https://www.beuselinck.fr/article248.html

Mageia : chiffrer sa partition home avec veracrypt

- Linux -

Date de mise en ligne : lundi 24 décembre 2018

J'utilise un ordinateur portable sous Mageia 6 qui m'accompagne dans les transports en communs et au boulot. Le risque de vol n'est donc pas nul et j'ai décidé de chiffrer mes données personnelles pour ne pas retrouver les photos de mes vacances à Rocamadour en libre diffusion sur le net.

Après avoir testé le chiffrage de LA partition home à l'aide de dm-crypt (voir l'article correspondant), je réfléchissais à un moyen de chiffrer seulement SA partition home. En d'autres terrmes, au lieu de chiffrer /home, on chiffre /home/beuz et pas /home/guest ni /home/toto...

De plus, je souhaitais utiliser un outil de chiffrement multi-OS donc veracrypt (successeur de truecrypt).

Voici les 3 étapes pour y arriver :

1. installer veracrypt et le rendre utilisable par un utilisateur normal
2. créer une partition chiffrée et y poser le contenu du dossier /home/beuz
3. Au démarrage de session, demander la clef de chiffrement et monter la partition

1ère étape : Installlation de veracrypt

Nous nous rendons sur la page "downloads" du site officiel(en) et téléchargeons la dernière version pour linux [1] ou la version legacy si vous avez un vieil ordinateur à base de pentium 3 ou moins.
 On décompresse le fichier téléchargé et on exécute l'un des 4 fichiers ainsi décompressé (généralement, le fichier veracrypt-1.23-setup-gui-x64 , "gui" pour l'installateur graphique et "x64" pour la version linux 64 bits) .
 En ligne de commande, cela donnera ça :

```
tar xjvf  veracrypt-1.23-setup.tar.bz2
 ./veracrypt-1.23-setup-gui-x64
```

Ensuite, il faut qu'un utilisateur normal puisse utiliser veracrypt (par défaut, seul root a ce droit). J'ai choisi de créer un groupe "verahome", de lui donner les droits d'exécuter veracrypt et de faire appartenir mon utilisateur "beuz" à ce groupe. En console administrateur ça donnera ça :

```
groupadd verahome
 usermod -a -G verahome beuz
 echo "# allow group verahome to run veracrypt" >> /etc/sudoers
 echo "%verahome ALL=(root) NOPASSWD:/usr/bin/veracrypt" >> /etc/sudoers
```

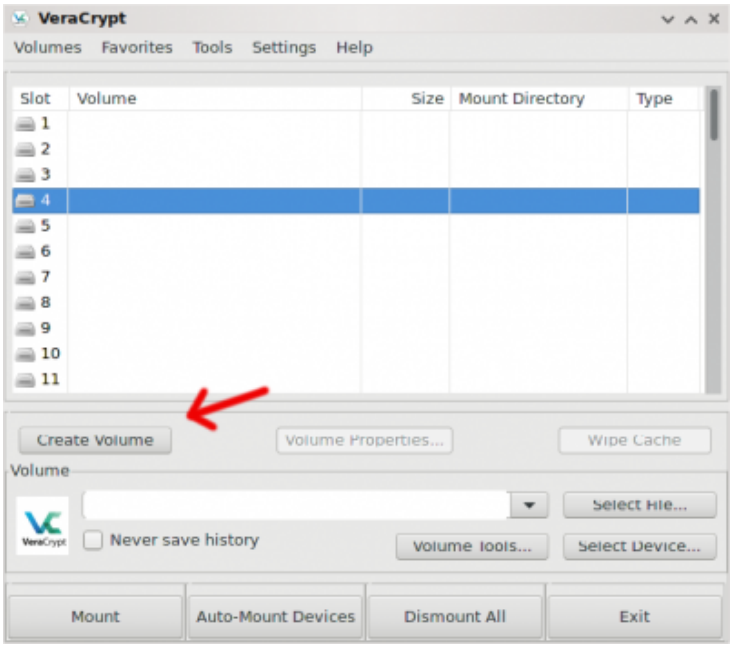
Attention au -G, le G doit être en majuscule. La version minuscule concerne le groupe principal et on ne veut surtout pas y toucher

Cela ne fonctionnera qu'au prochain démarrage de votre ordinateur mais avant cela nous allons effectuer l'étape suivante.

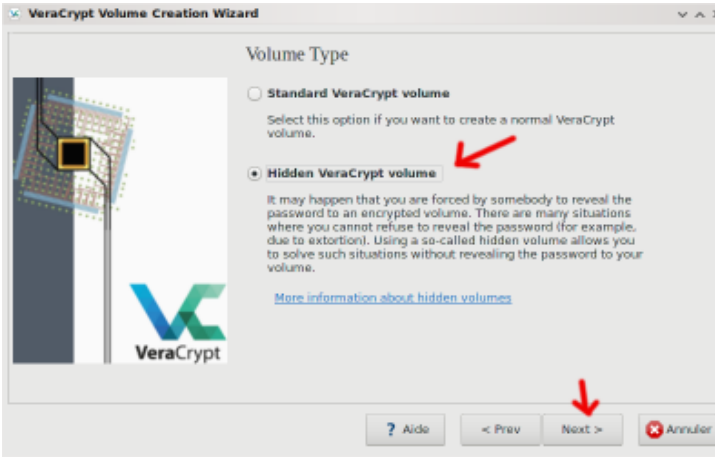
2ème étape : créer une partition chiffrée et y recopier le contenu de votre dossier personnel

Vous pouvez choisir de créer un conteneur "hidden", c'est-à-dire qu'on crée un premier conteneur normal dans lequel on cache un autre conteneur. Si vous tapez le mot de passe du conteneur normal, c'est celui-là qui s'ouvre et dedans vous mettez des fichiers persos sans intérêt pour un voleur. Par contre, si vous tapez le mot de passe du conteneur hidden, c'est ce dernier qui s'ouvre avec vos précieux fichiers. Cette option est destinée à leurrer un maitre-chanteur. S'il vous force à donner votre mot de passe, vous pourrez donner celui du conteneur normal, il aura l'illusion d'avoir obtenu le bon mot de passe.

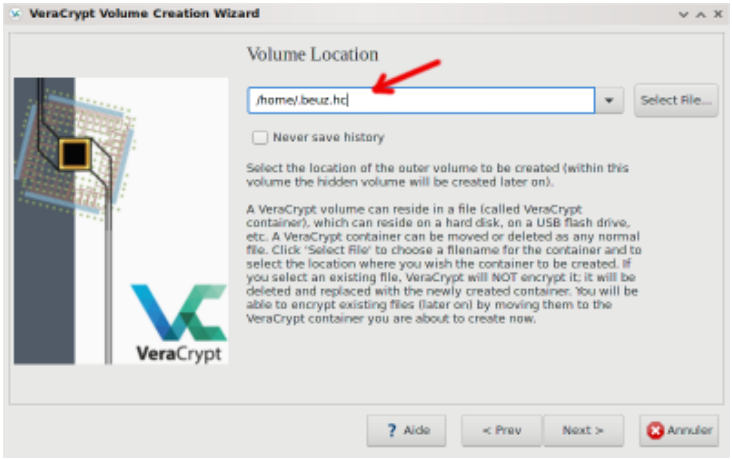
Lancez veracrypt dans une console administrateur et cliquez sur le bouton "Create volume".



Dans une série successive d'écrans, il vous est demandé de faire plusieurs choix.
Il vous est d'abord demandé si vous souhaitez créer un conteneur de type fichier ou de type partition. Nous laissons le choix "fichier" (create an encrypted file container) car nous n'avons pas de partition exclusivement dédiée à notre conteneur. Ensuite, on vous demande si vous voulez la double sécurité "hidden veracrypt volume" ou la sécurité simple "standard veracrypt volume".



J'ai donc choisi "hidden". La quatrième question est l'endroit où je vais stocker mon fichier-conteneur et sous quel nom. Je choisis /home/.beuz.hc . Il ne peut pas être dans /home/beuz puisqu'il finira par le remplacer. Le . avant beuz pour le cacher, le .hc pour me souvenir que c'est un hidden conteneur.

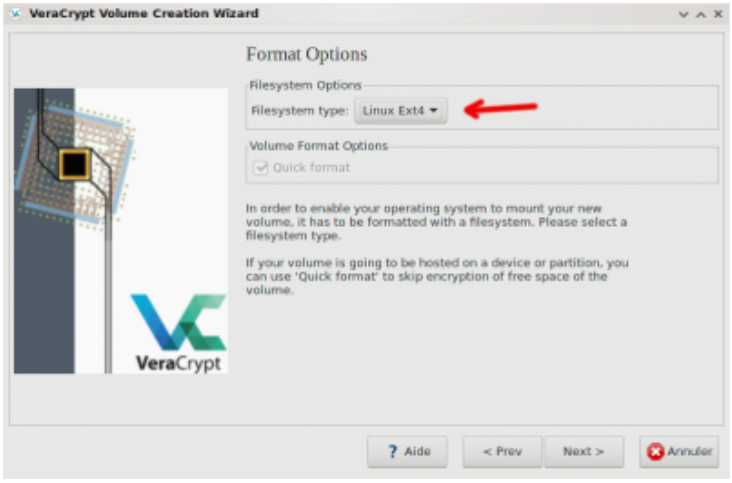


Ensuite, on passe à la création du conteneur "normal" celui destiné à leurrer mon maitre-chanteur. Dans veracrypt, il est désigné par le terme "outer". Je laisse les options par défaut de chiffrage puis je prête une attention toute particulière à la taille de mon conteneur. Il doit être suffisamment grand pour contenir à la fois le contenu actuel de mon home et à la fois le contenu du faux home, ainsi que de la place libre pour mes prochains fichiers. Donc très grand ! Par défaut, Veracrypt vous indique quelle place maximum il dispose en Gb (gigabyte) mais vous demande la taille Mb (megabyte). Ne vous trompez pas.. Ensuite, il vous faut choisir un mot de passe pour ce conteneur spécial maitre-chanteur. Vous pouvez par exemple mettre le même mot de passe que votre mot de passe de session puisque de toute façon, on suppose que votre maitre-chanteur vous l'a déjà extorqué.

Dans l'écran suivant, il vous est demandé de générer les clefs de cryptage en bougeant votre souris suffisamment longtemps avant de pouvoir cliquer sur le bouton "format". Une fois que c'est fait, i y a une opération très importante à faire : remplir le conteneur-leurre avec des fichiers sans intérêt *

On clique donc sur Open Outer Volume pour aller y coller nos fichiers sans importance et on y recopie également les dossiers .config et .local, les fichiers .bashrc .bash_completion .bash_profile .bash_logout .dmrc et .desktop (ou à minima le contenu de /etc/skel). Une fois que c'est fait, on peut cliquer sur "next" pour passer à la création du vrai espace caché "hidden".

Les mêmes questions seront posées avec les mêmes réponses. Attention toutefois, par défaut, la page "format options" vous propose un formatage en FAT32. Choisissez ext4.



Pour la partition Hidden, choisissez un mot de passe différent du mot de passe de session et différent du mot de passe "outer"

Il faut ensuite monter la partition hidden ainsi créée. Donc fermez l'assistant de création, si la partition apparait sur l'un des slots, démontez-là (c'est la partition "leurre" rappelez-vous) puis remonter-là en cliquant sur le bouton "mount" et cette fois, donnez le mot de passe de la partition "hidden". Une fois cellec-i monté, vous pouvez y recopier le contenu intégral de votre dossier personnel. En mode console :

```
cp -R /home/beuz/* /media/veracrypt1/
```

Plus tard, quand on aura vérifié le bon fonctionnement du conteneur hidden et qu'il contient bien tous nos fichiers, on supprimera de l'ancien /home/beuz les fichiers sensibles qui ne doivent plus être visibles de votre voleur/maitre-chanteur.

3ème étape : monter mon conteneur veracrypt à chaque session

Veracrypt est également utilisable en mode console et "scriptable". On va donc lancer le montage de la partition home chiffrée juste après le login de l'utilisateur. Il existe plusieurs méthodes (/etc/X11/gdm/PostLogin /etc/lxdm/Prelogin /etc/profile... J'ai choisi d'utiliser /etc/profile pour deux raisons, la première c'est qu'il n'est pas dans /home/beuz (que je cacherai avec le montage et la seconde est qu'il est indépendant du Display Manager).

J'ai donc ajouté à la fin de ce fichier les lignes suivantes :

```
cp $HOME/.Xauthority $TMPDIR/
 mount|grep -q $HOME
 if [ $? -eq 1 ]
 then
 echo "test $LOGNAME"
 if [ -f /home/.$LOGNAME.hc ]
 then
 LEPASS=`zenity --entry --text="Clef de $LOGNAME ?" --hide-text --title="VeraHome"`
 veracrypt -p=$LEPASS --mount /home/.$LOGNAME.hc $HOME
 cp $TMPDIR/.Xauthority $HOME/

 else
 echo "pas de fichier .hc"
```

```
fi
else
echo "$HOME déjà monté"
fi

rm -f $TMPDIR/.Xauthority
```

Quelques explications sur ces lignes :
 1- Au moment où je monte ma partition chiffrée , elle va recouvrir l'ancienne partition donc le jeton .Xauthority de session va disparaitre. C'est la raison pour laquelle vous voyez 3 lignes à ce sujet : Je mets le jeton dans un dossier temporaire, je monte ma partition, j'y colle le jeton et je l'efface du dossier temporaire.
 2- Je fais deux tests essentiels : est-ce qu'il y a bien un conteneur au nom de l'utilisateur et est-ce qu'il n'est pas déjà monté ?
 3- Je demande le mot de passe avec Zenity et je monte la partition chiffrée pour recouvrir l'ancienne partition

Voilà, il est temps de redémarrer l'ordinateur pour tester tout ça...

Après s'est connecté, une nouvelle fenêtre fait son apparition au démarrage "Clef de beuz ?"
 3 solutions s'offrent à moi :

- Je mets le mot de passe du conteneur chiffré et je peux travailler sur mes fichiers secrets
- Je mets le mot de passe du conteneur "outer" et mon voleur pense que c'est le bon puisque ça marche mais il ne verra pas mes fichiers secrets
- Je mets un mauvais mot de passe ou j'annule et je travaille alors sur mon ancien dossier personnel non chiffré.

A faire ultérieurement (quand vous serez certain que la partition chiffrée fonctionne bien) : supprimer les fichiers sensibles du dossier personnel non chiffré.

Améliorations à apporter : à la déconnexion, démonter le conteneur chiffré. Si le mot de passe est vide, ne pas lancer la tentative de montage.

Post-scriptum :

J'ai tenté de faire un script qui effectue toutes ces opérations. Vous pouvez le télécharger ci-dessous. Vous avez LE DEVOIR de le vérifier avant de l'exécuter. Enfin, vous êtes invité à l'améliorer et à en faire profiter tout le monde (utilisez par exemple les commentaires sur cet article).

---

[1] La version 1.19 existe dans les dépôts mageia 6 mais elle est ancienne et semble bugguer sur les conteneur "hidden". Mageia 7 contient bien la version 1.23.

