[FORT] Práctica 1: Fortificación del arranque de Linux

```
menuentry Entrada
  setroot=(hd0,msdos1)
  linux /vmlinux 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:

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.ED29EEEC2C1561E0BA29DC4BBE2C51DBCF9DCA71314D49550B01B1CB
54E5B49B025BC00CFCEF3E4457A2AA839A87D7DDAD700E1E9C8CF698D56566C5E6ED252A.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:

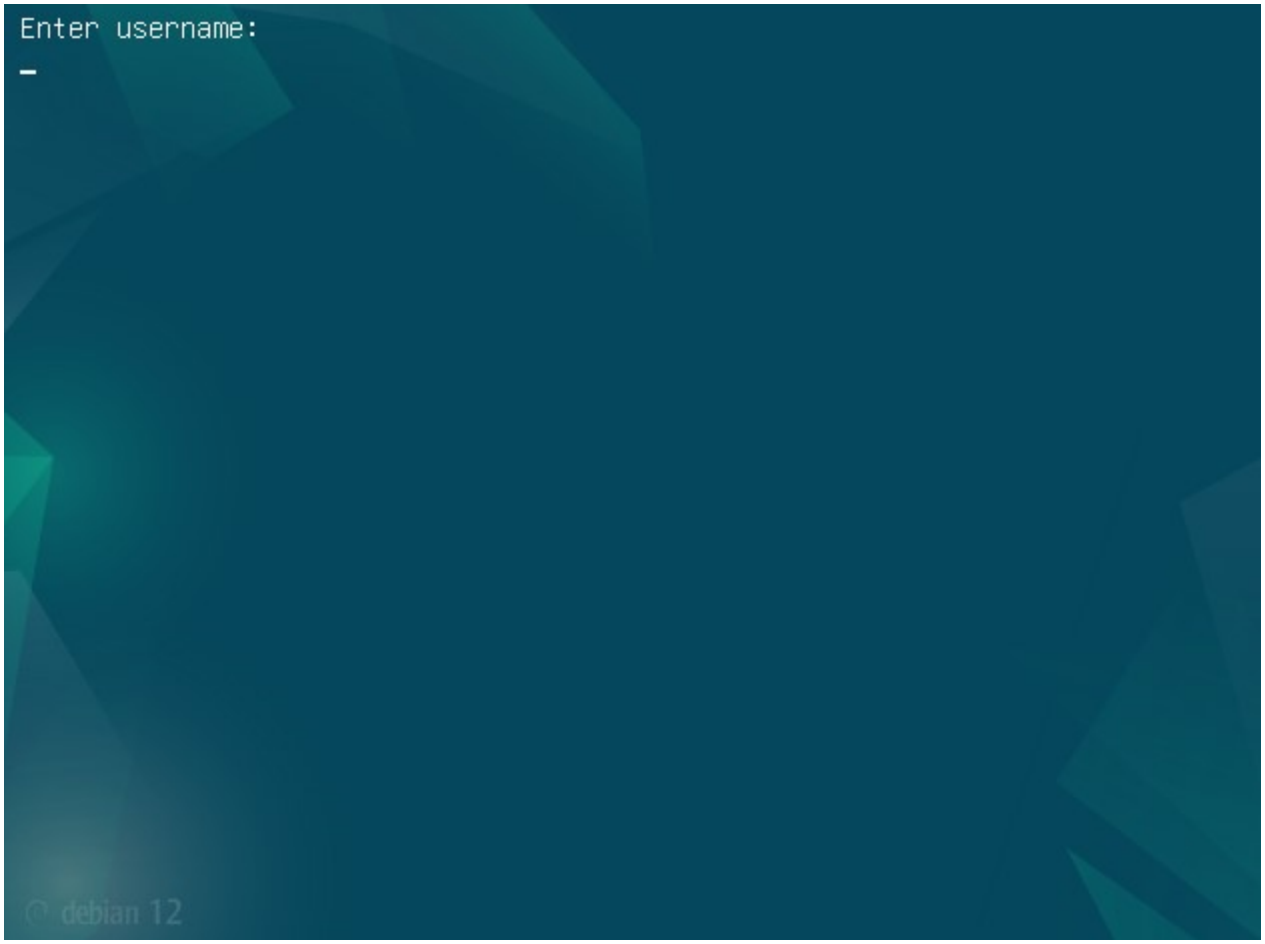
```
thejuanvisu@fso2025: ~
File  Edit  View  Search  Terminal  Help
  GNU nano 7.2                    /etc/grub.d/40_custom *
#!/bin/sh
exec tail -n +3 $0
set superusers="user1 user2 user3 user4"
password_pbkdf2 user1 grub.pbkdf2.sha512.10000.A7F8528A38A2DC27F2A7BCB937B4348019B6083A8D4A467F8980C7F121484EA8D>
password_pbkdf2 user2 grub.pbkdf2.sha512.10000.ED29EEEC2C1561E0BA29DC4BBE2C51DBCF9DCA71314D49550B01B1CB54E5B49B0>
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 comadnos 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

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