ES-12 CONFIGURACIÓN DE SEGURIDAD SERVIDORES UNIX/LINUX

1. Normatividad Relacionada

NO-07 Responsabilidad de usuarios
NO-11 Administración de Cuentas
NO-13 Comandos Especiales y Administración de Componentes Tecnológicos
NO-14 Administración y Configuración de Parámetros de Seguridad
NO-15 Nombres de Usuario
NO-19 Administración de Accesos a Componentes Tecnológicos
NO-20 Claves de Acceso
NO-40 Software y Hardware Utilizado
ES-03 Contraseñas de Acceso
ES-04 Parámetros de Acceso
ES-05 Registro de Eventos

2. Objetivos

Establecer los parámetros básicos de seguridad a configurar en los servidores con Sistema Operativo UNIX/LINUX.

3. Componentes Tecnológicos Afectados

Servidores con Sistema Operativo UNIX/LINUX.

4. Descripción

- Configuración de parámetros del sistema:
  - ✓ Intervalo mínimo de cambio de contraseña: 1 día
  - ✓ Tamaño mínimo de contraseña: 10
  - ✓ Tiempo de caducidad de una contraseña y cambio forzoso de la misma: 30 días
  - ✓ Permitir contraseñas nulas: NO
  - ✓ Permitir uso de contraseñas triviales: NO
  - ✓ Máximo número de intentos de acceso fallido antes de bloquear la cuenta: 3
  - ✓ Registrar a nivel de registros de auditoría los ingresos del usuario root al servidor: Si
  - ✓ Contraseña requerida para ingresar al sistema: Si

- ✓ Valor de identificadores de usuarios (UID) diferentes al root: Diferente a 0 y no debe repetirse.
- ✓ Valor de identificadores de grupos de usuarios (GID): No debe repetirse
- ✓ Permitir la existencia de grupos vacíos o sin usuarios: NO
- ✓ Asignar descripción de usuarios para identificar cada cuenta de usuario: SI
- ✓ Existencia de grupos de usuarios sin miembros, diferentes a los grupos creados por defecto (default): NO
- ✓ Chequeo periódico al archivo del script del login del sistema para asegurarse que no ha sido editado y que no contiene comandos no autorizados: SI
- ✓ Conservar al mínimo el número de archivos y directorios sobre los cuales todos los usuarios o grupos tienen privilegios de escritura: SI
- ✓ Asegurarse que solamente el usuario root es propietario (owner) de las páginas que ejecuta y que no se permiten acciones por todos los grupos o usuarios: Si
- ✓ Garantizar el privilegio owner solo a programas que lo requieran: Si
- ✓ Mantener activos en el sistema únicamente servicios de red necesarios: Si
- ✓ Propietario del archivo /etc/inetd.conf (en el cual se habilitan las conexiones de red): Root
- ✓ Permisos sobre archivo /etc/inetd.conf: No permitir modificar a grupos de usuario y usuarios diferentes a root
- ✓ Propietario del archivo /etc/host.equiv: Debe ser root. No permitir modificar a grupos de usuario y usuarios diferentes a root
- ✓ Asegurar que archivos .rhosts tienen como propietario una cuenta de usuario y que solo permiten escritura a esa cuenta: SI
- ✓ Restringir uso del FTP: SI
- ✓ Deshabilitar opciones de IPFORWARDING: SI
- ✓ Eliminación de usuarios por defecto: SI

- ✓ Tiempo máximo entre accesos al sistema luego que la contraseña para usuario root y usuarios privilegiados ó superusuarios es bloqueada: 5 minutos

- ✓ Tiempo máximo entre accesos al sistema luego que la contraseña para usuarios no privilegiados es bloqueada: Indefinido, hasta que el usuario lo solicite.

- ✓ Especificar dispositivo del sistema, donde se registren los intentos de uso del comando SU para el usuario root: SI

- ✓ Activar opciones de TCB (Trusted Computing Base): SI

- ✓ Se deben analizar periódicamente las cuentas deshabilitadas y determinar si deben ser eliminadas o no.