[Forensic] Récupération de masterkey LUKS dans la ram

Introduction

Cette page présente une méthode pour obtenir une clé de récupération d'une partition chiffrée LUKS (systèmes Linux) à partir de la RAM.

Manuel

Tout d'abord utilisez aeskeyfind pour extraire toutes les clés AES 128 et 256 de l'image de la ram :

```
aeskeyfind 'Kali_5.18.0-kali5-amd64.dmp' > all-aes-keys.txt
```

> Retirez les clés AES 128 bits car seules les clés AES 256 bits sont intéressantes (juxtaposition de deux clés 256 pour faire une clé 512 qui correspond à la taille d'une clé LUKS).

Inversez le sens des clés :

```
tac 'all-aes-keys.txt' | tr -d "\n" | fold -w 128 > KEYS.txt
```

Mettez chaque combinaison de clés dans un fichier MK (MasterKey) :

```
k=1 ; while read i ; do echo $i | xxd -r -p > ./MK$k ; k=$(($k+1)); done < KEYS.txt
```

Testez chaque possible MasterKey sur la partition chiffrée :

```
for i in MK* ; do sudo cryptsetup luksAddKey --master-key-file=$i /dev/loop0p3 ; done
```

> Vous pouvez **echo MK$i** pour afficher le fichier testé.

Puis déverrouillez la partition :

```
sudo cryptsetup luksOpen /dev/loop0p3 BIM
```

Revision #2
Created 2025-03-12 13:26:40 UTC by Elieroc
Updated 2025-03-12 14:15:26 UTC by Elieroc