

# [FORT] Práctica 1: Fortificación del arranque de Linux

```
menuentry Entrada
  setroot=(hd0,msdos1)
  linux /vmlinuz root=/dev/sda1
  initrd /initrd.img
```

## 1. Interrumpir el booteo y conseguir la forma cifrada de la contraseña de root

Para empezar pulsaremos c durante el arranque e introduciremos los siguientes comandos en la consola de Root:

```
set root=hd0,msdos1
ls /
cat /etc/shadow
```

Con Cat podremos ver las contraseñas cifradas, incluida la de Root:

```
2hDUxW2CpRNAP.nhYHuiY4z.lMiFL5SP.4ZBt0:20115:0:99999:7:::
user090:$6$JTQWRWZNK2xLxcRo$nj9agUDg8mrpSZbaSZjm/LyRL39MQLbR8k3ePbL4dQhc0dQu
90fqiv0R5cUSXKaQAaWlVkzU4odNoyjSLZpLT.:20115:0:99999:7:::
user091:$6$QRDgE3oSXrp13UxG$NKQ5.Rfja6hr7UVw0t6SD0FxfvqGIdPfUARKGP.l4Va2ekUt
hUpt0Jw6YTyy0mpdaLmB.4oY2u70wnif9mQAv/:20115:0:99999:7:::
user092:$6$q16IhEJkEQqPSFgc$ayyRDxbTS4myMxY0dk7.dnznYYJhVLEMBJ34A3PdS9420xBh
DR6A721P.Fa4.YyacBlWVkeH092mLJMmB4V9d1:20115:0:99999:7:::
user093:$6$tSG0AWP98koIwj4L$9YfMHjY153NTUfEcVl.H530jCT9XUCJz6LzGRQR1W0D26J5R
/Av.0lycQLq8Kckfx8v26y/5tW0mCw9uuIeW9/:20115:0:99999:7:::
user094:$6$mvJdAiBiPNP1Fkr0$issxN01N/d6JLPM6SKGXxA1uUy9cuywndbFGeWnRP8sU2PqU
zn2jnF4gEK0uo4If27PxX1Fj/d15XUSMdpIQD0:20115:0:99999:7:::
user095:$6$wP/N3Ega6C1iSu0h$IfkGvcQQItUgJILCpPZCbVjNGlRqzWmxersNvFmnmq8aUspP
vnythB3ljEdagLzYl0j6/IB3ivt8/JgZ2GbZi1:20115:0:99999:7:::
user096:$6$qBy70n2fCitIkL.g$QTAZqWE92GaPYlHhs8uJgm1U3op9NsNNk4y0H9Q180yUnH/j
qbAE0ebUwJPJEpINEvo0K059qujAb4EvQpPF0/:20115:0:99999:7:::
user097:$6$dCYTU8DNl0YV9tCq$dvtoUpXKJA1K6UKAvIiscNUz1ifqe483TupuU6D7ewirGuPw
ZjCkK0.pDobhsUoU/0yYJrcCUzh.nUfKDwx6c0:20115:0:99999:7:::
user098:$6$2uD67sTITMB3GteV$uj/t0Nyf4yEK2r3BAEeg3vDZH8cUjGH62Xf9zL3fRMPp52dX
S5kWoY0TfKF1IMba09mszEuuPhWSjJ/JwA0Mp.:20115:0:99999:7:::
user099:$6$t0Vdm8qIQCEGnq.$2HAhEHaQNHLt5e7IVacnqFYBQHeDyrXN4EMWguGq2w.cVhd/
fDplEATJAgulffXu.HmMDkrSUECVCMs20gNEh.:20115:0:99999:7:::
user100:$6$LJKJ6znoc14u1kTg$d2rBGshCumWbu4.QTGyy1xLzNd064Ek0Kfmgcf.UsgCr1Pq
9TnzDmBaAq67bXrXty/UECXfc.93mbvm7rDNn.:20115:0:99999:7:::
vboxadd!:20115:::
thejuanvisu:$y$j9T$P15GH7Lq10BkRGWKSmjX10$6ABpJkpxi0YVUw5p3P0wLnlzOXGuZA2pHv
aUPo25aH8:20123:0:99999:7:::
```

```
grub> s_
grub>
```

## 2. Conseguir Root editando los parámetros pasados al kernel cuando se bootea

Ya sea desde línea de comandos o editando el menú

## 3. Definir dos superusuarios de grub y establecer contraseñas para ellos

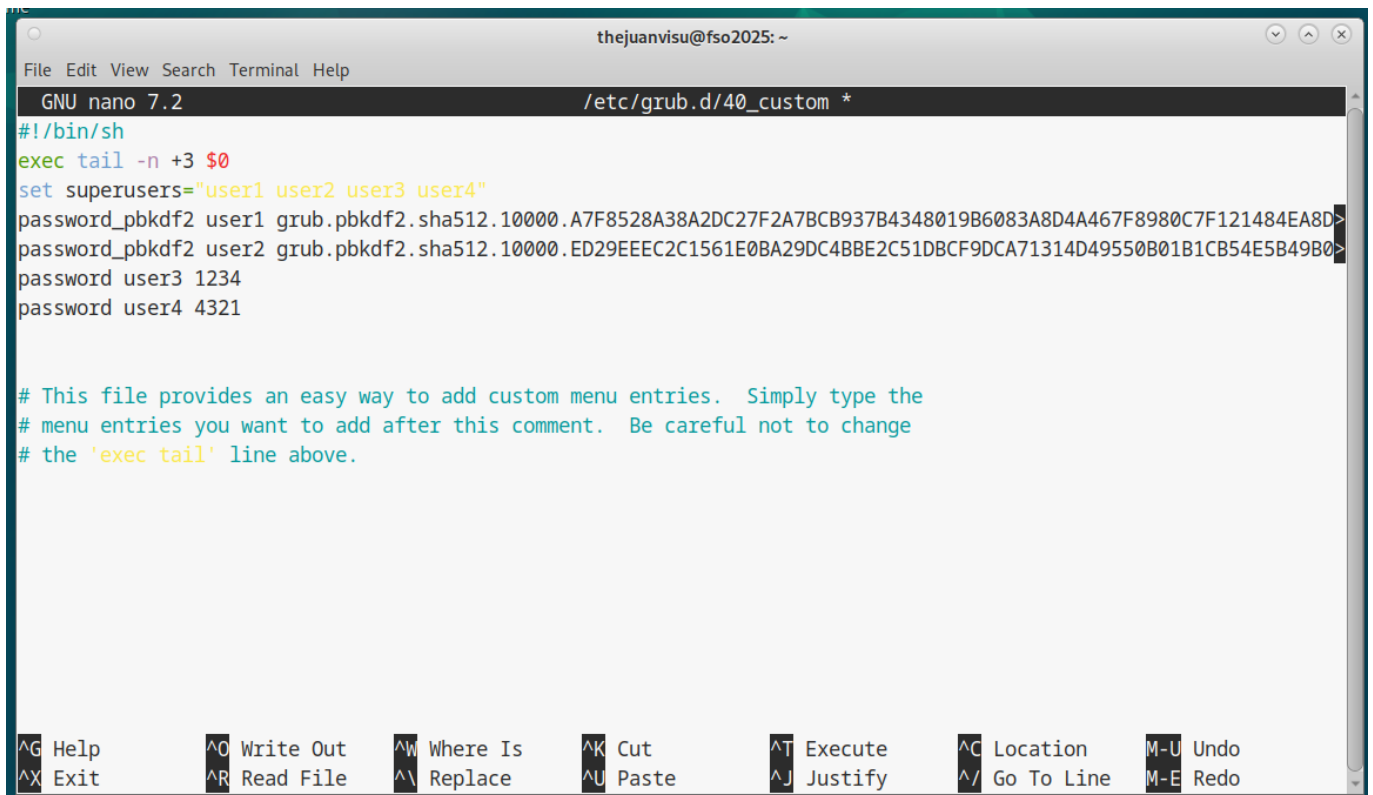
*2 en texto plano y 2 cifradas de forma que todavía existan cuando la configuración de Grub se actualiza*

Primero creamos dos contraseñas almacenadas en texto plano y, tras eso, para cifrar las contraseñas se usa el comando:

```
grub-mkpasswd-pbkdf2
```

```
thejuanvisu@fso2025:~$ grub-mkpasswd-pbkdf2
Enter password:
Reenter password:
PBKDF2 hash of your password is grub.pbkdf2.sha512.10000.A7F8528A38A2DC27F2A7BCB937B4348019B6083A8D4A467F8980C7F1
21484EA8D69601CEF87358B5E727577F285DB92709E60892C374FA1666EF25E8E6651F51.10A967E612DB9D58894001C9F2F837E032A1D529
BE22A74ADA32DCCC04AD6F434BCB201075A80F6F5CABC4D7ADFBDE3CD89FF41EF862E3FF4214D2C0F61734F7
thejuanvisu@fso2025:~$ grub-mkpasswd-pbkdf2
Enter password:
Reenter password:
PBKDF2 hash of your password is grub.pbkdf2.sha512.10000.ED29EEEC2C1561E0BA29DC4BBE2C51DBC9DCA71314D49550B01B1CB
54E5B49B025BC00CFCE3E4457A2AA839A87D7DDAD700E1E9C8CF698D56566C5E6ED252A.3F29457802CA55F1710923F80DDFA1E612BF1728
AC5D47D877232677DD7052BF067084593D7833031AD0A942DFCF75F243DB0F6D4358F077BD9F2CE49CD4E534
thejuanvisu@fso2025:~$
```

Tras eso se procede a modificar el archivo `/etc/grub.d/40_custom` y se añade dentro los super usuarios, en este caso tendremos `user1` y `user2` con contraseña segura y `user3` y `user4` con contraseña insegura:



```
thejuanvisu@fso2025: ~
File Edit View Search Terminal Help
GNU nano 7.2 /etc/grub.d/40_custom *
#!/bin/sh
exec tail -n +3 $0
set superusers="user1 user2 user3 user4"
password_pbkdf2 user1 grub.pbkdf2.sha512.10000.A7F8528A38A2DC27F2A7BCB937B4348019B6083A8D4A467F8980C7F121484EA8D>
password_pbkdf2 user2 grub.pbkdf2.sha512.10000.ED29EEEC2C1561E0BA29DC4BBE2C51DBC9DCA71314D49550B01B1CB54E5B49B0>
password user3 1234
password user4 4321

# This file provides an easy way to add custom menu entries.  Simply type the
# menu entries you want to add after this comment.  Be careful not to change
# the 'exec tail' line above.

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_/ Go To Line  M-E Redo
```

Tras eso actualizamos la configuración de grub:

```
root@fso2025:~# update-grub
Generating grub configuration file ...
Found background image: /usr/share/images/desktop-base/desktop-grub.png
Found linux image: /boot/vmlinuz-6.1.0-30-amd64
Found initrd image: /boot/initrd.img-6.1.0-30-amd64
Found linux image: /boot/vmlinuz-6.1.0-29-amd64
Found initrd image: /boot/initrd.img-6.1.0-29-amd64
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
done
root@fso2025:~#
```

## 4. Verificar que solo el superuser de grub pueda acceder a la línea de comandos del grub

Podemos observar que al reiniciar se nos solicita nombre y usuario para poder acceder a la terminal de grub:



## 5. Añade 2 entradas llamadas UserOnly y AlwaysAvailable

- AlwaysAvailable: Puede ser arrancada por cualquiera
- UserOnly: solo puede ser booteada por los usuarios
- Solo los superusuarios pueden bootear las entradas restantes

From:

<https://www.knoppia.net/> - **Knoppia**

Permanent link:

[https://www.knoppia.net/doku.php?id=master\\_cs:fortificacion:p1&rev=1738683826](https://www.knoppia.net/doku.php?id=master_cs:fortificacion:p1&rev=1738683826)

Last update: **2025/02/04 15:43**

