## Lab 10.2: Área de intercambio cifrada

En este ejercicio vamos a cifrar la **partición de intercambio**. La información escrita al dispositivo de intercambio puede contener información sensible. Debido a que el área de intercambio está sobre una partición, es importante considerar las implicancias de seguridad que tiene una partición de intercambio sin cifrar.

El proceso de cifrado es similar al del ejercicio previo, con la excepción de que no crearemos un sistema de archivos en este dispositivo de bloques cifrado.

En este caso vamos a usar el área de intercambio existente; primero la desactivaremos y luego formateada para el uso como área de intercambio cifrada. Podría ser un poco más seguro usar una partición nueva, o también usar la partición que creó en el ejercicio previo. Al final explicaremos qué hacer en caso de que tenga problemas para restablecer el sistema al punto original.

Vamos a discutir la administración del área de intercambio en un capítulo posterior, pero de todas formas mostraremos algunos comandos para trabajar con esta componente.

Una vez que haya terminado, puede volver a la partición original sin cifrar ejecutando el comando **mkswap** en el dispositivo.

1. Determine cuál es la partición que está usando actualmente para el área de intercambio y desactívela:

```
$ cat /proc/swaps
Filename                                Type            Size    Used    Priority
/dev/sda11                              partition       4193776 0       -1
$ sudo swapoff /dev/sda11
```

2. Realice los mismos pasos del ejercicio anterior para configurar el cifrado:

```
$ sudo cryptsetup luksFormat /dev/sda11  # may use --ciper aes option
$ sudo cryptsetup luksOpen   /dev/sda11  swapcrypt
```

3. Formatee el dispositivo cifrado para usarlo como área de intercambio:

```
$ sudo mkswap /dev/mapper/swapcrypt
```

4. Ahora active la partición y verifique si está funcionando:

```
$ sudo swapon /dev/mapper/swapcrypt
$ cat /proc/swaps
```

5. Para asegurarse que la partición de intercambio cifrada se active en el arranque, es necesario hacer dos cosas:

   (a) Agregue una línea a /etc/crypttab para que el sistema pregunte por la clave en el reinicio:

   ```
   swapcrypt  /dev/sda11   /dev/urandom  swap,cipher=aes-cbc-essiv:sha256,size=256
   ```

   (Note que /dev/urandom es preferido sobre /dev/random ya que podría estar relacionado a **entropy shortages, o problemas de rendimiento** como se lee en la página **man** de `crypttab`.)

   No es necesario que siga las opciones detalladas que siguen a continuación, pero las damos como ejemplo de lo que usted puede hacer.

   (b) Agregue una entrada al archivo `/etc/fstab` para que el dispositivo de aŕea de intercambio sea activado en el inicio.

   ```
   /dev/mapper/swapcrypt  none    swap    defaults    0 0
   ```

 

6. Reinicie y valide la configuración completa.

Para restaurar el sistema al punto original:

```
$ sudo swapoff /dev/mapper/swapcrypt
$ sudo cyyptsetup luksClose swapcrypt
$ sudo mkswap /dev/sda11
$ sudo swapon -a
```

Si el comando **swapon** falla, probablemente se debe a que el archivo /etc/fstab no describe adecuadamente la partición de intercambio. No hay ningún problema si la partición está descrita aquí por el dispositivo actual (/dev/sda11). Puede resolverlo al cambiar la línea a:

```
/dev/sda11  swap   swap  defaults 0 0
```

otra alternativa es asignarle una etiqueta al instante del formateo, como se muestra aquí:

```
$ sudo mkswap -L SWAP /dev/sda11
```

y luego agréguelo al archivo:

```
LABEL=SWAP  swap   swap  defaults 0 0
```

 