

Tema XI Ejercicio III: Cifrado De Una Unidad En Linux

Nicolás A. Ortega Froysa

11 de mayo de 2022

Índice

1. Introducción	3
2. Cifrado con LUKS	3
2.1. Creación del Dispositivo Cifrado	3
2.2. Abrir el Dispositivo Cifrado y Formatear	4
3. Conclusión	5
4. Derechos de Autor y Licencia	6

1. Introducción

El cifrado de dispositivos en GNU/Linux se puede hacer de varias maneras. Es posible hacerlo a nivel de formato de sistema de archivos, que es un sistema bastante común con sistemas como ZFS. Quizá lo más popular ahora mismo es usar el sistema de LUKS. Esto permite formatear una partición de un dispositivo de forma que esté cifrado, y sobre esta partición cifrada se puede tratar como si fuese un dispositivo virtual.

2. Cifrado con LUKS

Para este documento vamos a asumir que el dispositivo que queremos cifrar se encuentra en `/dev/sdX`. Todas las operaciones se deben de hacer como *root*. **Por favor, asegúrese de usar el nombre real de tu dispositivo.**

2.1. Creación del Dispositivo Cifrado

Antes de crear el dispositivo cifrado, es necesario hacer una copia de los datos que se encuentran ya en él. Asegúrese de esto antes de continuar, y de desmontar el dispositivo.

A continuación vamos a reescribir todos los bloques de nuestro dispositivo a cero usando el comando `dd`. De este modo no será posible recuperar ningún dato que se encontraba antes en él. Esto lo hacemos corriendo el comando siguiente:

```
$ dd if=/dev/zero of=/dev/sdX bs=1M
```

Este proceso puede tardar mucho tiempo dependiendo del tamaño del dispositivo. Para más seguridad, es también aconsejable usar en vez de `/dev/zero` el archivo `/dev/urandom`, ya que éste en vez de reescribir con ceros, reescribirá con caracteres aleatorios.

Posteriormente ya podemos cifrar el dispositivo en sí. Primero tenemos que crear la partición que vamos a cifrar. Como el dispositivo entero lo hemos borrado, vamos a crear una partición que ocupe todo el disco. Esto se hace usando el comando `fdisk`:

```
$ fdisk /dev/sdX
```

Esto nos abrirá la consola de `fdisk`, donde introducimos los siguientes comandos:

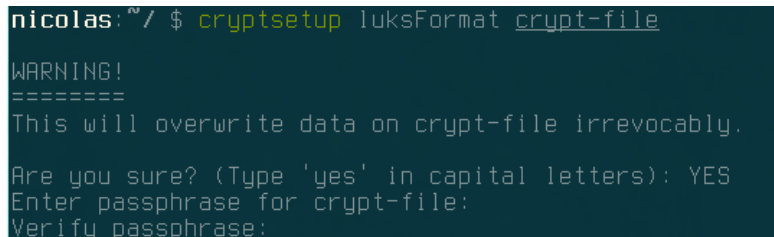
1. `n` para crear una partición nueva

2. `p` para designarla como partición primaria
3. `1` como número de partición (sale por defecto)
4. `Enter` para usar el sector primero que sale por defecto
5. `Enter` para usar el sector final que sale por defecto
6. `w` para guardar los cambios

Finalmente, ciframos el disco usando el comando `cryptsetup`. Esto se hace corriendo el comando siguiente:

```
$ cryptsetup luksFormat /dev/sdX
```

Este comando nos hará varias preguntas. En primer lugar nos preguntará si estamos seguros de hacer este procedimiento, ya que se perderán datos de manera irrecuperable. Como ya hemos hecho la copia, tenemos que meter **YES** (en mayúsculas). Después, nos pedirá introducir la contraseña que queremos usar, y verificar ésta. Cuando ya se introduce, tardará un rato en cifrar el dispositivo.



```
nicolas:~/ $ cryptsetup luksFormat crypt-file
WARNING!
=====
This will overwrite data on crypt-file irrevocably.
Are you sure? (Type 'yes' in capital letters): YES
Enter passphrase for crypt-file:
Verify passphrase:
```

Figura 1: Uso de `cryptsetup` en un archivo.

Ya se ha creado el dispositivo cifrado, pero aún tenemos que abrirlo y formatearlo para poder usarlo.

2.2. Abrir el Dispositivo Cifrado y Formatear

Abrir el dispositivo es también un proceso fácil: tan sólo hay que abrirlo especificando el nombre que quiere para el dispositivo virtual (en nuestro caso, `crypt-dev`).

```
$ cryptsetup luksOpen /dev/sdX crypt-dev
```

Ya se debería de encontrar nuestro dispositivo virtual en `/dev/mapper/crypt-dev`. Con esto se puede tratar como con cualquier otro dispositivo. En nuestro caso, vamos a formatearlo con formato EXT4 de forma siguiente:

```
$ mkfs.ext4 /dev/mapper/crypt-dev
```

Ahora ya sí que podemos acceder a `crypt-dev` como si fuese un dispositivo cualquiera. Cuando queremos cerrarlo para que no se pueda acceder, simplemente corremos el comando siguiente **después de haber desmontado el dispositivo virtual**:

```
$ cryptsetup luksClose crypt-dev
```

3. Conclusión

El cifrado con LUKS en GNU/Linux es bastante fácil. Facilita usar el dispositivo como un dispositivo normal virtual, y también permite cifrar una partición, dejando a otra sin cifrar. La verdad es que ya he tenido experiencia usando esta herramienta.^{1 2}

¹<https://themusicinnoise.net/blog/2017-02-20-parabola-with-lvm-on-luks.html>

²<https://themusicinnoise.net/blog/2017-02-21-encrypted-backup-drive.html>

4. Derechos de Autor y Licencia

Copyright © 2022 Nicolás A. Ortega Froysa <nicolas@ortegas.org>

Este documento se distribuye bajo los términos y condiciones de la licencia Creative Commons Attribution No Derivatives 4.0 International.