Tarea de reforzamiento de la seguridad	Descripción
Líneas base de configuación	Conjunto documentado de especificaciones dentro de un sistema que se utiliza como base para futuras compilaciones, versiones y actualizaciones.
Verificaciones de configuración	Actualización de los estándares de cifrado para los datos que se almacenan en bases de datos.
Desactivación de puertos no utilizados	Los puertos se pueden bloquear en cortafuegos, enrutadores, servidores y más para evitar el paso de tráfico de red potencialmente peligroso.
Cifrado utilizando los últimos estándares	Reglas o métodos utilizados para ocultar datos salientes y descubrir o descifrar los datos entrantes.
Mantenimiento del cortafuegos (firewall)	Implica revisar y actualizar las configuraciones de seguridad regularmente para estar siempre un paso por delante de las amenazas potenciales.
Eliminación de hardware y software	Asegura que todos los datos se borren correctamente del hardware antiguo antes de desecharlo.
Autenticación de múltiples factores (MFA)	Una medida de seguridad que exige que un usuario verifique su identidad de dos o más maneras para acceder a un sistema o red. Las opciones de MFA incluyen una contraseña, número PIN, insignia, contraseña de un solo uso (OTP) enviada a un teléfono celular, huella digital y más.

Privilegios de acceso a la red	Los privilegios de acceso a la red implican permitir, limitar o bloquear los privilegios de acceso a los activos de red para personas, roles, grupos, direcciones IP, direcciones MAC, etc.
Análisis de registros de red	El proceso de examinar los registros de red para identificar eventos de interés.
Políticas de contraseñas	Las últimas recomendaciones del Instituto Nacional de Estándares y Tecnología (NIST) para las políticas de contraseñas se centran en el uso de métodos de salting y hashing en lugar de requerir contraseñas demasiado complejas o solicitar su cambio frecuente.
Actualizaciones de parches	Una actualización de software y sistema operativo (SO) que aborda las vulnerabilidades de seguridad dentro de un programa o producto.
Prueba de penetración (pen test)	Una prueba de penetración es un ataque simulado que ayuda a identificar vulnerabilidades en sistemas, redes, sitios web, aplicaciones y procesos.
Filtrado de puertos	Una función del cortafuegos que bloquea o habilita ciertos números de puerto para limitar la comunicación no deseada.

Eliminación o desactivación de aplicaciones y servicios no utilizados	Las aplicaciones y servicios no utilizados pueden convertirse en un punto de vulnerabilidad, ya que es menos probable que se mantengan o actualicen con nuevas funciones de seguridad.
Copias de seguridad del servidor y del almacenamiento de datos	Las copias de seguridad del servidor y del almacenamiento de datos ayudan a proteger activos de datos de posibles pérdidas. Las copias de seguridad se pueden grabar y almacenar en una ubicación física o se pueden cargar/sincronizar en un repositorio en la nube.

Usos comunes

Para restaurar un sistema a una línea base previa después de una interrupción de la red o de cambios no autorizados en una línea base.

Para ver si hay algún cambio no autorizado en el sistema.

Antes de que ocurra un incidente, para evitar que los agentes de amenaza ingresen a la red a través del puerto abierto. Después de un incidente, se pueden usar para evitar que futuros ataques ocurran a través de puertos abiertos no utilizados.

Se puede implementar regularmente para evaluar si los estándares de cifrado actuales son seguros y efectivos para tu organización. Los estándares de cifrado también se pueden actualizar después de una filtración de datos.

Esto puede realizarse regularmente. Las reglas del firewall pueden actualizarse en respuesta a un evento que provoque un tráfico anormal en la red. Esta medida se puede usar para protegerse contra varios ataques DoS y DDoS.

Evitar amenazas a la red mediante la eliminación de software o hardware obsoleto o en desuso que no tiene los últimos parches de seguridad o actualizaciones. Los dispositivos sin parches pueden permitir que los agentes de amenaza accedan fácilmente a la red.

Puede ayudar a proteger contra ataques de fuerza bruta y eventos de seguridad similares. La MFA se puede implementar en cualquier momento, y es principalmente una técnica que se configura una vez y luego se mantiene.

Reduce el riesgo de que usuarios no autorizados y tráfico externo accedan a la red interna. Esto puede implementarse una vez, o reevaluarse según la probabilidad de ataques de ingeniería social o fuerza bruta.
Se puede configurar para alertar al equipo de seguridad cuando haya tráfico anormal en la red. Esto se puede usar antes de que ocurra un incidente y durante el seguimiento del tráfico de red, y también puede configurarse en respuesta a un ataque de ciberseguridad. Se trata de una herramienta común para analizar los registros de red es un SIEM.

Las políticas de contraseñas se utilizan para evitar que los atacantes adivinen fácilmente las contraseñas de los/las usuarios/as, ya sea manualmente o mediante el uso de un script para probar miles de contraseñas robadas (comúnmente llamado ataque de fuerza bruta).

Las actualizaciones de parches suelen incluir correcciones para problemas de seguridad. Es importante mantener los sistemas actualizados con los últimos parches de seguridad, ya que los atacantes serán alertados acerca de vulnerabilidades de seguridad cuando se publiquen los parches. Es muy probable que ataquen esa vulnerabilidad antes de que las personas finalmente apliquen los parches.

Las pruebas de penetración se usan para proteger y prevenir posibles ataques.

El filtrado de puertos se utiliza para controlar el tráfico de la red, y puede evitar que atacantes potenciales ingresen a una red privada.

Este procedimiento se utiliza para reducir las vulnerabilidades potenciales dentro de una red.

Las copias de seguridad se utilizan para restaurar datos perdidos en ataques, errores humanos, fallas de equipos y otras pérdidas no planificadas.