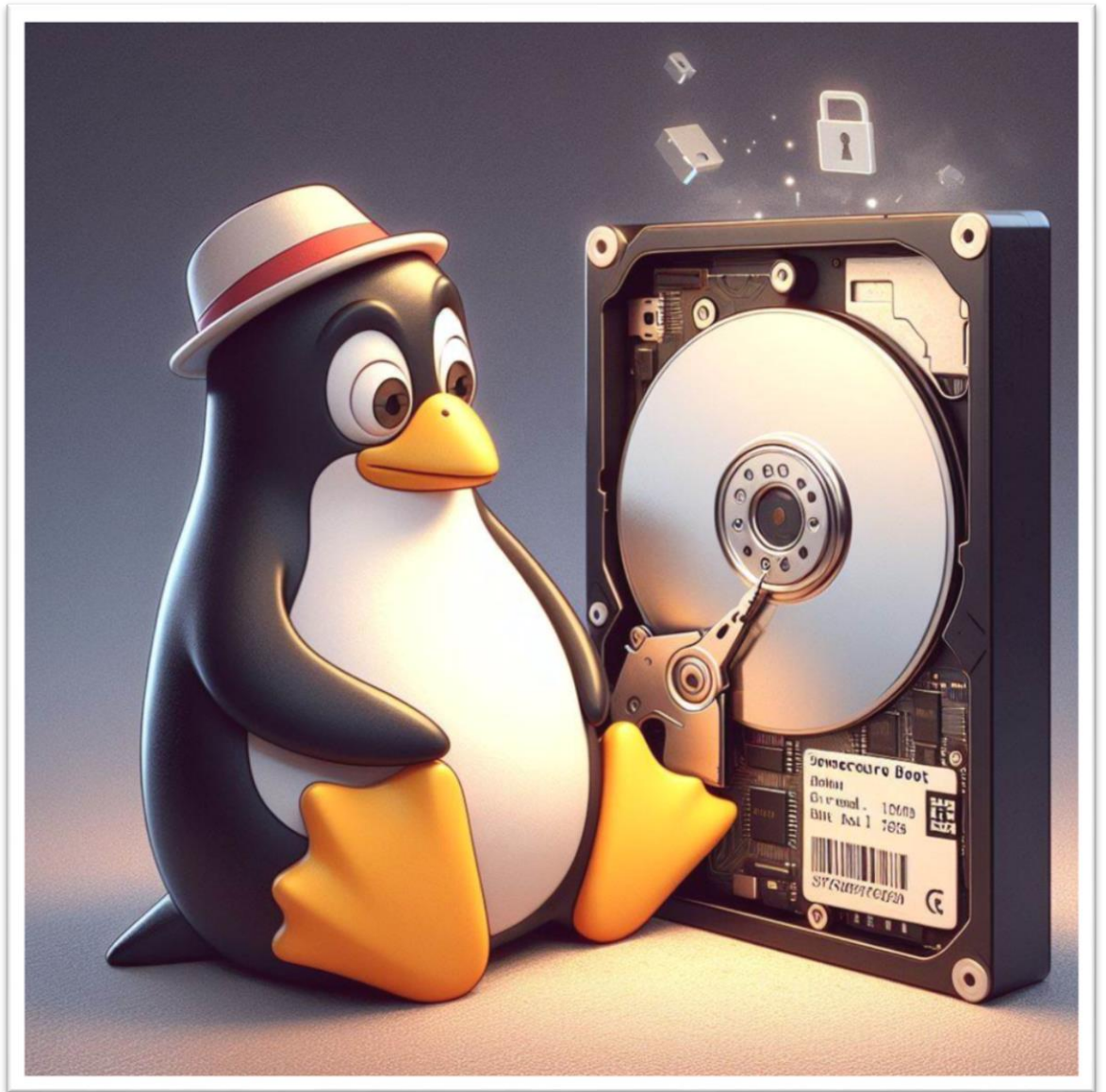


10 DE ABRIL DE 2024



ARRANQUE SEGURO CON GRUB

BASTIONADO DE SISTEMAS Y REDES

ERIC SERRANO MARÍN
I.E.S MARTINEZ MONTAÑES
CETI

Contenido

1. Introducción..... 2

2. Preparación del entorno..... 2

2.1 Vulnerabilidad de GRUB. 2

 Primera forma de acceder como root al sistema..... 2

 Segunda forma de acceder como root al sistema. 3

 Cambio de contraseña. 4

 Contraseñas de los usuarios. 4

3. Hardening de GRUB. 5

Ahora que está todo securizado, ¿están a salvo nuestros datos? ¿Por qué? ... 8

Conclusiones..... 8

1. Introducción.

GRUB es el gesto de arranque actual de los entornos Linux. Como hemos visto, para que no se convierta en una puerta trasera hacia nuestros sistemas necesitamos configurarlo correctamente. En esta actividad vamos a comprobar sus debilidades en caso de realizar una instalación por defecto y las medidas a tomar para hacerlo más seguro.

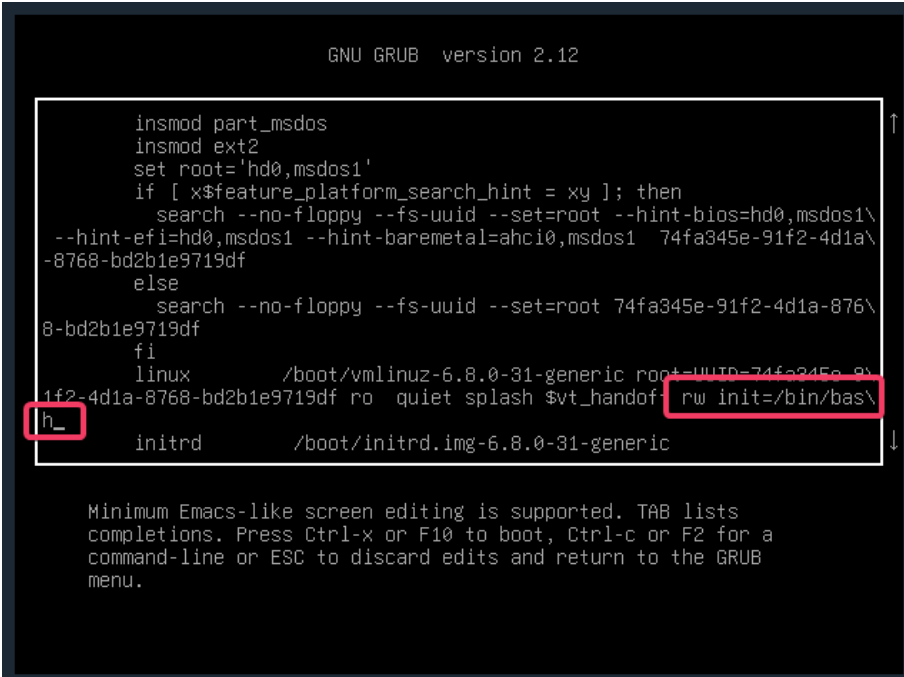
2. Preparación del entorno.

2.1 Vulnerabilidad de GRUB.

Grub tiene una consola integrada y permite visualizar el sistema de archivos. Extrae la password de los usuarios dados de alta en Ubuntu. Ahora arranca el sistema haciendo uso de la posibilidad de editar las opciones de arranque de Grub y cambia la contraseña de root. Una vez realizado esto prueba a acceder como root al sistema. Para esto, utiliza las dos técnicas vistas en clase. ¿Cómo podrías obtener el mismo resultado arrancando con un live CD? Pruébalo.

Dejaremos sostenido el shift cuando la máquina se esté encendiendo y después haremos clic en E.

Primera forma de acceder como root al sistema.



```
GNU GRUB version 2.12

insmod part_msdos
insmod ext2
set root='hd0,msdos1'
if [ x$feature_platform_search_hint = xy ]; then
  search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1\
--hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 74fa345e-91f2-4d1a\
-8768-bd2b1e9719df
else
  search --no-floppy --fs-uuid --set=root 74fa345e-91f2-4d1a-876\
8-bd2b1e9719df
fi
linux      /boot/vmlinuz-6.8.0-31-generic root=UUID=74fa345e-9\
1f2-4d1a-8768-bd2b1e9719df ro quiet splash $vt_handoff rw init=/bin/bas\
h_
initrd     /boot/initrd.img-6.8.0-31-generic


Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
command-line or ESC to discard edits and return to the GRUB
menu.
```

Añadir "rw init=/bin/bash" permitirá iniciar el sistema Ubuntu en modo de solo lectura con un shell bash como proceso inicial.

```
[ 5.117373] raid6: sse2x2   gen() 24005 MB/s
[ 5.149371] raid6: sse2x1   gen() 17715 MB/s
[ 5.152232] raid6: using algorithm sse2x2 gen() 24005 MB/s
[ 5.181264] raid6: .... xor() 13562 MB/s, rmw enabled
[ 5.183745] raid6: using ssse3x2 recovery algorithm
[ 5.187187] xor: measuring software checksum speed
[ 5.189941]   prefetch64-sse   : 27163 MB/sec
[ 5.192644]   generic_sse     : 19911 MB/sec
[ 5.194877] xor: using function: prefetch64-sse (27163 MB/sec)
[ 5.344878] Btrfs loaded, zoned=yes, fsverity=yes
Scanning for Btrfs filesystems
done.
Begin: Will now check root file system ... fsck from util-linux 2.39.3
[/usr/sbin/fsck.ext4 (1) -- /dev/sda1] fsck.ext4 -a -C0 /dev/sda1
lubuntu_2404: recovering journal
lubuntu_2404: clean, 282321/1036320 files, 1444385/4142505 blocks
done.
[ 5.626118] EXT4-fs (sda1): mounted filesystem 74fa345e-91f2-4d1a-8768-bd2b1e9719df r/w with ordered data mode. Quota mode: none.
done.
Begin: Running /scripts/local-bottom ... done.
Begin: Running /scripts/init-bottom ... done.
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/# _
```

Podemos observar cómo hemos entrado en una terminal root.

Segunda forma de acceder como root al sistema.



```
GNU GRUB  version 2.12

insmod part_msdos
insmod ext2
set root='hd0,msdos1'
if [ x$feature_platform_search_hint = xy ]; then
  search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1\
--hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 74fa345e-91f2-4d1a\
-8768-bd2b1e9719df
else
  search --no-floppy --fs-uuid --set=root 74fa345e-91f2-4d1a-876\
8-bd2b1e9719df
fi
linux      /boot/vmlinuz-6.8.0-31-generic root=UUID=74fa345e-9\
1f2-4d1a-8768-bd2b1e9719df rw single_ quiet splash $vt_handoff
initrd     /boot/initrd.img-6.8.0-31-generic

Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
command-line or ESC to discard edits and return to the GRUB
menu.
```

Añadiendo esto hará que el sistema arranque en modo lectura, escritura y en modo single user. El problema de esta forma es que nos está pidiendo la contraseña de root, por lo que no tendría mucho sentido ya que se supone que no sabemos la contraseña (en este caso si la sabemos).

```
rescue.service
[ OK ] Finished grub-initrd-fallback.service - GRUB failed boot detection.
[ OK ] Reached target rescue.target - Rescue Mode.
        Starting systemd-update-utmp-runlevel.service - Record Runlevel Change in UTMP...
[ OK ] Finished systemd-update-utmp-runlevel.service - Record Runlevel Change in UTMP.
You are in rescue mode. After logging in, type "journalctl -xb" to view
system logs, "systemctl reboot" to reboot, or "exit"
to continue bootup.
Contraseña de root para mantenimiento
(o pulse Control-D para continuar):
```

Cambio de contraseña.

Comando: passwd root

```
root@(none):/# passwd root
New password:
Retype new password:
passwd: password updated successfully
root@(none):/# _
```

Contraseñas de los usuarios.

Comando: cat /etc/shadow

```
syslog:!:19838:::::::
systemd-resolve:!:19838:::::::
uuidd:!:19838:::::::
usbmux:!:19838:::::::
tss:!:19838:::::::
kernoops:!:19838:::::::
whoopsie:!:19838:::::::
dnsmasq:!:19838:::::::
avahi:!:19838:::::::
tcpdump:!:19838:::::::
speech-dispatcher:!:19838:::::::
cups-pk-helper:!:19838:::::::
fwupd-refresh:!:19838:::::::
sddm:!:19838:::::::
saned:!:19838:::::::
geoclue:!:19838:::::::
cups-browsed:!:19838:::::::
hplip:!:19838:::::::
polkitd:!:19838:::::::
rtkit:!:19838:::::::
colord:!:19838:::::::
nm-openvpn:!:19838:::::::
ericsson:$y$j9T$PL/dskScqjbx1hQm1kX/e.$rhdb3Wol0Y7lvUq1dhC3tXVrSTqfYmuLEgl.MmlNmC8
:19839:0:99999:7:::
root@(none):/# _
```

3. Hardening de GRUB.

Visto lo visto, así no podemos dejar el sistema configurado. Ahora toca protegerlo. Para ello, vamos a hacer uso de una característica de GRUB que nos permite establecer una contraseña para poder modificar GRUB a la hora del arranque. Además, nos permitirá establecer qué usuarios pueden acceder a qué entradas del menú de arranque.

Para ello vamos a realizar las siguientes operaciones:

- Vamos a crear un superusuario en grub super con contraseña 12345.

Ahora nos vamos a ir a cambiar el fichero 00_header.

En el vamos a añadir las siguientes líneas:

- Cat << EOF: Inicia un bloque de texto que será pasado como entrada al comando cat.
- Set superusers="super": establece super como super usuario en grub.
- Password super 12345: asigna la contraseña 12345 al usuario super.
- EOF: marca el final del bloque de texto iniciado al principio.

```
450 cat << EOF
451 set superusers="super"
452 password super 12345
453 EOF
```

Ahora haremos un update a grub para que se realicen los cambios:

```
root@eric-virtualbox:/home/eric-sm/Desktop# update-grub
Sourcing file `/etc/default/grub'
Sourcing file `/etc/default/grub.d/lubuntu-grub-theme.cfg'
Generating grub configuration file ...
Found theme: /usr/share/grub/themes/lubuntu-grub-theme/theme.txt
Found linux image: /boot/vmlinuz-6.8.0-31-generic
Found initrd image: /boot/initrd.img-6.8.0-31-generic
Found memtest86+x64 image: /boot/memtest86+x64.bin
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.
Adding boot menu entry for UEFI Firmware Settings ...
done
```

Vamos a iniciar sesión en grub con super con contraseña 12345.

Gif del inicio de sesión: <https://i.imgur.com/6ZXvuZy.gif>

- Crearemos adicionalmente dos user1 con contraseña 11111 y user2 con contraseña 22222.

La creación de usuarios normales es parecida, solo que sobra la línea que dice superuser.

```
55 cat << EOF
56 password user1 11111
57 password user2 22222
58 EOF
59
```

Volvemos a hacer un update.

```
root@eric-virtualbox:/home/eric-sm/Desktop# update-grub
Sourcing file '/etc/default/grub'
Sourcing file '/etc/default/grub.d/lubuntu-grub-theme.cfg'
Generating grub configuration file ...
Found theme: /usr/share/grub/themes/lubuntu-grub-theme/theme.txt
Found linux image: /boot/vmlinuz-6.8.0-31-generic
Found initrd image: /boot/initrd.img-6.8.0-31-generic
Found memtest86+x64 image: /boot/memtest86+x64.bin
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.
Adding boot menu entry for UEFI Firmware Settings ...
done
```

- El arranque avanzado de Lubuntu sólo podrá ser ejecutado por super.

Para ello en el archivo 10_linux vamos a añadir --users super.

```
T1
echo "menuentry '$(echo "$title" | grub_quote)' --users super ${CLASS} \
$menuentry_id_option 'gnulinux-$version-$type-$boot_device_id' {" | sed "s/^/
$submenu_indentation/"
```

- Los test de memoria podrán lanzarlos tanto super como user1.

Añadiremos --users, super, user1 al archivo /etc/grub.d/20_memtest86+.

```
28 echo "menuentry '&(echo "$title" | grub_quote)' --users super,user1 ${CLASS} \
$menuentry_id_option 'gnulinux-$version-$type-$boot_device_id' {" | sed "s/^/
$submenu_indentation\"
```


- **Modifica la configuración para que haga uso de passwords encriptadas.**

El primer paso será usar el comando `grub-mdpasswd-pbkdf2` para encriptar la primera contraseña.

```
root@eric-virtualbox:/home/eric-sm/Desktop# grub-mkpasswd-pbkdf2
Introduzca la contraseña:
Reintroduzca la contraseña:
El hash PBKDF2 de su contraseña es grub.pbkdf2.sha512.10000.07C4C9500DF1A4D16CC17165F9F039B356989E10FB8CD931DFFB1
E2C20DE5B6D68C1B7C1E4F6A676540C03143F745F34E9CB6943D96908C515411CF2F187763B.CE0AEAC52EF37C455B9C42BE0F089405A518E
3FBB7CE665A393016E578E653C6EC12DFE7EA5F3115F4807E046FD86B5E0545FD73AB80159C8D48B3DB414782B5
root@eric-virtualbox:/home/eric-sm/Desktop#
```

Después vamos a copiarla y la vamos a añadir al archivo `00_header`. Hay que tener en cuenta que también habrá que cambiar “password” por `password_pbkdf2`.

```
0 cat << EOF
1 set superusers="super"
2 password_pbkdf2 super
   grub.pbkdf2.sha512.10000.07C4C9500DF1A4D16CC17165F9F039B356989E10FB8CD931DFFB1E2C20DE5B6D68C1B7C1E4F6A676540C03143F745F34E9CB6943D96908C5
3 EOF
```

Ya tendríamos la contraseña del usuario `super` encriptada.

Ahora vamos a hacer el mismo proceso con las demás.

```
0 cat << EOF
1 password_pbkdf2 user1
   grub.pbkdf2.sha512.10000.EC44C9C86B07BA4B3CEC43346E90DD0511FB3BAF7D8B0807E67CAA9C05645468660379C8FC5CE96A6982E2230EAD6B75797C55BD750079
   9BA0EFE1AF02EBFC74230BE8185B61E857FF03FAD1C5FD7272F0F47A946C8F202207935D9D40361CE3700AFEAC1445299E83C490823F15E0F864F9AF945F1DEA
2 password_pbkdf2 user2
   grub.pbkdf2.sha512.10000.81DF9C4AF901267FF63B6D45A12D20B6CF0F348E18177AAA9E1DAFC39FFCF38038E0AA5D142C916981E817DCE0E0AB4DD0D925CB3074D13
   77C403C961475C997DBA5717EA791729E51CC400BE63BC0378953E70AFA1308EB1FF481BD363040834807F4108A5219FFF15CEDDE69B394476052F8198B9909A
3 EOF
```

Y hacemos un update.

```
root@eric-virtualbox:/home/eric-sm/Desktop# update-grub
Sourcing file `/etc/default/grub'
Sourcing file `/etc/default/grub.d/lubuntu-grub-theme.cfg'
Generating grub configuration file ...
Found theme: /usr/share/grub/themes/lubuntu-grub-theme/theme.txt
Found linux image: /boot/vmlinuz-6.8.0-31-generic
Found initrd image: /boot/initrd.img-6.8.0-31-generic
Found memtest86+x64 image: /boot/memtest86+x64.bin
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.
Adding boot menu entry for UEFI Firmware Settings ...
done
root@eric-virtualbox:/home/eric-sm/Desktop#
```


Ahora que está todo securizado, ¿están a salvo nuestros datos?

¿Por qué?

No. Puedes seguir siendo vulnerable a un ataque, especialmente si alguien tiene acceso físico al dispositivo. Además, puede haber vulnerabilidades en el sistema operativo, también es importante tener en cuenta que aún es posible que un atacante eluda estas defensas con técnicas avanzadas, como vulnerabilidades utilizando ingeniería social o conocida para engañar a los usuarios. Ahora GRUB es más seguro, pero aún necesitamos administrar otras partes para mantener los datos protegidos.

Conclusiones

Esta práctica me ha permitido entender mejor la importancia de asegurar el gestor de arranque de GRUB, implementando medidas de seguridad, como establecer contraseñas encriptadas y restringir el acceso a ciertos usuarios y funciones del menú de arranque. Sin embargo, también he observado que estas medidas, aunque son importantes, no garantizan la protección completa.