El *«hardening»* es un término que se utiliza en el campo de la seguridad informática y se refiere a la práctica de aumentar la seguridad de un sistema o una red informática mediante la implementación de medidas y configuraciones específicas destinadas a reducir las vulnerabilidades y proteger contra posibles amenazas y ataques cibernéticos. El objetivo principal del hardening es hacer que un sistema sea más resistente a intrusiones y ataques maliciosos.

Algunas de las acciones típicas de hardening incluyen:

1. Actualización de software: Mantener el sistema operativo y el software actualizados con los últimos parches de seguridad es esencial para cerrar vulnerabilidades conocidas.
2. Configuración segura: Configurar el sistema de manera que solo se habiliten los servicios y funciones necesarios para el funcionamiento y que se desactiven o eliminen aquellos que no se utilizan o que representan un riesgo de seguridad.
3. Políticas de contraseñas fuertes: Requerir contraseñas complejas y cambiarlas regularmente.
4. Control de acceso: Limitar quiénes tienen acceso al sistema y qué permisos tienen. Implementar autenticación de múltiples factores siempre que sea posible.
5. Firewalls y filtrado de tráfico: Utilizar firewalls para controlar el tráfico de red y permitir solo las conexiones necesarias.
6. Auditoría y registro de eventos: Registrar y supervisar eventos del sistema para detectar y responder a actividades sospechosas.
7. Encriptación: Utilizar la encriptación para proteger datos confidenciales en reposo y en tránsito.
8. Actualizaciones regulares de seguridad: Mantenerse al tanto de las últimas amenazas y vulnerabilidades y aplicar medidas de seguridad adicionales según sea necesario.

El hardening es una parte fundamental de la seguridad informática, ya que ayuda a reducir la superficie de ataque y fortalece las defensas de un sistema contra las amenazas en constante evolución. Es una práctica esencial tanto para sistemas individuales como para redes empresariales para garantizar la integridad y la confidencialidad de los datos y la

continuidad de las operaciones.

Equipos o sistemas donde se puede aplicar el hardening

El proceso de «hardening» o endurecimiento de la seguridad puede aplicarse a una amplia variedad de equipos y sistemas, tanto en el ámbito de la informática como en otros campos donde la seguridad es una preocupación. Aquí hay una lista de algunos de los equipos y sistemas en los que se puede aplicar el hardening:

1. Servidores: Los servidores, ya sean servidores web, de bases de datos, de correo electrónico o cualquier otro tipo de servidor, son objetivos clave para aplicar medidas de hardening, ya que almacenan y gestionan datos críticos.
2. Sistemas operativos: Los sistemas operativos de servidores, computadoras de escritorio y dispositivos móviles pueden endurecerse para reducir las vulnerabilidades y mejorar la seguridad.
3. Firewalls y enrutadores: Los dispositivos de red, como firewalls y enrutadores, deben configurarse adecuadamente para controlar el tráfico de red y proteger la infraestructura de la red.
4. Dispositivos de red: Esto incluye conmutadores (switches), puntos de acceso inalámbrico y otros componentes de red que deben configurarse de manera segura.
5. Dispositivos IoT (Internet de las cosas): Los dispositivos IoT, como cámaras de seguridad, termostatos inteligentes y otros dispositivos conectados, a menudo son vulnerables y requieren medidas de hardening para protegerlos contra ataques.
6. Aplicaciones y software: Las aplicaciones y el software, especialmente aquellos utilizados en entornos empresariales, deben configurarse y mantenerse adecuadamente para reducir los riesgos de seguridad.
7. Equipos de usuario final: Las computadoras de escritorio, las laptops y los dispositivos móviles utilizados por los usuarios finales también pueden endurecerse para proteger los datos y la privacidad.
8. Dispositivos embebidos: Esto incluye sistemas integrados en productos como cámaras

de seguridad, dispositivos médicos y electrodomésticos inteligentes que deben protegerse contra amenazas cibernéticas.
9. Sistemas de control industrial (ICS): Los sistemas utilizados en entornos industriales, como sistemas de control de procesos y sistemas SCADA, deben endurecerse para garantizar la seguridad de las operaciones críticas.
10. Vehículos conectados: Los vehículos modernos están equipados con sistemas informáticos y de comunicación que pueden ser vulnerables a ataques; el hardening es esencial para proteger la seguridad de los vehículos y sus ocupantes.

El hardening no es una medida única que se aplica de la misma manera en todos estos equipos y sistemas, ya que las necesidades de seguridad y las amenazas varían. Por lo tanto, es importante adaptar las estrategias de hardening a cada caso específico, identificando las vulnerabilidades y tomando medidas adecuadas para fortalecer la seguridad.

Software empleado para hardening

Existen varias herramientas y software que pueden ayudarte en el proceso de hardening de sistemas y dispositivos. Estas herramientas están diseñadas para evaluar la seguridad de tus sistemas, identificar vulnerabilidades y proporcionar recomendaciones para fortalecer la seguridad. Algunas de las herramientas populares para el hardening son:

1. Microsoft Baseline Security Analyzer (MBSA): Esta herramienta de Microsoft escanea sistemas Windows en busca de vulnerabilidades y proporciona recomendaciones para mejorar la seguridad de los sistemas operativos Windows, así como de las aplicaciones de Microsoft.
2. OpenSCAP: El Protocolo de Seguridad Automatizada de Configuración Abierta (OpenSCAP) es una suite de herramientas de código abierto que permite evaluar la conformidad con estándares de seguridad, como el Esquema de Seguridad del Sistema Operativo (CIS) y el Estándar de Perfil de Seguridad (STIG) del Departamento de Defensa de EE. UU.
3. Nessus: Nessus es una herramienta de escaneo de vulnerabilidades que puede ayudarte a identificar problemas de seguridad en sistemas, aplicaciones y redes.

Ofrece una versión gratuita y una versión comercial.

4. CIS-CAT: El Centro de Seguridad de la Información (CIS) proporciona herramientas de evaluación de seguridad y documentos de guía para endurecer sistemas según las recomendaciones del CIS.
5. SCAP Workbench: SCAP Workbench es una herramienta gráfica que ayuda a los administradores de sistemas a evaluar y mejorar la seguridad de sistemas basados en SCAP (Security Content Automation Protocol).
6. Ansible: Ansible es una herramienta de automatización que se puede utilizar para implementar políticas de hardening en sistemas de manera automatizada. Puedes encontrar roles de Ansible específicos para hardening.
7. Chef InSpec: Chef InSpec es otra herramienta de automatización que permite definir y verificar políticas de seguridad como código. Puede utilizarse para auditar y endurecer sistemas de forma automatizada.
8. Docker Bench for Security: Si utilizas contenedores Docker, Docker Bench for Security es una herramienta que verifica automáticamente las configuraciones de seguridad de los contenedores Docker y el host subyacente.
9. QualysGuard: QualysGuard es una plataforma de seguridad en la nube que ofrece evaluaciones de seguridad, incluyendo escaneo de vulnerabilidades y cumplimiento de políticas.

Es importante destacar que estas herramientas a menudo se utilizan en conjunto con buenas prácticas de seguridad y análisis específicos para tu entorno. Además, las recomendaciones de seguridad pueden variar según el sistema operativo, la aplicación y las políticas específicas de tu organización, por lo que es fundamental personalizar el proceso de hardening de acuerdo con tus necesidades y requisitos de seguridad.

Auditorías de hardening

Una auditoría de hardening, también conocida como evaluación de endurecimiento de seguridad, es un proceso que implica revisar y evaluar la seguridad de un sistema o red para identificar y abordar vulnerabilidades y debilidades. El funcionamiento general de una auditoría de hardening es:

1. Recopilación de información: El proceso comienza recopilando información sobre el sistema o red que se va a auditar. Esto puede incluir detalles sobre la configuración del sistema, la infraestructura de red, los sistemas operativos, las aplicaciones y cualquier documentación de seguridad relevante.
2. Definición de estándares: Se establecen estándares de seguridad o directrices específicas que deben seguirse durante la auditoría. Estos estándares pueden basarse en las mejores prácticas de seguridad, normativas de cumplimiento (por ejemplo, PCI DSS, HIPAA) o requisitos internos de seguridad de la organización.
3. Escaneo y evaluación: Se utilizan herramientas de escaneo y evaluación de seguridad para analizar el sistema en busca de vulnerabilidades y debilidades. Estas herramientas pueden realizar análisis de configuración, escaneos de puertos, evaluación de políticas de contraseñas, detección de servicios innecesarios y más.
4. Comparación con estándares: Los resultados del escaneo se comparan con los estándares de seguridad definidos anteriormente. Se identifican las áreas en las que el sistema no cumple con los estándares y se documentan las deficiencias.
5. Priorización de hallazgos: Los hallazgos se priorizan según su gravedad y riesgo. Se determina qué vulnerabilidades son críticas y requieren una corrección inmediata, y cuáles pueden abordarse en una fase posterior.
6. Desarrollo de recomendaciones: Se desarrollan recomendaciones específicas para corregir las vulnerabilidades y debilidades identificadas. Estas recomendaciones pueden incluir cambios en la configuración del sistema, la aplicación de parches de seguridad, la mejora de políticas de contraseñas y otras medidas de seguridad.
7. Documentación: Se documentan todos los hallazgos, recomendaciones y acciones tomadas durante la auditoría. Esta documentación es importante para el seguimiento y la rendición de cuentas.
8. Implementación de correcciones: Se implementan las correcciones recomendadas de acuerdo con un plan de acción. Esto puede implicar cambios en la configuración, la instalación de actualizaciones de seguridad y otras medidas para endurecer el sistema.
9. Pruebas de validación: Después de realizar las correcciones, se realizan pruebas de validación para asegurarse de que las vulnerabilidades identificadas se han solucionado correctamente y que el sistema cumple con los estándares de seguridad

definidos.

10. Informe final: Se genera un informe final que resume los hallazgos de la auditoría, las correcciones implementadas y las recomendaciones para futuras mejoras de seguridad. Este informe se comparte con las partes interesadas y la dirección de la organización.
11. Seguimiento continuo: La auditoría de hardening es un proceso continuo. Después de implementar las correcciones, se debe realizar un seguimiento constante de la seguridad del sistema para garantizar que se mantenga en un estado seguro y para abordar nuevas amenazas y vulnerabilidades a medida que surjan.

En resumen, una auditoría de hardening implica evaluar y mejorar la seguridad de un sistema o red mediante la identificación de vulnerabilidades, la comparación con estándares de seguridad y la implementación de correcciones. Es un proceso crítico para garantizar la integridad y la seguridad de los sistemas informáticos en una organización.