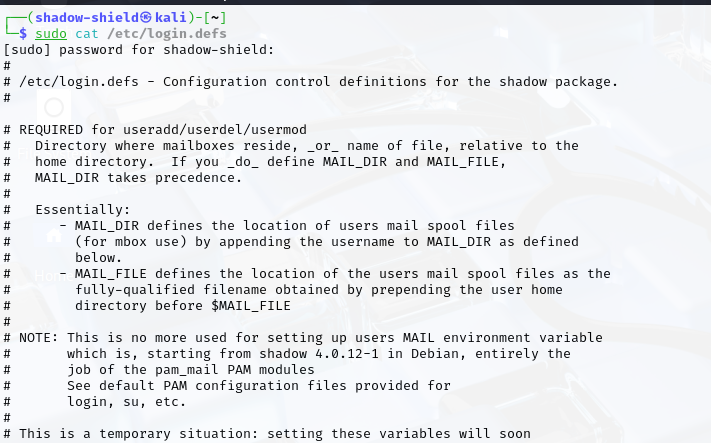
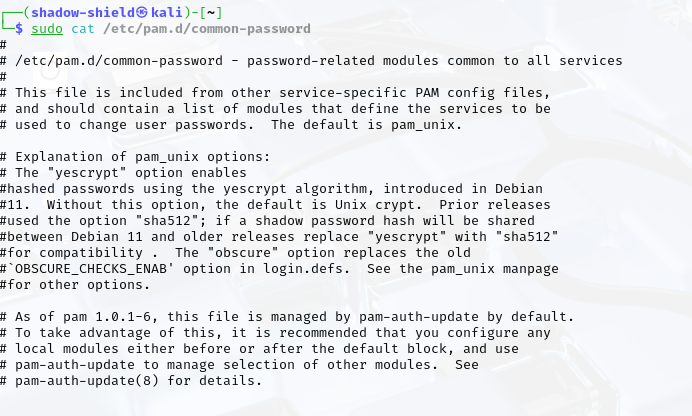
Laboratorio: Prácticas de Contraseña Segura (Creación y Gestión)

**Parte 1: Configuración de Políticas de Contraseñas Seguras**

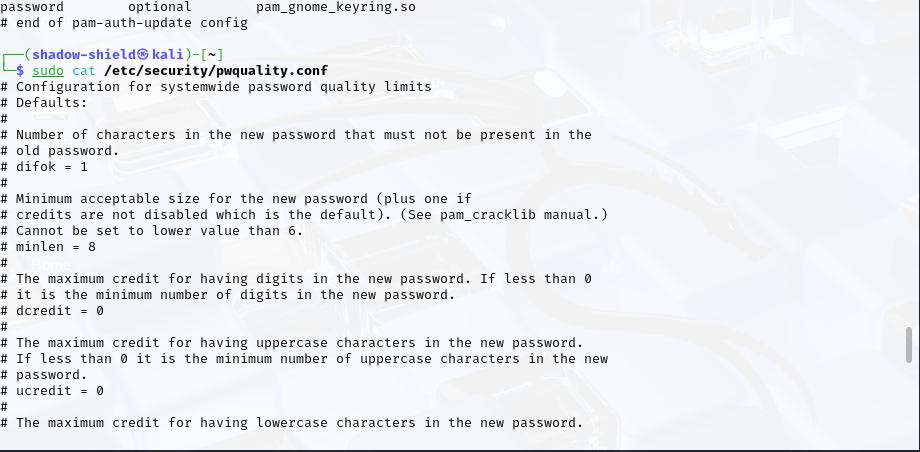
**Paso 1: Revisión de la Configuración Actual**

**sudo cat /etc/login.defs**

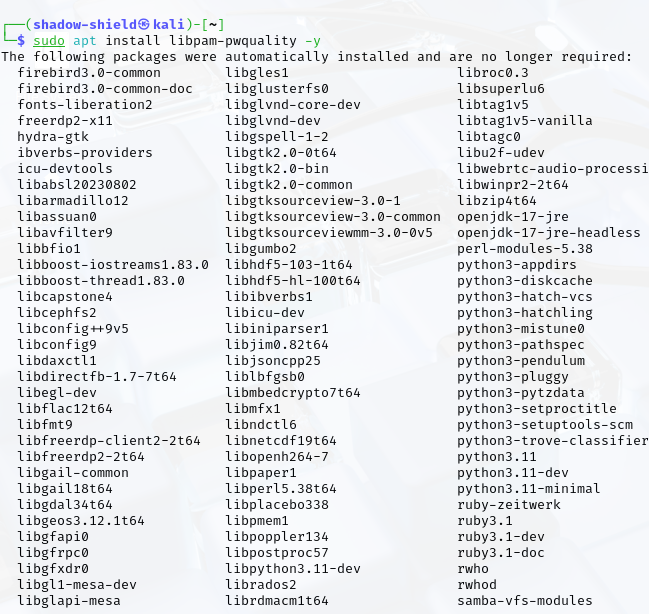


**sudo cat /etc/pam.d/common-password**

**Verificamos el archivo de configuración de pwquality**



**Paso 2: Establecer longitud mínima y complejidad**



**Editamos la configuración**



**Editamos PAM para aplicar estas reglas**

**sudo nano /etc/pam.d/common-password**



**PARTE 2: Implementar bloqueo tras intentos fallidos**

**Paso 3: Configurar pam\_faillock**

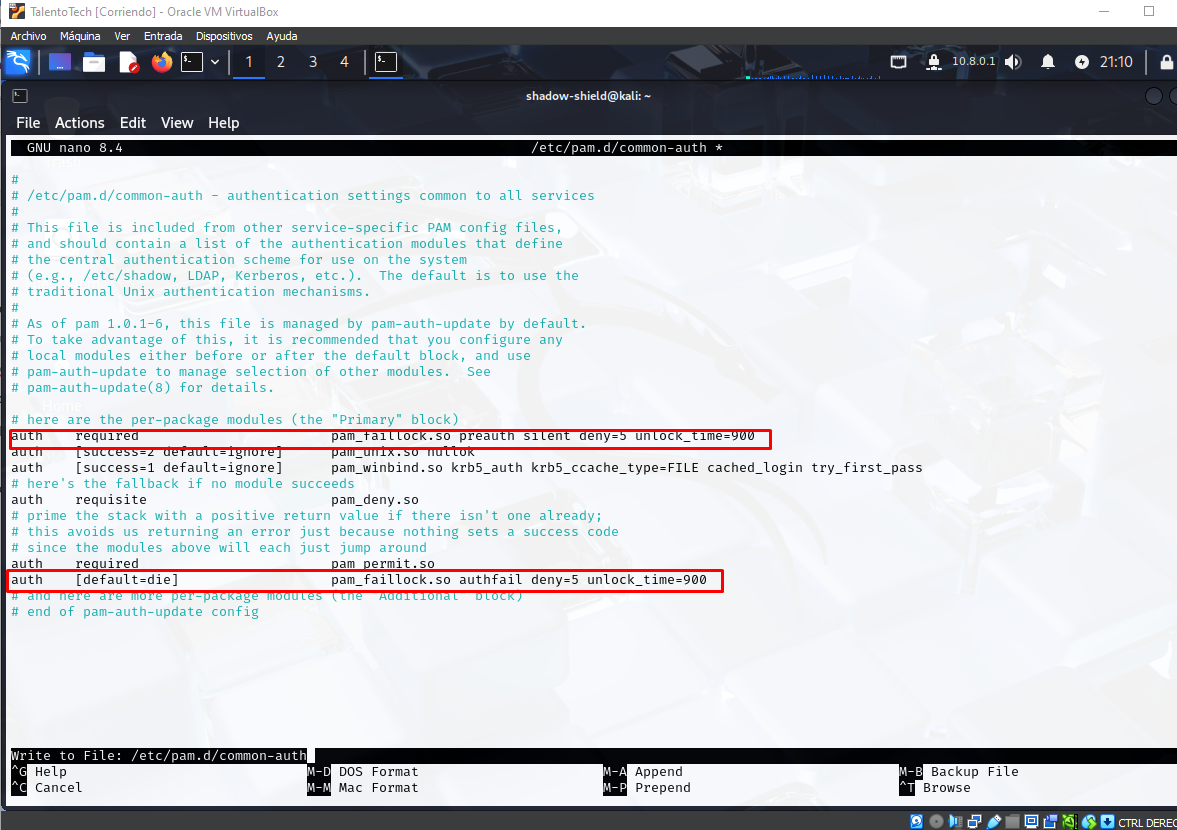
**sudo nano /etc/pam.d/common-auth**

Agrega al **inicio** del archivo

auth required pam\_faillock.so preauth silent deny=5 unlock\_time=900

**al** **final**

auth [default=die] pam\_faillock.so authfail deny=5 unlock\_time=900



**PARTE 3: Verificación y Documentación**

Paso 4: Verifica políticas de contraseña

Cambiamos la contraseña de un usuario y prueba requisitos

