110.3 Asegurar datos con cifrado - Ejercicios

Nota: Estos ejercicios te guiarán a través del cifrado de archivos con `gpg` y la comprensión conceptual de LUKS. La práctica real con LUKS debe hacerse con cuidado en una partición de prueba o un archivo loopback para evitar la pérdida de datos.

Ejercicio 10.3.1: Cifrando y Descifrando un Archivo con `gpg` (Simétrico)

- **Objetivo:** Proteger un archivo de texto con una frase de paso usando `gpg`.
- **Requisitos:** El paquete `gnupg` instalado (`sudo apt install gnupg` o `sudo dnf install gnupg`).
- **Desarrollo Paso a Paso:**
    1. Abre una terminal en tu directorio personal (`cd ~`).
    2. **Crea un archivo de texto con contenido sensible:** Ejecuta `echo "Mi contraseña secreta es p@$$wOrd123!" > archivo_secreto.txt`.
    3. **Cifra el archivo:** Ejecuta `gpg -c archivo_secreto.txt`. Te pedirá que ingreses y confirmes una frase de paso. **Recuerda esta frase de paso.**
    4. **Verifica que se creó el archivo cifrado:** Ejecuta `ls -l archivo_secreto.txt.gpg`.
    5. **Intenta ver el contenido del archivo cifrado:** Ejecuta `cat archivo_secreto.txt.gpg`. Verás datos binarios ininteligibles.
    6. **Elimina el archivo original (¡cuidado! hazlo solo si estás seguro de que el cifrado funcionó y tienes la frase de paso):** Ejecuta `rm archivo_secreto.txt`.
    7. **Descifra el archivo cifrado y muestra el contenido (a stdout):** Ejecuta `gpg archivo_secreto.txt.gpg`. Te pedirá la frase de paso. Si la ingresas correctamente, imprimirá el contenido original a la terminal.
    8. **Descifra el archivo cifrado y guarda la salida en un nuevo archivo:** Ejecuta `gpg -o archivo_descifrado.txt archivo_secreto.txt.gpg`. Ingresa la frase de paso.
    9. **Verifica el contenido del archivo descifrado:** Ejecuta `cat archivo_descifrado.txt`.
    10. **Limpia:** Ejecuta `rm archivo_secreto.txt.gpg archivo_descifrado.txt`.

Ejercicio 10.3.2: Comprendiendo LUKS y `cryptsetup` (Conceptual y Exploración)

- **Objetivo:** Entender el propósito de LUKS y cómo se interactúa con dispositivos cifrados.
- **Requisitos:** El paquete `cryptsetup` instalado (`sudo apt install cryptsetup` o `sudo dnf install cryptsetup`). Acceso a la línea de comandos.
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.

2. **Explora los comandos de `cryptsetup`:** Ejecuta `cryptsetup --help` o `man cryptsetup`. Busca comandos como `luksFormat`, `luksOpen`, `luksClose`, `luksDump`, `luksUUID`.
3. **Si tienes alguna partición cifrada (ej: swap o root si se configuró en la instalación), intenta ver su estado (requiere sudo):** Ejecuta `sudo cryptsetup status <nombre_dispositivo_cifrado>`. El nombre del dispositivo mapeado suele estar bajo `/dev/mapper/`. Puedes identificar dispositivos cifrados con `lsblk -f` buscando el tipo `crypto_LUKS`.
4. **(Conceptual - Pasos para cifrar una partición de prueba - NO EJECUTAR si no estás seguro y en una VM de prueba con una partición *vacía*):**
    - Identifica una partición vacía (ej: `/dev/sdb1`).
    - `sudo cryptsetup luksFormat /dev/sdb1` (¡Esto borra datos y pide frase de paso!)
    - `sudo cryptsetup luksOpen /dev/sdb1 mi_prueba_cifrada` (Pide frase de paso y crea `/dev/mapper/mi_prueba_cifrada`)
    - `sudo mkfs.ext4 /dev/mapper/mi_prueba_cifrada` (Formatea el dispositivo descifrado)
    - `sudo mkdir /mnt/cifrado_test` (Crea punto de montaje)
    - `sudo mount /dev/mapper/mi_prueba_cifrada /mnt/cifrado_test` (Monta el sistema de archivos)
    - ... Usar `/mnt/cifrado_test` ...
    - `sudo umount /mnt/cifrado_test` (Desmonta)
    - `sudo cryptsetup luksClose mi_prueba_cifrada` (Cierra el volumen cifrado)
5. **(Conceptual - Desbloqueo en el arranque):** Explica al usuario (o busca en `/etc/crypttab` y `/etc/fstab`) cómo se configuran las particiones LUKS para que se pidan las frases de paso durante el arranque y se monten automáticamente después del desbloqueo. `crypttab` mapea dispositivos cifrados a nombres, y `fstab` monta el dispositivo mapeado de `/dev/mapper/`.

Ejercicio 10.3.3: Verificando Swap Cifrado (Concepto)

- **Objetivo:** Comprobar si la partición de swap está cifrada (una práctica de seguridad recomendada).
- **Requisitos:** Acceso a la línea de comandos. Puede que se haya configurado durante la instalación de la VM.
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Lista los dispositivos de bloque con su información:** Ejecuta `lsblk -f`.
    3. **Busca tu partición de swap:** Identifica la línea que tiene `PARTLABEL="swap"` o `TYPE="swap"`.

4. **Verifica el campo FSTYPE o TYPE:** Si aparece `crypto_LUKS` o similar en esa línea, significa que tu partición de swap está cifrada con LUKS. Si aparece solo `swap`, no lo está.
5. **Verifica con `swapon`:** Ejecuta `swapon --show --raw`. Busca la columna `TYPE`. Si la swap está cifrada, el tipo puede ser `partition` pero el dispositivo listado en `/proc/swaps` (que `swapon` lee) puede apuntar a un dispositivo mapeado bajo `/dev/mapper/` (ej: `/dev/mapper/cryptswap1`).