Written by Admin
Sunday, 10 February 2013 18:22 - Last Updated Sunday, 10 February 2013 20:00

Linux encrypted swap-space

This guide will outline the basics of encrypting your swap-space in Linux; I'm using LInux Mint Maya in this example due to me ditching Ubuntu (sort of).

The benefits of having an encrypted swap-space are ones of security & plauseable deniability in the unfortunate event that your Linux machine fall into the wrong hands and someone tries to gain access to your important data; etc .... you get the Idea.

Here is a breakdown of the required steps to get your swap-space encrypted:

- Install the pre-requisites.
- Comment out the swap entry in your /etc/fstab file.
- Disable the swap-space (temporarily).
- Overwrite the swap partition with pseudo-random data.
- Add the cryptoswap entry to /etc/crypttab.
- Add a new entry in your /etc/fstab file for the encrypted swap-space.
- Verify.

Lets begin;

Linux encrypted swap-space

Written by Admin
Sunday, 10 February 2013 18:22 - Last Updated Sunday, 10 February 2013 20:00

Install the pre-requisites

Syntax: sudo apt-get install cryptsetup libpam-mount

Here we're installing the cryptsetup suite and the pam_mount library which is a pluggable authentication module to allow the mounting of volumes for a user session.

Comment out the swap entry in your /etc/fstab file

Syntax:

  sudo cp -p /etc/fstab /etc/fstab.bak ; sudo nano /etc/fstab

All we're doing here is taking a backup copy of our current /etc/fstab to /etc/fstab.bak then opening the /etc/fstab for editing; all as root (sudo).

In this file you see an entry similar to this:

  UUID=bc000b00-f00d-0a0a-0ce0-0ff0bb000ddd none   swap   sw   0   0

All we have to do here is insert a '#' at the beginning of this line, this will tell the mount process that this is a comment meaning that no action will be taken against this entry:

  #UUID=bc000b00-f00d-0a0a-0ce0-0ff0bb000ddd none   swap   sw   0   0

Disable swap-space (temporarily)

Linux encrypted swap-space

Written by Admin
Sunday, 10 February 2013 18:22 - Last Updated Sunday, 10 February 2013 20:00

Syntax:

  sudo swapoff /dev/sdxy

Where "/dev/sdxy" is the volume designation and partition number, you can get this from gParted if you are unsure (I'm not going to cover this here & besides if you need to encrypt your swap-space, I'd expect you to know what you're doing).

Make a note of the volume designation and partition number; we'll need it for the next few steps also.

Overwrite the swap partition with psuedo-random data

Syntax:

  sudo dd if=/dev/urandom of =/dev/sdxy bs=1M

Here we're overwriting the swap-space partition with pseudo-random data (further reading here: http://en.wikipedia.org/wiki//dev/random) if you're interested in the differences between /dev/random & /dev/urandom. You will need to change the value of "/dev/sdxy" based upon the configuration of your system.

Linux encrypted swap-space

Written by Admin
Sunday, 10 February 2013 18:22 - Last Updated Sunday, 10 February 2013 20:00

Add the cryptoswap entry to /dev/crypttab

Syntax:

  sudo gedit /etc/crypttab

Then we need to add the line:

  cryptoswap /dev/sdxy /dev/urandom
cipher=aes-cbc-essiv:sha256,size=256,hash=sha256,swap

Here we are telling the system that we want it to create an encrypted volume on "/dev/sdxy"
(change this to the correct information for your system).

Add a new entry in your /etc/fstab file for the encrypted swap-space

Syntax:

  sudo nano /etc/fstab

Add the following entry:

  /dev/mapper/cryptoswap none   swap   sw   0   0

Save the changes and reboot.

Linux encrypted swap-space

Written by Admin
Sunday, 10 February 2013 18:22 - Last Updated Sunday, 10 February 2013 20:00

Verify

All being well, you should have a system with an encrypted swap-space. To verify this issue the following command:

```
sudo cryptsetup status cryptoswap
```

You should see the following:

```
/dev/mapper/cryptoswap is active and is in use.
```

We're done.