Politica Contraseñas

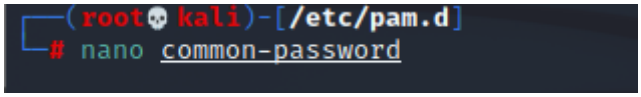
10/10/2023

Guillermo Bellettini
Seguridad
Creado por: Nicolas Pavel Ballesteros Barrado

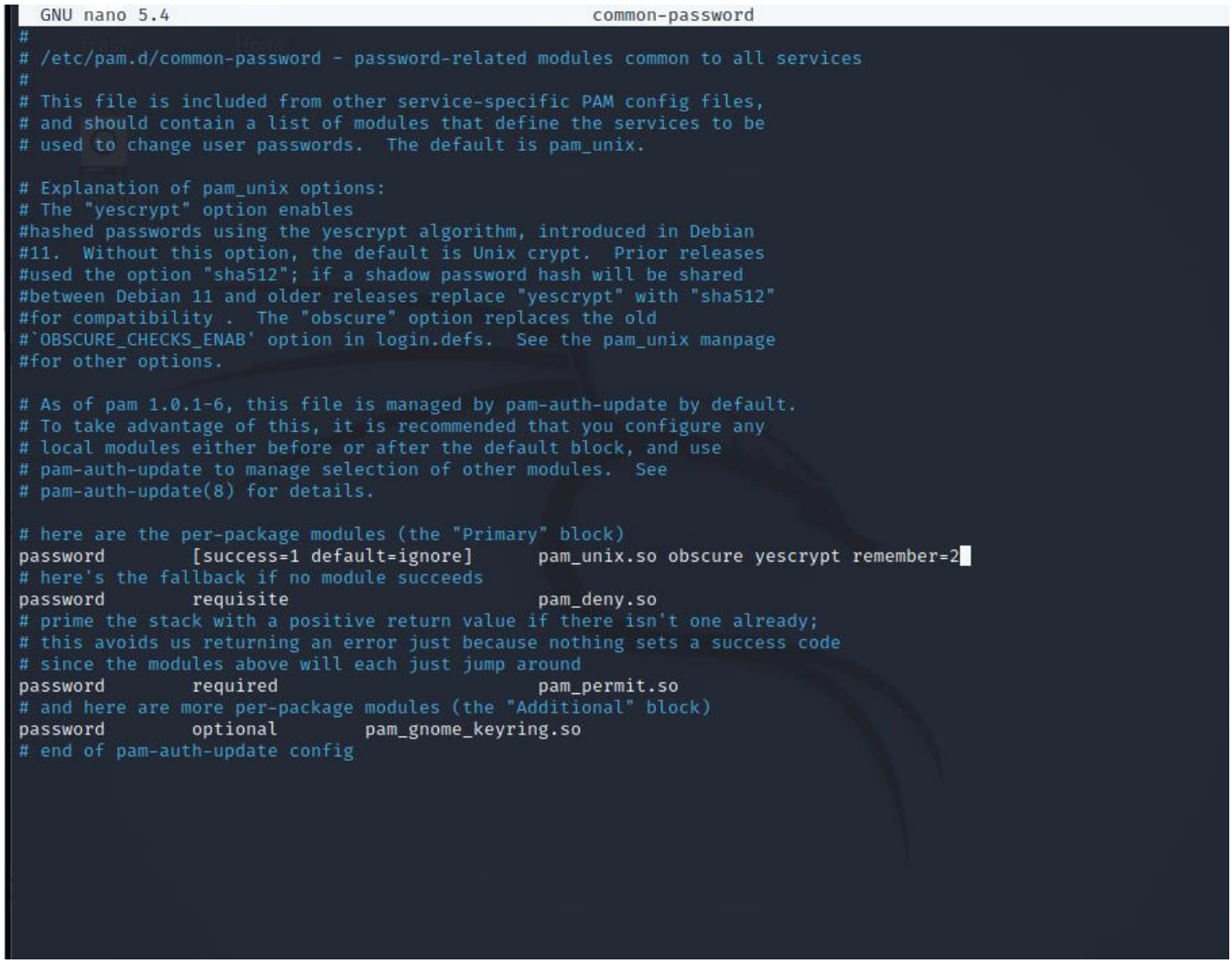
Contenido

Nos metemos en la ruta /etc/pam.d

Nos metemos en common-password

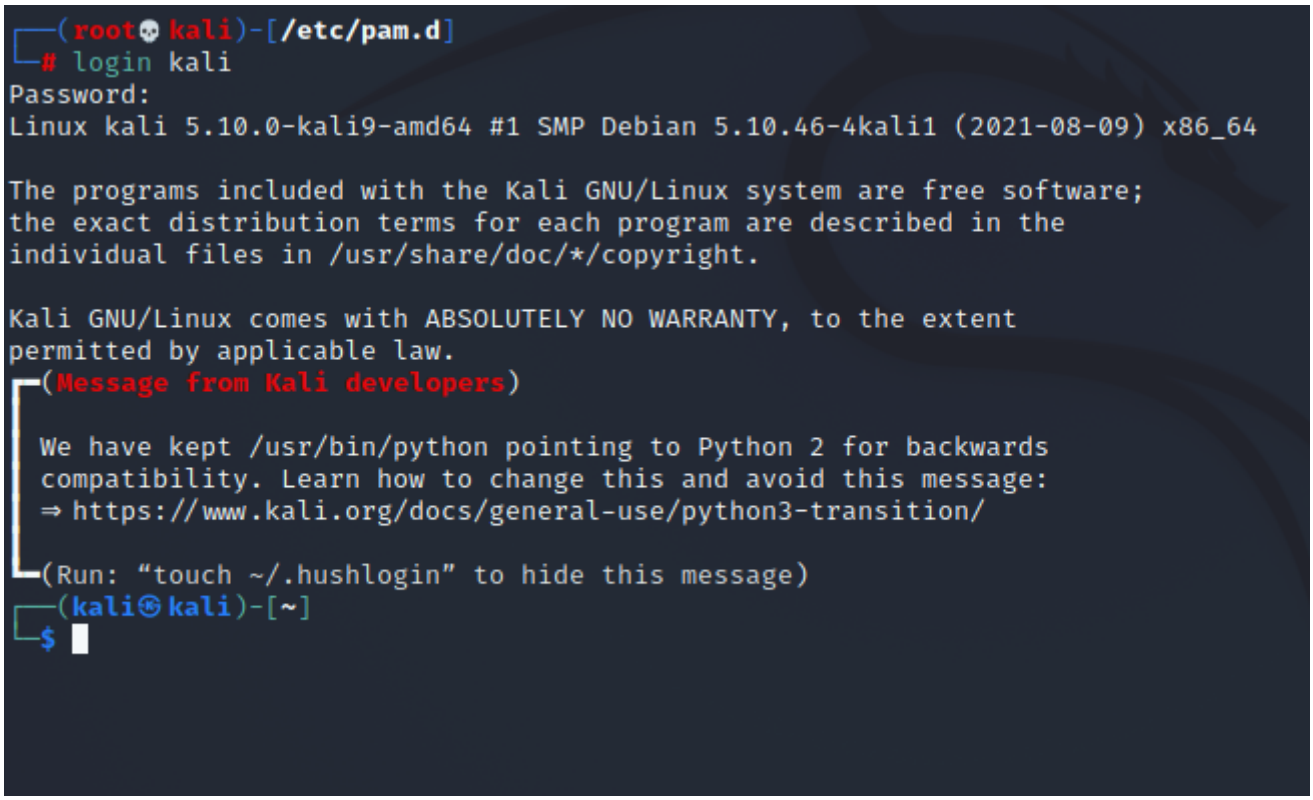


Ahora editamos el fichero

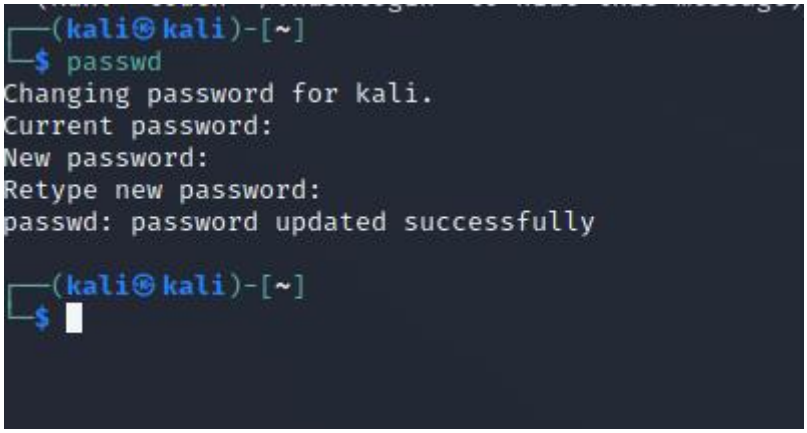


Ponemos el parámetro remember=2

Entramos con otro usuario que no es root



Cambiamos la contraseña



Nos dice que ya se ha actualizado la contraseña

Volvemos a logear con Kali

```
┌──(root💀kali)-[/etc/pam.d]
└─# login kali
Password:
Linux kali 5.10.0-kali9-amd64 #1 SMP Debian 5.10.46-4kali1 (2021-08-09) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Oct 10 12:06:33 EDT 2023 on pts/0
┌──(Message from Kali developers)
│
│ We have kept /usr/bin/python pointing to Python 2 for backwards
│ compatibility. Learn how to change this and avoid this message:
│ ⇒ https://www.kali.org/docs/general-use/python3-transition/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
┌──(kali㉿kali)-[~]
└─$
```

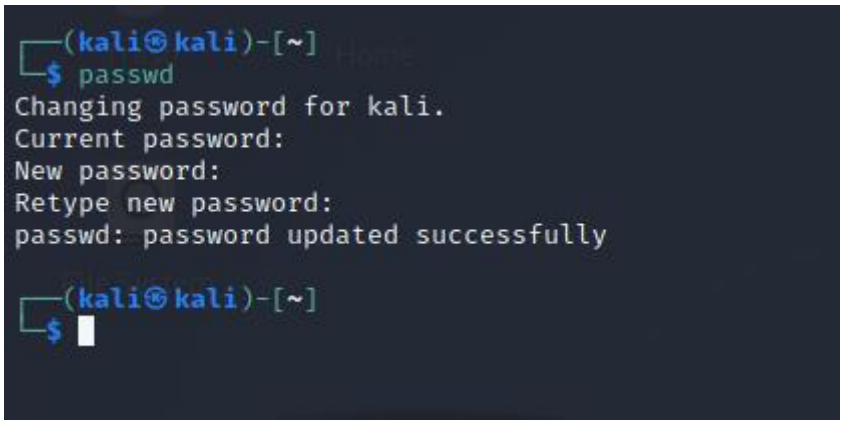
Vemos el almacenaje de las contraseñas

```
┌──(kali㉿kali)-[~]
└─$ more /etc/security/opasswd
more: cannot open /etc/security/opasswd: Permission denied

┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
┌──(root💀kali)-[/home/kali]
└─# more /etc/security/opasswd
kali:1000:1:$1$ASK49KqS$8xF2sF.CQbEQjE81h5myQ0

┌──(root💀kali)-[/home/kali]
└─#
```

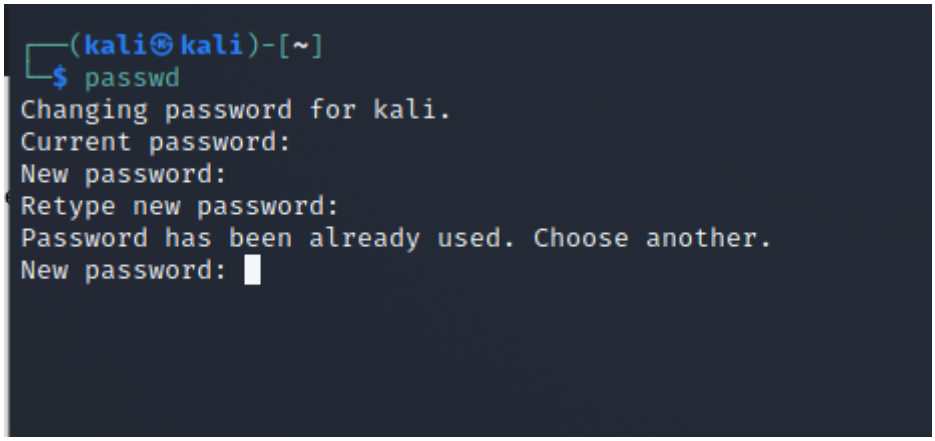
Cambiamos otra vez la contraseña



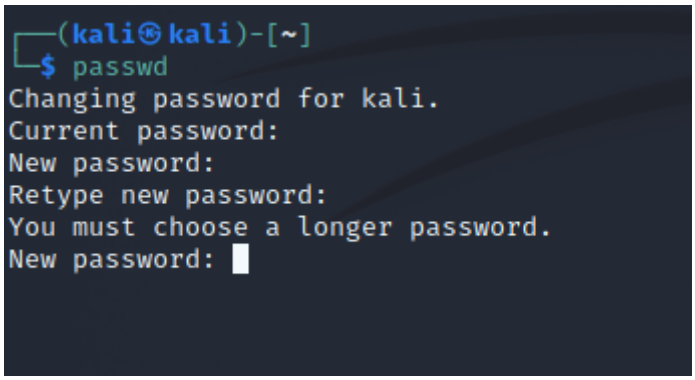
Vemos ahora las claves almacenadas

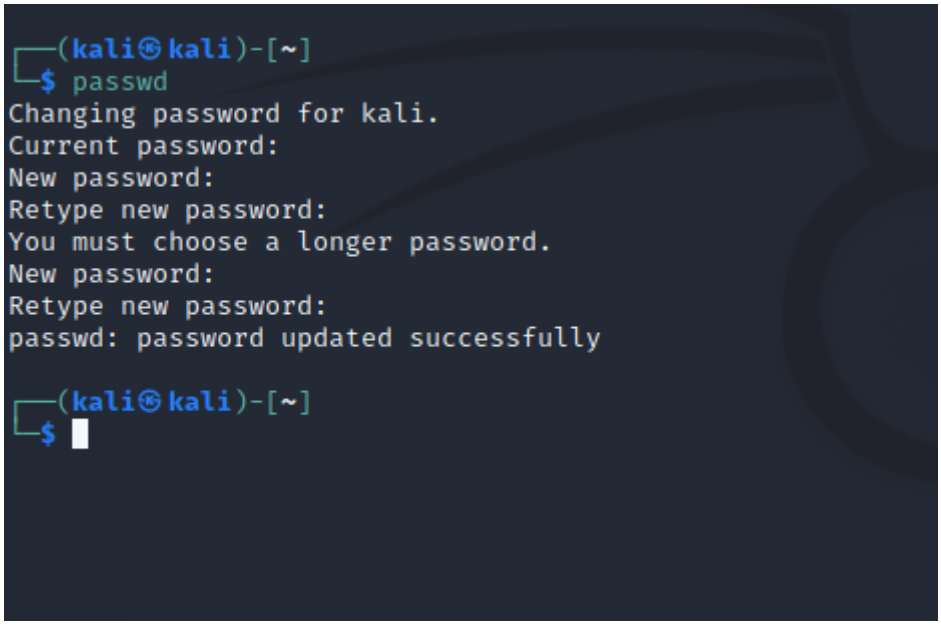
Ahora tenemos dos almacenadas

Volvemos a poner una contraseña de antes y nos dice que utilicemos otra



Ponemos la contraseña Kali y nos dice que tiene que ser mas larga





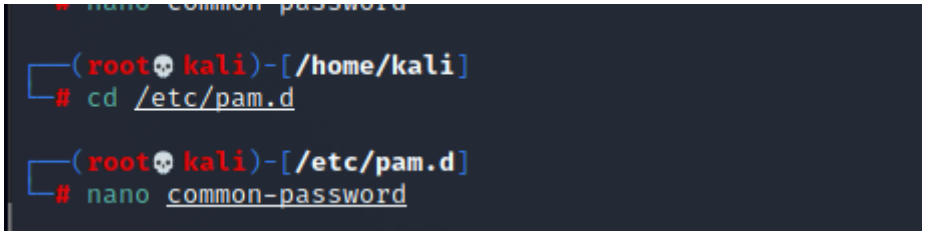
Ponemos kali1234 y nos acepta la contraseña

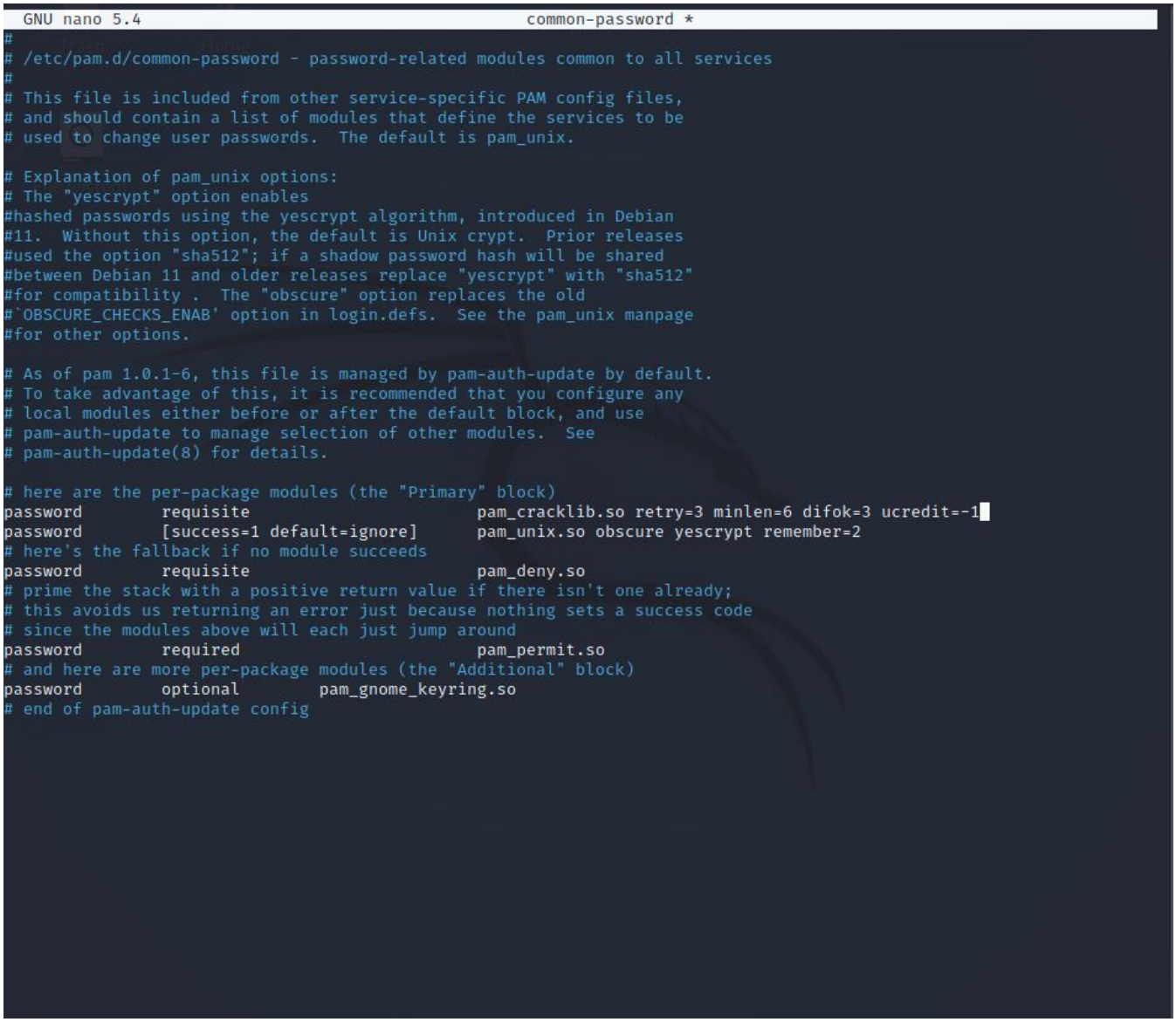
Ponemos otra vez el comando more /etc/security/opasswd

El sistema nos recuerda las dos ultimas contraseñas que hemos puesto

Actualizamos la contraseña a Admin1234

Editamos otra vez el fichero /etc/common-password

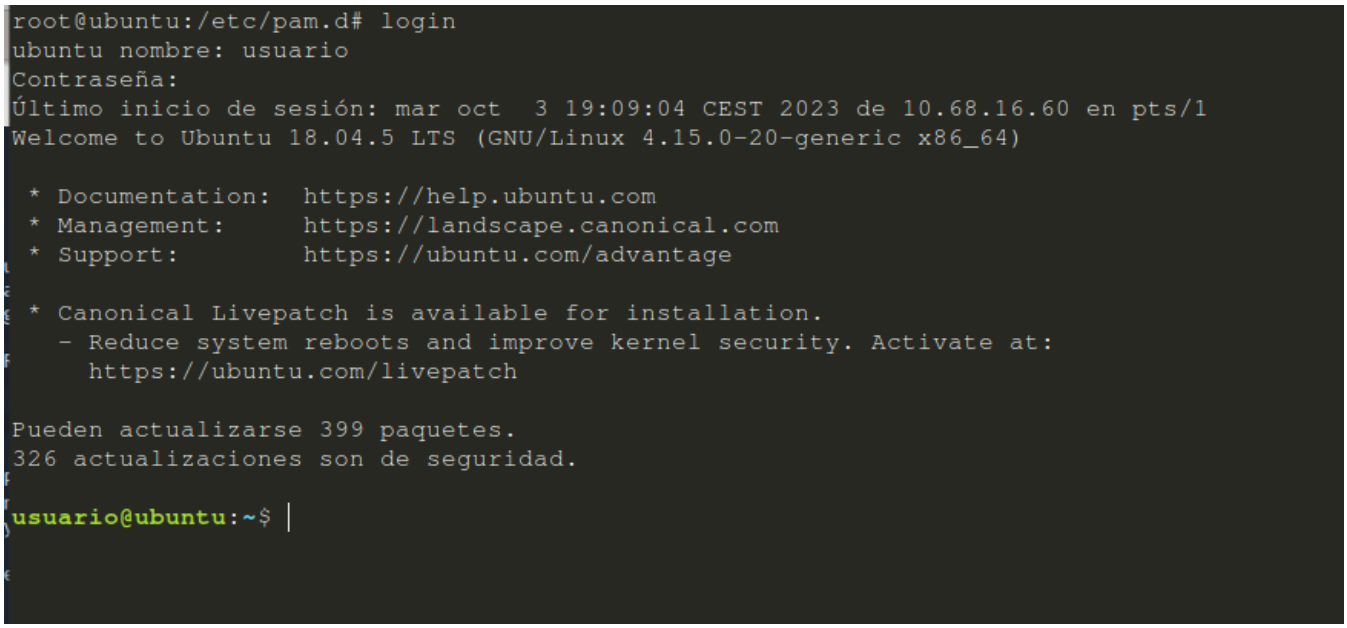




Ponemos que al menos haya un carácter en mayuscula

Nos metemos en kali

Entramos en usuario



Si ponemos la contraseña todo en minúsculas nos pone esto

```
usuario@ubuntu:~$ passwd
Cambiando la contraseña de usuario.
(actual) contraseña de UNIX:
Nueva contraseña:
CONTRASEÑA INCORRECTA: Es demasiado corta.
Nueva contraseña:
CONTRASEÑA INCORRECTA: es demasiado sencilla
Nueva contraseña:
```

Ahora la ponemos con mayuscula

```
usuario@ubuntu:~$ passwd
Cambiando la contraseña de usuario.
(actual) contraseña de UNIX:
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
usuario@ubuntu:~$
```

Y ahora nos la acepta la contraseña

Hacemos comando more /etc/login.dfs

```
1: root@ubuntu: /etc/pam.d
#
# /etc/login.defs - Configuration control definitions for the login package.
#
# Three items must be defined:  MAIL_DIR, ENV_SUPATH, and ENV_PATH.
# If unspecified, some arbitrary (and possibly incorrect) value will
# be assumed.  All other items are optional - if not specified then
# the described action or option will be inhibited.
#
# Comment lines (lines beginning with "#") and blank lines are ignored.
#
# Modified for Linux.  --marekm

# REQUIRED for useradd/userdel/usermod
#   Directory where mailboxes reside, _or_ name of file, relative to the
#   home directory.  If you _do_ define MAIL_DIR and MAIL_FILE,
#   MAIL_DIR takes precedence.
#
#   Essentially:
#      - MAIL_DIR defines the location of users mail spool files
#        (for mbox use) by appending the username to MAIL_DIR as defined
#        below.
#      - MAIL_FILE defines the location of the users mail spool files as the
#        fully-qualified filename obtained by prepending the user home
#        directory before $MAIL_FILE
#
# NOTE: This is no more used for setting up users MAIL environment variable
#       which is, starting from shadow 4.0.12-1 in Debian, entirely the
#       job of the pam_mail PAM modules
#       See default PAM configuration files provided for
#       login, su, etc.
#
# This is a temporary situation: setting these variables will soon
# move to /etc/default/useradd and the variables will then be
# no more supported
MAIL_DIR        /var/mail
#MAIL_FILE      .mail

#
# Enable logging and display of /var/log/faillog login failure info.
# This option conflicts with the pam_tally PAM module.
#
FAILLOG_ENAB            yes

#
```

Miramos los parámetros

```
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7

#
# Min/max values for automatic uid select
#
```

El pass_max_days 9999 dice que nunca expira, si le ponemos 30, cada 30 dias tendrían que cambiar su contraseña

El pass_warn_age te avisa 7 dias antes de que expire tu contraseña