

Proteger el grub con password

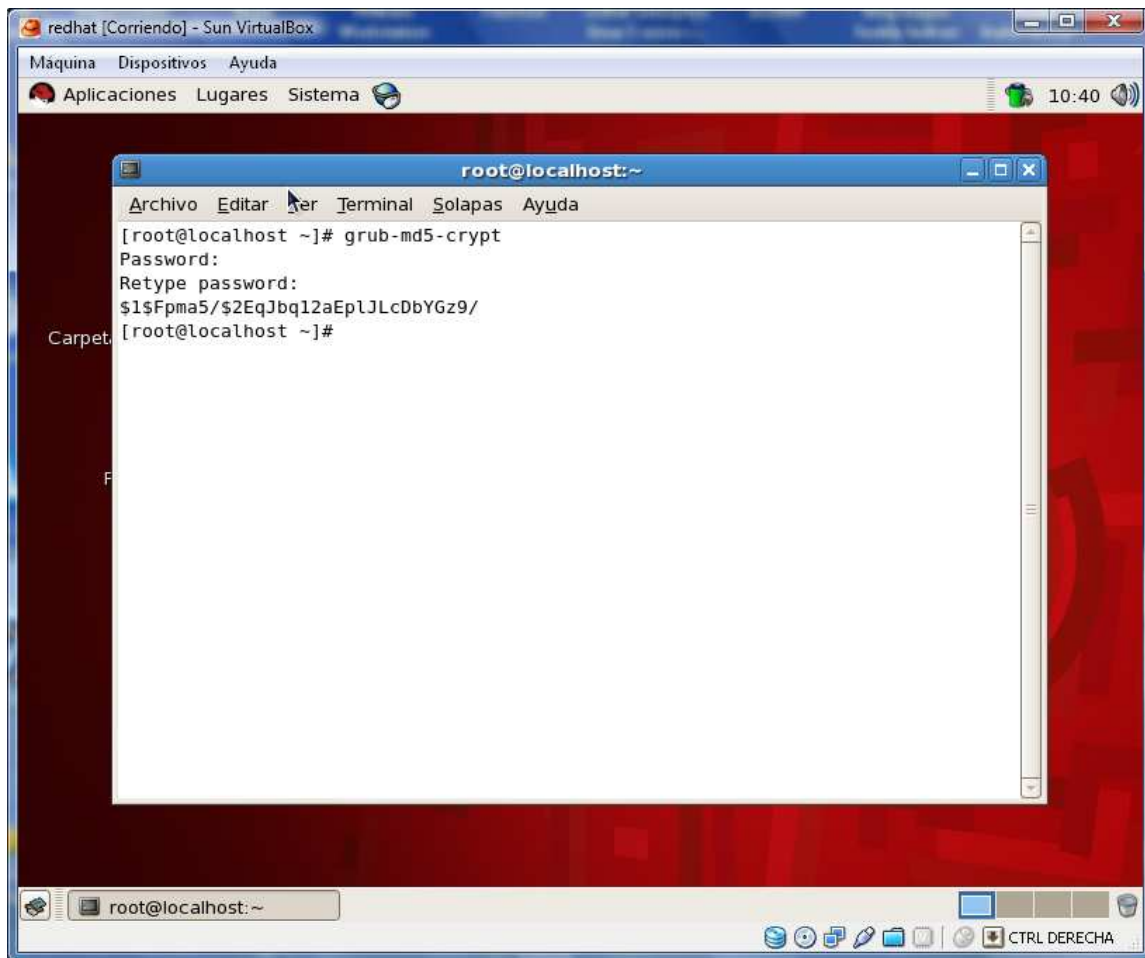
Freddy Alfonso Beltran

Contraseñas del gestor de arranque

A continuación se muestran las razones principales por las cuales se debe proteger el gestor de arranque de Linux:

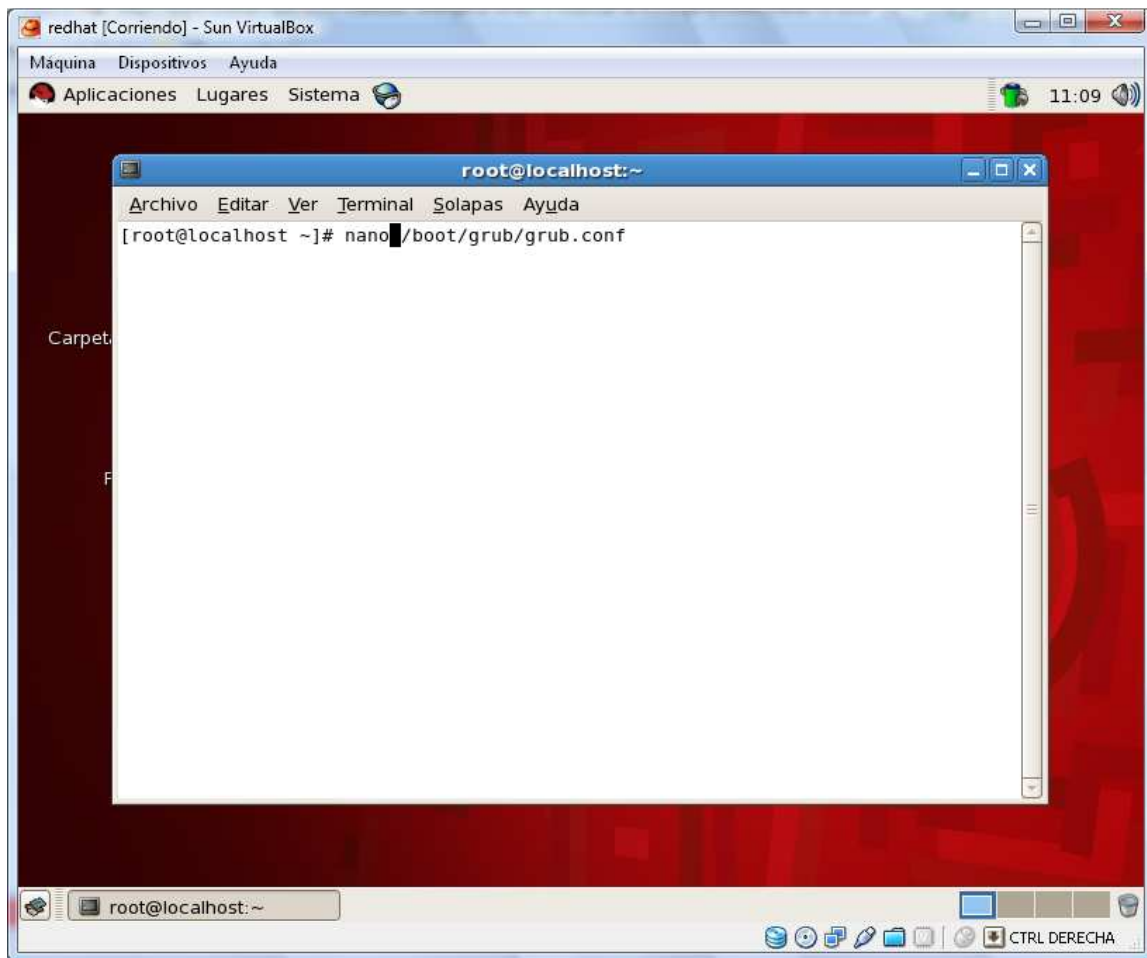
1. *Previene el acceso en modo monousuario* — Si un atacante puede arrancar en modo monousuario, se convierte en el superusuario de forma automática sin que se le solicite la contraseña de acceso.
2. *Previene el acceso a la consola de GRUB* — Si la máquina utiliza GRUB como el gestor de arranque, un atacante puede usar la interfaz del editor para cambiar su configuración o para reunir información usando el comando `cat`.
3. *Previene el acceso a sistemas operativos inseguros* — Si es un sistema de arranque dual, un atacante puede seleccionar un sistema operativo en el momento de arranque, tal como DOS, el cual ignora los controles de acceso y los permisos de archivos.

Genero la clave que para este caso es qwerty con el comando `grub-md5-crypt`



copio la cadena generada qwerty en formato MD5 para ubicarla en el archivo /boot/grub/grub.conf o en menú.lst

Edito este archivo con cualquier editor de texto, pero para este caso utilizo el nano



Después edito el archivo e inserto la clave encriptada

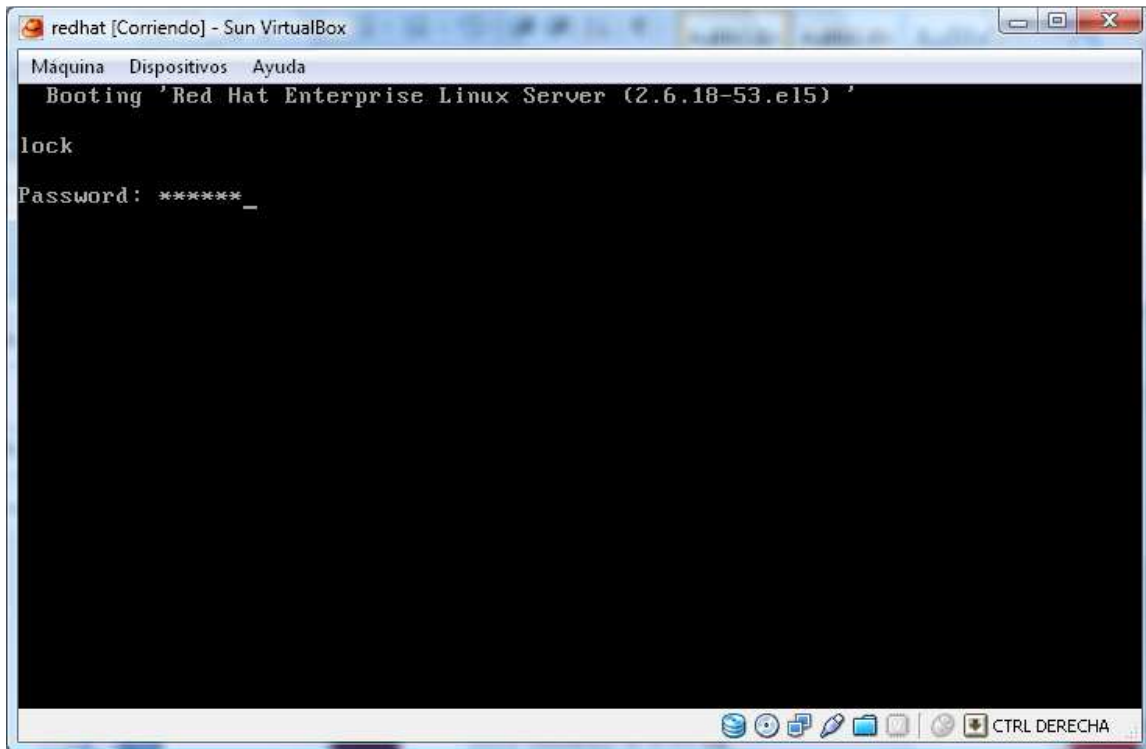
```
root@localhost:~  
Archivo Editar Ver Terminal Solapas Ayuda  
GNU nano 1.3.12 Fichero: /boot/grub/grub.conf Modificado  
default=0  
timeout=5  
splashimage=(hd0,0)/grub/splash.xpm.gz  
hiddenmenu  
  
#aqui inserto la clave encriptada en MD5  
  
title Red Hat Enterprise Linux Server (2.6.18-53.el5)  
  lock  
  password --md5 $1$Fpma5/$2EqJbq12aEp1JLcDbYGz9  
  root (hd0,0)  
  kernel /vmlinuz-2.6.18-53.el5 ro root=/dev/VolGroup00/LogVol00 rhgb quib  
  initrd /initrd-2.6.18-53.el5.img  
  
^G Ver ayuda ^O Guardar ^R L Fichero ^Y Pág Ant ^K CortarTxt ^C Pos act  
^X Salir ^J Justificar ^W Buscar ^V Pág Sig ^U UnCut Text ^T Ortografía
```

Guardamos y ya

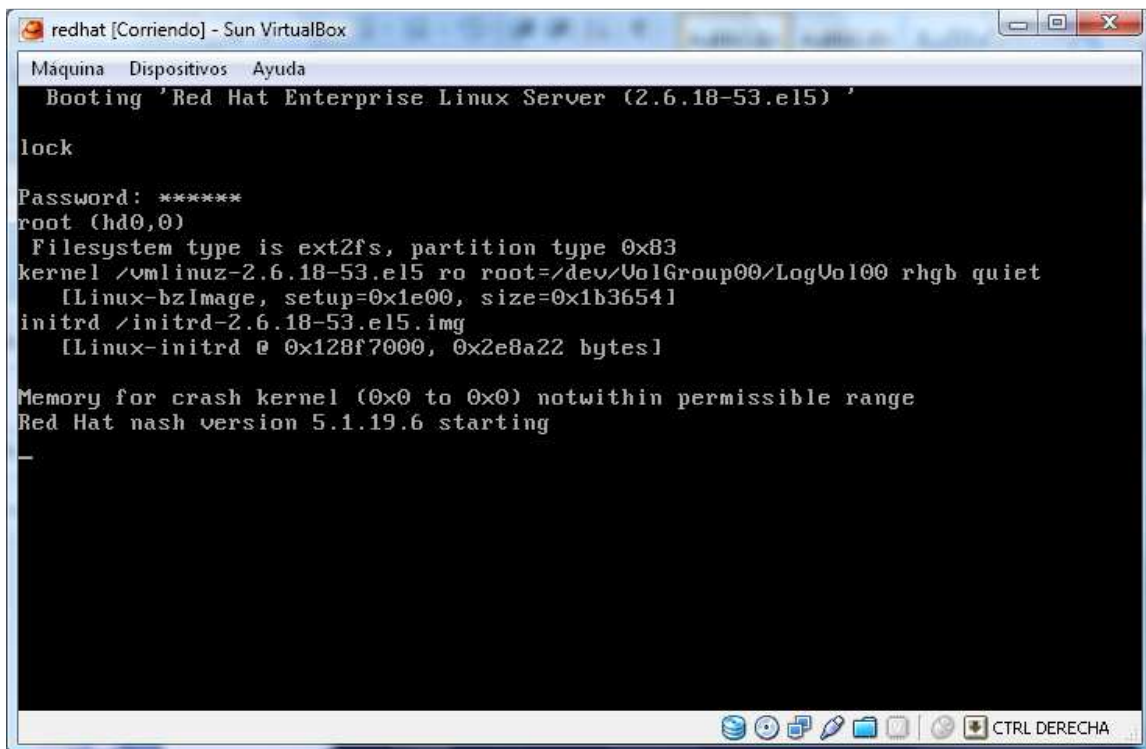
Cada vez que necesites cambiar la contraseña para el grub deberás efectuar el mismo procedimiento.

Ahora reiniciamos la maquina y después de 5 segundos observamos este pantallazo

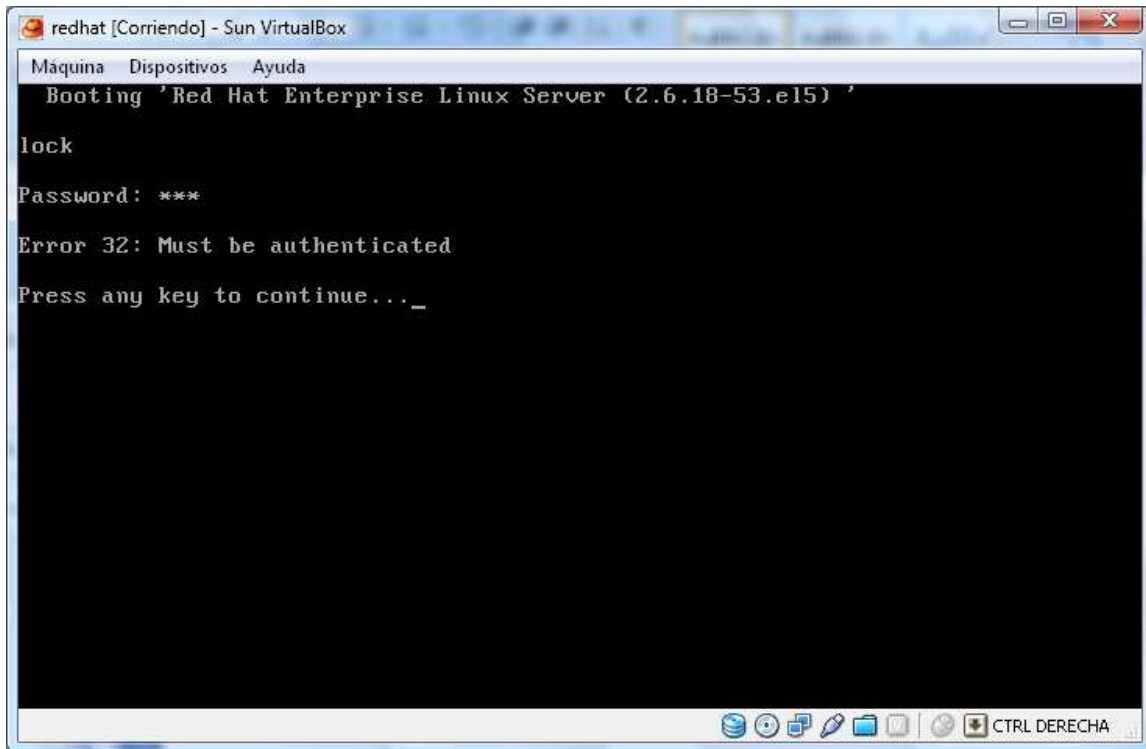
Que me indica que el grub ahora tiene una clave para ingresar y sin esta clave no puedes arrancar tu maquina Linux



Al darle la contraseña correcta se visualiza el arranque de nuestro Linux



Pero al digitarle con propósito de prueba una contraseña que no corresponde al ejercicio automáticamente se visualiza un error



Gracias y DIOS padre los bendiga