📁 LPIC-2 / 🖥️ Examen 210 - Gestión de Clientes de Red - Ejercicios

Nota: Estos ejercicios implican explorar y potencialmente modificar archivos de configuración que controlan el acceso al sistema. ***Realiza modificaciones SOLO en una VM de prueba dedicada.*** *Asegúrate de tener una forma de recuperar el acceso si te bloqueas (ej: snapshot de la VM, acceso a la consola como root antes de modificar). Necesitarás privilegios de superusuario (`sudo`).*

Ejercicio 10.2.1: Explorando el Directorio de Configuración PAM

- **Objetivo:** Localizar los archivos de configuración PAM para diferentes servicios.
- **Requisitos:** Acceso a la línea de comandos. Privilegios de superusuario (`sudo`).
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Lista el contenido del directorio principal de configuración de PAM:** Ejecuta `ls -l /etc/pam.d/`. Verás archivos con nombres de servicios como `login`, `sshd`, `su`, `passwd`, `common-auth`, `system-auth`.
    3. **Visualiza el archivo `login`:** Ejecuta `sudo less /etc/pam.d/login`. Busca las secciones (`auth`, `account`, `password`, `session`) y las líneas de reglas.
    4. **Visualiza el archivo `sshd` (si usas SSH):** Ejecuta `sudo less /etc/pam.d/sshd`.
    5. **Visualiza un archivo de inclusión común (Diferencias):** En Debian, visualiza `sudo less /etc/pam.d/common-auth`. En Red Hat, visualiza `sudo less /etc/pam.d/system-auth`. Estos archivos contienen reglas que se aplican a múltiples servicios.

Ejercicio 10.2.2: Entendiendo la Sintaxis de las Reglas PAM

- **Objetivo:** Identificar los componentes (`type`, `control`, `module-path`, `module-options`) en las líneas de configuración.
- **Requisitos:** Visualizar archivos de configuración PAM (Ej. 10.2.1).
- **Desarrollo Paso a Paso:**
    1. Abre una terminal y visualiza un archivo de configuración (ej: `/etc/pam.d/sshd`).
    2. **Examina las líneas una por una:**
        - `auth required pam_unix.so nullok_secure`: `type` es `auth`, `control` es `required`, `module-path` es `pam_unix.so`, `module-options` es `nullok_secure`.
        - `@include common-auth`: `@include` es un tipo especial, `common-auth` es el archivo a incluir.
        - `account required pam_nologin.so`: `type` es `account`, `control` es `required`, `module-path` es `pam_nologin.so`.
    3. **Busca diferentes flags de control (`required`, `requisite`, `sufficient`, `optional`).**

4. **Busca diferentes nombres de módulo (`pam_unix.so`, `pam_deny.so`, etc.).**

Ejercicio 10.2.3: Viendo el Archivo `/etc/pam.conf` (si existe)

- **Objetivo:** Verificar si el sistema utiliza el archivo único tradicional.
- **Requisitos:** Acceso a la línea de comandos.
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Verifica si el archivo existe:** Ejecuta `ls -l /etc/pam.conf`.
    3. **Si existe, verifica si es un enlace simbólico o un archivo real:** A menudo, es un enlace simbólico apuntando a un archivo de compatibilidad o simplemente no existe o está vacío en sistemas modernos que usan `/etc/pam.d/`. Si es un archivo real y contiene configuraciones, el sistema puede estar usando una configuración de PAM más antigua o personalizada.
    4. **Visualiza su contenido si existe:** Ejecuta `sudo less /etc/pam.conf`. La sintaxis es diferente a la de los archivos en `/etc/pam.d/`; cada línea comienza con el nombre del servicio.

Ejercicio 10.2.4: (Conceptual) Impacto de los Flags de Control (`required` vs `requisite`)

- **Objetivo:** Entender conceptualmente cómo un fallo se maneja de forma diferente.
- **Requisitos:** Comprensión de los flags.
- **Desarrollo Paso a Paso (Conceptual):**
    1. Imagina una pila `auth` con dos módulos:

        ```
        auth required pam_module_A.so
        auth required pam_module_B.so
        ```

        - Si `pam_module_A.so` falla, PAM continúa ejecutando `pam_module_B.so`. El usuario recibe el fallo al final, pero no sabe si fue A o B lo que falló.
    2. Imagina una pila `auth` con `requisite`:

        ```
        auth requisite pam_module_A.so
        auth required pam_module_B.so
        ```

        - Si `pam_module_A.so` falla, PAM DETIENE inmediatamente el procesamiento para `auth` y el usuario recibe el fallo. El fallo ocurre antes de que se evalúe `pam_module_B.so`. Esto es más rápido pero menos seguro en cuanto a información sobre el fallo.
    3. Imagina una pila `auth` con `sufficient`:

        ```
        auth sufficient pam_module_A.so
        auth required pam_module_B.so
        ```

        - Si `pam_module_A.so` tiene éxito, PAM DETIENE inmediatamente el procesamiento para `auth` y el usuario PASA la autenticación para este tipo,

incluso si `pam_module_B.so` *hubiera fallado*. Si `pam_module_A.so` falla, PAM continúa y el resultado dependerá de `pam_module_B.so` (que es `required`).

Ejercicio 10.2.5: (Conceptual) Añadiendo una Regla Simple (¡Con Precaución!)

- **Objetivo:** Entender el proceso de modificación de la configuración PAM.
- *Requisitos:* Privilegios de superusuario (`sudo`). **VM de prueba.** Acceso a la consola de root como respaldo.
- **Desarrollo Paso a Paso (Conceptual):**
    1. Abre una terminal.
    2. **Haz una copia de seguridad del archivo que vas a modificar:** Ejecuta `sudo cp /etc/pam.d/sshd /etc/pam.d/sshd.orig`. **CRUCIAL.**
    3. **Edita el archivo (requiere sudo):** Ejecuta `sudo vi /etc/pam.d/sshd`.
    4. **Añade una regla de prueba (¡Solo para entender, NO para dejarla!):** Podrías añadir una regla *antes* de las reglas existentes para ver su efecto. Por ejemplo, añadir una línea para denegar siempre:

        ```
        # Añadida para pruebas
        auth required pam_deny.so
        # Reglas originales debajo...
        auth      requisite     pam_nologin.so
        ...
        ```

        - **Advertencia:** Si haces esto y recargas SSH, no podrás loguearte por SSH.
    5. **Guarda y sal.**
    6. **Si modificaste `sshd`, DEBES probar el login desde OTRA terminal ANTES de cerrar la actual.** Si el login falla, usa la copia de seguridad en la terminal original (o la consola de root) para restaurar el archivo original: `sudo cp /etc/pam.d/sshd.orig /etc/pam.d/sshd`.
    7. **Los cambios en los archivos de `/etc/pam.d/` son leídos por las aplicaciones que usan PAM la próxima vez que un usuario intenta autenticarse/usar el servicio.** No suelen requerir reiniciar servicios (excepto quizás algunos servicios que cachean la configuración PAM). Para SSH, el cambio se aplica a las nuevas conexiones.

Ejercicio 10.2.6: Verificando Logs de PAM

- **Objetivo:** Ver dónde se registran los mensajes de PAM.
- **Requisitos:** Acceso a la línea de comandos. Haber intentado loguearse o usar `su`/`sudo` recientemente. Privilegios de superusuario (`sudo`) para acceder a logs.
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.

2. **Ver logs de autenticación (Debian/Ubuntu):** Ejecuta `sudo less /var/log/auth.log`. Busca líneas que contengan "PAM" o nombres de servicios como "sshd", "login", "su", "sudo".
3. **Ver logs de autenticación (Red Hat/CentOS/Fedora):** Ejecuta `sudo less /var/log/secure`. Busca líneas similares.
4. **Ver logs de PAM en el journal (si usas systemd):** Ejecuta `journalctl -f -p info -_COMM=sshd` (para seguir logs de sshd con prioridad info o mayor) o `journalctl -f SYSLOG_IDENTIFIER=sshd` o simplemente `journalctl -f` y busca mensajes de PAM o los servicios relevantes. Intenta loguearte en otra terminal mientras sigues los logs.