

# Prácticas de contraseña segura (creación y gestión)

## Configuración de Políticas de Contraseñas Seguras

1. Verificar la política de contraseñas actual en Linux se realiza revisando el archivo de configuración pam.d y el archivo /etc/login.defs:

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ sudo cat /etc/login.defs  
[sudo] password for kali:  
#  
# /etc/login.defs - Configuration control definitions for the shadow package.  
#  
# 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  
#  
#  
File Actions Edit View Help  
# Min/max values for automatic uid selection in useradd(8)  
#  
UID_MIN      1000  
UID_MAX      60000  
# System accounts  
#SYS_UID_MIN  101  
#SYS_UID_MAX  999  
# Extra per user uids  
SUB_UID_MIN  100000  
SUB_UID_MAX  600100000  
SUB_UID_COUNT 65536  
#  
# Min/max values for automatic gid selection in groupadd(8)  
#  
GID_MIN      1000  
GID_MAX      60000  
# System accounts  
#SYS_GID_MIN  101  
#SYS_GID_MAX  999  
# Extra per user group ids  
SUB_GID_MIN  100000  
SUB_GID_MAX  600100000  
SUB_GID_COUNT 65536  
#  
# Max number of login(1) retries if password is bad  
# This will most likely be overridden by PAM, since the default pam_unix module  
# has it's own built in of 3 retries. However, this is a safe fallback in case  
# you are using an authentication module that does not enforce PAM_MAXTRIES.  
#  
LOGIN_RETRIES 5  
#
```

```
File Actions Edit View Help
#
ENCRYPT_METHOD YESCRYPT
#
# Should login be allowed if we can't cd to the home directory?
# Default is no.
#
DEFAULT_HOME    yes
#
# The pwck(8) utility emits a warning for any system account with a home
# directory that does not exist. Some system accounts intentionally do
# not have a home directory. Such accounts may have this string as
# their home directory in /etc/passwd to avoid a spurious warning.
#
NONEXISTENT     /nonexistent
#
# If defined, this command is run when removing a user.
# It should remove any at/cron/print jobs etc. owned by
# the user to be removed (passed as the first argument).
#
USERDEL_CMD     /usr/sbin/userdel_local
#
# If set to yes, userdel(8) will remove the user's group if it contains no more
# members, and useradd(8) will create by default a group with the name of the
# user.
#
# Other former uses of this variable are not used in PAM environments, such as
# Debian.
#
USERGROUPS_ENAB yes
```

Se revisó la configuración de pam.d:

```
(kali@kali)~$
$ sudo cat /etc/pam.d/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 "vescrypt" 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 "vescrypt" with "sha512"
# for compatibility. The "obscure" option replaces the old
# "OBSOLETE_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=2 default=ignore] pam_unix.so obscure yescrypt
password    [success=1 default=ignore] pam_winbind.so try_authtok try_first_pass
# 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
```

Verificación con pwquality.conf:

```
(kali@kali)~$
$ sudo cat /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 = 8
#
# 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 = 0
#
# 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 = 0
#
# 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 = 0
#
# The maximum credit for having other characters in the new password.
# If less than 0 it is the minimum number of other characters in the new
# password.
# ocredit = 0
#
```

## 2. Configuración de la Longitud Mínima y Complejidad

### Instalación del módulo libpam

```

└─$ sudo apt install libpam-pwquality -y

The following packages were automatically installed and are no longer required:
  icu-devtools  libfuse3-3  libglapi-mesa  libibverbs0  libpython3.12-minimal  libpython3.12t64  python3.12-tk  strongswan
  libflac12t64  libgeos3.13.0  libcicu-dev  libpoppler145  libpython3.12-stdlib  python3-setproctitle  ruby-zeitwerk
Use 'sudo apt autoremove' to remove them.

Installing:
  libpam-pwquality

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 7
  Download size: 13.1 kB
  Space needed: 41.0 kB / 61.8 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 libpam-pwquality amd64 1.4.5-5 [13.1 kB]
Fetched 13.1 kB in 1s (12.8 kB/s)
Selecting previously unselected package libpam-pwquality:amd64.
(Reading database ... 417590 files and directories currently installed.)
Preparing to unpack .../libpam-pwquality_1.4.5-5_amd64.deb ...
Unpacking libpam-pwquality:amd64 (1.4.5-5) ...
Setting up libpam-pwquality:amd64 (1.4.5-5) ...
Processing triggers for man-db (2.13.0-1) ...

└─(kali㉿kali)-[~]
└─$

```

## Edición del archivo

```

└─$ nano /etc/security/pwquality.conf
GNU nano 8.4 /etc/security/pwquality.conf
# Length of substrings from the username to check for in the password
# The check is enabled if the value is greater than 0 and usercheck is enabled.
# usersubstr = 0
#
# Whether the check is enforced by the PAM module and possibly other
# applications.
# The new password is rejected if it fails the check and the value is not 0.
# enforcing = 1
#
# Path to the cracklib dictionaries. Default is to use the cracklib default.
# dictpath =
#
# Prompt user at most N times before returning with error. The default is 1.
# retry = 3
#
# Enforces pwquality checks on the root user password.
# Enabled if the option is present.
# enforce_for_root
#
# Skip testing the password quality for users that are not present in the
# /etc/passwd file.
# Enabled if the option is present.
# local_users_only

minlen = 12
dcredit = -1
ucredit = -1
lcredit = -1
ocredit = -1

└─$

```

## Aplicar las políticas modificando el archivo /etc/pam.d/common-password para que use el módulo pam\_pwquality.so

```

└─$ nano /etc/pam.d/common-password
# The "vescrypt" 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 "vescrypt" with "sha512"
# for compatibility. The "obscure" option replaces the old
# "OBSOLETE_CHECKS_ENABLED" 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_pwquality.so retry=3
password      [success=2 default=ignore] pam_unix.so obscure use_authtok try_first_pass yescrypt
password      [success=1 default=ignore] pam_winbind.so try_authtok try_first_pass
# 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

└─$

```

## Configuración de Bloqueo de Cuenta tras Intentos Fallidos

### Configuración con pam\_faillock:



```
# here are the per-package modules (the "Primary" block)
auth [success=2 default=ignore]      pam_unix.so nullok
auth [success=1 default=ignore]      pam_winbind.so krb5_auth krb5_ccache_type=FILE cached_login try_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)
# end of pam-auth-update config
auth required pam_faillock.so preauth silent deny=5 unlock_time=900
auth [default=die] pam_faillock.so authfail deny=5 unlock_time=900
```

Read 28 lines

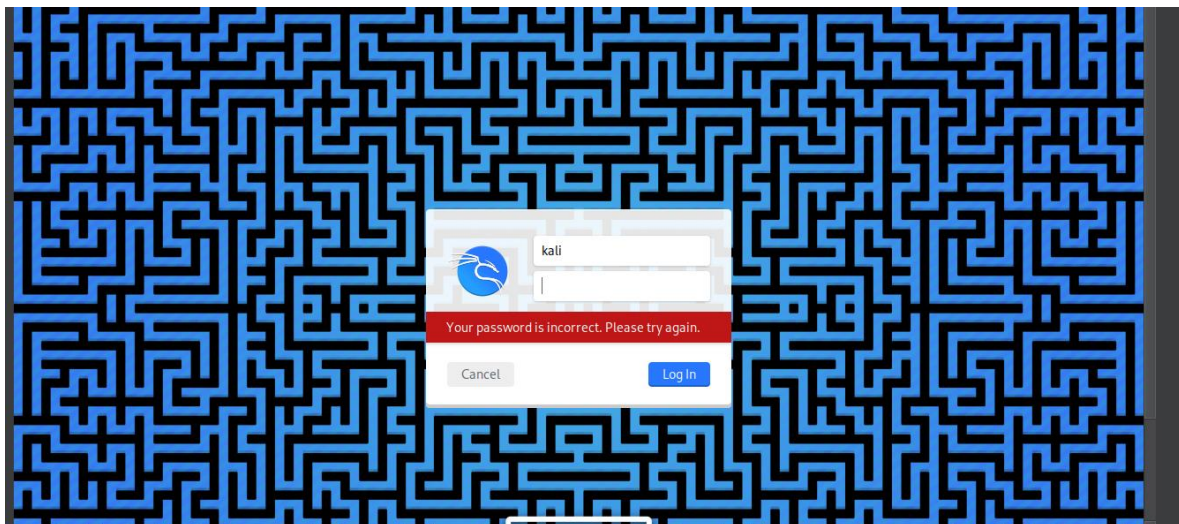
Help Exit Write Out Read File Where Is Replace Cut Paste Execute Justify Location Go To Line Undo Redo Set Mark Copy To Bracket Where Was Previous Next

## Verificación y Documentación de la Configuración

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

Changing password for kali.
Current password:
New password:
BAD PASSWORD: No password supplied
New password:
BAD PASSWORD: The password contains less than 1 uppercase letters
New password:
BAD PASSWORD: The password contains less than 1 uppercase letters
passwd: Have exhausted maximum number of retries for service
passwd: password unchanged
```

Luego de ingresar la contraseña incorrecta 5 veces, aunque se escriba la contraseña correcta esta no funciona



La práctica permitió reforzar conocimientos sobre políticas de contraseñas y mecanismos de protección frente a ataques de fuerza bruta. El sistema reaccionó adecuadamente en todos los casos.