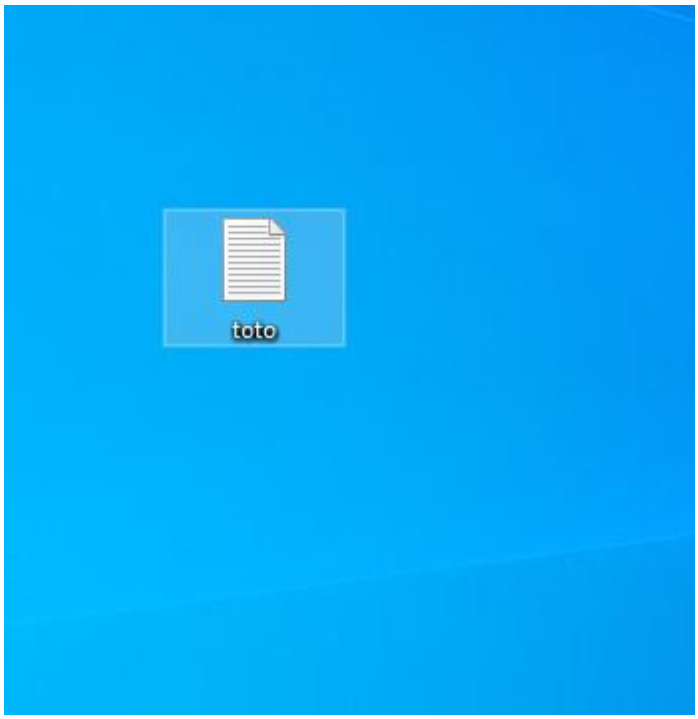
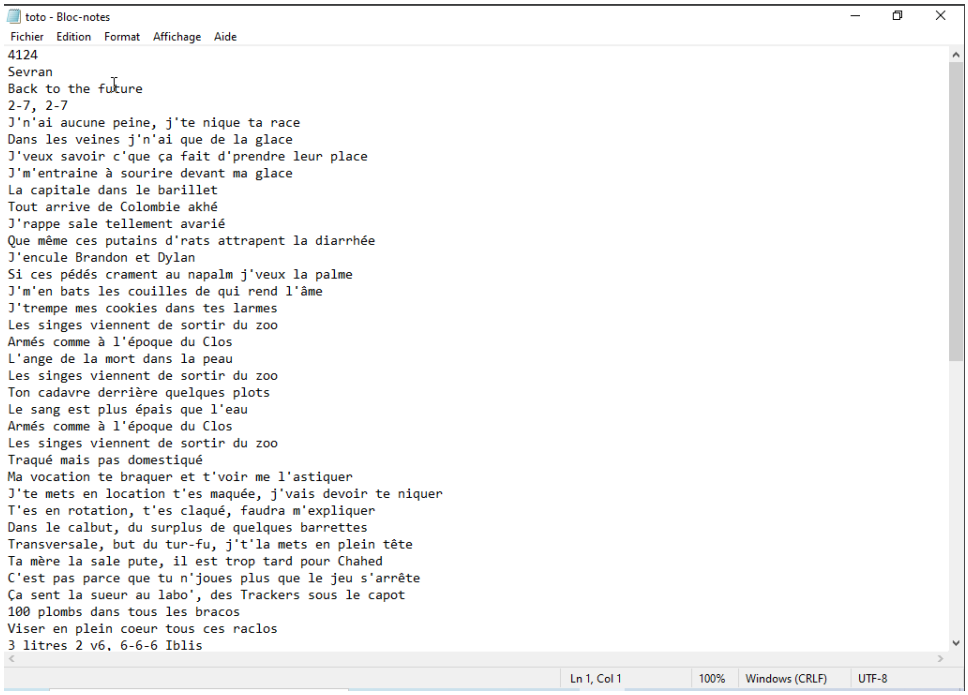
TP Intrusion simple Windows

Créez un fichier « toto.txt » sur le bureau.



Insérez-y les paroles de votre chanson préférée, pour mon cas c'est Zoo de Kaaris.

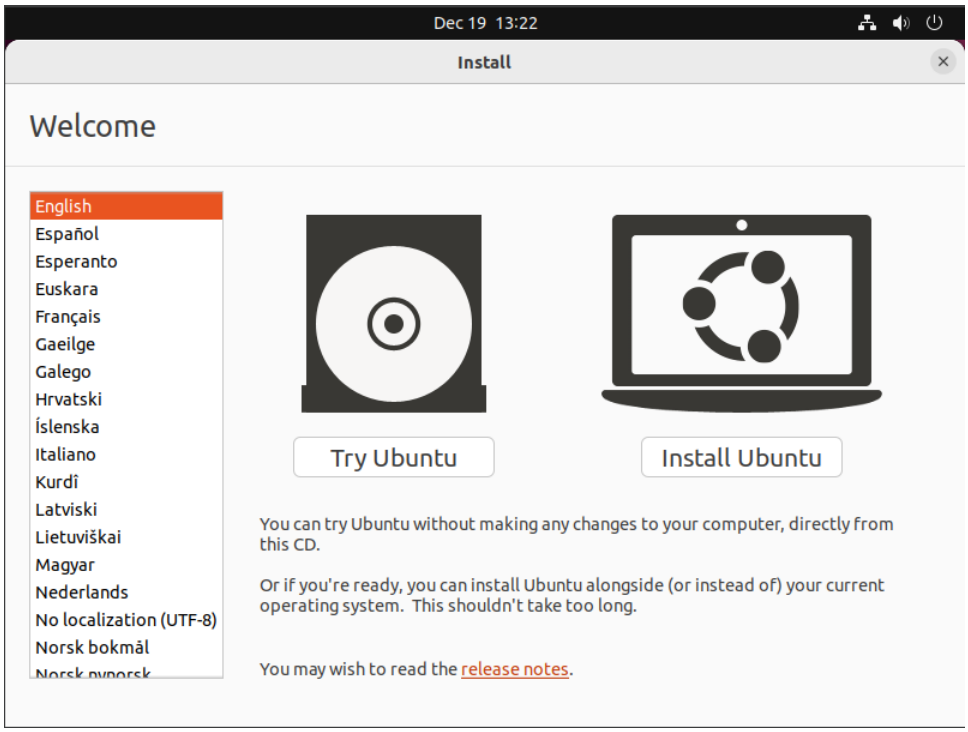


Eteignez votre VM.

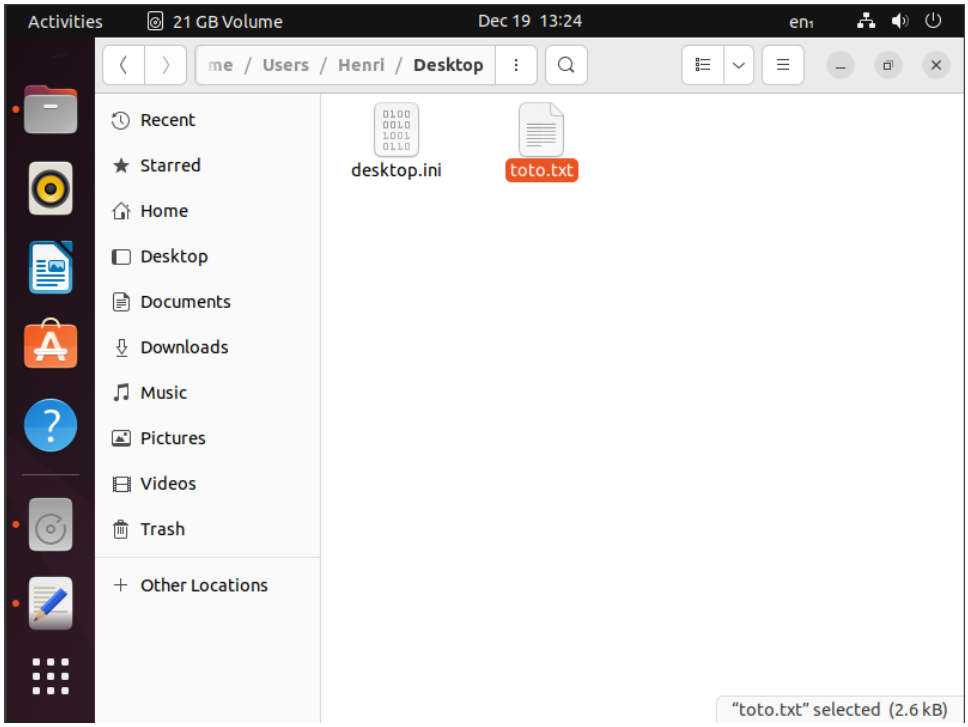
Bootez sur votre VM mais en utilisant une ISO de Ubuntu Desktop cette fois.

[Voici le tuto pour installer un iso sur votre VM]

Démarrez en mode live-DVD (« Essayer Ubuntu »)

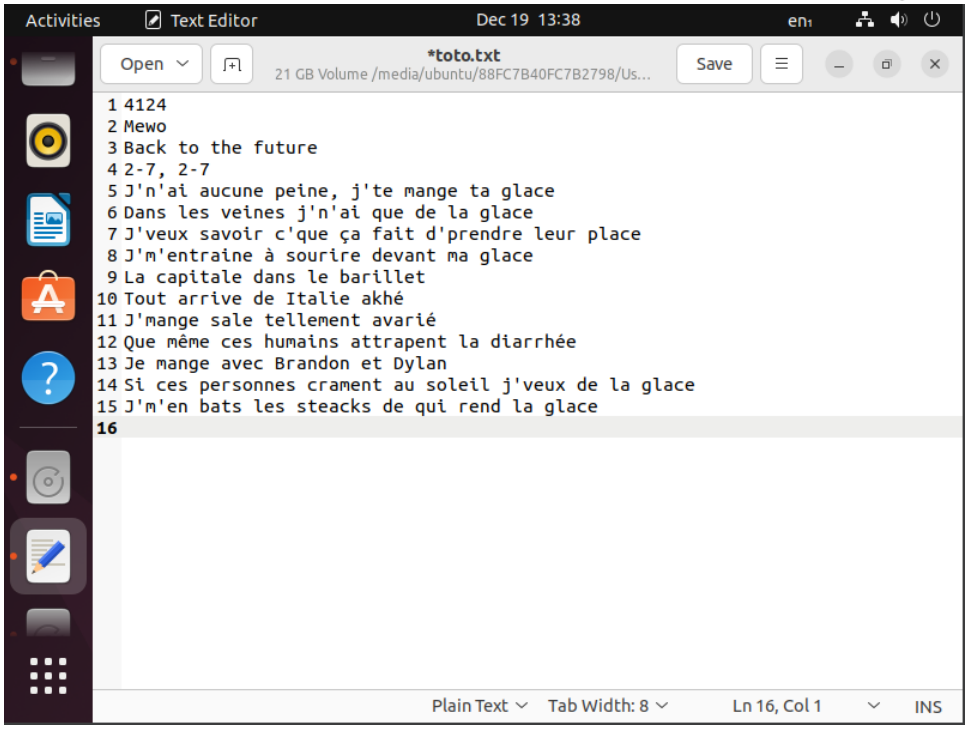


Tentez d’accéder au fichier « toto.txt ».



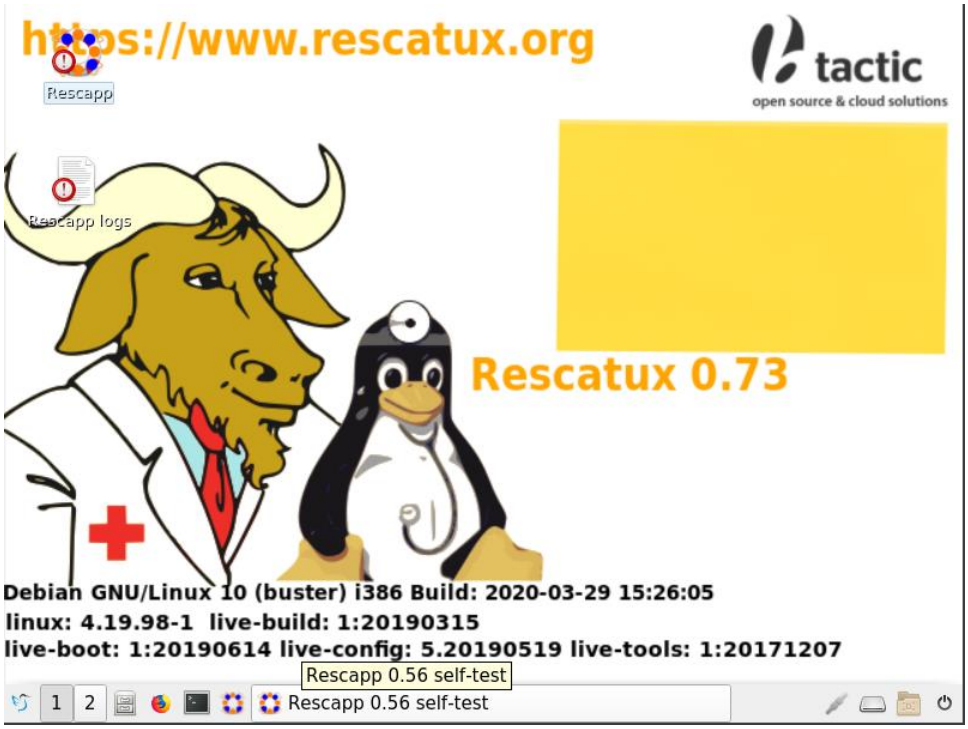
Est-ce possible de lire le fichier ? Est-il possible de modifier le ficher ?

Oui c’est possible de lire et de modifier comme ici j’ai modifié les insultes 😊

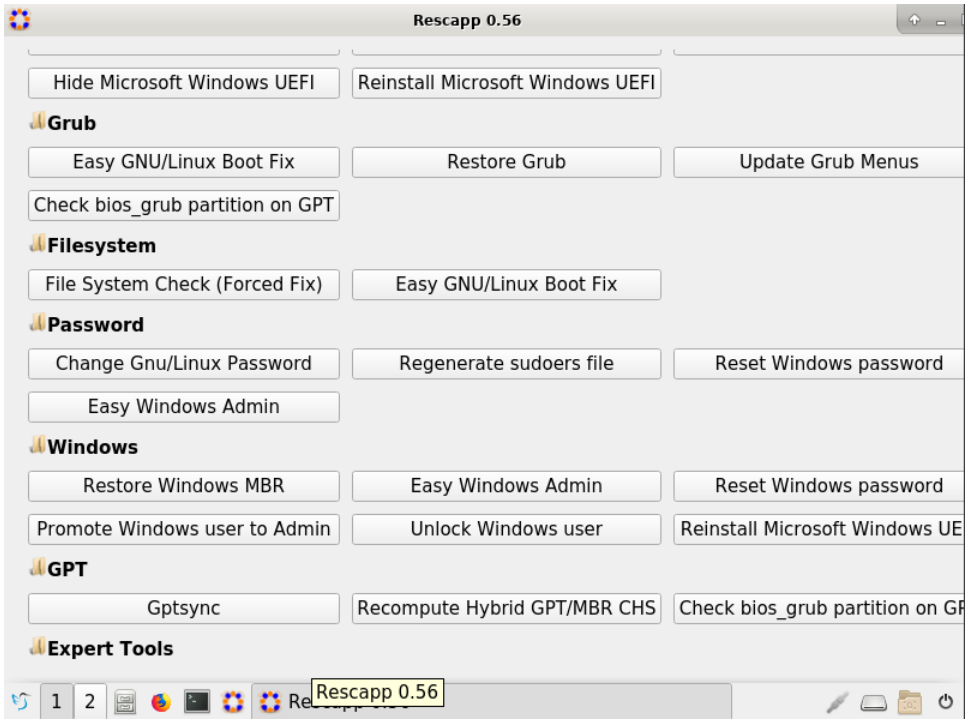


Méthode avec Rescatux :

Installer l'iso Rescatux et booter avec une clé sur votre machine

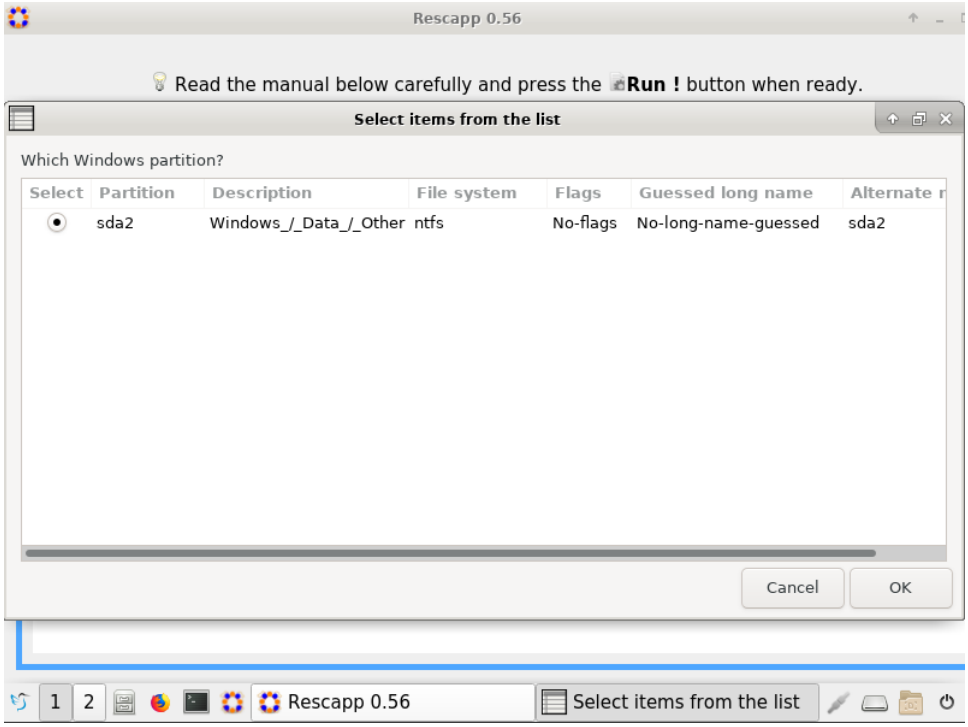


Lancez rescapp et sélectionnez "Reset Windows password" dans le groupe windows

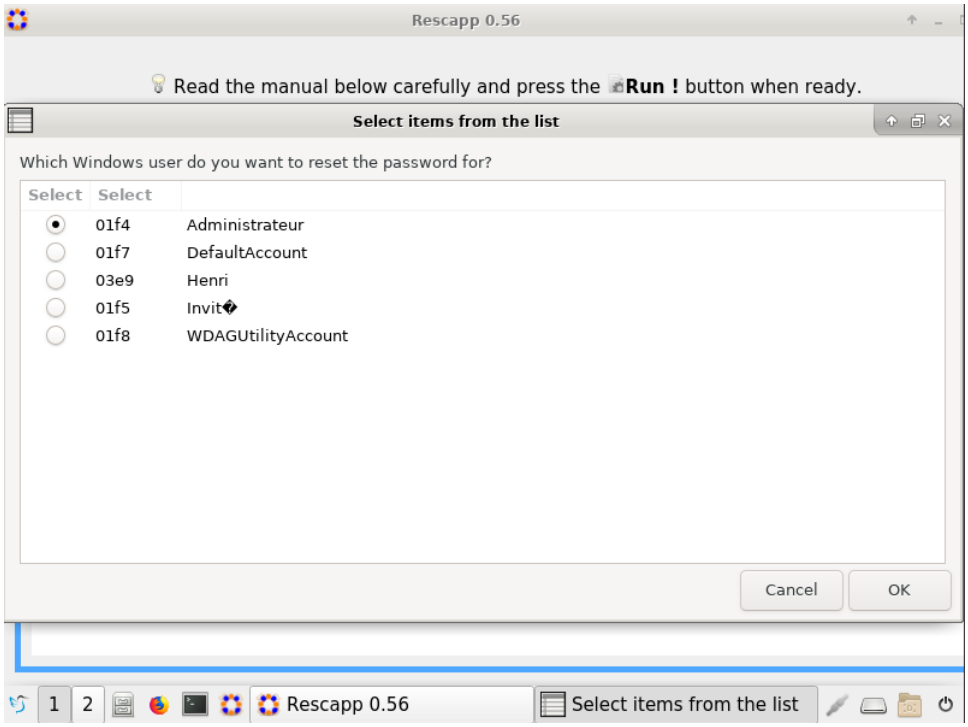


Cliquez sur “RUN”

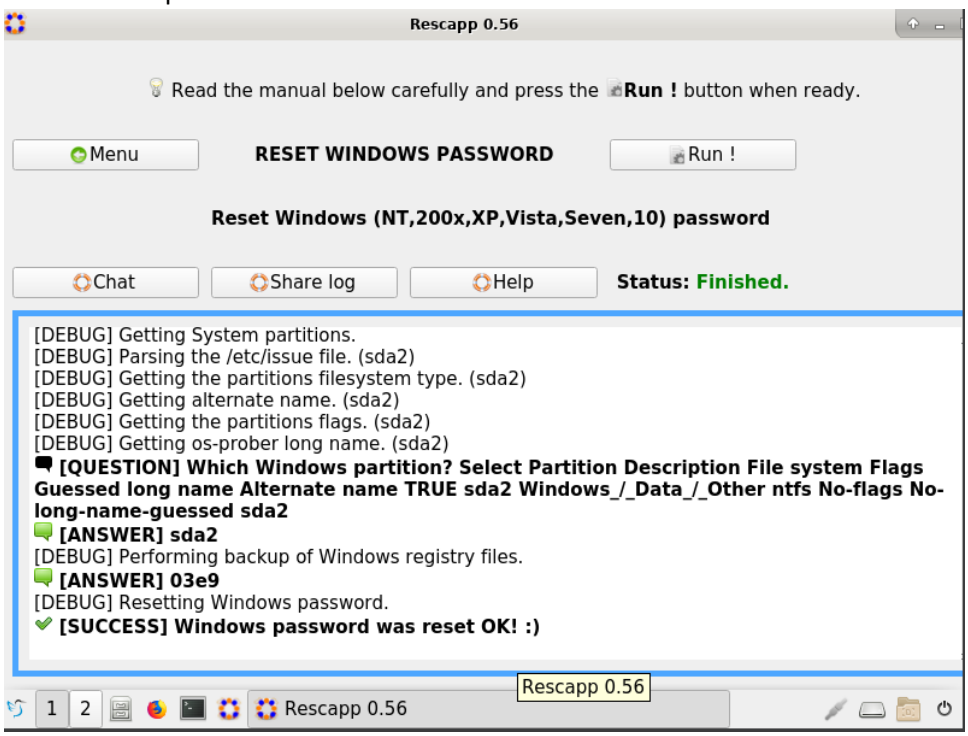
Sélectionnez le fichier sda2



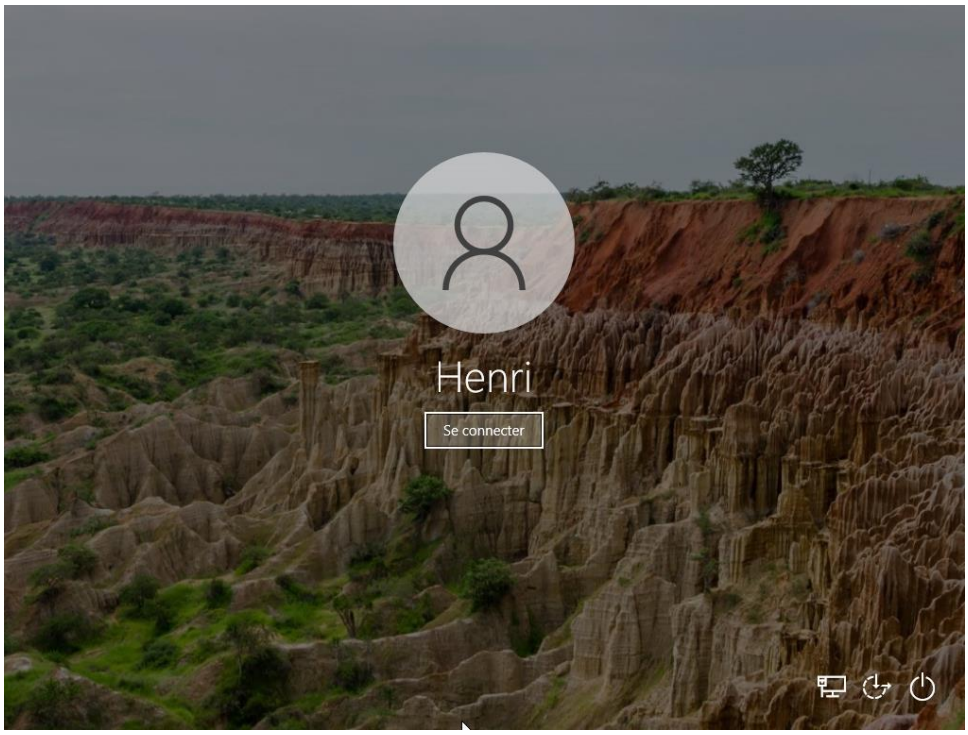
Choisissez le bon profile



Et voilà le mdp a été reset !



Voilà la preuve...



Quelle méthode s'approche le plus de la vidéo évoquée en introduction ?

La méthode d'approchant le plus de la vidéo et la méthode n2 avec Utilman, celle qui permet d'avoir accès au cmd.

Pensez-vous qu'on a le même souci sur Mac ou Linux ?

Oui ça fonctionne

Déterminez deux manières de se protéger de ce problème :

Étant donné que BitLocker est conçu pour protéger les ordinateurs contre de nombreuses attaques, il existe de nombreuses raisons pour lesquelles BitLocker peut démarrer en mode de récupération. Par exemple :

- Modification de l'ordre de démarrage du BIOS pour démarrer un autre lecteur avant le disque dur
- Ajout ou suppression de matériel, comme l'insertion d'une nouvelle carte dans l'ordinateur
- Retrait, insertion ou épuisement complet de la charge sur une batterie intelligente sur un ordinateur portable (source : Microsoft)