido en modo de recorrido es un tipo de EMI generado por la diferencia de carga eléctrica entre los cables eléctricos calientes y neutros.

La presurización positiva se refiere a una condición en la que el aire sale de una habitación si se abre una puerta, pero el aire exterior no entra. La presurización positiva es uno de los requisitos importantes de calefacción, ventilación y aire acondicionado (HVAC) y no está relacionada con EMI. Por lo general, las instalaciones de procesamiento de información deben tener unidades de aire acondicionado dedicadas para proporcionar control de temperatura y mantener los niveles de humedad del medio ambiente. El CA debe estar en una fuente de alimentación independiente y tener un interruptor de apagado de emergencia dedicado.

Una fuente de alimentación ininterrumpida (UPS) proporciona energía limpia ininterrumpida en ausencia de la fuente de alimentación principal.

El EMI generado por la diferencia de carga eléctrica entre los cables calientes y de tierra se conoce como ruido de modo común.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Tipos de interrupciones

---

Question #138 of 193

Question ID: 1105026

La administración le ha pedido que investigue el cifrado y que haga una recomendación sobre qué técnica de cifrado utilizar. Durante esta investigación, se examinan varios criptosistemas diferentes. ¿Qué parámetro determina su fuerza?

- ✓ **A)** la longitud de la clave
- ✗ **B)** la infraestructura de administración de claves
- ✗ **C)** el marco de seguridad
- ✗ **D)** el código de autenticación de mensajes (MAC)

explicación

La fuerza de un criptosistema está determinada por el algoritmo utilizado para cifrar y descifrar el mensaje y por la longitud de la clave utilizada en el proceso de cifrado. Cuanto más larga sea la clave, mayor será el tiempo que tarda un procesador en probar todos los valores posibles para averiguar el valor de clave que se puede utilizar para descifrar el mensaje. El período de tiempo puede ejecutarse en miles de años para cientos de sistemas multiprocesador.

Un criptosistema se refiere a un sistema de hardware o software que proporciona cifrado y descifrado de texto plano.

Una clave débil de un algoritmo de cifrado puede facilitar los ataques contra el algoritmo. Es importante que la clave se genere utilizando todo el espacio de claves del algoritmo. Esto garantizará una protección adecuada contra los ataques. Una clave corta facilita los ataques contra el algoritmo de cifrado.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Características del criptosistema

---

Question #139 of 193

Question ID: 1111722

Está preparando una propuesta de administración sobre el valor de usar criptografía para proteger su red. ¿Qué afirmación es cierta de la criptografía?

✗ **A)** La disponibilidad es una preocupación principal de la criptografía.
✗ **B)** La criptografía se utiliza para detectar divulgaciones fraudulentas.
✗ **C)** Las claves de la criptografía se pueden hacer públicas.
✓ **D)** La administración de claves es una preocupación principal de la criptografía.

explicación

La administración de claves es una de las consideraciones más cruciales de la criptografía.

Se requieren un algoritmo y una clave para el cifrado de datos. El algoritmo es conocido públicamente mientras que la clave se mantiene en secreto. La confidencialidad, integridad y autenticidad de los datos se pueden abordar a través de la criptografía solo si las claves no se ven comprometidas. Una sola clave se utiliza para el cifrado y descifrado en un criptosistema simétrico. Las claves independientes se utilizan para cifrar y descifrar datos en un criptosistema asimétrico. En ambos escenarios, la seguridad de las claves en un sistema criptográfico es una preocupación primordial. Las claves no deben verse comprometidas durante la transmisión del mensaje.

Las claves criptográficas no deben capturarse, modificarse, corromperse ni divulgarse a personas no autorizadas. Por lo tanto, es importante que se controle la distribución y administración de claves. Las siguientes personas son responsables de la administración de claves:

- Usuarios que protegen sus propias claves
- Administradores que mantienen claves públicas y privadas
- El servidor de autenticación que contiene, mantiene y distribuye las claves a las partes remitente y receptora

La administración eficaz de claves tiene los siguientes requisitos:

- La clave debe distribuirse y administrarse de forma segura.
- La clave debe generarse aleatoriamente y debe utilizar el espacio de claves completo del algoritmo.
- La duración de la clave debe basarse en la sensibilidad de los datos.
- Se debe realizar una copia de seguridad de la clave en caso de pérdida o destrucción de una clave.

- La clave debe eliminarse de forma segura.

La criptografía no se puede utilizar para detectar divulgaciones fraudulentas. El propósito principal de la criptografía es proteger la información confidencial contra la divulgación y no detectar divulgaciones fraudulentas. La criptografía también protege contra modificaciones fraudulentas de cualquier tipo.

La criptografía aborda la confidencialidad, integridad y autenticidad de los datos. No se ocupa de la disponibilidad de datos.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, gestión de claves

---

Question #140 of 193

Question ID: 1105056

¿Cuál es el propósito de la tecnología BitLocker?

- ✗ **A)** Bloquea el equipo para que no se pueda arrancar.
- ✗ **B)** Cifra los datos a medida que se transmiten a través de una red.
- ✗ **C)** Bloquea el disco duro para que no se pueda arrancar.
- ✓ **D)** Cifra el contenido de la unidad para que los datos no puedan ser robados.

explicación

La tecnología BitLocker cifra el contenido de la unidad para que no se puedan robar datos. BitLocker puede cifrar archivos de usuario y de sistema. Un administrador habilita o deshabilita BitLocker para todos los usuarios del equipo. Requiere hardware del Módulo de plataforma segura (TPM).

La tecnología BitLocker no tiene nada que ver con el bloqueo de un equipo o disco duro. Tampoco protege los datos que se transmiten a través de una red.

El Sistema de cifrado de archivos (EFS) también puede cifrar el contenido de un disco. Sin embargo, EFS está habilitado por usuario y solo puede cifrar archivos que pertenecen al usuario que habilita EFS. EFS no requiere ninguna configuración administrativa o de hardware especial.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

BitLocker

Question #141 of 193

Question ID: 1105002

La administración de su organización ha dedicado recientemente tiempo a discutir los ataques contra las empresas y su infraestructura. Durante la reunión, se discutió el ataque Stuxnet. ¿Contra qué tipo de sistema se produjo este ataque?

✗ **A)** Kerberos
✓ **B)** Scada
✗ **C)** VoIP
✗ **D)** radio

explicación

Un ataque Stuxnet se produce contra un sistema de control de supervisión y adquisición de datos (SCADA). Un sistema SCADA también se conoce como un sistema de control industrial. SCADA es una categoría de software que recopila datos en tiempo real desde ubicaciones remotas para controlar equipos y condiciones. Se utiliza para monitorear sistemas críticos y controlar la distribución de energía. En los últimos años, se ha vuelto aún más vital proteger estos sistemas. SCADA se utiliza en las industrias de energía, petróleo, telecomunicaciones, refinación de gas, tratamiento de agua y control de residuos.

Kerberos es un sistema de autenticación que incluye clientes, servidores y un centro de distribución de claves (KDC). El KDC proporcionar vales de clientes que los clientes utilizan para tener acceso a servidores y otros recursos.

El servidor de usuario de acceso telefónico de autenticación remota (RADIUS) es una tecnología de acceso remoto que permite a los usuarios remotos iniciar sesión de forma centralizada para tener acceso a los recursos de la red local.

La voz sobre IP (VoIP) es una tecnología que permite enrutar la comunicación de voz a través de una red IP.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Evaluar y mitigar las vulnerabilidades en dispositivos integrados

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Sistemas de Control Industrial

El gusano Stuxnet, http://us.norton.com/stuxnet

Question #142 of 193

Question ID: 1105076

¿Qué entidad emite certificados digitales?

- ✗ **A)** Bdc
- ✓ **B)** Ca
- ✗ **C)** DC
- ✗ **D)** Efs

explicación

Una entidad de certificación (CA) es una entidad que emite certificados digitales. Para crear un certificado digital, un usuario proporciona a una CA información de contacto y un par de claves pública y privada. A continuación, la CA comprueba la información proporcionada y crea un documento digital con la información de contacto y el par de claves del usuario. La CA cifra el documento digital con su clave privada para crear un certificado digital. A continuación, los usuarios pueden usar la clave pública de la CA para determinar si un certificado digital es válido.

Un controlador de dominio de reserva (BDC) es un servidor en una red de Windows NT que participa en servicios de directorio. Un controlador de dominio (DC) es un servidor en una red de Windows 2000 que participa en servicios de Active Directory. Sistema de cifrado de archivos (EFS) es una característica de Windows 2000 y Windows XP que permite a los usuarios cifrar archivos en volúmenes NTFS.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Autoridad de certificación (CA) y Autoridad de registro (RA)

Question #143 of 193

Question ID: 1105052

¿Cuál de las siguientes fue una máquina de rotor alemana utilizada en la Segunda Guerra Mundial?

- ✗ **A)** Lucifer
- ✗ **B)** Proyecto Ultra
- ✓ **C)** enigma
- ✗ **D)** Máquina púrpura

explicación

Enigma fue una máquina de cifrado de rotor alemana utilizada en la Segunda Guerra Mundial.

Lucifer fue un proyecto de IBM que introdujo ecuaciones y funciones complejas más tarde utilizadas por la Agencia de Seguridad Nacional de los Estados Unidos para establecer el Estándar de Cifrado de Datos (DES).

La Purple Machine fue la máquina de cifrado de rotor japonesa utilizada en la Segunda Guerra Mundial.

El Proyecto Ultra fue un proyecto inglés creado para romper los cifrados alemanes

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

enigma

Question #144 of 193

Question ID: 1105068

¿Qué afirmación NO es cierta del criptoanálisis?

- ✗ **A)** Es una herramienta utilizada para desarrollar un criptosistema seguro.
- ✓ **B)** Se utiliza para probar la fuerza de un algoritmo.
- ✗ **C)** Es un proceso de intentar la ingeniería inversa de un criptosistema.
- ✗ **D)** Se utiliza para forjar señales codificadas que serán aceptadas como auténticas.

explicación

El criptoanálisis no se utiliza para probar la fuerza de un algoritmo.

El criptoanálisis es el proceso de obtener texto plano a partir del texto cifrado sin conocer la clave secreta. El proceso se logra falsificando señales o texto. Estas señales falsificadas serán aceptadas como auténticas. El criptoanálisis se basa en las permutaciones y combinaciones que se utilizan como entradas durante el curso del análisis. El criptoanálisis también se conoce como un proceso de ingeniería inversa utilizado para obtener una salida de una entrada descifrada.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Criptoanálisis

---

Question #145 of 193

Question ID: 1114694

¿Qué opciones son componentes del núcleo de seguridad?

a. Software

b. hardware

c. Monitor de referencia

d. Base informática de confianza

- ✓ **A)** opciones A y B
- ✗ **B)** Opciones C y D
- ✗ **C)** Opción d
- ✗ **D)** opción A
- ✗ **E)** opción b
- ✗ **F)** opción c

explicación

El hardware, el software y el firmware son los componentes de un núcleo de seguridad. Estos componentes forman parte de la base informática de confianza (TCB). Los componentes de un núcleo de seguridad actúan como

mediadores entre los sujetos y los objetos implementando y haciendo cumplir el monitor de referencia que actúa como una máquina abstracta y regula el flujo de información.

El kernel de seguridad y el monitor de referencia trabajan juntos para ayudar a proteger el TCB.

TCB se define como una combinación de componentes del núcleo de seguridad. El núcleo de seguridad proporciona una base para construir un sistema informático de confianza. Los cuatro requisitos del núcleo de seguridad son los siguientes:

- El núcleo de seguridad debe proporcionar aislamiento para los procesos.
- Cada intento de acceder al sistema debe invocar el monitor de referencia.
- Se debe verificar el monitor de referencia y registrar todas las decisiones.
- El núcleo de seguridad debe ser lo suficientemente pequeño como para ser probado de una manera completa.

Un sistema informático que emplea las medidas de garantía de hardware y software necesarias para permitirle procesar varios niveles de información clasificada o confidencial se denomina sistema de confianza.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender las capacidades de seguridad de los sistemas de información (por ejemplo, protección de memoria, Módulo de plataforma segura (TPM), cifrado/descifrado)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Mecanismos de protección de software

---

Question #146 of 193

Question ID: 1111729

¿Qué control incluye mantraps y torniquetes?

✗ **A)** control ambiental
✗ **B)** control administrativo
✗ **C)** control técnico
✓ **D)** control físico

explicación

Mantraps, torniquetes, cercas, perros y guardias son ejemplos de controles de seguridad física. Un mantrap se refiere a un conjunto de puertas dobles vigiladas por un guardia de seguridad. Un torniquete es un tipo de puerta que permite

el movimiento en una sola dirección a la vez. Algunos ejemplos de controles de seguridad física son:

- Control de acceso al centro de datos
- Iniciar sesión y acompañar a los visitantes a las áreas sensibles
- Examen por la administración de la lista de personas con acceso físico a instalaciones sensibles

Un control técnico puede ser un componente del sistema operativo o una herramienta de software que garantiza que al personal no autorizado se le deniegue el acceso a los recursos del sistema. Esto determina la confidencialidad, integridad y disponibilidad de los recursos. Los controles técnicos también incluyen la configuración de la infraestructura. Algunos ejemplos de controles técnicos son los circuitos cerrados de televisión (CCTV), calefacción, ventilación y aire acondicionado (HVAC), alarmas y sistemas de control de acceso.

Un control administrativo se puede implementar mediante el uso de las políticas de seguridad, estándares y directrices establecidas por la alta dirección de la organización. Los procedimientos de la directiva de seguridad indican los objetivos de seguridad de la organización. Los controles administrativos incluyen la planificación de requisitos de instalaciones, la gestión de la seguridad de las instalaciones y los controles de personal. El Plan de Emergencia de Ocupantes (OEP), un procedimiento documentado para minimizar la pérdida de vidas y activos en caso de que ocurra una amenaza física, también se incluye en la categoría de controles administrativos.

Los controles ambientales incluyen contramedidas contra amenazas a la seguridad física, como incendios, inundaciones, electricidad estática, humedad y desastres causados por el hombre.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Torniquetes y Mantraps

---

Question #147 of 193

Question ID: 1104960

¿Qué entidad puede funcionar como sujeto y como objeto?

✓ **A)** programa

✗ **B)** grupo

✗ **C)** archivo

✗ **D)** usuario

explicación

Un programa puede funcionar como sujeto y como objeto. Un programa funciona como un objeto cuando un usuario o grupo tiene acceso al programa. En este ejemplo, el usuario o grupo es el sujeto y el programa es el objeto. Un programa funciona como un sujeto cuando el programa tiene acceso a datos en otra ubicación, como una base de datos. En este ejemplo, el programa es el sujeto y los datos o la base de datos en el objeto.

Los usuarios y grupos son siempre sujetos. Los archivos son objetos.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender los conceptos fundamentales de los modelos de seguridad

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Objetos y Sujetos

---

Question #148 of 193

Question ID: 1113938

Su organización ha identificado varios sitios como opciones para la reubicación. Uno de los lugares tiene un sistema de drenaje positivo. ¿Qué garantiza este sistema con referencia a la seguridad física?

✗ **A)** el aire sale de la habitación tan pronto como se abre la puerta

✗ **B)** el contenido de las tuberías de agua, gas y vapor fluye hacia el edificio

✗ **C)** el suministro limpio y constante de energía desde las cajas de distribución eléctrica hasta los dispositivos eléctricos

✓ **D)** el contenido de las tuberías de agua, gas y vapor fluye fuera del edificio

explicación

En el contexto de la seguridad física, un drenaje positivo garantiza que el contenido de las tuberías de agua, gas y vapor fluya fuera del edificio. Un drenaje positivo de las tuberías de agua, gas y vapor garantiza la protección de la instalación contra peligros, como fugas e incendios, al permitir que el contenido fluya fuera del edificio. Esto garantiza que el contenido de las tuberías no fluya hacia el edificio. Por ejemplo, el agua no debe viajar a través de las tuberías hacia la instalación en caso de una inundación. Las tuberías de agua, gas y vapor también deben tener válvulas de cierre adecuadas para apagar el suministro principal en caso de emergencia.

La presurización positiva mantiene la presión de aire dentro de la instalación para garantizar que el aire interior fluya hacia afuera a medida que la puerta se abre y que el aire exterior no entre. Esto garantiza que el humo y los

contaminantes peligrosos fluyan fuera del edificio en caso de incendio.

El contenido de agua, gas y tubería de vapor no debe fluir en el edificio. Al permitir solo un drenaje positivo, puede reducir los posibles daños causados por las inundaciones.

Los estabilizadores de voltaje y los acondicionadores de línea proporcionan un suministro limpio y constante de energía desde las cajas de distribución eléctrica hasta los dispositivos eléctricos.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar principios de seguridad al diseño de sitios e instalaciones

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, problemas de selección de instalaciones

---

Question #149 of 193

Question ID: 1104950

¿Qué diferencia a ITSEC de TCSEC?

- ✓ **A)** Itsec evalúa por separado la funcionalidad y la garantía.
- ✗ **B)** Las prácticas de desarrollo y la documentación se evalúan como parte de la funcionalidad del sistema.
- ✗ **C)** ITSEC no proporciona servicios de auditoría y autenticación a los usuarios.
- ✗ **D)** Las clasificaciones ITSEC no se asignan al Libro Naranja.

explicación

Los criterios de evaluación de seguridad de la tecnología de la información (ITSEC) evalúan los atributos de funcionalidad y garantía por separado. Este método de evaluación y calificación del sistema utilizado en Europa es diferente de los Criterios de evaluación de sistemas informáticos de confianza (TCSEC) en los que la funcionalidad y la garantía de un sistema se combinan para el proceso de evaluación. ITSEC aborda la integridad y la disponibilidad, así como la confidencialidad. TCSEC se ocupa únicamente de la confidencialidad y agrupa la funcionalidad y la garantía.

Most of the ITSEC ratings for a system can be mapped to the Orange Book. The services provided, such as authentication, auditing, and access control mechanisms, are interpreted by ITSEC as the functionality of the system. ITSEC defines assurance as the ability and the effectiveness of a system to perform consistently. Development

practices, documentation, and configuration management are evaluated for the assurance attribute. Maintaining data integrity and ensuring availability of the system at all times are two criteria that every system must meet.

ITSEC defines functionality and assurance as separate attributes because two distinct systems may have the same functionality but different assurance levels. The F6 through F10 ratings have been added to ITSEC to provide granular evaluation of functionality and assurance.

Objective:
Security Architecture and Engineering

Sub-Objective:
Understand the fundamental concepts of security models

References:

CISSP Cert Guide (3rd Edition), Chapter 3: Security Operations, ITSEC

Question #150 of 193

Question ID: 1114697

What is the best description of reduced instruction set computing (RISC)?

✗ **A)** computing using instructions that perform many operations per instruction

✗ **B)** processing that executes one instruction at a time

✗ **C)** processing that enables concurrent execution of multiple instructions

✓ **D)** computing using instructions that are simpler and require fewer clock cycles to execute

Explanation

Reduced instruction set computing (RISC) is computing using instructions that are simpler and require less clock cycles to execute.

Complex instruction set computing (CISC) is computing using instructions that perform many operations per instruction.

A scalar processing is processing that executes one instruction at a time.

Multiprocessing is processing that enables concurrent execution of multiple instructions. A scalar processor executes one instruction at a time. Superscalar processing is processing that enables concurrent execution of multiple instructions in the same pipeline stage. A pipelined processor increases the performance in a computer by overlapping the steps in different instructions.

Para fines de prueba, también debe comprender la canalización, que aumenta el rendimiento en un equipo al superponer los pasos de diferentes instrucciones.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Comprender las capacidades de seguridad de los sistemas de información (por ejemplo, protección de memoria, Módulo de plataforma segura (TPM), cifrado/descifrado)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, CPU

Comparación entre CISC y RISC, http://members.ii.net/~lawley/is/12/ca/risc/

Question #151 of 193

Question ID: 1114717

¿Qué afirmaciones son ciertas para los halones como agente de extinción de incendios?

un. El halón es seguro para los seres humanos.

B. Halón se ocupa de la clase A categoría de fuego.

c. El gas halón suprime el fuego por una reacción química.

d. FM-200 es un reemplazo aprobado por la EPA para el halón.

E. El halón está actualmente aprobado por la Agencia de Protección Ambiental (EPA).

- ✗ **A)** opción A
- ✗ **B)** Opción d
- ✗ **C)** opción b
- ✗ **D)** opción e
- ✗ **E)** opciones b, c y d
- ✗ **F)** opción c
- ✓ **G)** Opciones C y D
- ✗ **H)** opciones A y B

explicación

Los halones suprimen los incendios de clase B y C que involucran tanto equipos eléctricos como líquidos, como productos derivados del petróleo. El halón se utilizaba generalmente en centros de datos y salas de servidores que almacenaban equipos eléctricos. El halón actúa interrumpiendo las reacciones químicas de un incendio.

Se descubrió que el halón como agente de supresión agota el ozono y es potencialmente dañino para los seres humanos. Por lo tanto, en 1987, el Protocolo de Montreal prohibió el uso de halones. Los reemplazos aprobados por la EPA para el halón incluyen agua, FM-200, NAF-S-III, CEA-410, FE-13, argón, argonita e inergen. FM-200 se utiliza para los centros de datos como un sustituto de halón porque no daña las computadoras o los seres humanos.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, extinción de incendios

---

Question #152 of 193

Question ID: 1114710

Usted forma parte del equipo de diseño de la instalación de procesamiento de información de una organización. ¿Qué opción u opciones representan riesgos potenciales de seguridad física para el diseño?

a. suplantación de identidad

b. robo físico

c. Corte de energía

d. Daños en el hardware

e. Ataque de denegación de servicio (DoS)

- ✗ **A)** opción b
- ✗ **B)** opción e
- ✗ **C)** Opción d
- ✗ **D)** opciones a, b y c
- ✓ **E)** opciones b, c y d
- ✗ **F)** opción c
- ✗ **G)** opciones c, d y e
- ✗ **H)** opción A

explicación

Los principales riesgos de seguridad física incluyen el robo físico, la interrupción de servicios críticos, daños físicos a los activos de hardware, amenazas que afectan la confidencialidad y la integridad y disponibilidad de los recursos críticos de una organización.

La seguridad física aborda las siguientes categorías principales de riesgos:

- Interrupción de servicios: La falla de energía es un ejemplo de interrupción de servicios críticos que son vitales para las operaciones comerciales de una organización. Los daños en el hardware son un ejemplo de pérdida de servicios informáticos.
- Robo físico: El robo físico no solo equivale a la pérdida de un activo, sino que también conduce a la divulgación no autorizada de información.

Un ataque de denegación de servicio (DoS) y un ataque de suplantación de IP son amenazas basadas en la red y no suponen un riesgo para la seguridad física.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Plan de Seguridad Física

---

Question #153 of 193

Question ID: 1192935

Usted es el administrador de seguridad de una organización. La administración decide que toda la comunicación en la red debe cifrarse mediante el algoritmo de estándar de cifrado de datos (DES). ¿Qué afirmación es cierta de este algoritmo?

✗ **A)** El tamaño de clave efectivo de DES es de 64 bits.

✗ **B)** Un cifrado DES de 56 bits es 256 veces más seguro que un cifrado DES de 40 bits.

✗ **C)** Un algoritmo DES utiliza 32 rondas de cálculo.

✓ **D)** Un algoritmo Triple DES (3DES) utiliza 48 rondas de cálculo.

explicación

Un algoritmo Triple DES (3DES) utiliza 48 rondas de cálculo. Ofrece una alta resistencia al criptoanálisis diferencial porque utiliza muchas rondas. El proceso de cifrado y descifrado realizado por 3DES tarda más tiempo debido a la mayor potencia de procesamiento requerida.

El tamaño de clave real del Estándar de cifrado de datos (DES) es de 64 bits. Un tamaño de clave de 8 bits se utiliza para una comprobación de paridad. Por lo tanto, el tamaño de clave efectivo de DES es de 56 bits

El algoritmo DES utiliza 16 rondas de cálculo. El orden y el tipo de cálculos realizados dependen del valor proporcionado al algoritmo a través de los bloques de cifrado.

Según el siguiente cálculo, un cifrado DES de 56 bits es 65.536 veces más seguro que un cifrado DES de 40 bits:

240 = 1099511627776 y 256 = 72057594037927936

Por lo tanto, 72057594037927936 divide por 1099511627776 = 65.536.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Estándar de cifrado digital (DES) y Triple DES (3DES)

Question #154 of 193

Question ID: 1111717

¿Qué afirmación es cierta de FIPS 140?

- ✗ **A)** FIPS se ocupa de los productos de hardware.
- ✗ **B)** FIPS sólo se ocupa de software criptográfico.
- ✗ **C)** FIPS no valida el software para ser utilizado por las agencias gubernamentales.
- ✓ **D)** FIPS especifica los requisitos de seguridad para los módulos criptográficos de hardware y software.

explicación

La Publicación 140 de los Estándares Federales de Procesamiento de Información (FIPS) es un estándar federal de los Estados Unidos que especifica los requisitos de seguridad para los módulos criptográficos de hardware y software. Los requisitos publicados por el Instituto Nacional de Estándares y Tecnología (NIST) se aplican no solo a los módulos

criptográficos, sino también a la documentación correspondiente. El uso de módulos criptográficos de hardware y software es requerido por los Estados Unidos para toda implementación no clasificada de criptografía.

The four increasing levels of security in FIPS are as follows:

- Level 1 requires very limited security requirements and specifies that all components must be production grade.
- Level 2 specifies the security requirements of role-based authentication and physical tamper evidence.
- Level 3 requires identity-based authentication and physical tamper resistance, making it difficult for attackers.
- Level 4 specifies robustness against environmental attacks.

It is important to note that FIPS not only deals in cryptographic software but also in hardware modules. The U.S. Government and other prominent institutions use the hardware and software modules validated by FIPS 140.

The FIPS 140-1 and FIPS 140-2 validation certificates that are issued contain the following elements:

- nombre del módulo
- tipo de módulo, es decir, hardware, software y firmware
- Versión

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura de seguridad y prácticas de gestión de claves de ingeniería

Criptografía de sistema: use algoritmos compatibles con FIPS para cifrado, hash y firma, http://technet2.microsoft.com/WindowsServer/en/Library/6ff574cb-30c4-4ad9-8d5e-aee697c65b9b1033.mspx

---

Question #155 of 193

Question ID: 1111730

¿Qué práctica de seguridad NO aborda la protección física y ambiental de una instalación?

✗ **A)** Los sistemas de alerta de inundaciones se actualizan una vez al año.

✗ **B)** Los códigos de entrada en la instalación se cambian a intervalos regulares.

✗ **C)** La entrada y salida a la instalación son monitoreadas continuamente por CCTVs.

✓ **D)** Se adoptan medidas para impedir el robo de información por parte de personas no autorizadas.

explicación

Las medidas adoptadas para prevenir el robo de información, ya sea mediante la lectura, copia o alteración de información por parte de personas no autorizadas, no son efectivas para acceder a la protección física y ambiental de una instalación.

Las medidas para acceder a la protección física y ambiental de una instalación pueden incluir la siguiente información:

- Los sistemas de alerta de inundaciones se actualizan a intervalos regulares.
- Los códigos de entrada en la instalación se cambian a intervalos regulares.
- La entrada y salida de la instalación son monitoreadas continuamente por televisores de circuito cerrado (CCTVs).

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, controles de seguridad de sitios e instalaciones

---

Question #156 of 193

Question ID: 1105055

¿Qué tecnología requiere hardware del Módulo de plataforma segura (TPM)?

✗ **A)** IPSec
✗ **B)** NTFS
✓ **C)** BitLocker
✗ **D)** Efs

explicación

El cifrado de unidad BitLocker requiere hardware TPM. La tecnología BitLocker cifra el contenido de la unidad para que no se puedan robar datos. BitLocker puede cifrar archivos de usuario y de sistema. Un administrador habilita o deshabilita BitLocker para todos los usuarios del equipo.

Ninguna de las otras opciones requiere hardware tpm. El Sistema de cifrado de archivos (EFS) cifra el contenido de un disco. Sin embargo, EFS está habilitado por usuario y solo puede cifrar archivos que pertenecen al usuario que habilita EFS. EFS no requiere ninguna configuración administrativa o de hardware especial.

New Technology File System (NTFS) es el sistema de archivos de 32 bits utilizado por los sistemas operativos Windows.

El protocolo de seguridad de Internet (IPSec) es un protocolo que protege la comunicación a través de una red.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Módulo de plataforma segura (TPM)

Question #157 of 193

Question ID: 1104989

Su organización ha decidido implementar la computación en la nube y ha configurado la plataforma como servicio (PaaS) con un proveedor de nube. ¿Cuál es el enfoque principal de este tipo de implementación en la nube?

- ✗ **A)** administración de máquinas virtuales
- ✗ **B)** control de acceso
- ✓ **C)** protección de datos
- ✗ **D)** administración de acceso a aplicaciones

explicación

El enfoque principal de una implementación de computación en la nube de plataforma como servicio (PaaS) es la protección de datos.

El enfoque principal de una implementación de computación en la nube de software como servicio (SaaS) es la administración de acceso a aplicaciones.

El enfoque principal de una implementación de computación en la nube de infraestructura como servicio (IaaS) es la administración de máquinas virtuales.

Ninguna de las implementaciones de computación en la nube tiene el control de acceso como foco principal.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
evaluar y mitigar las vulnerabilidades de las arquitecturas de seguridad, los diseños y los elementos de la solución

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, sistemas basados en la nube

SaaS, PaaS e IaaS: una lista de comprobación de seguridad para modelos en la nube, http://www.csoonline.com/article/660065/saas-paas-and-iaas-a-security-checklist-for-cloud-models

---

Question #158 of 193

Question ID: 1104998

¿Cuál de los siguientes NO es una contramedida para mitigar los ganchos de mantenimiento?

✗ **A)** Cifrar toda la información confidencial contenida en el sistema.

✗ **B)** Utilice un IDS basado en host para registrar cualquier intento de acceder al sistema mediante uno de estos enlaces.

✗ **C)** Implemente la auditoría para complementar el IDS.

✓ **D)** Asegúrese de que si los conjuntos críticos de instrucciones no se ejecutan en orden y en su totalidad, los cambios que realizan se revierten o se impiden.

explicación

Una contramedida para mitigar los enlaces de mantenimiento NO incluye asegurarse de que los conjuntos críticos de instrucciones se ejecuten en orden y en su totalidad, o que se revierta o se impida realizar cambios. Esta es una técnica válida, pero es una mitigación para los ataques de tiempo de comprobación/tiempo de uso.

Todas las demás contramedidas enumeradas son para mitigar los ganchos de mantenimiento.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Evaluar y mitigar las vulnerabilidades en los sistemas basados en la web

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Vulnerabilidades en sistemas basados en web

---

Question #159 of 193

Question ID: 1105024

¿Cuál es otro término para la fuerza de criptografía?

- ✗ **A)** vector de inicialización
- ✗ **B)** clave pública
- ✓ **C)** factor de trabajo
- ✗ **D)** clave privada

explicación

Factor de trabajo es otro término para la fuerza de criptografía. El factor de trabajo es la cantidad de esfuerzo y recursos que se necesitarían para romper un criptosistema. Cuanto más esfuerzo y recursos se necesitarían para descifrar el criptosistema, menos probable es que se produzca un ataque de este tipo.

La clave pública de un criptosistema está disponible para cualquier persona.

La clave privada de un criptosistema es conocida solo por el propietario.

Un vector de inicialización es un valor aleatorio que se utiliza con el algoritmo para asegurarse de que los patrones no se producen durante el proceso de cifrado.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Factor de Trabajo [Seguridad Nacional] Ley y Definición Legal

---

Question #160 of 193

Question ID: 1105096

Su organización está utilizando el enfoque de prevención de delitos a través del diseño ambiental (CPTED) para asegurarse de que su sitio está diseñado correctamente. ¿Qué faceta de este enfoque incluye la puerta, la cerca, la iluminación y la colocación de paisajes?

- ✗ **A)** endurecimiento de objetivos
- ✗ **B)** vigilancia natural
- ✗ **C)** refuerzo territorial

✓ **D)** control de acceso natural

explicación

El control de acceso natural en el enfoque CPTED incluye la colocación de puertas, cercas, iluminación y paisajismo. Este control garantiza que se controla el tráfico.

La vigilancia natural en el enfoque CPTED incluye guardias de seguridad, circuito cerrado de televisión (CCTV), línea de visión, paisajismo bajo y entradas elevadas. La principal preocupación de esta faceta es garantizar que los delincuentes se sientan incómodos haciendo un ataque.

El refuerzo territorial en el enfoque CPTED incluye muros, cercas, paisajismo, iluminación, banderas y aceras que enfatizan o amplían el área de influencia de la compañía para que los usuarios sientan que son dueños del área.

El endurecimiento del objetivo no forma parte de CPTED. Es otro enfoque de la seguridad física, que hace hincapié en negar el acceso a través de barreras físicas y artificiales. El mejor enfoque es crear un entorno utilizando el enfoque CPTED y luego aplicar el endurecimiento del objetivo sobre el diseño CPTED.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar principios de seguridad al diseño de sitios e instalaciones

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, CPTED

Question #161 of 193

Question ID: 1105042

¿Qué produce las sumas de comprobación de 160 bits?

✗ **A)** Aes
✗ **B)** DES
✗ **C)** MD5
✓ **D)** Sha

explicación

El algoritmo hash seguro (SHA) genera sumas de comprobación de 160 bits.

El estándar de cifrado avanzado (AES) utiliza claves de cifrado de 128 bits, 192 bits y 256 bits y tamaños de bloque de 128 bits. El algoritmo MD5 produce sumas de comprobación de 128 bits y el estándar de cifrado de datos (DES) utiliza

claves de cifrado de 56 bits.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, SHA/SHA-2/SHA-3

Question #162 of 193

Question ID: 1132516

¿Qué ataque envía mensajes no solicitados a través de una conexión Bluetooth?

- ✓ **A)** jacking azul
- ✗ **B)** spamming
- ✗ **C)** bluesnarfing
- ✗ **D)** conducción de guerra

explicación

Blue jacking es un ataque que envía mensajes no solicitados a través de una conexión Bluetooth. Se puede considerar spam en un entorno Bluetooth.

Bluesnarfing es el acto de obtener acceso no autorizado a un dispositivo (y la red a la que está conectado) a través de su conexión Bluetooth.

La conducción de guerra es el acto de descubrir una red inalámbrica desprotegida conduciendo con una computadora portátil.

El spamming es el acto de enviar mensajes de correo electrónico no solicitados a través de un servidor de correo.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
evaluar y mitigar las vulnerabilidades de las arquitecturas de seguridad, los diseños y los elementos de la solución

Referencias:

Bluejacking, http://searchmobilecomputing.techtarget.com/sDefinition/0,sid40_gci961342,00.html

---

Question #163 of 193

Question ID: 1113942

¿Qué NO es un componente de una tarjeta de detección del sistema de transpondedor?

- ✓ **A)** espectro ensanchado
- ✗ **B)** transmisor
- ✗ **C)** batería
- ✗ **D)** receptor

explicación

El espectro ensanchado no es un componente de una tarjeta de detección del sistema de transpondedor. El espectro ensanchado es una parte de la tecnología inalámbrica.

Los lectores de proximidad pueden ser lectores activados por el usuario o de detección del sistema. Si el lector de proximidad está activado por el usuario, el usuario desliza la tarjeta y proporciona un número de secuencia válido como credenciales de acceso al lector. Esto concede al usuario acceso autorizado a la instalación. En un lector de proximidad de detección de sistema, el usuario no necesita realizar ninguna acción ni proporcionar credenciales. El sistema de control de acceso detecta automáticamente la presencia del usuario en un área especificada y autentica al usuario en función de las credenciales transmitidas al lector. El lector envía las credenciales de usuario a un servidor de autenticación para su procesamiento.

Las tarjetas de detección de sistemas se clasifican en las siguientes categorías:

- Los transpondedores tienen un receptor, un transmisor, un lugar para almacenar el código de acceso y una batería. Después de una solicitud de autenticación del lector, la tarjeta envía un código de acceso al lector y se le concede acceso autorizado al área de la instalación. Las tarjetas transpondedores se pueden leer sin deslizar la tarjeta a través de un lector de tarjetas.
- Los dispositivos pasivos utilizan la energía del lector. El lector transmite un campo electromagnético que es percibido por el dispositivo pasivo para garantizar la autenticación de credenciales de usuario.
- Los dispositivos alimentados por campo tienen su propia fuente de alimentación, y la tarjeta no depende del lector para la alimentación.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

¿Qué es un transpondedor RFID?, http://www.sag.com.tw/index.php?_Page=msg&md=support&pid=10

Question #164 of 193

Question ID: 1105051

Dados dos mensajes, M1 y M2, ¿cuál es el resultado menos probable cuando se utiliza la misma función hash unidireccional, H, para cifrar los mensajes?

✗ **A)** H(M1) > H(M2)

✗ **B)** H(M1) no es igual a H(M2)

✓ **C)** H(M1) = H(M2)

✗ **D)** H(M1) < H(M2)

explicación

Cuando se utiliza la misma función hash unidireccional para cifrar dos mensajes diferentes, es el resultado menos probable que H(M1) = H(M2). Cuando se aplica una función hash a dos mensajes diferentes, es poco probable que los dos valores hash resultantes sean los mismos. Esto significa que es computacionalmente inviable que dos mensajes tengan el mismo valor hash. Debido a esto, los hashes unidireccionales están libres de colisiones.

Todas las demás opciones tienen más probabilidades de ocurrir que los dos resultados serán los mismos.

Para una función hash criptográfica, H(M) es relativamente fácil de calcular para un mensaje determinado. Las funciones hash generan un resultado de longitud fija que es independiente de la longitud del mensaje de entrada. Las funciones unidireccionales son difíciles o imposibles de invertir.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Hash unidireccional

Funciones hash seguras unidireccionales,
http://www.cs.bham.ac.uk/~mdr/teaching/modules/security/lectures/hash.html

---

Question #165 of 193

Question ID: 1192927

Usted es responsable de administrar el entorno de virtualización de su empresa. ¿Qué característica NO se debe permitir en un host de virtualización?

✗ **A)** implementar IPsec

✗ **B)** implementar un firewall

✗ **C)** Supervisar los registros de sucesos

✓ **D)** navegar por Internet

explicación

No debe permitir la exploración de Internet en un host de virtualización. Esto puede presentar una posible brecha de seguridad a través de la introducción de spyware o malware. Todo lo que afecte a un host de virtualización también afecta a todos los equipos virtuales del host.

Debe implementar IPsec, implementar un firewall y supervisar los registros de eventos de un host de virtualización. IPsec ayuda cifrando los datos a medida que se transmiten a través de la red. Los firewalls impiden el acceso no autorizado a un equipo físico o virtual. Los registros de eventos ayudan a los administradores a detectar cuándo se han producido o se están intentando realizar infracciones de seguridad.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
evaluar y mitigar las vulnerabilidades de las arquitecturas de seguridad, los diseños y los elementos de la solución

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, virtualización

Seguridad y Virtualización, HYPERLINK "http://techgenix.com/security-virtualization/" \t "sean" http://www.windowsecurity.com/articles/Security-Virtualization.html

---

Question #166 of 193

Question ID: 1192938

¿Qué métodos de supresión se recomiendan cuando el papel, los laminados y los muebles de madera son los elementos de un incendio en la instalación?

un. Halón

B. Agua

c. Ácido sódico

d. Polvo seco

- ✗ **A)** Opciones C y D
- ✗ **B)** opción b
- ✗ **C)** Opción d
- ✗ **D)** opciones A y B
- ✓ **E)** Opciones B y C
- ✗ **F)** opción A
- ✗ **G)** opción c

explicación

El agua o el ácido de soda se deben utilizar para suprimir un fuego que tenga productos de madera, laminados y papel como elementos. El método de supresión debe basarse en el tipo de incendio en la instalación. La sustancia de supresión debe interferir con los elementos del fuego. Por ejemplo, el ácido sódico elimina el combustible mientras que el agua reduce la temperatura. El agua o el ácido de soda se utiliza para extinguir incendios de clase A.

El cableado eléctrico y las cajas de distribución son la causa más probable de incendios en los centros de datos. Los agentes de extinción de incendios de clase C, como halones o dióxido de carbono, se utilizan cuando el fuego involucra equipos eléctricos y cables. También se pueden utilizar para suprimir incendios de Clase B que incluyen líquidos, como productos derivados del petróleo y refrigerantes. Nunca use agua en un incendio de Clase B.

La producción de gas halón fue prohibida por el Protocolo de Montreal en 1987. El halón causa daños a la capa de ozono y es perjudicial para los seres humanos. El tratado requiere que los proveedores que ya tienen extintores de halones obtengan los extintores rellenados con reemplazos, como FM-200, aprobado por la Agencia de Protección Ambiental (EPA). Los agentes de halocarbono o agentes de gas inerte pueden ser sustitutos de Halon 1301 y Halon 1211 en sistemas de extinción de incendios de descarga de gas. Los agentes de halocarbono contienen uno o más compuestos orgánicos como componentes primarios, como los elementos flúor, cloro, bromo o yodo. Los agentes gaseosos inertes contienen como componentes primarios uno o más de los gases helio, neón, argón o nitrógeno. Algunos agentes gaseosos inertes también contienen dióxido de carbono como componente secundario. Los agentes de halocarbono son hidrofluorocarbonos (HFC), hidroclorofluorocarbonos (HCFC), perfluorocarbonos (PFC o FCs) o fluoroiodocarbonos (FICs). Los agentes de gas inerte comunes para los sistemas de extinción de incendios son IG-01, IG-100, IG-55 e IG-541. Los agentes de halocarbono crean niveles tóxicos de fluoruro de hidrógeno (HF).

El dióxido de carbono, también utilizado para extinguir incendios de clase B y C, elimina el oxígeno. El dióxido de carbono es perjudicial para los seres humanos y debe utilizarse en instalaciones desatendidas.

El polvo seco es un método de supresión para un fuego que tiene magnesio, sodio y potasio como sus elementos. El polvo seco extingue los incendios de clase D. Aunque el polvo seco también puede suprimir los incendios de Clase B y

C, las compañías comúnmente utilizan otras formas de supresión para incendios de Clase B y C. El único método de supresión de metales combustibles es el polvo seco.

Un sistema de extinción de incendios limpio no deja un residuo en las piezas electrónicas después de la evaporación. Un agente limpio se define como un extintor de incendios eléctricamente no conductor y no volátil que no deja un residuo en la evaporación. IG-55 e IG-01 son agentes de gas inerte de agente limpio que no se descomponen mensurablemente ni dejan descomposición corrosiva. El HCFC-22 es un agente de halocarbono que es un agente limpio.

El CO2 deja un residuo corrosivo. NO es un agente limpio y, por lo tanto, no se recomienda para los sistemas de extinción de incendios de instalaciones informáticas.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, extinción de incendios

---

Question #167 of 193

Question ID: 1105062

¿Qué algoritmo hash fue diseñado para ser utilizado con el Estándar de Firma Digital (DSS)?

- ✗ **A)** Resumen del mensaje 5 (MD5)
- ✗ **B)** HAVAL
- ✓ **C)** Algoritmo hash seguro (SHA)
- ✗ **D)** tigre

explicación

El algoritmo hash seguro (SHA) fue diseñado para ser utilizado con el DSS. Con este algoritmo, se introduce un mensaje de menos de 264 bits a SHA. El resumen del mensaje resultante de 160 bits se introduce en el algoritmo de firma digital (DSA), que genera la firma digital del mensaje.

Ninguno de los otros algoritmos hash se diseñó para su uso con DSS.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, SHA/SHA-2/SHA-3

Question #168 of 193

Question ID: 1104990

Su empresa hospeda varios sitios Web públicos en su servidor Web. Algunos de los sitios implementan el protocolo de capa de sockets seguros (SSL). ¿Qué afirmación NO es cierta de este protocolo?

- ✓ **A)** SSL opera en la capa de red del modelo OSI.
- ✗ **B)** SSL versión 2 proporciona autenticación del lado cliente.
- ✗ **C)** SSL se utiliza para proteger las transacciones de Internet.
- ✗ **D)** SSL tiene dos longitudes de clave de sesión posibles: 40 bits y 128 bits.
- ✗ **E)** SSL con TLS admite la autenticación de servidor y cliente.

explicación

El protocolo secure sockets layer (SSL) funciona en la capa de transporte del modelo OSI. Funciona junto con el Protocolo de transferencia de hipertexto (HTTP), que funciona en la capa de sesión para proporcionar conexiones HTTP seguras.

SSL se utiliza para proteger las transacciones de Internet. Fue desarrollado por Netscape. Cuando se utiliza SSL, la dirección del explorador tendrá el prefijo https://, en lugar del prefijo http://. Permite que una aplicación tenga comunicaciones autenticadas y cifradas a través de una red.

SSL versión 2 proporciona autenticación del lado cliente.

SSL con TLS admite la autenticación de servidor y cliente. SSL utiliza el cifrado de clave pública y proporciona cifrado de datos y autenticación de servidor. Para habilitar SSL para que funcione, el servidor y el explorador cliente deben tener SSL habilitado.

SSL tiene dos longitudes de clave de sesión posibles: 40 bits y 128 bits.

Una implementación común de SSL/TLS es la seguridad de la capa de transporte inalámbrica (WTLS) para redes inalámbricas. La transmisión WTLS es necesaria para atravesar redes cableadas e inalámbricas. Por lo tanto, los paquetes que se descifran en la puerta de enlace deben volver a cifrarse con SSL para su uso a través de redes cableadas. Ésta es una laguna de seguridad que se refiere como el problema de seguridad de la brecha WAP.

Si se está utilizando SSL para cifrar los mensajes que se transmiten a través de la red, una de las principales preocupaciones del profesional de la seguridad son las redes que viajará el mensaje que la empresa no controla.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
evaluar y mitigar las vulnerabilidades de las arquitecturas de seguridad, los diseños y los elementos de la solución

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, SSL/TLS

Question #169 of 193

Question ID: 1114706

Ha sido contratado como administrador de seguridad. La administración le informa de que la red utiliza el cifrado SKIP. ¿Qué afirmación es cierta de este protocolo?

- ✓ **A)** SKIP es un protocolo de distribución de claves.
- ✗ **B)** SKIP funciona en función de la respuesta por sesión.
- ✗ **C)** SKIP es sólo un protocolo de almacenamiento de claves.
- ✗ **D)** SKIP implementa IKE para la distribución y administración de claves.

explicación

El Protocolo simple de administración de claves para protocolos de Internet (SKIP) es un protocolo de administración y distribución de claves que se usa para la comunicación IP segura, como el Protocolo de seguridad de Internet (IPSec). SKIP utiliza el cifrado híbrido para transmitir claves de sesión. Estas claves de sesión se utilizan para cifrar datos en paquetes IP. SKIP utiliza un algoritmo de intercambio de claves, como el algoritmo Diffie-Hellman, para generar una clave de cifrado de claves que se utilizará entre dos partes. Una clave de sesión se utiliza con un algoritmo simétrico para cifrar los datos.

SKIP no es un protocolo de almacenamiento de claves. Es un protocolo de distribución y administración de claves similar al intercambio de claves de Internet (IKE).

SKIP funciona sesión por sesión, aunque no requiere comunicación previa para el establecimiento de sesiones. SKIP emplea estándares de cifrado, como el Estándar de cifrado de datos (DES) y Triple DES (3DES), para proporcionar una comunicación segura.

SKIP no implementa IKE para la distribución y administración de claves. IKE es un marco separado utilizado para intercambiar claves de forma segura para establecer una sesión IPSec.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Una visión general de los algoritmos criptográficos de criptografía en acción

http://www.garykessler.net/library/crypto.html

Question #170 of 193

Question ID: 1105048

¿Cuál de los siguientes NO se basa en el cifrado Feistel?

- ✗ **A)** REPARTO-128
- ✓ **B)** Diffie-Hellman
- ✗ **C)** pez globo
- ✗ **D)** listado

explicación

Diffie-Hellman NO se basa en el cifrado Feistel. El cifrado Feistel es un sistema simétrico. Diffie-Hellman es un sistema asimétrico.

El cifrado Feistel es un cifrado de bloques iterado que cifra dividiendo el bloque de texto plano en dos mitades. A continuación, el cifrado aplica una transformación a uno de los reducidos a la mitad con una subclave. El resultado de esta transformación es XORed con la mitad restante. La ronda se completa intercambiando las dos mitades. La mayoría de los sistemas simétricos se basan en Feistel, incluyendo Skipjack, Blowfish, CAST-128, DES, 3DES, GOST, RC2 y RC6.

El Gamal es una extensión de Diffie-Hellman. Diffie-Hellman y RSA forman parte de los estándares de criptografía de clave pública (PKCS) desarrollados por RSA Laboratories.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Lucifer por IBM

Cifrado feistel, http://cryptography.wikia.com/wiki/Feistel_cipher

---

Question #171 of 193

Question ID: 1105093

Las nuevas instalaciones de su organización deben estar construidas con material resistente al fuego. ¿Qué material se debe utilizar en su construcción del marco?

- ✗ **A)** acero
- ✗ **B)** madera pesada con una calificación de fuego de una hora
- ✓ **C)** varillas de acero encerradas en muros de hormigón
- ✗ **D)** madera no tratada

explicación

Las varillas de acero encerradas en paredes de hormigón se consideran materiales resistentes al fuego. El término resistente al fuego es un estándar utilizado para determinar la seguridad contra incendios de una sala de computadoras. La calificación resistente al fuego de los materiales de construcción es un factor importante en la determinación de la seguridad contra incendios de una sala de operaciones informáticas. El término resistente al fuego se refiere a materiales o edificios que tienen una calificación de resistencia al fuego de no menos de la norma especificada.

La madera no tratada es combustible. Se utiliza en la construcción de marcos de luz de viviendas.

La madera pesada con una tasa de fuego de una hora es combustible. Se utiliza en la construcción de marcos pesados. A menudo utiliza maderas densas de al menos cuatro pulgadas de espesor con pernos y placas de metal.

El acero no es combustible. Se utiliza en la construcción incombustible. Sin embargo, el acero puede perder su fuerza en un incendio, causando el colapso de un edificio.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar principios de seguridad al diseño de sitios e instalaciones

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Construcción

---

Question #172 of 193

Question ID: 1105021

¿Qué servicio proporcionado por un criptosistema es más importante para los militares?

✗ **A)** integridad

✗ **B)** norepudiation

✓ **C)** confidencialidad

✗ **D)** autenticación

explicación

La confidencialidad es el servicio más importante proporcionado por un criptosistema para los militares.

La integridad y confidencialidad es importante para las instituciones financieras. La integridad garantiza que los datos no se han cambiado.

La no devolución es importante si una agencia debe asegurarse de que el remitente no puede negar el envío del mensaje.

La autenticación es importante en la corte porque confirma quién envió el mensaje.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Confidencialidad

---

Question #173 of 193

Question ID: 1114711

El equipo tiene la tarea de identificar un sitio seguro para la infraestructura de instalaciones de una organización. ¿Qué opción representa las consideraciones de visibilidad involucradas en este proceso?

a. Iluminación

b. tipos de vecinos

c. controles medioambientales

d. Marcas y señales de edificios

e) Circuito cerrado de televisión (CCTV)

- ✗ **A)** opción e
- ✗ **B)** Opciones A y C
- ✗ **C)** opción A
- ✗ **D)** opción b
- ✗ **E)** opciones B y E
- ✗ **F)** Opción d
- ✗ **G)** opción c
- ✓ **H)** Opciones B y D

explicación

La visibilidad es una de las consideraciones implicadas en la identificación de una ubicación segura para la planificación de requisitos de la instalación. En las consideraciones de visibilidad, se identifican los tipos de vecinos alrededor de la ubicación elegida y se considera si la ubicación identificada debe marcarse como un área de proceso sensible para evitar la intrusión. Las otras consideraciones de visibilidad son las siguientes:

- Terreno circundante: Dependiendo de los requisitos de seguridad, la instalación puede ubicarse en valles montañosos para evitar el aprovechamiento de señales de comunicación y ocultar la identidad. Las colinas circundantes pueden ser naturales o creadas artificialmente. La instalación se puede disfrazar para que coincida con el terreno circundante.
- Población de la zona: Por lo general, las instalaciones ubicadas en un área de bajos ingresos o densamente poblada requerirían un mayor nivel de seguridad física y perimetral.

Además de la visibilidad, también se deben considerar otros problemas importantes de seguridad para las áreas circundantes, la accesibilidad y los desastres naturales. Las consideraciones de seguridad para las áreas circundantes incluyen cuestiones como la tasa de criminalidad de la zona y la proximidad a la policía, los bomberos y los servicios médicos.

Las consideraciones de accesibilidad incluyen el flujo de tráfico y la proximidad a autopistas, estaciones de tren y aeropuertos. Las consideraciones de seguridad para desastres naturales deben analizarse para ver si hay posibilidad de inundaciones, tornados, terremotos, huracanes y terrenos peligrosos, como deslizamientos de tierra, caída de rocas de montañas o nevadas excesivas.

El propósito principal de identificar una ubicación segura es tener un grado de visibilidad, ya sea alto o bajo, dependiendo de los requisitos empresariales de la organización. Las organizaciones que procesan datos confidenciales o confidenciales pueden preferir una visibilidad baja, mientras que otras pueden preferir una visibilidad alta.

El circuito cerrado de televisión (CCTV) y la iluminación forman parte de los controles físicos de seguridad, pero no forman parte de la planificación de la infraestructura de las instalaciones. Los controles ambientales se refieren a los

controles implementados por una organización para hacer frente a peligros y amenazas, como incendios, inundaciones y terremotos.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Visibilidad

---

Question #174 of 193

Question ID: 1111734

El centro de datos secundario de su empresa experimentó recientemente un incendio. Los equipos electrónicos del centro de datos han estado expuestos tanto al agua como al humo. Debe asegurarse de que todos los equipos se limpien correctamente. Todo el equipo ha sido apagado. También ha abierto todos los gabinetes, paneles y cubiertas para permitir que el agua fluya hacia afuera. ¿Qué debes hacer a continuación?

✗ **A)** Limpie con alcohol o soluciones de freón-alcohol, o rocíe con aerosoles de desplazamiento de agua.

✗ **B)** Utilice los solventes del freón o del Freón-alcohol para rociar los conectores, los backplanes, y las placas de circuito impreso.

✗ **C)** Aerosol inhibidor de la corrosión por pulverización para estabilizar las superficies de contacto del metal.

✓ **D)** Mueva todo el equipo a un ambiente con controles adecuados de temperatura y humedad.

explicación

Debe mover todo el equipo a un entorno con controles adecuados de temperatura y humedad.

La exposición al humo durante un incendio durante un período relativamente corto hace poco daño inmediato. La alimentación continua del equipo expuesto al humo o al agua puede aumentar el daño. La humedad y la corrosión por oxígeno constituyen el principal daño al equipo.

Para eliminar los contaminantes de humo del equipo, debe completar los siguientes pasos:

- Apague la alimentación del equipo.
- Mueva todo el equipo a un ambiente con controles adecuados de temperatura y humedad.

- Utilice los solventes del freón o del Freón-alcohol para rociar los conectores, los backplanes, y las placas de circuito impreso.
- Aerosol inhibidor de la corrosión por pulverización para estabilizar las superficies de contacto del metal.

Para eliminar el agua del equipo, debe completar los siguientes pasos:

- Apague toda la energía eléctrica al equipo. Abra las puertas de los gabinetes y quite los paneles y las cubiertas para permitir que el agua fluya hacia fuera.
- Mueva todo el equipo a un ambiente con controles adecuados de temperatura y humedad.
- Limpie con alcohol o soluciones de freón-alcohol o rocíe con aerosoles de desplazamiento de agua.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Implementar controles de seguridad del sitio y de la instalación

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura de seguridad e ingeniería secure data center

---

Question #175 of 193

Question ID: 1104964

¿Qué afirmación es cierta para el direccionamiento indirecto de memoria?

✓ **A)** El campo de dirección apunta a una celda de memoria que contiene la dirección del operando.

✗ **B)** El campo de dirección contiene la dirección del operando.

✗ **C)** Se utiliza un único acceso a memoria para buscar el operando.

✗ **D)** No tiene ninguna referencia de memoria para capturar datos.

explicación

El campo de dirección en el direccionamiento indirecto de memoria, apunta a una celda de memoria que contiene la dirección del operando. Este es el tipo de direccionamiento de memoria donde la ubicación de dirección que se especifica en la instrucción de programa contiene la dirección de la ubicación final deseada. El direccionamiento indirecto utiliza un gran espacio de direcciones y realiza varios accesos a memoria para buscar el operando. Esto hace que el direccionamiento indirecto sea más lento que el direccionamiento directo.

La opción que indica que no hay ninguna referencia de memoria en el direccionamiento indirecto es incorrecta. Las referencias de memoria no están presentes en el direccionamiento inmediato, donde el operando forma parte de la

instrucción. Aunque el direccionamiento en el direccionamiento inmediato es rápido, tiene un rango limitado.

Las opciones que indica que se utiliza un único acceso a memoria para buscar el operando y el campo de dirección contiene la dirección del operando son incorrectas. Es en el direccionamiento directo que se utiliza un único acceso a memoria para encontrar el operando y el campo de dirección contiene la dirección del operando. Por lo tanto, en el direccionamiento directo, no se necesitan cálculos adicionales para calcular la dirección efectiva del operando. El inconveniente del direccionamiento directo es el espacio de direcciones limitado.

La CPU utiliza direcciones absolutas. Las aplicaciones utilizan direcciones lógicas. Las direcciones relativas se basan en una dirección conocida y un valor de desplazamiento.

Objetivo:
Arquitectura e ingeniería de seguridad

Sub-Objective:
Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)

References:

CISSP Cert Guide (3rd Edition), Chapter 3: Security Architecture and Engineering, Indirect addressing

Address space and addressing modes, http://www.osdata.com/topic/language/asm/address.htm

---

Question #176 of 193

Question ID: 1104996

What is a rootkit?

- ✗ **A)** an application that uses tracking cookies to collect and report a user's activities
- ✗ **B)** a software application that displays advertisements while the application is executing
- ✗ **C)** a program that spreads itself through network connections
- ✓ **D)** a collection of programs that grants a hacker administrative access to a computer or network

Explanation

A rootkit is a collection of programs that grants a hacker administrative access to a computer or network. The hacker first gains access to a single system, and then uploads the rootkit to the hacked system.

Adware is a software application that displays advertisements while the application is executing. Some adware is also spyware if it monitors your Internet usage and personal information. Some adware will even allow credit card

information theft.

Spyware often uses tracking cookies to collect and report a user's activities. Not all spyware is adware, and not all adware is spyware. To define a program as spyware requires that your activities are monitored and tracked; to define a program as adware requires that advertisements are displayed.

A worm is a program that spreads itself through network connections.

Objective:
Security Architecture and Engineering

Sub-Objective:
Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

References:

CISSP Cert Guide (3rd Edition), Chapter 8: Software Development Security, Rootkit

---

Question #177 of 193

Question ID: 1105036

Which binary function is the basis of the functioning of a one-time pad?

✗ **A)** AND
✓ **B)** XOR
✗ **C)** XAND
✗ **D)** OR

Explanation

The binary function exclusive-OR (XOR) is performed as a part of the one-time pad functioning.

None of the other binary functions is the basis of a one-time pad's functioning.

A one-time pad is an encryption scheme that uses a non-repeating set of random bits to encrypt the message. The message bits are XORed to the bits in the pad to generate ciphertext. This ensures that encrypted messages are almost impossible to decrypt because each value is replaced by a non-repeating set of random values. The random pad or key should be at least the same size as the message. A randomly generated pad is used only once to encrypt the message. The receiving party decrypts the message by using the matching one-time pad and the key. The advantage of the one-time pad is that it is almost impossible to decrypt the message by analyzing the messages. This is because the encryption for each message is unique and is performed only once. This prevents detection of a pattern in the messages.

The problem with a one-time pad is the maintenance of key management and performance. Each party communicating with another party will require a one-time pad. Therefore, key management can be overwhelming.

The pad is as long as the message. This renders the processing required almost impractical for commercial applications.

Objective:
Security Architecture and Engineering

Sub-Objective:
Apply cryptography

References:

CISSP Cert Guide (3rd Edition), Chapter 3: Security Architecture and Engineering, Logical Operations (And, Or, Not, Exclusive Or)

Question #178 of 193

Question ID: 1113930

Un cliente ha solicitado un ordenador con un chip Clipper. ¿Qué es un chip Clipper?

- ✗ **A)** Es un chip de módem.
- ✓ **B)** Es un chip de cifrado.
- ✗ **C)** Es un número de serie único en el chip de la computadora.
- ✗ **D)** Es un algoritmo de cifrado.

explicación

El chip Clipper es un chip de cifrado basado en el algoritmo Skipjack. Fue diseñado por el Gobierno de los Estados Unidos para ser utilizado en dispositivos como computadoras y módems que podrían usar cifrado. El chip fue diseñado para la vigilancia de las actividades enemigas. El Escrowed Encryption Standard (EES) describe el chip Clipper.

La clave de unidad del chip Clipper cifra y descifra la clave de sesión, pero el mensaje no se cifra mediante la clave de unidad. Los mensajes se cifran mediante la clave de sesión, que de nuevo se cifra y se descifra mediante la clave de unidad. Por lo tanto, el chip Clipper consta de una tecla de unidad y una clave de sesión. El chip Clipper tiene los siguientes componentes:

- Un número de serie único en la base de datos
- Una copia de la clave de unidad correspondiente al número de serie de la base de datos

El valor de Campo de acceso a la aplicación de la ley (LEAF) se incluye en el mensaje cifrado enviado por el chip Clipper. El valor del campo contiene el número de serie que se utilizó originalmente para cifrar el mensaje. Basándose

en la clave de serie, la agencia de aplicación de la ley puede identificar la clave de unidad que se va a recuperar de la base de datos y puede descifrar el mensaje. La secuencia correcta para utilizar LEAF es la siguiente:

- Descifre el LEAF con la clave de familia, Kf.
- Recupere el identificador único, U, para el chip Clipper.
- Obtenga una orden judicial para obtener las dos mitades de la clave de unidad, Ku, que es única para cada chip Clipper.
- Recuperar el Ku.
- Recupere la clave de sesión, Ks.
- Utilice la clave de sesión para descifrar el mensaje.

El chip Clipper tiene las siguientes desventajas:

- La clave de unidad de 80 bits empleada por el chip Clipper se considera débil.
- La suma de comprobación de 16 bits utilizada por el chip Clipper puede ser derrotada.
- Cada sesión de comunicación se puede identificar fácilmente al permitir que la agencia de aplicación de la ley use la etiqueta de la identificación del chip Clipper para invadir la privacidad de los ciudadanos.
- El chip Clipper se basa en el algoritmo Skipjack clasificado y nunca se abre para revisión y pruebas públicas.

El chip Clipper ha perdido su soporte debido a las amenazas a la privacidad personal. La mayoría de las empresas recurrieron a programas de cifrado basados en software en lugar de chips de hardware, como el chip Clipper. Por lo tanto, en la mayoría de los casos, se ha abandonado el uso del chip Clipper.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 3: Arquitectura e Ingeniería de Seguridad, Skipjack

El chip clipper, http://epic.org/crypto/clipper/

Question #179 of 193

Question ID: 1114713

¿Qué métodos se pueden utilizar para reducir la electricidad estática?

a) Aerosoles antiestáticos

b. menor humedad

c. Suelos antiestáticos

d. Acondicionamiento de la línea eléctrica

- ✗ **A)** Opción d
- ✗ **B)** opción b
- ✗ **C)** opción A
- ✗ **D)** Opciones B y D
- ✗ **E)** opción c
- ✓ **F)** Opciones A y C

explicación

Los aerosoles antiestáticos se utilizan para reducir la electricidad estática. Los circuitos integrados y los transistores a la misma tensión no causan daños a los circuitos. En caso de diferencia en los voltajes, un aerosol antiestático es un método preventivo para contrarrestar los efectos causados por la electricidad estática.

El suelo antiestático debe utilizarse en las áreas de procesamiento de datos.

El acondicionamiento de la línea eléctrica no ayuda a reducir la electricidad estática. El acondicionamiento de la línea eléctrica es necesario en instalaciones donde la energía es muy inestable. El acondicionamiento mantiene los voltajes de línea dentro de un rango que un sistema puede manejar.

Objetivo:
Arquitectura e ingeniería de seguridad

Sub-Objective:
Implement site and facility security controls

References:

CISSP Cert Guide (3rd Edition), Chapter 3: Security Architecture and Engineering, Preventive Measures

---

Question #180 of 193

Question ID: 1111699

Your company has an e-commerce site that is publicly accessible over the Internet. The e-commerce site accepts credit card information from a customer and then processes the customer's transaction. Which standard or law would apply for this type of data?

- ✗ **A)** Basel II
- ✗ **B)** The Economic Espionage Act of 1996

✓ **C)** PCI DSS

✗ **D)** SOX

Explanation

The Payment Card Industry Data Security Standard (PCI DSS) applies to any entity that transmits, stores, or accepts credit card data. This is a private sector standard and not a law.

The Economic Espionage Act of 1996 protects companies from industry or corporate espionage, and specifically addresses technical, business, engineering, scientific, or financial trade secrets.

Basel II is an accord that went into effect in 2006. This accord affects financial institutions. Its three main pillars are as follows:

- Minimum Capital Requirements - determines the lowest amount of funds that a financial institute must keep in hand.
- Supervision - ensures oversight and review of risks and security measures.
- Market Discipline - requests members to disclose risk exposure and to validate market capital.

The Sarbanes-Oxley (SOX) Act of 2002 was written to prevent companies from committing fraud by knowingly providing inaccurate financial reports to shareholders and the public. It is mainly concerned with corporate accounting practices. Section 404 of this act specifically addresses information technology.

Objective:
Security Architecture and Engineering

Sub-Objective:
Understand the fundamental concepts of security models

References:

CISSP Cert Guide (3rd Edition), Chapter 3: Security Architecture and Engineering, Payment Card Industry Data Security Standard (PCI-DSS)

Question #181 of 193

Question ID: 1104970

What is meant by the term fail-safe?

✗ **A)** a system's ability to recover automatically through a reboot

✗ **B)** a system's ability to switch over to a backup system in the event of a failure

✗ **C)** a system's ability to preserve a secure state before and after failure

✓ **D)** a system's ability to terminate processes when a failure is identified

Explanation

Fail-safe systems provide the ability to automatically terminate the processes in response to a failure. An example would be an automated locking system that defaults to unlock in case of power failure.

A controlled system reboot refers to the ability of the system to recover through a reboot. A controlled system is a part of the trusted recovery procedures.

Fail-secure state refers to the ability of a system to maintain and preserve the secure state of the system in the event of a system failure. A fail-secure state implies that a system should be able to protect itself and its information assets if critical processes are terminated and if a system becomes unusable. An example would be an automated locking system that defaults to lock in case of power failure.

Fail-over systems provide the ability to recover by switching over to backup systems in the event of the failure of a primary system. This is also known as recovery control.

Another term that you need to understand is a fail soft. A fail soft is the termination of selected, non-critical processes after a hardware or software failure is detected.

Objective:
Security Architecture and Engineering

Sub-Objective:
Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)

References:

CISSP Cert Guide (3rd Edition), Chapter 3: Security Architecture and Engineering, Operating Systems

---

Question #182 of 193

Question ID: 1104952

Which component is NOT a part of the protection profile information used by the Common Criteria to evaluate products?

- ✗ **A)** EAL rating
- ✗ **B)** assurance requirements
- ✗ **C)** functionality requirements
- ✓ **D)** product test results

Explanation

The test results of a product are not a part of the protection profile. Product test results are evaluated after the tests are performed on the target of the evaluation, and an evaluation rating is assigned on the basis of these results.

The protection profile contains a set of security requirements including functionality and assurance criteria for a product and the rationale behind such requirements. The corresponding evaluation assurance level (EAL) rating intended for the product is also specified. The environmental conditions, the expected functional, the assurance levels, and the product objectives are also included in the protection profile when the product is evaluated by the Common Criteria for a target evaluation rating. Evaluation tests are performed for the targeted rating awarded to the target of evaluation, and the results are verified before granting an EAL rating to the intended product.

Components of the Common Criteria protection profile include Target of Evaluation (TOE) description, threats against the product that must be addressed, and security objectives.

Objective:
Security Architecture and Engineering

Sub-Objective:
Understand the fundamental concepts of security models

References:

CISSP Cert Guide (3rd Edition), Chapter 3: Security Operations, Common Criteria

---

Question #183 of 193

Question ID: 1105049

Which chip implements the U.S. Escrowed Encryption Standard and was developed by the National Security Agency (NSA)?

- ✗ **A)** HSM
- ✗ **B)** TPM
- ✓ **C)** Capstone
- ✗ **D)** Clipper chip

Explanation

Capstone implements the U.S. Escrowed Encryption Standard and was developed by the NSA. It implements the same algorithm as a Clipper chip.

Trusted Platform Module (TPM) and Hardware Security Module (HSM) are two chips that are used with full-disk encryption. While the Clipper chip was developed by the NSA, it uses the Skipjack algorithm.

Objective:
Security Architecture and Engineering

Sub-Objective:
Apply cryptography

References:

CISSP Cert Guide (3rd Edition), Chapter 3: Security Architecture and Engineering, Skipjack

---

Question #184 of 193

Question ID: 1114693

What is the best description of an execution domain?

- ✓ **A)** an isolated area that is used by trusted processes when they are run in privileged state
- ✗ **B)** memory space insulated from other running processes in a multiprocessing system
- ✗ **C)** components that fall outside the security perimeter of the TCB
- ✗ **D)** a communication channel between an applications and the kernel in the TCB

Explanation

An execution domain is an isolated area that is used by trusted process when they are run in privileged state. This is used in a trusted computing base (TCB).

A protection domain is memory space isolated from other running processes in a multiprocessing system.

A trusted path is the communication channel between applications and the kernel in the TCB.

Some components fall outside the security perimeter of the TCB. However, these components are not referred to as an execution domain.

Objective:
Security Architecture and Engineering

Sub-Objective:
Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)

References:

Question #185 of 193

Question ID: 1132511

Which statement is true of reverse engineering?

- ✗ **A)** It is used to hide the details of an object's functionality.
- ✗ **B)** It removes security flaws from object code.
- ✗ **C)** It involves compiling vendor object codes.
- ✓ **D)** It analyzes the operation of an application.

Explanation

Reverse engineering analyzes the structure, functioning, and operation application code to discover the principle behind the application.

Reverse engineering is associated with the decompilation of the object code. The object source code is confidential, and reverse engineering is used to understand the complex details of the object functionality.

Reverse engineering recognizes the security flaws but does not remove them.

Reverse engineering does not hide the details of an object's functionality. It actually discovers the details.

A common use of reverse engineering is to verify whether the competitor's products are breaching a company's patents or not. Reverse engineering can also be used with the malicious intention of decompiling the object code to gain access to the source code. Some security firms use reverse engineering to analyze the source code of an object and to detect possible loopholes that can be used by attackers.

Objective:
Security Architecture and Engineering

Sub-Objective:
Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

References:

CISSP Cert Guide (3rd Edition), Chapter 3: Software Development Security, Reverse engineering

What is reverse engineering?, http://searchcio-midmarket.techtarget.com/sDefinition/0,sid183_gci507015,00.html

Question #186 of 193

Question ID: 1105088

Which option will have the least effect on the confidentiality, integrity, and availability of the resources within the organization?

- ✗ **A)** lost keys to the door
- ✓ **B)** damaged hard drive
- ✗ **C)** primary power failure
- ✗ **D)** stolen computer

Explanation

A damaged hard drive will have least effect on the confidentiality, integrity, and availability of the resources within the organization because the data inside the damaged hard disk is rendered unusable and cannot be retrieved by any individual with malicious intentions.

Stolen computer and lost keys will have the most impact on the confidentially and integrity of the resources within the organization.

Power failure will have a direct impact on the availability of the system.

Objective:
Security Architecture and Engineering

Sub-Objective:
Apply cryptography

References:

CISSP Cert Guide (3rd Edition), Chapter 3: Security Architecture and Engineering Applied Cryptography

---

Question #187 of 193

Question ID: 1105004

During a recent network attack, a hacker used rainbow tables to guess network passwords. Which type of attack occurred?

- ✗ **A)** privilege escalation
- ✗ **B)** denial-of-service attack
- ✓ **C)** brute force password attack
- ✗ **D)** social engineering attack

Explanation

A brute force password attack can include the use of rainbow tables. A rainbow table is a lookup table that recovers a plaintext password from a password hash. It usually works well in finding weak passwords in use. Weak passwords are those passwords that are not complex or long enough. To implement strong passwords, you should force users to create passwords of at least eight characters in length that include letters, numbers, and special characters.

None of the other attacks uses rainbow tables. A social engineering attack occurs when hackers attempt to fool legitimate users into giving them their credentials. A denial-of-service attack occurs when a hacker exploits a system vulnerability to bring the attacked system down. Privilege escalation occurs when a user gains access to a system and then finds a way to gain administrative credentials by exploiting a design flaw in the application.

Objective:
Security Architecture and Engineering

Sub-Objective:
Apply cryptography

References:

CISSP Cert Guide (3rd Edition), Chapter 3: Security Architecture and Engineering, Brute Force

Frequently Asked Questions About Passwords (text search: Rainbow tables), http://technet.microsoft.com/en-us/library/cc512606.aspx

---

Question #188 of 193

Question ID: 1104982

Which types of computers are targeted by RedPill and Scooby Doo attacks?

- ✓ **A)** virtual machines
- ✗ **B)** Windows Vista clients
- ✗ **C)** terminal servers
- ✗ **D)** Windows Server 2008 computers

Explanation

RedPill and Scooby Doo attacks target virtual machines. These attacks attempt to detect virtual servers and machines on a network. Once the virtual machines are identified, various techniques are used to attack the virtual machines to breach the host and eventually the network.

RedPill and Scooby Doo attacks do not target Windows Server 2008 computers, Windows Vista clients, or terminal servers unless these computers exist as virtual servers or virtual machines.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
evaluar y mitigar las vulnerabilidades de las arquitecturas de seguridad, los diseños y los elementos de la solución

Referencias:

Ataques a más emuladores de máquinas virtuales, http://pferrie.tripod.com/papers/attacks2.pdf

---

Question #189 of 193

Question ID: 1104980

¿Qué riesgo de seguridad supone el archivo /etc/hosts.equiv en un sistema UNIX?

- ✓ **A)** Permite a todos los usuarios conectarse de forma remota sin autenticarse.
- ✗ **B)** Permite a todos los usuarios editar localmente la configuración de DNS.
- ✗ **C)** Permite a todos los usuarios conectarse localmente sin autenticarse.
- ✗ **D)** Permite a todos los usuarios editar de forma remota la configuración de DNS.

explicación

El archivo /etc/hosts.equiv supone un riesgo de seguridad en un sistema UNIX porque permite a todos los usuarios conectarse de forma remota sin autenticarse. A veces se utiliza si la autenticación en los sistemas remotos es equivalente al sistema local. Debe quitar este archivo si no tiene previsto utilizarlo.

El archivo /etc/hosts.equiv no plantea ninguno de los otros riesgos de seguridad.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
evaluar y mitigar las vulnerabilidades de las arquitecturas de seguridad, los diseños y los elementos de la solución

Referencias:

El archivo /etc/hosts.equiv, http://docs.oracle.com/cd/E19455-01/805-7229/remotehowtoaccess-36082/index.html

---

Question #190 of 193

Question ID: 1114704

Su organización debe asegurarse de que los mensajes están protegidos de los piratas informáticos mediante cifrado. La administración decide implementar el algoritmo hash seguro (SHA-1). ¿Qué afirmaciones NO son ciertas de este

algoritmo?

a. SHA-1 genera un valor hash de 128 bits.

b. SHA-1 fue diseñado por el NIST y la NSA.

c. SHA-1 es una función hash bidireccional de longitud variable.

d. SHA-1 fue diseñado para su uso en firmas digitales.

- ✗ **A)** opción A
- ✗ **B)** opción c
- ✗ **C)** Opciones B y D
- ✗ **D)** Opción d
- ✗ **E)** opción b
- ✓ **F)** Opciones A y C

explicación

Las opciones que indican que Secure Hash Algorithm-1 (SHA-1) genera un valor hash de 128 bits y es una función hash bidireccional de longitud variable NO son verdaderas. SHA-1 es una función unidireccional que genera un valor hash fijo de 160 bits. Garantiza la integridad del mensaje mediante el cálculo de un resumen del mensaje. SHA-1 procesa datos en longitudes de bloque de 512 bits.

SHA fue diseñado por el Instituto Nacional de Estándares y Tecnología (NIST) y la Agencia de Seguridad Nacional (NSA) para ser utilizado en firmas digitales.

SHA-1 no es un algoritmo de cifrado; es un algoritmo hash. Los algoritmos de cifrado se utilizan para cifrar mensajes y archivos. Los algoritmos hash se utilizan para proporcionar una huella digital de mensaje o archivo para asegurarse de que el mensaje o archivo no se ha modificado.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, SHA/SHA-2/SHA-3

Question #191 of 193

Question ID: 1114690

¿Qué características de un sistema son evaluadas por los Criterios de Evaluación de Sistemas Informáticos confiables (TCSEC)?

a. garantía

b. autenticidad

c. Funcionalidad

d. tiempo de respuesta

- ✗ **A)** Opciones B y D
- ✗ **B)** opción b
- ✗ **C)** opción c
- ✗ **D)** Opción d
- ✓ **E)** Opciones A y C
- ✗ **F)** opción A
- ✗ **G)** opciones A y B

explicación

Los criterios de evaluación de sistemas informáticos de confianza (TCSEC) evalúan la garantía y la funcionalidad de un sistema. La garantía y la funcionalidad del sistema se evalúan como un criterio único y combinado mientras se realizan pruebas para la verificación del sistema de acuerdo con las estipulaciones. También revisa la efectividad y confiabilidad de un producto.

El Departamento de Defensa de los Estados Unidos (DoD, por sus, por sus, por sus) desarrolló TCSEC para evaluar y calificar la eficacia, la garantía y la funcionalidad de los sistemas operativos, las aplicaciones y los productos de seguridad. Los sistemas de gestión de bases de datos no están cubiertos por TCSEC. Los criterios de evaluación se publican en un libro conocido como el Libro Naranja. El Libro Naranja especifica las clasificaciones de seguridad para los productos de diferentes proveedores. Los clientes pueden usar las clasificaciones para evaluar y comparar diferentes productos. Los fabricantes también pueden utilizar las clasificaciones para construir sus productos de acuerdo con las especificaciones. TCSEC clasifica los sistemas en divisiones jerárquicas de niveles de seguridad que van desde la protección verificada hasta la seguridad mínima. Inicialmente fundado como el Centro de Seguridad Informática del Departamento de Seguridad para garantizar que los centros que procesan información clasificada y confidencial utilizan sistemas informáticos de confianza, más tarde fue nombrado El Centro Nacional de Seguridad Informática (NCSC). El NCSC es una rama de la Agencia de Seguridad Nacional (NSA) que inicia la investigación y desarrolla y publica normas y criterios para sistemas de información confiables.

Una calificación más alta implica un mayor grado de confianza y seguridad. Por ejemplo, una clasificación B2 proporciona más seguridad que una clasificación C2. Una calificación más alta incluye los requisitos de una calificación más baja. Por ejemplo, una clasificación B2 incluye las características y especificaciones de una clasificación C2.

Common Criteria se ocupa de los atributos de funcionalidad y garantía de un producto. Common Criteria es un estándar de evaluación reconocido y aceptado en todo el mundo para productos de seguridad. Este criterio de evaluación reduce la complejidad de las calificaciones y garantiza que los proveedores fabriquen productos para los mercados internacionales. Por lo tanto, Common Criteria aborda la funcionalidad en términos de las tareas realizadas por un producto y garantiza que el producto funcionará según lo previsto. Las tres partes principales de los criterios comunes son 1) Introducción y modelo general, 2) Requisitos funcionales de seguridad y 3) Requisitos de garantía de seguridad. ISO/IEC 15408-1 es la versión de estándares internacionales de los Criterios Comunes.

Objetivo:
Arquitectura e ingeniería de seguridad

Sub-Objective:
Understand the fundamental concepts of security models

References:

CISSP Cert Guide (3rd Edition), Chapter 3: Security Operations, TCSEC

Question #192 of 193

Question ID: 1105043

What does the message authentication code (MAC) ensure?

- ✗ **A)** reproducción de mensajes
- ✓ **B)** integridad del mensaje
- ✗ **C)** confidencialidad de los mensajes
- ✗ **D)** disponibilidad de mensajes

explicación

El código de autenticación de mensajes (MAC), que también se conoce como código de integridad de mensajes (MIC), garantiza la integridad de los mensajes. MAC agrega capacidad de autenticación a una función de hash unidireccional.

El MAC no asegura la reproducción del mensaje. Proporciona protección contra ataques de reproducción de mensajes. Se puede realizar una reproducción de mensajes para obtener acceso a la información y volver a insertar la información en una conexión legítima a través de ataques, como ataques de tipo "Man in the middle".

MAC no puede garantizar la disponibilidad de los datos o del sistema.

Una función hash unidireccional no utiliza ninguna clave y solo garantiza que el mensaje que se transfiere no se altera calculando un valor de suma de comprobación. Los mensajes con hash unidireccional se pueden interceptar y se puede reproducir el hash. El hash unidireccional convierte un mensaje de longitud arbitraria en un valor de longitud fija.

Dado el valor de resumen, debería ser computacionalmente inviable encontrar el mensaje correspondiente. Debería ser imposible o raro derivar el mismo resumen de dos mensajes diferentes. MAC aplica una clave secreta al mensaje que sólo conoce el destinatario autorizado. La criptografía de encadenamiento de bloques utiliza MAC para garantizar la autenticidad del mensaje.

Hay dos tipos básicos de MAC: Hash-MAC (HMAC) y CBC-MAC. En HMAC, se anexa una clave simétrica al mensaje que sólo conoce el destinatario autorizado. Sin embargo, HMAC carece de confidencialidad. Cuando se utiliza una función HMAC, se combina una clave simétrica con el mensaje y, a continuación, ese resultado se coloca a través de un algoritmo hash. El resultado es un valor HMAC. HMAC proporciona autenticación de origen de datos e integridad de datos. En CBC-MAC, el mensaje se cifra con un cifrado de bloques simétrico en modo CBC. Algunos algoritmos MAC también utilizan cifrados de flujo. HMAC proporciona integridad y autenticación de origen de datos; CBC-MAC utiliza un cifrado de bloques para el proceso de creación de un MAC.

MAC fue desarrollado para prevenir el fraude en las transferencias electrónicas de fondos involucradas en transacciones en línea.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura e ingeniería de seguridad, Código de autenticación de mensajes

---

Question #193 of 193

Question ID: 1105089

¿Por qué los archivos del controlador de dispositivo deben estar firmados digitalmente?

- ✗ **A)** Para asegurarse de que los instala un usuario de confianza
- ✗ **B)** Para asegurarse de que no se cambian después de la instalación
- ✓ **C)** Para asegurarse de que proceden de un editor de confianza
- ✗ **D)** Para registrar la marca de tiempo de instalación

explicación

Los archivos de controlador de dispositivo deben estar firmados digitalmente para asegurarse de que proceden de un editor de confianza. Si no confía en la entidad que firma el archivo o si el archivo no está firmado, no debe confiar en el archivo y no debe instalarlo.

Ninguna de las otras razones es una razón válida para usar controladores de dispositivo firmados digitalmente. Para asegurarse de que los archivos no se cambian después de la instalación, debe validar la suma de comprobación del archivo. La suma de comprobación de la versión original del archivo debe guardarse para la comparación. Si la suma de comprobación cambia, el archivo se ha cambiado de alguna manera.

Para asegurarse de que los controladores de dispositivo son instalados por un usuario de confianza, debe implementar controles de acceso adecuados.

Cuando se instalan los controladores de dispositivo, la mayoría del sistema operativo registra una marca de tiempo de instalación como parte de las propiedades del archivo.

Objetivo:
Arquitectura e ingeniería de seguridad

Subobsecución:
Aplicar criptografía

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 3: Arquitectura de seguridad y firmas digitales de ingeniería