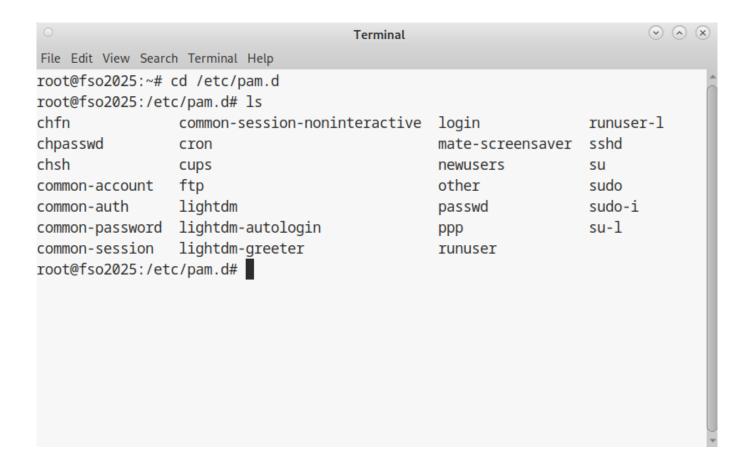
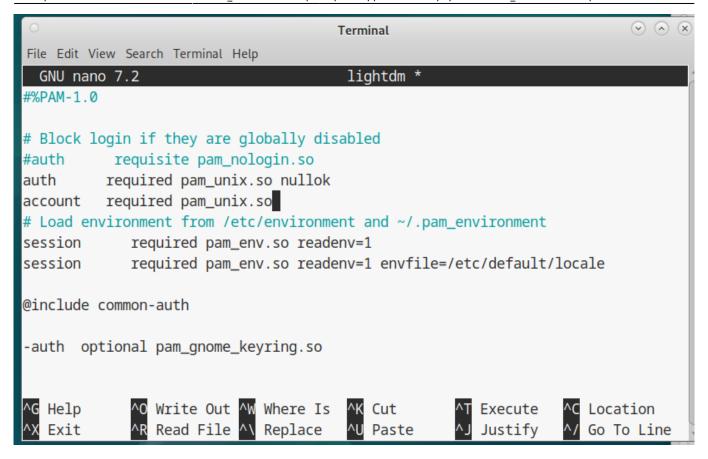
## [FORT] Práctica 4: Securizando las cuentas de usuario

### 1. Deshabilita el login a root, tanto en el Display Manager como en las Terminales Virtuales excepto tty3



Para deshabilitar estos permisos vamos a modificar los archivos de PAM que se encuentran en /etc/pam.d. Para deshabilitar el acceso a root en la interfaz gráfica modificamos el archivo lightdm con las siguientes lineas:

```
auth required pam_unix.so nullok account required pam_unix.so
```



Para deshabilitar los permisos en las terminales virtuales modificamos el archivo login con lo siguiente:

#### auth [success=1 default=ignore] pam securetty.so

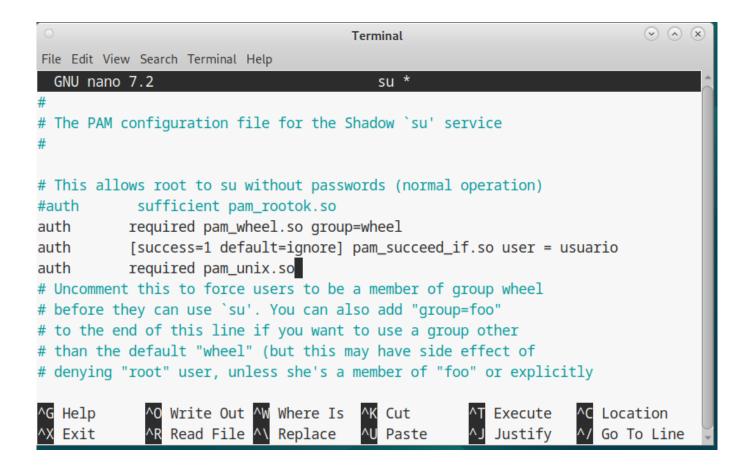
```
(v) (A) (X)
                                       Terminal
File Edit View Search Terminal Help
 GNU nano 7.2
                                         login
# The PAM configuration file for the Shadow `login' service
#
# Enforce a minimal delay in case of failure (in microseconds).
# (Replaces the `FAIL_DELAY' setting from login.defs)
# Note that other modules may require another minimal delay. (for example,
# to disable any delay, you should add the nodelay option to pam_unix)
            optional pam_faildelay.so delay=3000000
#auth
            [success=1 default=ignore] pam_securetty.so
auth
# Outputs an issue file prior to each login prompt (Replaces the
# ISSUE_FILE option from login.defs). Uncomment for use
# auth
             required
                        pam_issue.so issue=/etc/issue
                Write Out ^W Where Is
                                                                      Location
^G Help
                                           Cut
                                                        Execute
   Exit
                Read File ^\
                             Replace
                                           Paste
                                                        Justify
                                                                      Go To Line
```

# 2. Usando el módulo pam\_wheel.so haz que solo usuario, user001, user002, user003 y user004 puedan volverser root con SU.

Usuario no necesita saber la contraseña, mientras que los usuarios del 001 al 004 la necesitan para convertirse en root. Al resto de usuarios no se les preguntará por la contraseña.

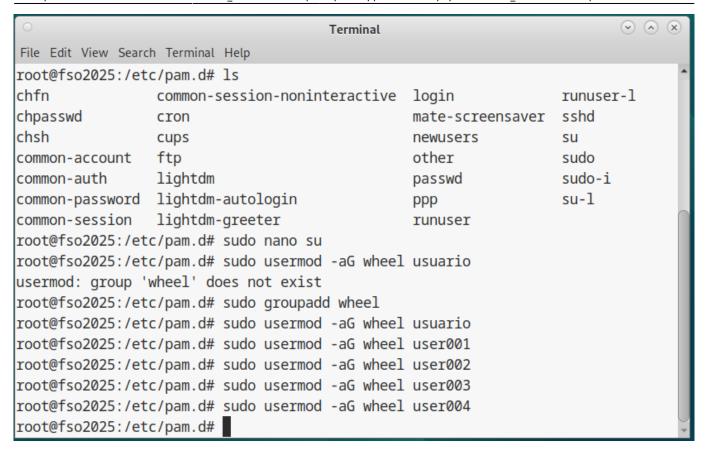
Para aplicar los ajustes debemos modificar el archivo /etc/pam.d/su con las siguientes líneas:

```
auth required pam_wheel.so group=wheel #Permite a los usuario del grupo Wheel a usar su sin contraseña auth [success=1 default=ignore] pam_succeed_if.so user = usuario #Permite al usuario "usuario" usar su sin contraseña auth required pam_unix.so #se configura para permitir que los usuarios indicados tengan que poner la contraseña
```



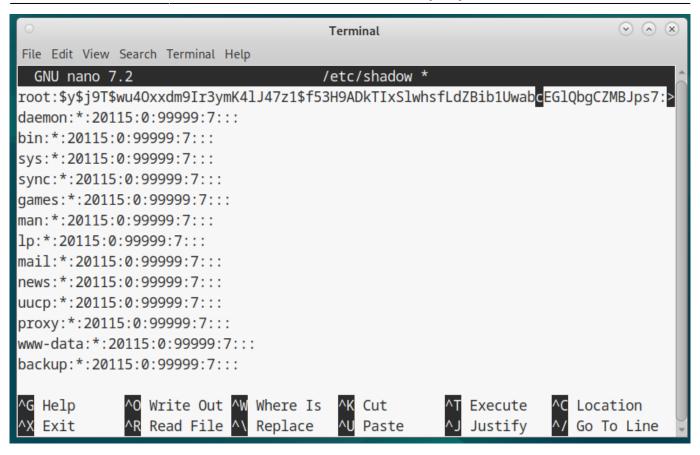
También debemos añadir a los usuarios en cuestión al grupo wheel con el siguiente comando:

```
sudo usermod -aG wheel usuario
sudo usermod -aG wheel user001
sudo usermod -aG wheel user002
sudo usermod -aG wheel user003
sudo usermod -aG wheel user004
```

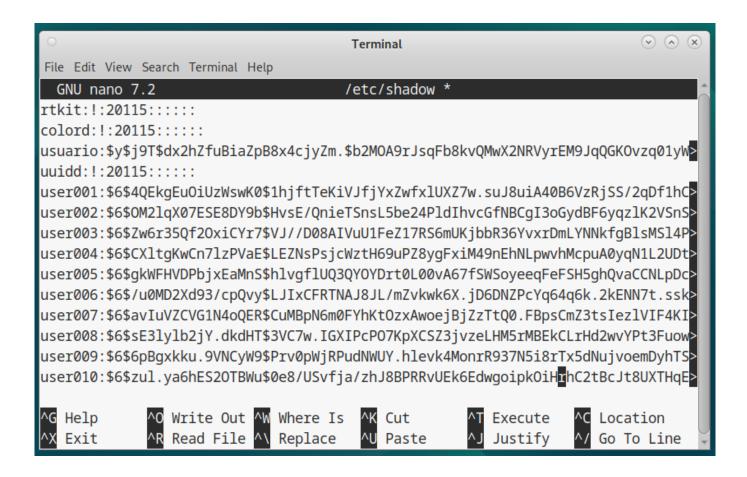


## 3. ¿Que método de cifrado se usa para las contraseñas? ¿Ha sido usado el mismo método para todas las contraseñas en el sistema?

Deberíamos usar SHA256 y cambiar las contraseñas de todos los usuarios a SHA256 ¿Como deberíamos hacer? Echando un vistazo a /etc/shadow podemos ver las contraseñas cifradas por un lado para root:



y por otro lado para los demás usuarios:

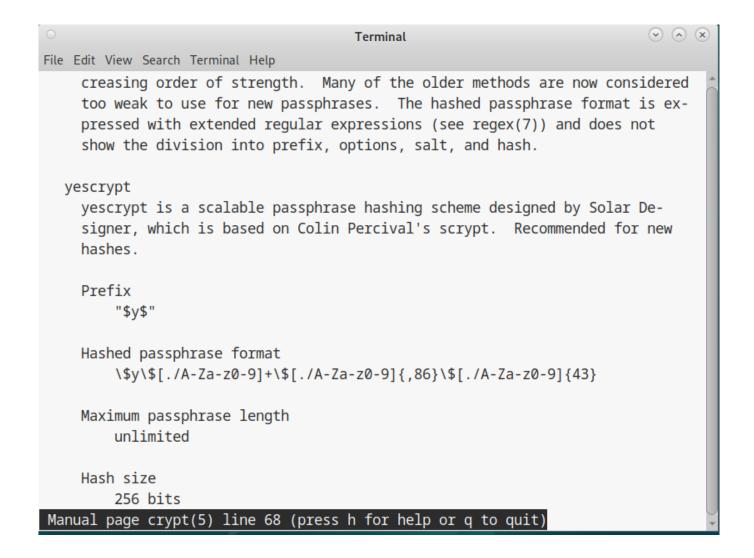


Las contraseñas en general comienzan con una cadena \\$<caracter>\\$, estos primeros 3 caracteres

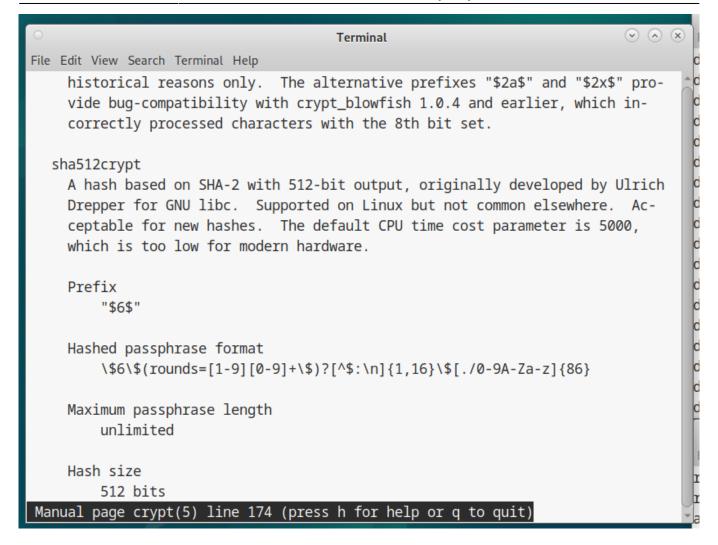
señalan en que cifrado viene cada contraseña, por lo que sabemos que:

- Root y usuario comienzan con \\$y\\$, por lo que sabemos que usa yescrypt
- El resto de usuarios comienzan con \\$6\\$, por lo que sabemos que usan SHA-512

Esto lo sabemos gracias a las salidas del comando man 5 crypt, donde podemos ver que es cada cifrado, por ejemplo, el de root y usuario sería el siguiente:

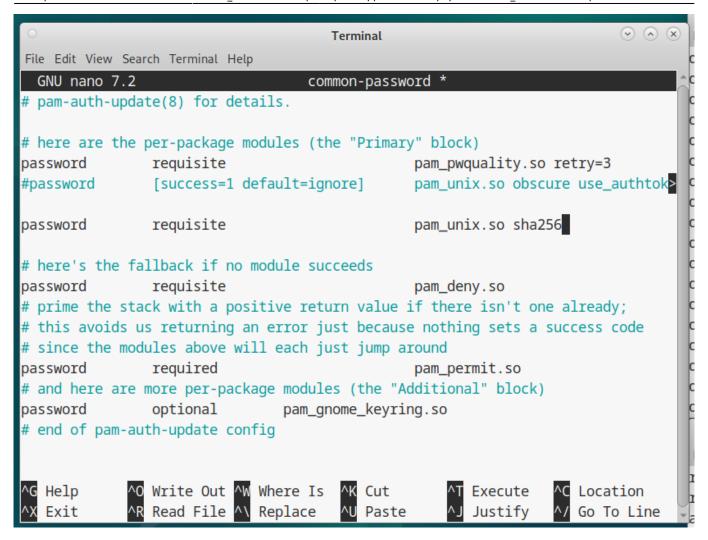


Y el del resto de usuarios sería el siguiente:



Para cmbiar el cifrado de todos los usuarios a SHA256 habría que primero cambiar cual es el cifrado predeterminado en /etc/pam.d/common-password con las siguientes líneas:

password requisite pam unix.so sha256



Y tras eso modificar todas las contraseñas con un script como este:

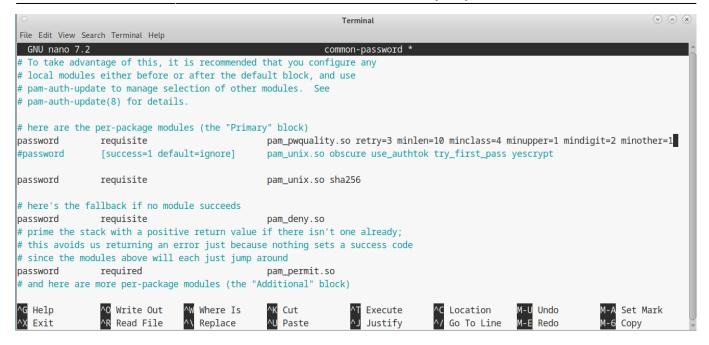
```
for user in $(cut -f1 -d: /etc/passwd); do
  sudo passwd --stdin $user
done
```

### 4. Fuerza los siguientes requisitos para los cambios de contraseña

- Al menos 10 caracteres
- Debe contener mayúsculas y minúsculas
- Debe contener al menos 2 dígitos
- Debe contener al menos un caracter no alphanumérico
- No puede ser una de las 3 contraseñas anteriores

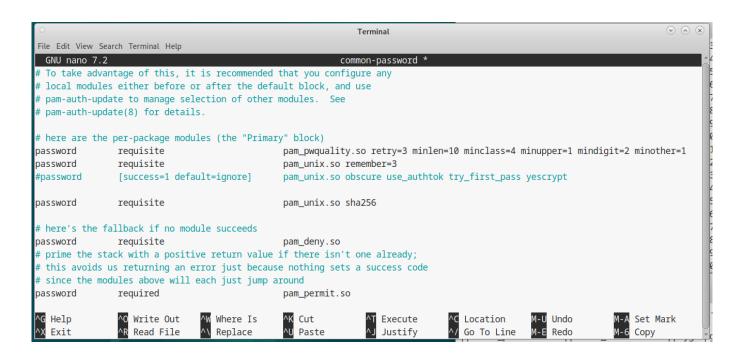
Para aplicar dichas políticas de contraseña debemos modificar el módulo common-password de PAM añadiendo la siguiente línea:

password requisite pam\_pwquality.so retry=3 minlen=10 minclass=4 minupper=1
mindigit=2 minother=1



Tras esto faltaría por establecer que no se puedan usar las 3 contraseñas anteriores, apara ello añadimos en el mismo fichero la siguiente línea:

password requisite pam\_unix.so remember=3



#### 5. El usuario user010 SOLO puede ejecutar ls, rm, vi y wc

Para poder limitar el usuario de estam manera debemos comenzar por

Last update: 2025/02/25 15:16

From:

http://knoppia.net/ - Knoppia

Permanent link:

http://knoppia.net/doku.php?id=master\_cs:fortificacion:p4&rev=1740496570

Last update: 2025/02/25 15:16

