

Politica Contraseñas

10/10/2023

Guillermo Bellettini

Seguridad

Creado por: Nicolas Pavel Ballesteros Barrado



Contenido

Politica Contraseñas	1
Nos metemos en la ruta /etc/pam.d	3
Nos metemos en common-password	3
Ahora editamos el fichero	4
Entramos con otro usuario que no es root	5
Cambiamos la contraseña	5
Volvemos a logear con Kali	6
Vemos el almacenaje de las contraseñas	6
Cambiamos otra vez la contraseña	7
Vemos ahora las claves almacenadas	7
Volvemos a poner una contraseña de antes y nos dice que utilicemos otra	7
Ponemos la contraseña Kali y nos dice que tiene que ser mas larga	8
Ponemos otra vez el comando more /etc/security/opasswd	8
Actualizamos la contraseña a Admin1234	9
Editamos otra vez el fichero /etc/common-password	9
Nos metemos en kali	11
Entramos en usuario	11
Hacemos comando more /etc/login.dfs	13

Nos metemos en la ruta /etc/pam.d

```
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root skull kali)-[/home/kali]
# cd /etc/pam.d

(root skull kali)-[/etc/pam.d]
#
```

Nos metemos en common-password

```
(root skull kali)-[/etc/pam.d]
# nano common-password
```

Ahora editamos el fichero

```
GNU nano 5.4                                common-password
#
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords. The default is pam_unix.

# Explanation of pam_unix options:
# The "yescrypt" option enables
# hashed passwords using the yescrypt algorithm, introduced in Debian
# 11. Without this option, the default is Unix crypt. Prior releases
# used the option "sha512"; if a shadow password hash will be shared
# between Debian 11 and older releases replace "yescrypt" with "sha512"
# for compatibility. The "obscure" option replaces the old
# 'OBSCURE_CHECKS_ENAB' option in login.defs. See the pam_unix manpage
# for other options.

# 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)
password      [success=1 default=ignore]      pam_unix.so obscure yescrypt remember=2
# here's the fallback if no module succeeds
password      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
password      required                       pam_permit.so
# and here are more per-package modules (the "Additional" block)
password      optional                       pam_gnome_keyring.so
# end of pam-auth-update config
```

Ponemos el parámetro remember=2

Entramos con otro usuario que no es root

```
(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.
(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)-[~]
$
```

Cambiamos la contraseña

```
(kali@kali)-[~]
$ passwd
Changing password for kali.
Current password:
New password:
Retype new password:
passwd: password updated successfully

(kali@kali)-[~]
$
```

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

```
(kali㉿kali)-[~]
$ passwd
Changing password for kali.
Current password:
New password:
Retype new password:
passwd: password updated successfully

(kali㉿kali)-[~]
$
```

Vemos ahora las claves almacenadas

```
(kali㉿kali)-[~]
$ sudo su
(root㉿kali)-[/home/kali]
# more /etc/security/opasswd
kali:1000:2:$1$ASK49KqS$8xF2sF.CQbEQjE81h5myQ0,$1$3lgAT1cL$mR9KrjZ8cLtztz1F1zKJ2/

(root㉿kali)-[/home/kali]
#
```

Ahora tenemos dos almacenadas

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

```
(kali㉿kali)-[~]
$ passwd
Changing password for kali.
Current password:
New password:
Retype new password:
Password has been already used. Choose another.
New password:
```

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

```
(kali@kali)-[~]
$ passwd
Changing password for kali.
Current password:
New password:
Retype new password:
You must choose a longer password.
New password: 
```

```
(kali@kali)-[~]
$ passwd
Changing password for kali.
Current password:
New password:
Retype new password:
You must choose a longer password.
New password:
Retype new password:
passwd: password updated successfully

(kali@kali)-[~]
$ 
```

Ponemos kali1234 y nos acepta la contraseña

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

```
[sudo] password for kali:
(root@kali)-[/home/kali]
# more /etc/security/opasswd
kali:1000:2:$1$QjcrPw7z$TKbMe.2TZuUJlFv30xUcs0,$1$X0M5Q9dA$fJxBeY4.l7J92VQriAA0h0

(root@kali)-[/home/kali]
# 
```

El sistema nos recuerda las dos ultimas contraseñas que hemos puesto

Actualizamos la contraseña a Admin1234

```
(kali㉿kali)-[~]  
$ sudo su  
(root㉿kali)-[/home/kali]  
# passwd kali  
New password:  
Retype new password:  
passwd: password updated successfully  
  
(root㉿kali)-[/home/kali]  
#
```

Editamos otra vez el fichero /etc/common-password

```
# nano common-password  
  
(root㉿kali)-[/home/kali]  
# cd /etc/pam.d  
  
(root㉿kali)-[/etc/pam.d]  
# nano common-password
```

```

GNU nano 5.4                                common-password *
#
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords. The default is pam_unix.

# Explanation of pam_unix options:
# The "yescrypt" option enables
# hashed passwords using the yescrypt algorithm, introduced in Debian
# 11. Without this option, the default is Unix crypt. Prior releases
# used the option "sha512"; if a shadow password hash will be shared
# between Debian 11 and older releases replace "yescrypt" with "sha512"
# for compatibility. The "obscure" option replaces the old
# 'OBSCURE_CHECKS_ENAB' option in login.defs. See the pam_unix manpage
# for other options.

# 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)
password      requisite          pam_cracklib.so retry=3 minlen=6 difok=3 ucredit=-1
password      [success=1 default=ignore] pam_unix.so obscure yescrypt remember=2
# here's the fallback if no module succeeds
password      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
password      required           pam_permit.so
# and here are more per-package modules (the "Additional" block)
password      optional           pam_gnome_keyring.so
# end of pam-auth-update config

```

Ponemos que al menos haya un carácter en mayúscula

Nos metemos en 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 12:17:35 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)-[~]
$
```

Entramos en usuario

```
root@ubuntu:/etc/pam.d# login
ubuntu nombre: usuario
Contraseña:
Último inicio de sesión: mar oct  3 19:09:04 CEST 2023 de 10.68.16.60 en pts/1
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-20-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

Pueden actualizarse 399 paquetes.
326 actualizaciones son de seguridad.
usuario@ubuntu:~$
```

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.defs

```
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 días tendrían que cambiar su contraseña

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