[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

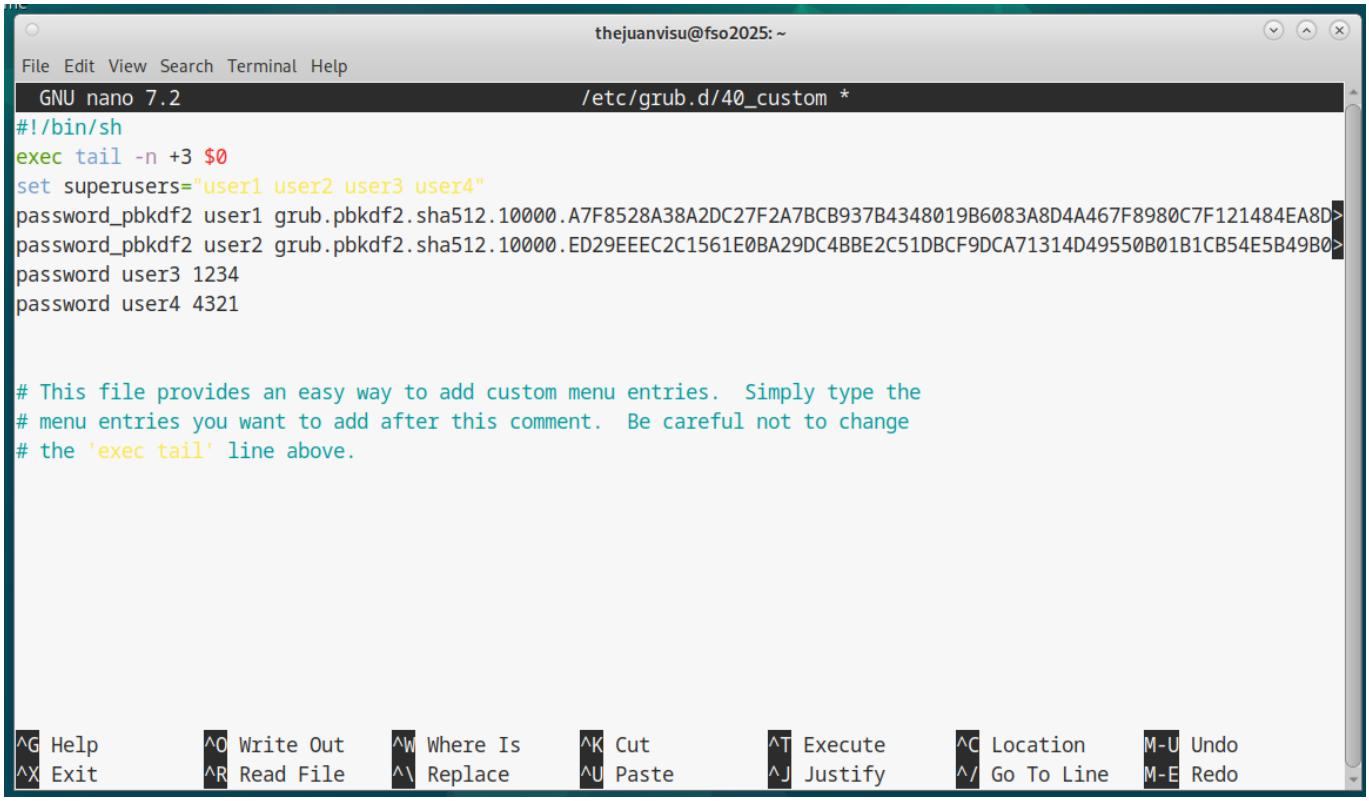
3. Definir dos superusuarios de grub y establecer contraseñas para ellos

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
```

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:

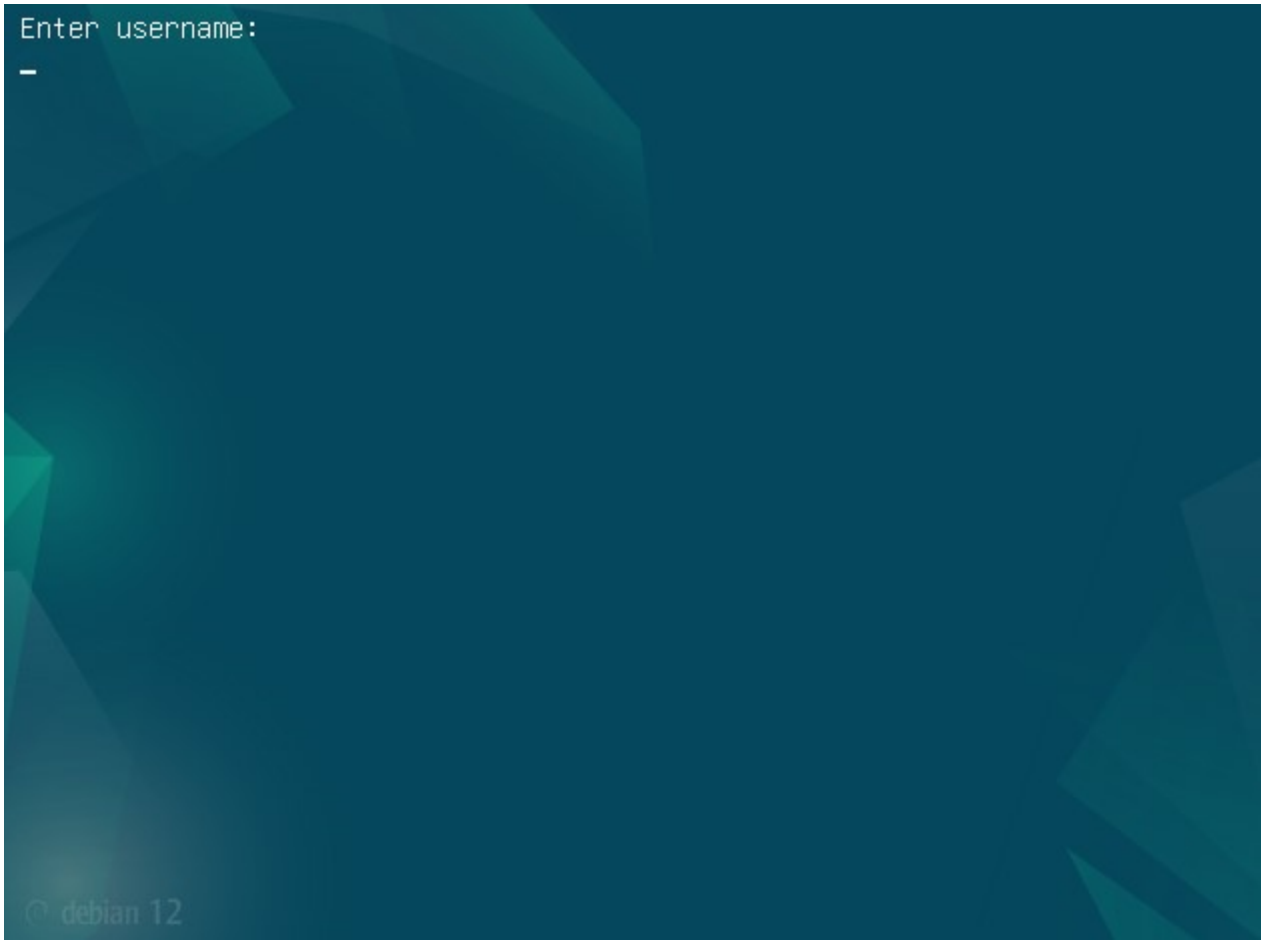


Tras eso actualizamos la configuración de grub:

```
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