

ANEXO PROTEGER EL GRUB Y LA BIOS



Grub Rescue Commands



PEDRO RUIZ NÚÑEZ

GRUB

```
pedro@kali: ~  
(pedro@kali)-[~]  
$ sudo nano /etc/grub.d/00_header  
[sudo] password for pedro:  
(pedro@kali)-[~]  
$
```

Sirve para acceder a una consola donde veremos que la compone y así poder modificar el contenido para poder añadir nuestros usuarios y contraseñas

```
GNU nano 5.4 /etc/grub.d/00_header *  
cmosclean $GRUB_BUTTON_CMOS_ADDRESS  
EOF  
fi  
  
# Play an initial tune  
if [ "x${GRUB_INIT_TUNE}" != "x" ] ; then  
    echo "play ${GRUB_INIT_TUNE}"  
fi  
  
if [ "x${GRUB_BADRAM}" != "x" ] ; then  
    echo "badram ${GRUB_BADRAM}"  
fi  
fi  
  
# Nuevos usuarios  
cat << EOF  
set superusers="root,pedro"  
password root 1234  
password pedro 4321  
EOF
```

Dentro de la consola anteriormente mencionada nos iremos al final y escribiremos el código que aparece marcada esto servirá para que cuando iniciemos otra vez tengamos que introducir esos datos

```
pedro@kali: ~  
[pedro@kali]-[~]  
$ sudo nano /etc/grub.d/00_header  
[sudo] password for pedro:  
[pedro@kali]-[~]  
$ sudo grub-mkpasswd-pbkdf2  
Introduzca la contraseña:  
Reintroduzca la contraseña:  
grub-mkpasswd-pbkdf2: error: las contraseñas no coinciden.  
[pedro@kali]-[~]  
$ sudo grub-mkpasswd-pbkdf2  
Introduzca la contraseña:  
Reintroduzca la contraseña:  
El hash PBKDF2 de su contraseña es grub.pbkdf2.sha512.10000.764A5E52E1ED4C9CEADB  
CBAF0A6853386A58B7968E36D7F0378306829E7D9EF2D5A540475287FB5E3A0FE906C5D0218FDE87  
28FB4D58AB29E3F57852A1D845FF.129A69DF66E751964308CA2E234EB62B317BD567365A5D26770  
3276996FD74DDD3B0A18D0EA63250B78197735E03C4E4E1AF06F363CB16D6FBC0B7865AADE9F9  
[pedro@kali]-[~]  
$
```

Le introducimos ese comando para que nos salga la contraseña cifrada y así sea mas complicada de deducir si sufrimos un ataque y así el atacante tenga mayor dificultad para poder acceder al sistema, por ello este código lo guardaremos porque nos servirá mas adelante

```
pedro@kali: ~  
Introduzca la contraseña:  
Reintroduzca la contraseña:  
grub-mkpasswd-pbkdf2: error: las contraseñas no coinciden.  
[pedro@kali]-[~]  
$ sudo grub-mkpasswd-pbkdf2  
Introduzca la contraseña:  
Reintroduzca la contraseña:  
El hash PBKDF2 de su contraseña es grub.pbkdf2.sha512.10000.764A5E52E1ED4C9CEADB  
CBAF0A6853386A58B7968E36D7F0378306829E7D9EF2D5A540475287FB5E3A0FE906C5D0218FDE87  
28FB4D58AB29E3F57852A1D845FF.129A69DF66E751964308CA2E234EB62B317BD567365A5D26770  
3276996FD74DDD3B0A18D0EA63250B78197735E03C4E4E1AF06F363CB16D6FBC0B7865AADE9F9  
[pedro@kali]-[~]  
$ sudo grub-mkpasswd-pbkdf2  
Introduzca la contraseña:  
Reintroduzca la contraseña:  
El hash PBKDF2 de su contraseña es grub.pbkdf2.sha512.10000.50FD1AFFAC091AA9E8F4  
04A66566D901DFE0E64A08E73351FF98B11B5531AD317284927B91867AFB2ED7A55616562331BA36  
B24608F5ED2B35B3479C443F57DD.D619C5916831F75F429BA750AC7DC0C3ACC8C10EAEAE4831C0F  
1C3C8E4788BB886D8509AAFE94939B61D663FC7BE5AC9C913AC7986FB6292702675A1F1AA17  
[pedro@kali]-[~]  
$
```

Lo mismo pero para el otro usuario que hemos asignado, al igual que en el otro guardaremos este dato para mas adelante

```
pedro@kali: ~  
GNU nano 5.4 /etc/grub.d/00_header *  
  
# Play an initial tune  
if [ "${GRUB_INIT_TUNE}" != "x" ]; then  
    echo "play ${GRUB_INIT_TUNE}"  
fi  
  
if [ "${GRUB_BADRAM}" != "x" ]; then  
    echo "badram ${GRUB_BADRAM}"  
fi  
  
# Nuevos usuarios  
cat << EOF  
set superusers="root,pedro"  
password_pbkdf2 root  
grub.pbkdf2.sha512.10000.764A5E52E1ED4C9CEADBCBAF0A6853386A58B7968E36D7F0378306  
password_pbkdf2 pedro  
grub.pbkdf2.sha512.10000.50FD1AFFAC091AA9E8F404A66566D901DFE0E64A08E73351FF98B1  
EOF  
  
^G Ayuda ^O Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación  
^X Salir ^R Leer fich. ^E Reemplazar ^U Pegar ^J Justificar ^_ Ir a línea
```

Volvemos a acceder a la consola para que ahora como anteriormente hicimos cambiaremos la contraseña que pusimos básica por el hash que hemos guardado; para que esto funcione tenemos que asignar cuidadosamente cada hash para cada usuario y a su vez esto tiene que ir con el nombre de usuario separado por un espacio sino lo que nos ocurriría es que al iniciar la maquina se nos rompería porque no tenemos asignada bien esa contraseña y no podremos acceder ya nunca mas

```
pedro@kali: ~  
-(pedro@kali)-[~]  
$  
-(pedro@kali)-[~]  
$ sudo nano /etc/grub.d/00_header 130 x  
-(pedro@kali)-[~]  
$  
-(pedro@kali)-[~]  
$ sudo nano /etc/grub.d/00_header 130 x  
-(pedro@kali)-[~]  
$ sudo update-grub2  
Generating grub configuration file ...  
Found theme: /boot/grub/themes/kali/theme.txt  
Found background image: /usr/share/images/desktop-base/desktop-grub.png  
Found linux image: /boot/vmlinuz-5.10.0-kali3-amd64  
Found initrd image: /boot/initrd.img-5.10.0-kali3-amd64  
done  
-(pedro@kali)-[~]  
$
```

Una vez hecho lo anterior guardaremos nuestra configuración y haremos un update para que la información sea la nueva que hemos realizado y así funcione como nosotros la hemos escrito



Si hemos hecho todo lo anterior correctamente al iniciar de nuevo nuestra maquina virtual de Kali tendría que salirnos esta pantalla muy parecida donde nos pedirán nuestro usuario y contraseña donde introduciremos los valores por defecto asignados y una vez que lo hagamos se nos iniciara todo tal y como siempre

BIOS

Nos vamos a Inicio > Configuración

Seleccionamos la opción Actualización y seguridad

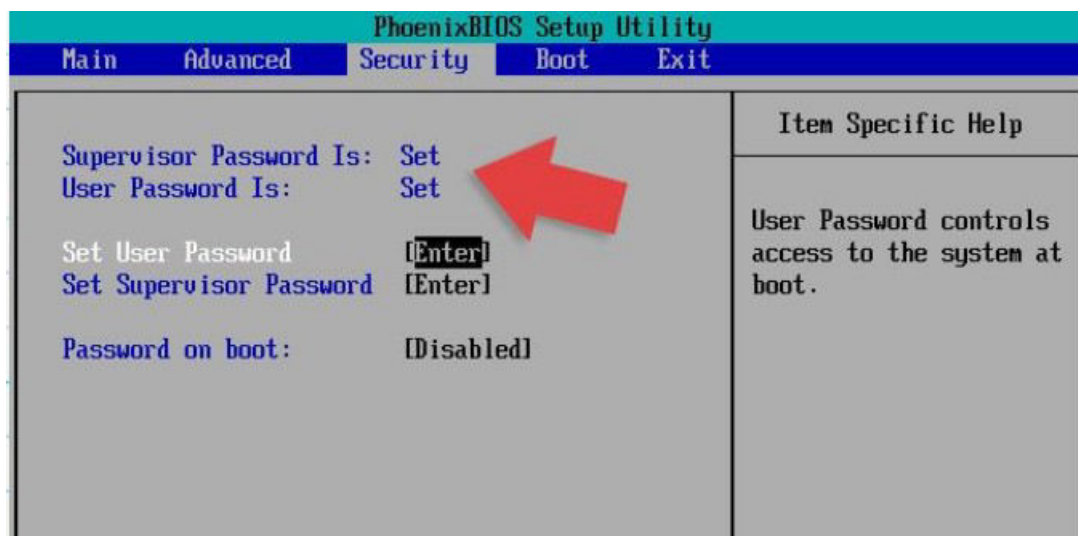
Vamos a Recuperación > Reiniciar ahora

Elegimos la opción Solucionar problemas

En opciones avanzadas clicamos en Configuración de firmware UEFI

Clicamos en el botón Reiniciar

El sistema reiniciará y mostrará el menú de arranque



Y lo unico que nos falta es asignar una contraseña y listo.