

# Taller BRS - Hardening GRUB - GNU/Linux

## ESCENARIO

### Máquina virtual:

Nome: Allow Boot GRUB HD

Tipo: Linux

Versión: Debian (64-bit)

RAM ≥ 2048MB

Orde de arranque: Óptica/Disco duro

CPU ≥ 2

PAE/NX habilitado

Almacenamento:

Unidade óptica(ISO): Debian Install amd64 DVD-1

Disco duro dinámico de 20GB

Rede: Soamente unha tarxeta activada en modo NAT

Xestor de arranque: GRUBv2

### Host Alumnado



**LIMITACIÓN DE RESPONSABILIDADE** O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

## 1. Realizar a práctica **1-Taller-BRS-Practica-Allow-Boot-GRUB-HD-GNU-Linux**

2. Arrancar co sistema operativo GNU/Linux instalado no disco duro.

3. Abrir sesión de usuario na contorna gráfica coas credenciais: **usuario/abc123**.

4. Abrir unha consola de comandos e executar:

\$ **su -** #Acceder á consola de root(administrador) a través do comando *su*, o cal solicita o contrasinal do usuario *root*. Escribir o contrasinal de *root* para acceder.

# **grub-mkpasswd-pbkdf2** #Crear un contrasinal para GRUB

Introduzca la contraseña:

Reintroduza la contraseña:

El hash PBKDF2 de su contraseña es grub.pbkdf2.sha512.10000.....

# **echo -e 'set superusers="hardeningGRUB"npasswd\_pbkdf2 hardeningGRUB contrasinal\_cifrado' >> /etc/grub.d/40\_custom** #Editar GRUB para que solicite o usuario *hardeningGRUB* (o cal non ten porque existir como usuario do sistema operativo, soamente é un usuario para a edición de GRUB) e o contrasinal xerado no comando anterior no arranque. Cambiar *contrasinal\_cifrado* polo *hash* calculado no comando anterior

# **tail -2 /etc/grub.d/40\_custom** #Ver os cambios efectuados co anterior comando en */etc/grub.d/40\_custom*

set superusers="hardeningGRUB"

passwd\_pbkdf2 hardeningGRUB grub.pbkdf2.sha512.10000.....

# **sed -i 's/CLASS="--class gnu-linux --class gnu --class os/& --unrestricted/' /etc/grub.d/10\_linux** #**IMPORTANTE:** Se non se pon a opción *--unrestricted* no arquivo *10\_linux* solicitarase usuario e contrasinal non soamente para a edición de GRUB senón tamén para o arranque do sistema operativo.

# **update-grub** Activar os cambios realizados a GRUB

# **init 6** Comando para enviar o runlevel (nivel de execución) do sistema operativo ao nivel 6, equivalente a reiniciar o sistema.

5. O xestor de arranque: **GRUB versión 2 ou GRUB 2** arranca por defecto na súa primeira opción en 5segundos. Entón, parar o arranque deste primeira opción premendo as teclas frechas abaixo ↓, arriba ↑.

6. Premer a tecla **e** (edit) para poder editar os parámetros de arranque do kernel.

- **OLLO!:** Lembrar que ao escribir o contrasinal en GRUB temos o teclado en americano e non en español.
- Agora para poder editar o xestor de arranque GRUB solicítase o usuario **hardeningGRUB** e o contrasinal configurado. Se non se introduce de forma correcta non se poderá acceder á edición do GRUB e voltarse ao menú de GRUB para elixir a opción de arranque.