Full disk encryption (devuan)

This is a quick summary of how to set up encryption during the installation of a Debian based system. It is actually not full disk, but full partition. It assumes you want a separate /, /home and swap, all encrypted. It uses LUKS and dm-crypt. For a detailed explanation, see https://xo.tc/full-disk-encryption-on-linux.html.

This is a summary of the excellent article at [https://xo.tc/setting-up-full-disk-encryption-on-debian-jessie.html]. I'm writing this more because he is very, very detailed with lots of pretty pictures, and I wanted a quick and dirty. Thus, if you want to "know" what you're doing, read his article. If you are pretty sure what you're doing and just want a recipe, use this.

- Figure out a good passphrase; something you'll remember (you'll type it everytime you boot), but is hard to crack (it secures all your data). I use https://xkpasswd.net/s/ to generate memorable but secure passphrases.
  - For very, very secure, use the default generator.
  - For less secure, but easier to remember, use the XKCD preset (when I do this, I set the SEPARATOR char to random).
- Do a base Devuan install. Should work for any Debian derivative.
- On partitioning scheme, create the following. NOTE
  - Partition 1, Primary, 256M, ext4, /boot
  - Partition 5, Logical, 10G, Physical volume for encryption
  - Partition 6, Logical, disk size minus 4G, Physical volume for encryption
  - Partition 7, Logical, 4G, do not use the partition
- Configure encrypted volumes
  - Create Encrypted Volumes
  - Select sda5 and 6 (/ and /home), then Continue, then Finish
- Enter the passphrase for both / and /home. Note that /home's password will be overridden later, so not critical
- Set sda5_crypt (the 10G one) as ext4, mount point /
- Set sda6_crypt (the big one) as ext5, mount point /home
- Done with partitioning, and select "no" when it complains about the lack of swap (we'll create it later)
- Finish installation as you like and reboot system
- Log in as root (or become root)
- Set up swap partition. This uses a random key generated at boot time, so each boot generates a new key. Following are the two commands to do that, adding a new line to /etc/crypttab and /etc/fstab
  - echo 'sda7_crypt /dev/sda7 /dev/urandom swap' » /etc/crypttab
  - echo '/dev/mapper/sda7_crypt none swap sw 0 0' » /etc/fstab
- Set it up so /home's partition actually uses a key (stored on /) with no passphrase. Again, the following are the commands from a prompt

```
mkdir /etc/keys
dd if=/dev/random of=/etc/keys/sda6.key bs=1 count=32 # create 32 byte key
chmod 400 /etc/keys/sda6.key
# add key file to /dev/sda6. When asked, use the key you created during
install
```

```
cryptsetup luksAddKey /dev/sda6 /etc/keys/sda6.key # add key to /home
# now, remove the key you used at install for sda6 (you'll be asked which to
to remove)
cryptsetup luksRemoveKey /dev/sda6
```

- edit /etc/crypttab, find sda6_crypt, change 'none' to /etc/keys/sda6.key

At this point, you should be able to reboot. You will be asked one time for the encryption key (the one for sda5, to be mounted on /). sda6 (mounted /home) should be decrypted automatically as soon as / is mounted and key can be found, and swap should also be mounted with a generated key.

Don't forget to Donate. The xkpasswd site is free, but they have to pay for hosting. Devuan is also free, but they have a **lot** of overhead. Donating to them ensures they are able to continue development of a systemd free Linux.