

# Práctica2 Seguridade Informática

## Allow Boot GRUB disco duro - GNU/Linux



### ESCENARIO

#### Máquina virtual ou física:

RAM  $\leq$  2048MB CPU  $\leq$  2 PAE/NX habilitado

Sistema operativo instalado: GNU/Linux 64bits

BIOS: Arranque disco duro

Xestor de arranque: GRUBv2



**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.

### NOTAS:

- **Instalación:** A instalación do sistema operativo GNU/Linux realizouse escollendo método de particionado: Guiado, disco completo, configurar LVM, e co esquema de particionado: /home, /var e /tmp, é dicir, seguindo os pasos do instalador:

```
[!!] Particionado de discos

Este instalador puede guiarle en el particionado del disco (utilizando distintos esquemas estándar) o, si lo desea, puede hacerlo de forma manual. Si escoge el sistema de particionado guiado tendrá la oportunidad más adelante de revisar y adaptar los resultados.

Se le preguntará qué disco a utilizar si elige particionado guiado para un disco completo.

Método de particionado:

Guiado - utilizar todo el disco
Guiado - utilizar el disco completo y configurar LVM
Guiado - utilizar todo el disco y configurar LVM cifrado
Manual

<Retroceder>
```

```
[!] Particionado de discos

Seleccionado para particionar:

SCSI1 (0,0,0) (sda) - ATA VBOX HARDISK: 85.9 GB

Este disco puede particionarse siguiendo uno o varios de los diferentes esquemas disponibles. Si no está seguro, escoja el primero de ellos.

Esquema de particionado:

Todos los ficheros en una partición (recomendado para novatos)
Separar la partición /home
Separar particiones /home, /var y /tmp

<Retroceder>
```

```
[!!] Particionado de discos

Se escribirán en los discos todos los cambios indicados a continuación si continúa. Si no lo hace podrá hacer cambios manualmente.

Se han modificado las tablas de particiones de los siguientes dispositivos:
LVM VG debian-vg, LV home
LVM VG debian-vg, LV root
LVM VG debian-vg, LV swap_1
LVM VG debian-vg, LV tmp
LVM VG debian-vg, LV var
SCSI1 (0,0,0) (sda)

Se formatearán las siguientes particiones:
LVM VG debian-vg, LV home como ext4
LVM VG debian-vg, LV root como ext4
LVM VG debian-vg, LV swap_1 como intercambio
LVM VG debian-vg, LV tmp como ext4
LVM VG debian-vg, LV var como ext4
partición #1 de SCSI1 (0,0,0) (sda) como ext2

¿Desea escribir los cambios en los discos?


<Sí> <No>
```

- Táboa de particións msdos
- Unha partición primaria e unha lóxica:
  - Boot do sistema: /dev/sda1 (/boot). Formato: ext2
  - LVM: /dev/sda5 (Contén os volumes lóxicos). Formato: Linux LVM
- Nome de usuario: usuario
- Nome computador: usuario-pc
- Contraseñal: abc123. (Olla que o contraseñal ten un caracter punto final)
- GRUB en /dev/sda sen contraseñal

- **Apagado normal do sistema operativo:** Para un correcto funcionamento da práctica o sistema operativo GNU/Linux debe ser apagado sen inconsistencias evitando problemas no sistema de ficheiros ext4.

## Práctica

### Arrancar co sistema operativo GNU/Linux instalado no disco duro

1. O xestor de arranque:  **GRUB versión 2 ou GRUB 2** arranca por defecto na súa primeira opción en 5 segundos. Entón, parar o arranque deste primeira opción premendo as teclas frechas abaixo ↓, arriba ↑.
2. Seleccionar a primeira opción de arranque.
3. Premer a tecla **e** (edit) para poder editar os parámetros de arranque do kernel.
4. Moverse coa tecla frecha abaixo ↓ ata chegar á liña onde aparecen os parámetros **ro quiet splash**
5. Substituír os parámetros **ro quiet splash** polos parámetros **rw init=/bin/bash**, e premer as teclas **<Ctrl> + x**, é dicir, **^x**, para arrancar a opción escollida con novos parámetros do kernel. Agora no arranque veremos que non chegamos a arrancar o sistema operativo porque o primeiro proceso a chamar (init ou systemd) está modificado a /bin/bash, co cal en vez de facer unha chamada ao arranque do sistema operativo facemos unha chamada a unha consola de comandos, polo que, accedemos a unha consola onde temos permisos de root (administrador). **Ollo!: Non está cargado completamente o sistema operativo, pero si está recoñecido o hardware.**
6. Executar:

```
# mount #Amosar os sistemas de ficheiros montados, é dicir, os que está a usar e podemos empregar neste sistema operativo instalado.  
# cat /proc/cmdline #Amosar o contido de /proc/cmdline que parámetros cos cales o kernel foi arrancado.  
# passwd usuario #Modificar o contrasinal do usuario de nome usuario. Pór como contrasinal 1234. Repetir o contrasinal. Ollo: Non aparecen asteriscos nin outro tipo de caracteres para impedir saber cantos e cales caracteres estamos a escribir.  
# passwd root #Modificar o contrasinal do usuario root. Pór como contrasinal 1234. Repetir o contrasinal. Ollo: Non aparecen asteriscos nin outro tipo de caracteres para impedir saber cantos e cales caracteres estamos a escribir.  
# reboot -f #Reiniciar de forma forzosa.
```

### Deixar arrancar o sistema operativo GNU/Linux dende disco duro

7. Comprobar que agora o contrasinal do usuario de nome **usuario** foi modificada.
8. Comprobar que agora o contrasinal do usuario **root** foi modificada.

Ricardo Feijoo Costa



This work is licensed under a **Creative Commons Attribution-ShareAlike 4.0 International License**