📁 LPIC-2 / 🔒 Tema 212 - La seguridad del sistema

7.6.4 212.4 Tareas de seguridad (peso: 3)

Teoría

La seguridad de un sistema Linux no es una configuración que se realiza una vez y se olvida. Requiere una gestión y monitorización continuas para protegerse contra nuevas amenazas y vulnerabilidades. Las "Tareas de seguridad" engloban un conjunto de prácticas regulares para mantener la postura de seguridad del sistema.

Tareas de Seguridad Clave:

1. **Mantener el Sistema Actualizado:**
    - **Propósito:** Las actualizaciones de software a menudo incluyen parches de seguridad para corregir vulnerabilidades descubiertas. Mantener el sistema y todas las aplicaciones instaladas actualizadas es una de las medidas de seguridad más importantes.
    - **Herramientas (Diferencias):**
        - **Debian/Ubuntu:** `apt update` (actualiza lista de paquetes), `apt upgrade` (instala actualizaciones).
        - **Red Hat/CentOS/Fedora:** `dnf check-update` (verifica actualizaciones), `dnf upgrade` (instala actualizaciones).
    - **Automatización:** Configurar actualizaciones automáticas (usando herramientas como `unattended-upgrades` en Debian/Ubuntu o `dnf-automatic` en Red Hat) o programar actualizaciones regulares usando cron o systemd timers.
2. **Gestión Segura de Usuarios y Grupos:**
    - **Propósito:** Asegurar que solo los usuarios autorizados tengan cuentas y que sus permisos sean los adecuados.
    - **Tareas:** Crear usuarios con contraseñas seguras (o preferiblemente autenticación por clave SSH para acceso remoto). Eliminar o deshabilitar cuentas de usuarios que ya no son necesarias. Revisar las membresías de grupo para asegurar que los usuarios solo pertenecen a los grupos que necesitan. Asegurar que los UID y GID son consistentes en entornos con NFS/LDAP si no se usa ID mapping (Revisado 209.3, 210.3).
3. **Permisos de Archivos y Directorios (DAC):**
    - **Propósito:** Controlar quién puede leer, escribir y ejecutar archivos y directorios utilizando los permisos tradicionales de usuario, grupo y otros.
    - **Tareas:** Asegurarse de que los archivos de configuración sensibles (`/etc/passwd`, `/etc/shadow`, `/etc/group`, `/etc/sudoers`, claves SSH privadas, configuraciones de servicios) tienen permisos restrictivos (solo legibles por root o usuarios/grupos específicos, nunca escribibles por "otros"). Asegurar que los

directorios de usuario tienen permisos apropiados (`700` o `750` para el home mismo, `.ssh` es `700`). El sticky bit (`+t`) en directorios escribibles por todos (ej: `/tmp`) evita que los usuarios borren archivos de otros.

4. **Acceso Privilegiado Seguro (`sudo`):**
    - **Propósito:** Permitir a usuarios específicos ejecutar comandos con privilegios de root de forma controlada, sin compartir la contraseña de root.
    - **Configuración:** Se configura en el archivo `/etc/sudoers` o en archivos separados en el directorio `/etc/sudoers.d/`. **Siempre editar `/etc/sudoers` con el comando `visudo`**; `visudo` verifica la sintaxis antes de guardar, evitando bloquear el acceso sudo.
    - **Sintaxis Básica en `sudoers`:** `usuario HOSTS = (RUNAS_USER) COMMANDS`. Ejemplo: `admin ALL = (ALL) ALL` (permite al usuario admin ejecutar cualquier comando como cualquier usuario en cualquier host). `editor ALL = (root) /bin/vi /etc/archivo.conf` (permite al usuario editor ejecutar vi como root solo en ese archivo).
    - **Diferencias:** La ubicación del directorio `/etc/sudoers.d/` y cómo se incluyen estos archivos en `/etc/sudoers` pueden tener ligeras variaciones entre distribuciones.
    - **Tarea:** Configurar `sudo` para dar solo los permisos necesarios a cada usuario o grupo.
5. **Revisión y Análisis de Logs:**
    - **Propósito:** Detectar patrones de actividad que puedan indicar un compromiso o un ataque en curso (intentos de login fallidos, acceso a archivos inusual, errores de servicio inesperados).
    - **Tarea:** Revisar regularmente los logs de autenticación (`/var/log/auth.log`, `/var/log/secure`), los logs de servicios específicos, y los logs del sistema (journald). Usar herramientas como `grep`, `journalctl`, `ausearch` (para logs de auditd) para buscar eventos relevantes.
6. **Políticas de Contraseña:**
    - **Propósito:** Forzar el uso de contraseñas fuertes, su cambio periódico y evitar la reutilización.
    - **Configuración:** Se configura principalmente a través de PAM (Revisado 210.2) usando módulos como `pam_pwquality.so` o `pam_cracklib.so` en la pila `password` de los servicios relevantes (ej: `system-auth`, `passwd`).
    - **Tarea:** Configurar y verificar que las políticas de contraseña están en vigor.
7. **Sistema de Auditoría del Kernel (`auditd`):**
    - **Propósito:** Proporcionar un registro detallado de eventos de seguridad que no se registran por defecto (ejecución de comandos específicos, acceso a archivos sensibles, cambios de permisos).

- **Tarea:** Configurar reglas de auditoría apropiadas en `/etc/audit/rules.d/` para monitorizar actividades clave y revisar periódicamente los logs generados por `auditd` (`/var/log/audit/audit.log`) usando `ausearch`. (Revisado 212.4 de lista anterior).

8. **Herramientas de Detección de Intrusiones (HIDS):**
    - **Propósito:** Detectar cambios en archivos (FIM) y buscar software malicioso (rootkits, backdoors).
    - **Tareas:** Configurar y programar (cron) verificaciones regulares de integridad de archivos con AIDE. Ejecutar escaneos periódicos de rootkits con `chkrootkit` y `rkhunter`. Revisar los informes generados. (Revisado 212.4 de lista anterior).
9. **Firewall y Seguridad de Servicios (Continuo):**
    - **Tareas:** Revisar y ajustar periódicamente las reglas del firewall (212.2). Revisar y endurecer las configuraciones de servicios (212.3) a medida que se descubren nuevas vulnerabilidades o se modifican los requisitos.
10. **Programación de Tareas de Seguridad:**
    - **Propósito:** Asegurar que las tareas de seguridad recurrentes se realicen automáticamente.
    - **Herramientas:** `cron` (`crontab -e`, `/etc/cron.d/`, `/etc/cron.hourly/`, etc.), systemd timers (`systemctl list-timers`).
    - **Tareas:** Programar actualizaciones del sistema, actualizaciones de bases de datos de virus/reglas de spam/AIDE, ejecuciones de escáneres de rootkits, rotación y archivo de logs (Revisado 208.2).