Capítulo 6 - Evaluación y Pruebas de Seguridad

En este capítulo se tratan los siguientes temas:

- **Diseñar y validar estrategias de evaluación, prueba y auditoría:** explica el uso de estrategias de evaluación, prueba y auditoría, incluidas las estrategias internas, externas y de terceros.
- **Realizar pruebas de control de seguridad:** Los conceptos discutidos incluyen el proceso de pruebas de control de seguridad, incluidas las evaluaciones de vulnerabilidad, las pruebas de penetración, las revisiones de registros, las transacciones sintéticas, la revisión y las pruebas de código, las pruebas de casos de mal uso, el análisis de cobertura de pruebas y las pruebas de interfaz.
- **Recopilar datos de procesos de seguridad:** Los conceptos discutidos incluyen NIST SP 800-137, administración de cuentas, revisión y aprobación de la administración, indicadores clave de rendimiento y riesgo, datos de verificación de copias de seguridad, capacitación y concientización, y recuperación ante desastres y continuidad del negocio.
- **Analizar e informar de las salidas de las pruebas:** explica la importancia de analizar y notificar las salidas de las pruebas, incluidos los informes automáticos y manuales.
- **Realizar o facilitar auditorías de seguridad:** describe los procesos de auditoría internos, externos y de terceros y los tres tipos de informes SOC.

La evaluación y las pruebas de seguridad abarcan el diseño, la realización y el análisis de pruebas de seguridad. Los profesionales de la seguridad deben comprender estos procesos para proteger sus activos de los ataques.

La evaluación y las pruebas de seguridad requieren una serie de métodos de prueba para determinar las vulnerabilidades y los riesgos de una organización. Ayuda a una organización a administrar los riesgos en la planificación, implementación, operación y mantenimiento de sistemas y procesos. Su objetivo es identificar cualquier deficiencia técnica, operativa y del sistema al principio del proceso, antes de que se implementen esas deficiencias. Cuanto antes pueda descubrir esas deficiencias, más barato será solucionarlas.

En este capítulo se describen las estrategias de evaluación y pruebas, las pruebas de control de seguridad, la recopilación de datos de procesos de seguridad, el análisis y la generación de informes de resultados de pruebas y auditorías internas, externas y de terceros.

Tabla de Contenidos

Diseñar y validar estrategias de evaluación y pruebas

Los profesionales de la seguridad deben asegurarse de que su organización planifica, diseña, ejecuta y valida las estrategias adecuadas de evaluación, prueba y auditoría de seguridad para garantizar que se mitigan los riesgos. Los profesionales de la seguridad deben asumir un papel de liderazgo para ayudar a la organización a implementar las estrategias adecuadas de evaluación, pruebas y auditoría de seguridad. La organización debe basarse en las mejores prácticas de la industria, las normas nacionales e internacionales y las prácticas y directrices recomendadas por los proveedores para garantizar que las estrategias se planifiquen e implementen adecuadamente.

Lo más probable es que las organizaciones establezcan un equipo que sea responsable de ejecutar cualquier evaluación, prueba y estrategias de auditoría. El equipo debe estar formado por personas que entiendan la evaluación de la seguridad, las pruebas y la auditoría, pero también debe incluir representantes de otras áreas de la organización. La comprobación y validación de la seguridad es una actividad continua que nunca se detiene realmente. Pero los profesionales de la seguridad deben ayudar a guiar a una organización en términos de cuándo se realiza mejor un tipo particular de evaluación o prueba.

Pruebas de seguridad

Las pruebas de seguridad garantizan que un control funciona correctamente. Se pueden realizar pruebas de seguridad manuales y automáticas. Las pruebas de seguridad deben llevarse a cabo de forma regular. Las pruebas de seguridad deben realizarse en todos los tipos de dispositivos.

Al realizar pruebas de seguridad, los profesionales de la seguridad deben comprender que afectará al rendimiento de los dispositivos implicados en la prueba de seguridad. Las pruebas de seguridad no siempre se pueden realizar durante las horas no pico. Solo realizar esta prueba durante las horas no pico también podría resultar en resultados sesgados.

Los profesionales de la seguridad deben tener en cuenta los siguientes factores al realizar pruebas de seguridad:

- impacto
- dificultad
- Tiempo necesario
- Cambios que podrían afectar al rendimiento
- Riesgo del sistema
- Criticidad del sistema
- Disponibilidad de las pruebas de seguridad
- Nivel de sensibilidad de la información
- Probabilidad de fallo técnico o mala configuración

Una vez realizadas las pruebas de seguridad, los profesionales de la seguridad deben analizar los resultados y hacer las recomendaciones adecuadas en función de esos resultados. Además, las propias herramientas de pruebas de seguridad se pueden configurar para enviar alertas o mensajes basados en desencadenadores o filtros preconfigurados. Sin un análisis adecuado, las pruebas de seguridad no proporcionan un beneficio a la organización.

Evaluaciones de seguridad

Las evaluaciones de seguridad son las revisiones del estado de seguridad y los informes de un sistema, aplicación u otro entorno. Durante esta evaluación, un profesional de la seguridad revisará los resultados de las pruebas de seguridad, identificará las vulnerabilidades y hará recomendaciones para la corrección. Las pruebas de seguridad conducen a evaluaciones de seguridad.

Los profesionales de la seguridad deben preparar un informe formal de evaluación de la seguridad que incluya todos los problemas y recomendaciones identificados. Además, deben documentar las medidas adoptadas sobre la base de las recomendaciones.

Auditoría de seguridad

La auditoría de seguridad es el proceso de proporcionar la prueba digital cuando alguien que está realizando ciertas actividades necesita ser identificado. Al igual que la evaluación y las pruebas de seguridad, se pueden realizar internamente, externamente y a través de un tercero. La auditoría de seguridad se trata con más detalle más adelante en este capítulo y en el capítulo 7,"Operacionesde seguridad".

Evaluación, pruebas y auditoría de seguridad interna, externa y de terceros

La evaluación, las pruebas y la auditoría de seguridad se realizan de tres maneras: interna, externa y de terceros. La evaluación interna, las pruebas y la auditoría son llevadas a cabo por el personal de la organización. La evaluación externa, las pruebas y la auditoría son llevadas a cabo por un proveedor o contratista contratado por la empresa.

A veces, la evaluación, las pruebas y la auditoría de terceros son realizadas por una parte que no tiene nada que ver con la empresa y que no ha participado previamente por ella. Este escenario a menudo surge como resultado de tener que cumplir con alguna norma o regulación o cuando se trata de acreditación o certificación. Muchos organismos de certificación o regulación pueden requerir la contratación de un tercero que no ha tenido una relación previa con la organización que se está evaluando. En este caso, el organismo certificador trabajará con la organización para contratar a un tercero aprobado.

Las empresas deben asegurarse de que, como mínimo, las pruebas y evaluaciones internas y externas se completen de forma regular.

Realizar pruebas de control de seguridad

Las organizaciones deben administrar las pruebas de control de seguridad que se producen para garantizar que todas las personas autorizadas prueben exhaustivamente todos los controles de seguridad. Las facetas de las pruebas de control de seguridad que las organizaciones deben incluir son las evaluaciones de vulnerabilidad, las pruebas de penetración, las revisiones de registros, las transacciones sintéticas, la revisión y las pruebas de código, las pruebas de casos de uso indebido, el análisis de cobertura de pruebas y las pruebas de interfaz.

Evaluación de vulnerabilidades

Una evaluación de vulnerabilidad ayuda a identificar las áreas de debilidad en una red. También puede ayudar a determinar la priorización de activos dentro de una organización. Una evaluación integral de la vulnerabilidad es parte del proceso de gestión de riesgos. Pero para el control de acceso, los profesionales de la seguridad deben usar evaluaciones de vulnerabilidad que se dirijan específicamente a los mecanismos de control de acceso.

Las evaluaciones de vulnerabilidad suelen dividirse en una de estas tres categorías:

- **Pruebas de personal:** revisa las prácticas y procedimientos estándar que siguen los usuarios.
- **Pruebas físicas:** Revisa las protecciones de las instalaciones y el perímetro.
- **Pruebas del sistema y de la red:** revisa los sistemas, los dispositivos y la topología de red.

El analista de seguridad que va a realizar una evaluación de vulnerabilidad debe comprender los sistemas y dispositivos que están en la red y los trabajos que realizan. El analista necesita esta información para poder evaluar las vulnerabilidades de los sistemas y dispositivos en función de las amenazas conocidas y potenciales para los sistemas y dispositivos.

Después de obtener conocimientos sobre los sistemas y dispositivos, el analista de seguridad debe examinar los controles existentes en su lugar e identificar cualquier amenaza contra estos controles. A continuación, el analista de seguridad puede utilizar toda la información recopilada para determinar qué herramientas automatizadas utilizar para buscar vulnerabilidades. Una vez completado el análisis de vulnerabilidades, el analista de seguridad debe comprobar los resultados para asegurarse de que son precisos y, a continuación, informar de los hallazgos a la administración, con sugerencias de medidas correctivas. Con esta información en la mano, el analista debe llevar a cabo el modelado de amenazas para identificar las amenazas que podrían afectar negativamente a los sistemas y dispositivos y los métodos de ataque que podrían utilizarse.

Las aplicaciones de evaluación de vulnerabilidades incluyen Nessus, Open Vulnerability Assessment System (OpenVAS), Core Impact, Nexpose, GFI LanGuard, QualysGuard y Microsoft Baseline Security Analyzer (MBSA). De estas aplicaciones, OpenVAS y MBSA son gratuitas.

Al seleccionar una herramienta de evaluación de vulnerabilidades, debe investigar las siguientes métricas: precisión, confiabilidad, escalabilidad e informes. La precisión es la métrica más importante. Un falso positivo generalmente resulta en tiempo dedicado a investigar un problema que no existe. Un falso negativo es más grave, ya que significa que el analizador no pudo identificar un problema que supone un riesgo de seguridad grave.

Análisis de detección de redes

Un examen de detección de red examina un intervalo de direcciones IP para determinar qué puertos están abiertos. Este tipo de análisis sólo muestra una lista de los sistemas de la red y los puertos en uso en la red. En realidad, no comprueba si hay vulnerabilidades.

La detección de topología implica determinar los dispositivos de la red, sus relaciones de conectividad entre sí y el esquema de direccionamiento IP interno en uso. Cualquier combinación de estas piezas de información permite a un hacker crear un "mapa" de la red, lo que le ayuda enormemente a evaluar e interpretar los datos que recopila en otras partes del proceso de piratería. Si tiene éxito completo, terminará con un diagrama de la red. Su desafío como profesional de la seguridad es determinar si este tipo de proceso de asignación es posible, utilizando las mismas herramientas que el atacante. En función de sus hallazgos, debe determinar los pasos a seguir para hacer que la detección de topología sea más difícil o, mejor aún, imposible.

La huella digital del sistema operativo es el proceso de usar algún método para determinar el sistema operativo que se ejecuta en un host o un servidor. Al identificar la versión del sistema operativo y el número de compilación, un hacker puede identificar vulnerabilidades comunes de ese sistema operativo utilizando documentación fácilmente disponible de Internet. Aunque muchos de los problemas se habrán solucionado en actualizaciones, Service Packs y revisiones posteriores, puede haber debilidades de día cero (problemas que no han sido ampliamente publicitados o abordados por el proveedor) que el hacker puede aprovechar en el ataque. Además, si no se ha aplicado alguno de los parches de seguridad relevantes, las debilidades que los parches estaban destinados a abordar existirán en la máquina. Por lo tanto, el propósito de intentar la huella digital del sistema operativo durante la evaluación es evaluar la facilidad relativa con la que se puede hacer e identificar métodos para hacerlo más difícil.

Los sistemas operativos tienen vulnerabilidades bien conocidas, al igual que los servicios comunes. Al determinar los servicios que se ejecutan en un sistema, un atacante también descubre posibles vulnerabilidades del servicio de las que puede intentar aprovecharse. Esto se hace típicamente con una exploración del puerto, en la cual se identifican todos los puertos "abiertos, " o "que escuchan." Una vez más, la mayor parte de estos problemas se habrá mitigado con los parches de seguridad adecuados, pero no siempre es así; no es raro que los analistas de seguridad descubran que a los sistemas que ejecutan servicios vulnerables les faltan los parches

de seguridad pertinentes. Por consiguiente, al realizar la detección de servicios, compruebe los parches en los sistemas que se encuentre que tienen puertos abiertos. También es recomendable cerrar los puertos no necesarios para que el sistema haga su trabajo.

Las herramientas de detección de redes pueden realizar los siguientes tipos de análisis:

- **Exploración TCP SYN:** Envía un paquete a cada puerto escaneado con el indicador SYN establecido. Si se recibe una respuesta con los indicadores SYN y ACK establecidos, el puerto está abierto.
- **Análisis de confirmación TCP:** envía un paquete a cada puerto con el indicador de confirmación establecido. Si no se recibe ninguna respuesta, después el puerto se marca como filtrado. Si se recibe una respuesta RST, el puerto se marca como sin filtrar.
- **Exploración de Navidad:** Envía un paquete con los indicadores FIN, PSH y URG establecidos. Si el puerto está abierto, no hay respuesta. Si se cierra el puerto, el destino responde con un paquete RST/ACK.

El resultado de este tipo de análisis es que los profesionales de la seguridad pueden determinar si los puertos están abiertos, cerrados o filtrados. Los puertos abiertos están siendo utilizados por una aplicación en el sistema remoto. Los puertos cerrados son puertos abiertos, pero no hay ninguna aplicación que acepte conexiones en ese puerto. Los puertos filtrados son puertos a los que no se puede llegar.

La herramienta de escaneo de descubrimiento de red más utilizada es Nmap.

Análisis de vulnerabilidades de red

Los análisis de vulnerabilidades de red realizan un análisis más complejo de la red que los análisis de detección de red. Estos análisis sondearán un sistema o red de destino para identificar vulnerabilidades. Las herramientas utilizadas en este tipo de análisis contendrán una base de datos de vulnerabilidades conocidas e identificarán si existe una vulnerabilidad específica en cada dispositivo.

Hay dos tipos de escáneres de vulnerabilidades:

- **Analizadores de vulnerabilidades pasivas:** un analizador de vulnerabilidades pasivas (PVS) supervisa el tráfico de red en la capa de paquetes para determinar la topología, los servicios y las vulnerabilidades. Evita la inestabilidad que se puede introducir en un sistema mediante la exploración activa de vulnerabilidades.

  Las herramientas PVS analizan el flujo de paquetes y buscan vulnerabilidades a través del análisis directo. Se implementan de la misma manera que los sistemas de detección de intrusiones (IDS) o los analizadores de paquetes. Un PVS puede elegir una sesión de red que se dirige a un servidor protegido y supervisarla tanto como sea necesario. El mayor beneficio de un PVS es su capacidad para hacer su trabajo sin afectar la red monitoreada.

Algunos ejemplos de PVSs son el Nessus Network Monitor (anteriormente Tenable PVS) y NetScanTools Pro.

- **Escáneres de vulnerabilidades activas:** mientras que los escáneres pasivos solo pueden recopilar información, los escáneres de vulnerabilidades activas (AVS) pueden tomar medidas para bloquear un ataque, como bloquear una dirección IP peligrosa. También se pueden utilizar para simular un ataque para evaluar la preparación. Funcionan enviando transmisiones a nodos y examinando las respuestas. Debido a esto, estos escáneres pueden interrumpir el tráfico de red. Algunos ejemplos son Nessus y Microsoft Baseline Security Analyzer (MBSA).

Independientemente de si es activo o pasivo, un escáner de vulnerabilidades no puede reemplazar la experiencia del personal de seguridad capacitado. Además, estos escáneres sólo son tan eficaces como las bases de datos de firmas de las que dependen, por lo que las bases de datos deben actualizarse periódicamente. Por último, los analizadores requieren ancho de banda y pueden ralentizar la red.

Para obtener el mejor rendimiento, puede colocar un analizador de vulnerabilidades en una subred que deba protegerse. También puede conectar un analizador a través de un cortafuegos a varias subredes; esto complica la configuración y requiere la apertura de puertos en el firewall, lo que podría ser problemático y podría afectar el rendimiento del firewall.

Las herramientas de análisis de vulnerabilidades de red más populares incluyen Qualys, Nessus y MBSA.

Los analizadores de vulnerabilidades pueden utilizar agentes instalados en los dispositivos o pueden no tener agentes. Mientras que muchos vendedores argumentan que el uso de agentes es siempre mejor, hay ventajas y desventajas de ambos, como se presenta en la Tabla 6-1.

Tabla 6-1 Análisis basado en servidor frente a análisis basado en agente

tipo	Tecnología	características
		Puede obtener información de máquinas desconectadas o máquinas en la DMZ
Basado en agentes	Tecnología pull	Ideal para ubicaciones remotas que tienen un ancho de banda limitado
		Menos dependiente de la conectividad de red
		Basado en políticas definidas en la consola central

tipo	Tecnología	características
		Bueno para redes con ancho de banda abundante
Basado en servidor	Tecnología Push	Depende de la conectividad de red
		La autoridad central realiza todo el análisis y la implementación

Algunos analizadores pueden realizar análisis basados en agentes y en servidores (también denominados análisis sin agentes o basados en sensores).

Análisis de vulnerabilidades de aplicaciones web

Debido a que las aplicaciones web son muy utilizadas en el mundo actual, las empresas deben asegurarse de que sus aplicaciones web permanezcan seguras y libres de vulnerabilidades. Los analizadores de vulnerabilidades de aplicaciones web son herramientas especiales que examinan las aplicaciones web en busca de vulnerabilidades conocidas.

Los escáneres de vulnerabilidades de aplicaciones web populares incluyen QualysGuard y Nexpose.

Pruebas de penetración

El objetivo de las pruebas de penetración, también conocidas como hacking ético, es simular un ataque para identificar cualquier amenaza que pueda provenir de recursos internos o externos que planean explotar las vulnerabilidades de un sistema o dispositivo.

Los pasos para realizar una prueba de penetración son los siguientes:

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

Se deben realizar pruebas internas y externas. Las pruebas internas se producen desde dentro de la red, mientras que las pruebas externas se originan fuera de la red y se dirigen a los servidores y dispositivos que son visibles públicamente.

Las estrategias para las pruebas de penetración se basan en los objetivos de prueba definidos por la organización. Entre las estrategias con las que debe estar familiarizado se incluyen las siguientes:

- **Prueba ciega:** El equipo de pruebas tiene un conocimiento limitado de los sistemas y dispositivos de red que utilizan información disponible públicamente. El equipo de seguridad de la organización sabe que se avecina un ataque. Esta prueba requiere más esfuerzo por parte del equipo de pruebas, y el equipo debe simular un ataque real.
- **Prueba doble ciego:** Esta prueba es como una prueba ciega, excepto que el equipo de seguridad de la organización *no* sabe que se avecina un ataque. Solo unas pocas personas de la organización conocen el ataque y no comparten esta información con el equipo de seguridad. Esta prueba normalmente requiere el mismo esfuerzo tanto para el equipo de pruebas como para el equipo de seguridad de la organización.
- **Prueba de destino:** tanto el equipo de pruebas como el equipo de seguridad de la organización reciben la máxima información sobre la red y el tipo de ataque que se producirá. Esta es la prueba más fácil de completar, pero no proporciona una imagen completa de la seguridad de la organización.

Las pruebas de penetración también se dividen en categorías basadas en la cantidad de información que se proporcionará. Las principales categorías con las que debe estar familiarizado son las siguientes:

- **Prueba de conocimiento cero:** El equipo de pruebas no tiene conocimientos sobre la red de la organización. El equipo de pruebas puede utilizar cualquier medio disponible para obtener información sobre la red de la organización. Esto también se conoce como pruebas cerradas o de caja negra.
- **Prueba de conocimiento parcial:** El equipo de pruebas se proporciona con conocimiento público sobre la red de la organización. Se pueden establecer límites para este tipo de prueba. Esto también se conoce como prueba de caja gris.
- **Prueba de conocimiento completo:** El equipo de pruebas se proporciona con todos los conocimientos disponibles con respecto a la red de la organización. Esta prueba se centra más en qué ataques se pueden llevar a cabo. Esto también se conoce como prueba de caja blanca.

Las aplicaciones de pruebas de penetración incluyen Metasploit, Wireshark, Core Impact, Nessus, Cain & Abel, Kali Linux y John the Ripper. Al seleccionar una herramienta de prueba de penetración, primero debe determinar qué sistemas desea probar. A continuación, investigue las diferentes herramientas para descubrir cuáles pueden realizar las pruebas que desea realizar para esos sistemas e investigue las metodologías de las herramientas para las pruebas. Además, la

organización necesita seleccionar a la persona correcta para llevar a cabo la prueba. Recuerde que las pruebas de penetración deben incluir métodos manuales, así como métodos automatizados porque confiar en solo uno de estos dos no producirá un resultado completo.

En el cuadro 6-2 se comparan las evaluaciones de vulnerabilidad y las pruebas de penetración.

Cuadro 6-2 Comparación de las evaluaciones de vulnerabilidad y las pruebas de penetración

	Evaluación de vulnerabilidades	Prueba de penetración
propósito	Identifica las vulnerabilidades que pueden poner en peligro un sistema.	Identifica formas de aprovechar las vulnerabilidades para eludir las características de seguridad de los sistemas.
cuando	Después de cambios significativos en el sistema. Programe al menos trimestralmente a partir de entonces.	Después de cambios significativos en el sistema. Programe al menos una vez al año a partir de entonces.
cómo	Utilice herramientas automatizadas con verificación manual de los problemas identificados.	Utilice métodos automatizados y manuales para proporcionar un informe completo.
Informes	Riesgos potenciales planteados por vulnerabilidades conocidas, clasificadas utilizando las puntuaciones base asociadas con cada vulnerabilidad. Deben proporcionarse informes internos y externos.	Descripción de cada problema descubierto, incluidos los riesgos específicos que el problema puede plantear y específicamente cómo y en qué medida puede ser explotado.
duración	Normalmente, de varios segundos a varios minutos por host analizado.	Días o semanas, dependiendo del alcance y tamaño del entorno a probar. Las pruebas pueden crecer en duración si los esfuerzos descubren un alcance adicional.

Registrar revisiones

Un *registro* es un registro de eventos que se producen en un activo de la organización, incluidos sistemas, redes, dispositivos e instalaciones. Cada entrada de un registro cubre un único evento que se produce en el activo. En la mayoría de los casos, hay registros independientes para diferentes tipos de eventos, incluidos los registros de seguridad, los registros del sistema operativo y los registros de aplicación. Debido a que se generan tantos registros en un solo dispositivo, muchas organizaciones tienen problemas para garantizar que los registros se revisen de manera oportuna. Sin embargo, la revisión del registro es probablemente uno de los pasos más importantes que una organización puede seguir para asegurarse de que los problemas se detectan antes de que se conviertan en problemas importantes.

Los registros de seguridad informática son especialmente importantes porque pueden ayudar a una organización a identificar incidentes de seguridad, infracciones de directivas y fraudes. La administración de registros garantiza que los registros de seguridad informática se almacenen con suficiente detalle durante un período de tiempo adecuado para que se puedan identificar auditorías, análisis forenses, investigaciones, líneas de base, tendencias y problemas a largo plazo.

El Instituto Nacional de Estándares y Tecnología (NIST) ha proporcionado dos publicaciones especiales relacionadas con la administración de registros: NIST SP 800-92, "Guide to Computer Security Log Management" y NIST SP 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations". Si bien ambas publicaciones especiales son utilizadas principalmente por agencias y organizaciones del gobierno federal, es posible que otras organizaciones quieran usarlas también debido a la gran cantidad de información que proporcionan. La siguiente sección cubre NIST SP 800-92 y NIST SP 800-137 se describe más adelante en este capítulo.

NIST SP 800-92

NIST SP 800-92 hace las siguientes recomendaciones para una administración de registros más eficiente y eficaz:

- Las organizaciones deben establecer directivas y procedimientos para la administración de registros. Como parte del proceso de planificación, una organización debe
    - Defina sus requisitos y objetivos de registro.
    - Desarrollar directivas que definan claramente los requisitos obligatorios y las recomendaciones sugeridas para las actividades de administración de registros.
    - Asegúrese de que las directivas y procedimientos relacionados incorporen y admitan los requisitos y recomendaciones de administración de registros.
- La administración debe proporcionar el apoyo necesario para los esfuerzos relacionados con la planificación de la administración de registros, la política y el desarrollo de procedimientos.
- Las organizaciones deben priorizar la administración de registros de forma adecuada en toda la organización.
- Las organizaciones deben crear y mantener una infraestructura de administración de registros.
- Las organizaciones deben proporcionar el apoyo adecuado a todo el personal con responsabilidades de gestión de registros.
- Las organizaciones deben establecer procesos operativos de administración de registros estándar. Esto incluye asegurarse de que los administradores
    - Supervise el estado de registro de todos los orígenes de registro.
    - Supervise la rotación de registros y los procesos de archivo.
    - Compruebe si hay actualizaciones y parches para el software de registro y adquirirlos, probarlos e implementarlos.

- Asegúrese de que el reloj de cada host de registro esté sincronizado con un origen de hora común.
- Vuelva a configurar el registro según sea necesario en función de los cambios de política, los cambios tecnológicos y otros factores.
- Documente e informe anomalías en la configuración, las configuraciones y los procesos del registro.

Según NIST SP 800-92, los componentes comunes de la infraestructura de administración de registros incluyen funciones generales (análisis de registros, filtrado de eventos y agregación de eventos), almacenamiento (rotación de registros, archivado de registros, reducción de registros, conversión de registros, normalización de registros y comprobación de integridad de archivos de registro), análisis de registros (correlación de eventos, visualización de registros e informes de registros) y eliminación de registros (eliminación de registros).

Syslog proporciona un marco simple para la generación, el almacenamiento y la transferencia de entradas de registro que cualquier sistema operativo, software de seguridad o aplicación podría usar si está diseñado para ello. Muchas fuentes de registro utilizan syslog como su formato de registro nativo u ofrecen características que permiten que sus formatos de registro se conviertan al formato syslog. Cada mensaje de Syslog tiene solamente tres porciones. La primera parte especifica la facilidad y la gravedad como valores numéricos. La segunda parte del mensaje contiene una marca de tiempo y el nombre de host o la dirección IP del origen del registro. La tercera parte es el contenido real del mensaje de registro.

No se definen campos estándar dentro del contenido del mensaje; está destinado a ser legible por el ser humano y no fácilmente analizable por máquina. Esto proporciona una flexibilidad muy alta para los generadores de registros, que pueden colocar cualquier información que consideren importante dentro del campo de contenido, pero hace que el análisis automatizado de los datos de registro sea muy difícil. Una sola fuente puede utilizar muchos formatos diferentes para su contenido de mensaje de registro, por lo que un programa de análisis tendría que estar familiarizado con cada formato y ser capaz de extraer el significado de los datos dentro de los campos de cada formato. Este problema se vuelve mucho más difícil cuando muchos orígenes generan mensajes de registro. Es posible que no sea factible comprender el significado de todos los mensajes de registro, por lo que el análisis podría limitarse a las búsquedas de palabras clave y patrones. Algunas organizaciones diseñan sus infraestructuras syslog para que tipos similares de mensajes se agrupen o se asignen códigos similares, lo que puede hacer que la automatización del análisis de registros sea más fácil de realizar.

Como la seguridad del registro se ha convertido en una mayor preocupación, se han creado varias implementaciones de syslog que ponen mayor énfasis en la seguridad. La mayoría se han basado en rfc 3195 de IETF, que fue diseñado específicamente para mejorar la seguridad de syslog. Las implementaciones basadas en este estándar pueden admitir la confidencialidad, integridad y disponibilidad de registros a través de varias características, incluida la entrega confiable de registros, la protección de confidencialidad de transmisión y la protección y autenticación de integridad de transmisión.

Los productos de gestión de eventos e información de seguridad (SIEM) permiten a los administradores consolidar todos los registros de información de seguridad. Esta consolidación garantiza que los administradores puedan realizar análisis en todos los registros de un único recurso en lugar de tener que analizar cada registro de su recurso independiente. La mayoría de los productos SIEM admiten dos formas de recopilar registros de generadores de registros:

- **Sin agente:** El servidor SIEM recibe datos de los hosts individuales sin necesidad de tener ningún software especial instalado en esos hosts. Algunos servidores extraen registros de los hosts, lo que normalmente se hace haciendo que el servidor se autentique en cada host y recupere sus registros con regularidad. En otros casos, los hosts insertan sus registros en el servidor, lo que generalmente implica que cada host se autentique en el servidor y transfiera sus registros regularmente. Independientemente de si los registros se insertan o se extraen, el servidor realiza el filtrado y la agregación de eventos y la normalización y el análisis de registros en los registros recopilados.
- **Basado en agente:** se instala un programa de agente en el host para realizar el filtrado de eventos y la agregación y normalización de registros para un tipo determinado de registro. A continuación, el host transmite los datos de registro normalizados al servidor SIEM, normalmente en tiempo real o casi en tiempo real para su análisis y almacenamiento. Es posible que sea necesario instalar varios agentes si un host tiene varios tipos de registros de interés. Algunos productos SIEM también ofrecen agentes para formatos genéricos como syslog y Simple Network Management Protocol (SNMP). Un agente genérico se utiliza principalmente para obtener datos de registro de un origen para el que no están disponibles un agente específico del formato y un método sin agente. Algunos productos también permiten a los administradores crear agentes personalizados para gestionar orígenes de registro no compatibles.

Hay ventajas y desventajas de cada método. La principal ventaja del enfoque sin agente es que no es necesario instalar, configurar y mantener los agentes en cada host de registro. La principal desventaja es la falta de filtrado y agregación en el nivel de host individual, lo que puede hacer que se transfieran cantidades significativamente mayores de datos a través de redes y aumentar la cantidad de tiempo que se tarda en filtrar y analizar los registros. Otra desventaja potencial del método sin agente es que el servidor SIEM puede necesitar credenciales para autenticarse en cada host de registro. En algunos casos, sólo uno de los dos métodos es factible; por ejemplo, es posible que no haya forma de recopilar registros de forma remota de un host determinado sin instalar un agente en él.

Los productos SIEM generalmente incluyen soporte para varias docenas de tipos de fuentes de registro, como sistemas operativos, software de seguridad, servidores de aplicaciones (por ejemplo, servidores web, servidores de correo electrónico) e incluso dispositivos de control de seguridad física como lectores de insignias. Para cada tipo de origen de registro compatible, excepto para formatos genéricos como syslog, los productos SIEM normalmente saben cómo categorizar los campos registrados más importantes. Esto mejora significativamente la normalización, el análisis y la correlación de los datos de registro sobre los realizados por el software con una comprensión menos granular de orígenes y formatos de registro específicos. Además, el software SIEM puede realizar la reducción de eventos al ignorar los campos de datos

que no son significativos para la seguridad informática, lo que potencialmente reduce el ancho de banda de red y el uso de almacenamiento de datos del software SIEM.

Normalmente, los administradores de sistemas, redes y seguridad son responsables de administrar el registro en sus sistemas, realizar análisis periódicos de sus datos de registro, documentar y notificar los resultados de sus actividades de administración de registros y garantizar que los datos de registro se proporcionen a la infraestructura de administración de registros de acuerdo con las directivas de la organización. Además, algunos de los administradores de seguridad de la organización actúan como administradores de infraestructura de administración de registros, con responsabilidades como las siguientes:

- Póngase en contacto con los administradores de nivel de sistema para obtener información adicional sobre un evento o para solicitar que investiguen un evento determinado.
- Identifique los cambios necesarios en las configuraciones de registro del sistema (por ejemplo, qué entradas y campos de datos se envían a los servidores de registro centralizados, qué formato de registro se debe utilizar) e informe a los administradores de nivel de sistema de los cambios necesarios.
- Iniciar respuestas a eventos, incluido el manejo de incidentes y problemas operativos (por ejemplo, un error de un componente de infraestructura de administración de registros).
- Asegúrese de que los datos de registro antiguos se archivan en medios extraíbles y se eliminan correctamente una vez que ya no son necesarios.
- Cooperar con las solicitudes de asesores legales, auditores y otros.
- Supervise el estado de la infraestructura de administración de registros (por ejemplo, fallas en el software de registro o en los medios de archivo de registros, fallas de los sistemas locales para transferir sus datos de registro) e inicie las respuestas adecuadas cuando se produzcan problemas.
- Pruebe e implemente actualizaciones y actualizaciones en los componentes de la infraestructura de administración de registros.
- Mantener la seguridad de la infraestructura de administración de registros.

Las organizaciones deben elaborar políticas que definan claramente los requisitos obligatorios y las recomendaciones sugeridas para varios aspectos de la administración de registros, incluida la generación de registros, la transmisión de registros, el almacenamiento y eliminación de registros y el análisis de registros. En la tabla 6-3 se proporcionan ejemplos de las opciones de configuración de registro que puede usar una organización. Los tipos de valores definidos en la Tabla 6-3 sólo deben aplicarse a los hosts y componentes de host especificados previamente por la organización como los que deben o deben registrar eventos relacionados con la seguridad.

Tabla 6-3 Ejemplos de opciones de configuración de registro

categoría	Sistemas de bajo impacto	Sistemas de impacto moderado	Sistemas de alto impacto
Duración de la retención de registros	1–2 semanas	1–3 meses	3–12 meses
Rotación de registros	Opcional (si se realiza, al menos cada semana o cada 25 MB)	Cada 6–24 horas o cada 2–5 MB	Cada 15–60 minutos o cada 0,5–1.0 MB
Frecuencia de transferencia de datos de registro (a SIEM)	Cada 3–24 horas	Cada 15-60 minutos	Al menos cada 5 minutos
Análisis de datos de registro local	Cada 1–7 días	Cada 12–24 horas	Al menos 6 veces al día
¿Comprobación de integridad de archivos para registros rotados?	opcional	Sí	Sí
¿Cifrar registros rotados?	opcional	opcional	Sí
¿Cifrar las transferencias de datos de registro a SIEM?	opcional	Sí	Sí

Transacciones sintéticas

El monitoreo sintético de transacciones, que es un tipo de monitoreo proactivo, a menudo se prefiere para sitios web y aplicaciones. Proporciona información sobre la disponibilidad y el rendimiento de una aplicación y advierte de cualquier problema potencial antes de que los usuarios experimenten cualquier degradación en el comportamiento de la aplicación. Utiliza agentes externos para ejecutar transacciones con scripts en una aplicación. Por ejemplo, System Center Operations Manager de Microsoft usa transacciones sintéticas para supervisar bases de datos, sitios web y uso de puertos TCP.

Por el contrario, el monitoreo de usuario real (RUM), que es un tipo de monitoreo pasivo, captura y analiza cada transacción de cada usuario de aplicación o sitio web. A diferencia de la supervisión sintética, que intenta obtener información sobre el rendimiento probando regularmente las interacciones sintéticas, RUM corta las conjeturas al ver exactamente cómo interactúan los usuarios con la aplicación.

Revisión y pruebas de código

La revisión y las pruebas de código deben producirse a lo largo de todo el ciclo de vida de desarrollo del sistema o de la aplicación. El objetivo de la revisión y las pruebas de código es identificar patrones de programación incorrectos, configuraciones incorrectas de seguridad, errores funcionales y errores lógicos.

En la fase de planeación y diseño, la revisión y las pruebas de código incluyen revisiones de seguridad de arquitectura y modelado de amenazas. En la fase de desarrollo, la revisión y las

pruebas de código incluyen el análisis de código fuente estático, la revisión manual de código, el análisis de código binario estático y la revisión binaria manual. Una vez que se implementa una aplicación, la revisión y las pruebas de código implican pruebas de penetración, análisis de vulnerabilidades y pruebas de exploración de datos.

La revisión formal del código implica un proceso cuidadoso y detallado con varios participantes y varias fases. En este tipo de revisión de código, los desarrolladores de software asisten a reuniones donde se revisa cada línea de código, generalmente utilizando copias impresas. La revisión ligera del código normalmente requiere menos sobrecarga que las inspecciones formales del código, aunque puede ser igualmente eficaz cuando se realiza correctamente. Entre los métodos de revisión de código se incluyen los siguientes:

- **Por encima del hombro:** un desarrollador mira por encima del hombro del autor mientras el autor recorre el código.
- **Pase de correo electrónico:** el código fuente se envía por correo electrónico a los revisores automáticamente después de que se protege el código.
- **Programación de pares:** Dos autores desarrollan código juntos en la misma estación de trabajo.
- **Revisión de código asistida por herramientas:** los autores y revisores usan herramientas diseñadas para la revisión de código por pares.
- **Pruebas de caja negra o pruebas de conocimiento cero:** el equipo no tiene conocimiento sobre la aplicación de la organización. El equipo puede utilizar cualquier medio a su disposición para obtener información sobre la aplicación de la organización. Esto también se conoce como pruebas cerradas.
- **Pruebas de caja blanca:** El equipo entra en el proceso con un profundo conocimiento de la aplicación o sistema. Con este conocimiento, el equipo crea casos de prueba para ejercitar cada ruta de acceso, campo de entrada y rutina de procesamiento.
- **Pruebas de caja gris:** El equipo se proporciona más información que en las pruebas de caja negra, mientras que no tanto como en las pruebas de caja blanca. Las pruebas de caja gris tienen la ventaja de no ser intrusivas mientras se mantiene el límite entre el desarrollador y el probador. Por otro lado, puede descubrir algunos de los problemas que podrían descubrirse con las pruebas de caja blanca.

En la Tabla 6-4 se comparan las pruebas de caja negra, caja gris y caja blanca.

Tabla 6-4 Pruebas de caja negra, caja gris y caja blanca

caja negra	Caja gris	Caja Blanca
Se desoyó el funcionamiento interno de la aplicación.	El funcionamiento interno de la aplicación es algo conocido.	El funcionamiento interno de la aplicación es completamente conocido.

caja negra	Caja gris	Caja Blanca
También se denomina pruebas de caja cerrada, basadas en datos y funcionales.	También se llama prueba translúcida, ya que el probador tiene conocimiento parcial.	También se conoce como pruebas de cuadro claro, estructurales o basadas en código.
Realizado por usuarios finales, evaluadores y desarrolladores.	Realizado por usuarios finales, evaluadores y desarrolladores.	Realizado por probadores y desarrolladores.
Menos tiempo.	Más tiempo que las pruebas de caja negra, pero menos que las pruebas de caja blanca.	Lo más exhaustivo y lento.

Otros tipos de pruebas incluyen pruebas dinámicas frente a estáticas y pruebas manuales frente a pruebas automáticas.

Proceso de revisión de código

La revisión del código varía de una organización a una organización a una organización. Las inspecciones de Fagan son las revisiones de código más formales que pueden ocurrir y deben adherirse al siguiente proceso:

1. plan
2. visión general
3. preparar
4. Inspeccionar
5. Reanudación
6. seguimiento

La mayoría de las organizaciones no se adhieren estrictamente al proceso de inspección de Fagan. Cada organización debe adoptar un proceso de revisión de código adecuado a sus requisitos empresariales. Cuanto más restrictivo sea el entorno, más formal debe ser el proceso de revisión de código.

Pruebas estáticas

Las pruebas estáticas analizan la seguridad del software sin ejecutar realmente el software. Esto normalmente se proporciona mediante la revisión del código fuente o la aplicación compilada. Las herramientas automatizadas se utilizan para detectar defectos de software comunes. Las herramientas de pruebas estáticas deben estar disponibles durante todo el proceso de diseño de software.

Pruebas dinámicas

Las pruebas dinámicas analizan la seguridad del software en el entorno de tiempo de ejecución. Con esta prueba, el evaluador no debe tener acceso al código fuente de la aplicación.

Las pruebas dinámicas a menudo incluyen el uso de transacciones sintéticas, que son transacciones con scripts que tienen un resultado conocido. Estas transacciones sintéticas se ejecutan en el código probado y, a continuación, la salida se compara con la salida esperada. Cualquier discrepancia entre los dos debe ser investigada para posibles defectos de código fuente.

Pruebas de Fuzz

Las pruebas de Fuzz son una herramienta de pruebas dinámicas que proporciona información al software para probar los límites del software y descubrir defectos. La entrada proporcionada puede ser generada aleatoriamente por la herramienta o creada especialmente para probar vulnerabilidades conocidas.

Los evaluadores de Fuzz incluyen Untidy, Peach Fuzzer y Microsoft SDL File/Regex Fuzzer.

Prueba de casos de mal uso

Las pruebas de casos de uso indebido, también denominadas pruebas negativas, prueban una aplicación para asegurarse de que la aplicación puede controlar la entrada no válida o el comportamiento inesperado. Esta prueba se completa para garantizar que una aplicación no se bloqueará y para mejorar la calidad de una aplicación mediante la identificación de sus puntos débiles. Cuando se realizan pruebas de conversión de uso indebido, las organizaciones deben esperar encontrar problemas. Las pruebas de uso indebido deben incluir pruebas que busquen lo siguiente:

- Los campos obligatorios deben rellenarse.
- Los campos con un tipo de datos definido solo pueden aceptar datos que son el tipo de datos necesario.
- Los campos con límites de caracteres solo permiten el número de caracteres configurado.
- Los campos con un rango de datos definido solo aceptan datos dentro de ese rango.
- Los campos solo aceptan datos válidos.

Análisis de cobertura de prueba

El análisis de cobertura de pruebas utiliza casos de prueba que se escriben con respecto a las especificaciones de requisitos de la aplicación. Las personas implicadas en este análisis no necesitan ver el código para escribir los casos de prueba. Una vez escrito un documento que describe todos los casos de prueba, los grupos de prueba hacen referencia a un porcentaje de los casos de prueba que se ejecutaron, que se pasaron, que no se pudo, etc. El desarrollador de aplicaciones normalmente realiza análisis de cobertura de pruebas como parte de las pruebas

unitarias. Los grupos de control de calidad utilizan el análisis general de la cobertura de la prueba para indicar las métricas de la prueba y la cobertura de acuerdo con el plan de pruebas.

El análisis de cobertura de prueba crea casos de prueba adicionales para aumentar la cobertura. Ayuda a los desarrolladores a encontrar áreas de una aplicación que no se ejercen mediante un conjunto de casos de prueba. Ayuda a determinar una medida cuantitativa de la cobertura del código, que mide indirectamente la calidad de la aplicación o el producto.

Una desventaja de la medición de cobertura de código es que mide la cobertura de lo que cubre el código, pero no puede probar lo que el código no cubre o lo que no se ha escrito. Además, este análisis analiza una estructura o función que ya existe y no las que aún no existen.

Pruebas de interfaz

Las pruebas de interfaz evalúan si los sistemas o componentes de una aplicación se pasan correctamente datos y controles entre sí. Comprueba si las interacciones del módulo funcionan correctamente y los errores se controlan correctamente. Las interfaces que se deben probar incluyen interfaces de cliente, interfaces de servidor, interfaces remotas, interfaces gráficas de usuario (GUI), interfaces de programación de aplicaciones (API), interfaces externas e internas e interfaces físicas.

Las pruebas de GUI implican probar la GUI de un producto para asegurarse de que cumple con sus especificaciones a través del uso de casos de prueba. Las pruebas de API prueban las API directamente de forma aislada y como parte de las transacciones de un extremo a otro realizadas durante las pruebas de integración para determinar si las API devuelven las respuestas correctas.

Recopilar datos del proceso de seguridad

Una vez probados los controles de seguridad, las organizaciones deben asegurarse de que recopilan los datos de proceso de seguridad adecuados. NIST SP 800-137 proporciona directrices para el desarrollo de un programa de monitoreo continuo de seguridad de la información (ISCM). Los profesionales de la seguridad deben asegurarse de que los datos de los procesos de seguridad que se recopilan incluyen la gestión de cuentas, la revisión de la gestión, los indicadores clave de rendimiento y riesgo, los datos de verificación de copias de seguridad, la capacitación y la sensibilización, y la recuperación ante desastres y la continuidad del negocio.

NIST SP 800-137

De acuerdo con NIST SP 800-137, *ISCM* se define como mantener un conocimiento continuo de la seguridad de la información, vulnerabilidades y amenazas para apoyar las decisiones de administración de riesgos de la organización.

Las organizaciones deben tomar las siguientes medidas para establecer, implementar y mantener iscm:

1. Defina una estrategia iscm basada en la tolerancia al riesgo que mantenga una visibilidad clara de los activos, el conocimiento de las vulnerabilidades, la información actualizada sobre amenazas y los impactos de la misión y el negocio.
2. Establezca un programa ISCM que incluya métricas, frecuencias de monitoreo de estado, frecuencias de evaluación de control y una arquitectura técnica ISCM.
3. Implementar un programa ISCM y recopilar la información relacionada con la seguridad necesaria para métricas, evaluaciones e informes. Automatice la recopilación, el análisis y la generación de informes de datos siempre que sea posible.
4. Analice los datos recogidos, informe los resultados, y determine las respuestas apropiadas. Puede ser necesario recopilar información adicional para aclarar o complementar los datos de seguimiento existentes.
5. Responda a los hallazgos con actividades o aceptación o aceptación, transferencia/uso compartido o evitación/rechazo de actividades de mitigación técnicas, de gestión y operativas.
6. Revise y actualice el programa de monitoreo, ajustando la estrategia de ISCM y madurando las capacidades de medición para aumentar la visibilidad de los activos y el conocimiento de las vulnerabilidades, permitir aún más el control basado en datos de la seguridad de la infraestructura de información de una organización y aumentar la resiliencia organizacional.

Administración de cuentas

La administración de cuentas es importante porque implica la adición y eliminación de cuentas a las que se concede acceso a sistemas o redes. Pero la administración de cuentas también implica cambiar los permisos o privilegios concedidos a esas cuentas. Si la administración de cuentas no se supervisa y registra correctamente, las organizaciones pueden descubrir que las cuentas se han creado con el único propósito de llevar a cabo actividades fraudulentas o maliciosas. Los controles de dos personas se deben usar con la administración de cuentas, a menudo implicando a un administrador que crea cuentas y a otro que asigna a esas cuentas los permisos o privilegios adecuados.

La escalada y la *revocación* son dos términos que son importantes para los profesionales de la seguridad. La extensión de la cuenta se produce cuando a una cuenta de usuario se le concede más permisos en función de las nuevas tareas de trabajo o de un cambio de trabajo completo. Los profesionales de la seguridad deben analizar completamente las necesidades de un usuario antes de cambiar los permisos o privilegios actuales, asegurándose de conceder solo los permisos o privilegios necesarios para la nueva tarea y quitar los que ya no son necesarios. Sin este análisis, los usuarios pueden conservar permisos que causan posibles problemas de seguridad porque ya no se conserva la separación de tareas. Por ejemplo, supongamos que se contrata a un usuario en el departamento de proveedores para imprimir todos los cheques de proveedor. Posteriormente este usuario recibe una promoción para aprobar el pago de las mismas cuentas. Si no se quita el permiso anterior de este usuario para imprimir cheques, este único usuario podría aprobar los cheques e imprimirlos, lo que es una infracción directa de la separación de tareas.

La revocación de la cuenta se produce cuando se revoca una cuenta de usuario porque un usuario ya no está con una organización. Los profesionales de la seguridad deben tener en cuenta que habrá objetos que pertenecen a este usuario. Si simplemente se elimina la cuenta de usuario, se puede perder el acceso a los objetos que pertenecen al usuario. Puede ser un mejor plan para deshabilitar la cuenta durante un período determinado. Las directivas de revocación de cuentas también deben distinguir entre revocar una cuenta para un usuario que renuncia a una organización y revocar una cuenta para un usuario que ha finalizado.

Revisión y aprobación de la administración

La revisión de la gestión de los datos del proceso de seguridad debería ser obligatoria. No importa cuántos datos recopile una organización sobre sus procesos de seguridad, los datos son inútiles si nunca son revisados por un administrador. Deben establecerse directrices y procedimientos para garantizar que el examen de la gestión se lleve a la mente de manera oportuna. Sin una revisión regular, incluso el problema de seguridad más pequeño se puede convertir rápidamente en una brecha de seguridad importante.

La revisión de la administración debe incluir un proceso de aprobación mediante el cual la administración revise las recomendaciones de los profesionales de la seguridad y apruebe o rechace las recomendaciones en función de los datos facilitados. Si se dan alternativas, la administración debe aprobar la alternativa que mejor satisfaga las necesidades de la organización. Los profesionales de la seguridad deben asegurarse de que los informes proporcionados a la administración sean lo más completos posible para que todos los datos se puedan analizar para garantizar que se selecciona la solución más adecuada.

Indicadores clave de rendimiento y riesgo

Mediante el uso de indicadores clave de rendimiento y riesgo de los datos de procesos de seguridad, las organizaciones identifican mejor cuándo es probable que se produzcan riesgos de seguridad. Los indicadores clave de rendimiento (IFP) permiten a las organizaciones determinar si los niveles de rendimiento están por debajo o por encima de las normas establecidas. Los indicadores clave de riesgo (KRIs) permiten a las organizaciones identificar si es más o menos probable que ocurran ciertos riesgos.

El NIST ha publicado el Marco para mejorar la *ciberseguridad de infraestructura crítica*, también conocido como el Marco de ciberseguridad, que se centra en el uso de impulsores de negocios para guiar las actividades de ciberseguridad y considerar los riesgos de ciberseguridad como parte de los procesos de gestión de riesgos de la organización. El marco consta de tres partes: el núcleo del marco, los perfiles del marco y los niveles de implementación del marco.

El Núcleo del Marco es un conjunto de actividades de ciberseguridad, resultados y referencias informativas que son comunes a todos los sectores de infraestructura crítica, proporcionando la orientación detallada para el desarrollo de perfiles organizacionales individuales. Framework Core consta de cinco funciones simultáneas y continuas: identificar, proteger, detectar, responder y recuperar.

Una vez identificada cada función, se registran las categorías y subcategorías de cada función. Los perfiles marco se desarrollan en función de las necesidades empresariales de las categorías y subcategorías. Mediante el uso de los perfiles del marco, el marco ayuda a una organización a alinear sus actividades de ciberseguridad con sus requisitos empresariales, tolerancias al riesgo y recursos.

Los niveles de implementación del marco proporcionan un mecanismo para que las organizaciones vean y comprendan las características de su enfoque para administrar el riesgo de ciberseguridad. Se utilizan los siguientes niveles: Nivel 1, parcial; Nivel 2, informado sobre el riesgo; Nivel 3, repetible; y Nivel 4, adaptativo.

Las organizaciones seguirán teniendo riesgos únicos (diferentes amenazas, diferentes vulnerabilidades y diferentes tolerancias al riesgo) y la forma en que implementen las prácticas en el marco variará. En última instancia, el marco está dirigido a reducir y gestionar mejor los riesgos de ciberseguridad y no es un enfoque único para la gestión de la ciberseguridad.

Datos de verificación de copia de seguridad

También se debe realizar una copia de seguridad de los datos del proceso de seguridad que se recopilen. Los profesionales de la seguridad deben asegurarse de que su organización cuenta con las directrices de copia de seguridad y restauración adecuadas para todos los datos de proceso de seguridad. Si no se realiza una copia de seguridad de los datos correctamente, un error puede provocar que los datos vitales se pierdan para siempre. Además, el personal debe probar el proceso de restauración de forma regular para asegurarse de que funciona como debería. Si una organización no puede restaurar una copia de seguridad correctamente, es posible que la organización no tenga la copia de seguridad.

Formación y sensibilización

Todo el personal debe comprender cualquier evaluación de seguridad y estrategias de prueba que emplee una organización. Es posible que el personal técnico deba recibir capacitación en los detalles sobre la evaluación y las pruebas de seguridad, incluidas las pruebas de control de seguridad y la recopilación de datos de procesos de seguridad. Sin embargo, a otros miembros del personal sólo les falta que se les dé más formación en materia de sensibilización sobre este tema. Los profesionales de seguridad deben ayudar al personal a comprender qué tipo de evaluación y pruebas se producen, qué es lo que captura este proceso y por qué esto es importante para la organización. La administración debe apoyar plenamente la evaluación de la seguridad y la estrategia de pruebas y debe comunicar a todo el personal y las partes interesadas la importancia de este programa.

Recuperación ante Desastres y Continuidad del Negocio

Los planes de recuperación ante desastres y continuidad del negocio que desarrolle una organización deben tener en cuenta la evaluación y las pruebas de seguridad, las pruebas de control de seguridad y la recopilación de datos de procesos de seguridad. A menudo, cuando una

organización entra en modo de recuperación ante desastres, el personal no piensa en estos procesos. De hecho, los controles de seguridad ordinarios a menudo se quedan en el camino en esos momentos. Un profesional de la seguridad es responsable de garantizar que esto no suceda. Los profesionales de la seguridad que participan en el desarrollo de los planes de recuperación ante desastres y continuidad del negocio deben cubrir todas estas áreas.

Analizar e informar de los resultados de las pruebas

El personal debe comprender los informes automatizados y manuales que se pueden realizar como parte de la evaluación y las pruebas de seguridad. Los resultados deben comunicarse oportunamente a la administración para asegurarse de que entienden el valor de este proceso. Puede ser necesario proporcionar diferentes informes dependiendo del nivel de comprensión de la audiencia. Por ejemplo, la administración de alto nivel puede necesitar sólo un resumen de los hallazgos. Sin embargo, el personal técnico debe recibir detalles de los hallazgos para asegurarse de que puede implementar los controles apropiados para mitigar o prevenir cualquier riesgo encontrado durante la evaluación y las pruebas de seguridad.

El personal puede necesitar capacitación especial sobre cómo ejecutar informes manuales y cómo analizar los resultados de los informes.

Realizar o facilitar auditorías de seguridad

Las organizaciones deben realizar auditorías internas, externas y de terceros como parte de cualquier evaluación de seguridad y estrategia de pruebas. Estas auditorías deben probar todos los controles de seguridad que están actualmente en vigor. Las siguientes son algunas directrices que se deben tener en cuenta como parte de un buen plan de auditoría de seguridad:

- Como mínimo, realice auditorías anuales para establecer una línea de base de seguridad.
- Determine los objetivos de su organización para la auditoría y compártalos con los auditores.
- Establezca las reglas básicas para la auditoría, incluidas las fechas y horas de la auditoría, antes de que comience la auditoría.
- Elija auditores que tengan experiencia en seguridad.
- Involucre a los gerentes de unidades de negocio al principio del proceso.
- Asegúrese de que los auditores confíen en la experiencia, no solo en las listas de verificación.
- Asegúrese de que el informe del auditor refleje los riesgos que la organización ha identificado.
- Asegúrese de que la auditoría se lleva a cabo correctamente.
- Asegúrese de que la auditoría cubre todos los sistemas y todas las políticas y procedimientos.
- Examine el informe cuando se complete la auditoría.

Recuerde que las auditorías internas son realizadas por personal dentro de la organización, mientras que las auditorías externas o de terceros son realizadas por personas ajenas a la organización u otra empresa. Ambos tipos de auditorías deben ocurrir.

Muchas regulaciones hoy en día requieren que se produjo la auditoría. Las organizaciones solían confiar en la Declaración de normas de auditoría (SAS) 70, que proporcionaba a los auditores información y verificación sobre los controles y procesos del centro de datos relacionados con los usuarios del centro de datos y sus informes financieros. Una auditoría SAS 70 verificó que los controles y procesos establecidos por un centro de datos se siguen realmente. La Declaración sobre estándares para compromisos de atestación (SSAE) 16, Reporting on Controls at a Service Organization, es una norma más reciente que verifica los controles y procesos y también requiere una afirmación por escrito con respecto al diseño y la efectividad operativa de los controles que se están revisando.

Una auditoría SSAE 16 da como resultado un informe de Control de organización de servicios (SOC) 1. Este informe se centra en los controles internos de la información financiera. Hay dos tipos de informes SOC 1:

- **SOC 1, Informe tipo 1:** Se centra en la opinión de los auditores sobre la precisión e integridad del diseño de controles, sistemas y/o servicios de la administración del centro de datos.
- **SOC 1, informe tipo 2:** Incluye el informe tipo 1, así como una auditoría de la eficacia de los controles durante un período de tiempo determinado, normalmente entre seis meses y un año.

Otros dos tipos de informes también están disponibles: SOC 2 y SOC 3. Ambas auditorías proporcionan puntos de referencia para los controles relacionados con la seguridad, disponibilidad, integridad del procesamiento, confidencialidad o privacidad de un sistema y su información. Un informe SOC 2 incluye pruebas y resultados de auditor de servicio, y un informe SOC 3 proporciona solo la descripción del sistema y la opinión del auditor. Un informe SOC 3 es para uso general y proporciona un nivel de certificación para los operadores de centros de datos que garantiza a los usuarios del centro de datos la seguridad de las instalaciones, la alta disponibilidad y la integridad del proceso. En el cuadro 6-5 se comparan brevemente los tres tipos de informes soc.

Tabla 6-5 Comparación de informes SOC

	Sobre qué informa	Quién lo usa
SOC 1	Controles internos de la información financiera	Auditores de usuarios y oficina de control

	Sobre qué informa	Quién lo usa
SOC 2	Seguridad, disponibilidad, integridad del procesamiento, confidencialidad o controles de privacidad	Administración, reguladores y otros; compartido bajo acuerdo de confidencialidad (NDA)
SOC 3	Seguridad, disponibilidad, integridad del procesamiento, confidencialidad o controles de privacidad	Disponible públicamente para cualquier persona

Tareas de preparación del examen

Como se mencionó en la sección"Acerca de la Guía de Certificados CISSP,Tercera Edición"en la Introducción, usted tiene un par de opciones para la preparación del examen: los ejercicios aquí, Capítulo 9, "Preparaciónfinal",y las preguntas de simulación del examen en el Pearson Test Prep Software Online.

Revisar todos los temas clave

Revise los temas más importantes de este capítulo, anotados con el icono Temas clave en el margen exterior de la página. En la tabla 6-6 se enumeran una referencia de estos temas clave y los números de página en los que se encuentra cada uno de ellos.

Cuadro 6-6 Temas clave del capítulo 6

Elemento tema clave	descripción	Número de página
lista	Tres categorías de evaluaciones de vulnerabilidad	536
Cuadro 6-1	Análisis basado en servidor frente a análisis basado en agente	539
lista	Pasos en una prueba de penetración	539
lista	Estrategias para pruebas de penetración	540
lista	Categorías de pruebas de penetración	540
Cuadro 6-2	Comparación de evaluaciones de vulnerabilidad y pruebas de penetración	541
lista	Recomendaciones de NIST SP 800-92 para la administración de registros	542
Cuadro 6-3	Ejemplos de opciones de configuración de registro	545
Cuadro 6-4	Pruebas de caja negra, caja gris y caja blanca	547
lista	Pasos para establecer, implementar y mantener ISCM	550
lista	Tipos de informes SOC 1	555

Elemento tema clave	descripción	Número de página
Cuadro 6-5	Comparación de informes SOC	555

Definir términos clave

Defina los siguientes términos clave de este capítulo y compruebe sus respuestas en el glosario:

administración de cuentas

analizador de vulnerabilidades activo (AVS)

pruebas de caja negra

prueba ciega

revisión y pruebas de código

prueba de doble anonimato

pruebas dinámicas

prueba de conocimiento completo

pruebas de exploración no aproximada

pruebas de caja gris

supervisión continua de la seguridad de la información (ISCM)

pruebas de interfaz

registro

revisión de registros

pruebas de casos de mal uso

pruebas negativas

análisis de detección de red

análisis de vulnerabilidad de red

NIST SP 800-137

NIST SP 800-92

huellas digitales del sistema operativo

prueba de conocimiento parcial

escáner de vulnerabilidad pasiva (PVS)

prueba de penetración

monitoreo de usuario real (RUM)

pruebas estáticas

supervisión de transacciones sintéticas

prueba de destino

análisis de cobertura de prueba

detección de topología

vulnerabilidad

evaluación de vulnerabilidad

pruebas de caja blanca

prueba de conocimiento cero

Responder preguntas de revisión

1. ¿Para cuál de las siguientes pruebas de penetración sabe el equipo de pruebas que se avecina un ataque, pero tiene un conocimiento limitado de los sistemas y dispositivos de red y solo información disponible públicamente?

1. Prueba de destino
2. Prueba física
3. Prueba ciega
4. Prueba doble ciego

2. ¿Cuál de los siguientes NO es una guía de acuerdo con NIST SP 800-92?

1. Las organizaciones deben establecer directivas y procedimientos para la administración de registros.

2. Las organizaciones deben crear y mantener una infraestructura de administración de registros.
3. Las organizaciones deben priorizar la administración de registros de forma adecuada en toda la organización.
4. Elija auditores con experiencia en seguridad.

3. Según NIST SP 800-92, ¿cuáles de las siguientes son facetas de la infraestructura de administración de registros? (Elija todo lo que se aplique).)

1. Funciones generales (análisis de registros, filtrado de eventos y agregación de eventos)
2. Almacenamiento (rotación de registros, archivado de registros, reducción de registros, conversión de registros, normalización de registros, comprobación de integridad de archivos de registro)
3. Análisis de registros (correlación de eventos, visualización de registros, informes de registros)
4. Eliminación de registros (eliminación de registros)

4. ¿Cuáles son las dos formas de recopilar registros mediante productos de administración de eventos e información de seguridad (SIEM), según NIST SP 800-92?

1. Pasivo y activo
2. Sin agente y basado en agentes
3. Empuje y tire de
4. Rendimiento y velocidad

5. ¿Qué método de monitoreo captura y analiza cada transacción de cada usuario de aplicación o sitio web?

1. ron
2. Supervisión de transacciones sintéticas
3. Revisión y pruebas de código
4. Pruebas de casos de mal uso

6. ¿Qué tipo de prueba también se conoce como prueba negativa?

1. ron
2. Supervisión de transacciones sintéticas
3. Revisión y pruebas de código
4. Pruebas de casos de mal uso

7. ¿Cuál es el primer paso del plan de monitoreo continuo de seguridad de la información (ISCM), de acuerdo con NIST SP 800-137?

1. Establecer un programa ISCM.
2. Definir la estrategia ISCM.
3. Implementar un programa ISCM.

4. Analizar los datos recogidos.

8. ¿Cuál es el segundo paso del plan de monitoreo continuo de seguridad de la información (ISCM), según NIST SP 800-137?

1. Establecer un programa ISCM.
2. Definir la estrategia ISCM.
3. Implementar un programa ISCM.
4. Analizar los datos recogidos.

9. ¿Cuál de los siguientes NO es una guía para auditorías internas, externas y de terceros?

1. Elija auditores con experiencia en seguridad.
2. Involucre a los gerentes de unidades de negocio al principio del proceso.
3. Como mínimo, realice auditorías bianuales para establecer una línea de base de seguridad.
4. Asegúrese de que la auditoría cubre todos los sistemas y todas las políticas y procedimientos.

10. ¿Qué informe soc debe ser compartido con el público en general?

1. SOC 1, Tipo 1
2. SOC 1, Tipo 2
3. SOC 2
4. SOC 3

11. ¿Cuál de los siguientes es el último paso en la realización de una prueba de penetración?

1. Documente los resultados de la prueba de penetración e informe de los hallazgos a la gerencia, con sugerencias para la acción correctiva.
2. Recopilar información sobre los métodos de ataque contra el sistema o dispositivo de destino.
3. Documente información sobre el sistema o dispositivo de destino.
4. Ejecutar ataques contra el sistema o dispositivo de destino para obtener acceso de usuario y con privilegios.

12. ¿En cuál de los siguientes elementos el equipo de pruebas no tiene ningún conocimiento de la red de la organización?

1. Pruebas de caja gris
2. Pruebas de caja negra
3. Pruebas de caja blanca
4. Pruebas físicas

13. ¿Cuál de los siguientes se define como una herramienta de prueba dinámica que proporciona entrada al software para probar los límites del software y descubrir defectos?

1. Pruebas de interfaz
2. Pruebas estáticas
3. Análisis de cobertura de prueba
4. Pruebas de Fuzz

14. ¿Qué factores deben seguir los profesionales de la seguridad al realizar pruebas de seguridad? (Elija todo lo que se aplique).)

1. Cambios que podrían afectar al rendimiento
2. Riesgo del sistema
3. Nivel de sensibilidad de la información
4. Probabilidad de fallo técnico o mala configuración

15. ¿Cuál de las siguientes opciones puede utilizar un pirata informático para identificar vulnerabilidades comunes en un sistema operativo que se ejecuta en un host o servidor?

1. Huellas digitales del sistema operativo
2. Análisis de detección de red
3. Indicadores clave de rendimiento y riesgo
4. Auditorías de terceros

Respuestas y explicaciones

1.c. Con una prueba a ciegas, el equipo de pruebas sabe que se avecina un ataque y tiene un conocimiento limitado de los sistemas y dispositivos de red y de la información disponible públicamente. Una prueba de destino se produce cuando el equipo de pruebas y el equipo de seguridad de la organización reciben la máxima información sobre la red y el tipo de ataque que se producirá. Una prueba física no es un tipo de prueba de penetración. Es un tipo de evaluación de vulnerabilidad. Una prueba doble ciego es como una prueba ciega, excepto que el equipo de seguridad de la organización no sabe que se avecina un ataque.

2. d. NIST SP 800-92 no incluye ninguna información sobre los auditores. Por lo tanto, la opción "Elegir auditores con experiencia en seguridad" NO es una guía de acuerdo con NIST SP 800-92.

3. a, b, c, d. Según NIST SP 800-92, las funciones de administración de registros deben incluir funciones generales (análisis de registros, filtrado de eventos y agregación de eventos), almacenamiento (rotación de registros, archivado de registros, reducción de registros, conversión de registros, normalización de registros, comprobación de integridad de archivos de registro), análisis de registros (correlación de eventos, visualización de registros, informes de registros) y eliminación de registros (eliminación de registros).

4.b. Las dos formas de recopilar registros mediante productos de administración de eventos e información de seguridad (SIEM), según NIST SP 800-92, son sin agente y basadas en agentes.

5. a. El monitoreo de usuarios reales (RUM) captura y analiza cada transacción de cada usuario de aplicación o sitio web.

6. d. Las pruebas de casos de mal uso también se conocen como pruebas negativas.

7.b. Los pasos en un programa ISCM, de acuerdo con NIST SP 800-137, son

1. Definir una estrategia ISCM.
2. Establecer un programa ISCM.
3. Implementar un programa ISCM y recopilar la información relacionada con la seguridad necesaria para métricas, evaluaciones e informes.
4. Analice los datos recogidos, informe los resultados, y determine las respuestas apropiadas.
5. Responder a los hallazgos.
6. Revisar y actualizar el programa de monitoreo.

8. a. Los pasos en un programa ISCM, de acuerdo con NIST SP 800-137, son

1. Definir una estrategia ISCM.
2. Establecer un programa ISCM.
3. Implementar un programa ISCM y recopilar la información relacionada con la seguridad necesaria para métricas, evaluaciones e informes.
4. Analice los datos recogidos, informe los resultados, y determine las respuestas apropiadas.
5. Responder a los hallazgos.
6. Revisar y actualizar el programa de monitoreo.

9.c. Las siguientes son directrices para auditorías internas, externas y de terceros:

- Como mínimo, realice auditorías anuales para establecer una línea de base de seguridad.
- Determine los objetivos de su organización para la auditoría y compártalos con los auditores.
- Establezca las reglas básicas para la auditoría, incluidas las fechas y horas de la auditoría, antes de que comience la auditoría.
- Elija auditores que tengan experiencia en seguridad.
- Involucre a los gerentes de unidades de negocio al principio del proceso.
- Asegúrese de que los auditores confíen en la experiencia, no solo en las listas de verificación.
- Asegúrese de que el informe del auditor refleje los riesgos que la organización ha identificado.
- Asegúrese de que la auditoría se lleva a cabo correctamente.
- Asegúrese de que la auditoría cubre todos los sistemas y todas las políticas y procedimientos.
- Examine el informe cuando se complete la auditoría.

10. d. SOC 3 es el único informe soc que debe ser compartido con el público en general.

11. a. Los pasos para realizar una prueba de penetración son los siguientes:

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

12.b. En las pruebas de caja negra, o pruebas de conocimiento cero, el equipo de pruebas no tiene conocimiento sobre la red de la organización. En las pruebas de caja blanca, el equipo de pruebas entra en el proceso de prueba con un profundo conocimiento de la aplicación o el sistema. En las pruebas de caja gris, el equipo de pruebas se proporciona más información que en las pruebas de caja negra, mientras que no tanto como en las pruebas de caja blanca. Las pruebas de caja gris tienen la ventaja de no ser intrusivas mientras se mantiene el límite entre el desarrollador y el probador. Las pruebas físicas revisan las protecciones de las instalaciones y el perímetro.

13. d. Las pruebas de Fuzz son una herramienta de pruebas dinámicas que proporciona información al software para probar los límites del software y descubrir defectos. La entrada proporcionada puede ser generada aleatoriamente por la herramienta o creada especialmente para probar vulnerabilidades conocidas. Las pruebas de interfaz evalúan si los sistemas o componentes de una aplicación se pasan correctamente datos y controles entre sí. Comprueba si las interacciones del módulo funcionan correctamente y los errores se controlan correctamente. Las pruebas estáticas analizan la seguridad del software sin ejecutar realmente el software. Esto normalmente se proporciona mediante la revisión del código fuente o la aplicación compilada. El análisis de cobertura de pruebas utiliza casos de prueba que se escriben con respecto a las especificaciones de requisitos de la aplicación.

14. a, b, c, d. Los profesionales de la seguridad deben tener en cuenta los siguientes factores al realizar pruebas de seguridad:

- impacto
- dificultad
- Tiempo necesario
- Cambios que podrían afectar al rendimiento
- Riesgo del sistema
- Criticidad del sistema
- Disponibilidad de las pruebas de seguridad
- Nivel de sensibilidad de la información
- Probabilidad de fallo técnico o mala configuración

15. a. La huella digital del sistema operativo es el proceso de usar algún método para determinar el sistema operativo que se ejecuta en un host o un servidor. Al identificar la versión del sistema operativo y el número de compilación, un hacker puede identificar vulnerabilidades comunes de ese sistema operativo utilizando documentación fácilmente disponible de Internet. Un examen de

detección de red examina un intervalo de direcciones IP para determinar qué puertos están abiertos. Este tipo de análisis sólo muestra una lista de los sistemas de la red y los puertos en uso en la red. En realidad, no comprueba si hay vulnerabilidades. Mediante el uso de indicadores clave de rendimiento y riesgo de los datos de procesos de seguridad, las organizaciones identifican mejor cuándo es probable que se produzcan riesgos de seguridad. Los indicadores clave de desempeño permiten a las organizaciones determinar si los niveles de desempeño están por debajo o por encima de las normas establecidas. Los indicadores de riesgo clave permiten a las organizaciones identificar si es más o menos probable que ocurran ciertos riesgos. Las organizaciones deben realizar auditorías internas, externas y de terceros como parte de cualquier evaluación de seguridad y estrategia de pruebas.