Dominio 5 - Identidad and Access Management IAM) Test ID: 177713607

Pregunta #1 de 105

Id. de pregunta: 1114754

¿Qué afirmaciones son ciertas para las tarjetas de memoria?

un. Las tarjetas de memoria tienen más memoria que las tarjetas inteligentes.

B. Las tarjetas de memoria pueden proporcionar autenticación de dos factores.

c. Las tarjetas de memoria no tienen potencia de procesamiento propia.

d. Las tarjetas de memoria pueden proporcionar contraseñas estáticas y dinámicas para la autenticación.

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

explicación

Las tarjetas de memoria no tienen potencia de procesamiento. Solo actúan como un repositorio de datos, como credenciales de usuario, que se pueden usar para la autenticación de usuarios.

Las tarjetas de memoria proporcionan autenticación de dos factores. Un usuario debe proporcionar un PIN junto con la tarjeta de memoria. La autenticación de dos factores se basa en algo que sabe, como una contraseña, y algo que tiene, como una tarjeta de memoria.

Las tarjetas de memoria actúan como dispositivos de almacenamiento simples y no tienen más memoria que las tarjetas inteligentes. Las tarjetas inteligentes, a veces denominadas tarjetas de procesador, pueden procesar información debido al procesador incorporado y al hardware auxiliar. Las tarjetas inteligentes tienen un procesador integrado y memoria.

Los tokens se asemejan a las tarjetas de crédito y se usan para proporcionar contraseñas de un solo uso (OTP), que son una combinación de contraseñas estáticas y dinámicas. Los tokens de acceso son los más adecuados para áreas de alta seguridad.

Una de las desventajas de las tarjetas de memoria es que son fáciles de falsificar.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 5: Gestión de identidad y acceso, tarjetas de memoria

---

Pregunta #2 de 105

Id. de pregunta: 1132533

Ha descubierto que el 25 % de los equipos de su organización han sido atacados. Como resultado, estos equipos se utilizaron como parte de un ataque de denegación de servicio distribuido (DDoS). ¿A qué clasificación o área pertenecen los ordenadores comprometidos?

- ✗ **A)** Honeypot
- ✓ **B)** botnet
- ✗ **C)** Dmz
- ✗ **D)** VPN

explicación

Los ordenadores comprometidos son miembros de una botnet. Una red de bots es creada por un hacker cuando el malware se copia en un equipo de la red que permite al pirata informático apoderarse del equipo. Las botnets se utilizan a menudo para llevar a cabo ataques distribuidos de denegación de servicio (DDoS).

Una zona desmilitarizada (DMZ) es un área protegida de una red local que contiene computadoras de acceso público. Botnets se pueden localizar en cualquier lugar de su red.

Una red privada virtual (VPN) es una conexión segura y privada a través de una red pública o de Internet. Botnets se pueden localizar en cualquier lugar de su red.

Un honeypot es un equipo que se configura en la red de una organización para actuar como una desviación para los atacantes. A menudo, los honeypots se dejan abiertos de tal manera que se aseguran de que sean atacados en lugar de los sistemas más importantes.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

Cissp Cert Guide (3ª edición), Capítulo 5, Gestión de identidad y acceso, DoS/DDoS

Pregunta #3 de 105

Id. de pregunta: 1105263

¿Cuál es la mejor contramedida para un ataque de desbordamiento de búfer en una aplicación comercial?

- ✗ **A)** Edite el código de la aplicación para incluir la comprobación de límites para asegurarse de que los datos son de una longitud aceptable.
- ✓ **B)** Actualice el software con las revisiones, actualizaciones y Service Packs más recientes.
- ✗ **C)** Implemente revisiones de código y control de calidad de forma regular.
- ✗ **D)** Implemente marcas de tiempo y números de secuencia.

explicación

La mejor contramedida para un ataque de desbordamiento de búfer en una aplicación comercial es actualizar el software con las revisiones, actualizaciones y Service Packs más recientes.

La mejor contramedida para los ataques de reproducción es la implementación de marcas de tiempo y números de secuencia.

La mejor contramedida para un ataque de desbordamiento de búfer en una aplicación propietaria desarrollada por la empresa sería editar el código de la aplicación para incluir la comprobación de límites para asegurarse de que los datos son de una longitud aceptable.

La mejor contramedida para los ganchos de mantenimiento es implementar revisiones de código y control de calidad de forma regular.

Un ataque de desbordamiento de búfer se puede detectar examinando los paquetes que se transmiten en la red mediante un rastreador de paquetes. Una cadena larga de números en medio de un paquete es indicativa de un ataque de desbordamiento de búfer.

Objetivo:
Administración de identidad y acceso (IAM)

Subobsecución:
Controlar el acceso físico y lógico a los activos

Referencias:

Cissp Cert Guide (3rd Edition), Chapter 5: Identity and Access Management, Buffer Overflow

Pregunta #4 de 105

Id. de pregunta: 1105337

La dirección de la empresa ha decidido implementar políticas de seguridad en toda la organización. Debe implementar un método de control de acceso que utilice la configuración de las directivas de seguridad preconfiguradas para tomar todas las decisiones. ¿Qué método de control de acceso debe implementar?

- ✓ **A)** control de acceso basado en reglas
- ✗ **B)** control de acceso obligatorio
- ✗ **C)** control de acceso discrecional
- ✗ **D)** control de acceso basado en roles

explicación

El control de acceso basado en reglas usa la configuración de las directivas de seguridad preconfiguradas para tomar todas las decisiones. Las reglas definidas suelen incluir horas y días de conexión. Este tipo de control de acceso lo utilizan las conexiones de acceso remoto.

Ninguna de las otras opciones es correcta.

El control de acceso discrecional (DAC) se considera el menos seguro porque la seguridad la aplican los propietarios de los datos y se descentraliza. El control de acceso basado en identidad se implementa en un modelo DAC.

El control de acceso obligatorio (MAC) proporciona el mecanismo de seguridad más estricto. Asigna etiquetas de seguridad tanto a los sujetos como a los objetos. Se basa en autorizaciones de seguridad. Este modelo se suele implementar en redes altamente seguras, como instalaciones militares. El modelo de celosía se basa en MAC. Los principios de privilegio mínimo y necesidad de saber se aplican más estrictamente en MAC. La propiedad de seguridad simple y la propiedad star son principios clave en MAC.

El control de acceso basado en roles (RBAC) no es tan estricto como MAC. Asigna seguridad en función de los roles y las responsabilidades. Por lo tanto, apoya la gestión de los derechos de acceso para grupos de sujetos. Se considera un modelo de control de acceso basado en tareas.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Modelos de control de acceso

Control de acceso obligatorio, discrecional, basado en roles y reglas, http://www.techotopia.com/index.php/Mandatory,_Discretionary,_Role_and_Rule_Based_Access_Control

---

Pregunta #5 de 105

Id. de pregunta: 1113987

¿Qué entidad puede usar un administrador para designar qué usuarios pueden acceder a un archivo?

- ✗ **A)** un servidor NAT
- ✗ **B)** un servidor proxy
- ✗ **C)** un cortafuegos
- ✓ **D)** una ACL

explicación

Una lista de control de acceso (ACL) es un mecanismo de seguridad que se utiliza para designar qué usuarios pueden obtener varios tipos de acceso, como el acceso de lectura, escritura y ejecución a los recursos de una red. Una ACL proporciona seguridad tan granular como el nivel de archivo. El modelo DAC usa ACL para identificar a los usuarios que tienen permisos para un recurso.

Un firewall permite y deniega el acceso a la red a través de puertos de comunicaciones. Un servidor NAT presenta direcciones públicas de protocolo Internet (IP) a Internet en nombre de equipos de una red privada. Se puede utilizar un servidor proxy para permitir que los hosts tengan acceso a los recursos de Internet. Un servidor proxy puede aumentar el rendimiento de una red almacenando en caché las páginas Web, lo que puede reducir la cantidad de tiempo necesario para que los clientes tengan acceso a las páginas Web.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Modelos de control de acceso

---

Pregunta #6 de 105

Id. de pregunta: 1111746

El centro de datos de su organización es una parte segura del edificio de su organización. La entrada al centro de datos requiere que los usuarios introduzcan una contraseña de cinco dígitos. Solo los usuarios del departamento de tecnología de la información (TI) pueden acceder al centro de datos y todo el personal del departamento de TI utiliza la misma contraseña de cinco dígitos.

Debe asegurarse de que la contraseña se cambia correctamente. ¿Qué directriz NO debe implementar?

- ✗ **A)** Cambie la contraseña al menos cada seis meses.
- ✗ **B)** Cambie la contraseña cuando un empleado del departamento de TI abandone la organización.
- ✓ **C)** Cambie la contraseña cuando un empleado del departamento de TI se vaya de licencia extendida.
- ✗ **D)** Cambie la contraseña cuando la contraseña se haya visto comprometida a sabiendas.

explicación

NO debe cambiar la contraseña cuando un empleado del departamento de TI se va de licencia prolongada.

Cuando el centro de datos está protegido por una contraseña, debe cumplir las siguientes directrices:

- Cambie la contraseña al menos cada seis meses.
- Cambie la contraseña cuando un empleado del departamento de TI abandone la organización.
- Cambie la contraseña cuando se haya visto comprometida a sabiendas.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Chapter5 Identity and Access Management, Prevent or Mitigate Access Control Threats

---

Pregunta #7 de 105

Id. de pregunta: 1105330

Trabaja para una organización que emplea empleados temporales de forma rotativa. La organización experimenta una alta rotación de empleados. ¿Qué modelo de control de acceso se utiliza mejor en este entorno?

- ✗ **A)** control de acceso obligatorio

✗ **B)** control de acceso discrecional

✓ **C)** control de acceso basado en roles

✗ **D)** control de acceso basado en identidad

explicación

El control de acceso basado en roles (RBAC) se usa mejor en un entorno donde hay una alta rotación de empleados. Cuando un empleado deja la empresa, es muy fácil agregar el reemplazo del empleado al rol que asegurarse de que el nuevo empleado tiene todos los permisos del antiguo empleado.

El control de acceso obligatorio (MAC) se utiliza mejor en un entorno donde la confidencialidad es la mayor preocupación. A cada sujeto y objeto se le da una etiqueta de seguridad. El esfuerzo administrativo en este modelo puede ser relativamente alto debido a este hecho.

El control de acceso discrecional (DAC) se usa en entornos donde los propietarios de datos necesitan controlar los permisos de acceso a sus archivos. La administración en este modelo suele estar descentralizada. DAC sería difícil en un entorno donde hay una alta rotación de empleados porque cada propietario de datos tendría que ser notificado de las renuncias y reemplazos de empleados.

El control de acceso basado en identidad se implementa normalmente en entornos DAC. El control de acceso basado en la identidad no debe utilizarse en un entorno en el que la rotación de empleados es elevada. En un entorno muy grande, este tipo de control de acceso sería una carga administrativa.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Modelos de control de acceso

---

Pregunta #8 de 105

Id. de pregunta: 1105350

¿Qué modelo de control de acceso proporciona el mecanismo de seguridad más estricto?

✓ **A)** control de acceso obligatorio

✗ **B)** control de acceso basado en identidad

✗ **C)** control de acceso discrecional

✗ **D)** control de acceso basado en roles

explicación

El control de acceso obligatorio (MAC) proporciona el mecanismo de seguridad más estricto. Asigna etiquetas de seguridad tanto a los sujetos como a los objetos. Este modelo se suele implementar en redes altamente seguras, como instalaciones militares.

El control de acceso basado en roles (RBAC) no es tan estricto como MAC. El control de acceso discrecional (DAC) se considera el menos seguro porque la seguridad la aplican los propietarios de los datos y se descentraliza. El control de acceso basado en identidad se implementa en un modelo DAC.

En un modelo de control de acceso seguro, un sujeto con una etiqueta menos segura no puede tener acceso a los objetos seguros.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Modelos de control de acceso

---

Pregunta #9 de 105

Id. de pregunta: 1114760

Como profesional de la seguridad, se le ha pedido que informe a una organización sobre qué modelo de control de acceso usar. Ha decidido que el control de acceso basado en roles (RBAC) es la mejor opción para la organización. ¿Cuáles son las ventajas de implementar este modelo de control de acceso?

a. Fácil de usar

b. Bajo costo de seguridad

c. Más fácil de implementar

d. Carácter discrecional

e. Entorno altamente seguro

✗ **A)** opción c
✗ **B)** Opción d
✗ **C)** sólo las opciones a, b y c
✓ **D)** Sólo opciones B y C

- ✗ **E)** todas las opciones
- ✗ **F)** opción e
- ✗ **G)** opción b
- ✗ **H)** opción A

explicación

El control de acceso basado en roles (RBAC) tiene un bajo costo de seguridad porque la seguridad se configura en función de los roles. Por esta razón, también es más fácil de implementar que los otros modelos de control de acceso.

RBAC NO es fácil de usar. El control de acceso discrecional (DAC) es más fácil de usar, ya que permite al propietario de los datos determinar los derechos de acceso de los usuarios. Si un usuario necesita acceso a un archivo, sólo tiene que ponerse en contacto con el propietario del archivo.

RBAC NO es de naturaleza discrecional. DAC es discrecional.

RBAC NO es un entorno altamente seguro. El control de acceso obligatorio (MAC) se considera un entorno altamente seguro porque a cada sujeto y objeto se le asigna una etiqueta de seguridad.

Con RBAC, es fácil aplicar privilegios mínimos para los usuarios generales. Debe crear el rol adecuado, configurar sus permisos y, a continuación, agregar los usuarios al rol. Un rol se define en función de las operaciones y tareas que se le deben conceder. Los roles se basan en la estructura de la organización y suelen ser jerárquicos.

RBAC es un modelo de control de acceso popular que se usa en aplicaciones comerciales, especialmente en aplicaciones en red de gran tamaño.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Modelos de control de acceso

---

Pregunta #10 de 105

Id. de pregunta: 1113989

¿Qué es un retrovirus?

- ✗ **A)** Un virus que se basa en un virus antiguo pero que se ha modificado para evitar su detección

✗ **B)** Un virus que modifica otros programas y bases de datos

✓ **C)** Un virus que ataca u omite el software antivirus

✗ **D)** Un virus que incluye código de protección que impide el examen externo de elementos críticos

explicación

Un virus retrovirus ataca o omite el software antivirus. Retrovirus incluso atacan el programa antivirus para destruir las definiciones de virus o para crear derivaciones para sí mismo.

En el momento de escribir este examen, no hay ningún nombre para un virus basado en un virus antiguo que se ha modificado para evitar la detección.

Un virus fago modifica otros programas y bases de datos. La única manera de eliminar el virus es volver a instalar las aplicaciones infectadas.

Un virus blindado incluye código protector que impide el examen de elementos críticos. La armadura intenta proteger el virus de la destrucción.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Administrar el ciclo de vida de aprovisionamiento de identidad y acceso

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5, Gestión de identidad y acceso, Virus

¿Qué es el retrovirus?, http://www.webopedia.com/TERM/R/retrovirus.html

---

Pregunta #11 de 105

Id. de pregunta: 1105290

¿Qué tipo de contraseña suele ser el más fácil de recordar?

✗ **A)** contraseña estática

✗ **B)** dynamic password

✗ **C)** software-generated password

✓ **D)** pass phrase

Explanation

Una frase de contraseña suele ser la más fácil de recordar. Aunque es más larga que una contraseña estática, se considera más fácil de recordar porque puede convertirla en una oración, como "IAmSoGladThatChristmasOnlyComesOnceAYear". La mayoría de los sistemas no utilizan la frase de contraseña real que el usuario escribe. En su lugar, colocan este valor a través de algún tipo de cifrado o función hash para crear otro formato de ese valor, denominado contraseña virtual.

Una contraseña estática es aquella generada por el usuario. Los cambios de contraseña en las contraseñas estáticas se producen a intervalos definidos por el administrador. Una contraseña estática se considera más difícil de recordar que una frase de contraseña porque es una sola palabra o una frase pequeña y generalmente se cambia con más frecuencia que una frase de contraseña. Las contraseñas estáticas siguen siendo las mismas con cada inicio de sesión, mientras que las contraseñas dinámicas cambian con cada inicio de sesión.

Una contraseña dinámica y una contraseña generada por software son la misma cosa. Son difíciles de recordar debido a su longitud y complejidad. Un token de contraseña dinámica asincrónica genera una nueva contraseña que no tiene que caber en una ventana de tiempo fija para la autenticación. Se debe utilizar un token de contraseña dinámica sincrónica en un tiempo fijo.

Las frases de contraseña no son susceptibles a ataques de fuerza bruta o diccionario porque son más complejas que las contraseñas normales.

Las contraseñas se consideran el control de acceso menos costoso de implementar, pero también son las menos seguras.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Administración de identidad y acceso, contraseñas de frase de contraseña

---

Pregunta #12 de 105

Id. de pregunta: 1105319

¿Qué protocolo concede TFT?

- ✓ **A)** Kerberos
- ✗ **B)** Telnet
- ✗ **C)** ARP
- ✗ **D)** L2TP

explicación

Kerberos es un protocolo que emite vales de concesión de vales (TFT), que los clientes pueden utilizar para solicitar claves de sesión. Un cliente Kerberos puede utilizar una clave de sesión para obtener acceso a los recursos.

El Protocolo de resolución de direcciones (ARP) se utiliza en redes TCP/IP para resolver direcciones de protocolo Internet (IP) en direcciones de control de acceso a medios (MAC). Las direcciones MAC se asignan a las tarjetas de interfaz de red (NIC) y se utilizan para identificar los recursos físicos de una red. IP se utiliza en redes TCP/IP para localizar hosts. ARP permite que Ethernet y TCP/IP interopere.

El Protocolo de túnel de capa 2 (L2TP) se puede utilizar para crear conexiones de red privada virtual (VPN) seguras.

Telnet es un protocolo TCP/IP que permite a un usuario conectarse de forma remota a un servidor a través de una interfaz basada en texto. A continuación, el usuario puede utilizar Telnet para emitir comandos de forma remota en el servidor como si fuera el equipo local.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Chapter 5: Identity and Access Management, , Kerberos

---

Pregunta #13 de 105

Id. de pregunta: 1105320

Su organización incluye un dominio de Active Directory con tres controladores de dominio. Los usuarios son miembros o unidades organizativas (UO) que se basan en la pertenencia de departamento. ¿Qué tipo de modelo de base de datos se usa en el dominio?

- ✓ **A)** un modelo de base de datos jerárquico
- ✗ **B)** un modelo de base de datos relacional
- ✗ **C)** un modelo de base de datos relacional de objetos
- ✗ **D)** un modelo de base de datos orientado a objetos

explicación

Un dominio de Active Directory, que utiliza el Protocolo ligero de acceso a directorios (LDAP), es un modelo de base de datos jerárquico. Un modelo de base de datos jerárquico utiliza una estructura de árbol lógico. LDAP es la implementación más común de un modelo de base de datos jerárquico.

Un modelo de base de datos relacional no se utiliza en el escenario. Un modelo de base de datos relacional utiliza filas y columnas para organizar los datos y presenta los datos en tablas. La entidad fundamental en una base de datos relacional es la relación. Las bases de datos relacionales son las más populares. SQL Server de Microsoft es una base de datos relacional.

Un modelo de base de datos orientado a objetos no se utiliza en este escenario. Un modelo de base de datos orientada a objetos (OODB) puede almacenar datos gráficos, de audio y de vídeo. Una base de datos orientada a objetos popular es db4objects de Versant Corporation.

En este escenario no se utiliza un modelo de base de datos relacional de objetos. Una base de datos relacional de objetos es una base de datos relacional con un front-end de software escrito en un lenguaje de programación orientado a objetos. Oracle 11g es una base de datos de relación de objetos.

Otro tipo de modelo de base de datos es el modelo de base de datos de red. Este modelo de base de datos expande el modelo de base de datos jerárquico. Un modelo de base de datos de red permite que un registro secundario tenga más de un elemento primario, mientras que un modelo de base de datos jerárquico permite que cada elemento secundario tenga solo un elemento primario.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Dominios de seguridad

---

Pregunta #14 de 105

Id. de pregunta: 1113978

¿Qué característica de un sistema biométrico no se tendrá en cuenta durante su implementación?

- ✗ **A)** capacidad de rechazar a personas no autorizadas
- ✓ **B)** capacidad de modificar el patrón de funcionamiento de un dispositivo biométrico
- ✗ **C)** capacidad para mantener un nivel estándar de rendimiento
- ✗ **D)** capacidad de autenticar a personas autorizadas

explicación

La capacidad de un sistema biométrico para modificar el patrón de funcionamiento de un dispositivo biométrico no es una consideración importante al implementar un sistema biométrico. La precisión y la facilidad de uso de un dispositivo

biométrico son consideraciones primordiales. Un sistema biométrico se considera eficaz si tiene las siguientes características:

- Capacidad de autenticar a personas autorizadas
- Capacidad de rechazar a personas no autorizadas
- Capacidad para mantener un nivel estándar de rendimiento sin mostrar signos de degradación

Los sistemas biométricos en su orden de efectividad son los siguientes:

- Escaneo de la palma de la mano
- Geometría de la mano
- Escaneo del iris
- Patrón de retina
- Huellas
- Impresión de voz
- Dinámica de la firma
- Dinámica de pulsaciones de teclas

Un escaneo de iris suele ser la tecnología biométrica más cara, según un gráfico de Zephyr. Un gráfico de Zephyr es un gráfico comparativo que se puede utilizar para comparar dos cosas cualesquiera y no se limita a la tecnología de la información. La comparación se puede realizar en características específicas o en todas las características generales.

Los escaneos de manos, los escaneos de retina y los sistemas biométricos de escaneo de voz no son tan costosos como los sistemas de escaneo de iris. La biometría es un medio automatizado de autenticación de la identidad basada en características fisiológicas o de comportamiento.

La autenticación a través de la biometría, como las huellas dactilares, los escaneos de palma de la mano y la geometría de la mano, se basa en resultados altamente sensibles. Un sistema biométrico es muy costoso y sensible, y debe ser muy preciso para cumplir con los requisitos de seguridad de la organización. La precisión resulta de mediciones repetidas de las características físicas y de comportamiento de los usuarios. Las inexactitudes más allá del límite de umbral suelen ser inaceptables. El objetivo de implementar un sistema biométrico es garantizar que solo los usuarios autorizados se autentiquen después de que sus credenciales se verifiquen con sus registros de referencia, y que a los usuarios no autorizados no se les conceda acceso falso a recursos confidenciales.

El alto rendimiento, el bajo tiempo de inscripción y la alta aceptabilidad del usuario afectarían positivamente la aceptación de un dispositivo biométrico.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Consideraciones biométricas

Biometría, http://searchsecurity.techtarget.com/definition/biometrics

---

Pregunta #15 de 105

Id. de pregunta: 1105329

¿Qué instrucción describe la relación entre los modelos de control de acceso y las técnicas de control de acceso?

✗ **A)** Los modelos de control de acceso diseñan las técnicas de control de acceso.

✗ **B)** Los modelos de control de acceso admiten las técnicas de control de acceso.

✗ **C)** Las técnicas de control de acceso diseñan los modelos de control de acceso.

✓ **D)** Las técnicas de control de acceso admiten los modelos de control de acceso.

explicación

Las técnicas de control de acceso admiten los modelos de control de acceso. En primer lugar, una empresa decide sobre el modelo de control de acceso que utilizará. El modelo de control de acceso es una descripción formal de la política de seguridad de la empresa. Una vez que se determina un modelo, se determina la técnica de control de acceso. La técnica utilizada garantiza que el modelo se implementa correctamente.

Ninguna de las otras opciones es correcta.

Una vez decidido el modelo y la técnica de control de accesos, la empresa puede determinar qué modelo administrativo utilizar: centralizado o descentralizado. Algunos modelos y técnicas obligan al uso de un determinado modelo administrativo.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Modelos de control de acceso

---

Pregunta #16 de 105

Id. de pregunta: 1105287

Ha implementado un sistema biométrico que analiza la dinámica de la firma. Este sistema biométrico es un ejemplo de qué categoría biométrica?

✗ **A)** psicológico

✗ **B)** fisiológico

✓ **C)** conductual

✗ **D)** biológico

explicación

Un sistema biométrico dinámico de firma es un ejemplo de un sistema biométrico conductual. Un sistema biométrico conductual analiza lo que hace una persona y cómo lo hace para controlar el acceso.

Hay dos categorías de sistemas biométricos: fisiológicos y conductuales. Un sistema biométrico fisiológico analiza los rasgos físicos de una persona para controlar el acceso. Este tipo de sistema incluye escaneos de retina, escaneos de iris, escaneos de huellas dactilares y escaneos de palma de la mano.

No existen categorías psicológicas o biológicas de sistemas biométricos.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Características conductuales de la gestión de identidad y acceso

---

Pregunta #17 de 105

Id. de pregunta: 1105364

Está realizando revisiones de cuentas de usuario. Debe determinar si se están utilizando cuentas de usuario. ¿Qué propiedad debe verificar?

✗ **A)** Si se requiere una contraseña

✗ **B)** Cuándo se configuró por última vez la contraseña

✗ **C)** Si las cuentas de usuario están deshabilitadas

✓ **D)** Cuándo se produjo el último inicio de sesión

explicación

Para determinar si se están utilizando cuentas de usuario, debe comprobar cuándo se produjo el último inicio de sesión para cada cuenta de usuario. Si una cuenta de usuario no ha iniciado sesión recientemente, el usuario no está cerrar la sesión correctamente o la cuenta de usuario ya no se utiliza.

No debe comprobar cuándo se configuró la contraseña por última vez. Si lo hace, se asegurará de que los usuarios cambien sus contraseñas según lo estipulado en la directiva de caducidad de contraseñas. Las contraseñas no se pueden cambiar si el usuario no está cerrar la sesión correctamente cada día.

No debe comprobar si se requiere una contraseña. Si lo hace, se asegurará de que las cuentas de usuario deben tener una contraseña.

No debe comprobar si las cuentas de usuario están deshabilitadas. No se utilizan cuentas de usuario deshabilitadas. Las cuentas de usuario a menudo se conservan en un estado deshabilitado durante un período de tiempo. Restaurar una cuenta de usuario una vez que se elimina es difícil.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Administrar el ciclo de vida de aprovisionamiento de identidad y acceso

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, gestión de identidad y cuentas

---

Pregunta #18 de 105

Id. de pregunta: 1105279

¿Cuál es el resultado de un aumento en los errores de tipo 2 de un sistema biométrico?

- ✓ **A)** Los usuarios no autorizados se autentican falsamente.
- ✗ **B)** Los registros de referencia se eliminan automáticamente.
- ✗ **C)** Se requiere que un usuario se autentique más de una vez.
- ✗ **D)** Los usuarios autorizados son rechazados falsamente.

explicación

Un aumento en los errores de tipo 2 de un sistema biométrico resulta en la autenticación errónea de usuarios no autorizados. Los errores de tipo 2 representan la tasa de aceptación falsa (FAR) del sistema biométrico.

Un usuario deberá autenticarse más de una vez en un sistema biométrico solo si los registros de referencia no son claros y distinguibles. El número de intentos de autenticación depende de los errores de tipo 1, no de los errores de tipo 2.

En caso de un aumento en el número de errores de tipo 1, se deniega a los usuarios autorizados el acceso a los recursos. Esto afecta a la productividad del usuario. Los errores de tipo 1 representan la tasa de rechazo falso (FRR) de un sistema biométrico. Un alto valor de FRR implica que un gran número de personas autorizadas están siendo

negadas el acceso por el sistema biométrico. La tasa de error de cruce (CER) es el punto en el cual el FRR iguala el FAR. La clasificación CER para un sistema biométrico es la medición más crítica utilizada para determinar la precisión del sistema. Un valor CER de 5 es mejor que un valor CER de 10.

Un sistema biométrico no elimina automáticamente los registros de referencia si hay un aumento en el número de errores de tipo 2. Se crea un registro de referencia para cada usuario a través de un proceso de inscripción que se usa para los intentos de autenticación posteriores.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Consideraciones biométricas

---

Pregunta #19 de 105

Id. de pregunta: 1192948

El personal de seguridad ha informe de que el sistema biométrico de huellas digitales de su organización está concediendo acceso a usuarios no autorizados. ¿Cuál es la razón más apropiada para este suceso?

- ✗ **A)** El sistema biométrico tiene una baja tasa de error cruzado.
- ✗ **B)** El sistema biométrico no tiene un amplio espacio de almacenamiento para todos los registros de los empleados.
- ✓ **C)** El sistema biométrico tiene una alta tasa de error de tipo 2 y permite la autenticación de usuarios no autorizados.
- ✗ **D)** Algunas características específicas de las huellas dactilares coinciden y conducen al problema.

explicación

El sistema biométrico tiene una alta tasa de error de tipo 2 y permite la autenticación de usuarios no autorizados. Un error de tipo 2 alto válido implica que las personas no autorizadas están siendo autenticadas falsamente por el sistema biométrico y que los intrusos podrían acceder a recursos críticos. Un alto nivel de precisión en un sistema biométrico conduce a una mayor aceptación del usuario y proporciona un mayor rendimiento. Las consideraciones principales al seleccionar un sistema biométrico deben ser la precisión, el rendimiento, la confiabilidad y la aceptación del usuario.

El rechazo de usuarios autorizados por un sistema biométrico se denomina error de tipo 1. La concesión de acceso a usuarios no autorizados por un sistema biométrico se denomina error de tipo 2. La precisión de los sistemas

biométricos se basa en la tasa de rechazo falso (FRR) que implica errores de tipo 1 y la tasa de aceptación falsa (FAR) que implica errores de tipo 2. Un valor alto de errores de tipo 1 implica que se rechaza un alto porcentaje de intentos de autenticación válidos y la productividad de los empleados se verá afectada negativamente, lo que provocará una menor aceptación del usuario.

La concesión de acceso a usuarios no autorizados no es el resultado directo de una baja tasa de error cruzado (CER). Un valor cer bajo para un dispositivo biométrico no implica que los errores de tipo 2 son altos para el dispositivo. El CER es afectado por los errores del tipo 2. Sin embargo, los errores de tipo 2 son en realidad la razón por la que se concede acceso a los usuarios no autorizados. El CER es el punto en el cual el FRR iguala el FAR. La clasificación CER para un sistema biométrico es la medición más crítica utilizada para medir la precisión del sistema. Un valor CER de 5 es mejor que un valor CER de 10.

No es posible que algunas características específicas de huellas digitales coincidan. Cada individuo tiene una huella digital única. Por lo tanto, las características de huellas digitales para dos empleados cualesquiera no coinciden. Esto garantiza que el sistema autentique sólo a los usuarios autorizados.

Si el dispositivo biométrico no tiene amplias capacidades de almacenamiento para almacenar los archivos de referencia para todos los empleados, el dispositivo solo autenticará a aquellos empleados que tengan sus registros de referencia en el dispositivo. Por lo tanto, el espacio de almacenamiento bajo no implica que el dispositivo biométrico esté autenticando a los usuarios no autorizados.

Se deben tener en cuenta los siguientes factores al seleccionar un sistema biométrico:

- Precisión y fiabilidad: Si un sistema biométrico rechaza a un usuario autorizado, se conoce como error de tipo I. Si el sistema biométrico acepta a un usuario no autorizado, se conoce como errores de tipo II. Los errores de tipo II son los más peligrosos. Sin embargo, el objetivo es minimizar la ocurrencia de ambos errores y aumentar la precisión del sistema biométrico
- Rendimiento: la fase de inscripción para algunos sistemas biométricos requiere que los usuarios repitan la acción para obtener un registro claro. El tiempo empleado no es deseable si hay muchos usuarios que se van a analizar. Por otra parte, los usuarios pueden frustrarse. Por lo tanto, el objetivo debería ser disponer de sistemas biométricos más rápidos.
- Aceptación del usuario: A veces a la gente no le gusta el uso de máquinas para leer los patrones de sus ojos o manos. Esta es una de las razones de la baja aceptación del usuario. El bajo rendimiento es otra razón.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Consideraciones biométricas

Pregunta #20 de 105

Id. de pregunta: 1111755

Está implementando nuevas directivas de contraseñas en la red de su empresa. Debe asegurarse de que los usuarios deben usar 20 contraseñas nuevas antes de reutilizar una antigua. ¿Qué configuración de directiva de contraseñas debe implementar?

✗ **A)** complejidad de la contraseña

✗ **B)** longitud de la contraseña

✗ **C)** antigüedad de la contraseña

✗ **D)** bloqueo de contraseña

✓ **E)** historial de contraseñas

explicación

Debe implementar la configuración de directiva historial de contraseñas. El historial de contraseñas le permite configurar cuántas contraseñas nuevas se deben crear antes de que se pueda reutilizar una antigua. Esta configuración mejora la seguridad al permitir a los administradores asegurarse de que las contraseñas antiguas no se reutilizan continuamente. Las contraseñas reutilizadas a veces se conocen como contraseñas giratorias.

La antigüedad de la contraseña configura el número mínimo o máximo de días que pasan antes de que un usuario deba cambiar la contraseña. Es una buena práctica de seguridad aplicar una antigüedad de la contraseña de 30 a 60 días. Algunas empresas obligan a los usuarios a cambiar sus contraseñas mensual o trimestralmente. Este intervalo debe determinarse en función de la importancia de la información y de la frecuencia con la que se utilizan las contraseñas. La configuración de la configuración de antigüedad de la contraseña se ve afectada por lo siguiente:

- la criticidad de la información a proteger
- la frecuencia de uso de la contraseña (historial de contraseñas)
- las responsabilidades y la autorización del usuario

La longitud de la contraseña configura el número mínimo de caracteres que se deben utilizar en una contraseña. Como mínimo, esta directiva debe configurarse en 7 u 8 caracteres. Tenga cuidado de no configurar este valor demasiado alto, ya que puede hacer que la contraseña sea muy difícil de recordar.

Bloqueo de contraseña configura el número de intentos de inicio de sesión no válidos que pueden producirse antes de que se bloquee una cuenta. Normalmente, esta directiva de bloqueo de contraseña también le permite configurar el número de días que la cuenta permanece en este estado. En algunos casos, es posible que desee configurar la directiva de bloqueo de cuenta para que se deba ponerse en contacto con un administrador para habilitar la cuenta de nuevo.

La complejidad de la contraseña configura qué caracteres deben componer una contraseña para reducir la posibilidad de ataques de diccionario o fuerza bruta. Una directiva de complejidad de contraseña típica obligaría al usuario a incorporar números, letras y caracteres especiales. Además, se pueden requerir letras mayúsculas y minúsculas. Una

contraseña que usa una buena combinación, como Ba1e$23q, es más segura que una contraseña que solo implementa partes de estos requisitos, como My32birthday, NewYears06 y John$59. Un ataque de fuerza bruta es más complejo que un ataque de diccionario porque el ataque de fuerza bruta debe funcionar a través de todas las combinaciones posibles.

Las directivas de cuenta deben aplicarse en todos los sistemas de la empresa. También es una buena práctica asegurarse de que las contraseñas están enmascaradas o cifradas. Este cifrado debe producirse en el dispositivo de almacenamiento en el que se encuentran. Además, se debe utilizar el cifrado cuando se transmiten a través de la red.

Como práctica recomendada, la contraseña de un usuario nunca debe ser la misma que la cuenta de inicio de sesión.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Administrar el ciclo de vida de aprovisionamiento de identidad y acceso

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, tipos de contraseñas y gestión

---

Pregunta #21 de 105

Id. de pregunta: 1105347

Se le ha contratado como administrador de seguridad para una organización que utiliza el control de acceso obligatorio (MAC). Cuando se usa este tipo de control de acceso, ¿qué entidades componen una etiqueta de seguridad?

- ✓ **A)** clasificación y categorías
- ✗ **B)** roles y privilegios
- ✗ **C)** definiciones y permisos
- ✗ **D)** identidades y derechos

explicación

Cuando se utiliza el control de acceso obligatorio (MAC), una etiqueta de seguridad o sensibilidad se compone de una clasificación y diferentes categorías. La clasificación indica el nivel de sensibilidad del sujeto u objeto, como secreto o alto secreto. Las diferentes categorías aplican las reglas de necesidad de conocer al categorizar los sujetos y objetos en categorías, como recursos humanos y contabilidad. Las categorías deben ser determinadas por la organización en función de las necesidades de control de acceso de la organización.

Las demás entidades no son partes válidas de una etiqueta de seguridad.

MAC es más prohibitivo en la naturaleza. Por lo tanto, es más seguro que el control de acceso discrecional (DAC). Sin embargo, DAC es más flexible y escalable que MAC. EL MAC define los niveles de seguridad que se imponen en todos los temas y objetos.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Modelos de control de acceso

---

Pregunta #22 de 105

Id. de pregunta: 1105284

¿Qué tipo de tarjeta tiene una antena que rodea la tarjeta para permitir que la tarjeta sea leída por el lector?

- ✗ **A)** Tarjeta inteligente de contacto
- ✗ **B)** tarjeta de memoria
- ✗ **C)** tarjeta inteligente
- ✓ **D)** tarjeta inteligente sin contacto

explicación

Una tarjeta inteligente sin contacto tiene una antena que rodea la tarjeta para permitir que la tarjeta sea leída por el lector. Cuando la tarjeta entra en el campo electrónico del lector, la antena de la tarjeta alimenta el chip interno de la tarjeta y se comunica con el lector.

Una tarjeta inteligente es una tarjeta que puede almacenar y procesar información. No todas las tarjetas inteligentes contienen una antena. Una tarjeta inteligente de contacto tiene un sello dorado en la cara de la tarjeta, en lugar de una antena dentro de la tarjeta. Este tipo de tarjeta inteligente requiere inserción física en el lector de tarjetas.

Una tarjeta de memoria almacena información, pero no puede procesarla. También requiere inserción física en el lector de tarjetas.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Tarjetas inteligentes de administración de identidad y acceso

---

Pregunta #23 de 105

Id. de pregunta: 1111751

La red de su empresa ha alcanzado un tamaño tan grande que cada vez es más difícil administrar cuentas de usuario y contraseñas. La administración le ha pedido que investigue una solución en la nube que podría implementar para facilitar la administración e implementar el inicio de sesión único. ¿Qué solución de implementación en la nube debe sugerir>

- ✓ **A)** IDaas
- ✗ **B)** Paas
- ✗ **C)** IPaaS
- ✗ **D)** DBaas

explicación

La identidad como servicio (IDaaS) es una solución de administración de identidades basada en la nube que permitirá a una organización implementar el inicio de sesión único. Una solución IDaaS a través de un proveedor de nube generalmente incluye lo siguiente:

- Inicio de sesión único
- aprovisionamiento
- Administración de contraseñas
- Control de acceso
- Controles de acceso granulares
- Administración centralizada
- Integración con servicios de directorio internos
- Integración con servicios externos

Integration Platform as a Service (IPaaS) es una solución basada en la nube que permite el desarrollo, la ejecución y el gobierno de flujos de integración para conectarse en procesos, servicios, aplicaciones y datos locales y basados en la nube dentro de organizaciones individuales o en múltiples organizaciones.

La base de datos como servicio (DBaaS) es una solución basada en la nube que admite aplicaciones, sin que el equipo de aplicaciones asuma la responsabilidad de las funciones tradicionales de administración de bases de datos.

La plataforma como servicio (PaaS) es una solución basada en la nube que permite a los clientes desarrollar, ejecutar y administrar aplicaciones web sin tener que crear y mantener la infraestructura normalmente asociada con el desarrollo y el inicio de una aplicación.

Objetivo:
Administración de identidad y acceso (IAM)

Subobsecución:
Integrar la identidad como un servicio de terceros

Referencias:

Cissp Cert Guide (3rd Edition), Chapter 5: Identity and Access Management, Identity as a Service (IDaaS) Implementation

Una guía sencilla de Cloud Computing, IaaS, PaaS, SaaS, BaaS, DBaaS, iPaaS, IDaaS, APIMaaS, http://cloudramblings.me/2014/02/11/a-simple-guide-to-cloud-computing-iaas-paas-saas-baas-dbaas-ipaas-idaas-apimaas/

Pregunta #24 de 105

Id. de pregunta: 1132534

¿Qué amenazas de seguridad NO se autorreplican?

a. gusano

b. virus

c. software espía

d. Caballo de Troya

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

explicación

El spyware y los caballos de Troya son amenazas de seguridad que NO se autorreplican. El spyware es en realidad un tipo de caballo de Troya. Estos programas se descargan e instalan inadvertidamente cuando el usuario está descargando otros programas.

Tanto los virus como los gusanos pueden autorreplicarse, lo que significa que el virus o gusano puede copiarse a sí mismo en varias ubicaciones.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Administrar el ciclo de vida de aprovisionamiento de identidad y acceso

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5, Gestión de identidad y acceso, Spyware

Spyware, http://searchsecurity.techtarget.com/sDefinition/0,sid14_gci214518,00.html

Ataques de caballo de Troya, http://www.irchelp.org/irchelp/security/trojan.html

---

Pregunta #25 de 105

Id. de pregunta: 1111748

Su organización ha decidido agregar la autenticación con tarjeta inteligente al esquema de autenticación. ¿Qué ataque NO es aplicable a una tarjeta inteligente?

- ✗ **A)** ataque físico
- ✗ **B)** ataque de ingeniería social
- ✗ **C)** ataque lógico
- ✓ **D)** ataque de diccionario

explicación

El propósito principal de un ataque de diccionario es identificar las contraseñas comparándolas con un gran número de palabras en un diccionario. Este ataque utiliza la lógica de que muchos usuarios eligen contraseñas que son palabras de diccionario. Un programa de ataque de diccionario se alimenta con listas de palabras. El programa intenta todas las permutaciones y combinaciones posibles para derivar la contraseña de usuario. Este tipo de ataque se lleva a cabo en realidad contra contraseñas, no tarjetas inteligentes.

Los ataques a tarjetas inteligentes se pueden clasificar de la siguiente manera:

- Un ataque físico implica la manipulación o alteración de las condiciones físicas estándar de la tarjeta inteligente, como la temperatura, el voltaje y la frecuencia, para obtener información confidencial. En un ataque físico, el atacante inicia una fluctuación de voltaje mediante el uso de equipos especiales precisamente durante el proceso de verificación del número de identificación personal (PIN). Esto permite que las funciones de la tarjeta se realicen

de la misma manera que la de un usuario legítimo. Los ataques físicos se pueden combinar con ataques lógicos para obtener acceso a información confidencial.

- Un ataque lógico se produce cuando los usuarios no autorizados obtienen acceso al sistema mediante la supervisión y captura de los bytes de datos que van y desde la tarjeta inteligente. Un ataque de temporización es un ejemplo de un ataque lógico en el que los patrones de bytes se envían a la tarjeta para obtener la clave privada.
- Un ataque de caballo de Troya implica una aplicación de caballo de Troya instalada en una estación de trabajo. Cuando un usuario habilita la clave privada mediante el envío de un PIN válido para una aplicación de confianza, la aplicación no autorizada envía una solicitud a la tarjeta para comprobar digitalmente los datos. El uso de una arquitectura de controlador de dispositivo de acceso único en el sistema operativo es una contramedida utilizada para evitar un ataque de caballo de Troya. En esta contramedida, el sistema operativo garantiza que sólo una aplicación utiliza la tarjeta inteligente en un momento determinado.

La ingeniería social es la práctica de obtener información confidencial manipulando o engañando a usuarios legítimos. La ingeniería social elude las medidas de seguridad tecnológicas manipulando a las personas para que revelen información de autenticación crucial. El objetivo principal de la ingeniería social es obtener acceso no autorizado a los sistemas o la información o cometer fraude, intrusión en la red, espionaje industrial, robo de identidad o interrupción de la red. Por ejemplo, un atacante o un intruso que se hace pasar por un técnico de red puede pedir a los empleados los PIN de sus tarjetas inteligentes con el pretexto de la seguridad. Los atacantes e intrusos pueden usar posteriormente el PIN para obtener acceso no autorizado a los recursos confidenciales de la organización. La ingeniería social a menudo implica afirmar la autoridad o tirar de rango, intimidar o amenazar, o elogiar o halagar para obtener acceso físico a una instalación segura.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Ataque de diccionario

---

Pregunta #26 de 105

Id. de pregunta: 1192954

¿Qué tipos de ataque afectan a las contraseñas?

a. oler

b. diccionario

c. Fuerza bruta

d. Datos

e. denegación de servicio

f. ingeniería social

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

explicación

Las contraseñas son susceptibles a olfato, ataques de diccionario, ataques de fuerza bruta y ataques de ingeniería social. Además, las contraseñas a veces se pueden obtener obteniendo acceso a una red y accediendo al archivo de contraseñas.

El diddling de datos es un ataque que cambia los datos. Los usuarios autorizados suelen perpetuar este ataque para obtener ganancias financieras.

Un ataque de denegación de servicio se produce cuando un atacante inunda un sistema con ciertos tipos de mensajes para evitar que el sistema responda a solicitudes válidas.

El olfato se produce cuando un atacante captura información de una red para obtener contraseñas de usuario. Muchas veces esta técnica proporciona al atacante varias contraseñas de usuario. Para evitar esto, siempre debe cifrar su contraseña cuando se almacena en medios electrónicos o se transmite a través de la red.

Un ataque de diccionario y un ataque de fuerza bruta son muy similares en que ambos se centran en descifrar la contraseña. Las herramientas utilizadas en los ataques de diccionario y fuerza bruta a veces se conocen como galletas de contraseña.

Los ataques de diccionario emplean el uso de un diccionario de palabras como contraseña para intentar acceder repetidamente a un sistema utilizando una cuenta de usuario válida. Para protegerse contra ataques de diccionario, se debe aplicar una directiva de complejidad de contraseñas que requiera el uso de caracteres, números y símbolos en mayúsculas y minúsculas. Se puede ejecutar un ataque de diccionario largo contra un archivo de contraseña cifrado siempre que el atacante tenga acceso al sistema, tenga acceso de lectura al archivo de contraseña y conozca el mecanismo de cifrado utilizado para cifrar el archivo de contraseñas.

Los ataques de fuerza bruta, a veces conocidos como ataques exhaustivos, generalmente recorren un número más sustancial de posibilidades que pueden incluir caracteres, números y símbolos. Una directiva de longitud de cuenta que requiere una contraseña más larga afectaría al tiempo que tardaría un ataque manual de fuerza bruta. Un ataque de fuerza bruta también puede ser posible si se utilizan un token y un número de identificación personal (PIN) para acceder a un sistema y el token realiza la comprobación sin conexión del PIN. Para protegerse contra ataques de fuerza bruta, se debe aplicar una directiva de bloqueo de cuenta que bloquee la cuenta de un usuario después de un determinado número de inicios de sesión incorrectos.

Los ataques de ingeniería social aprovechan la credulidad del usuario para detectar las credenciales del usuario. Un ejemplo de un ataque de ingeniería social es una llamada de un usuario desconocido que se identifica como miembro del departamento de TI y solicita sus credenciales. La única manera de protegerse contra los ataques de ingeniería social es educar a los usuarios para que reconozcan y eviten dichos ataques.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Amenazas de contraseña

---

Pregunta #27 de 105

Id. de pregunta: 1105282

¿Cuál es otro término para la autenticación de dos factores?

- ✗ **A)** autenticación con tarjeta inteligente
- ✗ **B)** autenticación de nombre de usuario y contraseña
- ✓ **C)** autenticación segura
- ✗ **D)** autenticación biométrica

explicación

Otro término para la autenticación en dos fases es autenticación segura. La autenticación segura utiliza dos métodos para autenticar a un usuario. Este tipo de autenticación se puede implementar de muchas maneras. A veces, un usuario debe proporcionar un nombre de usuario y una contraseña, y también debe usar la autenticación biométrica para verificar la identidad. Otras veces, un usuario debe proporcionar un nombre de usuario y una contraseña, y usar una tarjeta inteligente para comprobar la identidad.

La autenticación segura se autentica mediante algo que una persona sabe, tiene o es. Dos de ellos se pueden incluir como parte del proceso de autenticación.

La autenticación biométrica autentica a un usuario en función de algo que la persona es y realiza una búsqueda uno a uno para verificar la afirmación de una identidad por parte de una persona. Esto incluye huellas dactilares, escaneos de iris, escaneos de retina, escaneos de palma de la mano e impresiones de voz.

La autenticación con tarjeta inteligente autentica a un usuario en función de algo que tiene el usuario. La tarjeta inteligente se inserta o se coloca dentro del intervalo de lectura de un lector de tarjetas inteligentes. Una vez leída la tarjeta, el usuario a veces introduce un número de identificación personal (PIN). La autenticación de nombre de usuario/contraseña autentica a un usuario en función de algo que el usuario sabe. El usuario debe proporcionar el nombre de usuario y la contraseña.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Administración de identidad y acceso, un solo factor frente a la autenticación multifactor

---

Pregunta #28 de 105

Id. de pregunta: 1105342

Durante una auditoría de seguridad reciente en su organización, se descubrió un sujeto no autorizado. Solo debe descubrir los derechos de acceso para este tema. ¿Qué entidad debería revisar?

- ✗ **A)** grupo
- ✓ **B)** tabla de capacidades
- ✗ **C)** lista de control de acceso (ACL)
- ✗ **D)** función de derechos de acceso

explicación

Debe revisar la tabla de capacidades del sujeto. Una tabla de capacidades se utiliza para mostrar los derechos de acceso de un sujeto perteneciente a una tabla determinada. Los sujetos están enlazados a tablas de capacidades.

Un grupo es un subconjunto de usuarios que se agrupan en función de su rol, pertenencia al departamento u otros criterios de calificación que determine el administrador del sistema. Se pueden asignar permisos a grupos para reducir

el esfuerzo administrativo para configurar el acceso.

Se utiliza una lista de control de acceso (ACL) para mostrar los derechos de acceso que los sujetos pueden tomar sobre los objetos. Los objetos están enlazados a ACL.

No existe tal cosa como una función de derechos de acceso.

El modelo de matriz de control de acceso garantiza que se concede a los sujetos el acceso adecuado para los objetos. Consta de una lista de sujetos, una lista de objetos, una función que devuelve el tipo de un objeto y la propia matriz, donde los objetos son columnas y los sujetos son filas. Este modelo se implementa normalmente mediante ACL y tablas de capacidades. Las filas de una matriz de control de acceso indican las capacidades que un usuario tiene para una serie de recursos. Las columnas de una matriz de control de acceso indican las capacidades que varios usuarios tienen para un único recurso.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Modelos de control de acceso

---

Pregunta #29 de 105

Id. de pregunta: 1105325

¿Qué actividad NO está cubierta por el objetivo de confidencialidad de la tríada de la CIA?

- ✗ **A)** ingeniería social
- ✗ **B)** surf de hombro
- ✓ **C)** traición
- ✗ **D)** buceo en contenedores de basura

explicación

La traición o subversión no es una actividad que equivale a una violación de la confidencialidad. Por lo tanto, la traición no se puede definir en el objetivo de confidencialidad de la tríada de Confidencialidad, Integridad y Disponibilidad (CIA).

Traición o subversión se refiere a un intento de destruir un órgano de gobierno autorizado. La traición es el delito de deslealtad a la nación o al estado. La confidencialidad es el nivel mínimo de secreto que se mantiene para proteger la información confidencial de la divulgación no autorizada.

Todas las demás opciones afectan el objetivo de confidencialidad de la tríada de la CIA.

El buceo en contenedores de basura se refiere a buscar en el área de recolección de basura o cubo de basura para buscar documentos confidenciales no triturados. El buceo en contenedores de basura puede revelar información confidencial que puede afectar la confidencialidad e integridad de la información a las personas. Por ejemplo, las impresiones no trituradas que contienen detalles del proyecto pueden llegar a personas no autorizadas.

El shoulder surf se refiere a examinar la computadora de alguien desde atrás para robar información confidencial, como contraseñas de usuario o información relacionada con negocios. Dicha información se puede utilizar para entrar en la red o el sistema y puede afectar la confidencialidad y la integridad de los activos de información de la organización.

La ingeniería social se refiere a engañar a alguien para que comparta información clasificada disfrazándose de una persona autorizada o utilizando las habilidades de las personas para obtener información patentada o confidencial. La ingeniería social se puede utilizar si los métodos técnicos de inmiscuirse en una red son inadecuados. La ingeniería social se utiliza para revelar información confidencial, como las contraseñas del sistema, que luego son utilizadas por el intruso para obtener acceso no autorizado al sistema o a la red.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Dumpster Diving

---

Pregunta #30 de 105

Id. de pregunta: 1105361

Como consultor, ha creado una nueva estructura de seguridad para una empresa que requiere que se emitan contraseñas a todos los empleados. El departamento de TI de la compañía ha hecho varias recomendaciones de distribución de contraseñas. ¿Qué método es el más seguro?

✗ **A)** Enviar un correo electrónico a cada usuario que contenga la contraseña del usuario.

✗ **B)** Emita la misma contraseña a todos los usuarios. Tras el inicio de sesión inicial, fuerce a los usuarios a cambiar sus contraseñas.

✓ **C)** Indique a los usuarios que informen al departamento de TI con la identificación adecuada para la configuración de la contraseña.

✗ **D)** Indique a los usuarios que envíen un correo electrónico de solicitud de contraseña.

explicación

Debe indicar a los usuarios que informen al departamento de TI con la identificación adecuada para la configuración de la contraseña. Esto garantizará que los usuarios tengan acceso a la cuenta adecuada para crear una contraseña de usuario.

No es seguro indicar a los usuarios que envíen un correo electrónico de solicitud de contraseña. El correo electrónico no está cifrado. Por lo tanto, cualquiera puede interceptar mensajes de correo electrónico.

Enviar un correo electrónico a cada usuario que contiene la contraseña del usuario no es seguro porque se puede interceptar el correo electrónico.

Emitir la misma contraseña a todos los usuarios y obligar a los usuarios a cambiar sus contraseñas al iniciar sesión inicial no es seguro. Inicialmente, cualquier usuario podría tener acceso a la cuenta de otro usuario, especialmente si utiliza un esquema de nomenclatura común para las cuentas de usuario. Si un usuario accede a la cuenta de otro usuario, puede cambiar la contraseña de ese usuario y acceder a todos los datos del usuario.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Administrar el ciclo de vida de aprovisionamiento de identidad y acceso

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Administración de identidad y acceso, ciclo de vida de aprovisionamiento

---

Pregunta #31 de 105

Id. de pregunta: 1105324

Se le ha pedido que implemente una solución RADIUS que permita el uso de voz sobre IP (VoIP) y servicios inalámbricos. ¿Qué implementación de RAIDUS debe utilizar?

✗ **A)** TACACS
✓ **B)** diámetro
✗ **C)** XTACACS
✗ **D)** TACACS+

explicación

Debe utilizar Diameter. Diameter se creó para abordar las nuevas tecnologías que RADIUS no fue diseñado para manejar, incluida la voz sobre IP (VoIP) y los servicios inalámbricos. Aunque Diameter fue diseñado para ser compatible con RADIUS, algunos servidores RADIUS tienen problemas para trabajar con servidores Diameter.

El sistema de control de acceso del controlador de acceso de terminal (TACACS) es la implementación de CISCO del RADIUS. TACACS es la primera generación y combina el proceso de autenticación y auditoría. XTACACS es la segunda generación y separa los procesos de autenticación, autorización y auditoría. TACACS+ es la tercera generación y proporciona todas las características de XTACACS junto con la autenticación de usuario de contraseña dinámica de dos factores extendida.

Objective:
Identity and Access Management (IAM)

Sub-Objective:
Integrate identity as a third-party service

Referencias:

Guía del CERT CISSP (3ra edición),capítulo 5: Administración de la identidad y del acceso, RADIUS y TACACS+

Pregunta #32 de 105

Id. de pregunta: 1114763

La administración de la empresa ha decidido implementar directivas de grupo para garantizar que las directivas de seguridad de la empresa se aplican en toda la organización. Debe desarrollar las directivas de grupo adecuadas para su empresa. ¿Qué entidades puede administrar con estas nuevas directivas?

a. usuarios

b. Equipos cliente

c. Equipos servidor

d. Controladores de dominio

- ✗ **A)** Opción d
- ✗ **B)** ninguna de las opciones
- ✗ **C)** opción A
- ✗ **D)** opción b
- ✗ **E)** opción c
- ✓ **F)** todas las opciones

explicación

Las directivas de grupo se pueden usar para administrar usuarios, equipos cliente, equipos servidor y controladores de dominio. Las directivas de grupo son la forma más eficaz de administrar un gran número de usuarios o equipos. Por ejemplo, puede configurar una directiva de grupo que obligue a los usuarios a cambiar su contraseña en el siguiente inicio de sesión.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Sistemas de gestión de credenciales de gestión de identidad y acceso

---

Pregunta #33 de 105

Id. de pregunta: 1105357

Debe determinar qué usuarios tienen acceso a un equipo con Windows Server 2008 desde la red. ¿Qué categoría de auditoría debe habilitar?

- ✗ **A)** Auditar eventos de inicio de sesión de cuenta
- ✗ **B)** Administración de cuentas de auditoría
- ✓ **C)** Uso de privilegios de auditoría
- ✗ **D)** Auditar el acceso a objetos

explicación

La categoría de auditoría Auditar privilegios Usar auditará todas las instancias de usuarios que ejerzan sus derechos. Esta categoría audita todos los derechos que se encuentran en la directiva de seguridad local en Configuración de seguridad\Directivas locales\Asignación de derechos de usuario. La directiva Tener acceso al equipo desde la red permite a los usuarios tener acceso a un equipo desde la red.

La categoría de auditoría Auditar eventos de inicio de sesión de cuenta realiza un seguimiento de todos los intentos de iniciar sesión con una cuenta de usuario de dominio cuando está habilitada en controladores de dominio. Si habilita esta directiva en una estación de trabajo o servidor miembro, registrará los intentos de iniciar sesión mediante una cuenta local almacenada en la base de datos de cuentas de usuario de ese equipo.

La categoría auditoría De administración de cuentas de auditoría supervisa los cambios en las cuentas de usuario y los grupos.

La categoría de auditoría Auditar acceso a objetos realiza un seguimiento del acceso a todos los objetos fuera de Active Directory.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Administrar el ciclo de vida de aprovisionamiento de identidad y acceso

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Responsabilidad

Información general: Uso de privilegios de auditoría, http://www.ultimatewindowssecurity.com/Wiki/AuditCategory-PrivilegeUseLegacy.ashx

---

Pregunta #34 de 105

Id. de pregunta: 1192955

Está implementando la administración de acceso empresarial para su empresa. Debe asegurarse de que el sistema que implementa le permite configurar una confianza con otra empresa para que los usuarios puedan acceder a la red de la otra empresa sin necesidad de iniciar sesión de nuevo. ¿Qué debe implementar para asegurarse de que se puede configurar esta confianza?

- ✗ **A)** biometría
- ✗ **B)** tarjetas inteligentes
- ✓ **C)** administración de identidades federadas
- ✗ **D)** administración de contraseñas

explicación

Para asegurarse de que puede configurar una confianza con otra empresa que permita a los usuarios tener acceso a la red de la otra empresa sin volver a iniciar sesión, debe implementar la administración de identidades federadas. La administración de identidades federadas permite el inicio de sesión único (SSO) entre empresas.

La administración de contraseñas es necesaria en cualquier implementación de administración de acceso empresarial. Si las contraseñas no se administran correctamente, es probable que se produzcan infracciones de seguridad. Sin embargo, la administración de contraseñas no garantizará que se pueda configurar la confianza entre las empresas.

Las tarjetas inteligentes proporcionan un mecanismo de inicio de sesión y autenticación más seguro que las contraseñas. Sin embargo, las tarjetas inteligentes no garantizarán que se pueda configurar la confianza entre las empresas.

La biometría proporciona un mecanismo de inicio de sesión y autenticación más seguro que las contraseñas o las tarjetas inteligentes. Sin embargo, la biometría no garantizará que se pueda configurar la confianza entre las empresas.

La gestión de acceso empresarial (EAM) proporciona servicios de gestión de control de acceso a sistemas empresariales basados en web. EAM proporciona SSO, control de acceso basado en roles y adaptación de una variedad de mecanismos de autenticación, incluidas contraseñas, tarjetas inteligentes y biometría.

Objetivo:
Administración de identidad y acceso (IAM)

Subobsecución:
Integrar la identidad como un servicio de terceros

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Identity and Access Management Federated Identity Management

Tendencias en la gestión de acceso e identidad empresarial, http://searchsecurity.techtarget.com/tip/Trends-in-enterprise-identity-and-access-management?ShortReg=1&mboxConv=searchSecurity_RegActivate_Submit&

Las peores prácticas: Tres grandes errores de administración de identidad y acceso, http://searchsecurity.techtarget.com/tip/Worst-Practices-Three-big-identity-and-access-management-mistakes

---

Pregunta #35 de 105

Id. de pregunta: 1114766

Está diseñando los procedimientos para la revisión de la cuenta de usuario de su empresa. ¿Qué acciones debe incluir como parte de esta revisión?

un. Asegúrese de que todas las cuentas están activas.

B. Asegúrese de que no hay cuentas duplicadas.

c. Asegúrese de que todas las cuentas activas tienen una contraseña.

d. Asegúrese de que todas las contraseñas siguen las reglas de complejidad.

E. Asegúrese de que todas las cuentas se ajustan al principio de privilegios mínimos.

- ✗ **A)** opción e
- ✗ **B)** todas las opciones
- ✗ **C)** opción c
- ✗ **D)** opción b

✗ **E)** Sólo las opciones A y B

✗ **F)** opción A

✓ **G)** Opciones C y E Solamente

✗ **H)** Opción d

explicación

Al implementar revisiones de cuentas de usuario, debe asegurarse de que todas las cuentas de usuario activas tengan una contraseña y que todas las cuentas de usuario se ajusten al principio de privilegios mínimos.

No es necesario asegurarse de que todas las cuentas están activas. En la mayoría de los sistemas, normalmente hay algunas cuentas inactivas. Estas cuentas se pueden mantener para los empleados con licencia extendida. Además, no es necesario asegurarse de que no hay cuentas duplicadas. Las cuentas duplicadas pueden ser necesarias en algunos casos.

No es necesario asegurarse de que todas las contraseñas siguen las reglas de complejidad. Esto forma parte del mantenimiento de contraseñas, no del mantenimiento de cuentas.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Administrar el ciclo de vida de aprovisionamiento de identidad y acceso

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, gestión de identidad y cuentas

---

Pregunta #36 de 105

Id. de pregunta: 1105352

¿Qué modelo de control de acceso suele estar asociado a una directiva de seguridad de varios niveles?

✗ **A)** control de acceso discrecional (DAC)

✓ **B)** control de acceso obligatorio (MAC)

✗ **C)** control de acceso basado en roles (RBAC)

✗ **D)** control de acceso basado en reglas

explicación

Una directiva de seguridad de varios niveles se asocia generalmente al control de acceso obligatorio (MAC). En MAC, las etiquetas de sensibilidad, también llamadas etiquetas de seguridad, se adjuntan a todos los objetos. Estas

etiquetas de confidencialidad contienen una clasificación. Para que un sujeto tenga acceso de escritura a un objeto en una política de seguridad de varios niveles, la etiqueta de confidencialidad del sujeto debe dominar la etiqueta de confidencialidad del objeto.

El control de acceso basado en reglas es una técnica de control de acceso, no un modelo de control de acceso.

El control de acceso basado en roles (RBAC) permite que el acceso a los recursos esté controlado por el rol del usuario.

El control de acceso discrecional (DAC) permite al propietario del recurso determinar el nivel de acceso que tienen los usuarios.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Control de acceso obligatorio

---

Pregunta #37 de 105

Id. de pregunta: 1105274

Durante una transacción financiera reciente, se proporcionó una firma digital y efectivo digital. El efectivo digital se marca como identificado. ¿Qué se quiere decir con esto?

- ✗ **A)** se conoce la identidad de la institución financiera
- ✓ **B)** se conoce la identidad del titular del efectivo
- ✗ **C)** se conoce la identidad del comerciante
- ✗ **D)** Se conoce el tipo monetario del efectivo

explicación

Cuando el efectivo digital se marca como identificado, se conoce la identidad del titular del efectivo. Cuando el efectivo digital se marca como anónimo, se desconoce la identidad del titular del efectivo.

El efectivo digital anónimo no identifica al titular del efectivo y utiliza esquemas de firma ciega. El efectivo digital identificado utiliza firmas digitales convencionales para identificar al titular del efectivo.

Ninguna de las otras opciones es correcta.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Efectivo digital, http://www.cs.bham.ac.uk/~mdr/teaching/modules06/netsec/lectures/DigitalCash.html

---

Pregunta #38 de 105

Id. de pregunta: 1192942

Un atacante desea detectar qué dispositivos front-end están en uso en la red de su organización. ¿Qué tipo de dispositivo debe usar el atacante?

- ✗ **A)** Troyanos
- ✓ **B)** Sondas
- ✗ **C)** spyware
- ✗ **D)** cortafuegos

explicación

Un atacante debe usar sondeos para detectar qué dispositivos front-end están en uso en la red de su organización.

Los firewalls se utilizan para permitir o denegar cierto tráfico dentro o fuera de una red. El spyware es un tipo de malware que espía al usuario y registra las acciones del usuario y, a menudo, las entradas. Un caballo de Troya es un tipo de malware que engaña a los usuarios de su verdadera intención.

Objetivo:
Administración de identidad y acceso (IAM)

Subobsecución:
Controlar el acceso físico y lógico a los activos

Referencias:

Cómo controlar e identificar sondeos de red,
http://cecs.wright.edu/~pmateti/Courses/499/Probing/How%20to%20Handle%20Network%20Probes.htm

---

Pregunta #39 de 105

Id. de pregunta: 1111753

La administración le pide que proporcione una lista de todos los controles de acceso que detectarán cuando se produce un problema de seguridad. ¿Qué control es un ejemplo de esto?

- ✓ **A)** registro de auditoría
- ✗ **B)** lista de control de acceso (ACL)
- ✗ **C)** encriptación
- ✗ **D)** enrutador

explicación

Un registro de auditoría es un ejemplo de un control técnico detectivesco porque detecta las infracciones de seguridad una vez que se han producido. Un registro de auditoría también se considera un control técnico compensativo.

Los enrutadores, los firewalls y las listas de control de acceso (ACL) son ejemplos de controles técnicos preventivos porque evitan las infracciones de seguridad. Todos ellos son también controles técnicos compensativos.

Hay tres categorías de control de acceso: controles técnicos, administrativos y físicos. Un control técnico es un control que se pone en marcha para restringir el acceso. Los controles técnicos funcionan para proteger el acceso al sistema, la arquitectura y el acceso a la red, las zonas de control, la auditoría y el cifrado y los protocolos. Un administrativo se desarrolla para dictar cómo se implementan las políticas de seguridad para cumplir con los objetivos de seguridad de la empresa. Los controles administrativos incluyen políticas y procedimientos, controles de personal, estructura de supervisión, capacitación en seguridad y pruebas. Un control físico es un control que se implementa para proteger el acceso físico a un objeto, como un edificio, una sala o un equipo. Los controles físicos incluyen insignias, cerraduras, guardias, segregación de red, seguridad perimetral, controles informáticos, separación de áreas de trabajo, copias de seguridad y cableado.

Las tres categorías de control de acceso proporcionan siete funcionalidades o tipos diferentes:

- Preventivo - Un control preventivo previene brechas de seguridad y evita riesgos.
- Detective - Un control detective detecta las brechas de seguridad a medida que ocurren.
- Correctivo : un control correctivo restaura el control e intenta corregir cualquier daño infligido durante una infracción de seguridad.
- Disuasión - Un control disuasorio disuade posibles violaciones.
- Recuperación: un control de recuperación restaura los recursos.
- Compensativo: un control compensativo proporciona un control alternativo si otro control puede ser demasiado costoso. Por lo general, todos los controles se consideran compensativos.
- Directiva - Un control de directiva proporciona controles obligatorios basados en regulaciones o requisitos ambientales.

Cada categoría de control incluye controles que proporcionan funciones diferentes. Por ejemplo, una insignia de seguridad es tanto un control físico preventivo como un control físico compensativo. La supervisión y supervisión es tanto un control administrativo detectivesco como un control administrativo compensativo.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Responsabilidad

---

Pregunta #40 de 105

Id. de pregunta: 1114756

¿En qué situaciones debe una organización instruir a su fuerza de trabajo para que use varios dedos para la autenticación en un sistema biométrico?

un. La calidad de las huellas dactilares de los usuarios no es suficiente.

B. La organización necesita minimizar los errores de tipo 1.

c. La organización necesita permitir una autenticación más rápida de los empleados.

d. La organización necesita múltiples registros de referencia y, por lo tanto, un FAR más bajo.

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

explicación

Un gran porcentaje de la fuerza de trabajo no tiene una calidad de huellas dactilares que sea lo suficientemente buena para un escaneo de huellas dactilares. Esto implica que es difícil para un sistema biométrico verificar con precisión las credenciales de usuario. Se pueden utilizar varios dedos para proporcionar múltiples patrones a un sistema biométrico. Esto garantiza un mayor nivel de precisión durante la autenticación. Las estadísticas significativamente mejoradas obtenidas mediante el uso de escaneo de múltiples huellas dactilares da como resultado una tasa de rechazo falso (FRR) y una tasa de aceptación falsa (FAR) mejoradas.

El uso de varios dedos no permitirá una autenticación más rápida de los empleados. El tiempo que tarda un sistema biométrico en procesar las credenciales de usuario no depende del número de huellas dactilares utilizadas para el proceso de autenticación. Un sistema diferente, como un sistema de escaneo de dedos, permitiría una autenticación más rápida porque no hay tantas características para comparar en algunos otros sistemas.

Un sistema biométrico crea un único registro de referencia para cada usuario, independientemente del número de huellas dactilares que se han escaneado durante el proceso de inscripción. FAR y FRR no se ven afectados por el tamaño o el número de los registros de referencia.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 5: Gestión de identidad y acceso, Características fisiológicas

---

Pregunta #41 de 105

Id. de pregunta: 1192949

Su organización ha implementado un sistema biométrico de escaneo de geometría de mano que controlará el acceso al centro de procesamiento de datos. ¿Qué características NO son evaluadas por este sistema biométrico? (Elija todo lo que se aplique).)

- ✗ **A)** ancho de la mano
- ✓ **B)** finales de cresta
- ✗ **C)** ancho de los dedos
- ✗ **D)** longitud de los dedos
- ✓ **E)** tono de piel de la mano

explicación

Un sistema biométrico que realiza un escaneo de la geometría de la mano no evaluará las terminaciones de la cresta en los dedos o las características de la piel de la mano. Las terminaciones de cresta y las bifurcaciones en los dedos se evalúan mediante un sistema biométrico de escaneo de huellas dactilares, no mediante un sistema biométrico de escaneo de geometría de mano.

La geometría de la mano de una persona se puede utilizar como base de un sistema biométrico. La geometría de las manos de una persona, es decir, la forma de la mano, la longitud de los dedos y el ancho de la mano, son características únicas. Un sistema biométrico que realiza un escaneo de geometría de mano identificará esas

características para autenticar a un usuario. El sistema compara los atributos del usuario con los registros de referencia que se recopilaron durante la fase de inscripción. Si los atributos coinciden, se concede acceso al usuario. Los sistemas biométricos basados en el escaneo de geometría manual pueden usar la técnica mecánica o de detección de imágenes para autenticar las credenciales de usuario. Ambos métodos comprueban los atributos de mano de un usuario con fines de autenticación.

Actualmente no hay sistemas utilizados para escanear e identificar características únicas de la piel de una persona que se pueden utilizar para autenticar a la persona. Los resultados de una exploración de la piel no son precisos, pero se pueden almacenar como referencia. Una razón importante para NO usar un escaneo de piel como un sistema biométrico para la autenticación de empleados es la falta de cualquier estándar preciso y aceptable. Sin tal estándar, la autenticación podría ser cuestionada.

Una exploración facial se basa en la estructura ósea de un individuo, la cresta de la nariz, el ancho de los ojos, la estructura de la frente y la forma de la barbilla. Tales características son capturadas por una cámara y comparadas con los registros de referencia de un empleado reunidos durante el proceso de inscripción.

Los sistemas de huellas digitales coinciden con características únicas, denominadas coincidencia de minucias, para autenticar o denegar una solicitud de acceso. Un sistema biométrico de huellas dactilares basado en la coincidencia de minucias compara la ubicación y la dirección de las terminaciones de la cresta y las bifurcaciones de una huella digital.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 5: Gestión de identidad y acceso, Características fisiológicas

---

Pregunta #42 de 105

Id. de pregunta: 1114758

Su organización está considerando lanzar una solución de identidad como servicio (IDaaS) a través de un proveedor de nube. Necesita IDaaS para proporcionar los siguientes servicios:

A. Inicio de sesión único

B. Aprovisionamiento

C. Gestión de contraseñas

D. gobernanza del acceso

¿Cuáles se suelen incluir como parte de esta solución?

✗ **A)** Sólo C y D

✗ **B)** A, B y C

✓ **C)** Todos los servicios

✗ **D)** Sólo A y B

✗ **E)** Sólo B y C

explicación

Una solución IDaaS a través de un proveedor de nube generalmente incluye lo siguiente:

- Inicio de sesión único
- aprovisionamiento
- Administración de contraseñas
- Control de acceso

La solución también puede incluir lo siguiente:

- Controles de acceso granulares
- Administración centralizada
- Integración con servicios de directorio internos
- Integración con servicios externos

Objetivo:
Administración de identidad y acceso (IAM)

Subobsecución:
Integrar la identidad como un servicio de terceros

Referencias:

Cissp Cert Guide (3rd Edition), Chapter 5: Identity and Access Management, Identity as a Service (IDaaS) Implementation

---

Pregunta #43 de 105

Id. de pregunta: 1114762

¿Qué métodos de control de acceso se consideran de naturaleza no discrecional?

a. CAD

b. MAC

c. RBAC

d. CBAC

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

explicación

El control de acceso basado en roles (RBAC), el control de acceso obligatorio (MAC) y el control de acceso basado en contexto (CBAC) se consideran de naturaleza no discrecional. Los métodos no discrecionales son aquellos que se basan estrictamente en directivas de seguridad o niveles de seguridad para determinar el acceso a objetos.

El control de acceso discrecional (DAC) permite al propietario del recurso determinar el nivel de acceso a los recursos que se concede a un usuario.

Los métodos de control de acceso no discrecional suelen utilizar una autoridad central cuya responsabilidad es determinar los derechos de acceso de un sujeto en función de una política de seguridad. Dado que la autoridad de control de acceso no diseña la directiva de seguridad, sino que la aplica, el control de acceso se basa en el rol, las responsabilidades o los deberes del usuario dentro de la organización. El control de acceso basado en celosía es otro ejemplo de un método de control de acceso no discrecional.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Modelos de control de acceso

---

Pregunta #44 de 105

Id. de pregunta: 1105304

Su organización desea verificar a un empleado por el patrón de vasos sanguíneos en la parte posterior de los ojos del empleado. ¿Qué sistema biométrico se recomienda para la autenticación en esta situación?

✓ **A)** exploración de la retina

✗ **B)** exploración facial

✗ **C)** exploración del iris

✗ **D)** reconocimiento ocular

explicación

Un escáner de retina es un sistema biométrico que examina el patrón único de los vasos sanguíneos en la parte posterior del ojo de un individuo. En una exploración de la retina, un haz se proyecta dentro del ojo para capturar el patrón, y compararlo con los expedientes de la referencia del individuo. El empleado se autentica solo si se encuentra una coincidencia. El escaneo de retina proporciona una mejor precisión que el escaneo de iris.

Hay algunas desventajas de usar una exploración de la retina. Los empleados a veces son reacios a pasar por un escáner de retina porque la prueba se considera demasiado intrusiva. Además, los resultados de la exploración de la retina pueden alterar durante un período de tiempo. Otras desventajas son el gasto, el tiempo de inscripción y la complejidad que implica su implementación.

Una exploración del iris se basa en el examen de patrones únicos, colores, anillos y coronas del ojo de un individuo. Cada característica es capturada por una cámara y comparada con los registros de referencia de un empleado reunidos durante el proceso de inscripción. El escaneo de iris proporciona una mejor precisión que la huella digital, el reconocimiento de voz o el reconocimiento facial.

Una exploración facial se basa en la estructura ósea de un individuo, la cresta de la nariz, el ancho de los ojos, la estructura de la frente y la forma de la barbilla. Tales características son capturadas por una cámara y comparadas con los registros de referencia de un empleado reunidos durante el proceso de inscripción.

El reconocimiento ocular no es una tecnología de escaneo biométrico utilizada para la autenticación de un individuo.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 5: Gestión de identidad y acceso, Características fisiológicas

---

Pregunta #45 de 105

Id. de pregunta: 1113988

A su organización se le ha otorgado un contrato del gobierno federal. Se le ha indicado que configure un servidor con un sistema operativo que aplique las reglas de control de acceso requeridas por el gobierno federal. ¿Qué método de

control de acceso se implementará?

- ✓ **A)** control de acceso obligatorio
- ✗ **B)** control de acceso basado en identidad
- ✗ **C)** control de acceso basado en roles
- ✗ **D)** control de acceso discrecional

explicación

Se implementará el control de acceso obligatorio (MAC). Se utilizan etiquetas de seguridad, como secreto, alto secreto, etc. Este modelo requiere que se use un sistema operativo diseñado específicamente para él para aplicar sus reglas. SE Linux y Trusted Solaris son dos ejemplos de sistemas operativos diseñados específicamente para entornos MAC.

La mayoría de los sistemas operativos estándar se pueden utilizar para aplicar los otros métodos de control de acceso dados. Se pueden implementar mediante cuentas de usuario, cuentas de grupo y permisos.

En MAC, sólo un administrador puede cambiar la categoría o clasificación de un sujeto u objeto. Un derecho de acceso que está expresamente prohibido en la directiva de control de acceso nunca se puede conceder en un entorno MAC.

El control de acceso basado en identidad es un tipo de control de acceso discrecional.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Modelos de control de acceso

---

Pregunta #46 de 105

Id. de pregunta: 1105355

¿Qué tipo de virus incluye código de protección que impide el examen externo de elementos críticos?

- ✗ **A)** virus del fago
- ✗ **B)** virus de sigilo
- ✗ **C)** virus acompañante
- ✓ **D)** virus blindado

explicación

Un virus blindado incluye código de protección que impide el examen de elementos críticos, como los análisis mediante software antivirus. La armadura intenta dificultar la destrucción del virus.

Un virus complementario se une a programas legítimos y crea un programa con una extensión de archivo diferente. Cuando el usuario intenta acceder al programa legítimo, el virus complementario se ejecuta en lugar del programa legítimo.

Un virus fago modifica otros programas y bases de datos. La única manera de eliminar el virus es volver a instalar las aplicaciones infectadas.

Un virus oculto impide la detección al ocultarse de las aplicaciones. Puede informar de un tamaño de archivo diferente que el tamaño de archivo real como un método para evitar la detección.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Administrar el ciclo de vida de aprovisionamiento de identidad y acceso

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5, Gestión de identidad y acceso, Virus

Virus blindado, http://www.webopedia.com/TERM/A/Armored_Virus.html

---

Pregunta #47 de 105

Id. de pregunta: 1105296

Se le ha pedido que implemente un sistema biométrico que analice tanto los movimientos físicos realizados cuando se firma una firma como las características específicas de la firma en sí. ¿Qué método biométrico debe implementar?

- ✗ **A)** geometría de la mano
- ✗ **B)** dinámica de pulsaciones de teclas
- ✗ **C)** firma digital
- ✓ **D)** dinámica de firmas

explicación

Debe implementar la dinámica de firmas. La dinámica de firma es el método biométrico que analiza tanto los movimientos físicos realizados cuando se firma una firma como las características específicas de la firma de una

persona. Por lo general, captura la velocidad de la firma, la presión de la pluma al firmar y la forma en que se sostiene la pluma.

La geometría de la mano es un método biométrico que analiza la longitud y el ancho de la mano. Una firma digital es un método mediante el cual se verifica la identidad de la persona que envía los datos. Garantiza que los datos originales no se han modificado. La dinámica de pulsaciones de teclas registra la velocidad y el movimiento de un usuario al introducir una frase y la compara con los datos almacenados.

La verificación dinámica de firmas (DSV) es otro término para la dinámica de firmas.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, factores característicos

---

Pregunta #48 de 105

Id. de pregunta: 1105281

¿Qué sistema biométrico de identificación facial es el más utilizado?

- ✗ **A)** procesamiento automático de rostros
- ✗ **B)** eigenfaces
- ✗ **C)** red neuronal
- ✓ **D)** análisis de características

explicación

El análisis de características es el sistema biométrico de identificación facial más utilizado. Si bien es muy similar a la técnica de eigenfaces, el análisis de características permite cambios en las expresiones faciales, como fruncir el ceño y sonreír.

La técnica de las caras propias no es tan ampliamente utilizada como la técnica de análisis de características. Eigenfaces utiliza una escala de grises global bidimensional para identificar las características distintivas de la cara de una persona. Se está desarrollando una variación de la técnica de las caras propias llamada características propias. Se basa en métricas faciales.

Las redes neuronales no son tan ampliamente utilizadas debido a su complejidad. Comparan las características de la cara viva con las características de la cara de referencia, o la cara almacenada. Las redes neuronales pueden

identificar rostros en circunstancias menos que ideales.

El procesamiento automático de la cara utiliza relaciones de distancia entre los rasgos faciales. No es tan robusto como las otras tecnologías, pero puede ser una buena opción en situaciones poco iluminadas.

El sistema de identificación facial utiliza la detección y el reconocimiento para procesar las imágenes faciales.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, factores característicos

---

Pregunta #49 de 105

Id. de pregunta: 1192944

Se le ha pedido que controle el uso de unidades USB portátiles en su dominio de Windows. ¿Cuál es la mejor manera de hacerlo con el menor esfuerzo administrativo?

- ✗ **A)** Deshabilite los dispositivos USB a través de una directiva de grupo local.
- ✗ **B)** Quite el archivo .cab controlador de cada equipo.
- ✗ **C)** Deshabilite USB a través de los programas de BIOS de las computadoras.
- ✓ **D)** Deshabilite los dispositivos USB a través de una directiva de grupo de dominio.

explicación

Debe deshabilitar el uso de USB a través de una directiva de grupo de dominio. Esto proporcionará un medio centralizado para administrar dispositivos USB. Más adelante, si un usuario o grupo determinado necesita usar un dispositivo USB, puede crear una directiva de unidad USB diferente para ese usuario o grupo e implementarla en el nivel de dominio adecuado. Los dos principales riesgos de seguridad de las unidades USB son su facilidad de ocultación y la capacidad de datos. Es muy fácil ocultar una unidad USB o disfrazarla como otra cosa. Además, la capacidad de datos para dispositivos USB sigue aumentando, lo que permite que cientos de gigabytes (GB) de información se almacenen en un solo dispositivo.

No debe deshabilitar el uso de USB a través de una directiva de grupo local. Esto requeriría que la directiva de grupo se implementara en cada equipo. Además, sería posible que un usuario local cambiara esta configuración. Si necesita habilitar usbs para un usuario o grupo después de deshabilitar el uso de USB a través de una directiva de grupo local, sería necesario cambiar la directiva en cada equipo.

No debe deshabilitar el uso de USB a través de los programas de BIOS de las computadoras. Esto requeriría cambiar la configuración en cada equipo. También sería posible que los usuarios locales volviera a habilitar el uso de USB localmente. Más adelante, si necesitara habilitar USB para un usuario o grupo, sería necesario cambiar la configuración del BIOS en cada equipo.

No debe quitar el archivo driver.cab de cada equipo. Si bien esto impediría la instalación de la mayoría de los dispositivos USB, también afectaría a la instalación de cualquier dispositivo que requiera archivos de controladores de Windows.

Objetivo:
Administración de identidad y acceso (IAM)

Subobsecución:
Controlar el acceso físico y lógico a los activos

Referencias:

Deshabilitar el almacenamiento USB con la directiva de grupo, HYPERLINK "http://www.windowsdevcenter.com/pub/a/windows/2005/11/15/disabling-usb-storage-with-group-policy.html" \t "sean" http://www.windowsdevcenter.com/pub/a/windows/2005/11/15/disabling-usb-storage-with-group-policy.html

---

Pregunta #50 de 105

Id. de pregunta: 1105288

Su empresa implementa actualmente Kerberos para proporcionar autenticación a todos los usuarios de la red. La administración ha oído hablar recientemente de debilidades de seguridad en el protocolo Kerberos. Le han pedido que implemente un protocolo de autenticación que aborde los puntos débiles de Kerberos. ¿Qué protocolo debe implementar?

- ✗ **A)** TACACS
- ✓ **B)** sésamo
- ✗ **C)** radio
- ✗ **D)** XTACACS

explicación

Debe implementar Secure European System for Applications en un entorno de múltiples proveedores (SESAME). SESAME fue desarrollado para mejorar las debilidades de Kerberos. A diferencia de Kerberos, SESAME utiliza cifrado simétrico y asimétrico para proteger el intercambio de datos y autenticar a los sujetos. SESAME utiliza un servidor de autenticación de confianza en cada host. Incorpora dos certificados o vales, uno para la autenticación y otro que define los privilegios de acceso. Utiliza criptografía de clave pública para la distribución de claves secretas

RADIUS, TACACS y XTACACS son todos protocolos de autenticación para usuarios remotos. Ninguno de estos servicios se desarrolló para mejorar las debilidades de Kerberos.

Kerberos y SESAME proporcionan una entidad centralizada que se utiliza para autenticar a los usuarios. Esta misma entidad es responsable de ayudar a garantizar que los sujetos estén debidamente autorizados mediante tokens o tickets. Por lo tanto, ambos servicios direcciona la autorización y la autenticación.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, SESAME

Pregunta #51 de 105

Id. de pregunta: 1105299

¿Cuál es la forma más común de identificación y autenticación?

- ✗ **A)** biometría
- ✓ **B)** identificación del usuario con contraseña reutilizable
- ✗ **C)** tarjetas inteligentes
- ✗ **D)** autenticación de dos factores

explicación

La forma más común de identificación y autenticación es la identificación del usuario con contraseña reutilizable. Las identificaciones de usuario (ID) y las contraseñas son algo que un usuario sabe.

La biometría, aunque no es la forma más común de identificación y autenticación, es más segura que el uso de la identificación del usuario y las contraseñas. La biometría es algo que eres. Una huella digital, por ejemplo, sería más segura que una contraseña, porque su huella digital nunca cambiará.

Las tarjetas inteligentes, algo que tiene, no se implementan comúnmente debido a los gastos. Sin embargo, son más seguros que el uso de la identificación del usuario y las contraseñas. Las tarjetas inteligentes son un factor de autenticación de tipo 2.

La autenticación de dos factores debe incluir dos de las siguientes tres categorías: algo que sabes (Tipo I), algo que tienes (Tipo II) o algo que eres (Tipo III). La autenticación en dos fases no es tan común como el uso de la identificación de usuario y las contraseñas.

Las contraseñas se consideran el mecanismo de autenticación más débil. Las frases de contraseña son algo más fuertes debido a su complejidad.

Al evaluar los controles de identificación y autenticación, es bueno mantener una lista de usuarios autorizados y sus niveles de acceso aprobados. Se debe implementar una directiva de contraseñas que obligue a los usuarios a cambiar sus contraseñas a intervalos predefinidos. Las cuentas de usuario deben ser canceladas cuando se termina el empleo, o suspendidas mientras el usuario está de vacaciones o licencia. Las directivas de bloqueo de cuenta pueden garantizar que los intentos de inicio de sesión fallidos finalmente den lugar a que se bloquee una cuenta.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Identity and Access Management, Identification and Authentication Implementation

---

Pregunta #52 de 105

Id. de pregunta: 1105314

¿Qué permite a los usuarios de acceso remoto iniciar sesión en una red a través de una base de datos de autenticación compartida?

✗ **A)** DES
✓ **B)** radio
✗ **C)** SSH
✗ **D)** IPSec

explicación

El Servicio de usuario de acceso telefónico de acceso remoto (RADIUS) permite a los usuarios de acceso remoto iniciar sesión en una red a través de una base de datos de autenticación compartida. Cuando un usuario remoto inicia sesión en una red que utiliza RADIUS, un cliente RADIUS envía las credenciales de un usuario remoto a un servidor RADIUS. Un servidor RADIUS comprueba las credenciales de un usuario remoto y envía una respuesta al cliente RADIUS. Si las credenciales del usuario remoto son válidas, el cliente RADIUS permitirá al usuario remoto iniciar sesión en la red. Si las credenciales del usuario remoto no son válidas, el cliente RADIUS no permitirá que el usuario remoto inicie sesión en la red. Un programa de marcación de guerra es normalmente utilizado por los atacantes para acceder a la red interna de una empresa a través de su sistema de acceso remoto.

Estándar de cifrado de datos (DES) es un estándar de cifrado de clave privada que se puede utilizar para cifrar archivos. El protocolo de seguridad de Internet (IPSec) se puede utilizar para firmar y cifrar digitalmente paquetes de protocolo de Internet (IP). Secure Shell (SSH) es un método para proteger las sesiones entre equipos de red. SSH se utiliza a menudo en entornos Unix, pero también está disponible para equipos Windows y OS/2.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Guía del CERT CISSP (3ra edición),capítulo 5: Administración de la identidad y del acceso, RADIUS y TACACS+

Seguridad del protocolo RADIUS y mejores prácticas, http://technet.microsoft.com/en-us/library/bb742489.aspx

---

Pregunta #53 de 105

Id. de pregunta: 1192950

Una institución de investigación militar está planeando implementar un sistema biométrico para garantizar la privacidad y confidencialidad totales dentro de la institución. Cuatro proveedores diferentes han dado las especificaciones de sus sistemas biométricos. Teniendo en cuenta las siguientes especificaciones, ¿qué opción se recomienda para la institución?

- ✓ **A)** Proveedor A: Errores de tipo 1 80%, errores de tipo 2 1%, CER 4%
- ✗ **B)** Proveedor C: Errores de tipo 1 65%, errores de tipo 2 8%, CER 35%
- ✗ **C)** Proveedor D: Errores de tipo 1 15%, errores de tipo 2 50%, CER 30%
- ✗ **D)** Proveedor B: Errores de tipo 1 45%, errores de tipo 2 10 %, CER 8%

explicación

El sistema biométrico con el valor de tasa de error cruzado (CER) de 4 es mejor que los otros dispositivos biométricos.

Las instituciones de investigación militar son entornos de alta seguridad. Por lo tanto, los errores de tipo 2 deben mantenerse al mínimo. En una institución militar, un recuento alto de errores de tipo 1 no es de suma importancia. La consideración principal debe ser garantizar que el dispositivo biométrico no permita que un intruso no autorizado tenga acceso a sistemas críticos.

El rechazo de usuarios autorizados por un sistema biométrico se denomina error de tipo 1. La concesión de acceso a usuarios no autorizados por un sistema biométrico se denomina error de tipo 2. La precisión de los sistemas biométricos se basa en la Tasa de Rechazo Falso (FRR) que implica errores de tipo 1 y la Tasa de Aceptación Falsa

(FAR) que implica errores de Tipo 2. El CER es el punto en el cual el FRR iguala el FAR. La calificación CER para un sistema biométrico es la medición más crítica para medir la precisión del sistema. Un valor CER de 5 es mejor que un valor CER de 10. Por ejemplo, un sistema biométrico basado en patrones de voz tiene el valor cer más alto.

Un valor alto de error de tipo 1 implica que se rechazan muchos intentos de autenticación válidos y la productividad de los empleados podría verse afectada negativamente, lo que provocaría una menor aceptación del usuario. Un alto valor de error de tipo 2 implica que las personas no autorizadas están siendo autenticadas falsamente por el sistema biométrico y que se permite a los intrusos obtener acceso a los recursos críticos.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Consideraciones biométricas

---

Pregunta #54 de 105

Id. de pregunta: 1105316

En Kerberos 5, ¿qué entidad concede un vale? (Elija dos.)

- ✗ **A)** KDC
- ✓ **B)** como
- ✗ **C)** Tgt
- ✓ **D)** TGS

explicación

En Kerberos, a un cliente se le concede un TGT de un servidor de autenticación (AS), que a veces se conoce como un servidor de concesión de vales (TGS). A continuación, el cliente envía su TGT a un centro de distribución de claves (KDC) y el KDC envía una clave de sesión al cliente. A continuación, el cliente utiliza la clave de sesión para obtener acceso a los recursos de una red Kerberos. Dado que el KDC se basa en una marca de tiempo para determinar la antigüedad de una solicitud, se incluye una marca de tiempo durante los intercambios de claves. Si la marca de tiempo es anterior al período de gracia permitido para las solicitudes, es posible que un pirata informático intercepte la solicitud. Por lo tanto, una red que se basa en Kerberos para la autenticación requiere algún tipo de servicio de sincronización de hora para los hosts de una red.

Después de autenticar a un cliente en una red que utiliza Kerberos 5, se concede al cliente un vale de concesión de vales (TGT). Para asegurarse de que los vales caducan correctamente, sincronización de reloj utilizada en la

autenticación Kerberos. En un intercambio de Kerberos que implica un mensaje con un autenticador, el autenticador contiene el identificador de cliente y la marca de tiempo.

Kerberos es un protocolo de autenticación de red. Está diseñado para proporcionar una autenticación segura mediante criptografía de clave secreta. Kerberos está disponible en muchos productos comerciales. El protocolo Kerberos utiliza criptografía segura para que un cliente pueda demostrar su identidad a un servidor (y viceversa). Después de que un cliente y un servidor hayan utilizado Kerberos para demostrar su identidad, también pueden cifrar todas sus comunicaciones para garantizar la privacidad y la integridad de los datos a medida que avanzan en su negocio. Por todo esto, Kerberos aborda la confidencialidad y la integridad. Kerberos proporciona un servicio de comprobación de integridad para los mensajes entre dos entidades mediante el uso de una suma de comprobación.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Administración de identidad y acceso, Kerberos

---

Pregunta #55 de 105

Id. de pregunta: 1114765

Su empresa tiene varios servidores UNIX en su red. Estos servidores se configuraron antes de su empleo en la empresa y antes de que la empresa estableciera una directiva de seguridad de servidor. Le preocupa la cuenta raíz en estos servidores UNIX. ¿Qué pautas de seguridad debe seguir?

un. Deshabilite la cuenta raíz.

B. Solo permita el inicio de sesión root a través del shell remoto.

c. Permitir únicamente el inicio de sesión raíz a través de la consola local.

d. Limitar el acceso de administrador a la cuenta raíz.

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

✗ **G)** opción A

explicación

Solo debe permitir el inicio de sesión raíz mediante la consola local. Además, debe limitar el acceso de administrador a la cuenta raíz.

No es necesario deshabilitar la cuenta raíz en un servidor UNIX. Es una cuenta de superusuario que permite a los administradores realizar importantes funciones administrativas.

No debe permitir el inicio de sesión raíz utilizando solo el shell remoto. Si necesita acceder a un sistema unix de forma remota utilizando la cuenta raíz, debe utilizar el comando su. Una interfaz de software para el sistema operativo que implementa el control de acceso limitando los comandos del sistema que están disponibles para un usuario se denomina shell restringido.

Si alguna vez la cuenta raíz se ve comprometida, debe restablecer todas las contraseñas de usuario.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Administrar el ciclo de vida de aprovisionamiento de identidad y acceso

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, tipos de contraseñas y gestión

---

Pregunta #56 de 105

Id. de pregunta: 1105333

¿Qué tipo de restricción NO ayuda a limitar o controlar el acceso a un sistema?

✓ **A)** inicio de sesión único
✗ **B)** ubicación
✗ **C)** hora del día
✗ **D)** tipo de transacción

explicación

El inicio de sesión único no es una restricción. El inicio de sesión único permite a un usuario escribir credenciales una vez para tener acceso a todos los recursos de la red. Este principio protege contra la necesidad de que los usuarios recuerden varios nombres de usuario y contraseñas que a veces pueden producirse en entornos cliente/servidor.

Todas las demás opciones son restricciones que ayudan a limitar o controlar el acceso a un sistema.

Puede configurar restricciones de acceso basadas en la ubicación física o lógica. Esto incluye la configuración de determinadas funciones para que sólo se pueden realizar localmente mediante un inicio de sesión interactivo que se produce físicamente en la consola del servidor, no desde un equipo remoto. También puede configurar restricciones de ubicación mediante las cuales las direcciones de red se utilizan para limitar las conexiones remotas a un equipo.

Puede configurar las restricciones de acceso en función de la hora del día. Esto incluye la configuración del servidor para que ciertos usuarios o equipos sólo puedan iniciar sesión durante determinadas horas. Sin embargo, si por alguna razón un usuario debe trabajar fuera de las horas configuradas, se denegaría el acceso.

Puede configurar las restricciones de acceso en función del tipo de transacción. Esto incluye la configuración de permisos para usuarios individuales en función de lo que están intentando hacer. Puede permitir que ciertos usuarios solo lean un archivo determinado, pero permitir que otros usuarios lean y editen un archivo determinado.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

Cissp Cert Guide (3rd Edition), Chapter 5: Identity and Access Management, Content-Dependent Versus Context-Dependent

---

Pregunta #57 de 105

Id. de pregunta: 1105271

¿Qué se emplea cuando un empleado crea las cuentas de usuario y otro empleado configura los permisos de usuario?

- ✗ **A)** un control de dos hombres
- ✗ **B)** una colusión
- ✓ **C)** separación de funciones
- ✗ **D)** rotación de funciones

explicación

La separación de tareas se emplea cuando un empleado crea cuentas de usuario y otro empleado configura los permisos de usuario. Un administrador que es responsable de crear una cuenta de usuario no debe tener la autorización para configurar los permisos asociados a la cuenta. Por lo tanto, los derechos deben separarse.

La colusión es la participación de más de una persona en el fraude. La separación de funciones reduce drásticamente las posibilidades de colusión y ayuda a prevenir el fraude.

Un control de dos hombres implica que dos operadores revisan y aprueban el trabajo del otro. Un control de dos personas actúa como una verificación cruzada y reduce las posibilidades de fraude, minimizando los riesgos asociados con las operaciones que involucran información altamente confidencial. Un operador generalmente realiza montaje en disco o cinta, backup y recuperación, y manejo de hardware. Por lo general, no realizan la entrada de datos.

La rotación de tareas o rotación de puestos de trabajo implica la capacidad de un empleado para llevar a cabo las tareas de otro empleado dentro de la organización. En un entorno que utiliza la rotación de trabajos, un individuo puede realizar las tareas de más de un rol en la organización. Esto mantiene una verificación de las actividades de otros empleados, proporciona un recurso de respaldo y actúa como un elemento disuasorio para posibles fraudes.

La separación de funciones requiere la participación de más de una persona para llevar a cabo una tarea crítica. La separación de funciones garantiza que ninguna persona pueda comprometer un sistema y se considera valiosa para disuadir el fraude. La separación de funciones puede ser estática o dinámica. La separación estática de funciones se refiere a la asignación de individuos a roles y a la asignación de transacciones a roles. En la separación estática de funciones, un individuo puede ser un iniciador de la transacción o el autorizador de la transacción. En la separación dinámica de funciones, un individuo puede tener un doble papel en el que puede iniciar y autorizar transacciones.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso,

Separación de funciones en tecnología de la información, http://www.sans.edu/research/security-laboratory/article/it-separation-duties

---

Pregunta #58 de 105

Id. de pregunta: 1105344

Usted es un contratista de una organización que utiliza el control de acceso obligatorio (MAC). ¿Cuál es la entidad más importante en este entorno?

- ✗ **A)** controles determinados por el propietario
- ✗ **B)** controles basados en funciones
- ✗ **C)** listas de control de acceso (ACL)
- ✓ **D)** etiqueta de seguridad

explicación

Las etiquetas de seguridad son la entidad más importante y son necesarias en un entorno de control de acceso obligatorio (MAC). Se componen de una clasificación y diferentes categorías. La clasificación indica el nivel de sensibilidad del sujeto u objeto, como secreto o alto secreto. Las diferentes categorías aplican las reglas de necesidad de conocer al categorizar los sujetos y objetos en categorías, como recursos humanos y contabilidad. Las categorías deben ser determinadas por la organización en función de las necesidades de control de acceso de la organización.

Los controles basados en roles son entidades en un entorno de control de acceso basado en roles (RBAC). Las listas de control de acceso (ACL) son listas de sujetos que están autorizados a acceder a objetos específicos. Se utilizan en muchas implementaciones de hardware. Los controles determinados por el propietario se utilizan en un entorno de control de acceso discrecional (DACL).

Bajo MAC, se requiere el etiquetado.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Modelos de control de acceso

---

Pregunta #59 de 105

Id. de pregunta: 1105266

¿Cuál es el orden adecuado de las acciones para el control de acceso?

- ✗ **A)** autenticación, autorización, identificación
- ✗ **B)** autenticación, identificación, autorización
- ✗ **C)** identificación, autorización, autenticación
- ✓ **D)** identificación, autenticación, autorización

explicación

El orden adecuado de las acciones para el control de acceso es la identificación, la autenticación y la autorización.

La identificación es el proceso de identificación de un usuario basado en un nombre de usuario, identificación de usuario (ID) o número de cuenta. La autenticación es el proceso de validar al usuario con una segunda información, generalmente una contraseña, una frase de contraseña o un número de identificación personal (PIN). La autorización es el proceso de conceder al usuario acceso a los datos en función de la identidad y los permisos del usuario.

Objetivo:
Administración de identidad y acceso (IAM)

Subobsecución:
Controlar el acceso físico y lógico a los activos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Identity and Access Management, Identification and Authentication Implementation

---

Pregunta #60 de 105

Id. de pregunta: 1113980

La administración ha solicitado que Active Directory se implemente en la red. ¿Cuál es la función de este servicio?

- ✗ **A)** Es el servicio de directorio utilizado en una red Novell.
- ✓ **B)** Es el servicio de directorio utilizado en una red de Windows Server 2003.
- ✗ **C)** Es el servicio de autenticación utilizado en una red de Windows Server 2003.
- ✗ **D)** Es el servicio de autenticación utilizado en una red Novell.

explicación

Active Directory es el servicio de directorio utilizado en una red de Windows Server 2003 o 2008. Un servicio de directorio es una característica del sistema operativo que proporciona un repositorio central para localizar los recursos del sistema, incluidos los usuarios, los equipos y las impresoras.

Active Directory no se utiliza en una red Novell. El novell equivalente a Active Directory es novel directory service (NDS).

El servicio de autenticación (AS), una parte de Active Directory, realiza la autenticación en nombre del servicio de directorio.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Administración de identidad y acceso, Servicios de directorio

Pregunta #61 de 105

Id. de pregunta: 1192951

¿Por qué una organización NO debería implementar un sistema biométrico basado en tecnología de huellas dactilares?

✗ **A)** El valor CER del sistema biométrico es muy bajo.

✓ **B)** Los empleados son reacios a utilizar un sistema biométrico que escanea sus huellas dactilares.

✗ **C)** El sistema exige un inmenso mantenimiento de los gastos generales.

✗ **D)** Los resultados de la autenticación no siempre son precisos y confiables.

explicación

Un sistema biométrico basado en la toma de huellas dactilares tiene un bajo nivel de aceptación por parte del usuario. Al inscribirse para futuros intentos de autenticación, los empleados de una organización a menudo son reacios a proporcionar sus huellas digitales como credenciales. Una razón para esto es la posibilidad de que los funcionarios encargados de hacer cumplir la ley utilicen registros corporativos durante una investigación criminal. Por lo tanto, es posible que la organización no prefiera implementar un sistema biométrico basado en la tecnología de escaneo de huellas dactilares. Los sistemas biométricos más comúnmente implementados se basan en tecnologías de escaneo de iris y retina.

Cuando el valor cer es bajo, un sistema biométrico es una buena opción y debe ser desplegado. La tasa de error cruzado (CER) es el punto en el que la tasa de rechazo falso (FRR) es igual a la tasa de aceptación falsa (FAR). El CER se utiliza para comparar diferentes dispositivos biométricos. Un dispositivo biométrico con un valor cer bajo se considera mejor que uno con un valor cer alto. Un valor cer bajo indica un alto nivel de precisión. Por ejemplo, un valor CER de 5 es mejor que un valor CER de 10 porque indica un número menor de errores.

El mantenimiento de sobrecarga alta es una consideración secundaria al implementar la solución biométrica.

Los sistemas biométricos son los mecanismos de autenticación más caros. Dependiendo de las necesidades de seguridad de la organización, es posible que una organización prefiera implementar un sistema biométrico que cumpla los requisitos de seguridad de mantener la confidencialidad, integridad y disponibilidad de los recursos críticos.

Un sistema biométrico, como un escaneo de huellas dactilares, es un sistema de autenticación complejo y altamente sensible que proporciona un alto nivel de precisión y confiabilidad porque verifica un atributo personal único de un usuario. Los atributos son únicos para diferentes individuos. Un sistema biométrico puede proporcionar un mayor nivel de precisión que otros mecanismos de autenticación, como las contraseñas.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Consideraciones biométricas

---

Pregunta #62 de 105

Id. de pregunta: 1105267

Su gerente sospecha que su red está bajo ataque. Se le ha pedido que proporcione información sobre el flujo de tráfico e información estadística para su red. ¿Qué herramienta debe utilizar?

- ✗ **A)** escáner de puertos
- ✓ **B)** analizador de protocolos
- ✗ **C)** prueba de vulnerabilidad
- ✗ **D)** prueba de penetración

explicación

Un analizador de protocolos proporciona información sobre el flujo de tráfico e información estadística para su red. Un analizador de protocolos también se conoce como analizador de red o rastreador de paquetes.

Ninguna de las otras herramientas puede proporcionar esta información. Un analizador de puertos proporciona una lista de puertos y servicios abiertos en la red. Una prueba de penetración determina si la seguridad de la red está configurada correctamente para rechazar los ataques de piratas informáticos. Una prueba de vulnerabilidad comprueba la red en busca de vulnerabilidades conocidas y proporciona métodos de protección contra las vulnerabilidades.

Objetivo:
Administración de identidad y acceso (IAM)

Subobsecución:
Controlar el acceso físico y lógico a los activos

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Identity and Access Management Sniffing and Eavesdropping

---

Pregunta #63 de 105

Id. de pregunta: 1132525

La red permite a los usuarios remotos conectarse a través de Internet. Recientemente, los hackers han intentado violar su red. La administración ha decidido implementar un método de autenticación que comprueba ambos extremos de una conexión. ¿Qué método de autenticación debe implementar?

- ✓ **A)** autenticación mutua
- ✗ **B)** Autenticación Kerberos
- ✗ **C)** autenticación biométrica
- ✗ **D)** Autenticación RADIUS

explicación

La autenticación mutua comprueba la identidad de ambos extremos de la conexión. A menudo se conoce como autenticación bidireccional.

La autenticación biométrica autentica a un usuario en función de cierta calidad física, como una huella digital, un análisis del iris, un escáner de retina, etc.

La autenticación Kerberos requiere una base de datos de administración centralizada de todas las cuentas de usuario y contraseñas de recursos. No autentica ambos extremos de la conexión. Windows 2000 y versiones posteriores implementan Kerberos como el mecanismo principal para autenticar a los usuarios que solicitan acceso a una red.

RADIUS proporciona autenticación, autorización y contabilidad de usuario remoto centralizadas. No autentica ambos extremos de la conexión.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Autenticación mutua, http://searchfinancialsecurity.techtarget.com/sDefinition/0,sid185_gci1255857,00.html

---

Pregunta #64 de 105

Id. de pregunta: 1105359

Descubre que un equipo de la red ha sido infectado por la aplicación C2MyAzz. ¿Cuál es el efecto de este ataque?

- ✓ **A)** Captura las contraseñas de usuario a medida que se introducen.
- ✗ **B)** Supervisa el tráfico de red en tiempo real.
- ✗ **C)** Permite a otros controlar de forma remota el ordenador infectado.

✗ **D)** Distribuye información de dirección IP incorrecta para un host específico con la intención de desviar el tráfico de su verdadero destino.

explicación

C2MyAzz captura las contraseñas de usuario a medida que se introducen.

Snort es un ejemplo de una aplicación que supervisa el tráfico de red en tiempo real. El envenenamiento por DNS distribuye información de dirección IP incorrecta para un host específico con la intención de desviar el tráfico de su verdadero destino. Back Orifice 2000 (BO2K) permite a otros controlar de forma remota el equipo infectado.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Administrar el ciclo de vida de aprovisionamiento de identidad y acceso

Referencias:

PWS:Win32/C2myazz, https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=PWS%3aWin32%2fC2myazz

---

Pregunta #65 de 105

Id. de pregunta: 1114753

Cuando los usuarios inician sesión en la red localmente, deben proporcionar su nombre de usuario y contraseña. Cuando los usuarios inician sesión en la red de forma remota, deben proporcionar su nombre de usuario, contraseña y tarjeta inteligente.

¿Qué afirmaciones son ciertas con respecto a la seguridad de su organización?

un. El inicio de sesión de red local utiliza la autenticación de un factor.

B. El inicio de sesión de red local utiliza la autenticación en dos fases.

c. El inicio de sesión de red remota utiliza la autenticación de tres factores.

d. El inicio de sesión de red remota utiliza la autenticación de dos factores.

✗ **A)** Opciones B y C

✗ **B)** opción b

✗ **C)** opción A

✗ **D)** opción c

✗ **E)** Opción d

✓ **F)** Opciones A y D

explicación

El inicio de sesión de red local utiliza la autenticación de un factor. Aunque se presentan dos elementos, ambos elementos se consideran algo que usted sabe.

Un ejemplo de un sistema de autenticación de dos factores es una tarjeta atm y un número de identificación personal (PIN).

El inicio de sesión de red remota utiliza la autenticación en dos fases. Aunque se presentan tres elementos, dos elementos son algo que sabes y uno es algo que tienes.

La autenticación de tres factores utiliza algo que sabes (es decir, nombre de usuario o contraseña), algo que tienes (es decir, tarjeta inteligente) y algo que eres (es decir, autenticación biométrica).

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Administración de identidad y acceso, un solo factor frente a la autenticación multifactor

Autenticación de uno, dos y tres factores, https://pciguru.wordpress.com/2010/05/01/one-two-and-three-factor-authentication/

Pregunta #66 de 105

Id. de pregunta: 1192943

¿Qué ataque NO está dirigido solo a máquinas virtuales?

✗ **A)** LDT
✗ **B)** RedPill
✗ **C)** Scooby Doo
✓ **D)** Hombre en el medio

explicación

Un ataque de intermediario no es solo un ataque a máquinas virtuales. Es un ataque que utiliza escuchas para capturar información de autenticación.

Scooby Doo, RedPill y LDT son ataques dirigidos a máquinas virtuales.

Objetivo:
Administración de identidad y acceso (IAM)

Subobsecución:
Controlar el acceso físico y lógico a los activos

Referencias:

Ataques a más emuladores de máquina virtual, HYPERLINK "http://pferrie.tripod.com/papers/attacks2.pdf" \t "sean" http://pferrie.tripod.com/papers/attacks2.pdf

---

Pregunta #67 de 105

Id. de pregunta: 1105310

¿Qué característica de un dispositivo biométrico se debe considerar si una organización desea implementar un procedimiento de autenticación conveniente para los empleados sin comprometer la seguridad en la instalación?

- ✗ **A)** frr alto
- ✓ **B)** FRR bajo
- ✗ **C)** alto LEJOS
- ✗ **D)** bajo FAR

explicación

Una baja tasa de rechazo falso (FRR) de un sistema biométrico es la consideración principal para una organización que busca garantizar un procedimiento de autenticación conveniente para los usuarios. Un valor de FRR bajo implica un alto nivel de aceptación y rendimiento del usuario, pero proporciona baja seguridad. La precisión de los sistemas biométricos depende de la FRR, que se denomina error de tipo 1, y de la tasa de aceptación falsa (FAR), que se denomina error de tipo 2.

Se debe buscar un error far bajo o de tipo 2 cuando la seguridad, no la conveniencia es la principal preocupación. El valor de FAR debe ser bajo si la seguridad de la organización es la principal preocupación. Un valor FAR bajo garantiza que a los usuarios no autorizados no se les conceda acceso a recursos críticos.

Un FAR alto nunca es aceptable porque esto significa que se permite a los usuarios el acceso que no debería ser.

Un FRR alto frustrará a los usuarios porque los usuarios válidos pueden verse impedidos el acceso.

La tasa de error de cruce (CER) es el punto en el cual el FRR iguala el FAR. La clasificación CER para un sistema biométrico es la medición más crítica utilizada para determinar la precisión del sistema. Un valor CER de 5 es mejor que un valor CER de 10.

El rechazo de credenciales de usuario válidas por un sistema biométrico se denomina error de tipo 1. Conceder acceso a un usuario no autorizado se denomina error de tipo 2. Un alto número de errores de tipo 1 afecta negativamente a la productividad y aceptación de los empleados e indica que se rechazan muchos intentos de autenticación válidos. Un gran número de errores de tipo 2 indica que los usuarios no autorizados están siendo autenticados falsamente por el sistema biométrico.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Consideraciones biométricas

---

Pregunta #68 de 105

Id. de pregunta: 1192941

Un usuario informa de que no puede tener acceso a un servidor de archivos. Descubre que hay numerosas conexiones abiertas en el servidor de archivos desde varios servidores y enrutadores. ¿Qué tipo de ataque ha afectado al servidor de archivos?

- ✗ **A)** ataque man-in-the-middle
- ✗ **B)** elevación de privilegios
- ✓ **C)** ataque de denegación de servicio (DoS)
- ✗ **D)** ataque a la puerta trasera

explicación

El servidor de archivos se ha convertido en víctima de un ataque de denegación de servicio (DoS). Debido a que varios enrutadores y servidores están involucrados en el ataque, se ha producido realmente un ataque DoS distribuido (DDoS). Un ataque DDoS generalmente implica el secuestro de varios equipos y enrutadores para usarlos como agentes en el ataque, lo que abruma el ancho de banda de la víctima del ataque. Ejemplos de ataques DoS incluyen ping de muerte, pitufo y TCP SYN.

La elevación de privilegios suele producirse iniciando sesión en un sistema con su cuenta de usuario válida y, a continuación, encontrando una forma de acceder a archivos para los que no tiene permisos de acceso. Esto normalmente implica invocar un programa que puede cambiar los permisos, como Establecer ID de usuario (SUID) o Establecer ID de grupo (SGID), o invocar un programa que se ejecuta en un contexto administrativo. Existen varios métodos para tratar la elevación de privilegios, incluido el uso de cuentas con privilegios mínimos, la separación de

privilegios, etc. La escalada de privilegios también puede provocar ataques DoS. Un ejemplo de elevación de privilegios es obtener acceso a un archivo al que no debe acceder cambiando los permisos de su cuenta válida.

Las puertas traseras son aplicaciones ocultas que los proveedores crean para asegurarse de que pueden acceder a sus dispositivos. Después de instalar nuevos dispositivos o sistemas operativos, debe asegurarse de que todas las puertas traseras y contraseñas predeterminadas estén deshabilitadas o restablecidas. A menudo, los hackers primero intentan usar tales puertas traseras y contraseñas predeterminadas para acceder a nuevos dispositivos.

Un ataque de tipo "Man in the middle" se produce cuando un pirata informático intercepta mensajes de un remitente, los modifica y los envía a un receptor legítimo.

Objetivo:
Administración de identidad y acceso (IAM)

Subobsecución:
Controlar el acceso físico y lógico a los activos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, DoS/DDoS

Seguridad de la red: ataques DoS frente a DDoS, http://www.crime-research.org/articles/network-security-dos-ddos-attacks/

Pregunta #69 de 105

Id. de pregunta: 1105297

El sistema de autenticación de su empresa requiere que un usuario introduzca su ID de usuario y contraseña. La administración le ha solicitado que implemente un sistema biométrico que pueda funcionar junto con la contraseña para proporcionar una mayor seguridad. ¿Qué método biométrico debe implementar?

- ✗ **A)** cifrado de contraseñas
- ✗ **B)** comprobadores de contraseñas
- ✓ **C)** dinámica de pulsaciones de teclas
- ✗ **D)** caducidad de contraseñas

explicación

Debe implementar la dinámica de pulsaciones de teclas. La dinámica de pulsaciones de teclas o teclado puede funcionar junto con una contraseña para proporcionar una mayor seguridad. La dinámica de pulsaciones de teclas registra la velocidad y el movimiento de un usuario al introducir una frase y la compara con los datos almacenados.

Este tipo de autenticación, cuando se usa con una contraseña o frase de contraseña, aumenta la seguridad porque es más difícil duplicar el estilo de escritura de una persona que solo una contraseña o frase de contraseña.

Ninguna de las otras opciones es un método biométrico. La caducidad de contraseñas es un método de seguridad en el que una directiva de contraseñas obliga a un usuario a cambiar su contraseña después de un cierto período de tiempo. Un comprobador de contraseñas es una herramienta que detecta una contraseña débil. Su principal ventaja es que puede proteger su red contra ataques de diccionario o fuerza bruta. El cifrado de contraseña es un mecanismo de protección de contraseña mediante el cual la contraseña se cifra antes de que se transporte a través de la red.

La dinámica de pulsaciones de teclas se considera un dispositivo biométrico de bajo costo y no intrusivo que es transparente para los usuarios. Un término importante de dinámica de pulsaciones de teclas es tiempo de permanencia, que se refiere a la cantidad de tiempo que un usuario mantiene pulsada una tecla. Otro es el tiempo de vuelo, o el tiempo que se tarda en cambiar entre llaves.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, factores característicos

---

Pregunta #70 de 105

Id. de pregunta: 1105340

Una organización desea implementar el modelo de control de acceso que es más fácil de administrador. ¿Qué modelo de control de acceso deben usar?

- ✗ **A)** Mac
- ✓ **B)** RBAC
- ✗ **C)** Acl
- ✗ **D)** Dac

explicación

Deben usar el control de acceso basado en roles (RBAC). RBAC es el modelo de control de acceso más fácil de administrar. Con RBAC, cada usuario se asigna a uno o varios roles. Se conceden permisos de objeto a los roles. Los roles se determinan fácilmente en función de los roles definidos dentro de la organización. Algunos ejemplos de roles son el empleado de entrada de datos, el cajero bancario, el administrador de préstamos, el administrador de red, etc. De esta manera, RBAC se puede asignar a la estructura organizativa de la empresa.

Una lista de control de acceso (ACL) no es un modelo de control de acceso. Es una entidad de control de acceso que proporciona una tabla de sujetos y el nivel de acceso concedido a un objeto determinado.

El control de acceso obligatorio (MAC) generalmente se considera difícil de implementar debido a varios factores. En primer lugar, se requiere un sistema operativo especializado para una implementación adecuada. Además, a cada sujeto y objeto se le debe asignar una etiqueta de seguridad. Estas etiquetas se utilizan para determinar los derechos de acceso.

El control de acceso discrecional (DAC), aunque es más fácil de administrar que MAC, no es tan fácil de administrar como RBAC. Dac requiere que el propietario de los datos determine el nivel de acceso a objetos que se debe conceder a cada sujeto. Los sujetos pueden ser usuarios o grupos de usuarios. DAC es el método de control de acceso más fácil de implementar.

DAC y MAC se pueden reemplazar eficazmente por RBAC.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Modelos de control de acceso

---

Pregunta #71 de 105

Id. de pregunta: 1192947

Usted ha sido contratado como consultor de seguridad por una empresa de fabricación. Durante su mandato, sugiere que la empresa implemente un sistema de inicio de sesión único para evitar que los usuarios tengan que recordar varios ID de usuario y contraseñas al acceder a sistemas remotos. ¿Qué tecnologías podría implementar la organización?

a. CAD

b. MAC

c. RBAC

d. RADIO

E. Kerberos

f. SÉSAMO

g. Active Directory

✗ **A)** opción f

✗ **B)** opción A

✗ **C)** opción g

✗ **D)** opción b

✗ **E)** sólo las opciones a, b y c

✓ **F)** opciones e, f y g solamente

✗ **G)** opción c

✗ **H)** opción e

✗ **I)** Opción d

✗ **J)** opciones d, e, f y g solamente

explicación

La organización podría implementar Kerberos, Sistema europeo seguro para aplicaciones en un entorno de múltiples proveedores (SESAME) y Active Directory. Las tres tecnologías proporcionan autenticación de inicio de sesión único.

El control de acceso discrecional (DAC), el control de acceso obligatorio (MAC) y el control de acceso basado en roles (RBAC) son tres modelos de control de acceso que ayudan a las empresas a diseñar su estructura de control de acceso. Aunque funcionan con tecnologías de autenticación, no proporcionan autenticación de inicio de sesión único por sí mismos.

El Servicio de autenticación remota telefónica de usuario (RADIUS) es un protocolo de autenticación de usuario de acceso telefónico y de red privada virtual (VPN) que se usa para autenticar a los usuarios remotos. Proporciona funciones centralizadas de autenticación y contabilidad. Por sí solo, no proporciona autenticación de inicio de sesión único.

El inicio de sesión único proporciona muchas ventajas. Es un método de inicio de sesión eficiente porque los usuarios solo tienen que recordar una contraseña y solo necesitan iniciar sesión una vez. Se tiene acceso a los recursos más rápido porque no es necesario iniciar sesión para cada acceso a los recursos. Reduce los costos de administración de seguridad porque solo existe una cuenta para cada usuario. Reduce los costos de configuración porque solo es necesario crear una cuenta para cada usuario. El inicio de sesión único permite el uso de contraseñas más seguras.

Otras tecnologías que proporcionan autenticación de inicio de sesión único son los dominios de seguridad, los servicios de directorio y los clientes ligeros.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Administración de identidad y acceso, Inicio de sesión único

---

Pregunta #72 de 105

Id. de pregunta: 1105327

Está examinando una matriz de control de acceso para su organización. ¿Qué entidad corresponde a una fila de esta matriz?

- ✓ **A)** capacidad
- ✗ **B)** lista de control de acceso (ACL)
- ✗ **C)** objeto
- ✗ **D)** Asunto

explicación

Una capacidad corresponde a una fila de la matriz de control de acceso. Una capacidad es una lista de todos los permisos de acceso a los que se ha concedido a un sujeto.

Un objeto es una entidad de la matriz de control de acceso a la que se pueden conceder permisos a los sujetos. Una columna de una matriz de control de acceso corresponde a la lista de control de acceso (ACL) de un objeto.

Una fila de una matriz de control de acceso corresponde a las capacidades de un sujeto, no solo al sujeto.

Al almacenar una lista de derechos sobre cada tema, se logra la concesión de capacidades.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

Cissp Cert Guide (3rd Edition), Chapter 5: Identity and Access Management, Capabilities Table

---

Pregunta #73 de 105

Id. de pregunta: 1192952

¿Qué factor es el menos importante a tener en cuenta al implementar un sistema biométrico en una organización?

- ✓ **A)** alta productividad del sistema biométrico

✗ **B)** bajo tiempo de inscripción del sistema biométrico

✗ **C)** alta precisión del sistema biométrico

✗ **D)** alto rendimiento del sistema biométrico

explicación

La alta productividad no es un factor importante a tener en cuenta durante el despliegue de un sistema biométrico. La característica más importante a tener en cuenta durante la implementación de un sistema biométrico en una organización es el nivel de precisión que puede proporcionar.

Los otros factores que influyen en la selección de un sistema biométrico son los siguientes:

- Rendimiento: el rendimiento o el tiempo de procesamiento implica el tiempo que tarda un sistema biométrico en procesar una solicitud de autenticación iniciada por un usuario. Un alto rendimiento es un factor considerado durante la implementación de un sistema biométrico.
- Tiempo de inscripción bajo: durante la fase de inscripción, un usuario debe proporcionar credenciales, como una huella digital, varias veces para crear un registro de referencia único que se usará para futuros intentos de autenticación. El tiempo de inscripción para un sistema biométrico debe mantenerse en un mínimo. Un tiempo de inscripción bajo conduce a una mayor aceptación del usuario.
- Aceptación del usuario: Un sistema biométrico debe tener un alto nivel de aceptación del usuario. Los usuarios deben ser informados de que los recursos de la organización deben estar protegidos y que el sistema no es intrusivo.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Consideraciones biométricas

---

Pregunta #74 de 105

Id. de pregunta: 1192946

Recientemente, los usuarios de su organización han comenzado a quejarse del número de identificadores de usuario y contraseñas que deben recordar para tener acceso a diferentes recursos de la red. La administración le ha pedido que implemente un sistema en el que se conceda a los usuarios acceso a todos los recursos después de la autenticación de dominio inicial. ¿Qué tecnología debe implementar?

✓ **A)** inicio de sesión único

- ✗ **B)** Dac
- ✗ **C)** tarjetas inteligentes
- ✗ **D)** dispositivo biométrico
- ✗ **E)** Mac

explicación

Debe implementar el inicio de sesión único, el inicio de sesión único permite a los usuarios acceder libremente a todos los sistemas a los que se ha concedido acceso a su cuenta después de la autenticación inicial. Esto se considera tanto una ventaja como una desventaja. Es una ventaja porque el usuario solo tiene que iniciar sesión una vez y no tiene que volver a autenticarse constantemente al acceder a otros sistemas. Es una desventaja porque el acceso máximo autorizado es posible si una cuenta de usuario y su contraseña se ven comprometidas.

El control de acceso discrecional (DAC) y el control de acceso obligatorio (MAC) son modelos de control de acceso que ayudan a las empresas a diseñar su estructura de control de acceso. No proporcionan ningún mecanismo de autenticación por sí mismos.

Las tarjetas inteligentes son dispositivos de autenticación que pueden proporcionar una mayor seguridad al requerir la inserción de una tarjeta inteligente válida para iniciar sesión en el sistema. No determinan el nivel de acceso permitido a un sistema. Los sistemas de tarjetas inteligentes se consideran más confiables que los sistemas de devolución de llamada. Los sistemas de devolución de llamada no suelen ser prácticos porque requieren que los usuarios llamen desde un número de teléfono estático cada vez que acceden a la red. La mayoría de los usuarios acceden a la red de forma remota porque están en la carretera y se mueven de un lugar a otro. Una tarjeta de cajero automático bancario es un ejemplo de tarjeta inteligente.

Un dispositivo biométrico puede proporcionar una mayor seguridad al requerir la verificación de un activo personal, como una huella digital, para la autenticación. No determinan el nivel de acceso permitido a un sistema.

El inicio de sesión único se creó para eliminar la necesidad de mantener varias cuentas de usuario y contraseñas para acceder a varios sistemas. Con el inicio de sesión único, un usuario obtiene una cuenta y una contraseña que inicia sesión en el sistema y concede al usuario acceso a todos los sistemas a los que se ha concedido la cuenta del usuario. En una red de inicio de sesión único, el servidor de autenticación se considera un único punto de error. Si el servidor de autenticación deja de estar en el estado, no se puede completar la autenticación.

Al iniciar sesión en una estación de trabajo, el proceso de inicio de sesión debe validar al usuario sólo después de que se han proporcionado todos los datos de entrada. Este enfoque es necesario para garantizar que se ha presentado toda la información requerida y que no se ha proporcionado ninguna información que ayudaría a un cracker a intentar obtener acceso no autorizado a la estación de trabajo o a la red. Si se produce un error en un intento de inicio de sesión, no se debe proporcionar al usuario información sobre qué parte de la información de inicio de sesión solicitada era incorrecta. Por ejemplo, no debe tener un mensaje de error que indique que el problema es un nombre de usuario no válido o una contraseña no válida.

Objetivo:

Administración de identidad y acceso (IAM)

Subobjetivo:

Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Administración de identidad y acceso, Inicio de sesión único

---

Pregunta #75 de 105

Id. de pregunta: 1105280

¿Qué método utiliza un usuario o proceso para afirmar quiénes son o para afirmar quiénes dicen ser?

- ✗ **A)** autenticación
- ✗ **B)** autorización
- ✗ **C)** confidencialidad
- ✓ **D)** identificación

explicación

La identificación es el método utilizado por un usuario o proceso para reclamar quiénes son o para afirmar quiénes dicen ser. La identificación implica proporcionar su nombre de usuario, número de cuenta o alguna otra forma de identificación personal. Es el medio por el cual un usuario proporciona una notificación de su identidad a un sistema.

La autenticación es el proceso de ser reconocido por un sistema. La autenticación implica proporcionar una segunda información, como una contraseña, que se comprueba con una base de datos para comprobar su precisión. Si esta información coincide con la información almacenada, se autentica el asunto. Es la prueba o conciliación de la evidencia de la identidad de un usuario.

La autorización es el proceso de determinar si el usuario puede acceder a un objeto determinado dentro de un sistema. La autorización implica comprobar las credenciales de usuario para ver si el sujeto tiene los permisos necesarios para llevar a cabo una determinada acción. Son los derechos y permisos concedidos a un individuo para tener acceso a un recurso informático.

La confidencialidad garantiza que los datos no se divulguen a sujetos no autorizados. Es uno de los principios de la tríada de seguridad.

La rendición de cuentas es la capacidad de un sistema para determinar las acciones y el comportamiento de un solo individuo dentro de un sistema.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Conceptos de identificación y autenticación de identity and access management

---

Pregunta #76 de 105

Id. de pregunta: 1105349

¿Qué es una mejora de seguridad para Linux que se implementa utilizando un módulo de kernel cargable?

- ✗ **A)** control de acceso discrecional (DAC)
- ✗ **B)** control de acceso obligatorio (MAC)
- ✓ **C)** control de acceso obligatorio con marca de agua baja (LOMAC)
- ✗ **D)** control de acceso basado en roles (RBAC)

explicación

El control de acceso obligatorio de marca de agua baja (LOMAC) es una mejora de seguridad para Linux que se implementa utilizando un módulo de kernel cargable.

El control de acceso basado en roles (RBAC) es un modelo de control de acceso que configura el acceso de los usuarios en función del rol del usuario en la empresa. No es una implementación específica de Linux solamente.

El control de acceso discrecional (DAC) es un modelo de control de acceso que configura el acceso de usuario en función de la identidad y la asignación del usuario o de los grupos a los que pertenece el usuario. Este modelo deja la configuración a discreción de los propietarios de los recursos. No es una implementación específica de Linux solamente.

El control de acceso obligatorio (MAC) es un modelo de control de acceso que configura el acceso del usuario en función de la autorización de seguridad del usuario y la clasificación de seguridad del objeto. No es una implementación específica de Linux solamente.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Modelos de control de acceso

FreshMeat.net, Detalles del proyecto para LOMAC, http://freshmeat.net/projects/lomac

---

Pregunta #77 de 105

Id. de pregunta: 1113991

¿Cuál de los siguientes NO forma parte del ciclo de vida del aprovisionamiento de acceso?

✗ **A)** creación

✗ **B)** mantenimiento

✗ **C)** deleción

✓ **D)** autenticación

explicación

La autenticación no forma parte del ciclo de vida del aprovisionamiento de acceso. La autenticación es el proceso de verificación de la identidad de un sujeto que solicita acceso a un sistema o red.

La gestión de identidades es vital. Se debe seguir el ciclo de vida del aprovisionamiento de acceso para garantizar una administración de identidades adecuada. Entre los pasos del ciclo de vida se incluyen los siguientes:

- Creación: también denominada aprovisionamiento
- Mantenimiento- también conocido como revisión
- Eliminación: también denominada desaprovisionamiento, terminación o revocación

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Administrar el ciclo de vida de aprovisionamiento de identidad y acceso

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Administración de identidad y acceso, ciclo de vida de aprovisionamiento

---

Pregunta #78 de 105

Id. de pregunta: 1113990

Necesita mejorar la responsabilidad del usuario para la red de su empresa. ¿Qué características proporcionarán esto? (Elija todo lo que se aplique).)

- ✓ **A)** registros de auditoría
- ✓ **B)** listas de control de acceso (ACL)
- ✗ **C)** encriptación
- ✗ **D)** Contraseñas

explicación

Los registros de auditoría y las ACL mejoran la responsabilidad del usuario para la red de su empresa.

Las contraseñas mejoran la autenticación de usuario para la red de su empresa. El cifrado mejora la confidencialidad de los datos para la red de su empresa.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Administrar el ciclo de vida de aprovisionamiento de identidad y acceso

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Responsabilidad

La importancia de los registros de auditoría, http://www.datamation.com/columns/article.php/3578916/The-Importance-of-Audit-Logs.htm

---

Pregunta #79 de 105

Id. de pregunta: 1113986

¿Qué sistema de control de seguridad asigna roles a los usuarios para dictar el acceso a los recursos?

- ✗ **A)** Mac
- ✗ **B)** UDP
- ✓ **C)** RBAC
- ✗ **D)** Dac

explicación

En el control de acceso basado en roles (RBAC), a los usuarios se les asignan roles para realizar tareas específicas. Por ejemplo, un usuario podría estar asignado a un rol denominado estándar para el trabajo típico en un equipo y el mismo usuario podría asignarse a un rol denominado admin para el trabajo que requiere privilegios administrativos. En

un sistema RBAC, a los roles se les concede o deniega el acceso a los recursos de red. Los roles se utilizan para identificar a los usuarios que tienen permisos para un recurso.

En el control de acceso obligatorio (MAC), los usuarios y los recursos se asignan a los niveles de seguridad. En un sistema de seguridad basado en MAC, los usuarios pueden escribir documentos en o por encima de su nivel de seguridad asignado, y pueden leer documentos en o por debajo de su nivel de seguridad asignado. El ejército estadounidense utiliza MAC para acceder a documentos y recursos de red.

En el control de acceso discrecional (DAC), los usuarios se asignan a grupos y a los usuarios y grupos se les concede o deniega el acceso a carpetas y archivos. Cada carpeta y archivo de un sistema de seguridad DAC tiene una lista de control de acceso (ACL) que se usa para determinar qué usuarios y grupos pueden obtener acceso a un recurso de red. Protocolo de datagramas de usuario (UDP) es un protocolo que se utiliza en una red TCP/IP para admitir comunicaciones sin conexión; no es un sistema de control de seguridad.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Modelos de control de acceso

---

Pregunta #80 de 105

Id. de pregunta: 1105341

Un usuario en un entorno de oficina pequeña le explica que su oficina implementa un pequeño grupo de trabajo de Microsoft. Los usuarios suelen compartir carpetas entre sí. ¿Qué modelo de control de acceso se representa en este ejemplo?

✗ **A)** Acl
✗ **B)** Mac
✗ **C)** RBAC
✓ **D)** Dac

explicación

El modelo de control de acceso que se usa en un pequeño grupo de trabajo de Microsoft donde los usuarios suelen compartir carpetas entre sí es el control de acceso discrecional (DAC). El modelo DAC permite al propietario del recurso determinar el nivel de acceso a los recursos que se concede a un usuario y hace que el propietario de los datos sea responsable de conceder a otros usuarios acceso a los recursos de propiedad.

Dac es considerado por muchas empresas como una implementación de control de acceso que necesita saber. Los usuarios como propietarios de datos pueden determinar quién necesita acceso y cuándo se debe conceder ese acceso. Con un modelo DAC, el acceso a objetos se puede limitar a determinados días y determinadas horas del día. En DAC, los derechos de un sujeto deben ser suspendidos cuando está de licencia o vacaciones y deben ser despedidos cuando deja la empresa.

El modelo de control de acceso obligatorio (MAC) proporciona a los propietarios de datos cierto control sobre el acceso a los recursos, pero la determinación final del acceso a los recursos recae en el sistema operativo. En el entorno MAC, los sujetos y los objetos reciben etiquetas. Estas etiquetas ayudan a determinar el nivel de acceso que se concederá a los sujetos. Los propietarios de los datos tienen muy poco control sobre los derechos de acceso de otros usuarios.

El modelo de control de acceso basado en roles (RBAC) determina el acceso a objetos en función del rol de un sujeto en la empresa. En el entorno RBAC, un administrador administra la relación entre los sujetos y los objetos. El titular de los datos no tiene control sobre los derechos de acceso de otros usuarios.

Un modelo de control de acceso dicta cómo los sujetos acceden a los objetos.

Una lista de control de acceso (ACL) es una lista de sujetos y los permisos que esos sujetos tienen en un objeto determinado. Una ACL se puede usar en un entorno DAC.

Se utiliza una técnica de control de acceso para admitir un modelo de control de acceso. La técnica de control de acceso basada en reglas utiliza reglas para definir acciones aceptables e inaceptables entre sujetos y objetos. La técnica de control de acceso dependiente del contenido basa el acceso al objeto en el contenido del objeto. Si un departamento puede ver el historial de trabajo de los empleados y otro grupo no puede ver su historial de trabajo, se trata de un acceso dependiente del contenido. El acceso dependiente del contenido permite un control granular. La técnica de acceso dependiente del contexto basa el acceso al objeto en el contexto del objeto en lugar de en la sensibilidad de los datos. El control de acceso que depende de factores como la ubicación, la hora del día y el historial de acceso anterior es un control de acceso dependiente del contexto. Tenga en cuenta que el acceso dependiente del contexto puede aumentar el procesamiento y la sobrecarga de recursos.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Modelos de control de acceso

---

Pregunta #81 de 105

Id. de pregunta: 1105285

¿Qué tipo de autenticación garantiza la identidad de un usuario?

✗ **A)** una contraseña

✓ **B)** una exploración retiniana

✗ **C)** una tarjeta inteligente

✗ **D)** un token de seguridad

explicación

Una exploración retiniana ve el patrón de los vasos sanguíneos en la retina de un usuario para autenticar al usuario en una red. Un escáner de retina es una autenticación biométrica que puede garantizar la identidad de un usuario. Los métodos de autenticación biométrica escanean atributos físicos únicos para identificar al usuario.

Un token de seguridad es un pequeño dispositivo que genera contraseñas sensibles al tiempo. Una tarjeta inteligente es una pequeña tarjeta de plástico que contiene información de autenticación. Las contraseñas son otro método para autenticar a los usuarios. Las contraseñas permiten el acceso a los recursos. No se puede usar un token de seguridad, una tarjeta inteligente o una contraseña para garantizar la identidad del usuario que usa el método de autenticación.

Un sistema de autenticación que utiliza métodos de seguridad física, métodos de seguridad biométricos y métodos de seguridad basados en el conocimiento se conoce como sistema de autenticación multifactor.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, factores característicos

---

Pregunta #82 de 105

Id. de pregunta: 1105338

El departamento de investigación de su empresa ha decidido implementar un nuevo servidor de archivos. El jefe de departamento será responsable de conceder acceso a las carpetas y archivos en función de la identidad de un usuario o de un grupo. ¿Qué tipo de modelo de control de acceso se está utilizando?

✗ **A)** Acl

✓ **B)** Dac

✗ **C)** RBAC

✗ **D)** Mac

explicación

El control de acceso discrecional (DAC) se basa en la identidad. Esta identidad puede ser la identidad de un usuario o la identidad de un grupo, y a veces se conoce como control de acceso basado en identidad. DAC es el tipo de control de acceso que se usa en situaciones dinámicas locales donde los sujetos tienen la capacidad de especificar a qué recursos pueden tener acceso determinados usuarios.

Una lista de control de acceso (ACL) no es un modelo de control de acceso, aunque se usa en un modelo DAC. Es una entidad de control de acceso que enumera los niveles de acceso de usuario a un objeto determinado.

El control de acceso obligatorio (MAC) es un modelo basado en etiquetas de seguridad. El control de acceso basado en roles (RBAC) es un modelo basado en roles de usuario.

Se debe aplicar un modelo de control de acceso de manera preventiva. La directiva de seguridad de una empresa determina qué modelo de control de acceso se usará.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Modelos de control de acceso

---

Pregunta #83 de 105

Id. de pregunta: 1192945

Su red ha sido víctima de un ataque de control de acceso que implicó el uso de tablas de arco iris. ¿Qué contienen estas tablas?

✓ **A)** Todas las contraseñas posibles en formato hash

✗ **B)** todas las contraseñas aceptadas

✗ **C)** Todas las contraseñas aceptadas en formato hash

✗ **D)** todas las contraseñas posibles

explicación

Las tablas de arco iris contienen todas las contraseñas posibles en un formato hash. Los ataques de control de acceso contra contraseñas incluyen ataques de fuerza bruta, tablas de arco iris, ataques de diccionario, ataques de respuesta

y ataques de ingeniería social.

Ninguna de las otras opciones define adecuadamente el contenido de las tablas arco iris.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

CISSP Cert Guide (3rd Edition), Chapter 5, Identity and Access Management. Ataque de tabla arco iris

---

Pregunta #84 de 105

Id. de pregunta: 1113976

¿A qué tipo de ataque son particularmente susceptibles las redes inalámbricas?

- ✗ **A)** desbordamiento de búfer
- ✗ **B)** ataque asíncrono
- ✓ **C)** emanaciones capturando
- ✗ **D)** ganchos de mantenimiento

explicación

Las redes inalámbricas son particularmente susceptibles a la captura de emanaciones. La captura de emanaciones implica el uso de herramientas especiales para espiar las frecuencias de las ondas para capturar el tráfico.

Las redes inalámbricas no son particularmente susceptibles a los otros tipos de ataques enumerados.

Los ganchos de mantenimiento son puertas traseras en aplicaciones diseñadas por los desarrolladores de aplicaciones para realizar tareas de mantenimiento. Permite que el código se ejecute sin las comprobaciones de seguridad habituales.

Un desbordamiento de búfer se produce cuando se transmiten demasiados datos a una aplicación o sistema operativo.

Un ataque asincrónico, o un ataque de tiempo de comprobación/tiempo de uso (TDC/CDU), ocurre cuando un atacante interrumpe una tarea y cambia algo para dirigir el resultado.

Objetivo:
Administración de identidad y acceso (IAM)

Subobsecución:

Controlar el acceso físico y lógico a los activos

Referencias:

Cissp Cert Guide (3rd Edition), Chapter 5, Identity and Access Management, Emanating

---

Pregunta #85 de 105

Id. de pregunta: 1192953

Su empresa ha decidido permitir que los usuarios marquen a la red desde ubicaciones remotas. Dado que la seguridad es una preocupación importante para su empresa, debe implementar un sistema que proporcione autenticación, autorización y contabilidad de usuarios remotos centralizados. ¿Qué tecnología debe implementar?

- ✓ **A)** radio
- ✗ **B)** Dmz
- ✗ **C)** Inicio de sesión único
- ✗ **D)** VPN

explicación

Debe implementar el Servicio de autenticación remota telefónica de usuario (RADIUS). RADIUS proporciona autenticación, autorización y contabilidad de usuario remoto centralizadas. Tecnologías similares incluyen el sistema de control de acceso del controlador de acceso de terminal (TACACS), TACACS extendido, TACACS+ y Diameter.

Una red privada virtual (VPN) es una tecnología que permite a los usuarios acceder a los recursos de la red privada a través de una red pública, como Internet. Las técnicas de tunelización se utilizan para proteger los recursos internos.

Una zona desmilitarizada (DMZ) es una subred aislada en una red corporativa que contiene recursos a los que suelen tener acceso los usuarios públicos, como los usuarios de Internet. El DM se crea para aislar esos recursos para asegurarse de que otros recursos que deben permanecer privados no se ven comprometidos. Un DMZ se implementa generalmente con el uso de firewalls.

El inicio de sesión único es una característica mediante la cual un usuario inicia sesión una vez para acceder a todos los recursos de red.

RADIUS es definido por el RFC 2138 y 2139. Un servidor RADIUS actúa como el servidor de autenticación o un cliente proxy que reenvía las solicitudes de cliente a otros servidores de autenticación. El servidor de acceso a la red inicial, que suele ser un servidor VPN o un servidor de acceso telefónico, actúa como un cliente RADIUS reenviando la solicitud del cliente VPN o de acceso telefónico al servidor RADIUS. RADIUS es el protocolo que transporta la información entre la VPN o el cliente de acceso telefónico, el cliente RADIUS y el servidor RADIUS.

Las características centralizadas de la autenticación, de la autorización, y de las estadísticas del RADIUS permiten la administración central de todos los aspectos del login remoto. Las características de contabilidad permiten a los administradores realizar un seguimiento del uso y las estadísticas de red mediante el mantenimiento de una base de datos central.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Guía del CERT CISSP (3ra edición),capítulo 5: Administración de la identidad y del acceso, RADIUS y TACACS+

Pregunta #86 de 105

Id. de pregunta: 1105318

En Kerberos 5, ¿qué tipo de entidad se concede a un cliente después de autenticar un cliente?

- ✓ **A)** Tgt
- ✗ **B)** como
- ✗ **C)** TGS
- ✗ **D)** KDC

explicación

Después de autenticar a un cliente en una red que utiliza Kerberos 5, se concede al cliente un vale de concesión de vales (TGT). Para asegurarse de que los vales caducan correctamente, sincronización de reloj utilizada en la autenticación Kerberos. En un intercambio de Kerberos que implica un mensaje con un autenticador, el autenticador contiene el identificador de cliente y la marca de tiempo.

En Kerberos, a un cliente se le concede un TGT de un servidor de autenticación (AS), que a veces se conoce como un servidor de concesión de vales (TGS). A continuación, el cliente envía su TGT a un centro de distribución de claves (KDC) y el KDC envía una clave de sesión al cliente. A continuación, el cliente utiliza la clave de sesión para obtener acceso a los recursos de una red Kerberos. Dado que el KDC se basa en una marca de tiempo para determinar la antigüedad de una solicitud, se incluye una marca de tiempo durante los intercambios de claves. Si la marca de tiempo es anterior al período de gracia permitido para las solicitudes, es posible que un pirata informático intercepte la solicitud. Por lo tanto, una red que se basa en Kerberos para la autenticación requiere algún tipo de servicio de sincronización de hora para los hosts de una red.

Kerberos es un protocolo de autenticación de red. Está diseñado para proporcionar una autenticación segura mediante criptografía de clave secreta. Kerberos está disponible en muchos productos comerciales. El protocolo Kerberos utiliza criptografía segura para que un cliente pueda demostrar su identidad a un servidor (y viceversa). Después de que un cliente y un servidor hayan utilizado Kerberos para demostrar su identidad, también pueden cifrar todas sus comunicaciones para garantizar la privacidad y la integridad de los datos a medida que avanzan en su negocio. Por todo esto, Kerberos aborda la confidencialidad y la integridad. Kerberos proporciona un servicio de comprobación de integridad para los mensajes entre dos entidades mediante el uso de una suma de comprobación.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Chapter 5: Identity and Access Management, , Kerberos

---

Pregunta #87 de 105

Id. de pregunta: 1105272

Su organización usa el protocolo Kerberos para autenticar a los usuarios de la red. ¿Qué instrucción es verdadera del Centro de distribución de claves (KDC) cuando se utiliza este protocolo?

- ✗ **A)** El KDC se utiliza para capturar claves secretas a través de la red.
- ✗ **B)** El KDC se utiliza para mantener y distribuir claves públicas para cada sesión.
- ✗ **C)** El KDC sólo se utiliza para almacenar claves secretas.
- ✓ **D)** El KDC se utiliza para almacenar, distribuir y mantener claves de sesión criptográficas.

explicación

Durante el uso del protocolo Kerberos, el Centro de distribución de claves (KDC) almacena, distribuye y mantiene las claves de sesión criptográficas y las claves secretas. La clave maestra se utiliza para intercambiar las claves de sesión. Las claves se distribuyen automáticamente al cliente que se comunica y al servidor. El KDC también proporciona los servicios de autenticación para los usuarios. Kerberos consta de un KDC, un reino de entidades de seguridad (usuarios, servicios, aplicaciones y dispositivos), un servicio de autenticación, vales y un servicio de concesión de vales.

El cliente solicita acceso a los recursos a través del KDC. Como respuesta a la solicitud, el KDC genera una clave de sesión que es una combinación de las claves secretas del cliente y el servidor. El cliente y el servidor descifran la clave

de sesión para autenticarse correctamente entre sí e iniciar la comunicación.

El KDC hace algo más que simplemente almacenar las claves secretas.

El KDC no se puede utilizar para capturar claves secretas a través de la red. La captura de datos se realiza mediante el software packet sniffer.

El KDC es responsable de almacenar las claves secretas de los usuarios y de generar claves de sesión. Por lo tanto, KDC no trata con claves públicas para una sesión de usuario.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3ª edición),capítulo 5, administración de identidad y acceso, Kerberos

---

Pregunta #88 de 105

Id. de pregunta: 1114759

Ha implementado un sistema informático que está protegido por MAC. ¿Qué actividad(es) se consideran ilegales en este sistema?

a. Lectura hacia abajo

b. lectura

c. Amortización

d. redacción

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

explicación

Las actividades de lectura y anotación se consideran ilegales en un sistema informático protegido por el control de acceso obligatorio (MAC). MAC es un tipo de control de acceso no confidencial que utiliza niveles de seguridad y categorías para restringir el acceso a la información. MAC asume que los usuarios son descuidados y que no se puede confiar en los programas para llevar a cabo las necesidades de los usuarios. En una computadora MAC, los niveles de seguridad, como confidencial, secreto y alto secreto, son similares a los utilizados por el ejército de los EE. UU.

La lectura es la capacidad de los usuarios de una categoría de seguridad inferior para leer información que se encuentra en una categoría superior. La amortización es la capacidad de alguien en una categoría de seguridad superior para escribir archivos que los usuarios de categorías de seguridad inferiores pueden ver. Las actividades de lectura y escritura están permitidas en una computadora o red MAC.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Modelos de control de acceso

---

Pregunta #89 de 105

Id. de pregunta: 1114752

Se le ha pedido que implemente un sistema biométrico para proteger el centro de datos de su empresa. A la administración le preocupa que los errores en el sistema impidan que los usuarios acepten el sistema. La administración estipula que usted debe desplegar el sistema con la tasa de error cruzado más baja (CER). ¿Qué términos se utilizan en biometría para determinar este valor?

a. ACL

b. EAR

c. ERRAR

d. FAR

e. FRR

✗ **A)** Opción d
✓ **B)** Sólo opciones D y E
✗ **C)** opción e

- ✗ **D)** opción b
- ✗ **E)** opción c
- ✗ **F)** Sólo opciones B y C
- ✗ **G)** opción A

explicación

Dos términos que se utilizan en biometría para determinar la tasa de error cruzado (CER) son la tasa de aceptación falsa (FAR) y la tasa de rechazo falso (FRR). Un CER más bajo indica que el sistema biométrico es más preciso. Varios tipos biométricos se pueden comparar en términos de sus fortalezas y debilidades relativas con un gráfico de Zephyr.

Una lista de control de acceso (ACL) es una lista de asuntos y el permiso concedido a un objeto específico.

EAR y ERR son términos no válidos.

FAR, también conocido como un error de tipo 2, se produce cuando un sujeto no válido se concede acceso al sistema.

FRR, también conocido como un error de tipo 1, se produce cuando se deniega el acceso a un sujeto válido al sistema.

Otro término que afecta a los sistemas biométricos es la tasa de rendimiento, o la velocidad a la que los usuarios son escaneados y autenticados. Una tasa de rendimiento más alta es más aceptable que una menor. Sin embargo, si la tasa de rendimiento afecta a la CER del sistema, debe reducirse para mejorar la CER.

El tiempo de inscripción es el tiempo que se tarda en registrarse en el sistema proporcionando muestras de una característica biométrica. Durante la inscripción, el enfoque principal para obtener la información biométrica de una muestra recopilada de las características fisiológicas o de comportamiento de un individuo es la extracción de características.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Consideraciones biométricas

---

Pregunta #90 de 105

Id. de pregunta: 1105343

¿Qué instrucción describe mejor una lista de control de acceso (ACL)?

✗ **A)** Una lista de todos los niveles de acceso que se pueden conceder a un objeto determinado

✓ **B)** una lista de sujetos a los que se ha concedido acceso a un objeto específico, incluido el nivel de acceso concedido

✗ **C)** Una lista de todos los objetos a los que se ha concedido acceso a un sujeto

✗ **D)** Una lista de todos los sujetos a los que se ha concedido acceso a un objeto determinado

explicación

Una lista de control de acceso (ACL) es una lista de sujetos a los que se ha concedido acceso a un objeto específico, incluido el nivel de acceso concedido. Una ACL debe incluir los sujetos, los objetos y el nivel de acceso.

El control de acceso le permite controlar el comportamiento, el uso y el contenido de cualquier sistema, por ejemplo, un sistema IS. Lo utiliza principalmente el administrador del sistema para controlar el uso del sistema habilitando o restringiendo explícitamente el acceso. El propósito principal de los controles de acceso es mitigar los riesgos y reducir el potencial de pérdida. Una ACL coordina el acceso a los recursos del sistema (objetos) en función de algún identificador de usuario o entidad de equipo (asunto). Este identificador puede ser un nombre de usuario, un identificador personal o incluso una dirección IP. Una ACL normalmente permite o deniega explícitamente ciertos derechos o permisos. Normalmente, los tipos de acceso son leer, escribir, ejecutar, anexar, modificar, eliminar y crear. Los controles de acceso pueden ser controles físicos reales que controlan el acceso a objetos físicos, como edificios o salas, o controles reales del sistema que controlan el acceso a objetos dentro de un sistema determinado una vez que se ha concedido acceso físico, como el uso de nombres de usuario y contraseñas para iniciar sesión.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Modelos de control de acceso

---

Pregunta #91 de 105

Id. de pregunta: 1114755

¿Cuáles son las principales diferencias entre los sistemas biométricos de huellas dactilares y escaneo de dedos?

un. Los sistemas de huellas digitales requieren más tiempo para procesar una solicitud de autenticación de usuario.

B. Los sistemas de escaneo de dedos requieren un mayor tiempo de procesamiento para autenticar una solicitud de usuario.

c. Los sistemas de huellas dactilares inscriben toda la huella digital, pero los sistemas de escaneo de dedos extraen características específicas.

d. Los sistemas de huellas dactilares inscriben rasgos específicos de la huella digital, pero los sistemas de escaneo de dedos inscriben toda la huella digital.

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

explicación

Los sistemas de huellas digitales inscriben la huella digital completa de un usuario para futuros intentos de autenticación. Los sistemas de escaneo de dedos solo extraen características específicas de la huella digital y permiten un procesamiento más rápido de una solicitud de autenticación de usuario.

Todas las demás opciones son incorrectas.

Los sistemas de huellas digitales coinciden con características únicas, denominadas coincidencia de minucias, para autenticar o denegar una solicitud de acceso. Un sistema biométrico de huellas dactilares basado en la coincidencia de minucias compara la ubicación y la dirección de las terminaciones de la cresta y las bifurcaciones de una huella digital. Durante la inscripción y la verificación, la información relevante se recopila de los puntos de minucias. Los sistemas de huellas dactilares basados en la coincidencia de patrones globales representan un enfoque más macroscópico y evalúan el flujo de crestas en términos de arcos, bucles y verticilos.

La tecnología de escaneo de dedos difiere de los sistemas de huellas dactilares porque el primero extrae solo las características específicas de la huella digital. Esto requiere menos espacio en el disco duro y recursos del sistema, al tiempo que permite búsquedas y comparaciones de bases de datos más rápidas que los sistemas de huellas digitales.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 5: Gestión de identidad y acceso, Características fisiológicas

Pregunta #92 de 105

Id. de pregunta: 1105278

Durante una auditoría de seguridad reciente, descubre que algunos usuarios han sido redirigidos a un sitio Web falso mientras navega por Internet. ¿Qué tipo de ataque se ha producido?

- ✓ **A)** suplantación de hipervínculos
- ✗ **B)** Suplantación de paquetes ICMP
- ✗ **C)** ataque a tierra
- ✗ **D)** secuestro de direcciones de red

explicación

Se ha producido la suplantación de hipervínculos, también conocida como suplantación de identidad web. La suplantación de hipervínculos es utilizada por un atacante para persuadir al navegador de Internet de que se conecte a un servidor falso que aparece como una sesión válida. El propósito principal de la suplantación de hipervínculos es obtener acceso a información confidencial, como números PIN, números de tarjetas de crédito y datos bancarios de los usuarios.

La suplantación de hipervínculos aprovecha las ventajas de que las personas usen hipervínculos en lugar de direcciones DNS. En la mayoría de los escenarios, las direcciones DNS no son visibles y el usuario es redirigido a otro sitio Web falso después de hacer clic en un hipervínculo.

Un ataque terrestre implica el envío de un paquete TCP SYN falsificado con la dirección IP del host de destino y un puerto abierto que actúa como origen y destino al host de destino en un puerto abierto. El ataque a tierra hace que el sistema se congele o se bloquee porque la máquina responde continuamente a sí misma.

La suplantación de paquetes ICMP es utilizada por un ataque pitufo para llevar a cabo un ataque de denegación de servicio (DoS). Un pitufo es un ataque DoS que utiliza mensajes ping de difusión falsificados para inundar un host de destino. En un ataque de este tipo, el atacante envía una gran cantidad de paquetes de eco ICMP con una dirección IP de origen falsificada similar a la del host de destino a direcciones de difusión IP. Esto da lugar al host de destino que es inundado con las respuestas de eco de la red entera. Esto también hace que el sistema se congele o se bloquee.

El secuestro de direcciones de red permite al atacante redirigir el tráfico de datos de un dispositivo de red a un equipo personal. El secuestro de direcciones de red, que también se conoce como secuestro de sesión, permite a un atacante capturar y analizar los datos dirigidos a un sistema de destino. El atacante puede obtener acceso a recursos críticos y credenciales de usuario, como contraseñas, y acceso no autorizado a los sistemas críticos de una organización. El secuestro de sesión implica tomar el control de una conexión existente después de que el usuario haya creado correctamente una sesión autenticada.

Objetivo:

Administración de identidad y acceso (IAM)

Subobjetivo:

Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Spoofing

---

Pregunta #93 de 105

Id. de pregunta: 1114749

¿Qué método implica eludir un bloqueo por intrusión?

a. Rastrillar

b. shimming

c. spamming

d. Inundación SYN

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

explicación

Rastrillar es una técnica utilizada por los intrusos para eludir un bloqueo. Por ejemplo, un pico se utiliza para eludir un bloqueo de vaso de alfiler. Shimming es una técnica en la que un usuario autorizado desmonta una cerradura sin el uso de una llave de funcionamiento. Por lo tanto, la selección de bloqueos es un ejemplo de shimming.

El spam consiste en enviar un gran número de correos electrónicos comerciales no solicitados a clientes desprevenidos. El correo no deseado inunda el buzón de correo de un usuario y sobrecarga una red, lo que afecta negativamente al rendimiento de la red.

Una inundación SYN es un ejemplo de ataque basado en red. En un ataque de inundación SYN, el atacante envía repetidamente paquetes de sincronización (SYN) desde una dirección IP falsificada al equipo host de la víctima. El equipo host de la víctima responde con paquetes de confirmación de sincronización (SYN-ACK) válidos y sigue esperando el paquete de confirmación (ACK) para establecer un proceso de protocolo de enlace tcp de tres vías para la transferencia de datos. En ausencia de los paquetes ACK desde el equipo malintencionado, el equipo host de la

víctima continúa respondiendo a cada intento de conexión desde el equipo hostil. Esto da como resultado la denegación de servicio a hosts legítimos debido al agotamiento de recursos.

Objetivo:
Administración de identidad y acceso (IAM)

Subobsecución:
Controlar el acceso físico y lógico a los activos

Referencias:

El método del rastrillo: Una breve guía, https://www.bumpmylock.com/pages/the-rake-method-a-brief-guide.html

---

Pregunta #94 de 105

Id. de pregunta: 1105295

Una organización requiere que una instalación de investigación esté protegida por la forma más alta de sistema de control de acceso. La organización decide implementar la biometría. Se le ha consultado sobre qué sistema biométrico implementar. La administración desea minimizar los problemas de intrusión de privacidad para los usuarios. ¿Qué método biométrico debería sugerir en función de la preocupación de la dirección?

- ✗ **A)** Huellas
- ✗ **B)** exploración del iris
- ✓ **C)** impresión de voz
- ✗ **D)** exploración retiniana

explicación

Debe sugerir un sistema biométrico de impresión de voz basado en la preocupación de la gerencia. Una impresión de voz se considera menos intrusiva que las otras opciones dadas.

Tanto una exploración del iris como una exploración retiniana se consideran más intrusivas debido a la naturaleza en la que se completa la exploración. La mayoría de las personas son reacias a que un escáner lea cualquier geometría de ojos.

Una huella digital es más intrusiva que una impresión de voz. La mayoría de las personas son reacias a dar su huella dactilar porque las huellas dactilares se pueden utilizar para la aplicación de la ley.

Una impresión de voz es muy fácil de obtener. Su propósito principal es distinguir la forma de hablar y los patrones de voz de una persona. Los sistemas de impresión de voz son fáciles de implementar en comparación con otros métodos biométricos. Las impresiones de voz suelen ser fiables y flexibles.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, factores característicos

---

Pregunta #95 de 105

Id. de pregunta: 1105331

Está examinando una matriz de control de acceso para su organización. ¿Qué entidad corresponde a una columna de esta matriz?

- ✗ **A)** capacidad
- ✓ **B)** objeto
- ✗ **C)** Asunto
- ✗ **D)** lista de control de acceso (ACL)

explicación

Un objeto es una entidad de la matriz de control de acceso a la que se pueden conceder permisos a los sujetos. Una columna de una matriz de control de acceso corresponde a la lista de control de acceso (ACL) de un objeto.

Una capacidad corresponde a una fila de la matriz de control de acceso. Una capacidad es una lista de todos los permisos de acceso a los que se ha concedido a un sujeto.

Una fila de una matriz de control de acceso corresponde a las capacidades de un sujeto, no solo al sujeto.

Al almacenar una lista de derechos sobre cada tema, se logra la concesión de capacidades.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Modelos de control de acceso

---

Pregunta #96 de 105

Id. de pregunta: 1114750

¿Qué tipos de contraseña suelen ser los más difíciles de recordar?

a. Contraseña estática

b. Contraseña dinámica

c. contraseña cognitiva

d. Contraseña generada por el usuario

e. Contraseña generada por software

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

explicación

Las contraseñas dinámicas y las contraseñas generadas por software son la misma cosa. También se denominan contraseñas de un solo uso porque solo se utilizan durante una sesión de inicio de sesión. En la siguiente sesión de inicio de sesión, se genera una nueva contraseña. Suelen ser las contraseñas más difíciles de recordar porque son muy complejas. Debido a su complejidad, también son más difíciles de adivinar.

Una contraseña estática, también denominada contraseña generada por el usuario, es aquella creada por el usuario. Por lo general, es muy fácil de recordar para el usuario. En la mayoría de las empresas, la directiva de contraseñas garantiza que las contraseñas estáticas caduquen después de un cierto período de tiempo.

Una contraseña cognitiva es una contraseña que se basa en algún hecho u opinión personal. Uno de los usos más populares es por motivos de seguridad para obtener información confidencial. Las contraseñas cognitivas son cosas como el apellido de soltera de tu madre, tu color favorito o la escuela de la que te graduaste.

Las contraseñas de una sola vez, o dinámicas, se consideran más seguras que las contraseñas estáticas y las frases de contraseña. Por lo general, son generados por una pieza de software. Si el generador de contraseñas se ve comprometido, todo el sistema está en peligro. Hay diferentes tipos de generadores de contraseñas.

Un dispositivo de token, a veces denominado dispositivo de transacción, suele ser un dispositivo de mano que presenta a un usuario una lista de caracteres que se escribirán como contraseña para el equipo. Sólo el dispositivo y

el servidor de autenticación conocen la contraseña. Cuando se utiliza un protocolo de desafío/respuesta con implementaciones de dispositivo de token, el servicio de autenticación genera un desafío y el token inteligente genera una respuesta basada en el desafío. En la autenticación de desafío-respuesta, el usuario escribe un valor aleatorio enviado por el servidor de autenticación en un dispositivo de token. El dispositivo token comparte el conocimiento de una clave secreta criptográfica con el servidor de autenticación y calcula una respuesta basada en el valor de desafío y la clave secreta.

Un dispositivo de token sincrónico se sincroniza con el servidor de autenticación en función de la hora o un contador. El dispositivo de valor de tiempo debe tener la misma hora que el servidor de autenticación. El valor de hora y una clave secreta se utilizan para crear la contraseña de un solo uso, que se muestra para el usuario. El dispositivo de valor de contador utiliza un valor de autenticación. Se aplica un algoritmo hash al valor y a un secreto y se muestra la contraseña de un solo uso para el usuario.

Un dispositivo de token asincrónico autentica al usuario mediante un mecanismo de desafío/respuesta. El servidor de autenticación genera valores aleatorios. El usuario introduce este valor aleatorio, lo cifra y lo transmite. A continuación, se genera una contraseña de un solo uso.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

20 Herramientas de escritorio para generar y administrar contraseñas, https://www.hongkiat.com/blog/password-tools/

Pregunta #97 de 105

Id. de pregunta: 1105332

Está diseñando el control de acceso para la red de su organización. Debe asegurarse de que el acceso a los recursos de red está restringido. ¿Qué criterios se pueden utilizar para ello?

- ✗ **A)** grupos
- ✗ **B)** tipo de transacción
- ✓ **C)** todas las opciones
- ✗ **D)** Papeles
- ✗ **E)** ubicación
- ✗ **F)** hora del día

explicación

Los roles, los grupos, la ubicación, la hora del día y el tipo de transacción se pueden usar para restringir el acceso a los recursos. Independientemente de los criterios utilizados, la administración de acceso se puede simplificar agrupando objetos y sujetos.

Los roles se basan en el trabajo de un sujeto dentro de la empresa. A los roles solo se les conceden los derechos y privilegios necesarios para completar las asignaciones de trabajo.

Los grupos se crean para incorporar usuarios que necesitan los mismos permisos de acceso en una entidad común. Cuando estos usuarios necesitan acceso a un recurso, el permiso se concede a todo el grupo. El uso de grupos simplifica la administración del control de acceso.

Las ubicaciones se pueden usar para restringir el acceso de los usuarios a los recursos limitando la ubicación desde la que un sujeto puede iniciar sesión. Un dominio de Microsoft Windows puede restringir el acceso de los usuarios al dominio limitando el equipo desde el que un usuario puede iniciar sesión en el dominio. Esto se hace escribiendo el nombre de equipo desde el que el usuario puede tener acceso al dominio a las propiedades de la cuenta del usuario.

La hora del día se puede usar para restringir el acceso de los usuarios a los recursos limitando los días y las horas en que un usuario está autorizado a trabajar. Una cuenta de usuario de Microsoft Windows se puede editar para permitir sólo ciertos tiempos de inicio de sesión.

El tipo de transacción es un método de restricción de acceso de uso común en las bases de datos. A los sujetos se les otorgan permisos de acceso en función de los tipos de transacción. Por ejemplo, un usuario puede tener permiso para ver la compensación de los empleados, pero no se le permite editarla.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

CISSP Cert Guide (3rd Edition), Chapter 5: Identity and Access Management, , Content-Dependent Versus Context-Dependent

---

Pregunta #98 de 105

Id. de pregunta: 1111756

La directiva de seguridad de dominio de su empresa establece que las revisiones de cuentas de usuario deben realizarse dos veces al año. Se le ha pedido que realice revisiones de cuentas de usuario. ¿Qué debes hacer?

✗ **A)** Asegúrese de que los usuarios están accediendo al sistema en el momento adecuado.

✓ **B)** Asegúrese de que las cuentas de usuario corresponden a empleados válidos.

✗ **C)** Informar a los usuarios de que se están llevando a cabo revisiones de cuentas de usuario.

✗ **D)** Asegúrese de que los usuarios acceden al sistema en las fechas adecuadas.

explicación

Al realizar revisiones de cuentas de usuario, debe asegurarse de que los usuarios tienen el nivel adecuado de acceso y que las cuentas de usuario corresponden a empleados válidos. Comprobar el nivel adecuado de acceso garantiza que a las cuentas de usuario no se les han concedido más permisos de los necesarios. La comprobación de que las cuentas de usuario corresponden a empleados válidos garantiza que no existan cuentas no válidas.

No debe asegurarse de que los usuarios acceden al sistema en las fechas o horas adecuadas. No es necesario verificar esta información normalmente. Sin embargo, si sospecha que una cuenta de usuario se ha visto comprometida, puede comprobar si la cuenta de usuario se utiliza durante las horas en las que el usuario no está en el trabajo.

No debe informar a los usuarios de que se están llevando a cabo revisiones de cuentas de usuario.

Las organizaciones deben tener un proceso para solicitar, establecer, emitir y cerrar cuentas de usuario, realizar un seguimiento de los usuarios y sus respectivas autorizaciones de acceso, y administrar estas funciones. Como parte de la administración de cuentas de usuario, una organización debe asegurarse de que se implementan las siguientes directivas:

- Los usuarios deben ser rotados fuera de sus deberes actuales.
- Las cuentas de los usuarios deben revisarse periódicamente.
- Se debe implementar un proceso para realizar un seguimiento de las autorizaciones de acceso.
- El personal que se ha ocupado de puestos delicados debe ser reerenado periódicamente.

Las revisiones de cuentas de usuario pueden examinar la conformidad con el concepto de privilegio mínimo. Las revisiones de cuentas de usuario se pueden realizar en todo el sistema o aplicación por aplicación.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Administrar el ciclo de vida de aprovisionamiento de identidad y acceso

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, gestión de identidad y cuentas

Pregunta #99 de 105

Id. de pregunta: 1114761

Usted es el administrador de seguridad de una organización que utiliza el control de acceso obligatorio (MAC). Bajo este tipo de control de acceso, ¿qué entidad(es) existirían como objetos?

a. un archivo

b. un usuario

c. un grupo

d. una impresora

e. un ordenador

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

explicación

En MAC, un archivo, impresora o equipo existiría como un objeto. Los objetos son recursos a los que se tiene acceso.

Un usuario o grupo existiría como sujeto. Los sujetos son entidades que tienen acceso a objetos.

En un entorno MAC, un privilegio que no está expresamente permitido está prohibido. Una autorización es un privilegio. Si un sujeto necesita acceso a un objeto, el administrador es la única persona que puede determinar si se permite el acceso en función de la directiva de seguridad.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetiva:
Implementar y administrar mecanismos de autorización

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, Modelos de control de acceso

Pregunta #100 de 105

Id. de pregunta: 1105275

¿Qué afirmación NO es cierta de la certificación cruzada?

✗ **A)** La certificación cruzada se utiliza principalmente para establecer la confianza entre diferentes PKIs.

✗ **B)** La certificación cruzada crea una jerarquía de PKI general.

✓ **C)** La certificación cruzada comprueba la autenticidad de los certificados en la ruta de certificación.

✗ **D)** La certificación cruzada permite a los usuarios validar el certificado de los demás cuando están certificados bajo diferentes jerarquías de certificación.

explicación

La certificación cruzada no comprueba la autenticidad de los certificados en la ruta de certificación. Esta función se realiza mediante la validación de la ruta de certificación.

La certificación cruzada se utiliza principalmente para establecer la confianza entre diferentes PKI y crear una jerarquía pki general. La certificación cruzada permite a los usuarios validar el certificado de los demás cuando están certificados bajo diferentes jerarquías de certificación.

El propósito principal de la certificación cruzada es crear una relación de confianza entre diferentes jerarquías de certificación cuando los usuarios que pertenecen a jerarquías diferentes deben comunicarse y pueden requerir autenticación para las conexiones legítimas. El proceso implica el establecimiento de una relación de confianza entre dos entidades de certificación (CA) a través de la firma de la clave pública de otra CA en un certificado denominado certificado cruzado.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Administración de identidad y acceso, Administración de identidades federadas

Redes de directivas de certificación cruzada y PKI, http://www.entrust.com/resources/pdf/cross_certification.pdf

---

Pregunta #101 de 105

Id. de pregunta: 1105317

Su organización ha implementado recientemente Kerberos en la red de Windows Server 2003. A la administración le preocupa que las entidades implicadas en Kerberos estén protegidas. ¿Cuál es el componente más importante en este entorno?

- ✗ **A)** claves de sesión
- ✗ **B)** servicio de autenticación (AS)
- ✗ **C)** ticket de concesión de vales (TGT)
- ✗ **D)** Directores
- ✓ **E)** Centro de distribución de claves (KDC)

explicación

El Centro de distribución de claves (KDC) es el componente más importante en un entorno Kerberos. Es responsable de administrar todas las claves secretas, autenticar a todos los usuarios y emitir vales a los usuarios válidos.

Ninguno de los otros componentes enumerados son tan importantes como el KDC.

Las entidades principales son las entidades a las que el KDC presta servicios. Pueden ser usuarios, aplicaciones o servicios.

Las claves de sesión son claves simétricas que se utilizan para cifrar y descifrar la información que se pasa entre las entidades de seguridad y el KDC. Mediante la criptografía de clave simétrica, Kerberos autentica a los clientes en otras entidades de una red y facilita las comunicaciones mediante la asignación de claves de sesión.

Un vale de concesión de vales (TGT) es la entidad emitida por el servicio de autenticación (AS) en el KDC a una entidad de seguridad. El TGT demuestra la identidad principal a lo largo del proceso de comunicación.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Chapter 5: Identity and Access Management, , Kerberos

---

Pregunta #102 de 105

Id. de pregunta: 1111747

Está implementando un dispositivo biométrico para acceder a un área restringida de su edificio. La ubicación donde se ubicará el dispositivo biométrico tiene muchas ventanas y mucha luz solar natural. Le preocupa que la cantidad de sol

que brilla en el lector biométrico pueda afectar la precisión del sistema. ¿Qué tipo de dispositivo biométrico puede verse afectado por esto?

- ✓ **A)** exploración del iris
- ✗ **B)** exploración de la retina
- ✗ **C)** Huellas
- ✗ **D)** exploración facial

explicación

Una exploración del iris puede verse afectada por el sol que brilla en el lector biométrico. La colocación del dispositivo biométrico utilizado para realizar la exploración del iris es muy importante. Debe colocar el lector correctamente en la instalación para asegurarse de que el sol no brille en la abertura.

Una exploración del iris examina los patrones únicos, colores, anillos y coronas del ojo de un individuo. Cada característica es capturada por una cámara y comparada con los registros de referencia del empleado que se recopilaron durante la fase de inscripción.

Los resultados de la exploración del iris se utilizan ampliamente en los sistemas de identificación de personal en las organizaciones. El iris es un órgano protegido, lo que hace que los patrones oculares capturados a través de la exploración del iris sean estables a lo largo de la vida.

Las exploraciones del iris superan las siguientes desventajas de las exploraciones de retina:

- menos costoso
- menos tiempo de inscripción para los empleados
- menos complejo que la exploración de la retina
- menos tiempo de autenticación de usuario

Ninguno de los otros dispositivos biométricos enumerados se vería afectado por el sol brillando en el lector. Una exploración de la retina examina la retina de un usuario para obtener el patrón de los vasos sanguíneos. Una exploración facial examina la cara de una persona para medir diferentes atributos, como la estructura ósea, la cresta de la nariz, el ancho de los ojos, etc. Un dispositivo de huellas dactilares examina las crestas y otras características de una huella digital.

Un escaneo de dedos difiere de un escáner de huellas dactilares. Un escaneo de dedos extrae características sobre el dedo en sí. Un escaneo de huellas dactilares extrae características sobre la huella digital solamente.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, factores característicos

---

Pregunta #103 de 105

Id. de pregunta: 1113977

¿Qué es TEMPEST?

- ✗ **A)** un sistema electrónico de control de acceso
- ✗ **B)** un dispositivo de cifrado
- ✓ **C)** un programa del gobierno de los Estados Unidos que reduce las emanaciones de equipos electrónicos
- ✗ **D)** un sistema de inteligencia artificial que resuelve problemas

explicación

TEMPEST es un programa del gobierno de los Estados Unidos que reduce las emanaciones de equipos electrónicos para reducir los ataques de escuchas.

El chip Clipper es un dispositivo de cifrado desarrollado por el gobierno de los Estados Unidos.

Ninguna de las otras opciones es correcta. Un sistema electrónico de control de acceso utiliza tarjetas inteligentes o biometría para verificar la identidad de un usuario antes de que se le conceda acceso a un edificio o habitación. Los sistemas expertos utilizan la inteligencia artificial para resolver problemas.

Objetivo:
Administración de identidad y acceso (IAM)

Subobsecución:
Controlar el acceso físico y lógico a los activos

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, emanando

---

Pregunta #104 de 105

Id. de pregunta: 1105289

Su empresa tiene varios servidores UNIX en su red. Un compañero de trabajo de TI le ha notificado que ha notado que todos estos servidores UNIX tienen un archivo /etc/shadow. ¿Cuál es la mejor descripción de la finalidad de este archivo?

✓ **A)** Para almacenar contraseñas de usuario en un formato protegido

✗ **B)** Para almacenar la contraseña de root

✗ **C)** Para almacenar contraseñas de usuario

✗ **D)** Para almacenar la configuración de directiva de seguridad de contraseñas

explicación

El propósito del archivo /etc/shadow en un sistema UNIX es almacenar contraseñas de usuario en un formato protegido. Sólo el usuario root puede acceder a este archivo. Los datos de instantáneas impiden que los usuarios vean el contenido del archivo de contraseñas.

Ninguna de las otras opciones es el propósito de este archivo.

Objetivo:
Administración de identidad y acceso (IAM)

Subobjetivo:
Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5: Gestión de identidad y acceso, tipos de contraseñas y gestión

TLDP.org, contraseña de Linux y formatos de archivo de sombra, http://www.tldp.org/LDP/lame/LAME/linux-admin-made-easy/shadow-file-formats.html

---

Pregunta #105 de 105

Id. de pregunta: 1105291

Se le ha pedido que implemente una nueva directiva de administración de contraseñas que incluya el uso de contraseñas cognitivas para comprobar la identidad de un usuario. ¿Cuál es la explicación más correcta de este tipo de contraseña?

✓ **A)** una contraseña que se basa en algún hecho u opinión personal

✗ **B)** una contraseña que se compone de una frase larga

✗ **C)** una contraseña que se compone de dos palabras totalmente no relacionadas

✗ **D)** Una contraseña creada por un generador de contraseñas

explicación

Una contraseña cognitiva se basa en algún hecho u opinión personal. Las contraseñas cognitivas son cosas como el apellido de soltera de tu madre, tu color favorito o la escuela de la que te graduaste.

Una contraseña que se compone de una frase larga es una frase de contraseña. Estas contraseñas suelen ser más difíciles de descifrar usando un ataque de fuerza bruta debido a su longitud y complejidad.

Una contraseña creada por un generador de contraseñas es una contraseña generada por software. También se conoce como contraseña de un solo uso o dinámica. Este tipo de contraseña es muy difícil de recordar.

Una contraseña que se compone de dos palabras no relacionadas es una contraseña de composición.

Una contraseña es algo que sabes o memorizaste.

Objetivo:

Administración de identidad y acceso (IAM)

Subobjetivo:

Administrar la identificación y autenticación de personas, dispositivos y servicios

Referencias:

Cissp Cert Guide (3ª Edición), Capítulo 5: Gestión de identidad y acceso, contraseñas cognitivas