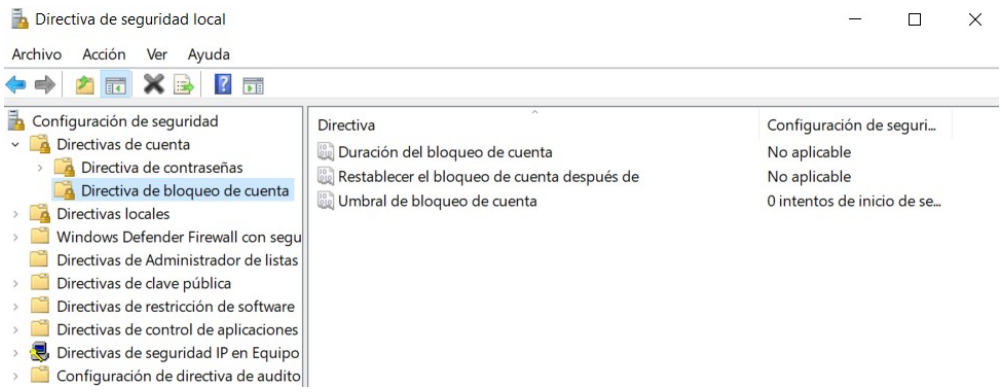
ACTIVITAT | Directiva de bloqueig de compte a Windows

Un altre aspecte que pot millorar el nostre nivell de seguretat pel que fa a les contrasenyes del comptes d'usuari és aplicar directives per a bloquejar els usuaris que facin un número d'intents erronis en l'accés al equip.

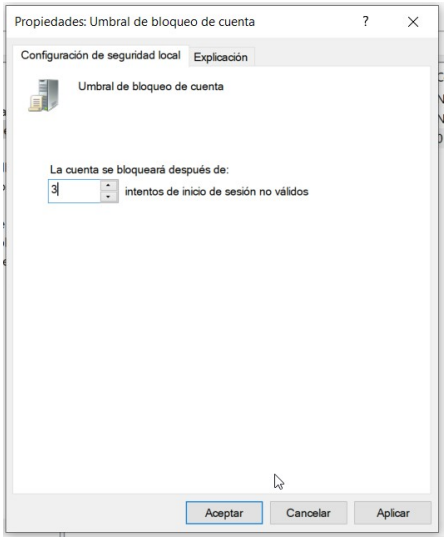
Accedeix a les directives de comptes d'usuari i explica les 3 directives relacionades amb el bloqueig de comptes d'usuari. Fes algunes proves amb un usuari per veure els missatges que envia el sistema quan es bloqueja un usuari. Com es pot desbloquejar posteriorment?

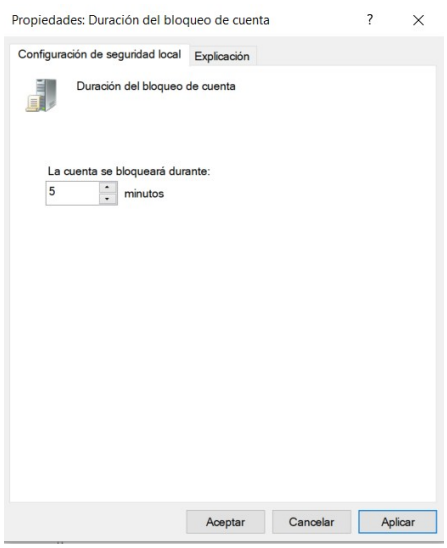
- Directivas de cuentas de usuario:

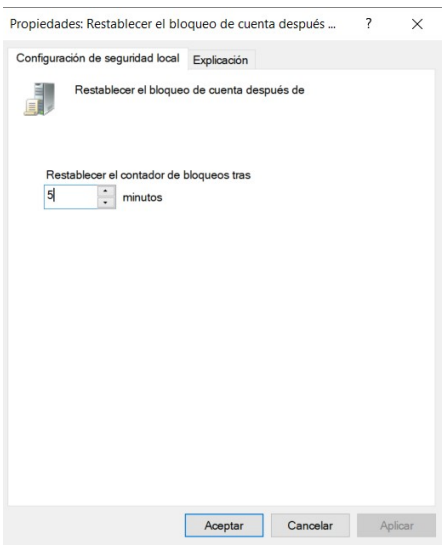
- **Duración del bloqueo de cuenta:** Establece el periodo de tiempo para mantener una cuenta bloqueada después de que esta alcance todos los intentos fallidos.
- **Umbral de bloqueo de cuenta:** Determina el numero de intentos para poder iniciar sesión antes de que se bloquee la cuenta.
- **Restablecer bloqueo de cuenta después de:** Define el tiempo que debe transcurrir para que los intentos del umbral de bloqueo de cuenta se reinicien.



- Configuración de directivas de usuario:







- Prueba de bloquear usuario:

Para desbloquear una cuenta hay dos opciones:

- Esperar el tiempo necesario para que se desbloquee.
- Entrar con una cuenta que tenga privilegios y desbloquear al usuario manualmente desde la pestaña de seguridad.

ACTIVITAT Política de contrasenyes a Ubuntu

Anem a treballar amb l'exposat anteriorment dissenyant una política de contrasenyes pel nostre sistema Ubuntu que compleixi les següents condicions:

Ha d'utilitzar els paràmetres de seguretat que proporcional la llibreria pam_cracklib per defecte.

Un usuari tindrà 3 opcions per ficar correctament la seva contrasenya.

Aquesta tindrà una longitud mínima de 10 caràcters, dels quals només un ha de ser en majúscules i com a mínim 2 han de ser números.

A més, s'ha de conservar un historial de les últimes 2 contrasenyes que no es podran reutilitzar.

A més, la contrasenya caducarà cada mes, i s'avisarà 3 dies abans a l'usuari de que cal canviar-la.

Un cop fetes aquestes configuracions, crea un nou usuari i comprova que la teva política de contrasenyes funciona correctament. Afegim un punt extra per tal de que investiguis:

- Com puc aconseguir que en el meu sistema no estigués permesa específicament una contrasenya concreta, per exemple: asWd345jku, que tindria que ser vàlida segons la política de contrasenyes anteriors?

- Instalación libpam-cracklib:
sudo apt install libpam-cracklib

```
willy@willy-VirtualBox:~/Desktop$ sudo apt install libpam-cracklib
[sudo] password for willy:
Reading package lists... Done
Building dependency tree... Done
```

- Configurar la longitud mínima, uso de mayúsculas y números:
sudo nano /etc/security/pwquality.conf

+ minlen = 10

```
# Minimum acceptable size for the new password (plus one if
# credits are not disabled which is the default). (See pam_cracklib manual.)
# Cannot be set to lower value than 6.
# minlen = 10
```

+ 1 mayúscula y 2 o mas números

```
The maximum credit for having uppercase characters in the new password.
If less than 0 it is the minimum number of uppercase characters in the new
password.
ucredit = +1
```

```
The maximum credit for having digits in the new password. If less than 0
it is the minimum number of digits in the new password.
dcredit = -2
```

- Configurar el historial de contraseñas:

(ultimas dos passw no se pueden modificar)

```
# Number of characters in the new password that must not be present in the
# old password.
# difok = 2
```

- Configurar la caducidad de la contraseña y el aviso:
sudo nano /etc/login.defs

```
# Password aging controls:
#
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#       PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   30
PASS_MIN_DAYS   0
PASS_WARN_AGE   3
```

- Creación de usuario y prueba de contraseñas incorrectas

```
willy@willy-VirtualBox:~/Desktop$ sudo adduser kevin
Adding user `kevin' ...
Adding new group `kevin' (1001) ...
Adding new user `kevin' (1001) with group `kevin' ...
Creating home directory `/home/kevin' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
```

- Solo minúsculas

```
Retype new password:
Sorry, passwords do not match.
```

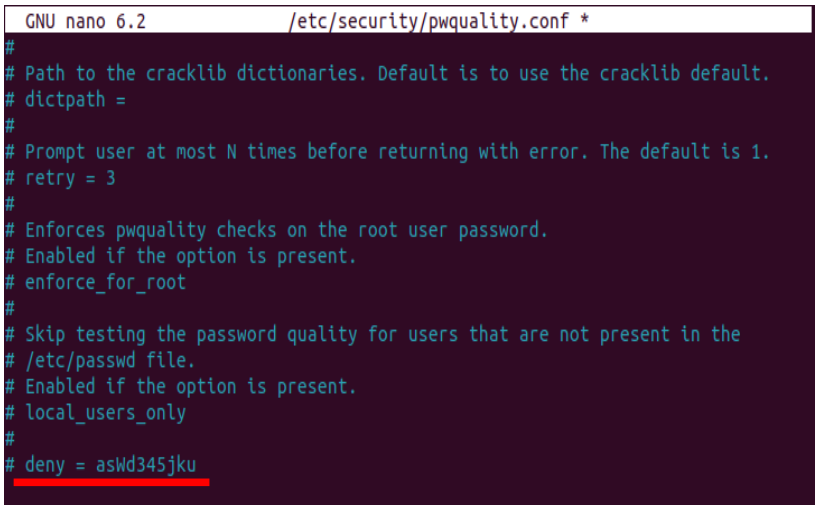
- Sin mayúsculas o sin números

```
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
```

- Contraseña corta

- Dentro del archivo pam_pwquality.conf, podemos agregar la siguiente línea para excluir contraseñas específicas:

deny = asWd345jku



webgrafia:

https://learn.microsoft.com/es-es/windows/security/threat-protection/security-policy-settings/account-lockout-policy
https://medium.com/guayoyo/configura-la-política-de-contraseñas-en-debian-y-ubuntu-para-proteger-más-tu-equipo-8ceaaa54da38

pdf seguretat de comptes d'usuari