110.1 Realizar tareas de administración de seguridad - Ejercicios

*Nota: Estos ejercicios implican trabajar con configuraciones de seguridad sensibles (`sudoers`, gestión de grupos). Realízalos **SIEMPRE en un entorno de prueba (VM)** con usuarios/grupos de prueba. Necesitarás privilegios de superusuario (`sudo`).*

Ejercicio 10.1.1: Verificando la Pertenencia a Grupos de Sudo

- **Objetivo:** Identificar qué grupos tienen acceso a `sudo` y ver si tu usuario pertenece a ellos.
- **Requisitos:** Acceso a la línea de comandos.
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Identifica el grupo sudo relevante para tu distribución:** Es `sudo` en Debian/Ubuntu o `wheel` en RHEL/Fedora.
    3. **Verifica tu pertenencia a grupos:** Ejecuta `id`. Busca el grupo `sudo` o `wheel` en la lista de tus grupos. Si apareces, probablemente tienes acceso sudo a través de ese grupo (dependiendo de la configuración en `/etc/sudoers`).
    4. **Verifica quién más pertenece a ese grupo:** Ejecuta `getent group sudo` (Debian/Ubuntu) o `getent group wheel` (RHEL/Fedora). Esto lista los miembros del grupo.

Ejercicio 10.1.2: Explorando `/etc/sudoers` con `visudo`

- **Objetivo:** Ver el archivo de configuración de `sudo` de forma segura.
- **Requisitos:** Privilegios de superusuario (`sudo`).
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Abre el archivo `/etc/sudoers` con `visudo`:** Ejecuta `sudo visudo`. Esto abrirá el archivo en tu editor predeterminado (probablemente `vi` o `nano`).
    3. **Busca las reglas de acceso:**
        - Busca líneas que definan el acceso para el grupo `sudo` o `wheel`. A menudo verás una línea como `%sudo ALL=(ALL:ALL) ALL` (en Debian) o `%wheel ALL=(ALL) ALL` (en Red Hat), que significa que los miembros de ese grupo (`%`) pueden ejecutar comandos (`ALL`) como cualquier usuario (`ALL:ALL` o `ALL`) en cualquier host (`ALL`).
        - Busca reglas para usuarios individuales si existen.
        - Busca la directiva `Defaults` para ver opciones de seguridad globales.
    4. **Sal del editor SIN GUARDAR cambios:** Presiona `Esc` (si estás en `vi`), luego `:q!` y Enter. Si estás en `nano`, presiona `Ctrl+X` y responde `n` cuando pregunte si quieres guardar. Es crucial salir sin guardar si no estás realizando un cambio intencional.

Ejercicio 10.1.3: Añadiendo/Quitando un Usuario a un Grupo de Sudo (¡En VM de Prueba!)

- **Objetivo:** Dar o quitar acceso sudo a un usuario de prueba modificando su pertenencia a grupos.
- **Requisitos:** Un usuario de prueba (`testuser`) creado (ver Ej. 7.1.2). Identificar el grupo sudo relevante. Privilegios de superusuario (`sudo`). **Realiza este ejercicio solo en una VM de prueba.**
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Añade el usuario de prueba al grupo sudo (Debian/Ubuntu):** Ejecuta `sudo usermod -aG sudo testuser`.
    3. **Añade el usuario de prueba al grupo sudo (Red Hat/Fedora):** Ejecuta `sudo usermod -aG wheel testuser`.
    4. **Verifica que el usuario pertenece al grupo:** Ejecuta `id testuser`. Deberías ver el grupo `sudo` o `wheel` en la lista.
    5. **Prueba el acceso sudo como el usuario de prueba:** Abre una *nueva* terminal (o cierra sesión y vuelve a entrar como `testuser`). Ejecuta `sudo ls /root`. Se te pedirá la contraseña de `testuser`. Si ingresas la contraseña correcta, debería listar el contenido del directorio root.
    6. **Regresa a tu usuario normal (si cambiaste de usuario):** Ejecuta `exit`.
    7. **Quita el usuario de prueba del grupo sudo (Debian/Ubuntu):** Ejecuta `sudo deluser testuser sudo`.
    8. **Quita el usuario de prueba del grupo sudo (Red Hat/Fedora - requiere cambiar la lista de grupos completos):** Ejecuta `sudo usermod -G <grupos_actuales_sin_wheel> testuser`. Primero, identifica sus grupos actuales con `id testuser`. Luego usa `usermod -G` con esa lista menos `wheel`. O una alternativa más simple si solo está en ese grupo: `gpasswd -d testuser wheel`.
    9. **Verifica que el usuario ya no pertenece al grupo:** Ejecuta `id testuser`. No debería aparecer el grupo `sudo` o `wheel`.
    10. **Verifica que el acceso sudo fue removido (en una nueva sesión como testuser):** Intenta ejecutar `sudo ls /root` como `testuser`. Debería fallar con un mensaje de que el usuario no está en el archivo sudoers o no tiene permisos.
    11. **Limpia:** Si creaste `testuser`, puedes eliminarlo (`sudo userdel -r testuser`).

Ejercicio 10.1.4: Monitorizando Actividad de Login

- **Objetivo:** Usar comandos para ver quién ha iniciado sesión y quién está actualmente activo.
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Muestra un historial de logins recientes:** Ejecuta `last`. Verás una lista de usuarios, terminales, hosts de origen y tiempos de conexión/desconexión (leyendo `/var/log/wtmp`).

3. **Muestra quién está actualmente logueado:** Ejecuta `who`.
4. **Muestra quién está logueado y qué están haciendo:** Ejecuta `w`.

Ejercicio 10.1.5: Verificando la Integridad de Paquetes (Concepto)

- **Objetivo:** Entender cómo usar el gestor de paquetes para verificar la integridad de los archivos instalados.
- **Requisitos:** Acceso a la línea de comandos. Privilegios de superusuario (`sudo`).
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Verifica un paquete (Rama Debian/Ubuntu):** Ejecuta `sudo dpkg --verify bash` (o `dpkg -V bash`). Si no aparece ninguna salida, significa que los archivos instalados por el paquete `bash` coinciden con lo esperado según la base de datos de `dpkg`. Si hay salida, indicará discrepancias (ej: tamaño de archivo, suma de verificación, permisos).
    3. **Verifica un paquete (Rama Red Hat/Fedora):** Ejecuta `sudo rpm -V bash`. Similar a `dpkg -V`, si no hay salida, está bien. La salida indicará diferencias encontradas.
    4. **(Concepto):** Esta verificación compara los archivos instalados actualmente en el sistema con la información almacenada en la base de datos del gestor de paquetes (tamaño, sumas de verificación, permisos, propietario, etc.). Es una herramienta útil para detectar si los archivos del sistema han sido modificados inesperadamente (por un ataque o un error manual).