PREV
Capítulo 4 Comunicación y seguridad de la red

PRÓXIMO
Capítulo 6 Evaluación y pruebas de seguridad

CAPÍTULO 5

Gestión de identidad y acceso

Este dominio incluye preguntas de los siguientes temas:

- Métodos y tecnologías de identificación
- Métodos, modelos y tecnologías de autenticación
- Modelos discrecionales, obligatorios y no discretionarios
- Prácticas de rendición de cuentas, monitoreo y auditoría
- Registro y prueba de identidad
- Identidad como servicio
- Amenazas de acceder a prácticas y tecnologías de control

Controlar el acceso a los recursos es un elemento vital de cualquier programa de seguridad de la información. Controlar quién puede acceder a qué y cuándo ayuda a proteger los activos de información y los recursos de la empresa de la modificación y divulgación no autorizadas. Por lo tanto, los controles de acceso abordan los tres servicios de la tríada AIC (disponibilidad, integridad y confidencialidad), ya sea de carácter técnico, físico o administrativo. Los profesionales de la seguridad deben comprender los principios que subyace detrás de los controles de acceso para garantizar su adecuación y correcta implementación.

PREGUNTAS Q

1 . ¿Cuál de las siguientes opciones NO describe correctamente un servicio de directorio?

R. Administra objetos dentro de un directorio mediante espacios de nombres.

B. Aplica la directiva de seguridad mediante la realización de funciones de control de acceso y gestión de identidades.

C. Asigna espacios de nombres a cada objeto en bases de datos que se basan en el estándar X.509 y a los que tiene acceso LDAP.

D. Permite a un administrador configurar y administrar cómo se lleva a cabo la identificación dentro de la red.

2 . A Hannah se le ha asignado la tarea de instalar software de administración de acceso web (WAM). ¿Cuál es la mejor descripción para qué se utiliza wam comúnmente?

R. Controlar las entidades externas que solicitan acceso a través de bases de datos X.500

B. Controlar las entidades externas que solicitan acceso a objetos internos

C. Controlar las entidades internas que solicitan acceso a través de bases de datos X.500

D. Controlar las entidades internas que solicitan acceso a objetos externos

3 . Hay varios tipos de enfoques de administración de contraseñas utilizados por los sistemas de administración de identidades. ¿Cuál de los siguientes reduce el volumen de llamadas de help-desk, pero también es criticado por la facilidad con la que un hacker podría obtener acceso a múltiples recursos si una contraseña se ve comprometida?

R. Restablecimiento de contraseña de administración

B. Restablecimiento de contraseña de autoservicio

C. Sincronización de contraseñas

D. Restablecimiento asistido de contraseña

4 . En los Estados Unidos, las agencias federales deben adherirse a la "Verificación de Identidad Personal" de la Norma Federal de Procesamiento de Información (FIPS, por susape) 201-2, que discute las medidas técnicas de autenticación para empleados y contratistas federales. Esta norma debe seguirse para garantizar cuál de las siguientes condiciones?

R. Que los empleados del gobierno están debidamente autorizados para el trabajo asignado

B. Que a los empleados públicos sólo se les permite el acceso a los datos de su nivel de autorización

C. Que la identidad del empleado del gobierno ha sido debidamente verificada

D. Que los datos a los que los empleados gubernamentales tienen acceso han sido clasificados adecuadamente

5 . ¿Cuál de las siguientes opciones NO describe el control de acceso basado en roles compatible con la privacidad?

R. Es un ejemplo de un modelo discrecional de control de acceso.

B. Los controles de acceso detallados indican el tipo de datos a los que los usuarios pueden acceder en función del nivel de sensibilidad a la privacidad de los datos.

C. Es una extensión del control de acceso basado en roles.

D. Debe utilizarse para integrar políticas de privacidad y políticas de control de acceso.

6 . Security Assertion Markup Language (SAML) es un estándar basado en XML para intercambiar datos de autenticación y autorización entre sistemas en diferentes dominios de seguridad. SAML permite el uso compartido de información de autenticación, como cómo se llevó a cabo la autenticación, los atributos de entidad y a qué está autorizada la entidad para acceder. SAML se utiliza con mayor frecuencia en entornos basados en web que requieren capacidad de inicio de sesión único (SSO). ¿Cuál de los siguientes tiene una definición correcta asociada al componente SAML correspondiente?

R. Se utilizan dos aserciones SAML (autenticación, autorización) que indican que una autoridad SAML validó un asunto específico.

B. Las aserciones SAML se utilizan con mayor frecuencia para permitir la federación de identidades y la autorización distribuida.

C. La especificación de enlace SAML describe cómo incrustar mensajes SAML dentro de los protocolos TCP y UDP.

D. Los perfiles SAML definen cómo se deben implementar los mensajes SAML, las aserciones y los protocolos en SSL y TLS.

7 . A Brian se le ha pedido que trabaje en el directorio virtual del nuevo sistema de gestión de identidades de su empresa. ¿Cuál de los siguientes describe mejor un directorio virtual?

R. Meta-directorio

B. Información de atributos de usuario almacenada en una base de datos de recursos humanos

C. Contenedor virtual para datos de múltiples fuentes

D. Un servicio que permite a un administrador configurar y administrar cómo se lleva a cabo la identificación

8 . ¿Cuál de las siguientes describe con precisión la identidad como servicio (IDaaS)?

R. Una forma de inicio de sesión único (SSO) que abarca varias entidades de una empresa

B. Una forma de SSO que abarca varias empresas independientes

C. Una forma de proporcionar SSO sin múltiples formas de autenticación

D. Una forma de demostrar identidad sin tener que firmar

9 . ¿Cuál de los siguientes describe correctamente una identidad federada y su rol dentro de los procesos de administración de identidades?

R. Una identidad noportable que se puede usar a través de los límites empresariales

B. Una identidad portátil que se puede utilizar a través de los límites empresariales

C. Una identidad que se puede usar en directorios virtuales de intranet y almacenes de identidades

D. Una identidad especificada por nombres de dominio que se pueden usar a través de los límites empresariales

10. Las contramedidas de seguridad deben ser transparentes para los usuarios y atacantes. ¿Cuál de los siguientes NO describe la transparencia?

R. Las actividades del usuario son monitoreadas y rastreadas sin afectar negativamente al rendimiento del sistema.

B. Las actividades del usuario son monitoreadas y rastreadas sin que el usuario conozca el mecanismo que está llevando a cabo.

C. Se permite a los usuarios acceder de una manera que no afecte negativamente a los procesos empresariales.

D. Los intentos de acceso no autorizados se deniegan y se registran sin que el intruso sepa sobre el mecanismo que está llevando a cabo esto.

11. ¿Qué lenguaje de marcado permite el uso compartido de directivas de seguridad de aplicaciones para garantizar que todas las aplicaciones sigan las mismas reglas de seguridad?

R. XML

B. SPML

C. XACML

D. GML

12. La importancia de proteger los registros de auditoría generados por ordenadores y dispositivos de red se destaca por el hecho de que es requerido por muchas de las regulaciones actuales. ¿Cuál de los siguientes NO explica por qué se deben proteger los registros de auditoría?

R. Si no están debidamente protegidos, es posible que estos registros no sean admisibles durante un proceso judicial.

B. Los registros de auditoría contienen datos confidenciales y solo deben ser accesibles para un determinado subconjunto de personas.

C. Los intrusos pueden intentar fregar los registros para ocultar sus actividades.

D. El formato de los registros debe ser desconocido y no estar disponible para el intruso.

13. De lo siguiente, ¿en qué se basa el elemento principal en el que se basa una tabla de capacidades?

R. Un tema

B. Un objeto

C. Un producto

D. Una aplicación

14. ¿Qué lenguaje de marcado permite a una empresa enviar solicitudes de servicio y a la empresa receptora proporcionar acceso a estos servicios?

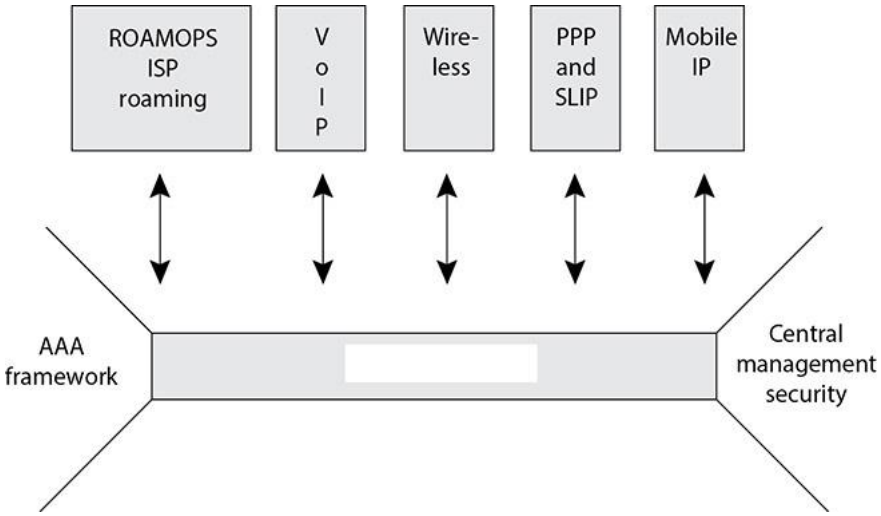
R. XML

B. SPML

C. SGML

D. HTML

15. Existen varios tipos diferentes de protocolos de control de acceso centralizados. ¿Cuál de los siguientes se ilustra en el gráfico que sigue?



R. diámetro

B. perro guardián

C. radio

D. TACACS+

16. Se utiliza una matriz de control de acceso en muchos sistemas operativos y aplicaciones para controlar el acceso entre sujetos y objetos. ¿Cuál es la columna de este tipo de matriz a la que se hace referencia?

Access Control Matrix

Subject	File1	File2	File3	File4
Larry	Read	Read, Write	Read	Read, Write
Curly	Full Control	No Access	Full Control	Read
Mo	Read, Write	Full Control	Read	Full Control
Bob	Full Control	Full Control	No Access	No Access

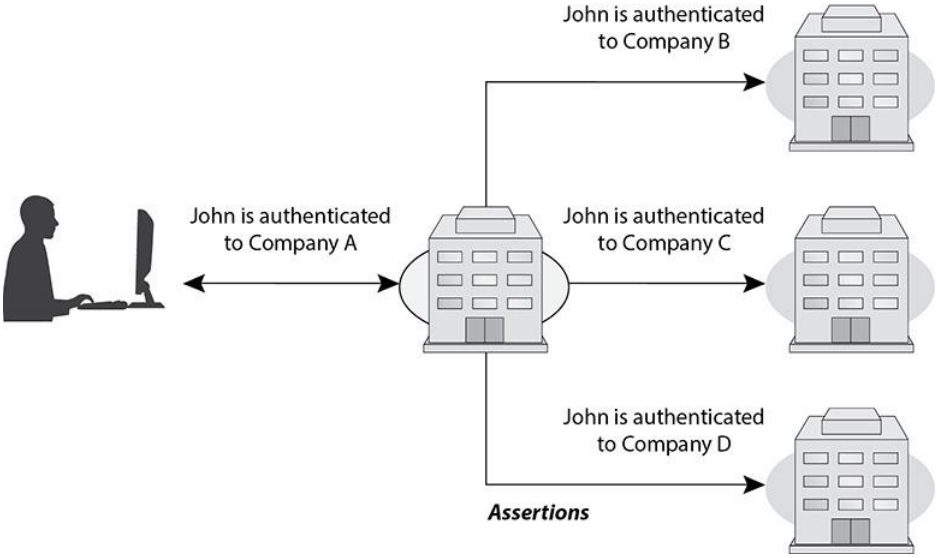
R. Tabla de capacidades

B. Interfaz restringida

C. Valor basado en roles

D. Acl

17. ¿Qué tecnología dentro de la gestión de la identidad se ilustra en el gráfico que sigue?



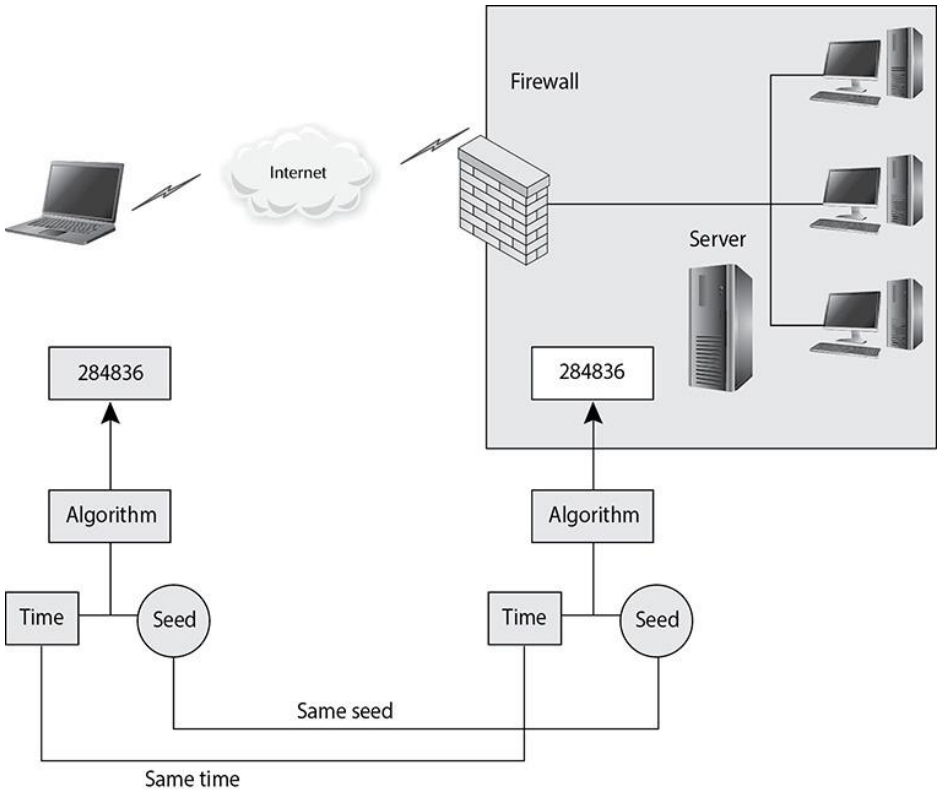
R. Aprovisionamiento de usuarios

B. Identidad federada

C. Directorios

D. Gestión del acceso web

18. Hay diferentes maneras en que tecnologías específicas pueden crear contraseñas únicas con fines de autenticación. ¿Qué tipo de tecnología se ilustra en el gráfico que sigue?



R. Token sincrónico de contador

B. Token asincrónico

C. Token obligatorio

D. Token sincrónico

19. ¿Cuál de las siguientes características describe mejor cómo SAML, SOAP y HTTP suelen trabajar juntos en un entorno que proporciona servicios web?

R. Los atributos de seguridad se colocan en formato SAML. La solicitud de servicio web y los datos de autenticación se cifran en un mensaje SOAP. El mensaje se transmite en una conexión HTTP.

B. Los atributos de seguridad se colocan en formato SAML. La solicitud de servicio web y los datos de autenticación se encapsulan en un mensaje SOAP. El mensaje se transmite en una conexión HTTP a través de TLS.

C. Los datos de autenticación se colocan en formato SAML. Los datos de solicitud y autenticación del servicio web se encapsulan en un mensaje SOAP. El mensaje se transmite en una conexión HTTP.

D. Los datos de autenticación se colocan en formato SAML. La solicitud HTTP y los datos de autenticación se encapsulan en un mensaje SOAP. El mensaje se transmite en una conexión HTTP.

20. Jill está estableciendo un programa de ventas en toda la empresa que requerirá diferentes grupos de usuarios con diferentes privilegios para acceder a

la información en una base de datos centralizada. ¿Cómo debe proteger el administrador de seguridad la base de datos?

R. Aumente los controles de seguridad de la base de datos y proporcione más granularidad.

B. Implemente controles de acceso que muestren los permisos de cada usuario cada vez que tengan acceso a la base de datos.

C. Cambie la etiqueta de clasificación de la base de datos a un estado de seguridad más alto.

D. Disminuya la seguridad para que todos los usuarios puedan acceder a la información según sea necesario.

21. Bethany está trabajando en un sistema de control de acceso obligatorio (MAC). Ella ha estado trabajando en un archivo que fue clasificado como Secreto. Ya no puede acceder a este archivo porque ha sido reclasificado como Top Secret. Ella deduce que el proyecto en el que estaba trabajando acaba de aumentar en confidencialidad y ahora sabe más sobre este proyecto de lo que su autorización y necesidad de saber permite. ¿Cuál de los siguientes se refiere a un concepto que intenta evitar que se produzca este tipo de escenario?

R. Canal de almacenamiento encubierto

B. Ataque de inferencia

C. Noninterference

D. agregación

22. Se pueden realizar varios ataques contra tarjetas inteligentes. Side-channel es una clase de ataques que no intenta comprometer un defecto o debilidad. ¿Cuál de los siguientes no es un ataque de canal lateral?

R. Análisis diferencial de potencia

B. Análisis de microprobing

C. Análisis de tiempos

D. Análisis electromagnético

23. Emily está escuchando el tráfico de red y capturando contraseñas mientras se envían al servidor de autenticación. Ella planea usar las contraseñas como parte de un ataque futuro. ¿Qué tipo de ataque es éste?

R. Ataque con fuerza bruta

B. ataque de diccionario

C. Ataque a la ingeniería social

D. Ataque de repetición

24. ¿Cuál de las siguientes maneras es la mejor manera de reducir los ataques de fuerza bruta que permiten a los intrusos descubrir las contraseñas de los usuarios?

R. Aumente el nivel de recorte.

B. Bloquee una cuenta durante un cierto período de tiempo después de alcanzar el nivel de recorte.

C. Una vez alcanzado un umbral de intentos de inicio de sesión fallidos, el administrador debe bloquear físicamente la cuenta.

D. Elija un algoritmo más débil que cifre el archivo de contraseña.

25. Phishing y pharming son similares. ¿Cuál de los siguientes describe correctamente la diferencia entre phishing y pharming?

R. La información personal se recopila de las víctimas a través de sitios web de aspecto legítimo en ataques de phishing, mientras que la información personal se recopila de las víctimas a través de correo electrónico en ataques de faring.

B. Los ataques de phishing apuntan a los destinatarios de correo electrónico a un formulario donde las víctimas introducen información personal, mientras que los ataques de pharming utilizan formularios emergentes en sitios web legítimos para recopilar información personal de las víctimas.

C. Las víctimas son señaladas a un sitio web falso con un nombre de dominio que se parece al nombre de dominio de un sitio legítimo en un ataque de phishing, mientras que las víctimas son dirigidas a un sitio web falso como resultado de un nombre de dominio legítimo que se traduce incorrectamente por el servidor DNS en un ataque faring.

D. El phishing es un ataque técnico, mientras que el pharming es un tipo de ingeniería social.

26. Existen varios tipos de sistemas de detección de intrusiones (IDS). ¿Qué tipo de IDS crea un perfil de las actividades normales de un entorno y asigna una puntuación de anomalía a los paquetes basados en el perfil?

R. Basado en el Estado

B. Anomalía estadística

C. Sistema de detección de uso indebido

D. Firma de protocolo basada en

27. Un IDS basado en reglas adopta un enfoque diferente de un sistema basado en firmas o anomalías. ¿Cuál de los siguientes es característico de un IDS basado en reglas?

R. Utiliza la programación IF/THEN dentro de sistemas expertos

B. Identifica los protocolos utilizados fuera de sus límites comunes

C. Compara patrones con varias actividades a la vez

D. Puede detectar nuevos ataques

28. Tom trabaja en una gran empresa minorista que recientemente implementó la identificación por radiofrecuencia (RFID) para gestionar mejor sus procesos de inventario. Los empleados utilizan escáneres para recopilar información relacionada con el producto en lugar de buscar manualmente los datos del producto. Tom ha descubierto que los clientes maliciosos han llevado a cabo ataques a la tecnología RFID para reducir la cantidad que pagan en los artículos de la tienda. ¿Cuál de las siguientes es la razón más probable para la existencia de este tipo de vulnerabilidad?

R. El equipo de seguridad de la compañía no entiende cómo asegurar este tipo de tecnología.

B. El costo de integrar la seguridad dentro de RFID es prohibitivo para los costos.

C. La tecnología tiene bajas capacidades de procesamiento y el cifrado es muy intensivo en procesadores.

D. RFID es una tecnología nueva y emergente, y la industria actualmente no tiene maneras de asegurarlo.

29. Tanya es el administrador de seguridad de una gran empresa minorista distribuida. La red de la compañía tiene muchos dispositivos de red y dispositivos de software diferentes que generan registros y datos de auditoría. Tanya y su personal se han visto abrumados por tratar de revisar todos los archivos de registro al intentar identificar si algo sospechoso está ocurriendo dentro de la red. ¿Cuál de las siguientes es la mejor solución para que esta empresa la implemente?

R. Información de seguridad y gestión de eventos

B. Herramientas de correlación de eventos

C. Sistemas de detección de intrusiones

D. Herramientas de gestión de correlación de eventos de seguridad

30. La Agencia logística del departamento de defensa de un país es responsable de garantizar que todos los materiales necesarios lleguen a los lugares adecuados para apoyar las actividades diarias del departamento. Los datos que esta agencia mantiene deben estar protegidos de acuerdo con los tres principios principales de seguridad de los controles de seguridad. ¿Para las responsabilidades de esta agencia, qué principio de seguridad tiene la máxima prioridad?

R. confidencialidad

B. integridad

C. disponibilidad

D. privacidad

31. Claudia es la CISO de una institución financiera global, supervisando la seguridad de cientos de millones de cuentas bancarias. ¿Cuál de los tres principios principales de seguridad debería considerar más importantes a la hora de priorizar los controles que su empresa debería implementar?

R. confidencialidad

B. integridad

C. disponibilidad

D. autenticidad

32. ¿Cuál de los siguientes es un ejemplo de un sistema de gestión de credenciales, también conocido como sistema de gestión de identidades (IdM)?

R. Un registro histórico de las actividades realizadas por los usuarios una vez que han presentado sus credenciales a un sistema central de autorización

B. Una base de datos de las credenciales que se han registrado a cada individuo en una empresa, con el fin de correlacionar a los usuarios con los nombres de usuario y las configuraciones regionales

C. Un sistema de información de seguridad y gestión de eventos (SIEM) que contiene los registros de varios sistemas de credencialización de la empresa, para la correlación de actividades por ID

D. Un Centro de distribución de claves Kerberos (KDC) que contiene las claves simétricas de todas las entidades y sistemas de un reino kerberos, que se puede administrar de forma centralizada para asegurarse de que está actualizado con respecto a las adiciones y eliminaciones de claves

33. ¿Cuál de los siguientes atributos se utiliza para autenticar biométricamente la identidad de un usuario?

R. Algo que sabes

B. Algo que tienes

C. Algo que eres

D. En algún lugar donde estés

34. Dentro de la autenticación biométrica, ¿qué es una tasa de error tipo II?

R. La tasa de errores en la que el sistema acepta falsamente la autenticación de una persona que no es a quien pretenden ser

B. La tasa de errores en la que el sistema rechaza falsamente la autenticación de una persona que es a quien pretenden ser

C. La tasa de errores que produce el sistema cuando los rechazos falsos y las aceptaciones falsas son iguales

D. La tasa de errores en la que el sistema no acepta o rechaza la autenticación de una persona independientemente de su validez

35. ¿Cuál de los siguientes criterios es la consideración más importante para la selección e implementación de un sistema de autenticación biométrica?

R. Tasa de aceptación falsa (FAR) o tasa de error tipo II

B. Tasa de rechazo falso (FRR) o tasa de error tipo I

C. Velocidad de error de cruce (CER) o tasa de error igual (EER)

D. Velocidad de procesamiento

36. Aunque "algo que usted sabe", en forma de contraseñas, es el factor de autenticación más común todavía utilizado hoy en día, se considera uno de los más débiles. Esto se debe a que las contraseñas son fáciles de compartir para los usuarios, y relativamente fáciles de robar o adivinar para los adversarios. ¿Cuál de las siguientes medidas es la mejor manera de contrarrestar los ataques a esta forma de autenticación?

R. Almacene todas las contraseñas solo en forma cifrada, de modo que recuperarlas requiera una clave especial para descifrarlas para la autenticación.

B. Utilice una directiva de contraseñas para asegurarse de que las contraseñas se eligen de tal manera que no son fáciles de adivinar para un atacante ni fáciles de hacer para un atacante.

C. Requiere que todas las contraseñas se compongan de una combinación de caracteres únicos, independientemente de la longitud.

D. Asegúrese de que las cuentas están bloqueadas después de un número mínimo de conjeturas incorrectas en un corto período de tiempo.

37. ¿Cuál de las siguientes es la secuencia correcta en el proceso de autenticación Kerberos con respecto a contraseñas, centros de distribución de claves (KDC), servidores de concesión de vales (TGS), tickets de concesión de vales (TGT), servicios y vales de servicio?

R. El usuario proporciona un nombre de usuario/contraseña a la estación de trabajo, la estación de trabajo obtiene un TGT del TGS, y posteriormente obtiene un ticket de servicio del KDC, que presenta al servicio.

B. La estación de trabajo obtiene un TGT del KDC, que el usuario valida con una contraseña. A continuación, el TGT se cambia por un vale de servicio del TGS, que se presenta al servicio.

C. El usuario proporciona un nombre de usuario/contraseña a la estación de trabajo, la estación de trabajo obtiene un TGT del KDC, y posteriormente obtiene un ticket de servicio del TGS, que presenta al servicio.

D. El usuario obtiene un ticket de servicio del servicio. A continuación, el usuario valida este vale con un nombre de usuario/contraseña proporcionado al TGS, que da lugar a un TGT que es validado adicionalmente por el KDC en un paso final.

38. En uso práctico, ¿cuál de los siguientes describe mejor una "sesión"?

R. Cualquier intercambio de datos entre dos puntos finales discretos, a lo largo de cualquier duración arbitraria

B. Cualquier intercambio autenticado entre dos partes que se utiliza para llevar a cabo una conversación, con un comienzo discreto, período de actividad y terminación

C. Cualquier período discreto de tiempo que un usuario haya iniciado sesión en una estación de trabajo

D. El volumen de datos intercambiados entre dos sistemas durante un período de tiempo discreto

39. El uso de "servidores de recursos" y "servidores de autorización" para permitir que un servicio web "cliente" (como LinkedIn) acceda a un "propietario de recursos" (como Google) para la autorización federada es un sello distintivo de qué estándar abierto?

R. OpenID

B. Saml

C. Sso

D. OhAuth

40. ¿Cuál de las siguientes no es cierto de OpenID Connect (OIDC)?

R. Se utiliza principalmente como un mecanismo de inicio de sesión único (SSO) basado en estándares abiertos entre plataformas dispares dentro de un entorno empresarial.

B. Se coloca en capas en el protocolo OAuth para permitir la autenticación y la autorización de forma transparente para las solicitudes de recursos de cliente.

C. Admite tres flujos: flujo de código de autorización, flujo implícito y flujo híbrido.

D. Implica redirecciones del navegador desde el proveedor OpenID de nuevo a la parte de confianza utilizando códigos de autorización.

41. ¿Cuál de los siguientes atributos se agrega más allá de los mecanismos tradicionales de control de acceso (RBAC, MAC y DAC) para implementar ABAC?

R. Temas

B. Objetos

C. Acciones

D. contexto

CLAVE DE RESPUESTA RÁPIDA

1 . C

2 . B

3 . C

4 . C

5 . un

6 . B

7 . C

8 . B

9 . B

10. A

11. C

12. D

13. A

14. B

15. A

16. D

17. B

18. D

19. C

20. A

21. C

22. B

23. D

24. B

25. C

26. B

27. A

28. C

29. A

30. A

31. B

32. D

33. C

34. A

35. D

36. B

37. C

38. B

39. D

40. A

41. D

RESPUESTAS A

1 . ¿Cuál de las siguientes opciones NO describe correctamente un servicio de directorio?

R. Administra objetos dentro de un directorio mediante espacios de nombres.

B. Aplica la directiva de seguridad mediante la realización de funciones de control de acceso y gestión de identidades.

C. Asigna espacios de nombres a cada objeto en bases de datos que se basan en el estándar X.509 y a los que tiene acceso LDAP.

D. Permite a un administrador configurar y administrar cómo se lleva a cabo la identificación dentro de la red.

☑ **C.** La mayoría de las empresas tienen algún tipo de directorio que contiene información relativa a los recursos de red y usuarios de la empresa. La mayoría de los directorios siguen un formato jerárquico de base de datos, basado en el estándar X.500 (no X.509), y un tipo de protocolo, como en el Protocolo ligero de acceso a directorios (LDAP), que permite a los sujetos y aplicaciones interactuar con el directorio. Las aplicaciones pueden solicitar información sobre un usuario determinado realizando una solicitud LDAP al directorio y los usuarios pueden solicitar información sobre un recurso específico mediante una solicitud similar. Un servicio de directorio asigna nombres distintivos (DN) a cada objeto de bases de datos basadas en el estándar X.500 al que tiene acceso LDAP. Cada nombre distintivo representa una colección de atributos sobre un objeto específico y se almacena en el directorio como una entrada.

☒ **A** es incorrecto porque un servicio de directorio administra objetos dentro de bases de datos jerárquicas. El servicio de directorio permite a un administrador configurar y administrar cómo se lleva a cabo la identificación, autenticación,

autorización y control de acceso dentro de la red. Los objetos del directorio se etiquetan e identifican con espacios de nombres, que es la forma en que el servicio de directorio mantiene los objetos organizados.

☒ **B** es incorrecto porque los servicios de directorio aplican la directiva de seguridad configurada mediante la realización de funciones de control de acceso y administración de identidades. Por ejemplo, cuando un usuario inicia sesión en un controlador de dominio en un entorno Windows, el servicio de directorio (Active Directory) determina a qué recursos de red puede y no puede tener acceso.

☒ **D** es incorrecto porque los servicios de directorio permiten a un administrador configurar y administrar cómo se lleva a cabo la identificación dentro de la red. También permite la configuración y administración de la autenticación, la autorización y el control de acceso.

2 . A Hannah se le ha asignado la tarea de instalar software de administración de acceso web (WAM). ¿Cuál es la mejor descripción para qué se utiliza wam comúnmente?

R. Controlar las entidades externas que solicitan acceso a través de bases de datos X.500

B. Controlar las entidades externas que solicitan acceso a objetos internos

C. Controlar las entidades internas que solicitan acceso a través de bases de datos X.500

D. Controlar las entidades internas que solicitan acceso a objetos externos

☑ **B.** El software de administración de acceso web (WAM) controla a qué pueden acceder los usuarios cuando utilizan un explorador web para interactuar con activos empresariales basados en web. Este tipo de tecnología se está volviendo continuamente más robusta y experimentando un mayor despliegue. Esto se debe al mayor uso del comercio electrónico, la banca en línea, la prestación de contenidos, los servicios web y mucho más. Los componentes y actividades básicos de un proceso de administración de control de acceso web son los siguientes:

1. El usuario envía credenciales al servidor web.

2. El servidor web solicita a la plataforma WAM que autentique al usuario. WAM autentica contra el directorio LDAP y recupera las autorizaciones de la base de datos de directivas.

3. Solicitudes de usuario para acceder a un recurso (objeto).

4. El servidor web verifica que el acceso a objetos está autorizado y permite el acceso al recurso solicitado.

☒ **A** es incorrecto porque un servicio de directorio debe llevar a cabo el control de acceso en el directorio de una base de datos X.500, no software de administración de acceso web. El servicio de directorio administra las entradas y los datos y aplica la directiva de seguridad configurada mediante la realización de funciones de control de acceso y administración de identidades. Algunos ejemplos de servicios de directorio son Active Directory y NetIQ eDirectory. Aunque las solicitudes de acceso basadas en web pueden ser a objetos retenidos dentro de una base de datos, WAM controla principalmente la comunicación entre exploradores web y servidores. Los servidores web deben comunicarse a una base de datos back-end, normalmente a través de un servicio de directorio.

☒ **C** es incorrecto porque un servicio de directorio debe llevar a cabo el control de acceso para las entidades internas que solicitan acceso a una base de datos X.500 mediante el LDAP. Este tipo de base de datos proporciona una estructura jerárquica para la organización de objetos (sujetos y recursos). El servicio de directorio desarrolla nombres distintivos únicos para cada objeto y anexa el atributo correspondiente a cada objeto según sea necesario. El servicio de directorio aplica una directiva de seguridad (configurada por el administrador) para controlar cómo interactúan los sujetos y objetos. Aunque las solicitudes de acceso basadas en web pueden ser a objetos retenidos dentro de una base de datos, WAM controla principalmente la comunicación entre exploradores web y servidores. WAM se desarrolló principalmente para la comunicación externa a interna, aunque también se puede utilizar para la comunicación interno a interna. La respuesta B es la mejor respuesta de las cuatro proporcionadas.

☒ **D** es incorrecto porque el software WAM se utiliza más comúnmente para controlar entidades externas que solicitan acceso a objetos internos; no al revés, como lo indica la opción de respuesta. Por ejemplo, WAM puede ser utilizado por un banco para controlar el acceso de sus clientes a los datos de la cuenta back-end.

3 . Hay varios tipos de enfoques de administración de contraseñas utilizados por los sistemas de administración de identidades. ¿Cuál de los siguientes reduce el volumen de llamadas de help-desk, pero también es criticado por la facilidad con la que un hacker podría obtener acceso a múltiples recursos si una contraseña se ve comprometida?

R. Restablecimiento de contraseña de administración

B. Restablecimiento de contraseña de autoservicio

C. Sincronización de contraseñas

D. Restablecimiento asistido de contraseña

☑ **C.** La sincronización de contraseñas está diseñada para reducir la complejidad de mantenerse al día con diferentes contraseñas para diferentes sistemas. La tecnología de sincronización de contraseñas puede permitir a los

usuarios mantener una sola contraseña en varios sistemas mediante la sincronización transparente de la contraseña a otros sistemas y aplicaciones. Esto reduce el volumen de llamadas del servicio de asistencia. Una crítica a este enfoque es que dado que sólo una contraseña se utiliza para acceder a diferentes recursos, ahora el hacker sólo tiene que averiguar una credencial establecida para obtener acceso no autorizado a todos los recursos.

A es incorrecto porque no hay tal cosa como un restablecimiento de contraseña de administración. Esta respuesta es un distractador. Los enfoques más comunes de administración de contraseñas son sincronización de contraseñas, restablecimiento de contraseña de autoservicio y restablecimiento asistido de contraseñas.

B es incorrecto porque el restablecimiento de contraseña de autoservicio no se ocupa necesariamente de varias contraseñas. Sin embargo, ayuda a reducir el volumen total de llamadas de help-desk relacionadas con contraseña. En el caso del restablecimiento de contraseña de autoservicio, los usuarios pueden restablecer sus propias contraseñas. Por ejemplo, cuando un usuario olvida su contraseña, se le puede pedir que responda a las preguntas que identificó durante el proceso de registro. Si la respuesta que da coincide con la información que proporcionó durante el registro, se le concede la capacidad de cambiar su contraseña.

D es incorrecto porque el restablecimiento asistido de contraseña no se ocupa necesariamente de varias contraseñas. Reduce el proceso de resolución de problemas de contraseña al permitir que el servicio de ayuda autentique a un usuario antes de restablecer su contraseña. El llamador debe identificarse y autenticarse a través de la herramienta de administración de contraseñas antes de que se pueda cambiar la contraseña. Una vez actualizada la contraseña, el sistema al que el usuario está autenticando debe requerir que el usuario cambie su contraseña de nuevo. Esto aseguraría que sólo ella (y no ella y la persona de ayuda) conozca su contraseña. El objetivo de un producto de restablecimiento de contraseña asistido es reducir el costo de las llamadas de soporte técnico y asegurarse de que todas las llamadas se procesan de una manera uniforme, consistente y segura.

4 . En los Estados Unidos, las agencias federales deben adherirse a la "Verificación de Identidad Personal" de la Norma Federal de Procesamiento de Información (FIPS, por susape) 201-2, que discute las medidas técnicas de autenticación para empleados y contratistas federales. Esta norma debe seguirse para garantizar cuál de las siguientes condiciones?

R. Que los empleados del gobierno están debidamente autorizados para el trabajo asignado

B. Que a los empleados públicos sólo se les permite el acceso a los datos de su nivel de autorización

C. Que la identidad del empleado del gobierno ha sido debidamente verificada

D. Que los datos a los que los empleados gubernamentales tienen acceso han sido clasificados adecuadamente

☑ **C.** FIPS 201-2 especifica los estándares del gobierno de ee. UU. para la verificación de identidad personal (PIV, por sus días), dando diversos requisitos de seguridad. El acceso de los empleados gubernamentales y los agentes contratados a información restringida depende de su nivel de autorización y de su necesidad de conocerla, pero ante todo el gobierno requiere la seguridad de que el individuo es quien dice ser.

☒ **A** es incorrecto porque los empleados gubernamentales deben ser debidamente autorizados para la información a la que se les concede acceso, pero antes de dicho acceso, su verdadera identidad debe estar disponible para su revisión y afirmación.

☒ **B** es incorrecto porque a los empleados públicos solo se les debe permitir el acceso a la información que están autorizados a conocer y tener la necesidad de acceder. Pero una vez más, esto debe basarse en un nivel específico de garantía de que la autorización que poseen es válida.

☒ **D** es incorrecta porque la clasificación de datos no está directamente relacionada con la Verificación de identidad personal.

5 . ¿Cuál de las siguientes opciones NO describe el control de acceso basado en roles compatible con la privacidad?

R. Es un ejemplo de un modelo discrecional de control de acceso.

B. Los controles de acceso detallados indican el tipo de datos a los que los usuarios pueden acceder en función del nivel de sensibilidad a la privacidad de los datos.

C. Es una extensión del control de acceso basado en roles.

D. Debe utilizarse para integrar políticas de privacidad y políticas de control de acceso.

☑ **R.** Un sistema que utiliza el control de acceso discrecional (DAC) permite al propietario del recurso especificar qué sujetos pueden tener acceso a recursos específicos. Este modelo se denomina discrecional porque el control del acceso se basa en la discreción del propietario. Muchas veces los gerentes de departamento, o gerentes de unidades de negocio, son los propietarios de los datos dentro de su departamento específico. Al ser el propietario, pueden especificar quién debe tener acceso y quién no. El control de acceso basado en roles con control de privacidad es una extensión del control de acceso basado en roles (RBAC). Hay tres modelos principales de control de acceso: DAC, control

de acceso obligatorio (MAC) y RBAC. El control de acceso basado en roles compatible con la privacidad es un tipo de RBAC, no DAC.

B es incorrecto porque el control de acceso basado en roles compatible con la privacidad se basa en controles de acceso detallados que indican el tipo de datos a los que los usuarios pueden acceder en función del nivel de sensibilidad a la privacidad de los datos. Otros modelos de control de acceso, como MAC, DAC y RBAC, no se prestan para proteger el nivel de privacidad de los datos, sino las funciones que los usuarios pueden llevar a cabo. Por ejemplo, los administradores pueden acceder a una carpeta de privacidad, pero debe haber un control de acceso más detallado que indique, por ejemplo, que pueden acceder a las direcciones de casa de los clientes, pero no a los números de Seguro Social. La industria ha avanzado a necesitar un control de acceso mucho más detallado cuando se trata de información confidencial de privacidad como en los números de Seguro Social y los datos de tarjetas de crédito, razón por la cual se desarrolló un control de acceso basado en roles consciente de la privacidad.

C es incorrecto porque el control de acceso basado en roles compatible con la privacidad es una extensión del control de acceso basado en roles. Los derechos de acceso se determinan en función del rol y las responsabilidades del usuario dentro de la empresa, y del nivel de privacidad de los datos a los que necesita acceso.

D es incorrecto porque los idiomas utilizados para las políticas de privacidad y las políticas de control de acceso deben ser los mismos o integrados cuando se utiliza el control de acceso basado en roles con capacidad de privacidad. El objetivo del uso del control de acceso basado en roles con conciencia de privacidad es hacer que el control de acceso sea mucho más detallado y se centre en los datos relacionados con la privacidad, por lo que debería usar el mismo tipo de términos e idioma que la política y estándares de control de acceso originales de la organización.

6 . Security Assertion Markup Language (SAML) es un estándar basado en XML para intercambiar datos de autenticación y autorización entre sistemas en diferentes dominios de seguridad. SAML permite el uso compartido de información de autenticación, como cómo se llevó a cabo la autenticación, los atributos de entidad y a qué está autorizada la entidad para acceder. SAML se utiliza con mayor frecuencia en entornos basados en web que requieren capacidad de inicio de sesión único (SSO). ¿Cuál de los siguientes tiene una definición correcta asociada al componente SAML correspondiente?

R. Se utilizan dos aserciones SAML (autenticación, autorización) que indican que una autoridad SAML validó un asunto específico.

B. Las aserciones SAML se utilizan con mayor frecuencia para permitir la federación de identidades y la autorización distribuida.

C. La especificación de enlace SAML describe cómo incrustar mensajes SAML dentro de los protocolos TCP y UDP.

D. Los perfiles SAML definen cómo se deben implementar los mensajes SAML, las aserciones y los protocolos en SSL y TLS.

☑ **B.** SAML proporciona un modelo para permitir que dos partes compartan información de autenticación sobre una entidad. Las dos partes se consideran el proveedor de servicios y el proveedor de identidades. El proveedor de identidades afirma información sobre la entidad de seguridad, como si el sujeto se ha autenticado o tiene un atributo determinado. El proveedor de servicios utiliza la información proporcionada por el proveedor de identidades para tomar decisiones de acceso, incluidas, entre otras, si confiar o no en la afirmación del proveedor de identidades. Al confiar en la información del proveedor de identidades, el proveedor de servicios puede proporcionar servicios sin necesidad de que la entidad de seguridad se autentique de nuevo. Este marco permite la identificación federada y la autenticación distribuida entre dominios.

☒ **A** es incorrecto porque hay tres tipos de aserciones SAML (autenticación, atributo, autorización) que indican una autoridad SAML validada un asunto específico. La aserción de autenticación valida que el sujeto fue autenticado por una autoridad SAML a través de una manera específica. Por ejemplo, una aserción podría indicar que Sam Long se autentificó en una fecha específica, en un momento específico, mediante el uso de un certificado digital y la autenticación es válida durante 30 minutos. La parte que afirma envía estos datos de autenticación a la parte de confianza para que el sujeto se pueda autenticar en el sistema de la parte de confianza y el sujeto no necesite iniciar sesión de nuevo.

☒ **C** es incorrecto porque la especificación de enlace SAML describe cómo incrustar mensajes SAML dentro de protocolos de comunicaciones o mensajería para permitir el intercambio de mensajes de solicitud-respuesta SAML. Los enlaces SAML definen cómo se llevan a cabo estos intercambios de mensajes en protocolos de capa de aplicación (por ejemplo, SOAP, HTTP), no protocolos de capa de transporte como TCP y UDP. La especificación SAML define el protocolo SAML, que es un protocolo de solicitud y respuesta basado en XML para procesar aserciones SAML. Esto significa que esta especificación pertenece a los datos de carga útil de un paquete, que trabaja en la capa de aplicación del modelo OSI. Las capas de transporte se encuentran en una parte inferior de la pila de red y no tienen ninguna interacción directa con esta especificación XML.

☒ **D** es incorrecto porque los perfiles SAML definen cómo se deben implementar los mensajes SAML, las aserciones y los protocolos en los casos de uso. Esta especificación no se ocupa de los protocolos de la capa de sesión y transporte como en SSL y TLS. Cada perfil dentro de la especificación SAML describe cómo se deben usar mensajes SAML, aserciones y protocolos en escenarios específicos. Por ejemplo, un perfil SAML describe cómo se va a usar SAML para admitir un único entorno de inicio de sesión en varias aplicaciones

web. Este perfil define cómo se admitirá un cliente compatible con SAML (es decir, el explorador web) y cómo se deben administrar los datos de identificación entre varios proveedores de servicios.

7 . A Brian se le ha pedido que trabaje en el directorio virtual del nuevo sistema de gestión de identidades de su empresa. ¿Cuál de los siguientes describe mejor un directorio virtual?

R. Meta-directorio

B. Información de atributos de usuario almacenada en una base de datos de recursos humanos

C. Contenedor virtual para datos de múltiples fuentes

D. Un servicio que permite a un administrador configurar y administrar cómo se lleva a cabo la identificación

☑ **C.** Un directorio de red es un contenedor para usuarios y recursos de red. Un directorio no contiene (ni conoce) todos los usuarios y recursos de la empresa, por lo que se debe usar una colección de directorios. Un directorio virtual recopila la información necesaria utilizada de orígenes dispersos por toda la red y los almacena en un directorio virtual central (contenedor virtual). Esto proporciona una vista unificada de la información de identidad digital de todos los usuarios en toda la empresa. El directorio virtual se sincroniza periódicamente con todos los almacenes de identidades (directorios de red individuales) para garantizar que todas las aplicaciones y componentes de administración de identidades de la empresa utilicen la información más actualizada.

☒ **A** es incorrecto porque mientras que un directorio virtual es similar a un meta-directorio, el meta-directorio funciona con un directorio, mientras que un directorio virtual funciona con varios orígenes de datos. Cuando un componente de administración de identidades realiza una llamada a un directorio virtual, tiene la capacidad de analizar directorios diferentes en toda la empresa, mientras que un meta-directorio solo tiene la capacidad de analizar el único directorio al que está asociado.

☒ **B** es incorrecto porque describe mejor un almacén de identidades. Una gran cantidad de información almacenada en un directorio de administración de identidades está dispersa en toda la empresa. La información de atributos de usuario (estado del empleado, descripción del trabajo, departamento, etc.) normalmente se almacena en la base de datos de recursos humanos; la información de autenticación podría estar en un servidor Kerberos; la información de identificación de roles y grupos puede estar en una base de datos SQL; y la información de autenticación orientada a recursos se puede almacenar en Active Directory en un controlador de dominio. Estos se conocen comúnmente como almacenes de identidades y se encuentran en diferentes

lugares de la red. Muchos productos de administración de identidades utilizan directorios virtuales para llamar a los datos de estos almacenes de identidades.

☒ **D** es incorrecto porque describe el servicio de directorio. El servicio de directorio permite a un administrador configurar y administrar cómo se produce la identificación, autenticación, autorización y control de acceso dentro de la red. Administra los objetos dentro de un directorio mediante espacios de nombres y aplica la directiva de seguridad configurada mediante la realización de funciones de control de acceso y administración de identidades.

8 . ¿Cuál de las siguientes describe con precisión la identidad como servicio (IDaaS)?

R. Una forma de inicio de sesión único (SSO) que abarca varias entidades de una empresa

B. Una forma de SSO que abarca varias empresas independientes

C. Una forma de proporcionar SSO sin múltiples formas de autenticación

D. Una forma de demostrar identidad sin tener que firmar

☑ **B.** Los proveedores de IDaaS permiten a sus clientes tener una forma de SSO que funciona en varias cuentas independientes para proveedores independientes. Un ejemplo común es la capacidad de usar una cuenta de Google para crear una página de Facebook.

☒ **A** es incorrecto porque SSO que abarca varias entidades dentro de una empresa es más comúnmente aprovisionado por una infraestructura de clave pública (PKI) como lo proporciona Active Directory en un entorno de Microsoft o a través de un protocolo 802.1X para otras tecnologías.

☒ **C** es incorrecto porque cualquier solución SSO debe proporcionar la autenticación multifactor.

☒ **D** es incorrecto porque todas las demostraciones de identidad requieren que la autenticación sea válida.

9 . ¿Cuál de los siguientes describe correctamente una identidad federada y su rol dentro de los procesos de administración de identidades?

R. Una identidad noportable que se puede usar a través de los límites empresariales

B. Una identidad portátil que se puede utilizar a través de los límites empresariales

C. Una identidad que se puede usar en directorios virtuales de intranet y almacenes de identidades

D. Una identidad especificada por nombres de dominio que se pueden usar a través de los límites empresariales

☑ **B.** Una identidad federada es una identidad portátil y sus derechos asociados que se pueden usar a través de los límites empresariales. Permite autenticar a un usuario en varios sistemas y empresas de TI. La federación de identidades se basa en vincular las identidades distintas de un usuario en dos o más ubicaciones sin necesidad de sincronizar o consolidar la información del directorio. La identidad federada ofrece a las empresas y a los consumidores una forma más cómoda de acceder a los recursos distribuidos y es un componente clave del comercio electrónico.

☒ **A** es incorrecto porque una identidad federada es portátil. No se podía usar a través de los límites empresariales si no era portátil, y ese es el punto de una identidad federada. El mundo se hace más pequeño a medida que la tecnología acerca a las personas y las empresas. Muchas veces, cuando estamos interactuando con un solo sitio web, en realidad estamos interactuando con varias empresas diferentes, simplemente no lo sabemos. La razón por la que no sabemos es porque estas empresas están compartiendo nuestra identidad y la información de autenticación entre bastidores. Esto se hace para mejorar la facilidad de uso para el usuario.

☒ **C** es incorrecto porque una identidad federada está pensada para usarse a través de los límites empresariales, no dentro de la organización. En otras palabras, su uso se extiende más allá de la organización propietaria de los datos de usuario. Mediante identidades federadas, las organizaciones con diferentes tecnologías para servicios de directorio, seguridad y autenticación pueden compartir aplicaciones, lo que permite a los usuarios iniciar sesión en varias aplicaciones con el mismo ID de usuario, contraseña, etc.

☒ **D** es incorrecto porque un nombre de dominio no especifica una identidad federada. Una identidad federada es una identidad portátil y sus derechos asociados. Incluye el nombre de usuario, la contraseña y otra información de identificación personal utilizada para iniciar sesión en una aplicación.

10. Las contramedidas de seguridad deben ser transparentes para los usuarios y atacantes. ¿Cuál de los siguientes NO describe la transparencia?

R. Las actividades del usuario son monitoreadas y rastreadas sin afectar negativamente al rendimiento del sistema.

B. Las actividades del usuario son monitoreadas y rastreadas sin que el usuario conozca el mecanismo que está llevando a cabo.

C. Se permite a los usuarios acceder de una manera que no afecte negativamente a los procesos empresariales.

D. Los intentos de acceso no autorizados se deniegan y se registran sin que el intruso sepa sobre el mecanismo que está llevando a cabo esto.

☑ **R.** Desafortunadamente, los componentes de seguridad suelen afectar al rendimiento del sistema de una manera u otra, aunque muchas veces es imperceptible para el usuario. Existe la posibilidad de que si el rendimiento de un sistema es notablemente lento, esto podría ser una indicación de que las contramedidas de seguridad están en su lugar. La razón por la que los controles deben ser transparentes es para que los usuarios y intrusos no sepan lo suficiente como para poder deshabilitarlos o omitirlos. Los controles tampoco deben interponerse en el camino de la empresa pudía llevar a cabo las funciones necesarias.

☒ **B** es incorrecto porque la transparencia consiste en que las actividades se supervisan y rastrean sin el conocimiento del usuario del mecanismo que realiza la supervisión y el seguimiento. Si bien es una práctica recomendada decirles a los usuarios si su uso de computadoras está siendo monitoreado, no es necesario decirles cómo se están monitoreando. Si los usuarios son conscientes de los mecanismos que supervisan sus actividades, es posible que intente deshabilitarlas o omitirlas.

☒ **C** es incorrecto porque debe haber un equilibrio entre seguridad y usabilidad. Esto significa que se debe permitir el acceso a los usuarios, cuando proceda, sin afectar a los procesos empresariales. Deberían tener los medios para hacer su trabajo.

☒ **D** es incorrecto porque no desea que los intrusos sepan acerca de los mecanismos en su lugar para denegar y registrar intentos de acceso no autorizados. Un intruso podría usar este conocimiento para deshabilitar o omitir el mecanismo y obtener acceso no autorizado a los recursos de red.

11. ¿Qué lenguaje de marcado permite el uso compartido de directivas de seguridad de aplicaciones para garantizar que todas las aplicaciones sigan las mismas reglas de seguridad?

R. XML

B. SPML

C. XACML

D. GML

☑ **C.** Dos o más empresas pueden tener un modelo de confianza configurado para compartir métodos de identidad, autorización y autenticación. Esto significa que si Bill se autentica en el software de su empresa, este software puede pasar los parámetros de autenticación al software de su socio. Esto permite a Bill interactuar con el software del socio sin tener que autenticarse dos veces. Esto puede ocurrir a través del lenguaje de marcado de control de acceso extensible (XACML), que permite a dos o más organizaciones compartir directivas de seguridad de aplicaciones en función de su modelo de confianza. XACML es un lenguaje de marcado y modelo de procesamiento que se

implementa en XML. Declara las directivas de control de acceso y describe cómo interpretarlas.

☒ **A** es incorrecto porque XML (Extensible Markup Language) es un método para codificar electrónicamente documentos y representar estructuras de datos como las de los servicios web. XML no se utiliza para compartir información de seguridad. XML es un estándar abierto que es más robusto que su predecesor, HTML. Además de servir como lenguaje de marcado en sí mismo, XML sirve como base para otros estándares XML más específicos del sector. XML permite a las empresas utilizar un lenguaje de marcado que satisface sus diferentes necesidades mientras todavía pueden comunicarse entre sí.

☒ **B** es incorrecto porque el lenguaje de marcado de aprovisionamiento de servicios (SPML) es utilizado por las empresas para intercambiar información de aprovisionamiento de usuarios, recursos y servicios, no información de seguridad de aplicaciones. SPML es un marco basado en XML desarrollado por OASIS con el objetivo de permitir que las plataformas empresariales (como portales web y servidores de aplicaciones) generen solicitudes de aprovisionamiento en varias empresas con el fin de la configuración segura y rápida de servicios y aplicaciones web.

☒ **D** es incorrecto porque Generalized Markup Language (GML) es un método creado por IBM para dar formato a documentos. Describe un documento en términos de sus partes (capítulos, párrafos, listas, etc.) y su relación (niveles de partida). GML fue predecesor de Standard Generalized Markup Language (SGML) y Hypertext Markup Language (HTML).

12. La importancia de proteger los registros de auditoría generados por ordenadores y dispositivos de red se destaca por el hecho de que es requerido por muchas de las regulaciones actuales. ¿Cuál de los siguientes NO explica por qué se deben proteger los registros de auditoría?

R. Si no están debidamente protegidos, es posible que estos registros no sean admisibles durante un proceso judicial.

B. Los registros de auditoría contienen datos confidenciales y solo deben ser accesibles para un determinado subconjunto de personas.

C. Los intrusos pueden intentar fregar los registros para ocultar sus actividades.

D. El formato de los registros debe ser desconocido y no estar disponible para el intruso.

☑ **D.** Las herramientas de auditoría son controles técnicos que realizan un seguimiento de la actividad dentro de una red, en un dispositivo de red o en un equipo específico. Aunque la auditoría no es una actividad que deniegue a una entidad acceso a una red o equipo, realizará un seguimiento de las actividades para que un administrador de seguridad pueda comprender los tipos de acceso que se produjeron, identificar una infracción de seguridad o advertir al

administrador de actividades sospechosas. Esta información se puede utilizar para señalar las debilidades de otros controles técnicos y ayudar al administrador a comprender dónde se deben realizar los cambios para conservar el nivel de seguridad necesario dentro del entorno. Los intrusos también pueden usar esta información para explotar esas debilidades, por lo que los registros de auditoría deben protegerse mediante permisos, derechos y controles de integridad, como en algoritmos hash. Sin embargo, el formato de los registros de sistemas se estandariza comúnmente con todos los sistemas similares. Ocultar formatos de registro no es una contramedida habitual y no es una razón para proteger los archivos de registro de auditoría.

A es incorrecto porque se debe tener el debido cuidado para proteger los registros de auditoría para que sean admisibles en los tribunales. Los seguimientos de auditoría se pueden usar para proporcionar alertas sobre cualquier actividad sospechosa que se pueda investigar más adelante. Además, pueden ser valiosos para determinar exactamente hasta dónde ha llegado un ataque y el alcance del daño que pudo haber sido causado. Es importante asegurarse de que se mantiene una cadena de custodia adecuada para garantizar que los datos recopilados puedan representarse correcta y precisamente en caso de que deban utilizarse para eventos posteriores, como procedimientos penales o investigaciones.

B es incorrecto porque solo el administrador y el personal de seguridad deben poder ver, modificar y eliminar la información de seguimiento de auditoría. Ninguna otra persona debería ser capaz de ver estos datos, y mucho menos modificarlos o eliminarlos. La integridad de los datos se puede garantizar con el uso de firmas digitales, herramientas de resumen de mensajes y controles de acceso sólidos. Su confidencialidad puede ser protegida con controles de cifrado y acceso, si es necesario, y se puede almacenar en medios de escritura una vez para evitar la pérdida o modificación de los datos. Los intentos de acceso no autorizados para auditar registros deben ser capturados e informados.

C es incorrecta porque la instrucción es true. Si un intruso irrumpe en su casa, hará todo lo posible para cubrir sus huellas al no dejar huellas dactilares o cualquier otra pista que pueda ser utilizada para vincularlo a la actividad criminal. Lo mismo ocurre con el fraude informático y la actividad ilegal. El intruso trabajará para cubrir sus huellas. Los atacantes a menudo eliminan los registros de auditoría que tienen esta información incriminatoria. (La eliminación de estos datos dentro de los registros de auditoría se denomina *depuración*.) La eliminación de esta información puede hacer que el administrador no sea alertado o consciente de la infracción de seguridad y pueda destruir datos valiosos. Por lo tanto, los registros de auditoría deben estar protegidos por un control de acceso estricto.

13. De lo siguiente, ¿en qué se basa el elemento principal en el que se basa una tabla de capacidades?

R. Un tema

B. Un objeto

C. Un producto

D. Una aplicación

☑ **R.** Una tabla de capacidad especifica los derechos de acceso que un determinado sujeto posee relativos a objetos específicos. Una lista de capacidades (también denominada tabla de capacidades) es diferente de una lista de control de acceso (ACL) porque el sujeto está enlazado a la tabla de capacidad, mientras que el objeto está enlazado a la ACL. Una capacidad puede ser en forma de token, vale o clave. Cuando un sujeto presenta un componente de capacidad, el sistema operativo (o aplicación) revisará los derechos de acceso y las operaciones descritas en el componente de capacidad y permitirá que el sujeto lleve a cabo solo esas funciones. Un componente de capacidad es una estructura de datos que contiene un identificador de objeto único y los derechos de acceso que el sujeto tiene a ese objeto. El objeto puede ser un archivo, matriz, segmento de memoria o puerto.

☒ **B** es incorrecto porque un objeto está enlazado a una lista de control de acceso (ACL), no a un componente de capacidad. Las ACL se utilizan en varios sistemas operativos, aplicaciones y configuraciones de enrutadores. Son listas de sujetos que están autorizados para acceder a un objeto específico y definen qué nivel de autorización se concede. La autorización se puede especificar a un individuo o grupo. Las ACL asignan valores de la matriz de control de acceso al objeto. Mientras que una capacidad corresponde a una fila en la matriz de control de acceso, la ACL corresponde a una columna de la matriz.

☒ **C** es incorrecto porque un producto puede ser un objeto o sujeto. Si un usuario intenta acceder a un producto (como un programa), el usuario es el sujeto y el producto es el objeto. Si un producto intenta tener acceso a una base de datos, el producto es el asunto y la base de datos es el objeto. Aunque un producto podría ser un tema en una lista de capacidades, por ejemplo, la mejor respuesta es A. Una lista de capacidades indica a qué objetos puede tener acceso un sujeto y las operaciones que se pueden llevar a cabo en esos objetos.

☒ **D** es incorrecto porque esto es similar a la respuesta C. Si un usuario intenta acceder a una aplicación, el usuario es el sujeto y la aplicación es el objeto. Si una aplicación intenta tener acceso a una base de datos, la aplicación es el asunto y la base de datos es el objeto. Aunque una aplicación podría ser un asunto en una lista de capacidades, por ejemplo, la mejor respuesta es A. Una lista de capacidades indica a qué objetos puede tener acceso un sujeto y las operaciones que se pueden llevar a cabo en esos objetos.

14. ¿Qué lenguaje de marcado permite a una empresa enviar solicitudes de servicio y a la empresa receptora proporcionar acceso a estos servicios?

R. XML

B. SPML

C. SGML

D. HTML

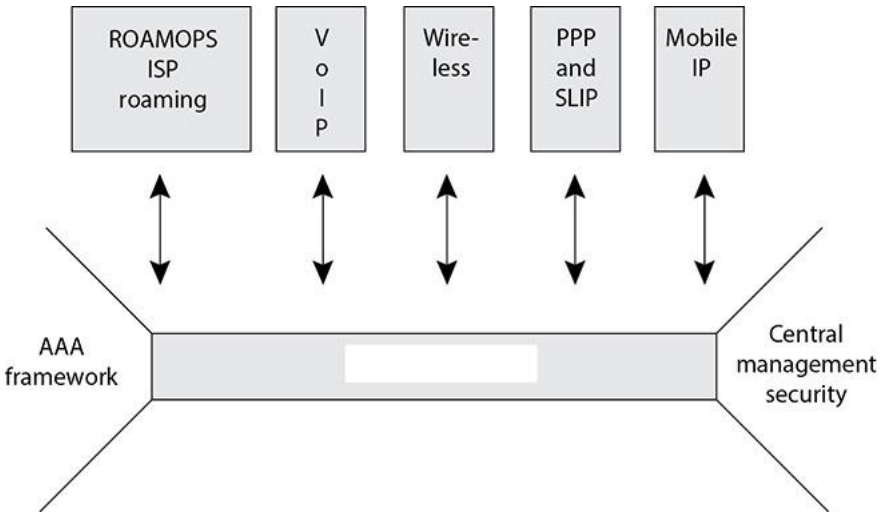
☑ **B.** Service Provisioning Markup Language (SPML) es un lenguaje de marcado, basado en el marco de lenguaje de marcado extensible (XML), que intercambia información sobre qué usuarios deben tener acceso a qué recursos y servicios. Así que digamos que una compañía automotriz y una compañía de neumáticos sólo permiten a los gerentes de inventario dentro de la compañía automotriz pedir neumáticos. Si Bob inicia sesión en el software de inventario de la compañía automovilística y pide 40 neumáticos, ¿cómo sabe la compañía de neumáticos que esta solicitud proviene de un proveedor autorizado y un usuario del grupo Administradores de inventario? El software de la compañía automovilística puede pasar información de identidad de usuario y grupo al software de la compañía de neumáticos. La compañía de neumáticos utiliza esta información de identidad para tomar una decisión de autorización que luego permite llenar la solicitud de Bob de 40 neumáticos. Dado que las empresas de envío y recepción siguen un estándar (XML), este tipo de interoperabilidad puede tener lugar.

☒ **A** es incorrecto porque no es la mejor respuesta a la pregunta. SPML, que se basa en XML, permite a las interfaces de empresa pasar solicitudes de servicio y a la empresa receptora aprovisionar el acceso a estos servicios. Esta interoperabilidad es posible porque las empresas utilizan XML, que es un conjunto de reglas para codificar electrónicamente documentos y comunicación basada en web. XML también se utiliza para codificar estructuras de datos arbitrarias, como en los servicios web. Permite a grupos o empresas crear formatos de información, como SPML, que permiten un medio coherente de compartir datos.

☒ **C** es incorrecto porque el lenguaje de marcado generalizado estándar (SGML) fue uno de los primeros lenguajes de marcado desarrollados. No proporciona el acceso de los usuarios ni la funcionalidad de aprovisionamiento. SGML era un estándar que define etiquetas de marcado generalizadas para documentos. Es un sucesor del lenguaje de marcado generalizado y llegó mucho antes que XML o SPML.

☒ **D** es incorrecto porque el lenguaje de marcado de hipertexto (HTML) se desarrolló para anotar páginas web. HTML es un precursor de XML y SGML. HTML proporciona un medio para denotando semántica estructural para el texto y otros elementos que se encuentran en una página web. Se puede utilizar para incrustar imágenes y objetos y crear formularios interactivos. Sin embargo, no puede permitir que las interfaces de empresa pasen las solicitudes de servicio y la empresa receptora aprovisione el acceso a estos servicios.

15. Existen varios tipos diferentes de protocolos de control de acceso centralizados. ¿Cuál de los siguientes se ilustra en el gráfico que sigue?



R. diámetro

B. perro guardián

C. radio

D. TACACS+

☑ **R.** El diámetro es un protocolo de autenticación, autorización y auditoría (AAA) que proporciona el mismo tipo de funcionalidad que radius y TACACS+, pero también proporciona más flexibilidad y capacidades para satisfacer las nuevas demandas de las redes complejas y diversas de hoy en día. En un momento dado, toda la comunicación remota tuvo lugar a través de conexiones de protocolo punto a punto (PPP) y protocolo de Internet de línea serie (SLIP), y los usuarios se autenticaron a través del Protocolo de autenticación de contraseña (PAP) o el Protocolo de autenticación de protocolo de autenticación de protocolo de protocolo de apretón de manos de desafío (CHAP). La tecnología se ha vuelto mucho más complicada y hay más dispositivos y protocolos para elegir que nunca. El protocolo Diameter permite que los dispositivos inalámbricos, los teléfonos inteligentes y otros dispositivos puedan autenticarse en redes utilizando protocolos de itinerancia, IP móvil, Ethernet a través de PPP, voz sobre IP (VoIP) y otros.

☒ **B** es incorrecto porque los temporizadores de vigilancia se utilizan comúnmente para detectar fallas de software, como un proceso que termina anormalmente o cuelga. La funcionalidad del guardián envía un tipo de paquete "latido" para determinar si un servicio está respondiendo. Si no es así, el proceso se puede terminar o restablecer. Estos paquetes ayudan a prevenir contra interbloqueos de software, bucles infinitos y problemas de priorización de procesos. Esta funcionalidad se puede utilizar en los protocolos AAA para determinar si los paquetes necesitan ser re-enviados y si las conexiones que

experimentan los problemas deben ser cerradas y reabiertas, pero no es un protocolo de control de acceso sí mismo.

☒ **C** es incorrecto porque el servicio de usuario de acceso telefónico de autenticación remota (RADIUS) es un protocolo de red y proporciona autenticación, autorización y auditoría cliente/servidor para los usuarios remotos. Una red puede tener servidores de acceso, DSL, ISDN o una línea T1 dedicada a que los usuarios remotos se comuniquen. El servidor de acceso solicita las credenciales de inicio de sesión del usuario remoto y las pasa de nuevo a un servidor RADIUS, que alberga los nombres de usuario y los valores de contraseña. El usuario remoto es un cliente para el servidor de acceso, y el servidor de acceso es un cliente para el servidor radius.

☒ **D** es incorrecto porque el sistema de control de acceso del controlador de acceso del terminal access plus (TACACS+) proporciona básicamente la misma funcionalidad que radius. El protocolo RADIUS combina la funcionalidad de autenticación y autorización. TACACS+ utiliza una verdadera arquitectura AAA, que separa cada función hacia fuera. Esto proporciona a un administrador de red más flexibilidad en la forma en que se autentican los usuarios remotos. Ni TACACS+ ni RADIUS pueden llevar a cabo estos servicios para los dispositivos que necesitan comunicarse sobre VoIP, IP móvil u otros tipos similares de protocolos.

16. Se utiliza una matriz de control de acceso en muchos sistemas operativos y aplicaciones para controlar el acceso entre sujetos y objetos. ¿Cuál es la columna de este tipo de matriz a la que se hace referencia?

Access Control Matrix

Subject	File1	File2	File3	File4
Larry	Read	Read, Write	Read	Read, Write
Curly	Full Control	No Access	Full Control	Read
Mo	Read, Write	Full Control	Read	Full Control
Bob	Full Control	Full Control	No Access	No Access

R. Tabla de capacidades

B. Interfaz restringida

C. Valor basado en roles

D. Acl

☑ **D.** Las listas de control de acceso (ACL) asignan valores de la matriz de control de acceso al objeto. Mientras que una capacidad corresponde a una fila en la matriz de control de acceso, la ACL corresponde a una columna de la matriz. Las ACL se utilizan en varios sistemas operativos, aplicaciones y configuraciones de enrutadores. Son listas de sujetos que están autorizados para

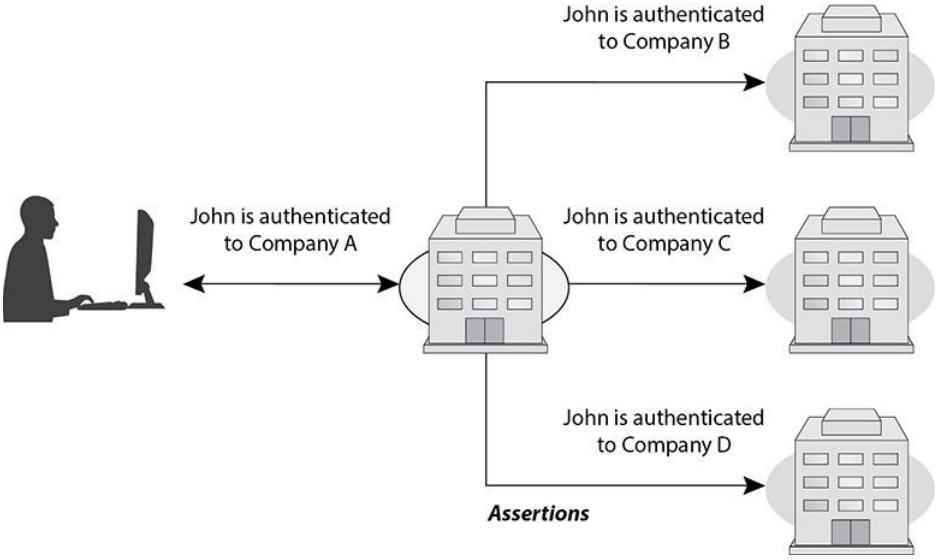
acceder a objetos específicos, y definen qué nivel de autorización se concede. La autorización se puede especificar a un individuo o grupo. Por lo tanto, la ACL está enlazada a un objeto e indica qué sujetos pueden tener acceso a él, y una tabla de capacidad está enlazada a un asunto e indica a qué objetos puede tener acceso ese sujeto.

A es incorrecto porque una capacidad puede estar en forma de token, vale o clave y es una fila dentro de una matriz de control de acceso. Cuando un sujeto presenta un componente de capacidad, el sistema operativo (o aplicación) revisará los derechos de acceso y las operaciones descritas en el componente de capacidad y permitirá que el sujeto lleve a cabo solo esas funciones. Un componente de capacidad es una estructura de datos que contiene un identificador de objeto único y los derechos de acceso que el sujeto tiene a ese objeto. El objeto puede ser un archivo, matriz, segmento de memoria o puerto. Cada usuario, proceso y aplicación en un sistema de capacidades tiene una lista de capacidades que puede llevar a cabo.

B es incorrecto porque las interfaces de usuario restringidas restringen las capacidades de acceso de los usuarios al no permitirles solicitar ciertas funciones o información o tener acceso a recursos específicos del sistema. Existen tres tipos principales de interfaces restringidas: menús y shells, vistas de base de datos e interfaces físicamente restringidas. Cuando se utilizan restricciones de menú y shell, las opciones que se dan a los usuarios son los comandos que pueden ejecutar. Por ejemplo, si un administrador desea que los usuarios puedan ejecutar un solo programa, ese programa sería la única opción disponible en el menú. Si se utilizaran vaciados restringidos, el shell contendría solo los comandos que el administrador desea que los usuarios puedan ejecutar.

C es incorrecto porque un modelo de control de acceso basado en roles (RBAC), también denominado control de acceso no discretionario, utiliza un conjunto administrado de controles administrados de forma centralizada para determinar cómo interactúan los sujetos y objetos. Este tipo de modelo permite que el acceso a los recursos se base en el rol que el usuario mantiene dentro de la empresa. Se conoce como nodiscretionario porque la asignación de un usuario a un rol se impone inevitablemente. Esto significa que si se le asigna sólo al rol de contratista en una empresa, no hay nada que pueda hacer al respecto. No tiene la discreción de determinar qué rol se le asignará.

17. ¿Qué tecnología dentro de la gestión de la identidad se ilustra en el gráfico que sigue?



A. Aprovisionamiento de usuarios

B. Identidad federada

C. Directorios

D. Gestión del acceso web

☑ **B.** Una identidad federada es una identidad portátil y sus derechos asociados que se pueden usar a través de los límites empresariales. Permite autenticar a un usuario en varios sistemas y empresas de TI. La federación de identidades se basa en vincular las identidades distintas de un usuario en dos o más ubicaciones sin necesidad de sincronizar o consolidar la información del directorio. La identidad federada ofrece a las empresas y a los consumidores una forma más cómoda de acceder a los recursos distribuidos y es un componente clave del comercio electrónico.

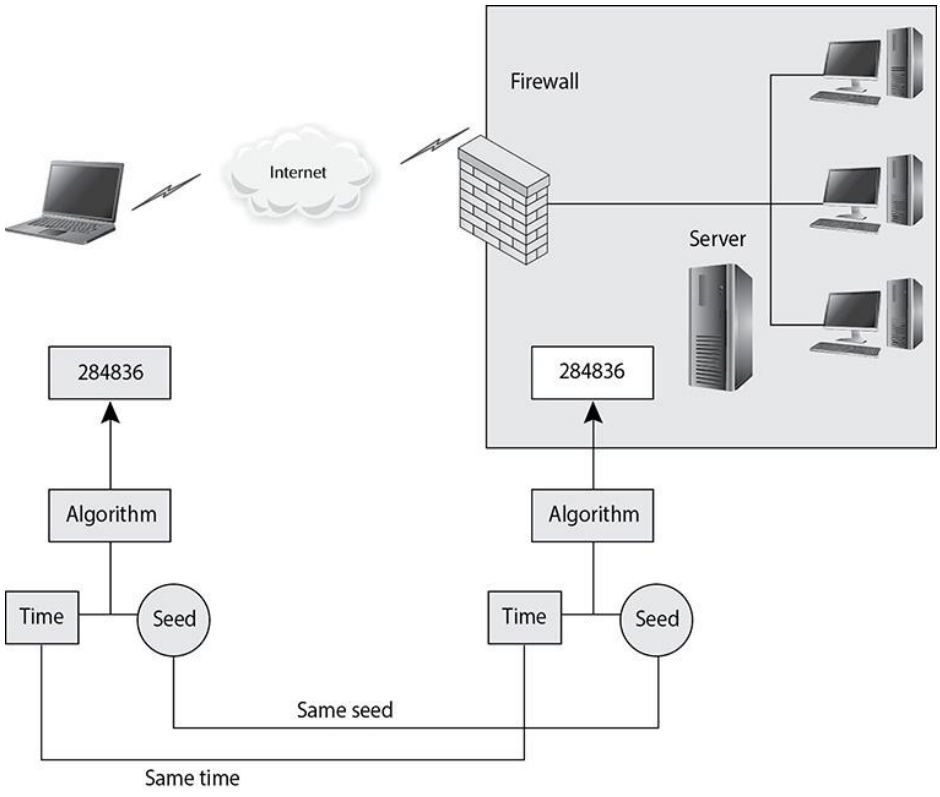
☒ **A** es incorrecto porque el aprovisionamiento de usuarios hace referencia a la creación, mantenimiento y desactivación de objetos y atributos de usuario tal como existen en uno o varios sistemas, directorios o aplicaciones en respuesta a procesos empresariales. El software de aprovisionamiento de usuarios puede incluir uno o varios de los siguientes componentes: propagación de cambios, flujo de trabajo de autoservicio, administración consolidada de usuarios, administración de usuarios delegada y control de cambios federado. Los objetos de usuario pueden representar empleados, contratistas, proveedores, socios, clientes u otros destinatarios de un servicio. Los servicios pueden incluir correo electrónico, acceso a una base de datos, acceso a un servidor de archivos o mainframe, etc. El aprovisionamiento de usuarios puede ser una función con identificación de federación, pero esto no es lo que ilustra el gráfico.

☒ **C** es incorrecto porque si bien la mayoría de las empresas tienen algún tipo de directorio que contiene información relativa a los recursos de red y usuarios de la empresa, esos directorios no suelen distribuirse entre diferentes empresas. La mayoría de los directorios siguen un formato jerárquico de base de datos,

basado en el estándar X.500, y un tipo de protocolo, como en el Protocolo ligero de acceso a directorios (LDAP), que permite a los sujetos y aplicaciones interactuar con el directorio. Las aplicaciones pueden solicitar información sobre un usuario determinado realizando una solicitud LDAP al directorio y los usuarios pueden solicitar información sobre un recurso específico mediante una solicitud similar. Aunque los directorios pueden funcionar dentro de un marco federado, esto no es lo que muestra el gráfico.

D es incorrecto porque el software de administración de acceso web (WAM) controla a qué pueden acceder los usuarios cuando utilizan un explorador web para interactuar con activos empresariales basados en web. Este tipo de tecnología se está volviendo continuamente más robusta y experimentando un mayor despliegue. Esto se debe al mayor uso del comercio electrónico, la banca en línea, la prestación de contenidos, los servicios web y mucho más. Más complejidad viene con todas las diferentes maneras en que un usuario puede autenticar (contraseña, certificado digital, token y otros), los recursos y servicios que pueden estar disponibles para el usuario (fondos de transferencia, producto de compra, perfil de actualización, etc.) y los componentes de infraestructura necesarios. La infraestructura normalmente se compone de una granja de servidores web (muchos servidores), un directorio que contiene las cuentas y atributos de los usuarios, una base de datos, un par de firewalls y algunos enrutadores, todos distribuidos en una arquitectura en niveles.

18. Hay diferentes maneras en que tecnologías específicas pueden crear contraseñas únicas con fines de autenticación. ¿Qué tipo de tecnología se ilustra en el gráfico que sigue?



R. Token sincrónico de contador

B. Token asincrónico

C. Token obligatorio

D. Token sincrónico

☑ **D.** Un dispositivo de token sincrónico se sincroniza con el servicio de autenticación mediante el tiempo o un contador como la parte principal del proceso de autenticación. Si la sincronización se basa en el tiempo, como se muestra en este gráfico, el dispositivo token y el servicio de autenticación deben contener la misma hora dentro de sus relojes internos. El valor de tiempo en el dispositivo token y una clave secreta se utilizan para crear la contraseña única, que se muestra al usuario. El usuario escribe este valor y un identificador de usuario en el equipo, que, a continuación, los pasa al servidor que ejecuta el servicio de autenticación. El servicio de autenticación descifra este valor y lo compara con el valor que esperaba. Si los dos coinciden, se autentica al usuario y se le permite usar el equipo y los recursos.

☒ **A** es incorrecto porque si el dispositivo token y el servicio de autenticación usan la contra-sincronización, no se basa en el tiempo como se muestra en el gráfico. Al usar un dispositivo de token de contra-sincronización, el usuario tendrá que iniciar la creación de la contraseña única pulsando un botón en el dispositivo de token. Esto hace que el dispositivo token y el servicio de autenticación avancen al siguiente valor de autenticación. Este valor y un secreto base se han hash y se muestran al usuario. El usuario escribe este valor resultante junto con un ID de usuario que se va a autenticar. En la sincronización basada en tiempo o en contra, el dispositivo de token y el servicio de autenticación deben compartir la misma clave base secreta utilizada para el cifrado y el descifrado.

☒ **B** es incorrecto porque un dispositivo token que usa un método de generación de tokens asincrónico emplea un esquema de desafío/respuesta para autenticar al usuario. Esta tecnología no utiliza la sincronización, sino que utiliza pasos discretos en su proceso de autenticación. En esta situación, el servidor de autenticación envía al usuario un desafío, un valor aleatorio también denominado nonce. El usuario escribe este valor aleatorio en el dispositivo de token, que lo cifra y devuelve un valor que el usuario utiliza como contraseña única. El usuario envía este valor, junto con un nombre de usuario, al servidor de autenticación. Si el servidor de autenticación puede descifrar el valor y es el mismo valor de desafío enviado anteriormente, se autentica al usuario.

☒ **C** es incorrecto porque no existe tal cosa como un token obligatorio. Esta es una respuesta distraída.

19. ¿Cuál de las siguientes características describe mejor cómo SAML, SOAP y HTTP suelen trabajar juntos en un entorno que proporciona servicios web?

R. Los atributos de seguridad se colocan en formato SAML. La solicitud de servicio web y los datos de autenticación se cifran en un mensaje SOAP. El

mensaje se transmite en una conexión HTTP.

B. Los atributos de seguridad se colocan en formato SAML. La solicitud de servicio web y los datos de autenticación se encapsulan en un mensaje SOAP. El mensaje se transmite en una conexión HTTP a través de TLS.

C. Los datos de autenticación se colocan en formato SAML. Los datos de solicitud y autenticación del servicio web se encapsulan en un mensaje SOAP. El mensaje se transmite en una conexión HTTP.

D. Los datos de autenticación se colocan en formato SAML. La solicitud HTTP y los datos de autenticación se encapsulan en un mensaje SOAP. El mensaje se transmite en una conexión HTTP.

☑ **C.** Por ejemplo, al iniciar sesión en el portal de su empresa y hacer doble clic en un vínculo (por ejemplo, Salesforce), el portal de su empresa llevará esta solicitud y sus datos de autenticación y los empaquetará en un formato de lenguaje de marcado de aserción de seguridad (SAML) y encapsulará esos datos en un mensaje soap (Protocolo simple de acceso a objetos). Este mensaje se transmitiría a través de una conexión HTTP al sitio del proveedor de Salesforce y, una vez autenticado, puede interactuar con el software del proveedor. SAML empaqueta datos de autenticación, paquetes SOAP para arriba solicitudes de servicio web y datos SAML, y la solicitud se transmite a través de una conexión HTTP.

☒ **A** es incorrecto porque SAML es un estándar abierto basado en XML para intercambiar datos de autenticación y autorización entre dominios de seguridad, es decir, entre un proveedor de identidades (un productor de aserciones) y un proveedor de servicios (un consumidor de aserciones). Por lo tanto, los datos de autenticación se usan con SAML, no con atributos de seguridad. Además, SOAP encapsula los mensajes, no los cifra.

☒ **B** es incorrecto porque los datos de autenticación se utilizan con SAML y la transmisión no tiene lugar sobre una conexión TLS de forma predeterminada. La transmisión puede tener lugar a través de SSL o TLS, pero esto no fue lo que se describió en la pregunta.

☒ **D** es incorrecto porque SOAP encapsula las solicitudes y los datos del servicio web, no HTTP. Después de que SOAP encapsula los datos del servicio web, se encapsula con HTTP con fines de transmisión.

20. Jill está estableciendo un programa de ventas en toda la empresa que requerirá diferentes grupos de usuarios con diferentes privilegios para acceder a la información en una base de datos centralizada. ¿Cómo debe proteger el administrador de seguridad la base de datos?

R. Aumente los controles de seguridad de la base de datos y proporcione más granularidad.

B. Implemente controles de acceso que muestren los permisos de cada usuario cada vez que tengan acceso a la base de datos.

C. Cambie la etiqueta de clasificación de la base de datos a un estado de seguridad más alto.

D. Disminuya la seguridad para que todos los usuarios puedan acceder a la información según sea necesario.

☑ **R.** El mejor enfoque para proteger la base de datos en esta situación sería aumentar los controles y asignar permisos muy granulares. Estas medidas garantizarían que los usuarios no puedan abusar de sus privilegios y que se mantenga la confidencialidad de la información. La granularidad de los permisos proporciona a los administradores de red y a los profesionales de seguridad un control adicional sobre los recursos que se encargan de proteger, y un excelente nivel de detalle les permite dar a las personas el nivel preciso de acceso que necesitan.

☒ **B** es incorrecto porque la implementación de controles de acceso que muestran los permisos de cada usuario cada vez que acceden a la base de datos es un ejemplo de un control. No es la forma general de tratar el acceso de los usuarios a una base de datos completa de información. Esto puede ser un ejemplo de aumento de los controles de seguridad de la base de datos, pero es sólo un ejemplo, y se necesitaría más.

☒ **C** es incorrecto porque el nivel de clasificación de la información en la base de datos se determinó previamente en función de sus niveles de confidencialidad, integridad y disponibilidad. Estos niveles no cambian simplemente porque más usuarios necesitan acceso a los datos. Por lo tanto, nunca aumentaría ni disminuiría el nivel de clasificación de la información cuando más usuarios o grupos necesitan acceder a esa información. Aumentar el nivel de clasificación sólo significaría que un subconjunto más pequeño de usuarios podría tener acceso a la base de datos.

☒ **D** es incorrecto porque pone los datos en riesgo. Si se reduce la seguridad para que todos los usuarios puedan acceder a ella según sea necesario, los usuarios con privilegios más bajos podrán acceder a datos de niveles de clasificación más altos. Una menor seguridad también facilita que los intrusos entren en la base de datos. Como se indica en la respuesta C, un nivel de clasificación no se cambia solo porque el número de usuarios que necesitan acceder a los datos aumenta o disminuye.

21. Bethany está trabajando en un sistema de control de acceso obligatorio (MAC). Ella ha estado trabajando en un archivo que fue clasificado como Secreto. Ya no puede acceder a este archivo porque ha sido reclasificado como Top Secret. Ella deduce que el proyecto en el que estaba trabajando acaba de aumentar en confidencialidad y ahora sabe más sobre este proyecto de lo que su

autorización y necesidad de saber permite. ¿Cuál de los siguientes se refiere a un concepto que intenta evitar que se produzca este tipo de escenario?

R. Canal de almacenamiento encubierto

B. Ataque de inferencia

C. Noninterference

D. agregación

☑ **C.** Las propiedades de seguridad multinivel se pueden expresar de muchas maneras, siendo una no interferencia. Este concepto se implementa para garantizar que cualquier acción que tenga lugar en un nivel de seguridad más alto no afecte ni interfiera con las acciones que tienen lugar en un nivel inferior. Por lo tanto, si una entidad en un nivel de seguridad superior realiza una acción, no puede cambiar el estado de la entidad en el nivel inferior. Si una entidad de nivel inferior tuviera conocimiento de una determinada actividad que realizaba una entidad de un nivel superior y el estado del sistema cambiara para esta entidad de nivel inferior, la entidad podría deducir demasiada información sobre las actividades del estado superior, lo que a su vez es una forma de filtrar información.

☒ **A** es incorrecto porque un canal encubierto permite la capacidad de compartir información entre procesos que no estaban destinados a comunicarse. La nointerferencia es un modelo destinado a prevenir canales encubiertos junto con otras formas maliciosas de comunicarse. El modelo examina los recursos compartidos que usarán los diferentes usuarios de un sistema e intenta identificar cómo se puede pasar la información de un proceso que funciona en una autorización de seguridad más alta a un proceso que funciona con una autorización de seguridad más baja. Si dos usuarios están trabajando en el mismo sistema al mismo tiempo, lo más probable es que tengan que compartir algún tipo de recursos. Por lo tanto, el modelo se compone de reglas para garantizar que el Usuario A no pueda llevar a cabo ninguna actividad que pueda permitir al Usuario B inferir información que no tenga la autorización para conocer.

☒ **B** es incorrecto porque un ataque de inferencia se refiere a la capacidad de Bethany para inferir que el proyecto en el que estaba trabajando ahora es Top Secret y ha aumentado en importancia y secretismo. La pregunta es preguntar por el concepto que ayuda a prevenir un ataque de inferencia. Un ataque de inferencia ocurre cuando alguien tiene acceso a algún tipo de información y puede inferir (o adivinar) algo que no tiene el nivel de autorización o la autoridad para saber. Por ejemplo, supongamos que Tom está trabajando en un archivo que contiene información sobre los suministros que se envían a Rusia. Cierra fuera de ese archivo y una hora más tarde intenta abrir el mismo archivo. Durante este tiempo, la clasificación del archivo se ha elevado a Top Secret, por lo que cuando Tom intenta acceder a él, se le niega. Tom puede inferir que algún

tipo de misión top secret se está preparando para tener lugar con Rusia. Él no tiene autorización para saber esto; por lo tanto, sería un ataque de inferencia o "información de filtración"."

☒ **D** es incorrecta porque la agregación es el acto de combinar información de orígenes independientes. La combinación de los datos constituye nueva información, a la que el sujeto no tiene los derechos de acceso necesarios. La información combinada puede tener una sensibilidad mayor que la de las partes individuales. La agregación se produce cuando un usuario no tiene la autorización o el permiso para acceder a información específica, pero tiene permiso para acceder a los componentes de esta información. A continuación, puede averiguar el resto y obtener información restringida.

22. Se pueden realizar varios ataques contra tarjetas inteligentes. Side-channel es una clase de ataques que no intenta comprometer un defecto o debilidad. ¿Cuál de los siguientes no es un ataque de canal lateral?

R. Análisis diferencial de potencia

B. Análisis de microprobing

C. Análisis de tiempos

D. Análisis electromagnético

☑ **B.** Un ataque no invasivo es aquel en el que el atacante observa cómo funciona algo y cómo reacciona en diferentes situaciones en lugar de tratar de "invadirlo" con medidas más intrusivas. Ejemplos de ataques de canal lateral son generación de fallas, análisis de potencia diferencial, análisis electromagnético, sincronización y ataques de software. Este tipo de ataques se utilizan para descubrir información confidencial sobre cómo funciona un componente sin intentar comprometer ningún tipo de defecto o debilidad. Un ataque con tarjeta inteligente más intrusivo es la microprobing. La microprobing utiliza agujas y vibraciones ultrasónicas para eliminar el material protector exterior en los circuitos de la tarjeta. Una vez completado esto, se puede acceder y manipular los datos pulsando directamente en los chips rom de la tarjeta.

☒ **A** es incorrecto porque el análisis de potencia diferencial (DPA) es un ataque no invasivo. DPA implica examinar las emisiones de energía liberadas durante el procesamiento. Mediante el análisis estadístico de datos de varias operaciones criptográficas, por ejemplo, un atacante puede determinar los valores intermedios dentro de cálculos criptográficos. Esto se puede hacer sin ningún conocimiento de cómo se diseña el dispositivo de destino. Por lo tanto, un atacante puede extraer claves criptográficas u otra información confidencial de la tarjeta.

☒ **C** es incorrecto porque un análisis de tiempo es un ataque no invasivo. Implica calcular el tiempo que tarda una función específica en completar su tarea. Los ataques de análisis de tiempo se basan en medir cuánto tiempo tardan

varios cálculos en realizarse. Por ejemplo, observando cuánto tiempo tarda una tarjeta inteligente en transferir información clave, a veces es posible determinar cuánto tiempo dura la clave en este caso.

☒ **D** es incorrecto porque el análisis electromagnético es un ataque no invasivo que implica examinar las frecuencias emitidas. Todas las corrientes eléctricas emiten emanaciones electromagnéticas. En las tarjetas inteligentes, el consumo de energía y, por lo tanto, el campo de emanación electromagnética varían a medida que se procesan los datos. Un análisis electromagnético intenta hacer correlaciones entre los datos y las emanaciones electromagnéticas en un esfuerzo por descubrir claves criptográficas u otra información sensible en la tarjeta inteligente.

23. Emily está escuchando el tráfico de red y capturando contraseñas mientras se envían al servidor de autenticación. Ella planea usar las contraseñas como parte de un ataque futuro. ¿Qué tipo de ataque es éste?

R. Ataque con fuerza bruta

B. ataque de diccionario

C. Ataque a la ingeniería social

D. Ataque de repetición

☑ **D.** Un ataque de reproducción se produce cuando un intruso obtiene y almacena información y más tarde la usa para obtener acceso no autorizado. En este caso, Emily está utilizando una técnica llamada monitoreo electrónico (sniffing) para obtener contraseñas que se envían a través del cable a un servidor de autenticación. Más adelante puede usar las contraseñas para obtener acceso a los recursos de red. Incluso si las contraseñas están cifradas, la retransmisión de credenciales válidas puede ser suficiente para obtener acceso.

☒ **A** es incorrecto porque un ataque de fuerza bruta se realiza con herramientas que recorren muchas combinaciones de caracteres, números y símbolos posibles para descubrir una contraseña. Una forma de evitar un ataque de fuerza bruta exitoso es restringir el número de intentos de inicio de sesión que se pueden realizar en un sistema. Un administrador puede establecer parámetros operativos que permiten aceptar un cierto número de intentos de inicio de sesión fallidos antes de que un usuario se bloquee; este es un tipo de nivel de recorte.

☒ **B** es incorrecto porque un ataque de diccionario implica la comparación automatizada de la contraseña del usuario con archivos de miles de palabras hasta que se encuentra una coincidencia. Los ataques de diccionario se realizan correctamente porque los usuarios tienden a elegir contraseñas que son cortas, son palabras simples o son variaciones predecibles de las palabras del diccionario.

☒ **C** es incorrecto porque en un ataque de ingeniería social el atacante convence falsamente a un individuo de que tiene la autorización necesaria para acceder a recursos específicos. La ingeniería social se lleva a cabo contra las personas directamente y no se considera necesariamente un ataque técnico. La mejor defensa contra la ingeniería social es la educación de los usuarios. Los requisitos de contraseñas, la protección y la generación deben abordarse en los programas de concienciación sobre la seguridad para que los usuarios entiendan por qué deben proteger sus contraseñas y cómo se pueden robar contraseñas.

24. ¿Cuál de las siguientes maneras es la mejor manera de reducir los ataques de fuerza bruta que permiten a los intrusos descubrir las contraseñas de los usuarios?

R. Aumente el nivel de recorte.

B. Bloquee una cuenta durante un cierto período de tiempo después de alcanzar el nivel de recorte.

C. Una vez alcanzado un umbral de intentos de inicio de sesión fallidos, el administrador debe bloquear físicamente la cuenta.

D. Elija un algoritmo más débil que cifre el archivo de contraseña.

☑ **B.** Un ataque de fuerza bruta es un ataque que intenta continuamente diferentes entradas para lograr un objetivo predefinido, que luego se puede utilizar para obtener credenciales para el acceso no autorizado. Un ataque de fuerza bruta para descubrir contraseñas significa que el intruso está intentando todas las secuencias posibles de caracteres para descubrir la contraseña correcta. Si la cuenta se deshabilitara (o bloqueara) después de que se produjera este tipo de intento de ataque, esto resultaría ser una buena contramedida.

☒ **A** es incorrecto porque los niveles de recorte deben implementarse para establecer una línea base de la actividad del usuario y errores aceptables. Una entidad que intenta iniciar sesión en una cuenta debe bloquearse una vez que se cumpla el nivel de recorte. Un nivel de recorte más alto ofrece a un atacante más intentos entre alertas o bloqueo. Disminuir el nivel de recorte sería una buena contramedida.

☒ **C** es incorrecto porque no es práctico tener un administrador bloquear cuentas físicamente. Este tipo de actividad se puede cuidar fácilmente a través de mecanismos de software automatizados. Las cuentas deben bloquearse automáticamente durante un cierto período de tiempo después de que se haya alcanzado un umbral de intentos de inicio de sesión fallidos.

☒ **D** es incorrecto porque el uso de un algoritmo más débil que cifra las contraseñas y / o archivos de contraseña aumentaría la probabilidad de éxito de un ataque de fuerza bruta.

25. Phishing y pharming son similares. ¿Cuál de los siguientes describe correctamente la diferencia entre phishing y pharming?

R. La información personal se recopila de las víctimas a través de sitios web de aspecto legítimo en ataques de phishing, mientras que la información personal se recopila de las víctimas a través de correo electrónico en ataques de faring.

B. Los ataques de phishing apuntan a los destinatarios de correo electrónico a un formulario donde las víctimas introducen información personal, mientras que los ataques de pharming utilizan formularios emergentes en sitios web legítimos para recopilar información personal de las víctimas.

C. Las víctimas son señaladas a un sitio web falso con un nombre de dominio que se parece al nombre de dominio de un sitio legítimo en un ataque de phishing, mientras que las víctimas son dirigidas a un sitio web falso como resultado de un nombre de dominio legítimo que se traduce incorrectamente por el servidor DNS en un ataque faring.

D. El phishing es un ataque técnico, mientras que el pharming es un tipo de ingeniería social.

☑ **C.** Tanto en phishing como en pharming, los atacantes pueden crear sitios web que se parecen mucho a sitios legítimos en un esfuerzo por recopilar información personal de las víctimas. En un ataque de phishing, los atacantes pueden proporcionar direcciones URL con nombres de dominio que se parecen mucho a la dirección del sitio legítimo. Por ejemplo, www.amazon.com (http://www.amazon.com) podría volverse www.amzaon.com. (http://www.amzaon.com) O utilice un símbolo @especialmente colocado. Por ejemplo, www.msn.com@notmsn.com llevaría a la víctima al sitio web notmsn.com (http://notmsn.com) y proporcionaría el nombre de usuario de www.msn.com (http://www.msn.com) a este sitio web. El nombre de usuario www.msn.com (http://www.msn.com) no sería un nombre de usuario válido para notmsn.com, (http://notmsn.com)por lo que a la víctima sólo se le mostraría la página de inicio de notmsn.com (http://notmsn.com). Ahora, notmsn.com (http://notmsn.com) es un sitio nefasto creado para verse y sentirse como www.msn.com. (http://www.msn.com) La víctima siente que está en el sitio legítimo e inicia sesión con sus credenciales. En un ataque faring, a la víctima se le da un nombre de dominio legítimo, pero ese nombre de dominio se redirige al sitio web del atacante como resultado de la intoxicación por DNS. Cuando el servidor DNS es envenenado para llevar a cabo un ataque faring, los registros se han cambiado de modo que en lugar de enviar la dirección IP correcta para www.logicalsecurity.com, (http://www.logicalsecurity.com)envía la dirección IP de un sitio web de aspecto legítimo, pero falso, creado por el atacante.

☒ **A** es incorrecto porque un ataque faring no implica comúnmente la recopilación de información a través de correo electrónico. De hecho, el beneficio de un ataque faring al atacante es que puede afectar a una gran cantidad de víctimas sin la necesidad de enviar correos electrónicos. Al igual que

un ataque de phishing, un ataque de faring implica un sitio web aparentemente legítimo, pero falso. Las víctimas son dirigidas al sitio web falso porque el nombre de host se resuelve incorrectamente como resultado de la intoxicación por DNS.

☒ **B** es incorrecto porque ambas descripciones son verdaderas de los ataques de phishing. Los ataques faring no utilizan formularios emergentes. Sin embargo, algunos ataques de phishing utilizan formularios emergentes cuando una víctima está en un sitio web legítimo. Así que si estuvieras en el sitio web real de tu banco y apareciera una ventana emergente pidiéndote información sensible, esto probablemente no te preocuparía, ya que te estabas comunicando con el sitio web de tu banco real. Puede creer que la ventana provendó del servidor web de su banco, por lo que la rellena según las instrucciones. Desafortunadamente, esta ventana emergente podría ser de otra fuente por completo, y sus datos podrían ser colocados justo en las manos del atacante, no en las de su banco.

☒ **D** es incorrecto porque ambos ataques son formas técnicas de llevar a cabo la ingeniería social. El phishing es un tipo de ingeniería social con el objetivo de obtener información personal, credenciales, números de tarjetas de crédito o datos financieros. Los atacantes se atraen, o pescan, para obtener datos confidenciales a través de varios métodos diferentes, como el correo electrónico y los formularios emergentes. El faring implica envenenamiento por DNS. El atacante modifica los registros de un servidor DNS para que resuelva un nombre de host en una dirección IP incorrecta. El sistema de la víctima envía una solicitud a un servidor DNS envenenado, que señala a la víctima a un sitio web diferente. Este sitio web diferente se ve y se siente como el sitio web solicitado, por lo que el usuario introduce su nombre de usuario y contraseña e incluso puede ser presentado con páginas web que parecen legítimas.

26. Existen varios tipos de sistemas de detección de intrusiones (IDS). ¿Qué tipo de IDS crea un perfil de las actividades normales de un entorno y asigna una puntuación de anomalía a los paquetes basados en el perfil?

R. Basado en el Estado

B. Anomalía estadística

C. Sistema de detección de uso indebido

D. Firma de protocolo basada en

☑ **B.** Un IDS basado en anomalías estadísticas es un sistema basado en el comportamiento. Los productos IDS basados en el comportamiento no usan firmas predefinidas, sino que se colocan en modo de aprendizaje para crear un perfil de las actividades "normales" de un entorno. Este perfil se basa en el muestreo continuo de las actividades del entorno. Cuanto más tiempo se ponga el IDS en un modo de aprendizaje, en la mayoría de los casos, más preciso será un perfil que creará y mejor protección proporcionará. Después de crear este perfil, se comparan todo el tráfico y las actividades futuras. Con el uso de

algoritmos estadísticos complejos, el IDS busca anomalías en el tráfico de red o la actividad del usuario. Cada paquete recibe una puntuación de anomalía, que indica su grado de irregularidad. Si la puntuación es superior al umbral establecido de comportamiento "normal", se llevará a cabo la acción preconfigurada.

☒ **A** es incorrecto porque un IDS basado en estado tiene reglas que describen qué secuencias de transición de estado deben sonar una alarma. El estado inicial es el estado antes de la ejecución de un ataque y el estado comprometido es el estado después de una penetración correcta. La actividad que tiene lugar entre el estado inicial y comprometido es lo que busca el IDS basado en estado y envía una alerta si alguna de las secuencias de transición de estado coincide con sus reglas preconfiguradas.

☒ **C** es incorrecto porque un sistema de detección de uso indebido es simplemente otro nombre para un IDS basado en firmas, que compara la actividad de la red o del sistema con las firmas o modelos de cómo se llevan a cabo los ataques. Cualquier acción que no se reconozca como un ataque se considera aceptable. Los IDS basados en firmas son los productos IDS más populares hoy en día, y su eficacia depende de actualizar regularmente el software con nuevas firmas, como con el software antivirus. Este tipo de IDS es débil contra nuevos tipos de ataques porque solo puede reconocer aquellos que se han identificado previamente y han tenido firmas escritas para ellos.

☒ **D** es incorrecto porque un IDS basado en firma de protocolo no es un IDS formal. Esta es una respuesta distraída.

27. Un IDS basado en reglas adopta un enfoque diferente de un sistema basado en firmas o anomalías. ¿Cuál de los siguientes es característico de un IDS basado en reglas?

R. Utiliza la programación IF/THEN dentro de sistemas expertos

B. Identifica los protocolos utilizados fuera de sus límites comunes

C. Compara patrones con varias actividades a la vez

D. Puede detectar nuevos ataques

☑ **R.** La detección de intrusiones basada en reglas se asocia comúnmente con el uso de un sistema experto. Un sistema experto se compone de una base de conocimiento, un motor de inferencia y programación basada en reglas. El conocimiento se representa como reglas, y los datos a analizar se conocen como hechos. El conocimiento del sistema está escrito en programación basada en reglas (acción IF situation THEN). Estas reglas se aplican a los hechos, los datos que provienen de un sensor o un sistema que está siendo monitoreado. Por ejemplo, un IDS extrae datos del registro de auditoría de un sistema y los almacena temporalmente en su base de datos de hechos. A continuación, las reglas preconfiguradas se aplican a estos datos para indicar si se está

produciendo algo sospechoso. En nuestro escenario, la regla indica "SI *un usuario raíz crea File1* Y crea *File2* DE TAL manera que *están en el mismo directorio* ENTONCES hay una llamada a la alerta de *envío*de *Administrative Tool* TRIGGER ." Esta regla se ha definido de tal manera que si un usuario raíz crea dos archivos en el mismo directorio y, a continuación, realiza una llamada a una herramienta administrativa específica, se debe enviar una alerta.

B es incorrecto porque un IDS basado en anomalías de protocolo identifica los protocolos utilizados fuera de sus límites comunes. El IDS tiene conocimiento específico de cada protocolo que supervisará. Una anomalía de protocolo pertenece al formato y comportamiento de un protocolo. Si un protocolo tiene un formato diferente o está demostrando un comportamiento anormal, el IDS activa una alarma.

C es incorrecto porque un IDS de coincidencia con estado compara patrones con varias actividades a la vez. Es un tipo de IDS basado en firmas, lo que significa que hace coincidencia de patrones, similar al software antivirus. Estado es una instantánea de los valores de un sistema operativo en ubicaciones de memoria volátiles, semipermanentes y permanentes. En un IDS basado en estado, el estado inicial es el estado anterior a la ejecución de un ataque y el estado comprometido es el estado después de la penetración correcta. El IDS tiene reglas que describen qué secuencias de transición de estado deben sonar una alarma.

D es incorrecto porque un IDS basado en reglas no puede detectar nuevos ataques. Un IDS basado en anomalías puede detectar nuevos ataques porque no se basa en reglas o firmas predeterminadas, que solo están disponibles después de que los investigadores de seguridad hayan tenido tiempo de estudiar un ataque. En su lugar, un IDS basado en anomalías aprende las actividades "normales" de un entorno y activa una alarma cuando detecta actividad que difiere de la norma. Los tres tipos de IDS basados en anomalías son estadístico, protocolo y tráfico. También se denominan comportamiento o heurística.

28. Tom trabaja en una gran empresa minorista que recientemente implementó la identificación por radiofrecuencia (RFID) para gestionar mejor sus procesos de inventario. Los empleados utilizan escáneres para recopilar información relacionada con el producto en lugar de buscar manualmente los datos del producto. Tom ha descubierto que los clientes maliciosos han llevado a cabo ataques a la tecnología RFID para reducir la cantidad que pagan en los artículos de la tienda. ¿Cuál de las siguientes es la razón más probable para la existencia de este tipo de vulnerabilidad?

R. El equipo de seguridad de la compañía no entiende cómo asegurar este tipo de tecnología.

B. El costo de integrar la seguridad dentro de RFID es prohibitivo para los costos.

C. La tecnología tiene bajas capacidades de procesamiento y el cifrado es muy intensivo en procesadores.

D. RFID es una tecnología nueva y emergente, y la industria actualmente no tiene maneras de asegurarlo.

☑ **C.** Un problema de seguridad común con RFID es que los datos se pueden capturar a medida que se mueven de la etiqueta al lector y se modifican. Mientras que el cifrado se puede integrar como una contramedida, no es común porque RFID es una tecnología que tiene bajas capacidades de procesamiento y el cifrado es muy intensivo en procesador.

☒ **A** es incorrecto porque no es necesariamente la mejor respuesta aquí. La empresa en la pregunta puede entender RFID y sus problemas de seguridad comunes, pero la seguridad generalmente tiene que integrarse dentro de la tecnología RFID. Esto significa que el proveedor del producto RFID tendría que integrar la seguridad en el producto, y las soluciones de seguridad disponibles son comúnmente limitadas porque las etiquetas RFID y los lectores no suelen tener la potencia de procesamiento necesaria para llevar a cabo las funciones criptográficas necesarias.

☒ **B** es incorrecto porque el costo de integrar la seguridad en los productos RFID puede o no ser un factor. Por lo general, se reduce a la limitación de la tecnología en sí, no necesariamente a los costos involucrados.

☒ **D** es incorrecto porque no es la mejor respuesta aquí. RFID ha existido durante muchos años, y muchos en la industria entienden cómo funciona y sus problemas de seguridad. La integración de la seguridad en una tecnología con tantas limitaciones exige necesidades y motivación reales. En la mayoría de las situaciones, los datos que se transfieren a través de RFID no son excesivamente sensibles, por lo que no ha habido una verdadera necesidad percibida de integrar la seguridad en él. A medida que RFID evoluciona, lo más probable es que esté mejor equipado para manejar las contramedidas de seguridad, pero la industria aún no ha llegado completamente a este lugar.

29. Tanya es el administrador de seguridad de una gran empresa minorista distribuida. La red de la compañía tiene muchos dispositivos de red y dispositivos de software diferentes que generan registros y datos de auditoría. Tanya y su personal se han visto abrumados por tratar de revisar todos los archivos de registro al intentar identificar si algo sospechoso está ocurriendo dentro de la red. ¿Cuál de las siguientes es la mejor solución para que esta empresa la implemente?

R. Información de seguridad y gestión de eventos

B. Herramientas de correlación de eventos

C. Sistemas de detección de intrusiones

D. Herramientas de gestión de correlación de eventos de seguridad

☑ **R.** Hoy en día, muchas organizaciones están implementando sistemas de gestión de eventos de seguridad (SEM), también llamados sistemas de información de seguridad y gestión de eventos (SIEM). Estos productos recopilan registros de varios dispositivos (servidores, firewalls, enrutadores, etc.) e intentan correlacionar los datos de registro y proporcionar capacidades de análisis. Las empresas también tienen diferentes tipos de soluciones en una red (IDS, IPS, antimalware, proxies, etc.) recopilando registros en varios formatos propietarios, que requieren centralización, estandarización y normalización. Los formatos de registro son diferentes por tipo de producto y proveedor; por lo tanto, SIEM los coloca en un formato estandarizado para informes útiles.

☒ **B** es incorrecto porque la respuesta A proporciona una representación más precisa de la solución necesaria. Las herramientas SEM y SIEM se centran en eventos maliciosos y proporcionan una capacidad de administración centralizada. Los registros se agregan comúnmente a un sistema, y el software SIEM "traduce" los registros en un formato estandarizado. La estandarización permite analizar los datos de registro e generar informes.

☒ **C** es incorrecto porque un sistema de detección de intrusiones es un producto que identifica actividades maliciosas y lleva a cabo actividades de notificación. Aunque estos tipos de productos pueden agregar registros para su análisis, no tienen la capacidad de estandarizar formatos de registro de diferentes tipos de productos.

☒ **D** es incorrecto porque no es la mejor respuesta aquí. Se puede argumentar que las herramientas de gestión de correlación de eventos de seguridad es la respuesta correcta que "Información de seguridad y gestión de eventos" está llevando a cabo, pero en el examen se le pedirá que elija la *mejor* respuesta. La información de seguridad y la administración de eventos (SIEM) es el término real que el sector utiliza para los productos que proporcionan este tipo de funcionalidad.

30. La Agencia logística del departamento de defensa de un país es responsable de garantizar que todos los materiales necesarios lleguen a los lugares adecuados para apoyar las actividades diarias del departamento. Los datos que esta agencia mantiene deben estar protegidos de acuerdo con los tres principios principales de seguridad de los controles de seguridad. ¿Para las responsabilidades de esta agencia, qué principio de seguridad tiene la máxima prioridad?

R. confidencialidad

B. integridad

C. disponibilidad

D. privacidad

☑ **R.** Los tres principios principales de seguridad para todos y cada uno de los controles de seguridad son disponibilidad, integridad y confidencialidad (AIC). Es evidente que cada uno de ellos es una preocupación para la misión de esta organización. Sin embargo, la confidencialidad en cuanto a la disposición y ubicación de estos materiales es de la más alta prioridad. Si un adversario tuviera acceso al conocimiento de algo tan mundano como donde se estaban enviando grandes volúmenes de papel higiénico, podrían inferir movimientos de tropas antes de una acción ofensiva militar.

☒ **B** es incorrecto porque, aunque una operación podría verse gravemente afectada si un adversario fuera capaz de comprometer el despliegue logístico de materiales para una unidad militar violando la integridad de los datos al respecto, esto presupone primero una violación de su confidencialidad.

☒ **C** es incorrecta porque, aunque la disponibilidad de sistemas logísticos militares es claramente una prioridad extremadamente alta para un despliegue plenamente funcional, en este contexto la confidencialidad de qué sistemas y datos son clave para cualquier operación dada es de mayor prioridad.

☒ **D** es incorrecto porque, aunque la privacidad es una consideración cada vez más importante, no se considera uno de los tres principios principales de seguridad, ya que en realidad es un aspecto específico de la confidencialidad.

31. Claudia es la CISO de una institución financiera global, supervisando la seguridad de cientos de millones de cuentas bancarias. ¿Cuál de los tres principios principales de seguridad debería considerar más importantes a la hora de priorizar los controles que su empresa debería implementar?

R. confidencialidad

B. integridad

C. disponibilidad

D. autenticidad

☑ **B.** Los tres principios principales de seguridad para todos y cada uno de los controles de seguridad son disponibilidad, integridad y confidencialidad (AIC). Claramente cada uno de ellos es una preocupación por la seguridad de la organización de Claudia. Sin embargo, entre ellos, la integridad de los datos de la cuenta es lo más importante. La integridad es la garantía de que los datos de la cuenta bancaria no han sido alterados de manera no autorizada. Un compromiso de este principio podría significar esencialmente que el dinero de los titulares de cuentas ha sido robado, que el banco ha sido robado.

☒ **R** es incorrecto porque, aunque Claudia debe preocuparse por la confidencialidad de los datos de los titulares de sus cuentas, lo más probable es

que cumpla con las regulaciones bancarias y de privacidad en varios países, la amenaza de que una cuenta sea modificada por un atacante es mucho mayor.

☒ **C** es incorrecta porque, aunque ciertamente el banco de Claudia debe preocuparse por la disponibilidad de datos y sistemas para soportar transacciones 24/7, la amenaza de la modificación no autorizada de las cuentas de los 1 y 0 (¡dinero!) es de mayor preocupación para un banco.

☒ **D** es incorrecta porque la autenticidad de las entidades que intentan realizar transacciones también es una preocupación, pero solo en la medida en que las transacciones nunca dan lugar a modificaciones no autorizadas en los detalles de la cuenta. Este es un problema de integridad ante todo.

32. ¿Cuál de los siguientes es un ejemplo de un sistema de gestión de credenciales, también conocido como sistema de gestión de identidades (IdM)?

R. Un registro histórico de las actividades realizadas por los usuarios una vez que han presentado sus credenciales a un sistema central de autorización

B. Una base de datos de las credenciales que se han registrado a cada individuo en una empresa, con el fin de correlacionar a los usuarios con los nombres de usuario y las configuraciones regionales

C. Un sistema de información de seguridad y gestión de eventos (SIEM) que contiene los registros de varios sistemas de credencialización de la empresa, para la correlación de actividades por ID

D. Un Centro de distribución de claves Kerberos (KDC) que contiene las claves simétricas de todas las entidades y sistemas de un reino kerberos, que se puede administrar de forma centralizada para asegurarse de que está actualizado con respecto a las adiciones y eliminaciones de claves

☑ **D.** Kerberos es una solución común a la administración de credenciales e identidades, facilitando todas las necesidades de dicho sistema, incluida la creación de cuentas en todos los sistemas, la asignación de detalles y privilegios de la cuenta y el desmantelamiento de cuentas cuando ya no son necesarias. Es la tecnología principal detrás de Active Directory de Microsoft, que es la solución idm más común en un entorno empresarial.

☒ **A** es incorrecto porque, aunque es importante poder revisar las actividades históricas de usuarios individuales cuyas credenciales han sido aprovisionadas por un sistema de autorización central, esta es solo una característica de un sistema IdM robusto.

☒ **B** es incorrecto porque, aunque el almacén de datos de la información de la cuenta es una característica central de un sistema de administración de credenciales, la capacidad de administrar estos datos en el día a día es la característica destacada.

☒ **C** es incorrecto porque, aunque un SIEM puede ser útil para realizar un seguimiento de las actividades de los usuarios acreditados en varios sistemas de un entorno grande, su uso depende de un sistema de administración de credenciales centralizado como Kerberos o Active Directory.

33. ¿Cuál de los siguientes atributos se utiliza para autenticar biométricamente la identidad de un usuario?

R. Algo que sabes

B. Algo que tienes

C. Algo que eres

D. En algún lugar donde estés

☑ **C.** Cada uno de "algo que sabes", "algo que tienes" y "algo que eres" son factores clásicos de autenticación utilizados para validar la afirmación de identidad de un usuario. La autenticación biométrica busca autenticar a un usuario en función de algún atributo físico único del usuario, como una huella digital, el patrón de color pixilado granular del iris del ojo o el patrón digitalizado de una voz. Esto es innato para el usuario, y por lo tanto comprende "algo que eres."

☒ **A** es incorrecto porque algo que un usuario sabe, como una contraseña, una frase de contraseña o un número pin, es algo que se puede compartir fácilmente entre los usuarios, por lo que no es un atributo innato solo para un usuario.

☒ **B** es incorrecto porque, del mismo modo, algo que un usuario posee físicamente, como un token, una tarjeta o una clave física, se puede transferir o robar fácilmente. Como tal, no es necesariamente exclusivo de un usuario.

☒ **D** es incorrecto porque "algún lugar donde estás" ciertamente no es innato para el usuario. Es un factor de autenticación más nuevo que podría ser, por ejemplo, una geolocalización proporcionada por un sistema GPS o la fisicidad de un inicio de sesión en la consola (que coloca al usuario en un centro de datos, tal vez). Se puede usar en la autenticación multifactor, pero no es particularmente útil por sí solo.

34. Dentro de la autenticación biométrica, ¿qué es una tasa de error tipo II?

R. La tasa de errores en la que el sistema acepta falsamente la autenticación de una persona que no es a quien pretenden ser

B. La tasa de errores en la que el sistema rechaza falsamente la autenticación de una persona que es a quien pretenden ser

C. La tasa de errores que produce el sistema cuando los rechazos falsos y las aceptaciones falsas son iguales

D. La tasa de errores en la que el sistema no acepta o rechaza la autenticación de una persona independientemente de su validez

☑ **R.** La tasa de aceptación falsa (FAR) es la tasa de errores de tipo II dentro de un sistema biométrico y representa la velocidad a la que un sistema acepta impostores a los que se debería haber declinado el acceso. Estos son los errores más críticos que un sistema biométrico debe ajustarse para minimizar.

☒ **B** es incorrecta porque describe la tasa de rechazo falso (FRR), que es la tasa de errores de tipo I dentro de un sistema biométrico y representa la velocidad a la que un sistema rechaza a los usuarios auténticos a los que se debería haber concedido acceso. Los errores de tipo I son los errores menos críticos, ya que no dan lugar a una omisión de autenticación, pero son una molestia para el usuario, que debe intentar de nuevo autenticarse correctamente.

☒ **C** es incorrecto porque describe la tasa de error de cruce (CER), que es el punto en el ajuste de sensibilidad de un sistema biométrico en el que las FAR y frr son iguales. El CER se utiliza como una métrica de rendimiento para cualquier sistema biométrico dado, de modo que cuanto más bajo sea el CER, más preciso se puede configurar el sistema para que sea.

☒ **D** es incorrecta porque la velocidad a la que un sistema no funciona por completo, ya sea a través de FAR o FRR, no es una métrica utilizada para la evaluación del rendimiento de un sistema biométrico, pero probablemente representa un error sistémico.

35. ¿Cuál de los siguientes criterios es la consideración más importante para la selección e implementación de un sistema de autenticación biométrica?

R. Tasa de aceptación falsa (FAR) o tasa de error tipo II

B. Tasa de rechazo falso (FRR) o tasa de error tipo I

C. Velocidad de error de cruce (CER) o tasa de error igual (EER)

D. Velocidad de procesamiento

☑ **D.** La velocidad de procesamiento es el tiempo que tarda un sistema biométrico en autenticar realmente a un usuario tras la presentación de la parte del cuerpo. Independientemente de lo bien que se pueda ajustar un sistema con respecto a FAR, FRR o CER, a menos que el sistema pueda procesar un rendimiento suficiente de las personas en la implementación real, se convertirá en un costoso cuello de botella. Al igual que los sistemas diferentes tienen umbrales diferentes para la precisión, tienen umbrales diferentes para el rendimiento, basados en la parte del cuerpo que se utiliza para la autenticación.

☒ **A, B** y **C** son incorrectas porque, aunque todas estas medidas son críticas en la consideración de qué tipo de sistema implementar, la consideración más crítica en el mundo real es si el sistema puede o no satisfacer las necesidades de

los usuarios que se autentican y la misión comercial que el sistema se ha desplegado para apoyar.

36. Aunque "algo que usted sabe", en forma de contraseñas, es el factor de autenticación más común todavía utilizado hoy en día, se considera uno de los más débiles. Esto se debe a que las contraseñas son fáciles de compartir para los usuarios, y relativamente fáciles de robar o adivinar para los adversarios. ¿Cuál de las siguientes medidas es la mejor manera de contrarrestar los ataques a esta forma de autenticación?

R. Almacene todas las contraseñas solo en forma cifrada, de modo que recuperarlas requiera una clave especial para descifrarlas para la autenticación.

B. Utilice una directiva de contraseñas para asegurarse de que las contraseñas se eligen de tal manera que no son fáciles de adivinar para un atacante ni fáciles de hacer para un atacante.

C. Requiere que todas las contraseñas se compongan de una combinación de caracteres únicos, independientemente de la longitud.

D. Asegúrese de que las cuentas están bloqueadas después de un número mínimo de conjeturas incorrectas en un corto período de tiempo.

☑ **B.** Emplear una directiva de contraseña completa es el mejor método para garantizar que las contraseñas seleccionadas por los usuarios sean lo más seguras posible contra todas las formas de ataque. Esto incluye hacerlos menos fáciles de adivinar, prohibiendo el uso de cadenas asociadas con atributos conocedores del usuario, como nombres, fechas de nacimiento, etc. Las contraseñas también deben incluir cierta complejidad más allá de las palabras simples del diccionario, lo que normalmente requiere el uso de algunos caracteres especiales para hacerlos menos propensos a ser brutos por la fuerza. Lo más importante es que deben ser necesarios para ser tan largos como prácticos dado el sistema que los implementa. El envejecimiento de las contraseñas y las auditorías periódicas de fuerza también son prácticas recomendadas.

☒ **A** es incorrecto porque, aunque almacenar contraseñas en forma cifrada sólo es absolutamente necesario, el cifrado utilizado no debe ser reversible con ninguna clave. El hash unidireccional de contraseñas satisface este requisito. Aun así, el cifrado no es más que un aspecto de una política de contraseñas destacada.

☒ **C** es incorrecto porque, como se proporciona en la explicación de respuesta correcta, la complejidad de la contraseña es un requisito necesario pero no suficiente. Aplicar un requisito de longitud de contraseña más allá de 15 caracteres como mínimo forma parte de una directiva de contraseña eficaz.

☒ **D** es incorrecto porque el bloqueo de la cuenta después de un pequeño umbral de actividad de adivinanzas de contraseñas también es un aspecto

necesario pero insuficiente de una directiva de contraseña efectiva.

37. ¿Cuál de las siguientes es la secuencia correcta en el proceso de autenticación Kerberos con respecto a contraseñas, centros de distribución de claves (KDC), servidores de concesión de vales (TGS), tickets de concesión de vales (TGT), servicios y vales de servicio?

R. El usuario proporciona un nombre de usuario/contraseña a la estación de trabajo, la estación de trabajo obtiene un TGT del TGS, y posteriormente obtiene un ticket de servicio del KDC, que presenta al servicio.

B. La estación de trabajo obtiene un TGT del KDC, que el usuario valida con una contraseña. A continuación, el TGT se cambia por un vale de servicio del TGS, que se presenta al servicio.

C. El usuario proporciona un nombre de usuario/contraseña a la estación de trabajo, la estación de trabajo obtiene un TGT del KDC, y posteriormente obtiene un ticket de servicio del TGS, que presenta al servicio.

D. El usuario obtiene un ticket de servicio del servicio. A continuación, el usuario valida este vale con un nombre de usuario/contraseña proporcionado al TGS, que da lugar a un TGT que es validado adicionalmente por el KDC en un paso final.

☑ **C.** El usuario primero debe autenticarse en la estación de trabajo con un nombre de usuario y una contraseña. Estas credenciales son reenviadas por la estación de trabajo al servicio de autenticación (AS) en el KDC, que después devuelve un TGT cifrado con la clave secreta del TGS. Más adelante, cuando se requiere un servicio, el TGT se presenta de nuevo al TGS que puede autenticarlo y que, a continuación, devuelve un vale de servicio cifrado con la clave secreta del servicio. Cuando el vale de servicio se presenta al servicio, se puede producir la autenticación mutua: el servicio sabe que el usuario debe ser auténtico, porque el usuario no podría tener un vale de servicio válido sin haberse autenticado en el KDC y TGS, y el usuario sabe que el servicio es auténtico, porque puede descifrar el vale de servicio.

☒ **A** es incorrecto porque la autenticación con el KDC precede a la interacción con el TGS.

☒ **B** es incorrecto porque el usuario primero debe autenticarse con la estación de trabajo, de modo que tenga las credenciales para autenticarse con el KDC.

☒ **D** es incorrecta porque esta secuencia no tiene sentido y está completamente fuera de orden.

38. En uso práctico, ¿cuál de los siguientes describe mejor una "sesión"?

R. Cualquier intercambio de datos entre dos puntos finales discretos, a lo largo de cualquier duración arbitraria

B. Cualquier intercambio autenticado entre dos partes que se utiliza para llevar a cabo una conversación, con un comienzo discreto, período de actividad y terminación

C. Cualquier período discreto de tiempo que un usuario haya iniciado sesión en una estación de trabajo

D. El volumen de datos intercambiados entre dos sistemas durante un período de tiempo discreto

☑ **B.** En los usos más prácticos de la palabra, una "sesión" implica alguna forma inicial de autenticación entre dos partes, ya sea entre un usuario y una estación de trabajo o entre dos sistemas en una red. Después de la fase de autenticación en el inicio de la sesión, las dos partes llevan a cabo un intercambio de datos de forma interactiva y, a continuación, terminan el intercambio cuando la sesión ya no es necesaria, más comúnmente a través de mutuo acuerdo. Por lo tanto, una sesión tiene un comienzo discreto, un período de actividad interactiva y una terminación discreta.

☒ **A** es incorrecta porque esta definición, aunque vagamente precisa, falla los componentes más comunes de la iniciación mutua/autenticación y la terminación. Aunque la duración puede ser arbitraria en longitud, por lo general es discretamente limitada.

☒ **C** es incorrecto porque un usuario que inicia sesión en una estación de trabajo ciertamente puede ser considerado una sesión por esta definición, pero es un caso especial. Las sesiones pueden transpirar entre sistemas y servicios por igual.

☒ **D** es incorrecto porque, aunque los datos se intercambiarán durante cualquier sesión, el volumen de los que se trata no es lo que define una sesión, sino más bien la naturaleza conversacional del intercambio.

39. El uso de "servidores de recursos" y "servidores de autorización" para permitir que un servicio web "cliente" (como LinkedIn) acceda a un "propietario de recursos" (como Google) para la autorización federada es un sello distintivo de qué estándar abierto?

R. OpenID

B. Saml

C. Sso

D. OhAuth

☑ **D.** OAuth es un estándar abierto para la autorización de sitio web a sitio web (no autenticación). Se usa para permitir que una cuenta a la que se autentica un usuario en un sitio acceda a recursos en otro sitio de terceros.

☒ **A** es incorrecto porque OpenID es un estándar abierto no para la autorización, sino para la autenticación por un sitio de terceros que mantiene las credenciales reales para ese usuario. Involucra a una "parte de confianza" y un "proveedor" de OpenID.

☒ **B** es incorrecto porque el lenguaje de marcado de aserción de seguridad (SAML) es un estándar basado en XML para transmitir autenticación en un sistema de administración de identidades federadas, normalmente de una empresa a otra.

☒ **C** es incorrecto porque el inicio de sesión único (SSO), aunque también un mecanismo de autenticación, no es un estándar abierto y normalmente se administra y se utiliza dentro de una sola empresa para el acceso heterogéneo del sistema.

40. ¿Cuál de las siguientes no es cierto de OpenID Connect (OIDC)?

R. Se utiliza principalmente como un mecanismo de inicio de sesión único (SSO) basado en estándares abiertos entre plataformas dispares dentro de un entorno empresarial.

B. Se coloca en capas en el protocolo OAuth para permitir la autenticación y la autorización de forma transparente para las solicitudes de recursos de cliente.

C. Admite tres flujos: flujo de código de autorización, flujo implícito y flujo híbrido.

D. Implica redirecciones del navegador desde el proveedor OpenID de nuevo a la parte de confianza utilizando códigos de autorización.

☑ **R.** OAuth, OpenID y OIDC son todos protocolos y estándares abiertos para su uso en la autenticación y autorización en empresas, en lugar de dentro, para facilitar la administración de identidades federadas (IdM).

☒ **B** es incorrecto porque es una verdadera instrucción que OIDC está en capas en OAuth 2.0, extendiéndolo para poder proporcionar autorización para servicios de terceros, de forma transparente al usuario, además de autenticación.

☒ **C** es incorrecto porque es una verdadera instrucción que OIDC soporta los tres flujos. El flujo de código de autorización proporciona un código de autorización al usuario de confianza, que luego se usa para solicitar directamente un token de identificador al proveedor de identidades (IdP). El flujo implícito proporciona al usuario de confianza el token de identificador directamente, que se pasa a través del explorador del usuario. El flujo híbrido utiliza una combinación de los dos.

☒ **D** es incorrecto porque es una verdadera instrucción que OIDC implica redirecciones del explorador desde el proveedor OpenID de nuevo al usuario de

confianza mediante códigos de autorización (en flujos híbridos, como se describe en la opción C, anteriormente).

41. ¿Cuál de los siguientes atributos se agrega más allá de los mecanismos tradicionales de control de acceso (RBAC, MAC y DAC) para implementar ABAC?

R. Temas

B. Objetos

C. Acciones

D. contexto

☑ **D.** Los métodos tradicionales, como el control de acceso basado en roles (RBAC), el control de acceso obligatorio (MAC) y el control de acceso discrecional (DAC), se basan en categorías de temas y objetos, y asignan acciones que se pueden realizar en función de combinaciones de los dos. El control de acceso basado en atributos (ABAC) incluye contextos, como la hora del día, el estado o la fase de un proyecto y otros eventos contextuales, con el fin de proporcionar una mayor granularidad a la que se puede acceder a los objetos por qué sujetos, cuándo y cómo.

☒ **A** es incorrecto porque todos los sistemas de control de acceso emplean temas (qué usuarios y sistemas) y sus niveles de autorización.

☒ **B** es incorrecto porque todos los sistemas de control de acceso emplean objetos (archivos, carpetas, procesos y otros recursos) y sus etiquetas de clasificación o sensibilidad.

☒ **C** es incorrecto porque todos los sistemas de control de acceso también emplean acciones que se pueden realizar (lectura, escritura, ejecución, etc.).