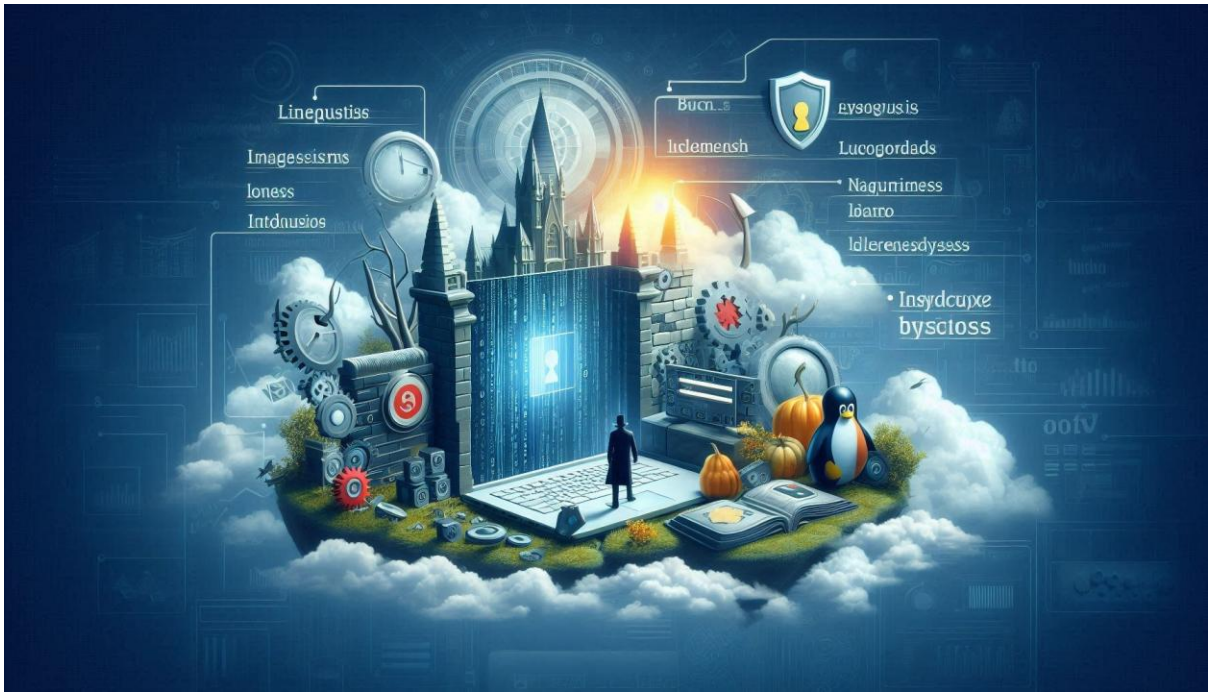


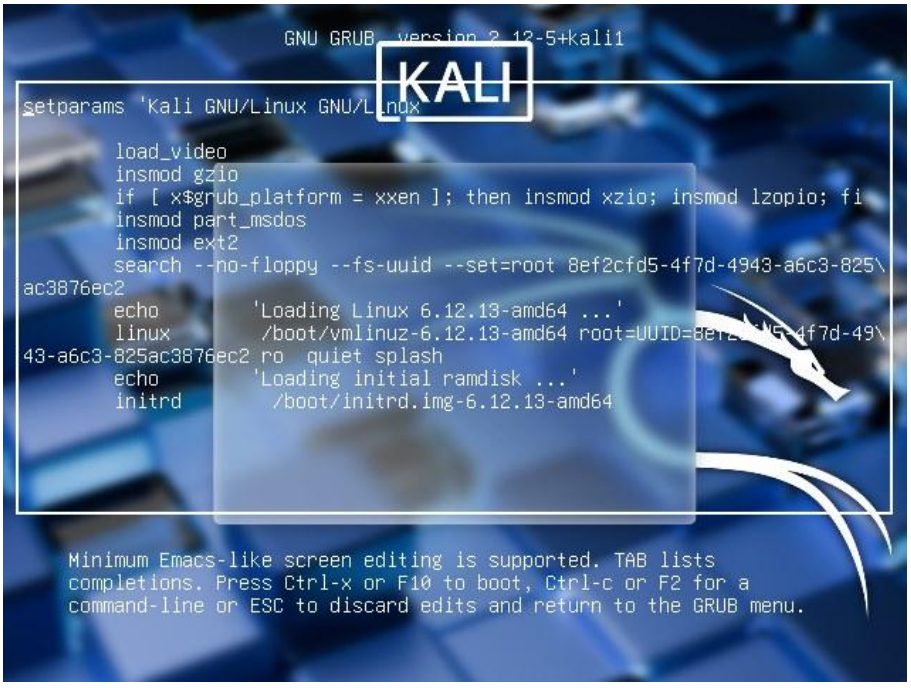
Bypass login Linux

El «bypass» del login mediante el GRUB implica acceder a un sistema Linux sin pasar por el proceso habitual de inicio de sesión. Esto se logra mediante la manipulación del cargador de arranque GRUB, que es responsable de iniciar el sistema operativo. Al realizar ciertos cambios en la configuración del GRUB, se puede ingresar directamente al sistema sin requerir credenciales de inicio de sesión, lo cual puede representar un riesgo de seguridad si no se protege adecuadamente

Para ello, lo que haremos será modificar unas líneas en grub para que, en lugar de realizar un arranque convencional, se ejecute una Shell con los privilegios de un super usuario.

Primero enciende la máquina y espera hasta que muestre el cargador de arranque grub en la pantalla.

Para abrir la terminal de grub, debemos pulsar la tecla **e** en la pantalla de selección de OS a arrancar.

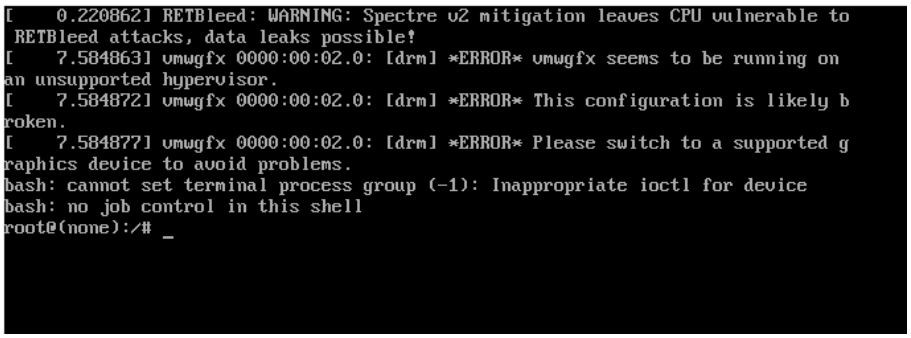


En aquí la sección de Linux tenemos que hacer algunos cambios primero tenemos que hacer es cambiar la **ro** que significa leer solo por **rw** que significa read&write/lectura y escritura y en la última de la línea necesitamos agregar **init=/bin/bash**

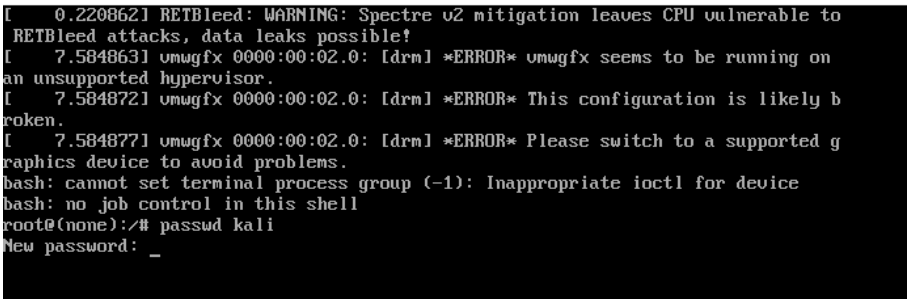
Cuando se realizan todos los cambios presione **CTRL+X** para guardar y salir

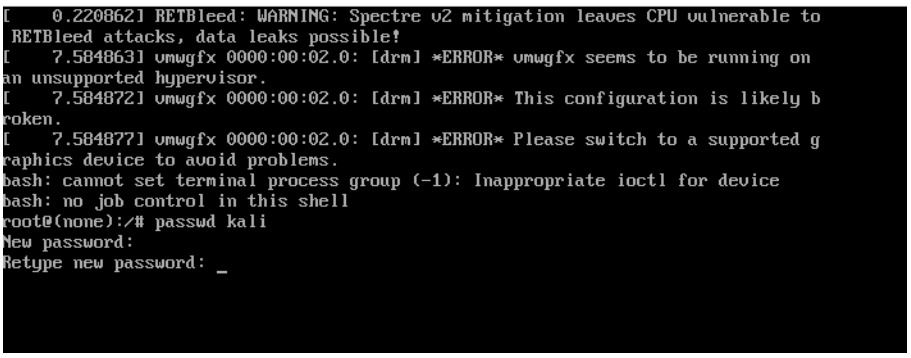
Podemos acceder a todos los archivos y vamos a cambiar la contraseña del usuario que necesitemos; en este caso la del superusuario Kali

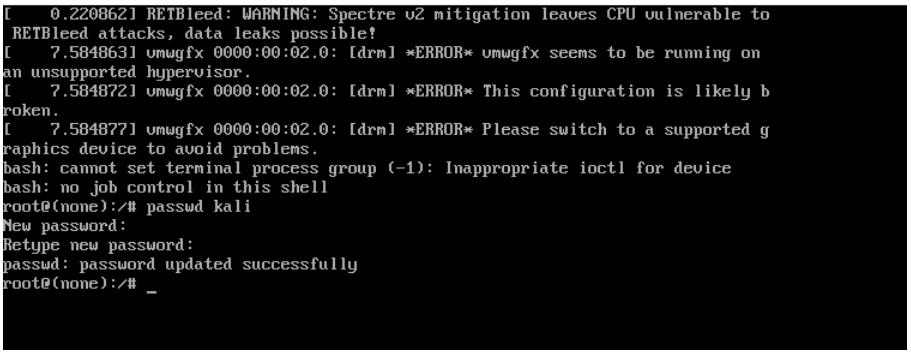
passwd Kali

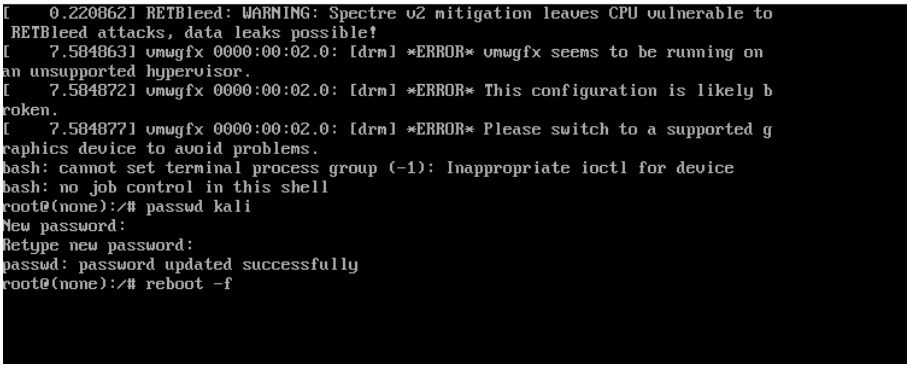


Nos pedirá que repitamos el nuevo password

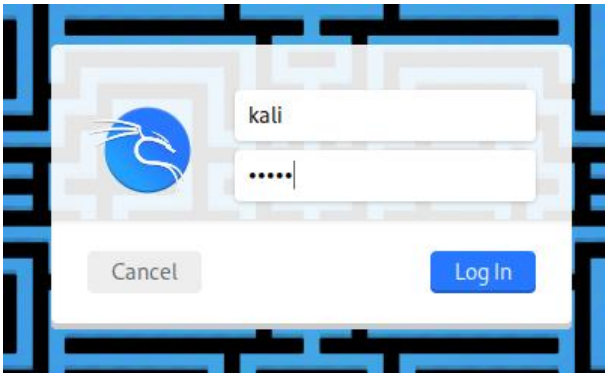








Una vez cambiada la contraseña reiniciaremos mediante **reboot -f** e iniciaremos sesión con la contraseña que hayamos modificado.



La solución estándar es añadir un **usuario de GRUB** (llamado *superuser*) protegido por contraseña. Esto restringe la capacidad de editar el menú de arranque solo a ese usuario.

1. Generar la Contraseña Cifrada (Hash)

Necesitas generar un *hash* seguro de tu contraseña utilizando el algoritmo **PBKDF2**, ya que las contraseñas en texto plano no se utilizan en la configuración de GRUB.

1. Abre la terminal y ejecuta el siguiente comando:

```
grub-mkpasswd-pbkdf2
```

2. El sistema te pedirá que ingreses la contraseña deseada y que la confirmes.
3. El comando generará una línea de salida similar a esta:
4. GRUB2 password hash is grub.pbkdf2.sha512.10000.A92A...[MUCHO MÁS TEXTO]
5. **Copia toda esta línea de salida, comenzando por grub.pbkdf2,** ya que la necesitarás en el siguiente paso.

2. Editar el Archivo de Configuración de GRUB

Para aplicar la protección de contraseña a nivel global, debes editar el archivo que genera la configuración principal de GRUB.

1. Abre el archivo de configuración principal de GRUB con privilegios de *root*:

```
sudo nano /etc/grub.d/00_header
```

2. **IMPORTANTE:** Desplázate hasta la línea que dice cat << EOF (generalmente al principio del archivo) y **justo antes de esa línea,** añade las siguientes dos líneas, reemplazando el contenido entre comillas:
    - USUARIO_GRUB: Define un nombre de usuario que tendrá la autoridad (*superuser*).
    - [HASH COPIADO]: Pega el *hash* completo que generaste en el Paso 1.

```
set superusers="USUARIO_GRUB"
password_pbkdf2 USUARIO_GRUB [HASH COPIADO]
```

Ejemplo práctico:

```
set superusers="admin"
password_pbkdf2 admin grub.pbkdf2.sha512.10000.A92A...
```

3. Guarda el archivo (Ctrl+O) y sal de nano (Ctrl+X).

3. Aplicar la Configuración de GRUB

Para que los cambios surtan efecto, debes regenerar el archivo de configuración final de GRUB (/boot/grub/grub.cfg).

1. Ejecuta el comando para actualizar la configuración:

```
sudo update-grub
```

2. Verás que el sistema procesa los archivos del directorio /etc/grub.d/ y actualiza el archivo de configuración.

4. Verificar la Protección

Finalmente, **reinicia el sistema** para verificar que la contraseña funciona correctamente:

1. Reinicia el sistema:

sudo reboot

2. Cuando aparezca el menú de GRUB, intenta presionar la tecla e (para editar la entrada).
3. Si la configuración fue exitosa, el sistema te pedirá el **nombre de usuario** (USUARIO_GRUB) y la **contraseña** que definiste en el Paso 1.
    - Los usuarios sin la contraseña aún podrán iniciar el sistema operativo normalmente, pero no podrán modificar los parámetros de arranque. Esto mitiga el riesgo de seguridad de la escalada de privilegios a través del menú de GRUB.