Exercise 10.2 Encrypted Swap

In this exercise, we will be encrypting the **swap partition**. Data written to the swap device can contain sensitive information. Because swap is backed by an actual partition, it is important to consider the security implications of having an unencrypted swap partition.

The process for encrypting is similar to the previous exercise, except we will not create a file system on the encrypted block device.

In this case, we are also going to use the existing swap device by first de-activating it and then formatting it for use as an encrypted swap device. It would be a little bit safer to use a fresh partition below, or you can safely reuse the encrypted partition you set up in the previous exercise. At the end we explain what to do if you have problems restoring.

(We will discuss swap management in a later chapter, but will show the few and easy commands for dealing with swap partitions here.)

You may want to revert back to the original unencrypted partition when we are done by just running **mkswap** on it again when it is not being used.

1. Find out what partition you are currently using for swap and then deactivate it:

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

2. Do the same steps as in the previous exercise to set up encryption:

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

3. Format the encrypted device to use with swap:

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

4. Now test to see if it actually works by activating it:

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

5. To ensure the encrypted swap partition can be activated at boot you need to do two things:

   (a) Add a line to `/etc/crypttab` so that the system prompts for the passphrase on reboot:

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

   (Note `/dev/urandom` is preferred over `/dev/random` for reasons involving potential **entropy shortages** as discussed in the **man** page for `crypttab`.) You don't need the detailed options that follow, but we give them as an example of what more you can do.

   (b) Add an entry to the `/etc/fstab` file so that the swap device is activated on boot.

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

6. You can validate the entire configuration by rebooting.

To restore your original unencrypted partition:

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

If the **swapon** command fails it is likely because `/etc/fstab` no longer properly describes the swap partition. If this partition is described in there by actual device node (`/dev/sda11`) there won't be a problem. You can fix either by changing the line in there to be:

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

or by giving a label when formatting and using it as in:

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

and then putting in the file:

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