🔐 Examen 110 - Seguridad

110.3 Asegurar datos con cifrado

Teoría

El cifrado (o encriptación) es el proceso de convertir datos (texto plano) en un formato ilegible (texto cifrado) utilizando un algoritmo y una clave. Solo alguien que posea la clave correcta puede descifrar los datos y convertirlos de nuevo a su formato original. Cifrar datos es fundamental para garantizar la **confidencialidad**, especialmente para información sensible.

Existen dos escenarios principales para el cifrado:

- **Cifrado en Tránsito:** Protege los datos mientras se transmiten a través de una red (ej: HTTPS para conexiones web, SSH para acceso remoto). Vimos pinceladas de esto en 109.1 y 110.2.
- **Cifrado en Reposo:** Protege los datos mientras están almacenados en un medio (disco duro, pendrive, archivos individuales). Este objetivo se centra en esto.

Herramientas Comunes para Cifrado en Reposo (Relevantes para LPIC-1):

1. **Cifrado de Archivos Individuales con GnuPG (GNU Privacy Guard):**
    - GnuPG (`gpg`) es una implementación de OpenPGP. Permite cifrar y firmar datos. Soporta cifrado simétrico (con contraseña) y asimétrico (con clave pública/privada).
    - Para LPIC-1 básico, el enfoque suele estar en el **cifrado simétrico** para proteger archivos con una contraseña o frase de paso.
    - `gpg -c <nombre_archivo>`: Cifra el archivo especificado usando cifrado simétrico. Te pedirá una frase de paso dos veces. Crea un archivo cifrado con el mismo nombre y extensión `.gpg` (ej: `archivo.txt.gpg`). El archivo original *no se elimina*.
    - `gpg <nombre_archivo.gpg>`: Descifra un archivo cifrado con `gpg`. Te pedirá la frase de paso utilizada para cifrarlo. La salida descifrada se envía a la salida estándar (puedes redirigirla a un archivo).
        - `gpg -o <archivo_salida> <nombre_archivo.gpg>`: Descifra y guarda la salida en un archivo específico.
    - **Nota:** El paquete es típicamente `gnupg` en ambas ramas (Debian/Red Hat).
2. **Cifrado de Dispositivos de Bloque con LUKS (Linux Unified Key Setup):**
    - LUKS es un estándar para el cifrado de dispositivos de bloque (particiones, discos completos, volúmenes lógicos). Proporciona un formato estándar en disco y herramientas de gestión.
    - Beneficio: Cuando el sistema está apagado (o el dispositivo desmontado y cerrado), los datos son inaccesibles sin la clave (frase de paso o archivo de clave). Esto protege contra el robo físico del hardware.
    - La gestión de volúmenes LUKS se realiza con la herramienta **`cryptsetup`**.

- **Proceso Básico (Simplificado):**
    - **Preparar el dispositivo:** Decide qué partición o dispositivo usarás (¡se borrarán todos los datos existentes!). Ej: `/dev/sdb1`.
    - **Crear el volumen LUKS:** Inicializa el dispositivo con LUKS. `sudo cryptsetup luksFormat /dev/sdb1`. Esto sobrescribirá el inicio del dispositivo, creará la cabecera LUKS y te pedirá que establezcas una frase de paso fuerte.
    - **Abrir el volumen LUKS:** Hacer que el dispositivo cifrado sea accesible como un dispositivo de bloque estándar (mapeado). `sudo cryptsetup luksOpen /dev/sdb1 mi_volumen_cifrado`. Te pedirá la frase de paso LUKS. Si tiene éxito, creará un nuevo dispositivo de bloque descifrado en `/dev/mapper/mi_volumen_cifrado`.
    - **Formatear el dispositivo abierto:** Crear un sistema de archivos en el dispositivo descifrado. `sudo mkfs.ext4 /dev/mapper/mi_volumen_cifrado`. Ahora puedes usar este dispositivo como cualquier partición normal.
    - **Montar el sistema de archivos:** Montar el dispositivo descifrado a un punto de montaje. `sudo mount /dev/mapper/mi_volumen_cifrado /mnt/datos_cifrados`.
    - **Usar el sistema de archivos:** Ahora puedes leer y escribir archivos en `/mnt/datos_cifrados`.
    - **Desmontar y Cerrar:** Para proteger los datos, debes desmontar el sistema de archivos y luego cerrar el volumen LUKS. `sudo umount /mnt/datos_cifrados`. `sudo cryptsetup luksClose mi_volumen_cifrado`. Esto hace que el dispositivo cifrado original (`/dev/sdb1`) vuelva a ser inaccesible sin abrirlo de nuevo.
- **Nota:** Los volúmenes LUKS necesitan abrirse cada vez que el sistema arranca (lo que requiere ingresar la frase de paso durante el arranque si cifras la raíz o el home, o manualmente después del arranque para otras particiones). La automatización del desbloqueo (ej: usando archivos de clave en un medio separado) es posible pero más avanzada.
- **Paquetes:** La herramienta `cryptsetup` suele venir en el paquete `cryptsetup` en ambas ramas.
- **LPIC-1:** El conocimiento requerido suele ser sobre el *proceso* y los *comandos* básicos (`luksFormat`, `luksOpen`, `luksClose`), no necesariamente la configuración avanzada o la implementación en fstab/cripttab.

Consideraciones de Seguridad Adicionales:

- **Gestión de Claves/Frases de Paso:** Las frases de paso y las claves privadas deben ser fuertes y estar bien protegidas. La pérdida de la clave significa la pérdida *permanente* de los datos cifrados.

- **Backups:** Asegúrate de que tu estrategia de backup maneje los datos cifrados correctamente. Puedes hacer backup de los datos *descifrados* o hacer backup del volumen cifrado *completo* (en cuyo caso necesitas la clave para restaurar y acceder a los datos).
- **Swap Cifrado:** Es una buena práctica cifrar la partición de swap para evitar que datos sensibles en memoria (como contraseñas) se escriban en el disco en texto plano. Esto a menudo se configura durante la instalación o se habilita después.