

Seguretat lògica

Seguretat lògica

Activitat 1: Definir una Política de contrasenyes en Windows

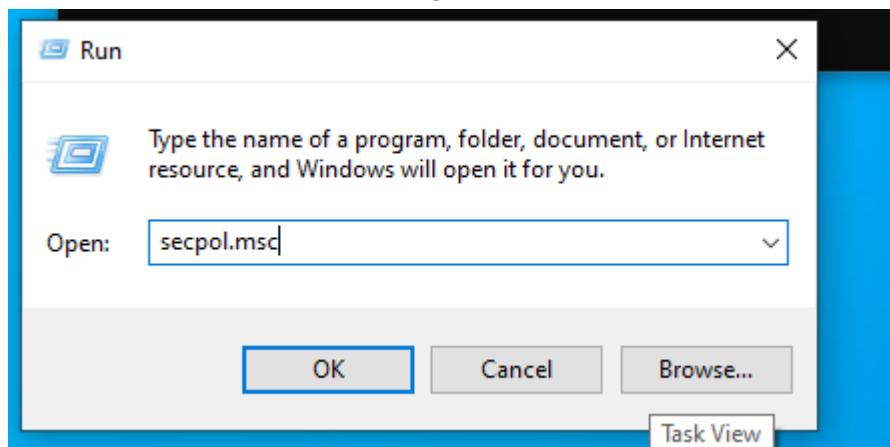
- Crear tres usuaris amb contrasenyes simples:

- Obre el Gestor d'Usuaris de Windows
- Crea usuaris amb contrasenyes:

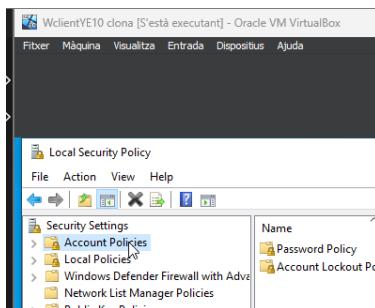
The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The user has run the command "net user usuario1 12345 /add" which completed successfully. Then, they ran "net user usuario1 castanya /add" which also completed successfully. Finally, they ran "net user usuario2 moniato /add" which completed successfully. The prompt ends with "C:\Windows\system32>".

- Definir una política de contrasenyes:

- Obre l'Editor de Polítiques de Seguretat Local (secpol.msc)

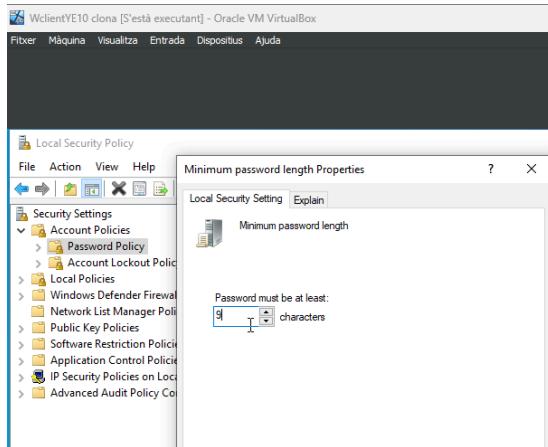


- Ves a Polítiques de Comptes > Polítiques de contrasenyes.

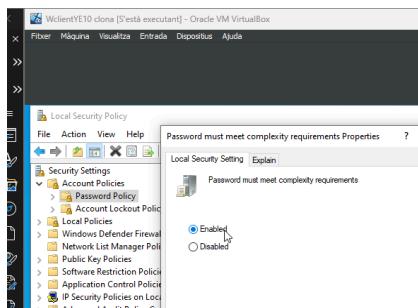


○ Configura:

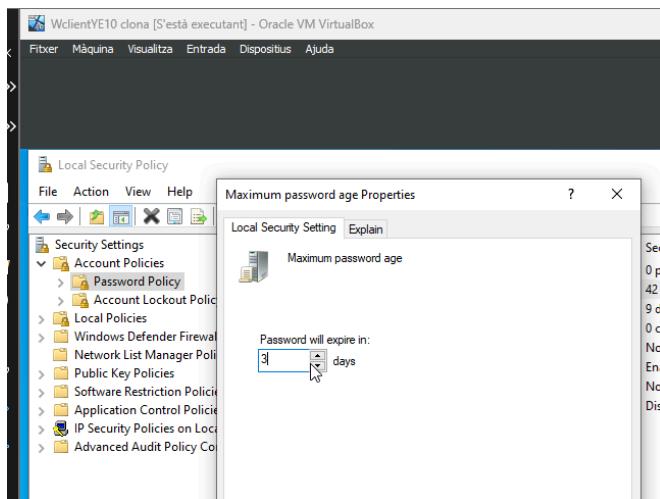
- Longitud mínima de la contrasenya: 9 caràcters.



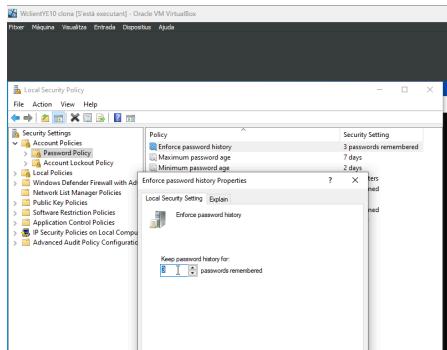
- Complexitat de contrasenyes: Habilitat (números, lletres i símbols).



- Durada màxima de la contrasenya: 3 dies.

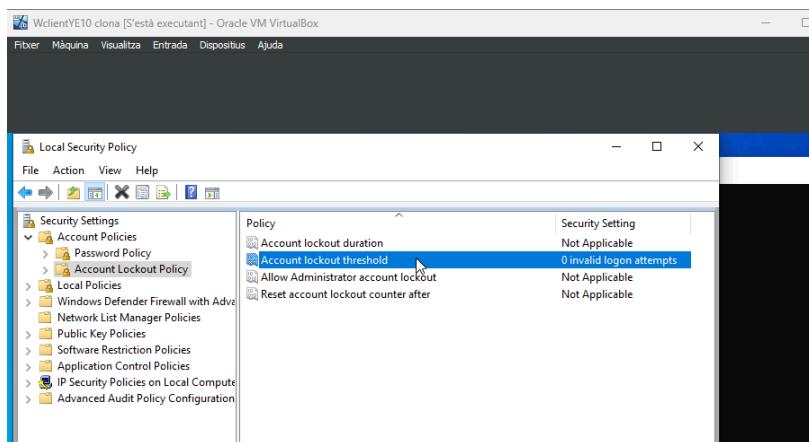


■ Conservar les darreres contrasenyes: 3 contrasenyes anteriors.



3. Bloqueig del compte:

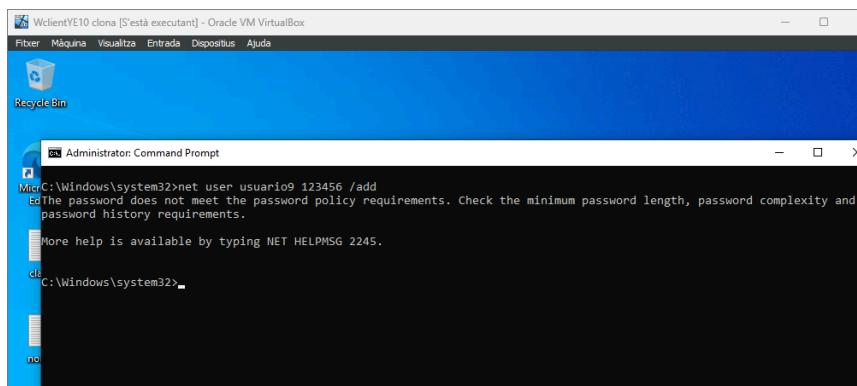
- Ves a Polítiques de Comptes > Política de bloqueig de comptes.



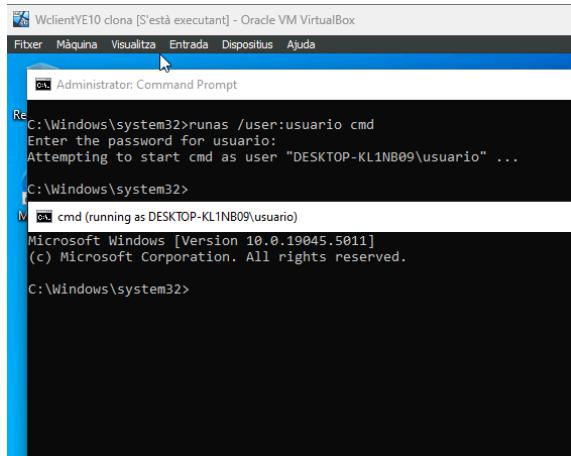
- Configura el bloqueig després de 3 intents fallits.

4. Provar la política:

- Reinicia el sistema.
- Intenta crear un usuari nou amb una contrasenya simple (no complirà la política).

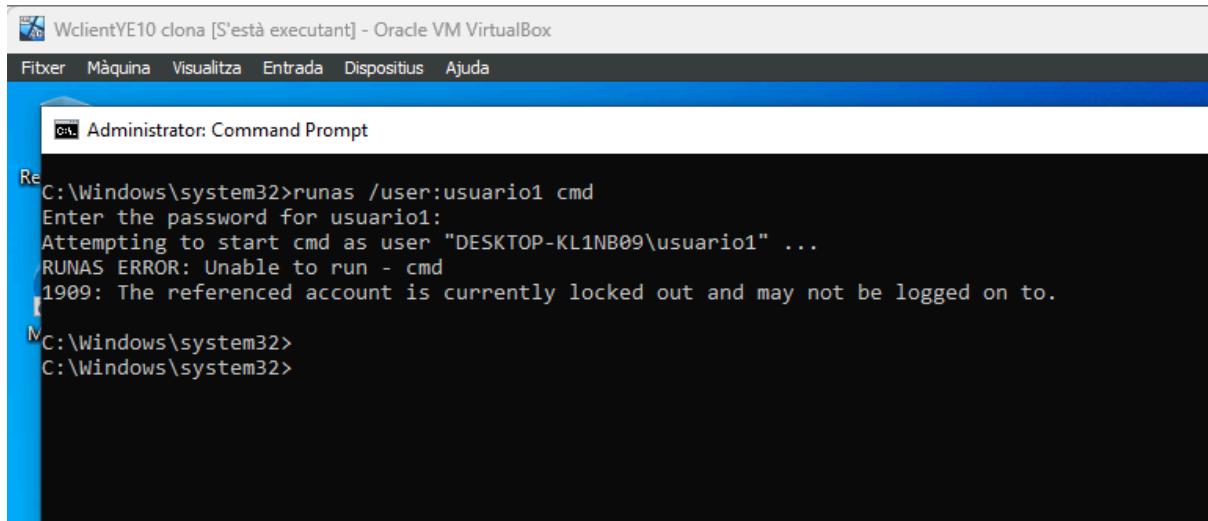


- Intenta accedir amb un dels usuaris antics (comprova que les contrasenyes ja no són vàlides).



WclientYE10 clona [S'està executant] - Oracle VM VirtualBox
Fitxer MÀquina Visualitzar Entrada Dispositius Ajuda
Administrator: Command Prompt
C:\Windows\system32>runas /user:usuario cmd
Enter the password for usuario:
Attempting to start cmd as user "DESKTOP-KL1NB09\usuario" ...
C:\Windows\system32>
M:\> cmd (running as DESKTOP-KL1NB09\usuario)
Microsoft Windows [Version 10.0.19045.5011]
(c) Microsoft Corporation. All rights reserved.
C:\Windows\system32>

- Prova fallar la contrasenya 4 vegades i comprova que el compte es bloqueja.



WclientYE10 clona [S'està executant] - Oracle VM VirtualBox
Fitxer MÀquina Visualitzar Entrada Dispositius Ajuda
Administrator: Command Prompt
Re C:\Windows\system32>runas /user:usuario1 cmd
Enter the password for usuario1:
Attempting to start cmd as user "DESKTOP-KL1NB09\usuario1" ...
RUNAS ERROR: Unable to run - cmd
1909: The referenced account is currently locked out and may not be logged on to.
M:\>C:\Windows\system32>
C:\Windows\system32>

Activitat 2

Hash SHA512

92f39f7f2a869838cd5085e6f17fc82109bcf98cd62a47cbc379e38de80bbc0213a23cee6e4a1
3de6caae0add8a390272d6f0883c274320b1ff60dbcfc6dd750

De quin password estem parlant?

Admin1234

Com l'has obtingut?

<https://md5hashing.net/hash/>

Activitat 3: Contrasenyes amb John The Ripper

1. Instal·lar John The Ripper:

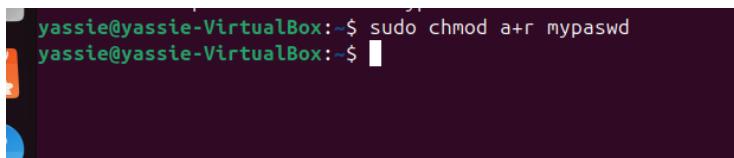
```
yassie@yassie-VirtualBox:~$ sudo apt install john
E: Operación inválida: istall
yassie@yassie-VirtualBox:~$ sudo apt install john
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  john-data
Se instalarán los siguientes paquetes NUEVOS:
  john john-data
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 32 no actualizados.
Se necesita descargar 9.351 kB de archivos.
Se utilizarán 20,6 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://es.archive.ubuntu.com/ubuntu noble/main amd64 john-data all 1.9.0-2
build1 [9.141 kB]
3% [1 john-data 373 kB/9.141 kB 4%]                                         42,6 kB/s 3min 30s
```

2. Fusionar els fitxers /etc/passwd i /etc/shadow:



```
yassie@yassie-VirtualBox:~$ sudo unshadow /etc/passwd /etc/shadow > mypasswd
yassie@yassie-VirtualBox:~$
```

3. Modifica permisos del fitxer:



```
yassie@yassie-VirtualBox:~$ sudo chmod a+r mypasswd
yassie@yassie-VirtualBox:~$
```

4. Executar John per desxifrar contrasenyes:

```
yassie@yassie-VirtualBox:~$ sudo john mypasswd
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1234          (yassie)
1234          (pio)
1234          (emma)
3g 0:00:00:26 100% 2/3 0.1133g/s 100.1p/s 111.7c/s 111.7C/s 123456..pepper
Use the "--show" option to display all of the cracked passwords reliably
Session completed
yassie@yassie-VirtualBox:~$
```

5. Si els hash comencen amb \$y\$:

```
yassie@yassie-VirtualBox:~$ sudo john --format=crypt mypasswd
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/64])
No password hashes left to crack (see FAQ)
yassie@yassie-VirtualBox:~$
```

(no hay)

6. Crear un diccionari per atacar les contrasenyes:

i. Crea un fitxer

7.  yassie@yassie-VirtualBox:~\$ nano dicionario.txt

En aquest fitxer, escriu una llista de possibles contrasenyes.

```
yassie@yassie-VirtualBox:~$ cat dicionario.txt
1234
password
13454
```

8. Executar l'atac de diccionari amb John The Ripper

John The Ripper llegirà les contrasenyes del fitxer dicioario.txt i les provarà una per una contra les contrasenyes xifrades del fitxer mypasswd.

```
sudo john --wordlist=mydictionary.txt mypasswd
```

```
yassie@yassie-VirtualBox:~$ sudo john --wordlist=diccionario.txt mypaswd
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/64])
No password hashes left to crack (see FAQ)
yassie@yassie-VirtualBox:~$ sudo john --show mypaswd
yassie:1234:1000:1000:yassie:/home/yassie:/bin/bash
emma:1234:1001:1001:,,,:/home/emma:/bin/bash
pio:1234:1002:1002:pio,,,:/home/pio:/bin/bash

3 password hashes cracked, 0 left
yassie@yassie-VirtualBox:~$
```

Activitat 4

1. Crear usuaris:

```
yassie@yassie-VirtualBox:~$ sudo john --wordlist=diccionario.txt mypaswd
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/64])
No password hashes left to crack (see FAQ)
yassie@yassie-VirtualBox:~$ sudo john --show mypaswd
yassie:1234:1000:1000:yassie:/home/yassie:/bin/bash
emma:1234:1001:1001:,,,:/home/emma:/bin/bash
pio:1234:1002:1002:pio,,,:/home/pio:/bin/bash

3 password hashes cracked, 0 left
yassie@yassie-VirtualBox:~$
```

2. Assignar les contrasenyes simples:

```
yassie@yassie-VirtualBox:~$ sudo echo user1:12345 | sudo chpasswd
CONTRASEÑA INCORRECTA: La contraseña tiene menos de 8 caracteres
yassie@yassie-VirtualBox:~$ sudo echo user1:1Ab | sudo chpasswd
CONTRASEÑA INCORRECTA: La contraseña tiene menos de 8 caracteres
yassie@yassie-VirtualBox:~$ sudo echo user1:12345 | sudo chpasswd
CONTRASEÑA INCORRECTA: La contraseña tiene menos de 8 caracteres
yassie@yassie-VirtualBox:~$ sudo echo user2:1Ab | sudo chpasswd
CONTRASEÑA INCORRECTA: La contraseña tiene menos de 8 caracteres
yassie@yassie-VirtualBox:~$ sudo echo user3:patata | sudo chpasswd
CONTRASEÑA INCORRECTA: La contraseña tiene menos de 8 caracteres
```

3. Configurar la política de contrasenyes:

Edita el fitxer /etc/security/pwquality.conf per afegir la política de llargada de contrasenyes:

```
yassie@yassie-VirtualBox:~$ sudo nano /etc/security/pwquality.conf
yassie@yassie-VirtualBox:~$
```

```
GNU nano 7.2          /etc/security/pwquality.conf *
# Configuration for systemwide password quality limits
# Defaults:
#
# Number of characters in the new password that must not be present in the
# old password.
# difok = 1
#
# 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 = 9
#
# The maximum credit for having digits in the new password. If less than 0
```

4. Complexitat de la contrasenya: Lletres majúscules, minúscules i números

En el mateix fitxer (/etc/security/pwquality.conf)

```
# 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 = -1
#
# 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 lowercase characters in the new password.
# If less than 0 it is the minimum number of lowercase characters in the new
# password.
# lcredit = -1
```

5. Caducitat de la contrasenya: cada mes

Configura la caducitat de la contrasenya per a tots els usuaris editant /etc/login.defs:

```
yassie@yassie-VirtualBox:~$ sudo nano /etc/login.defs
```

```
GNU nano 7.2          /etc/login.defs *
SHELLCHAR      025
UMASK         022

# HOME_MODE is used by useradd(8) and newusers(8) to set the mode for new
# home directories.
# If HOME_MODE is not set, the value of UMASK is used to create the mode.
HOME_MODE      0750

#
# 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  7
```

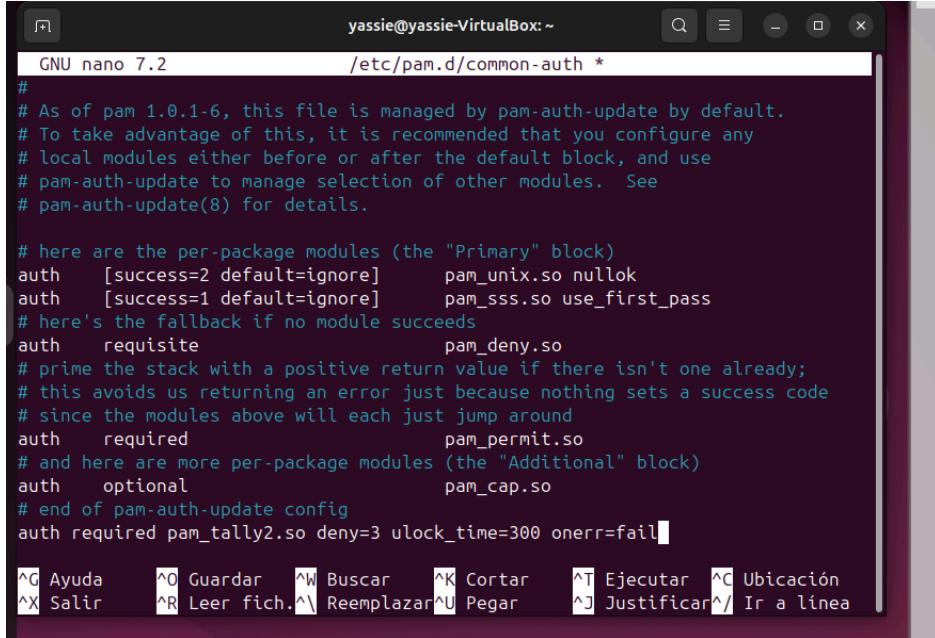
6. Bloqueig del compte: 3 fallades

Configura el bloqueig d'un compte després de 3 intents fallits editant el fitxer /etc/pam.d/common-auth:

```
yassie@yassie-VirtualBox:~$ sudo nano /etc/pam.d/common-auth
yassie@yassie-VirtualBox:~$
```

7. Afegeix la següent línia al final del fitxer:

auth required pam_tally2.so deny=3 unlock_time=300 onerr=fail



The screenshot shows a terminal window titled "yassie@yassie-VirtualBox: ~". The window contains the contents of the file "/etc/pam.d/common-auth". The file is a configuration script for the Pluggable Authentication Modules (PAM) system. It defines several authentication modules and their behavior. The terminal window has a dark background with light-colored text. At the bottom, there is a menu bar with various keyboard shortcuts in Spanish.

```
GNU nano 7.2          /etc/pam.d/common-auth *

#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
auth    [success=2 default=ignore]      pam_unix.so nullok
auth    [success=1 default=ignore]      pam_sss.so use_first_pass
# here's the fallback if no module succeeds
auth    requisite                  pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth    required                  pam_permit.so
# and here are more per-package modules (the "Additional" block)
auth    optional                  pam_cap.so
# end of pam-auth-update config
auth required pam_tally2.so deny=3 ulock_time=300 onerr=fail

^G Ayuda      ^O Guardar   ^W Buscar   ^K Cortar   ^T Ejecutar   ^C Ubicación
^X Salir      ^R Leer fich. ^A Reemplazar ^U Pegar    ^J Justificar ^I Ir a linea
```