Domain 6 - Security Assessment and Testing

Test ID: 178283618

Pregunta #1 de 29

Id. de pregunta: 1111759

Está en el proceso de definir e implementar un programa de supervisión continua de seguridad de la información (ISCM) para su organización de acuerdo con NIST SP 800-137. ¿Cuál es una entrada esperada para definir este programa?

- ✗ **A)** informes sobre el estado de seguridad
- ✓ **B)** evaluación de riesgos organizacionales
- ✗ **C)** especificación de automatización
- ✗ **D)** requisitos de presentación de informes

explicación

La evaluación de riesgos de la organización es una entrada para el paso Definir la estrategia ISCM. También es una entrada para el paso Establecer el programa ISCM. NIST SP 800-137 guía el desarrollo de monitoreo continuo de seguridad de la información (ISCM) para sistemas de información y organizaciones federales. Define los siguientes pasos para establecer, implementar y mantener ISCM:

- Definir una estrategia ISCM.
- Establecer un programa ISCM.
- Implementar un programa ISCM.
- Analice los datos y divulgue los resultados.
- Responder a los hallazgos.
- Revisar y actualizar la estrategia y el programa de ISCM.

Los requisitos de informes son una entrada para el paso Establecer un programa ISCM. Las especificaciones de automatización son una entrada para el paso Implementar un programa ISCM. Los informes sobre el estado de seguridad son una entrada para el paso Responder a la búsqueda.

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Realizar pruebas de control de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 6: Evaluación y pruebas de seguridad, NIST SP 800-137

NIST SP 800-137, http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

Pregunta #2 de 29

Id. de pregunta: 1192958

Su empresa ha contratado a una empresa de seguridad para probar la seguridad de su red. ¿Qué tendría que usarse fuera de su red?

- ✓ **A)** probador de penetración
- ✗ **B)** escáner de puertos
- ✗ **C)** analizador de protocolos
- ✗ **D)** analizador de vulnerabilidades

explicación

Un probador de penetración tendría que ser utilizado fuera de su red. Esto pone a prueba la seguridad de la red para ver si se puede penetrar. Sólo se puede penetrar en una red desde fuera de ella.

Ninguna de las otras pruebas debe utilizarse fuera de la red. Un analizador de vulnerabilidades comprueba la red en busca de vulnerabilidades conocidas y proporciona métodos de protección contra las vulnerabilidades. Un analizador de puertos identifica los puertos y servicios que están disponibles en la red. Un analizador de protocolos captura paquetes en la red.

Una prueba de penetración se origina fuera de la red. Un análisis de vulnerabilidad generalmente se origina dentro de la red.

Una prueba de penetración debe incluir los siguientes pasos:

Los pasos formales en la prueba de penetración son los siguientes:

1. Documente información sobre el sistema o dispositivo de destino. (Esto es descubrimiento.)
2. Recopilar información sobre los métodos de ataque contra el sistema o dispositivo de destino. Esto incluye la realización de análisis de puertos. (Esto es enumeración.)
3. Identificar las vulnerabilidades conocidas del sistema o dispositivo de destino. (Se trata de la asignación de vulnerabilidades).
4. Ejecutar ataques contra el sistema o dispositivo de destino para obtener acceso de usuario y con privilegios. (Esto es explotación.)
5. Documente los resultados de la prueba de penetración e informe de los hallazgos a la gerencia, con sugerencias para la acción correctiva. (Esto es informar).

Las direcciones IP de las computadoras generalmente se descubren durante una prueba de penetración. A medida que se descubran los componentes de la red, se determinarán los métodos utilizados.

Objetivo:

Evaluación y pruebas de seguridad

Subobsecución:

Analizar la salida de la prueba y generar un informe

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 6: Evaluación y pruebas de seguridad, pruebas de penetración

Reconocimiento de pruebas de penetración,
http://searchsecuritychannel.techtarget.com/tip/0,289483,sid97_gci1235335,00.html

---

Pregunta #3 de 29

Id. de pregunta: 1113994

Debe proporcionar informes SOC 2 y SOC 3 sobre la seguridad, disponibilidad, confidencialidad, integridad del procesamiento y privacidad de los controles operativos. Como parte de estos informes, debe proporcionar información sobre la divulgación de datos a terceros. ¿A qué principio de SOC 2 y SOC 3 se aplica esta información?

✗ **A)** seguridad

✓ **B)** privacidad

✗ **C)** confidencialidad

✗ **D)** disponibilidad

explicación

La divulgación de datos a terceros se aplica al principio de privacidad de SOC 2 y SOC 3. La privacidad incluye la administración, el aviso de privacidad, las recopilaciones de datos, el uso y la retención de datos, el acceso a los datos, la calidad de los datos y el monitoreo y la aplicación.

La seguridad incluye la política de seguridad de TI, el conocimiento de la seguridad, la evaluación de riesgos, el acceso lógico y físico, la supervisión de la seguridad, la autenticación de usuarios, la administración de incidentes, la clasificación de activos, la seguridad del personal y otros temas.

La confidencialidad incluye la política de confidencialidad, la confidencialidad de entrada, la confidencialidad del procesamiento de datos, la confidencialidad de la salida, la divulgación de información y la confidencialidad del desarrollo de sistemas.

La disponibilidad incluye backup y restauración de datos, controles ambientales, recuperación ante desastres, continuidad del negocio y proceso de disponibilidad.

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Realizar o facilitar auditorías de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 6: Evaluación y pruebas de seguridad, realizar auditorías

---

Pregunta #4 de 29

Id. de pregunta: 1105376

Durante una conferencia de seguridad reciente, asistió a una formación que explicaba la diferencia entre la supervisión de seguridad activa y pasiva. ¿Qué es una medida pasiva que se puede utilizar para detectar ataques de hackers?

- ✗ **A)** terminación de la conexión
- ✗ **B)** terminación del proceso
- ✗ **C)** reconfiguración del cortafuegos
- ✓ **D)** registro de eventos

explicación

El registro de eventos es una medida pasiva que se puede utilizar para detectar ataques de piratas informáticos. El registro de eventos se considera una medida pasiva porque no crea obstáculos a los ataques. Sin embargo, los administradores pueden revisar los archivos de registro después de un ataque para determinar el origen y los medios del ataque. La información obtenida de los archivos de registro se puede utilizar para implementar medidas de prevención activas. Los archivos de registro también se pueden usar como evidencia legal al procesar a los atacantes, por lo que los archivos de registro deben protegerse y se deben tomar medidas para garantizar su integridad.

La terminación de la conexión, la reconfiguración del firewall y la terminación del proceso son medidas activas para la prevención de ataques de piratas informáticos; estos métodos establecen obstáculos destinados a excluir, o al menos limitar, la posibilidad de ataque.

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Realizar pruebas de control de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 6: Evaluación y pruebas de seguridad, Análisis de vulnerabilidades de red

Pregunta #5 de 29

Id. de pregunta: 1105368

Está investigando el posible acceso no autorizado a un equipo con Windows Server 2003. El primer paso en la directiva de investigación de su empresa indica que se deben documentar las conexiones de red actuales. ¿Qué comando debe usar?

✗ **A)** tracert

✗ **B)** ipconfig

✗ **C)** Señal

✓ **D)** netstat

explicación

Debe utilizar el comando netstat. Esta herramienta muestra las conexiones entrantes y salientes, las tablas de enrutamiento y las estadísticas de la interfaz de red.

La herramienta ping se utiliza para probar la disponibilidad de un equipo a través de una red. Puede hacer ping a los equipos en función de su nombre de host DNS o dirección IP.

La herramienta ipconfig muestra la dirección IP, la máscara de subred y la puerta de enlace predeterminada de un equipo. También se puede utilizar para liberar y renovar una concesión de dirección IP del Protocolo de host de configuración dinámica (DHCP). La herramienta equivalente de UNIX es ifconfig.

La herramienta tracert se utiliza para determinar la ruta que toma un paquete a través de una red IP de Windows. Los equipos UNIX tienen una herramienta similar llamada traceroute.

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Realizar pruebas de control de seguridad

Referencias:

Netstat, http://www.netstat.net/

Pregunta #6 de 29

Id. de pregunta: 1105366

Su empresa debe cumplir con los requisitos de un organismo de certificación de ciberseguridad. La administración le ha solicitado que realice una prueba antes de solicitar esta certificación. ¿Qué tipo de prueba debe realizar?

✗ **A)** Realizar una evaluación o auditoría externa utilizando personal de la empresa.

✗ **B)** Realice una evaluación o auditoría interna utilizando personal del organismo de certificación.

✓ **C)** Realizar una evaluación o auditoría interna utilizando personal de la empresa.

✗ **D)** Realizar una evaluación o auditoría externa utilizando personal del organismo de certificación.

explicación

Debe realizar una evaluación o auditoría interna utilizando personal de la empresa. Las evaluaciones o auditorías internas deben realizarse primero para que el personal pueda trabajar en la corrección de cualquier vulnerabilidad, riesgo o problema identificado.

No debe realizar una evaluación externa o auditoría de ningún tipo hasta después de haber realizado una evaluación o auditoría interna y resuelto tantos de los problemas identificados allí como sea posible.

No debe realizar una evaluación o auditoría interna o externa utilizando personal del organismo de certificación hasta después de que el personal de la organización haya realizado estas evaluaciones y trabajado para solucionar los problemas identificados.

Las evaluaciones o auditorías internas se completan desde dentro de la empresa y pueden ser completadas por personal de la empresa o de un tercero. Las evaluaciones externas se completan desde fuera de la empresa y pueden ser completadas por personal de la empresa o de un tercero. Si bien algunos organismos de certificación proporcionarán personal para realizar la evaluación o auditoría como parte del proceso de certificación, algunos pueden requerir que las organizaciones trabajen con una organización de terceros para realizar la evaluación o auditoría.

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Diseñar y validar estrategias de evaluación, prueba y auditoría

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 6: Evaluación y pruebas de seguridad, Diseño y validación de estrategias de evaluación y pruebas

---

Pregunta #7 de 29

Id. de pregunta: 1192957

Instale un analizador de red para capturar el tráfico de la red como parte de la directiva de seguridad de su empresa. Más adelante, usted examina los paquetes capturados y descubre que solamente el tráfico de la subred 1 fue capturado. Usted necesita capturar los paquetes de las cuatro subredes en su red.

¿Qué podrías hacer?

un. Instale un escáner de puertos.

B. Instale el analizador de red en las cuatro subredes.

c. Instalar un analizador de red distribuido.

d. Instale el analizador de red en un enrutador.

E. Instale el analizador de red en el firewall.

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

explicación

Puede instalar el analizador de red en las cuatro subredes o instalar un analizador de red distribuido. Los analizadores de red estándar solo capturan paquetes en la subred local. Para capturar paquetes en una red de varias subredes, puede instalar el analizador de red en las cuatro subredes. Como alternativa, puede adquirir un analizador de red que pueda capturar todos los paquetes de las subredes. Un analizador de red distribuido normalmente consta de un analizador de red de estación de trabajo dedicado instalado en una subred y sondeos de software instalados en las otras subredes.

No debe instalar un analizador de puertos. Un analizador de puertos informa de los puertos y servicios que se están utilizando en la red.

No debe instalar el analizador de red en un enrutador. Esto permitirá solamente que usted capture los paquetes en las dos subredes conectadas con el router.

No debe instalar el analizador de red en el firewall. Esto solo le permitirá capturar paquetes en las subredes conectadas al firewall.

Objetivo:

Evaluación y pruebas de seguridad

Subobsecución:

Realizar pruebas de control de seguridad

Referencias:

¿Qué es un Packet Sniffer?, HYPERLINK "https://www.lifewire.com/what-is-a-packet-sniffer-2487312" \t "sean" http://netsecurity.about.com/od/informationresources/a/What-Is-A-Packet-Sniffer.htm

---

Pregunta #8 de 29

Id. de pregunta: 1105386

¿Cuál de los siguientes NO es parte de una prueba de penetración?

- ✗ **A)** enumeración
- ✗ **B)** explotación
- ✓ **C)** Aplicación de los controles
- ✗ **D)** descubrimiento

explicación

Una prueba de penetración NO incluye la implementación de controles. Los controles se implementan en base a las recomendaciones del informe final de la prueba de penetración. Sin embargo, estos controles no se implementan como parte de la prueba de penetración. Es un proceso u operación independiente.

Una prueba de penetración debe incluir los siguientes pasos:

Los pasos formales en la prueba de penetración son los siguientes:

1. Documente información sobre el sistema o dispositivo de destino. (Esto es descubrimiento.)
2. Recopilar información sobre los métodos de ataque contra el sistema o dispositivo de destino. Esto incluye la realización de análisis de puertos. (Esto es enumeración.)
3. Identificar las vulnerabilidades conocidas del sistema o dispositivo de destino. (Se trata de la asignación de vulnerabilidades).
4. Ejecutar ataques contra el sistema o dispositivo de destino para obtener acceso de usuario y con privilegios. (Esto es explotación.)
5. Documente los resultados de la prueba de penetración e informe de los hallazgos a la gerencia, con sugerencias para la acción correctiva. (Esto es informar).

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Recopilar datos de procesos de seguridad (por ejemplo, técnicos y administrativos)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 6: Evaluación y pruebas de seguridad, pruebas de penetración

---

Pregunta #9 de 29

Id. de pregunta: 1105381

La política de seguridad de su empresa establece que las contraseñas nunca deben transmitirse en texto sin formato. Debe determinar si se está siguiendo esta directiva. ¿Qué herramienta debe utilizar?

- ✗ **A)** descifrador de contraseñas
- ✓ **B)** analizador de protocolos
- ✗ **C)** analizador de vulnerabilidades
- ✗ **D)** asignador de red

explicación

Debe utilizar un analizador de protocolos para determinar si las contraseñas se transmiten en texto sin formato. Los analizadores de protocolo capturan los paquetes a medida que se transmiten en la red. Si una contraseña se transmite en texto sin formato, podrá ver la contraseña en el paquete. Los analizadores de protocolo también se denominan analizadores de red o rastreadores de paquetes.

Un descifrador de contraseñas se utiliza para probar la seguridad de sus contraseñas. Intenta obtener una contraseña mediante ataques de diccionario o fuerza bruta.

Un analizador de vulnerabilidades comprueba la red en busca de vulnerabilidades conocidas y sugiere formas de evitar las vulnerabilidades.

Un asignador de red obtiene un mapa visual de la topología de la red, incluidos todos los dispositivos de la red.

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Realizar pruebas de control de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 5 Identidad y Gestión de Acceso Sniffer Attack

Pregunta #10 de 29

Id. de pregunta: 1192956

¿Cuál es la definición correcta de las pruebas de penetración?

- ✗ **A)** intrusión de hackers
- ✗ **B)** procedimientos de respuesta de seguridad realizados para el endurecimiento de sistemas y aplicaciones
- ✗ **C)** procedimientos de respuesta de seguridad realizados para detectar ataques de fuerza bruta
- ✓ **D)** Procedimiento de prueba realizado por profesionales de seguridad con aprobación de la administración

explicación

Las pruebas de penetración, que también se llaman piratería ética, son realizadas por profesionales de la seguridad después de recibir la aprobación de la gerencia. Cuando las herramientas de seguridad son utilizadas por los expertos en seguridad para explotar las vulnerabilidades del sistema con fines éticos, se denomina pruebas de penetración o piratería ética. Los hackers éticos encuentran pero no explotan las vulnerabilidades que encuentran en la infraestructura de red de una organización. El objetivo principal de las pruebas de penetración o hacking ético es evaluar la capacidad del sistema para resistir ataques y demostrar que existen vulnerabilidades del sistema y de la red.

Las pruebas de penetración implican el uso de herramientas para simular ataques a la red y a los sistemas informáticos después de solicitar la aprobación previa y la autorización de la alta dirección. Inicialmente, debe definir objetivos de administración y realizar revisiones de configuración, evaluaciones de vulnerabilidad e ingeniería social. Las pruebas de penetración se realizan para verificar los errores de seguridad que se descubrieron durante la evaluación de vulnerabilidad y se limitan a probar el impacto de la vulnerabilidad en la seguridad de la infraestructura. Este proceso permite a una organización tomar medidas correctivas, como parchear los sistemas contra vulnerabilidades o errores. Un equipo de prueba de penetración informa de los hallazgos a la alta dirección después de completar el proceso de documentación. ISS, Ballista y SATAN son algunos ejemplos de pruebas de penetración o herramientas de hacking ético utilizadas para identificar vulnerabilidades de redes y sistemas.

La intrusión realizada por hackers con una intención maliciosa se denomina piratería o cracking en lugar de hacking ético y pruebas de penetración.

Las pruebas de penetración no se utilizan para detectar ataques, como los ataques de fuerza bruta. Las pruebas de penetración están diseñadas para identificar vulnerabilidades en el sistema mediante el uso de herramientas de seguridad. Para detectar ataques de piratería, puede utilizar un IDS o un firewall.

Los procedimientos de respuesta de seguridad llevados a cabo para el endurecimiento del sistema y la aplicación se llevan a cabo después de que se hayan identificado los fallos de seguridad mediante el uso de la piratería ética. Los procedimientos de respuesta de seguridad pueden ser de naturaleza detectivesca o correctiva. Algunos ejemplos de procedimientos de respuesta de seguridad son el análisis de registros y la provisión de respuestas a incidentes.

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Realizar pruebas de control de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 6: Evaluación y pruebas de seguridad, pruebas de penetración

---

Pregunta #11 de 29

Id. de pregunta: 1192959

Está utilizando un analizador de red para supervisar el tráfico en la red. Los usuarios informan de que las sesiones se cuelgan intermitentemente durante todo el día. Sospecha que su red está bajo ataque. Decide utilizar el analizador de red para determinar el problema.

¿Qué información debe examinar?

- ✓ **A)** captura de paquetes
- ✗ **B)** estadísticas de puertos
- ✗ **C)** estadísticas de la estación
- ✗ **D)** estadísticas de protocolo

explicación

Usted debe utilizar la información de la captura de paquetes para examinar las sesiones que están colgando intermitentemente a lo largo del día. Usted necesitará examinar los paquetes que son enviados y determinar qué dispositivos no pudieron responder. Una captura de paquetes proporciona información detallada sobre cada paquete de la red.

Todas las demás opciones deben utilizarse solamente si usted sabe qué protocolo, estación (dispositivo), o puerto es la causa del problema.

No debe utilizar estadísticas de protocolo para este problema porque no está seguro de qué protocolo, si existe, está causando el problema.

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Analizar la salida de la prueba y generar un informe

Referencias:

¿Qué es un Packet Sniffer?, HYPERLINK "https://www.lifewire.com/what-is-a-packet-sniffer-2487312" \t "sean" http://netsecurity.about.com/od/informationresources/a/What-Is-A-Packet-Sniffer.htm

---

Pregunta #12 de 29

Id. de pregunta: 1302572

¿Qué es un escáner de vulnerabilidades?

- ✗ **A)** Una aplicación que protege un sistema contra virus
- ✗ **B)** Una aplicación que detecta cuándo se producen intrusiones en la red e identifica al personal adecuado
- ✗ **C)** Una aplicación que identifica puertos y servicios que están expuestos en una red
- ✓ **D)** Una aplicación que identifica problemas de seguridad en una red y ofrece sugerencias sobre cómo evitar los problemas

explicación

Un analizador de vulnerabilidades es una aplicación que identifica problemas de seguridad en una red y ofrece sugerencias sobre cómo evitar los problemas. A menudo, un escáner de vulnerabilidades va más allá de lo que puede hacer un escáner de puertos.

Un analizador de puertos es una aplicación que identifica los puertos y servicios que están expuestos en una red.

Un sistema de detección de intrusiones (IDS) es una aplicación que detecta cuándo se producen intrusiones en la red e identifica al personal adecuado.

Un detector de virus es una aplicación que protege un sistema contra virus.

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Realizar pruebas de control de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 6: Evaluación y pruebas de seguridad, Evaluación de vulnerabilidades

Pregunta #13 de 29

Id. de pregunta: 1111763

Se le ha pedido que lleve a cabo una prueba de penetración en la red de su organización. Se obtiene una huella de la red. ¿Qué debes hacer a continuación?

- ✓ **A)** Realice las exploraciones del puerto y la identificación del recurso.
- ✗ **B)** Intente obtener acceso no autorizado aprovechando las vulnerabilidades.
- ✗ **C)** Informar a la dirección.
- ✗ **D)** Identificar vulnerabilidades en sistemas y recursos.

explicación

Debe realizar análisis de puertos e identificación de recursos.

Una prueba de penetración debe incluir los siguientes pasos:

- Descubrimiento : obtenga la huella y la información sobre el objetivo y los métodos de ataque que se pueden utilizar.
- Enumeración: realice análisis de puertos e identificación de recursos.
- Mapeo de vulnerabilidades: identifique las vulnerabilidades en los sistemas y recursos.
- Explotación: intente obtener acceso no autorizado aprovechando las vulnerabilidades.
- Informe - Informe de los resultados a la administración con contramedidas sugeridas.

Los pasos formales en la prueba de penetración son los siguientes:

- Documente información sobre el sistema o dispositivo de destino. (Esto es descubrimiento.)
- Recopilar información sobre los métodos de ataque contra el sistema o dispositivo de destino. Esto incluye la realización de análisis de puertos. (Esto es enumeración.)
- Identificar las vulnerabilidades conocidas del sistema o dispositivo de destino. (Se trata de la asignación de vulnerabilidades).
- Ejecutar ataques contra el sistema o dispositivo de destino para obtener acceso de usuario y con privilegios. (Esto es explotación.)
- Documente los resultados de la prueba de penetración e informe de los hallazgos a la gerencia, con sugerencias para la acción correctiva. (Esto es informar).

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Recopilar datos de procesos de seguridad (por ejemplo, técnicos y administrativos)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 6: Evaluación y pruebas de seguridad, pruebas de penetración

---

Pregunta #14 de 29

Id. de pregunta: 1105394

Su empresa ha implementado una evaluación y pruebas de seguridad, estrategia que incluye un programa de monitoreo continuo de seguridad de la información (SCM). Como parte de este programa, debe proporcionar un informe detallado para los usuarios, auditores y otras partes interesadas que se centre en la seguridad, la disponibilidad, la confidencialidad, la integridad del procesamiento y la privacidad. ¿Qué informe debe proporcionar?

- ✓ **A)** SOC 2
- ✗ **B)** SOC 3
- ✗ **C)** SAS 70
- ✗ **D)** SOC 1

explicación

Debe proporcionar a los usuarios, auditores y otras partes interesadas un informe SOC 2. Este informe se centra en la seguridad, la disponibilidad, la confidencialidad, la integridad del procesamiento y la privacidad.

SAS 70 se centró específicamente en los riesgos relacionados con la información financiera. Se retiró en 2011.

Soc 1 se centra en los riesgos y controles de información financiera. Es un informe detallado para usuarios y auditores.

SOC 3 es un breve informe para la difusión pública que se centra en la seguridad, la disponibilidad, la confidencialidad, la integridad del procesamiento y la privacidad.

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Realizar o facilitar auditorías de seguridad

References:

CISSP Cert Guide (3rd Edition), Chapter 6: Security Assessment and Testing, Conduct Audits

---

Pregunta #15 de 29

Id. de pregunta: 1111762

¿Qué metodología se utiliza para analizar las vulnerabilidades del sistema operativo en un proyecto de pruebas de penetración?

✗ **A)** Metodología del proyecto de seguridad de aplicaciones web abiertas

✗ **B)** evaluación de la vulnerabilidad y metodología de recuperación

✗ **C)** metodología de huellas digitales del sistema operativo

✓ **D)** metodología de hipótesis de defectos

explicación

La metodología de hipótesis de defectos se utiliza para analizar las vulnerabilidades del sistema operativo en un proyecto de pruebas de penetración. La metodología de hipótesis de defectos se refiere a una técnica de análisis y penetración de sistemas en la que se analizan las especificaciones y la documentación de un sistema operativo para compilar una lista de posibles defectos. Los defectos se priorizan de acuerdo con las siguientes consideraciones:

- existencia de un defecto
- facilidad con la que se puede explotar un defecto
- el grado de control o compromiso de la falla puede conducir a

La lista priorizado se utiliza para realizar pruebas de penetración de sistemas operativos.

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Realizar pruebas de control de seguridad

Referencias:

Análisis de las herramientas de huellas digitales del sistema operativo activo remoto, http://www.packetwatch.net/documents/papers/osdetection.pdf

Guía para pruebas de penetración, Parte 5: Metodología y estándares de prueba, http://searchnetworking.techtarget.com/general/0,295582,sid7_gci1083724,00.html

---

Pregunta #16 de 29

Id. de pregunta: 1111758

¿Durante qué paso del NIST SP 800-137 se toman las decisiones sobre las respuestas de riesgo?

✗ **A)** Revisar y actualizar el programa y la estrategia de monitoreo.

✗ **B)** Establecer el programa ISCM.

✗ **C)** Definir la estrategia ISCM.

✓ **D)** Responder a los hallazgos.

explicación

Las decisiones sobre las respuestas de riesgo se toman durante la etapa Responder a los hallazgos del NIST SP 800-137. Se consideran una salida de este paso.

NIST SP 800-137 guía el desarrollo de monitoreo continuo de seguridad de la información (ISCM) para sistemas de información y organizaciones federales. Define los siguientes pasos para establecer, implementar y mantener ISCM:

- Definir una estrategia ISCM.
- Establecer un programa ISCM.
- Implementar un programa ISCM.
- Analice los datos y divulgue los resultados.
- Responder a los hallazgos.
- Revisar y actualizar la estrategia y el programa de ISCM.

Las decisiones sobre las respuestas de riesgo no forman parte de ninguno de los otros pasos enumerados del NIST SP 800-137.

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Realizar pruebas de control de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 6: Evaluación y pruebas de seguridad, NIST SP 800-137

NIST SP 800-137, http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

---

Pregunta #17 de 29

Id. de pregunta: 1105388

Está diseñando la solución de informes para el programa de supervisión continua de seguridad de la información (SCM) de su empresa. Debe crear un mecanismo mediante el cual los usuarios finales puedan crear los informes que necesitan. Configure la solución de inteligencia empresarial (BI), conéctelo a los orígenes de datos, establezca la configuración de seguridad y determine a qué objetos pueden tener acceso los usuarios. ¿Qué tipo de informes está implementando?

✗ **A)** fuente de distribución de datos

✗ **B)** informes periódicos

✗ **C)** informes automatizados

✓ **D)** presentación de informes ad hoc

explicación

Los informes ad hoc se usan al configurar la solución de inteligencia empresarial (BI), conectarla a los orígenes de datos, establecer la configuración de seguridad y determinar a qué objetos pueden tener acceso los usuarios.

Los informes automatizados entregan información mediante la configuración anticipada de los informes que deben ejecutarse y, a continuación, la generación y entrega automática de estos informes. Con los informes automatizados, los usuarios no crean los informes que necesitan.

Los informes periódicos son muy similares a los informes automatizados. Permite generar informes de forma regular para la información que siempre se necesita. Con los informes periódicos, los usuarios no crean los informes que necesitan.

Una fuente de distribución de datos permite a los usuarios recibir datos actualizados de orígenes de datos. Una fuente web o una fuente RSS son formas populares de fuentes de datos. Con las fuentes de distribución de datos, los usuarios reciben información, no informes.

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Analizar la salida de la prueba y generar un informe

Referencias:

Presentación de informes ad hoc, https://www.logianalytics.com/resources/bi-encyclopedia/ad-hoc-reporting/

Pregunta #18 de 29

Id. de pregunta: 1114767

¿Qué programas son herramientas utilizadas para obtener contraseñas de usuario?

un. L0phtCrack

B. Juan el Destripador

c. Tripwire

d. Grieta

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

explicación

L0phtCrack, John el Destripador y Crack son herramientas utilizadas para obtener contraseñas de usuario.

Tripwire NO se utiliza para obtener contraseñas de usuario.

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Realizar pruebas de control de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 6: Evaluación y pruebas de seguridad, pruebas de penetración

---

Pregunta #19 de 29

Id. de pregunta: 1114769

¿Qué afirmación es cierta del registro de eventos?

- ✓ **A)** Solo el personal de administración del sistema, auditoría interna y seguridad debe tener acceso a los archivos de registro.
- ✗ **B)** Los registros del sistema y de la aplicación deben entregarse a través de la red en texto sin formato.
- ✗ **C)** Los registros del sistema y de la aplicación deben permitir la modificación de las entradas existentes.
- ✗ **D)** El registro debe realizarse una vez al día.

explicación

Para garantizar la confidencialidad e integridad de los registros, sólo el personal de administración del sistema, el personal de auditoría interna y el personal de seguridad deben tener acceso a los archivos de registro con fines de

análisis y revisión. El registro permite al personal de administración de red detectar puntos vulnerables en una red, identificar problemas de rendimiento, registrar actividades sospechosas de un usuario específico o un sistema e identificar una brecha de seguridad. Es importante que los registros se revisen periódicamente y se archiven. El período de un archivo de registro depende de la confidencialidad de los datos y de la directiva de retención de la organización.

El registro no debe realizarse una vez al día. El registro debe estar habilitado permanentemente en todos los sistemas informáticos y equipos de infraestructura, como enrutadores y firewalls, para monitorear constantemente las operaciones. Los eventos se pueden registrar para sistemas Windows y UNIX. En un sistema UNIX, los eventos registrados incluyen el uso de Setuid y Setgid. En los sistemas Windows, los eventos registrados incluyen intentos de inicio de sesión correctos y no exitosos. Para ambos sistemas, también se deben registrar los cambios de permisos de archivo.

Los registros del sistema y de la aplicación no deben permitir la modificación de las entradas existentes. El registro proporciona información detallada sobre el uso de recursos del sistema y las actividades del sistema. En caso de intrusión, el registro proporciona los registros del sistema y las pistas de auditoría, lo que ayuda a detectar el origen de un ataque.

Los registros del sistema y de la aplicación no deben entregarse a través de la red en texto sin formato. Si los datos de registro se transfieren a través de un vínculo WAN, se recomienda que dicha información se cifre mientras viaja a través de la red. El cifrado de registros garantiza la confidencialidad e integridad de la información. Otras recomendaciones al transferir datos de registro a través de un vínculo WAN son las siguientes:

Los registros deben estar centralizados para facilitar la recopilación y el análisis.

Todos los sistemas informáticos y equipos de infraestructura deben tener su reloj sincronizado con un servidor de hora central, y las entradas del registro deben contener marcas de fecha y hora.

Los archivos de registro deben almacenarse en un sistema seguro mediante un estricto control de acceso para evitar modificaciones, destrucción o eliminación.

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Realizar pruebas de control de seguridad

Referencias:

CISSP Cert Guide (3rd Edition), Chapter 5 Identity and Access Management Accountability

---

Pregunta #20 de 29

Id. de pregunta: 1111764

¿Cuál es el paso final en una prueba de penetración?

✗ **A)** Ejecutar ataques contra el sistema de destino.

✗ **B)** Implemente los controles adecuados para evitar los problemas identificados en el informe.

✓ **C)** Documente los resultados e informe de los hallazgos a la gerencia.

✗ **D)** Identificar las vulnerabilidades conocidas del sistema de destino.

explicación

El paso final en una prueba de penetración es documentar los resultados e informar de los hallazgos a la gerencia.

Una prueba de penetración no incluye la implementación de los controles adecuados para prevenir los problemas identificados en el informe. Como parte de una prueba de penetración, solo debe proporcionar recomendaciones. La implementación de cualquiera de las recomendaciones sugeridas es independiente de la prueba de penetración y tiene su propio proceso.

Una prueba de penetración debe incluir los siguientes pasos:

- Descubrimiento : obtenga la huella y la información sobre el objetivo y los métodos de ataque que se pueden utilizar.
- Enumeración: realice análisis de puertos e identificación de recursos.
- Mapeo de vulnerabilidades: identifique las vulnerabilidades en los sistemas y recursos.
- Explotación: intente obtener acceso no autorizado aprovechando las vulnerabilidades.
- Informe - Informe de los resultados a la administración con contramedidas sugeridas.
- Descubrimiento : obtenga la huella y la información sobre el objetivo y los métodos de ataque que se pueden utilizar.
- Enumeración: realice análisis de puertos e identificación de recursos.
- Mapeo de vulnerabilidades: identifique las vulnerabilidades en los sistemas y recursos.
- Explotación: intente obtener acceso no autorizado aprovechando las vulnerabilidades.
- Informe - Informe de los resultados a la administración con contramedidas sugeridas.
- Descubrimiento : obtenga la huella y la información sobre el objetivo y los métodos de ataque que se pueden utilizar.
- Enumeración: realice análisis de puertos e identificación de recursos.
- Mapeo de vulnerabilidades: identifique las vulnerabilidades en los sistemas y recursos.
- Explotación: intente obtener acceso no autorizado aprovechando las vulnerabilidades.
- Informe - Informe de los resultados a la administración con contramedidas sugeridas.

Los pasos formales en la prueba de penetración son los siguientes:

1. Documente información sobre el sistema o dispositivo de destino. (Esto es descubrimiento.)
2. Recopilar información sobre los métodos de ataque contra el sistema o dispositivo de destino. Esto incluye la realización de análisis de puertos. (Esto es enumeración.)

3. Identificar las vulnerabilidades conocidas del sistema o dispositivo de destino. (Se trata de la asignación de vulnerabilidades).
4. Ejecutar ataques contra el sistema o dispositivo de destino para obtener acceso de usuario y con privilegios. (Esto es explotación.)
5. Documente los resultados de la prueba de penetración e informe de los hallazgos a la gerencia, con sugerencias para la acción correctiva. (Esto es informar).

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Recopilar datos de procesos de seguridad (por ejemplo, técnicos y administrativos)

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 6: Evaluación y pruebas de seguridad, pruebas de penetración

---

Pregunta #21 de 29

Id. de pregunta: 1192960

Está utilizando un analizador de red para supervisar el tráfico en la red. Un usuario informa de problemas para comunicarse con el servidor de archivos. Sospecha que el servidor de archivos es víctima de un ataque de denegación de servicio. Decide utilizar el analizador de red para determinar el problema.

¿Qué información debe examinar?

✗ **A)** captura de paquetes
✗ **B)** estadísticas de puertos
✓ **C)** estadísticas de la estación
✗ **D)** estadísticas de protocolo

explicación

Debe utilizar estadísticas de estación (dispositivo) para examinar la comunicación entre el equipo del usuario y el servidor de archivos. El tráfico de ambos equipos debe examinarse para determinar exactamente dónde se produce un error en la comunicación.

No debe utilizar estadísticas de protocolo porque no sabe qué protocolo, si existe, está causando el problema.

Usted no debe utilizar la información de la captura de paquetes porque ésta proporcionará la información sobre todos los paquetes. Usted sabe qué equipos son parte del problema. Por lo tanto, el examen de las estadísticas de las estaciones proporcionaría información más pertinente.

No debe utilizar estadísticas de puerto porque no sabe qué puerto, si existe, está causando el problema.

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Analizar la salida de la prueba y generar un informe

Referencias:

¿Qué es un Packet Sniffer?, HYPERLINK "https://www.lifewire.com/what-is-a-packet-sniffer-2487312" \t "sean" http://netsecurity.about.com/od/informationresources/a/What-Is-A-Packet-Sniffer.htm

---

Pregunta #22 de 29

Id. de pregunta: 1105380

¿Qué tipo de evaluación de vulnerabilidad tiene más probabilidades de demostrar el éxito o el fracaso de un posible ataque?

- ✓ **A)** prueba de doble anonimato
- ✗ **B)** prueba ciega
- ✗ **C)** prueba dirigida
- ✗ **D)** prueba de penetración

explicación

Es más probable que una prueba doble ciego demuestre el éxito o el fracaso de un posible ataque. En esta prueba, el equipo de seguridad de la red que se está probando NO conoce la prueba. Esta prueba evalúa cómo reacciona el equipo al ataque.

En una prueba ciega, el equipo de seguridad de la red que se está probando conoce la prueba. Los evaluadores sólo tienen información disponible públicamente en la red.

En una prueba específica, las pruebas se llevan a cabo en áreas o sistemas específicos.

En una prueba de penetración, la seguridad de un ordenador o red se prueba para descubrir vulnerabilidades y debilidades. Las pruebas a ciegas, las pruebas doble ciego y las pruebas específicas son tipos específicos de pruebas de penetración.

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Realizar pruebas de control de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 6: Evaluación y pruebas de seguridad, pruebas de penetración

---

Pregunta #23 de 29

Id. de pregunta: 1105375

¿Qué herramienta se utiliza para realizar una prueba de vulnerabilidad?

- ✗ **A)** prueba de penetración
- ✗ **B)** prueba de caja negra
- ✗ **C)** prueba de caja blanca
- ✓ **D)** herramienta de escaneo

explicación

Una herramienta de análisis se utiliza para realizar una prueba de vulnerabilidad. Una prueba de vulnerabilidad identifica las vulnerabilidades en una red. Una vez identificadas las vulnerabilidades, una prueba de penetración explota las vulnerabilidades identificadas para demostrar que la vulnerabilidad realmente existe.

Una prueba de penetración tiene varias formas de explotar las vulnerabilidades del sistema. Una prueba de caja blanca es una prueba de penetración donde el hacker ético se le da la red y los detalles del sistema para dirigirse mejor al ataque. Una prueba de caja negra se realiza "en la oscuridad", lo que significa que el hacker ético no tiene conocimiento previo de la red o sistema.

Una prueba de vulnerabilidad y una prueba de penetración NO son lo mismo. Una prueba de vulnerabilidad conduce a la prueba de penetración. Primero debe identificar las vulnerabilidades en la prueba de vulnerabilidad y, a continuación, intentar explotar las vulnerabilidades mediante una prueba de penetración.

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Realizar pruebas de control de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 6: Evaluación y pruebas de seguridad, Análisis de vulnerabilidades de red

---

Pregunta #24 de 29

Id. de pregunta: 1111760

Está definiendo e implementando un programa de supervisión continua de seguridad de la información (ISCM) para su organización de acuerdo con NIST SP 800-137. Actualmente está recopilando la información relacionada con la seguridad necesaria para métricas, evaluaciones e informes. ¿Qué paso de NIST SP 800-137 está completando?

✗ **A)** Establecer un programa ISCM.

✓ **B)** Implementar un programa ISCM.

✗ **C)** Definir una estrategia ISCM.

✗ **D)** Analice los datos recogidos, e informe los resultados.

explicación

Está completando el paso Implementar un programa ISCM de NIST SP 800-137. NIST SP 800-137 guía el desarrollo y proporciona información sobre el monitoreo continuo de seguridad de la información (ISCM) para sistemas de información y organizaciones federales. Define los siguientes pasos para establecer, implementar y mantener ISCM:

- Definir una estrategia ISCM.
- Establecer un programa ISCM.
- Implementar un programa ISCM.
- Analice los datos y divulgue los resultados.
- Responder a los hallazgos.
- Revisar y actualizar la estrategia y el programa de ISCM.

La definición de una estrategia iscm implica determinar la estrategia oficial de iscm de su organización. El establecimiento de un programa ISCM determina las métricas, el monitoreo y las frecuencias de evaluación además de la arquitectura ISCM. El análisis de los datos recopilados y los resultados de los informes determina cualquier problema e implementa la respuesta adecuada. Responder a los hallazgos implica implementar nuevos controles que aborden cualquier hallazgo que tenga. Revisar y actualizar el programa de monitoreo implica asegurarse de que el programa sigue siendo relevante y le permite realizar los cambios necesarios en el programa.

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Realizar pruebas de control de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 6: Evaluación y pruebas de seguridad, NIST SP 800-137

NIST SP 800-137, http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

Pregunta #25 de 29

Id. de pregunta: 1111757

Haga coincidir las herramientas de la izquierda con las descripciones dadas a la derecha.

{UCMS id=5721518380154880 type=Activity}

explicación

Las herramientas y sus descripciones deben coincidir de la siguiente manera:

- Wireshark - Analizador de protocolo de red
- Nessus - Escáner de vulnerabilidades
- Snort - Sistema de detección de intrusiones en la red
- Cain y Abel - Herramienta de recuperación de contraseña

Hay muchas herramientas que se pueden utilizar para administrar la seguridad y los componentes de red. Debe familiarizarse con la función que proporcionan las herramientas. Un buen lugar para comenzar es con la referencia proporcionada en la sección referencias de esta pregunta.

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Realizar pruebas de control de seguridad

Referencias:

CISSP Cert Guide (3rd Edition), Capítulo 6: Evaluación y pruebas de seguridad, realizar pruebas de control de seguridad

---

Pregunta #26 de 29

Id. de pregunta: 1105378

¿Qué herramienta NO es una aplicación de puerta trasera?

✗ **A)** Orificio trasero
✓ **B)** Nessus
✗ **C)** Paraíso de los Maestros
✗ **D)** NetBus

explicación

Nessus NO es una aplicación de puerta trasera. Es un escáner de vulnerabilidades de red.

Back Orifice, NetBus y Masters Paradise son aplicaciones de puerta trasera. Estas aplicaciones funcionan instalando una aplicación cliente en el equipo atacado y, a continuación, utilizando una aplicación remota para obtener acceso al equipo atacado.

Las puertas traseras también pueden ser mecanismos creados por los hackers para obtener acceso a la red en un momento posterior. Las puertas traseras son muy difíciles de rastrear, ya que un intruso a menudo creará varias vías en una red para ser explotadas más tarde. La única forma real de asegurarse de que estas vías se cierran después de un ataque es restaurar el sistema operativo desde el medio original, aplicar los parches y restaurar todos los datos y aplicaciones

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Realizar pruebas de control de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 6: Evaluación y pruebas de seguridad, Evaluación de vulnerabilidades

Nessus(http://www.nessus.org/nessus/

Información sobre Back Orifice y NetBus, http://www.symantec.com/avcenter/warn/backorifice.html

---

Pregunta #27 de 29

Id. de pregunta: 1113992

Usted ha sido contratado como ingeniero de seguridad para una nueva agencia del gobierno federal. Se le ha pedido que implemente un programa de monitoreo continuo de seguridad de la información (ISCM) para la agencia. ¿Qué estándar debe consultar?

- ✗ **A)** NIST SP 800-92
- ✗ **B)** NIST SP 800-121
- ✓ **C)** NIST SP 800-137
- ✗ **D)** NIST SP 800-53

explicación

Debe consultar a NIST SP 800-137 para obtener información sobre el monitoreo continuo de seguridad (ISCM) para organizaciones y sistemas de información federales. Este estándar define los siguientes pasos para establecer, implementar y mantener ISCM:

- Definir una estrategia ISCM.

- Establecer un programa ISCM.
- Implementar un programa ISCM.
- Analice los datos y divulgue los resultados.
- Responder a los hallazgos.
- Revisar y actualizar la estrategia y el programa de ISCM.

NIST SP 800-53 cubre los controles de seguridad y privacidad para los sistemas de información y organizaciones federales. NIST SP 800-92 cubre las directrices para la administración de registros de seguridad informática. NIST SP 800-121 cubre las directrices para la seguridad Bluetooth.

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Realizar pruebas de control de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 6: Evaluación y pruebas de seguridad, NIST SP 800-137

NIST SP 800-137, http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

---

Pregunta #28 de 29

Id. de pregunta: 1105393

Debe proporcionar informes SOC 2 y SOC 3 sobre la seguridad, disponibilidad, confidencialidad, integridad del procesamiento y privacidad de los controles operativos. Como parte de estos informes, debe proporcionar información sobre la copia de seguridad y restauración de datos. ¿A qué principio de SOC 2 y SOC 3 se aplica esta información?

✗ **A)** privacidad
✗ **B)** confidencialidad
✓ **C)** disponibilidad
✗ **D)** seguridad

explicación

La copia de seguridad y restauración de datos se aplica al principio de disponibilidad de los informes SOC 2 y SOC 3. La disponibilidad también incluye controles ambientales, recuperación ante desastres, continuidad del negocio y proceso de disponibilidad.

La privacidad incluye la administración, el aviso de privacidad, las recopilaciones de datos, el uso y la retención de datos, el acceso a los datos, la divulgación de datos a terceros, la calidad de los datos y el monitoreo y la aplicación.

La seguridad incluye la política de seguridad de TI, el conocimiento de la seguridad, la evaluación de riesgos, el acceso lógico y físico, la supervisión de la seguridad, la autenticación de usuarios, la administración de incidentes, la clasificación de activos, la seguridad del personal y otros temas.

La confidencialidad incluye la política de confidencialidad, la confidencialidad de entrada, la confidencialidad del procesamiento de datos, la confidencialidad de la salida, la divulgación de información y la confidencialidad del desarrollo de sistemas.

Objetivo:
Evaluación y pruebas de seguridad

Subobsecución:
Realizar o facilitar auditorías de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 6: Evaluación y pruebas de seguridad, realizar auditorías

---

Pregunta #29 de 29

Id. de pregunta: 1105391

Se le ha pedido que administre el programa de monitoreo continuo de seguridad de la información (ISCM) de su empresa. ¿Cuál de las siguientes afirmaciones con respecto a los informes automatizados frente a los manuales es FALSE?

✗ **A)** Las herramientas automatizadas reconocen patrones y relaciones que pueden escapar a la atención de los analistas humanos o al monitoreo manual.

✓ **B)** Las herramientas manuales son más exhaustivas en sus informes que los métodos automatizados.

✗ **C)** Las herramientas automatizadas mejoran la fiabilidad de la supervisión de la información relacionada con la seguridad.

✗ **D)** Las herramientas automatizadas reducen los costos de monitoreo de la información relacionada con la seguridad.

explicación

Las herramientas manuales NO son más exhaustivas en sus informes que los métodos automatizados.

Todas las demás afirmaciones son ciertas. Las herramientas automatizadas reconocen patrones y relaciones que pueden escapar a la atención de los analistas humanos o al monitoreo manual. Las herramientas automatizadas reducen los costos y mejoran la confiabilidad de la supervisión de la información relacionada con la seguridad.

Objetivo:

Evaluación y pruebas de seguridad

Subobsecución:

Realizar o facilitar auditorías de seguridad

Referencias:

Cissp Cert Guide (3rd Edition), Capítulo 6: Evaluación y pruebas de seguridad, NIST SP 800-137