Université Clermont Auvergne

Direction Opérationnelle des Systèmes d'Information – Pôle proximité

Déchiffrer un disque Bitlocker à l'aide de Kali-Linux.

Avant-propos : L'objectif de ce document est de permettre à un administrateur système et réseau de lire le contenu d'un disque chiffré avec Bitlocker, sous Linux et à des fins de récupération de données.

Ce document est valable pour Kali-Linux en mode « live forensic ». Il ne décrit pas la création du live-usb. Il ne décrit pas non plus la procédure sur d'autres distributions de Linux, même si le fonctionnement doit globalement être le même.

On suppose que le disque à déchiffrer est /dev/sda3.

Etape 1 : Installer le logiciel « dislocker ».

apt-get install dislocker

Etape 2 : Créer les dossiers de travail dans /mnt

mkdir /mnt/dislocker

mkdir /mnt/decrypted

Etape 3 : Déchiffrer le disque dans un fichier afin de pouvoir le monter par la suite :

dislocker-fuse -V /dev/sda3 -u /mnt/dislocker

dislocker-fuse [-hqrsv] [-l LOG_FILE] [-O OFFSET] [-V VOLUME DECRYPTMETHOD -F[N]] [-- ARGS…]

DECRYPTMETHOD = -p[RECOVERY_PASSWORD] | -f BEK_FILE | -u[USER_PASSWORD] | -k FVEK_FILE

Ici, le système demande le mot de passe utilisateur à cause du paramètre -u. S vous ne connaissez pas la mot de passe, le paramètre -p vous permet d'utiliser la clef de recouvrement que vous devriez avoir stocké en sureté.

Un fichier « dislocker-file » est créé dans /mnt/dislocker.

Etape 4 : Il faut « monter » ce fichier dans /mnt/decrypted

mount /mnt/dislocker/dislocker-file /mnt/decrypted

Etape 5 : On liste le contenu de /mnt/decrypted :

ls -lah /mnt/decrypted

Vous avez désormais accès au contenu du disque chiffré Bitlocker.