HARDENING

- Gestion de Parches.
- Separación de funciones.
- Autenticacion.
- Fortalecimiento
  - Sistema Operativo.
  - Servicios de Red.
  - Aplicaciones.
  - Base de Datos.
  - Contraseñas.

Gestion de Parchos

Cuando se prepara un servidor de gestión de parches, es necesario tener en cuenta lo siguiente.

- ★ Software Integrity Verification.
- ★ Operating System Security.
- ★ Network Services Security.
- ★ Operating System and Services Auditing.
- ★ Access Policy Implementation.
- ★ Homologation Directives Application.
- ★ Logging Enable Implementation.
- ★ Physical Security.

Verificación de Integridad de Software

Todos los softwares que se descarguen al servidor de gestión de parches deben verificarse la integridad, para evitar que estén alterados o corruptos.

Ej. Checksum Tools.

Seguridad del Sistema Operativo

Antes de implementar el servidor en un entorno de producción, la tarea a ejecutar debe estar totalmente definida.

Una vez definida se comienza el proceso de actualización, eliminación de servicios innecesarios, y aplicación de un conjunto de cumplimiento de seguridad para completar el proceso de fortalecimiento (Hardening).

Seguridad en Servicio de Red

Los protocolos de red deben ser verificados de configuraciones incorrectas y fortalecidos para evitar la explotación de bugs a través de ellos.

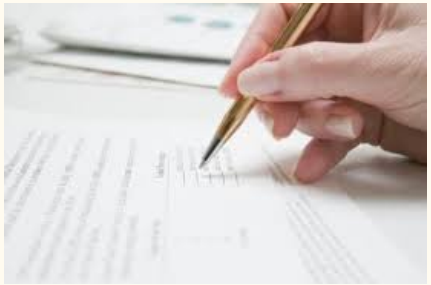
Auditoria de Sistemas Operativos y Servicios de Red

Una vez completado el proceso de aplicar los Baselines a los servicios de Red y NOS, es recomendable correr ciertos procedimientos de auditoría, para validar la correcta implementación del servidor.

Implementacion de politicas de acceso

Aquí se deberá configurar los accesos de red para permitir solamente a usuarios autorizados. Esto evitará el uso de servicios sin autorización y nos asegurara que el servidor solamente tendrá acceso desde ciertos host y servicios de red.

Homologación directivas de aplicación



Una vez finalizado el proceso anterior, todos los pasos de implementación deben ser documentados y el servidor debe ser llevado desde el entorno de pruebas al de producción desde cero y cualquier cambio futuro debe ser validado primero en el entorno de prueba y luego llevado nuevamente a producción.

Implementacion de logs

Con el objetivo de auditar y aplicar técnicas forenses en caso de un incidente, se deberá habilitar los logs del Sistema Operativo y Servicios necesarios.

Seguridad Física

Es importante llevar a cabo la implementación de seguridad física para proteger el activo.

- Colocarlo en un Data Center.
- Monitorear la instalación del sistema de medición del nivel de flujo de aire.
- Controlar y monitorear el acceso a solo personas autorizadas.
- Monitorear los detectores de incendios y demás sensores que vigilen el buen funcionamiento del mismo.
- Implementacion de camaras de vigilancia.
- Implementación de backups de fuente de energía.
- Implementar password en el BIOS.
- Remover todos los dispositivos portables luego de la implementación(usb, cd-rom…)