El fichero /etc/login.defs

Establece una serie de configuraciones para la administración y el acceso de los usuarios en el sistema. Directivas más importantes:

- **De gestión**
  - *UID_MIN, UID_MAX*: mínimo y máximo de los UID's que se asignan a los nuevos usuarios
  - *GID_MIN, GID_MAX*: mínimo y máximo de los GID's que se asignan a los nuevos grupos
  - *UMASK*: Establece la máscara de permisos para los nuevos directorios home que se crean en el sistema. Por defecto 022, mejor seguridad 077
- **Para identificación**
  - *LOGIN_RETRIES*: Cantidad de intentos permitidos si la contraseña es incorrecta
  - *LOGIN_TIMEOUT*: Tiempo de espera para el login
  - *DEFAULT_HOME*: Establece si un usuario se puede loguear si no tiene acceso a su directorio home

El fichero /etc/login.defs

Directivas más importantes:

- **Para contraseñas**
  - *PASS_MAX_DAYS*: Número de días de validez de la contraseña
  - *PASS_MIN_DAYS*: Número de días mínimos entre cambio de contraseña
  - *PASS_WARN_AGE*: Número de días para que empiece a avisar de que la contraseña va a caducar.
  - *ENCRYPT_METHOD*: Indica el método de cifrado para las contraseñas, por defecto SHA512

Algunas directivas de este fichero han sido sustituidas por métodos más modernos, sobre todo por el uso de PAM (Pluggable Authentication Modules)

Complejidad de las contraseñas

Para poder configurar la complejidad de las contraseñas de nuestro sistema se usa el módulo de PAM pwquality (que mejora cracklib).

Su fichero de configuración es el `/etc/security/pwquality.conf`.

Opciones:

- **minlen**: Tamaño mínimo aceptable para la nueva contraseña.
- **dcredit**: Crédito máximo por tener *dígitos* en la nueva contraseña.
- **ucredit**: Crédito máximo por tener letras *mayúsculas* en la nueva contraseña.
- **lcredit**: Crédito máximo por tener letras *minúsculas* en la nueva contraseña.
- **ocredit**: Crédito máximo por tener *otros caracteres* en la nueva contraseña.

Un número negativo indica el numero mínimo de caracteres de esa clase

SEGURIDAD EN LA GESTIÓN DE USUARIOS

Opciones de pwquality:

- **difok**: Número de caracteres en la nueva contraseña que no deben coincidir con la contraseña anterior.
- **badwords**: Lista de palabras separadas por espacios que no deben incluirse en la contraseña.
- **minclass**: Número mínimo de clases de caracteres requeridas para la nueva contraseña
- **maxrepeat**: Número máximo de caracteres repetidos.
- **maxclassrepeat**: Número máximo de caracteres consecutivos en la misma clase.
- **dictpath**: Ruta a los diccionarios de clacklib.

Con el comando **pwscore** podemos comprobar la robustez de una contraseña

Bloquear usuario por accesos fallidos

Una buena política para un sistema es bloquear a los usuarios que introduzcan mal su contraseña de forma continuada. Esto puede prevenir ataques de fuerza bruta o accesos no autorizados. Para conseguirlo desde PAM vamos a utilizar la librería **pam_tally2**

Para utilizarlo tendremos que añadirlo al fichero */etc/pam.d/common-auth*

```
auth    required    pam_tally2.so    deny=4    unlock_time=900    even_deny_root
```

- **deny**: El límite de intentos permitidos, al llegar, se bloquea al usuario.
- **even_deny_root**: Indica que también se bloqueará al root
- **unlock_time**: Cantidad de segundos que tienen que pasar hasta que se desbloquee al usuario.

Con el comando pam_tally2 podemos ver un registro de intentos fallidos y por usuario. Con *-u nombre_usuario* filtra por usuario y con *--reset* pone a cero los contadores de fallos