Title: Cifrar disco duro con luks Date: 2015-11-12 14:34 Modified: 2015-11-12 14:34 Category: Linux Tags: linux, consola, luks Slug: EncryptLuks Authors: procamora Summary: LUKS es un estándar para el encriptado de discos en Linux. A diferencia de otras soluciones, LUKS almacena la configuración necesaria en las cabecera de las particiones.

Introducción

LUKS es un estándar para el encriptado de discos en Linux. A diferencia de otras soluciones, LUKS almacena la configuración necesaria en las cabecera de las particiones, lo que nos permite llevarnos los discos a otro sistema fácilmente. Voy a detallar brevemente como preparar un disco encriptado con LUKS, utilizando Debian 6.

1) Instalar cryptsetup-luks

```
sudo apt-get install cryptsetup
```

Comprobar que nuestro kernel tiene cargado el módulo dm-crypt:

```
sudo lsmod | grep dm_crypt
```

Si no es así lo tendremos que cargar con modprobe. `modprobe dm-crypt`

2) Preparar disco En mi caso voy a utilizar un disco duro externo (sde), podemos ver que actualmente tiene una única partición:

```
sudo fdisk -l /dev/sde
```

```
Disco /dev/sde: 1500.3 GB, 1500301910016 bytes
255 heads, 63 sectors/track, 182401 cylinders
Units = cilindros of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000abcce

Disposit. Inicio    Comienzo      Fin      Bloques  Id  Sistema
/dev/sde1               1      182401  1465136001   83  Linux
```

Una buena práctica antes de encriptar un disco, sobre todo si este no es nuevo, es comprobar que funciona perfectamente y no tiene bloques erróneos. Para ello podemos usar la utilidad badblocks:

```
sudo badblocks -s -w /dev/sde1 -b 4096
```

Tener en cuenta que esta operación tarda varias horas.

3) Encriptar el filesystem

```
sudo cryptsetup luksFormat /dev/sde1
```

Nota: se ha de indicar YES en mayusculas.

Podemos comprobar la cabecera luck con:

```
sudo cryptsetup -v luksDump /dev/sde1
```

```
LUKS header information for /dev/sde1
Version:           1
Cipher name:       aes
Cipher mode:       cbc-essiv:sha256
Hash spec:         sha1
Payload offset:    2056
MK bits:           256
```

Al tratarse de un filesystem encriptado debemos mapearlo ya que no se puede leer directamente. En este ejemplo el sistema de ficheros lo mapeamos a CryptHome:

‘sudo cryptsetup luksOpen /dev/sde1 CryptHome

4) Formatear partición

```
sudo mkfs.ext3 /dev/mapper/CryptHome
sudo tune2fs -i 0 -c 0 /dev/mapper/CryptHome
```

5) Montar/desmontar volumen Para montar el volumen a mano:

```
sudo mkdir /mnt/CryptHome
sudo mount /dev/mapper/CryptHome /mnt/CryptHome
```

Y para desmontarlo:

```
sudo umount /mnt/CryptHome
sudo cryptsetup luksClose /dev/mapper/CryptHome
```

para montar la partición en un directorio (/home)

```
sudo vim /etc/fstab
```

/dev/mapper/CryptHome /home ext4 rw 0 0

Esto es para que se monte al inicio del equipo y pida la password

```
sudo vim /etc/crypttab
```

CryptHome /dev/sda6 none luks