

Práctica2 Seguridade Informática

Allow Boot dispositivo extraíble: CD/DVD/USB - GNU/Linux



ESCENARIO

Máquina virtual ou física:

RAM ≤ 2048MB CPU ≤ 2 PAE/NX habilitado

Sistema operativo instalado: GNU/Linux 64bits

ISO/CD/DVD/USB: Kali Live amd64

BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB



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?

<Si> <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: debian
- Contraseñal: abc123. (Olla que o contraseñal ten un caracter punto final)
- GRUB en /dev/sda sen contraseñal

■ Práctica chroot



Práctica

Arrancar co sistema operativo GNU/Linux instalado no disco duro

1. Na contorna gráfica abrir un terminal e executar:

```
usuario@debian:~$ su - #Acceder á consola de root(administrador) a través do comando su, o cal solicita o contrasinal do usuario root
```

```
root@debian:~# fdisk -l /dev/sda #Amosar a táboa de particións do disco /dev/sda
```

```
Disco /dev/sda: 80 GiB, 85899345920 bytes, 167772160 sectores
Modelo de disco: VBOX HARDDISK
Unidades: sectores de 1 * 512 = 512 bytes
Tamaño de sector (lógico/físico): 512 bytes / 512 bytes
Tamaño de E/S (mínimo/óptimo): 512 bytes / 512 bytes
Tipo de etiqueta de disco: dos
Identificador del disco: 0x00f71fcd
```

Disposit.	Inicio	Comienzo	Final	Sectores	Tamaño	Id	Tipo
/dev/sda1	*	2048	999423	997376	487M	83	Linux
/dev/sda2		1001470	167770111	166768642	79,5G	5	Extendida
/dev/sda5		1001472	167770111	166768640	79,5G	8e	Linux LVM

```
root@debian:~# mount | grep sda #Amosar os sistemas de ficheiros montados correspondentes ao patrón buscado: sda
```

```
/dev/sda1 on /boot type ext2 (rw,relatime)
```

```
root@debian:~# mount | grep debian #Amosar os sistemas de ficheiros montados correspondentes ao patrón buscado: debian
```

```
/dev/mapper/debian--vg-root on / type ext4 (rw,relatime,errors=remount-ro)
/dev/mapper/debian--vg-tmp on /tmp type ext4 (rw,relatime)
/dev/mapper/debian--vg-var on /var type ext4 (rw,relatime)
/dev/mapper/debian--vg-home on /home type ext4 (rw,relatime)
```



Práctica LVM2

- pvscan; vgscan; lvscan #Permiten escanear respectivamente: volumes físicos, grupos de volumes e volumes lóxicos existentes.
- pvdisplay; vgdisplay; lvdisplay #Amosa respectivamente información das propiedades dos volumes físicos, grupos de volumes e volumes lóxicos.
- pvs; vgs; lvs #Amosa respectivamente información resumida sobre volumes físicos, grupos de volumes e volumes lóxicos.

```
root@debian:~# pvscan #Amosar os volumes físicos recoñecidos no sistema.
```

```
PV /dev/sda5   VG debian-vg      lvm2 [ <79,52 GiB / 0    free]
Total: 1 [ <79,52 GiB] / in use: 1 [ <79,52 GiB] / in no VG: 0 [ 0    ]
```

```
root@debian:~# vgscan #Amosar os grupos de volumes recoñecidos no sistema.
```

```
Found volume group "debian-vg" using metadata type lvm2
```

```
root@debian:~# lvscan #Amosar os volumes lóxicos recoñecidos no sistema.
```

```
ACTIVE          '/dev/debian-vg/root' [15,05 GiB] inherit
ACTIVE          '/dev/debian-vg/var' [5,32 GiB] inherit
ACTIVE          '/dev/debian-vg/swap_1' [976,00 MiB] inherit
ACTIVE          '/dev/debian-vg/tmp' [992,00 MiB] inherit
ACTIVE          '/dev/debian-vg/home' [57,22 GiB] inherit
```

NOTA: Temos que ter en mente esta estrutura de particionamento para montala do mesmo xeito á hora de realizar a práctica a través de GRUB para o cambio de contrasinais.

```
root@debian:~# init 0 #Comando para enviar o runlevel (nivel de execución) do sistema operativo ao nivel 0, equivalente a apagar o sistema.
```

Arrancar coa Kali Live amd64

2. Na contorna gráfica abrir un terminal e executar:

```
$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
```

```
$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
```

```
# mount | grep sda #Amosar os sistemas de ficheiros montados correspondentes ao patrón buscado: sda. Neste caso non atopamos nada, é dicir, non temos montada /boot no sistema de ficheiros. Deberemos montala.
```

```
# mount | grep debian #Amosar os sistemas de ficheiros montados correspondentes ao patrón buscado: debian. Neste caso non atopamos nada, é dicir, non temos montado os volumes lóxicos /tmp, /var e /home dentro de /. Deberemos montar estes volumes.
```

```
# pvscan #Amosar os volumes físicos recoñecidos no sistema. Neste caso a saída é a mesma que se arrancamos por defecto dende disco duro o sistema operativo, é dicir, recoñecemos os mesmos volumes físicos.
```

```
PV /dev/sda5   VG debian-vg      lvm2 [<79,52 GiB / 0    free]
Total: 1 [<79,52 GiB] / in use: 1 [<79,52 GiB] / in no VG: 0 [0    ]
```

```
# vgscan #Amosar os grupos de volumes recoñecidos no sistema. Neste caso a saída é a mesma que se arrancamos por defecto dende disco duro o sistema operativo, é dicir, recoñecemos os mesmos grupos de volumes.
```

```
Found volume group "debian-vg" using metadata type lvm2
```

```
# lvscan #Amosar os volumes lóxicos recoñecidos no sistema. Neste caso a saída é a mesma que se arrancamos por defecto dende disco duro o sistema operativo, é dicir, recoñecemos os mesmos volumes lóxicos.
```

```
ACTIVE          '/dev/debian-vg/root' [15,05 GiB] inherit
ACTIVE          '/dev/debian-vg/var' [5,32 GiB] inherit
ACTIVE          '/dev/debian-vg/swap_1' [976,00 MiB] inherit
ACTIVE          '/dev/debian-vg/tmp' [992,00 MiB] inherit
ACTIVE          '/dev/debian-vg/home' [57,22 GiB] inherit
```

```
# ls -l /dev/mapper/debian* #Listar os volumes lóxicos recoñecidos no sistema. A opción -l permite listar por liña cada concurrencia atopada.
```

```
/dev/mapper/debian--vg-home
/dev/mapper/debian--vg-root
/dev/mapper/debian--vg-swap_1
/dev/mapper/debian--vg-tmp
/dev/mapper/debian--vg-var
```

```
# mkdir /mnt/recuperar #Crear o directorio /mnt/recuperar.
```

```
# mount -t auto /dev/mapper/debian--vg-root /mnt/recuperar #Montar o volume lóxico debian--vg-root no directorio /mnt/recuperar. Coa opción -t auto solicitamos ao comando mount a autodetección do sistema de ficheiros de montaxe.
```

```
# mount -t auto /dev/mapper/debian--vg-home /mnt/recuperar/home #Montar o volume lóxico debian--vg-home no directorio /mnt/recuperar/home. Coa opción -t auto solicitamos ao comando mount a autodetección do sistema de ficheiros de montaxe.
```

```
# mount -t auto /dev/mapper/debian--vg-var /mnt/recuperar/var #Montar o volume lóxico debian--vg-var no directorio /mnt/recuperar/var. Coa opción -t auto solicitamos ao comando mount a autodetección do sistema de ficheiros de montaxe.
```

```
# mount -t auto /dev/mapper/debian--vg-tmp /mnt/recuperar/tmp #Montar o volume lóxico debian--vg-var no directorio /mnt/recuperar/tmp. Coa opción -t auto solicitamos ao comando mount a autodetección do sistema de ficheiros de montaxe.
```

ls /dev/sda* #Listar os dispositivos de bloques /dev/sda recoñecidos no sistema.

/dev/sda /dev/sda1 /dev/sda2 /dev/sda5

mount -t auto /dev/sda1 /mnt/recuperar/boot #Montar a partición primaria /dev/sda1 no directorio /mnt/recuperar/boot. Coa opción -t auto solicitamos ao comando mount a autodetección do sistema de ficheiros de montaxe.

mount | tail -5 #Amosar as últimas 5 liñas da lista dos dispositivos montados.

```
/dev/mapper/debian--vg-root on /mnt/recuperar type ext4 (rw,relatime)
/dev/mapper/debian--vg-home on /mnt/recuperar/home type ext4 (rw,relatime)
/dev/mapper/debian--vg-var on /mnt/recuperar/var type ext4 (rw,relatime)
/dev/mapper/debian--vg-tmp on /mnt/recuperar/tmp type ext4 (rw,relatime)
/dev/sda1 on /mnt/recuperar/boot type ext2 (rw,relatime)
```

mount --bind /dev /mnt/recuperar/dev # Montar o cartafol /dev dentro de /mnt/recuperar/dev para poder ter acceso a todos os dispositivos recoñecidos pola distribución live.

A opción --bind permite facer uso do mesmo sistema de ficheiros en 2 lugares distintos. Por exemplo, /dev pode ser empregado en /dev e en /mnt/recuperar/dev

mount --bind /proc /mnt/recuperar/proc #Montar o cartafol /proc dentro de /mnt/recuperar/proc para poder ter acceso ao kernel grazas a distribución live.

mount --bind /sys /mnt/recuperar/sys #Montar o cartafol /sys dentro de /mnt/recuperar/sys para poder ter acceso ao kernel grazas a distribución live.

chroot /mnt/recuperar /bin/bash #Crear a xaula chroot. Con este comando creamos unha xaula: un entorno pechado para a distribución Linux dentro de recuperar, de tal xeito, que unha vez dentro da xaula soamente existe ésta, e dicir, soamente existe a distribución Linux instalada no disco duro /dev/sda a recuperar, xa non estamos traballando na Live.

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.

exit #Saír da xaula chroot para voltar á consola local do usuario root.

umount /mnt/recuperar/dev /mnt/recuperar/proc /mnt/recuperar/sys /mnt/recuperar/boot /mnt/recuperar/home /mnt/recuperar/var /mnt/recuperar/tmp /mnt/recuperar #Desmontar as unidades montadas.

init 0 #Comando para enviar o runlevel (nivel de execución) do sistema operativo ao nivel 0, equivalente a apagar o sistema.

Arrancar a máquina GNU/Linux sen o dispositivo extraíble conectado

\$ Comprobar que agora o contrasinal do usuario de nome **usuario** foi modificada.

\$ 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**