

BOOTCAMP ESPECIALIDAD GNU/LINUX (2023)

Lab 03 - Usuarios grupos y permisos

Pedro Antonio Mayorgas Parejo

7 de agosto de 2023

Índice

1	Creación de los Grupos	3
2	Creación de la política de seguridad de contraseñas	3
3	Creación de los usuarios.	6
4	Creación de los permisos sobre las carpetas	8

1. Creación de los Grupos

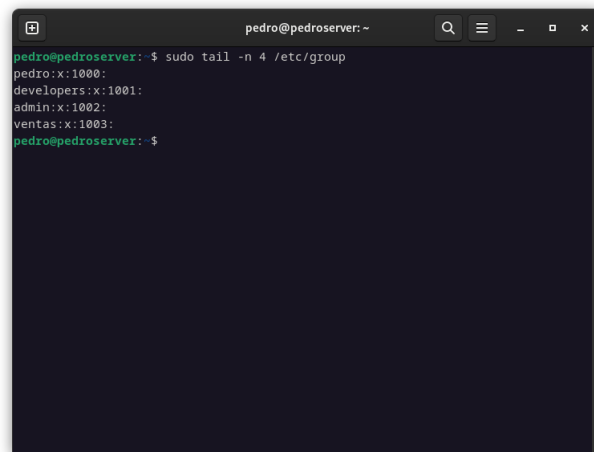
Creación de los grupos:

- Developers
- Admins
- Ventas

Comandos utilizados.

- 1 `sudo addgroup developers`
- 2 `sudo addgroup admin`
- 3 `sudo addgroup ventas`

Una vez creados podemos comprobar los grupos con un simple tail, en el directorio `/etc/group`.



```
pedro@pedroserver: ~  
pedro@pedroserver:~$ sudo tail -n 4 /etc/group  
pedro:x:1000:  
developers:x:1001:  
admin:x:1002:  
ventas:x:1003:  
pedro@pedroserver:~$
```

Figura 1: Demostración de que los grupos han sido creados

2. Creación de la política de seguridad de contraseñas

Para la creación de la política de seguridad, necesitamos un módulo adicional de PAM, dicho módulo nos permite que cuando un usuario cambie de contraseña, esta sea comprobada por este módulo se asegura que bajo los parámetros que hemos introducido en un fichero localizado en `/etc/pam.d/common-password`, se asegure de la longitud y la diferencia de caracteres. Fuente Debian ¹. Package ²

Lo que necesitamos es la siguiente línea, que nos permite cumplir con los siguientes requisitos:

¹<https://www.debian.org/doc/manuals/securing-debian-manual/ch04s11.en.html>

²<https://packages.debian.org/buster/libpam-cracklib>

1. 8 caracteres mínimo.
2. 3 tipos de caracteres diferentes.

```

1 sudo apt install libpam-cracklib
2 sudo nano /etc/pam.d/common-password
3
4 # Dentro del fichero introducimos lo siguiente.
5 password required pam_cracklib.so retry=3 minlen=8 difok=3

```

Enumeración de los parámetros de la línea de parámetros del módulo libpam-cracklib.

1. retry=3 - Se refiere a los intentos que tiene el usuario de introducir una contraseña buena en passwd.
2. minlen=8 - Se refiere a la cantidad mínima de caracteres que necesita la contraseña.
3. difok=3 - Se especifica el nº mínimo de caracteres que tiene que tener de diferencia con respecto a la contraseña antigua. Por ejemplo: Password -> Password123. Está permitido, pero es una contraseña débil, pero para ello se pueden poner parámetros especiales que incrementen la seguridad como lcredit, ucredit, dcredit, ocredit. Que implican obligar a los usuarios que tengan un crédito negativo, que utilicen una cierta cantidad de caracteres en mayúsculas, números, o caracteres especiales.

Manual de consulta de la información de libpam-cracklib ³

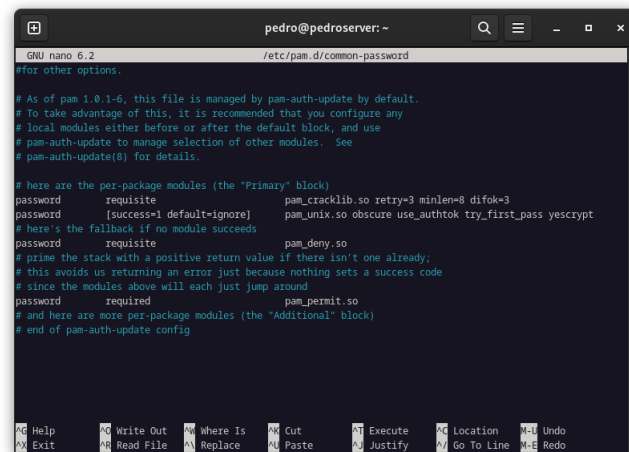
```

pedro@pedroserver: ~
pedro@pedroserver:~$ sudo apt install libpam-cracklib
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  cracklib-runtime libcrack2 wamerican
The following NEW packages will be installed:
  cracklib-runtime libcrack2 libpam-cracklib wamerican
0 upgraded, 4 newly installed, 0 to remove and 2 not upgraded.
Need to get 429 kB of archives.
After this operation, 1,897 kB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://es.archive.ubuntu.com/ubuntu jammy/main amd64 libcrack2 amd64 2.9.6-3.4build4 [29.6 kB]
Get:2 http://es.archive.ubuntu.com/ubuntu jammy/main amd64 cracklib-runtime amd64 2.9.6-3.4build4 [149 kB]
Get:3 http://es.archive.ubuntu.com/ubuntu jammy/main amd64 wamerican all 2020.12.07-2 [236 kB]
Get:4 http://es.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libpam-cracklib amd64 1.4.0-11ubuntu2.3 [13.5 kB]
Fetched 429 kB in 2s (226 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libcrack2:amd64.
(Reading database ... 74142 files and directories currently installed.)

```

Figura 2: Instalación de libpam-cracklib

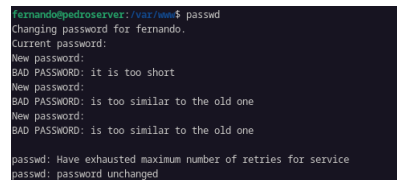
³https://deer-run.com/users/hal/sysadmin/pam_cracklib.html



```
pedro@pedroserver: ~  
GNU nano 6.2 /etc/pam.d/common-password  
#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=8 difok=3  
password      [success=1 default=ignore]   pam_unix.so obscure use_authtok try_first_pass yescrypt  
# 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)  
# end of pam-auth-update config  
  
⌘ Help      ⌘ Write Out  ⌘ Where Is   ⌘ Cut        ⌘ Execute    ⌘ Location   ⌘ Undo  
⌘ Exit      ⌘ Read File  ⌘ Replace    ⌘ Paste      ⌘ Justify    ⌘ Go To Line ⌘ Redo
```

Figura 3: Introducción de la línea de libpam-cracklib

Si creamos contraseñas muy similares, no nos permitirá hacer nada.



```
fernando@pedroserver: /opt/newt$ passwd  
Changing password for fernando.  
Current password:  
New password:  
BAD PASSWORD: it is too short  
New password:  
BAD PASSWORD: is too similar to the old one  
New password:  
BAD PASSWORD: is too similar to the old one  
  
passwd: Have exhausted maximum number of retries for service  
passwd: password unchanged
```

Figura 4: Provocando fallos y contraseñas muy similares

3. Creación de los usuarios.

- Fernando y Pedro2 perteneciente al grupo ->Developers
- Ivan y Leticia perteneciente al grupo ->Admins
- Manu y Javi perteneciente al grupo ->Ventas

Comandos utilizados:

```
1 sudo useradd -g developers -e 'date -d "1 days" +%Y-%m-%d' -s /bin/bash -m -k /etc/skel --password 'openssl passwd -1 -salt xyz password' fernando ;
2
3 sudo useradd -g developers -e 'date -d "1 days" +%Y-%m-%d' -s /bin/bash -m -k /etc/skel --password 'openssl passwd -1 -salt xyz password' pedro2 ;
4
5 sudo useradd -g admin -e 'date -d "1 days" +%Y-%m-%d' -s /bin/bash -m -k /etc/skel --password 'openssl passwd -1 -salt xyz password' ivan ;
6
7 sudo useradd -g admin -e 'date -d "1 days" +%Y-%m-%d' -s /bin/bash -m -k /etc/skel --password 'openssl passwd -1 -salt xyz password' leticia ;
8
9 sudo useradd -g ventas -e 'date -d "1 days" +%Y-%m-%d' -s /bin/bash -m -k /etc/skel --password 'openssl passwd -1 -salt xyz password' javi ;
10
11 sudo useradd -g ventas -e 'date -d "1 days" +%Y-%m-%d' -s /bin/bash -m -k /etc/skel --password 'openssl passwd -1 -salt xyz password' manu ;
```

El comando utilizado, implica que se cree una caducidad de las cuentas de usuario de un día a partir de su creación. Luego se indica que se crea una contraseña por defecto y se añade a los grupos indicados.

```
pedro@pedroserver: ~  
pedro@pedroserver:~$ sudo useradd -g developers -e 'date -d "1 days" +%Y-%m-%d' -s /bin/bash -m -k /etc/skel --password 'openssl passwd -1 -salt xyz password' fernando ;  
pedro@pedroserver:~$ sudo useradd -g developers -e 'date -d "1 days" +%Y-%m-%d' -s /bin/bash -m -k /etc/skel --password 'openssl passwd -1 -salt xyz password' pedro2 ;  
pedro@pedroserver:~$ sudo useradd -g admin -e 'date -d "1 days" +%Y-%m-%d' -s /bin/bash -m -k /etc/skel --password 'openssl passwd -1 -salt xyz password' ivan ;  
pedro@pedroserver:~$ sudo useradd -g admin -e 'date -d "1 days" +%Y-%m-%d' -s /bin/bash -m -k /etc/skel --password 'openssl passwd -1 -salt xyz password' leticia ;  
pedro@pedroserver:~$ sudo useradd -g ventas -e 'date -d "1 days" +%Y-%m-%d' -s /bin/bash -m -k /etc/skel --password 'openssl passwd -1 -salt xyz password' javi ;  
pedro@pedroserver:~$ sudo useradd -g ventas -e 'date -d "1 days" +%Y-%m-%d' -s /bin/bash -m -k /etc/skel --password 'openssl passwd -1 -salt xyz password' manu ;  
pedro@pedroserver:~$ su fernando  
Password:  
fernando@pedroserver:/home/pedro$ cd  
fernando@pedroserver:/home/pedro$ pwd  
/home/fernando  
fernando@pedroserver:/home/pedro$ exit  
exit  
pedro@pedroserver:~$ su ivan  
Password:  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
ivan@pedroserver:/home/pedro$ id -g  
1002  
ivan@pedroserver:/home/pedro$ cat /etc/group | grep 'id -g'  
admin:x:1002:  
ivan@pedroserver:/home/pedro$ exit  
exit  
pedro@pedroserver:~$ su manu  
Password:  
manu@pedroserver:/home/pedro$ cat /etc/group | grep 'id -g'  
ventas:x:1003:  
manu@pedroserver:/home/pedro$ exit  
exit  
pedro@pedroserver:~$ su pedro2  
Password:  
pedro2@pedroserver:/home/pedro$ cat /etc/group | grep 'id -g'
```

Figura 5: Demostración de la creación de usuarios y pruebas de que han sido creados en su grupo

```
pedro@pedroserver: ~  
pedro@pedroserver:~$ sudo useradd -g admin -e 'date -d "1 days" +%Y-%m-%d' -s /bin/bash -m -k /etc/skel --password 'openssl passwd -1 -salt xyz password' ivan ;  
pedro@pedroserver:~$ sudo useradd -g admin -e 'date -d "1 days" +%Y-%m-%d' -s /bin/bash -m -k /etc/skel --password 'openssl passwd -1 -salt xyz password' leticia ;  
pedro@pedroserver:~$ sudo useradd -g ventas -e 'date -d "1 days" +%Y-%m-%d' -s /bin/bash -m -k /etc/skel --password 'openssl passwd -1 -salt xyz password' javi ;  
pedro@pedroserver:~$ sudo useradd -g ventas -e 'date -d "1 days" +%Y-%m-%d' -s /bin/bash -m -k /etc/skel --password 'openssl passwd -1 -salt xyz password' manu ;  
pedro@pedroserver:~$ su fernando  
Password:  
fernando@pedroserver:/home/pedro$ cd  
fernando@pedroserver:/home/pedro$ pwd  
/home/fernando  
fernando@pedroserver:/home/pedro$ exit  
exit  
pedro@pedroserver:~$ su ivan  
Password:  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
ivan@pedroserver:/home/pedro$ id -g  
1002  
ivan@pedroserver:/home/pedro$ cat /etc/group | grep 'id -g'  
admin:x:1002:  
ivan@pedroserver:/home/pedro$ exit  
exit  
pedro@pedroserver:~$ su manu  
Password:  
manu@pedroserver:/home/pedro$ cat /etc/group | grep 'id -g'  
ventas:x:1003:  
manu@pedroserver:/home/pedro$ exit  
exit  
pedro@pedroserver:~$ su pedro2  
Password:  
pedro2@pedroserver:/home/pedro$ cat /etc/group | grep 'id -g'  
developers:x:1001:  
pedro2@pedroserver:/home/pedro$ exit  
exit  
pedro@pedroserver:~$
```

Figura 6: Demostración de que la creación de usuarios y pruebas parte 2

En las pruebas obtenemos los GID de los grupos a los que pertenece el usuario y los cotejamos con el fichero **/etc/group**, verificando que se hayan creado con un GID asignado.

4. Creación de los permisos sobre las carpetas

Utilizamos ACL para la gestión de los permisos sobre las carpetas. Esto es porque si modificamos a nivel de sistema de ficheros, podemos dejar sin acceso a los grupos legítimos o originales el acceso, lectura, escritura y ejecución de los ficheros/directorios.

Instalamos el paquete de ACL que es necesario.

```
1 sudo apt install acl
```

Luego el paquete tiene dos herramientas que son muy útiles, una de ver los permisos y los grupos. Otra de asignarlos sobre grupos sin modificar los permisos originales.

```
1 sudo mkdir /var/www
2 sudo mkdir /var/public
3 # Permisos de developers
4 sudo setfacl -RPm g:developers:rwX /var/www
5 sudo setfacl -RPm g:developers:rwX /var/public
6 sudo setfacl -RPm g:developers:r— /media
7
8 # Permisos de admin
9 sudo setfacl -RPm g:admin:rwX /
10
11 # Permisos de ventas
12 sudo setfacl -RPm g:ventas:rwX /var/ventas
13 sudo setfacl -RPm g:ventas:rwX /var/public
```

El setfacl de la raíz rompe el sistema, ya que crea conflictos con los archivos del sistema generando que no tengan un comportamiento correcto, lo que no es recomendable utilizar esta parte del ejercicio en el futuro.

Referencias usadas: ⁴ ⁵

⁴<https://www.redhat.com/sysadmin/linux-access-control-lists>

⁵<https://linux.die.net/man/1/setfacl>