

- **NOMBRE: Enrique Martínez Añón**
- **FECHA INICIO: 11-12-23**
- **FECHA FINAL: 17-12-23**
- **UNIDAD: U5 Seguretat Activa: Sistema Operatiu**
- **CASO PRÁCTICO: Activitat. Protege el GRUB**
- **ENUNCIADO: Protege el GRUB**
- **VERSIÓN ACTIVIDAD: A**
- **DIFICULTAD: BAJO**
- **TIEMPO ESTIMADO: 1:30**
- **TIEMPO REAL: 0:30**
- **CONCLUSIÓN:**

## **INDICE**

### **MOTIVOS PARA PROTEGER EL GRUB**

Hay gente que realmente se toma molestias para evitar accesos no autorizados a su ordenador a través de permisos de usuarios, de firewalls, de contraseñas, etc. A pesar de esto muchos de estos usuarios olvidan proteger el Grub. Si el Grub de nuestro equipo no está protegido cualquier usuario con un nivel medio/bajo puede realizar las siguientes acciones:

- Editando los parámetros del Grub es fácil acceder a nuestro ordenador como superusuario o usuario root. Si un atacante puede acceder a nuestro equipo como usuario root tendrá el control total del equipo y de la información almacenada en él.
- Sin necesidad de introducir ningún usuario ni contraseña un atacante puede abrir un intérprete de órdenes para intentar recabar información de nuestro equipo, para modificar configuraciones, etc.
- En el caso de tener el control sobre el Grub, podemos prevenir que ciertos usuarios puedan usar sistemas operativos inseguros, o sistemas operativos que simplemente no queremos que se usen.

En definitiva, si no protegemos el Grub, estaremos dejando un agujero de seguridad muy grande a la totalidad de personas que tengan acceso directo a nuestro ordenador. Este agujero de seguridad permitirá al atacante hacerse con el control absoluto de nuestro equipo de forma muy fácil y rápida.

## APARTADOS

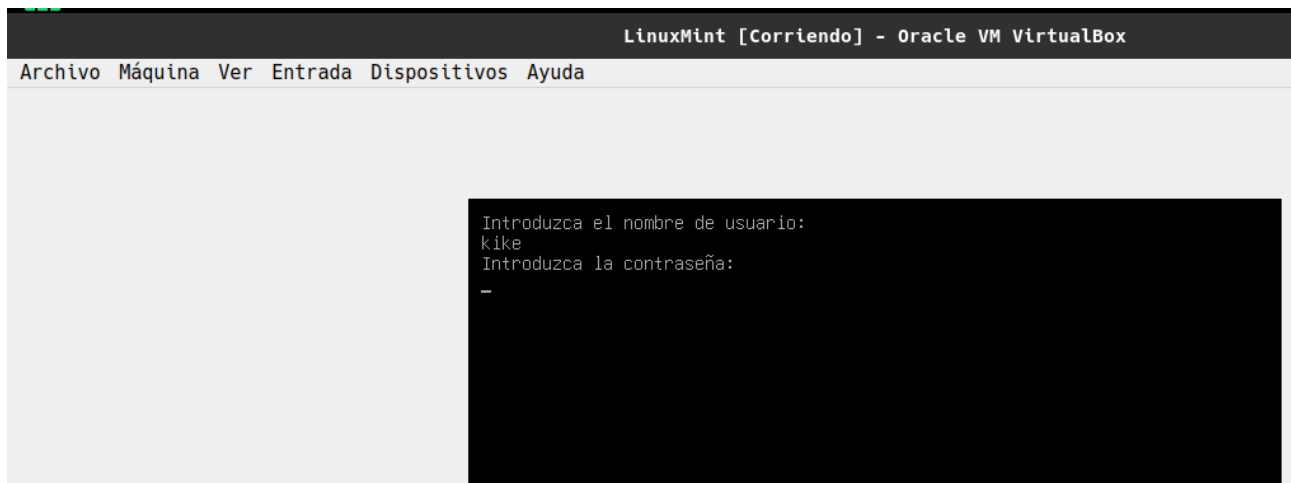
Protege una máquina virtual con ubuntu server. El modo de proteger el Grub será mediante una contraseña o password. Si aplicamos los pasos detallados en este apartado conseguiremos los siguientes resultados:

1. Bloquear el acceso a la línea de comandos del Grub.
2. Bloquear la posibilidad de edición de las entradas del Grub.
3. Bloquear la posibilidad de ejecución de todas las entradas del Grub.

```
LinuxMint [Corriendo] - Ora
Archivo Máquina Ver Entrada Dispositivos Ayuda
kike@kike-VirtualB
Archivo Editar Ver Buscar Terminal Ayuda
kike@kike-VirtualBox:~$ sudo cp /boot/grub/grub.cfg ~/grub.cfg.old
[sudo] contraseña para kike:
kike@kike-VirtualBox:~$ sudo cp /etc/grub.d/00_header ~/00_header.old
kike@kike-VirtualBox:~$ sudo cp /etc/grub.d/10_linux ~/10_linux.old
kike@kike-VirtualBox:~$ sudo cp /etc/grub.d/30_os-prober ~/30_os-prober.old
kike@kike-VirtualBox:~$
```

```
# Añadido por mi para modificar el grub
cat << EOF
set superusers="root,kike"
password pbkdf2 root grub.pbkdf2.sha512.10000.D8799A47CA137E3028EEB906C18B28DF9A5487C29138E7F4ACE201619E1B3463E18BA3A8DC45CE77135B5C2781848B98D3E834CA0C4400F5AFF5CCB5EB
01B81.FD506EC28BDE2188C2E22ADA011C5D393615E84F40754046AFDE942237FD5B7158B65CE70E5D1A922F9C48AC5A1E4F0AC3C1C95D0EE6AAF89B0B0B18EF515344
password pbkdf2 kike grub.pbkdf2.sha512.10000.D8799A47CA137E3028EEB906C18B28DF9A5487C29138E7F4ACE201619E1B3463E18BA3A8DC45CE77135B5C2781848B98D3E834CA0C4400F5AFF5CCB5EB
01B81.FD506EC28BDE2188C2E22ADA011C5D393615E84F40754046AFDE942237FD5B7158B65CE70E5D1A922F9C48AC5A1E4F0AC3C1C95D0EE6AAF89B0B0B18EF515344
EOF
kike@kike-VirtualBox:~$
```

```
kike@kike-VirtualBox:~$
kike@kike-VirtualBox:~$ sudo update-grub2
Sourcing file `/etc/default/grub'
Sourcing file `/etc/default/grub.d/50_linuxmint.cfg'
Sourcing file `/etc/default/grub.d/init-select.cfg'
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-5.15.0-88-generic
Found initrd image: /boot/initrd.img-5.15.0-88-generic
Found linux image: /boot/vmlinuz-5.15.0-76-generic
Found initrd image: /boot/initrd.img-5.15.0-76-generic
Warning: os-prober will be executed to detect other bootable partitions.
Its output will be used to detect bootable binaries on them and create new boot entries.
done
kike@kike-VirtualBox:~$
```



## BIBLIOGRAFIA

Tutorial proteger el grub: <https://geekland.eu/proteger-el-grub-con-contrasena/>