

Creación de Usuarios y Política de seguridad

Alejandro Rodríguez Rojas

Sumario

Ejercicio 1.....	3
Ejercicio2.....	5
Ejercicio 3.....	5
Ejercicio 4.....	5
Ejercicio 5.....	6
Ejercicio 6.....	7
Ejercicio 7.....	7
Ejercicio 8.....	8
Ejercicio 9.....	8
Ejercicio 10.....	8
Ejercicio 11.....	9
Ejercicio 12.....	10
Ejercicio 13.....	10

Ejercicio 1

Crea dos usuarios de nombre externo1 y externo2, que tengan el UID 1200 y UID 1201 respectivamente, tengan como comentario Becarios. Además tendrán como shell /bin/bash, y sus propios directorios personales. Ambos deben pertenecer al grupo externos de GID 1300.

Para hacer este ejercicio deberemos usar el comando newuser que funciona con la nomenclatura de /etc/passwd o /etc/shadow:

```
Dusuario:contraseña:UID:GID:GCOS:dir_ppal:shell
```

Y deberemos usar pwgen para generar una contraseña aleatoria

```
apt-get install pwgen
```

```
alexrr@pc-alex:~$ pwgen -ns 10 2
YNRB9SMNIG x5T5zruiWJ
alexrr@pc-alex:~$ for i in {1..2};do echo Externo$i:${pwgen -ns 10 1};done > Externos.txt
alexrr@pc-alex:~$ cat Externos.txt
Externo1:E0gJ2b0P0j
Externo2:8LSPe1Qmoe
alexrr@pc-alex:~$
```

Con esto tendremos las contraseñas ya guardadas en un fichero.

Escribimos en un fichero las siguientes lineas:

```
alexrr@pc-alex:~$ cat becarios.txt
externo1:E0gJ2b0P0j:1200:1300:Becarios,,,:/home/externo1:/bin/bash
externo2:8LSPe1Qmoe:1201:1300:Becarios,,,:/home/externo2:/bin/bash
alexrr@pc-alex:~$
```

Cambiamos los permisos del archivo para que solo pueda leerlo el administrador:

```
chmod 400 becarios.txt
```

Debemos crear el grupo externo con la GID indicada:

```
groupadd externos -g 1300
```

*-g es el parámetro que indica el GID

Hemos sustituido los valores por los mostrados en el ejercicio.

Hacemos uso del comando newuser:

newusers {archivo}

```
root@pc-alex:/home/alexrr# newusers becarios.txt
```

```
root@pc-alex:/home/alexrr# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,:/run/systemd/resolve:/bin/false
apt:x:104:65534:/nonexistent:/bin/false
rtkit:x:105:110:RealtimeKit,,:/proc:/bin/false
dnsmasq:x:106:65534:dnsmasq,,:/var/lib/misc:/bin/false
avahi-autoipd:x:107:111:Avahi autoip daemon,,:/var/lib/avahi-autoipd:/bin/false
messagebus:x:108:112:/var/run/dbus:/bin/false
usbmux:x:109:46:usbmux daemon,,:/var/lib/usbmux:/bin/false
geoclue:x:110:116:/var/lib/geoclue:/bin/false
speech-dispatcher:x:111:29:Speech Dispatcher,,:/var/run/speech-dispatcher:/bin/false
lightdm:x:112:117:Light Display Manager:/var/lib/lightdm:/bin/false
pulse:x:113:118:PulseAudio daemon,,:/var/run/pulse:/bin/false
avahi:x:114:121:Avahi mDNS daemon,,:/var/run/avahi-daemon:/bin/false
colord:x:115:122:colord colour management daemon,,:/var/lib/colord:/bin/false
saned:x:116:123:/var/lib/saned:/bin/false
hplip:x:117:7:HPLIP system user,,:/var/run/hplip:/bin/false
Debian-gdm:x:118:124:Gnome Display Manager:/var/lib/gdm3:/bin/false
alexrr:x:1000:1000:Alex,,:/home/alexrr:/bin/bash
mysql:x:119:125:MySQL Server,,:/nonexistent:/bin/false
postgres:x:120:126:PostgreSQL administrator,,:/var/lib/postgresql:/bin/bash
oracle:x:1001:1001:/u01/app/oracle:/bin/bash
uidd:x:121:128:/run/uidd:/bin/false
sshd:x:122:65534:/run/sshd:/usr/sbin/nologin
telnetd:x:123:129:/nonexistent:/bin/false
systemd-coredump:x:999:999:systemd Core Dumper:./sbin/nologin
prueba:x:1002:1002:/home/prueba:
libvirt-qemu:x:64055:105:Libvirt Qemu,,:/var/lib/libvirt:/bin/false
externo1:x:1200:1300:Becarios,,:/home/externo1:/bin/bash
externo2:x:1201:1300:Becarios,,:/home/externo2:/bin/bash
root@pc-alex:/home/alexrr#
```

```

root@pc-alex:/home/alexrr# cat /etc/shadow
root:$6$RmLH/DRj$FmpxC51pd4UmsGsnrC5oBzNx1bkrrEvUoKSMuaPwzb7RbcoSrFQYpzX28gHmNdfFIRGi8QHEy0PqP.EFyZ/X/:17878:0:99999:7:::
daemon*:17878:0:99999:7:::
bin*:17878:0:99999:7:::
sys*:17878:0:99999:7:::
sync*:17878:0:99999:7:::
games*:17878:0:99999:7:::
man*:17878:0:99999:7:::
lp*:17878:0:99999:7:::
mail*:17878:0:99999:7:::
news*:17878:0:99999:7:::
uucp*:17878:0:99999:7:::
proxy*:17878:0:99999:7:::
www-data*:17878:0:99999:7:::
backup*:17878:0:99999:7:::
list*:17878:0:99999:7:::
irc*:17878:0:99999:7:::
gnats*:17878:0:99999:7:::
nobody*:17878:0:99999:7:::
systemd-timesync*:17878:0:99999:7:::
systemd-network*:17878:0:99999:7:::
systemd-resolve*:17878:0:99999:7:::
apt*:17878:0:99999:7:::
rtkit*:17878:0:99999:7:::
dnsmasq*:17878:0:99999:7:::
avahi-autoipd*:17878:0:99999:7:::
messagebus*:17878:0:99999:7:::
usbmux*:17878:0:99999:7:::
geoclue*:17878:0:99999:7:::
speech-dispatcher:!:17878:0:99999:7:::
lightdm*:17878:0:99999:7:::
pulse*:17878:0:99999:7:::
avahi*:17878:0:99999:7:::
colord*:17878:0:99999:7:::
saned*:17878:0:99999:7:::
hplip*:17878:0:99999:7:::
Debian-gdm*:17878:0:99999:7:::
alexrr:$6$sFegCDa/$7Wm0b3KIyGMrdsg8wtbzoR4S5Qs0rBjT9ttMt60UGakfFRvKQGMt/wNV0YwkGrBellU2ie9me6xF0.RyT4/n/:17879:0:99999:7:::
mysql:!:17878:0:99999:7:::
postgres:$6$TnFrEsDQ$g2ZZIOXA1CE0Vq/rYAzNCr3uu1SIcUBop9hW0DUNYcnyovmaWsUk5XVjumXBfXB0T1ESVjGfUKgEDBtEXW40:17878:0:99999:7:::
oracle:!:17878:0:99999:7:::
uidd*:17879:0:99999:7:::
sshd*:17879:0:99999:7:::
telnetd*:17879:0:99999:7:::
systemd-coredump:!:17879:0:99999:7:::
prueba:$6$XNruFH8H$xS0YkgEQhuwZ2xyu6I0n4TIXp5GIn4cPt/UBGXN2Cp0XBv0eRr52CHF0jBzjKPsTyuHQf3Z/piItjYmMuvvr.:17883:0:99999:7:::
libvirt-qemu:!:17884:0:99999:7:::
externo1:$6$f0e2VFav$c6tQpXrCSu0yUHFib3yK0cMLFKIe27pB9HreyPt/qE5YIannrGvoGU4PXTgeDheDoBRJ5X4uF1mTEuFruTQum0:17906:0:99999:7:::
externo2:$6$SXjZnUJV$sPLt4naMGDQ7axiui99xhQ20N10XL7DCTaYAE0zAS1r0.50GCTX1m0sVHihohBZ2HfeYA8ANxIqGIUk82w/N0:17906:0:99999:7:::
root@pc-alex:/home/alexrr#

```

Ejercicio2

Quando el usuario intenta acceder al sistema, ¿qué es lo que ocurre?, indica los procedimientos que seguirías como administrador para investigar y solventar el problema.

Si a los usuarios no se les pone contraseña(anteriormente la he puesto), la cuenta estará bloqueada, por lo que un administrador tendría que ponerle una contraseña para que los demás usuarios puedan acceder a dicha cuenta:

```

passwd externo1
passwd externo2

```

Si no queremos introducirle la contraseña, podremos desbloquear la cuenta manualmente(No es recomendable)

```

usermod externo1 -U
usermod externo2 -U

```

Ejercicio 3

Añade un grupo con el nombre itinerantes con GID 1400.

Para añadir un nuevo grupo utilizaremos el siguiente comando:

groupadd {nombre} -g {GID}

*-g es el parametro que indica GID

```
alexrr@pc-alex:~$ groupadd itinerantes -g 1400
bash: groupadd: no se encontró la orden
alexrr@pc-alex:~$ sudo su
[sudo] password for alexrr:
root@pc-alex:/home/alexrr# groupadd itinerantes -g 1400
root@pc-alex:/home/alexrr#
```

Ejercicio 4

Editamos el archivo con:

nano /etc/group

Y añadimos a la derecha el nombre del usuario

```
GNU nano 2.7.4
ssh:x:113:
bluetooth:x:114:alexrr
lpadmin:x:115:alexrr
geoclue:x:116:
lightdm:x:117:
pulse:x:118:
pulse-access:x:119:
scanner:x:120:saned,alexrr
avahi:x:121:
colord:x:122:
saned:x:123:
Debian-gdm:x:124:
alexrr:x:1000:
mysql:x:125:
postgres:x:126:
dba:x:1001:
vboxusers:x:127:
uidd:x:128:
telnetd:x:129:
kvm:x:105:
systemd-coredump:x:999:
wireshark:x:130:
prueba:x:1002:
ubridge:x:131:
libvirt:x:132:
libvirt-gemu:x:64055:libvirt-gemu
externos:x:1300:
itinerantes:x:1400:externo1
```

Ejercicio 5

Modifica la información de cambio de contraseña de externo1. No se puede cambiar la contraseña antes de 10 días, y es obligatorio cambiar la contraseña cada 30 días. Indica las diferentes métodos que puedes emplear.

Para verificar la caducidad de la cuenta debemos usar el comando chage

chage -l externo1

```
alexrr@pc-alex:~$ groupadd itinerantes -g 1400
bash: groupadd: no se encontró la orden
alexrr@pc-alex:~$ sudo su
[sudo] password for alexrr:
root@pc-alex:/home/alexrr# groupadd itinerantes -g 1400
root@pc-alex:/home/alexrr# nano /etc/group
root@pc-alex:/home/alexrr# nano /etc/group
root@pc-alex:/home/alexrr# chage -l externo1
Último cambio de contraseña                : ene 10, 2019
La contraseña caduca                        : nunca
Contraseña inactiva                        : nunca
La cuenta caduca                           : nunca
Número de días mínimo entre cambio de contraseña : 0
Número de días máximo entre cambio de contraseña : 99999
Número de días de aviso antes de que caduque la contraseña : 7
root@pc-alex:/home/alexrr#
```

En este caso nunca caducará la contraseña, por ello para cambiarlo debemos usar los siguientes parámetros

-l : Sirve para observar la caducidad de la cuenta

-m: Sirve para cambiar el número de días mínimo entre cambio de contraseña

-M: Sirve para cambiar el número de días máximo entre cambio de contraseña

```
root@pc-alex:/home/alexrr# chage -m 10 -M 30 externo1
root@pc-alex:/home/alexrr# chage -l externo1
Último cambio de contraseña                : ene 10, 2019
La contraseña caduca                        : feb 09, 2019
Contraseña inactiva                        : nunca
La cuenta caduca                           : nunca
Número de días mínimo entre cambio de contraseña : 10
Número de días máximo entre cambio de contraseña : 30
Número de días de aviso antes de que caduque la contraseña : 7
root@pc-alex:/home/alexrr#
```

Ejercicio 6

¿Qué realizan los comandos pwck y grpck? . ¿Para que lo emplearías?.

Pwck → Verifica la correcta integridad de los usuarios en el sistema

grpck → Verifica la correcta integridad de los grupos en el sistema

Su uso sería para verificar que un usuario o grupo está creado correctamente, por ejemplo para verificar que la carpeta personal está creada o que la contraseña este caducada y por tanto la cuenta este bloqueada.

Ejercicio 7

Crea las carpetas externos e itinerantes. Dichas carpetas pertenecerán a root, y al grupo de su nombre. En las carpetas externos e itinerantes, todos los miembros pertenecientes a un grupo, podrán acceder y escribir en su carpeta, es decir grupo externos en carpeta externos, todo objeto creado por un usuario debe pertenecer al grupo. Crea la carpeta publica, en ellas podrán acceder y escribir todo usuario del sistema pero no podrán borrar objetos que no les pertenezcan.

Para crear las carpetas debemos usar el comando:

mkdir externos itinerantes

Luego usamos el comando chgrp para cambiar los permisos de grupos:

```
root@pc-alex:/home/alexrr/prueba# ls -l
total 8
drwxr-xr-x 2 root root 4096 ene 10 10:02 externos
drwxr-xr-x 2 root root 4096 ene 10 10:02 itinerantes
root@pc-alex:/home/alexrr/prueba# chgrp externos/ externos
root@pc-alex:/home/alexrr/prueba# chgrp externos externos/
root@pc-alex:/home/alexrr/prueba# chgrp itinerantes itinerantes/
root@pc-alex:/home/alexrr/prueba# ls -l
total 8
drwxr-xr-x 2 root externos 4096 ene 10 10:02 externos
drwxr-xr-x 2 root itinerantes 4096 ene 10 10:02 itinerantes
```

Para que los miembros pertenecientes a un grupo puedan acceder y escribir en su carpeta debemos darle los permisos de lectura, escritura y ejecución.

```
root@pc-alex:/home/alexrr/prueba# chmod 770 externos/
root@pc-alex:/home/alexrr/prueba# chmod 770 itinerantes/
root@pc-alex:/home/alexrr/prueba# ls -l
total 8
drwxrwx--- 2 root externos 4096 ene 10 10:02 externos
drwxrwx--- 2 root itinerantes 4096 ene 10 10:02 itinerantes
root@pc-alex:/home/alexrr/prueba#
```


Para crear la carpeta publica volvemos a utilizar el comando:

```
mkdir publica
```

Y cambiamos los permisos:

```
root@pc-alex:/home/alexrr/prueba# chmod 766 publica/
root@pc-alex:/home/alexrr/prueba# ls -l
total 12
drwxrwx--- 2 root externos  4096 ene 10 10:02 externos
drwxrwx--- 2 root itinerantes 4096 ene 10 10:02 itinerantes
drwxrw-rw- 2 root root      4096 ene 10 10:14 publica
root@pc-alex:/home/alexrr/prueba#
```

Ejercicio 8

Pon una contraseña al grupo itinerantes. La contraseña será: itinerantes.

Para cambiar la contraseña utilizaremos el comando:

```
gpasswd {nombre grupo}
```

```
root@pc-alex:/home/alexrr/prueba# gpasswd itinerantes
Cambiando la contraseña para el grupo itinerantes
Nueva contraseña:
Vuelva a introducir la nueva contraseña:
root@pc-alex:/home/alexrr/prueba#
```

Ejercicio 9

¿Cómo podría acceder el usuario externo2 a la carpeta de itinerantes?.

Necesitaría contactar con el administrador del sistema para que le añadiese al grupo de itinerantes con el comando:

```
adduser externo2 itinerantes
```

O también cambiando el propietario de la carpeta:

```
chown externo2:itinerantes /itinerantes
```

Ejercicio 10

Analiza las funciones que realizan los ficheros en conexiones **no ssh**:

`/etc/issue`
`/etc/issue.net`
`/etc/motd`

Pon ejemplos de aplicación.

`/etc/issue` → Es el mensaje de bienvenida antes de que un usuario haga su log in

`/etc/issue.net` → Es el mensaje de bienvenida al usuario que se conecta a nuestra máquina.

`*/etc/issue` actua como ambos ficheros hasta que `/etc/issue.net` sea configurado

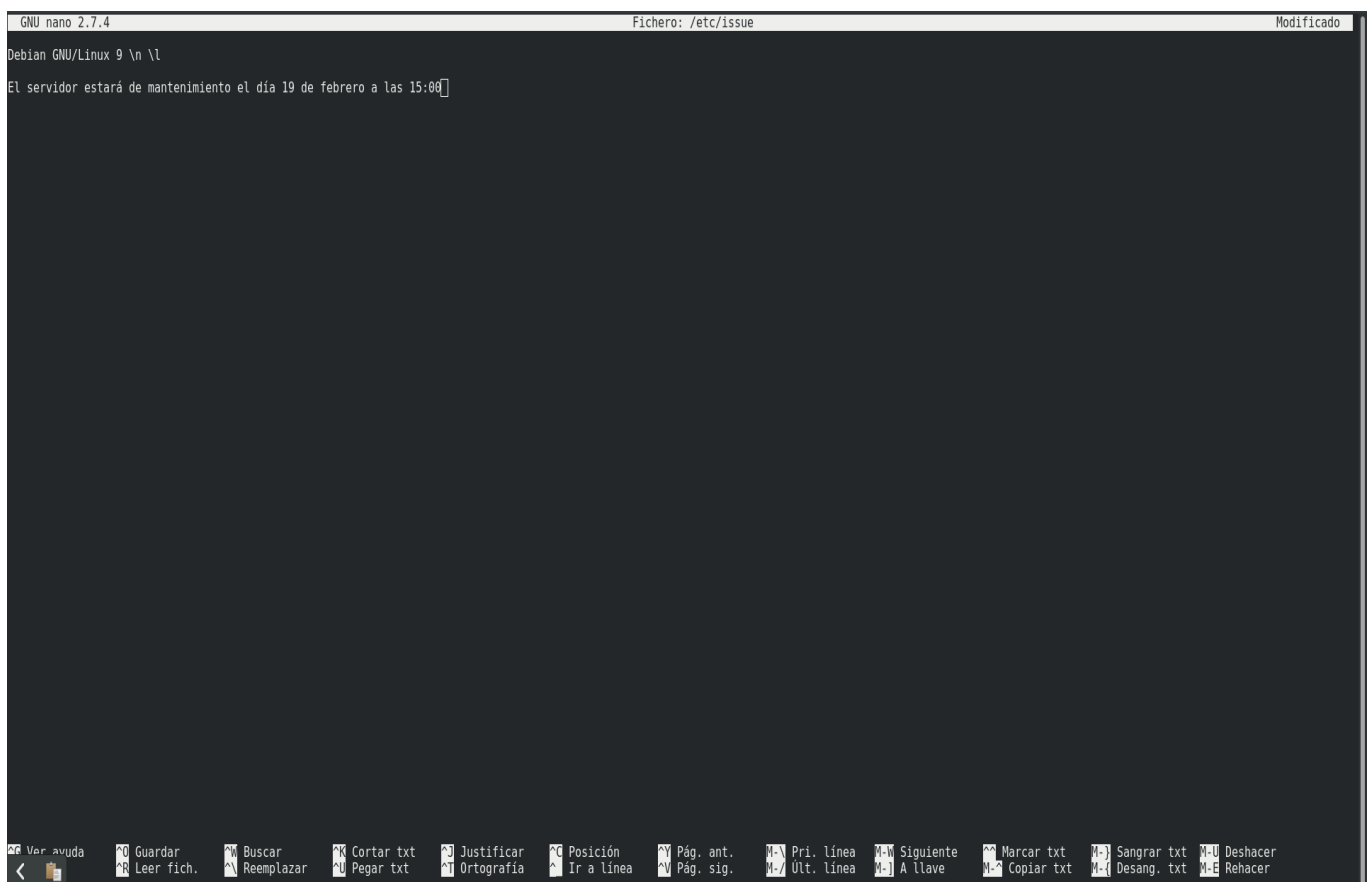
`/etc/motd` → Es el mensaje que aparece cuando un usuario se conecta a una terminal.

Un ejemplo de aplicación para los `/etc/issues` seria avisar al usuario del hardware que tuviera dicho ordenador/servidor, tambien la fecha cuando inició,etc.

Un ejemplo de aplicación de `/etc/motd` seria alertar al usuario que él sería mensajes de avisos, configurar varios parámetros para el usuario,etc.

Ejercicio 11

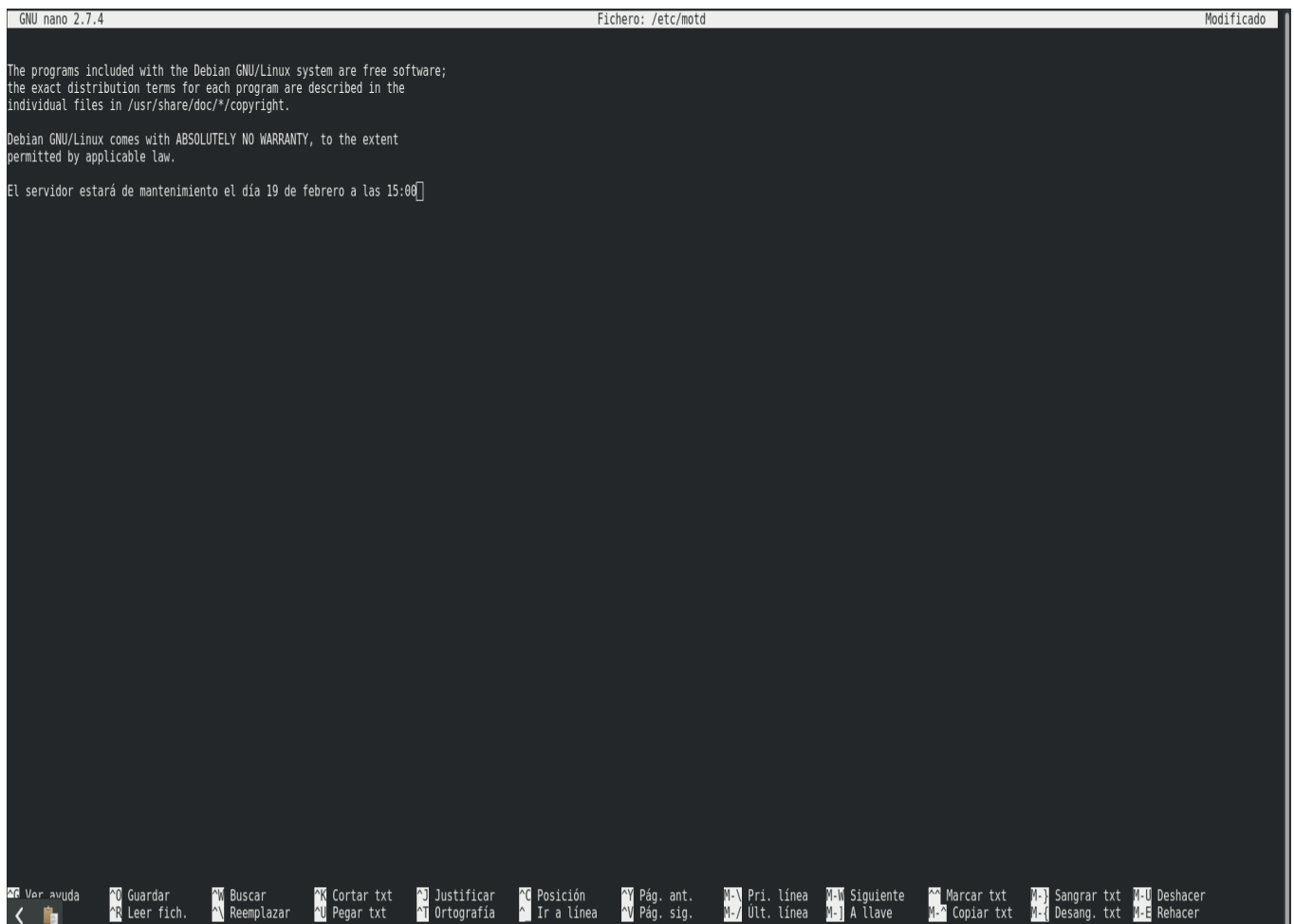
Si queremos avisar al usuario antes de entrar en su login editaremos el archivo `/etc/issue` o `/etc/issue.net`



```
GNU nano 2.7.4                                Fichero: /etc/issue                                Modificado
Debian GNU/Linux 9 \n \l
El servidor estará de mantenimiento el día 19 de febrero a las 15:00

Ver ayuda  Guardar  Buscar  Cortar txt  Justificar  Posición  Pág. ant.  M-V Pri. línea  M-W Siguiente  Marcar txt  M-} Sangrar txt  M-U Deshacer
< Leer fich.  Reemplazar  Pegar txt  Ortografía  Ir a línea  Pág. sig.  M- Ult. línea  M-] A llave  M-~ Copiar txt  M-~ Desang. txt  M-E Rehacer
```

Y si queremos avisar al usuario cuando hace login en una terminal pues editariamos el `/etc/motd`



```
GNU nano 2.7.4                                Fichero: /etc/motd                                Modificado

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

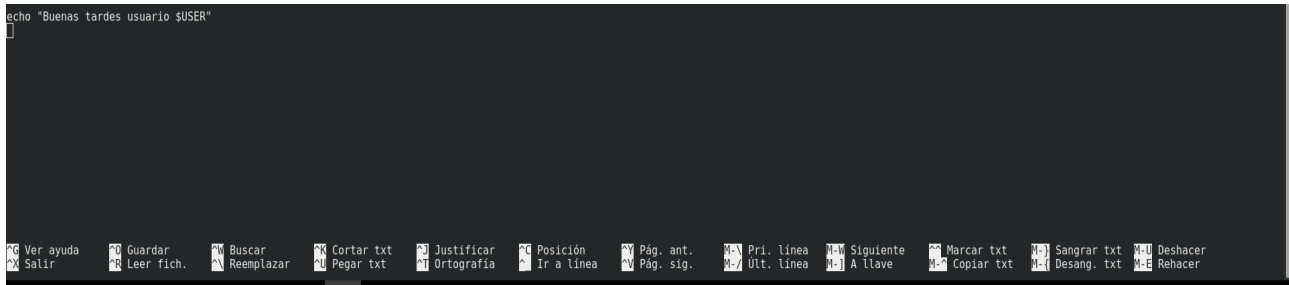
El servidor estará de mantenimiento el día 19 de febrero a las 15:00

Var avuda  Guardar  Buscar  Cortar txt  Justificar  Posición  Pág. ant.  Pri. línea  Siguiente  Marcar txt  Sangrar txt  Deshacer
<  Leer fich.  Reemplazar  Pegar txt  Ortografía  Ir a línea  Pág. sig.  Ult. línea  A llave  Copiar txt  Desang. txt  Rehacer
```

Ejercicio 12

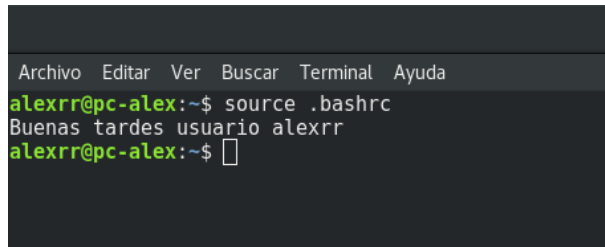
¿Cómo configurarías mensaje personalizados de inicio para un usuario concreto?

Como cada usuario tiene en su `/home/user` un script que ejecuta la bash, podremos usar eso como método de mensaje de bienvenida personalizado cada vez que inicie la bash



```
echo "Buenas tardes usuario $USER"
```

The screenshot shows a terminal window with a dark background. At the top, the command `echo "Buenas tardes usuario $USER"` is entered. Below it, the output `Buenas tardes usuario alexrr` is displayed. At the bottom of the window, there is a menu bar with various icons and text labels: Ver ayuda, Guardar, Buscar, Cortar txt, Justificar, Posición, Pág. ant., Pri. línea, Siguiente, Marcar txt, Sangrar txt, Deshacer, Salir, Leer fich., Reemplazar, Pegar txt, Ortografía, Ir a línea, Pág. sig., Ult. línea, A llave, Copiar txt, Desang. txt, and Rehacer.



```
alexrr@pc-alex:~$ source .bashrc
Buenas tardes usuario alexrr
alexrr@pc-alex:~$
```

The screenshot shows a terminal window with a dark background. The prompt `alexrr@pc-alex:~$` is followed by the command `source .bashrc`. The output `Buenas tardes usuario alexrr` is displayed. The prompt `alexrr@pc-alex:~$` is followed by a cursor.

Ejercicio 13

En el supuesto de acceder a la terminal vía ssh, ¿cómo lo configurarías?. Modificación de /etc/ssh/sshd_config

LoginGraceTime: Estableceremos el tiempo necesario para introducir la contraseña, evitando que el atacante tenga que “pensar mucho”.

Con esto evitaremos que un atacante intente averiguar la contraseña mediante fuerza bruta.

MaxAuthTries: Número de intentos permitidos al introducir la contraseña antes de desconectarnos.

Esto serviría también para lo dicho anteriormente, el atacante no podrá ingresar contraseñas por fuerza bruta.

MaxStartups: Número de logins simultáneos desde una IP, para evitar que se pueda utilizar la fuerza bruta con varias sesiones a la vez.

Con esto evitaremos que nuestro ordenador o servidor se ralentice por una masiva entrada de pcs.

AllowUsers: Es crear una lista blanca de usuario. Este parámetro nos permite configurar los usuarios que podrán conectarse. Una medida muy restrictiva pero a la vez muy segura ya que bloqueará todas las conexiones de los usuarios que no estén en el listado. Los usuarios que tengamos aquí podrán conectarse, y el resto no.

Con esto nos aseguraremos que solo unos usuarios puedan entrar por ssh al ordenador o servidor

DenyUsers: Parecido al anterior, pero ahora creamos una lista negra. Los usuarios que tengamos aquí no podrán conectarse, y el resto sí.

Si sacamos del usuario que ataca a nuestro ordenador o servidor la IP, podremos bloquearlo mediante esta opción

AllowGroups/DenyGroups: Exactamente igual a lo anterior, pero en lugar de crear una lista blanca/negra de usuarios, es de grupos de usuarios.

Con esto podremos habilitar o deshabilitar grupos de usuarios para que entren por ssh.