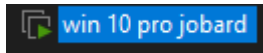


TP Intrusion Windows

1. Création de la VM



2. Création d'un mot de passe simple (mdp)
3. Création du fichier toto à récupérer via le Ubuntu plus tard. Il contient les paroles d'une des meilleures musique jamais produite (Devil in a new Dress par Kanye West accompagné de Rick Ross.)



4. Accès au BIOS de la VM en appuyant sur F2.
5. Booting sur un cd ROM
6. Modifications de l'iso afin de boot sur l'Ubuntu
7. Une fois sur l'Ubuntu, nous allons accéder à notre fichier toto.txt en suivant ces étapes:

Tout d'abord nous devons accéder à notre disque dur:



32 GB Volume

19.0 GB / 31.6 GB available /dev/sda2

Une fois dans celui-ci, nous allons choisir le dossier Users comme ci dessous:



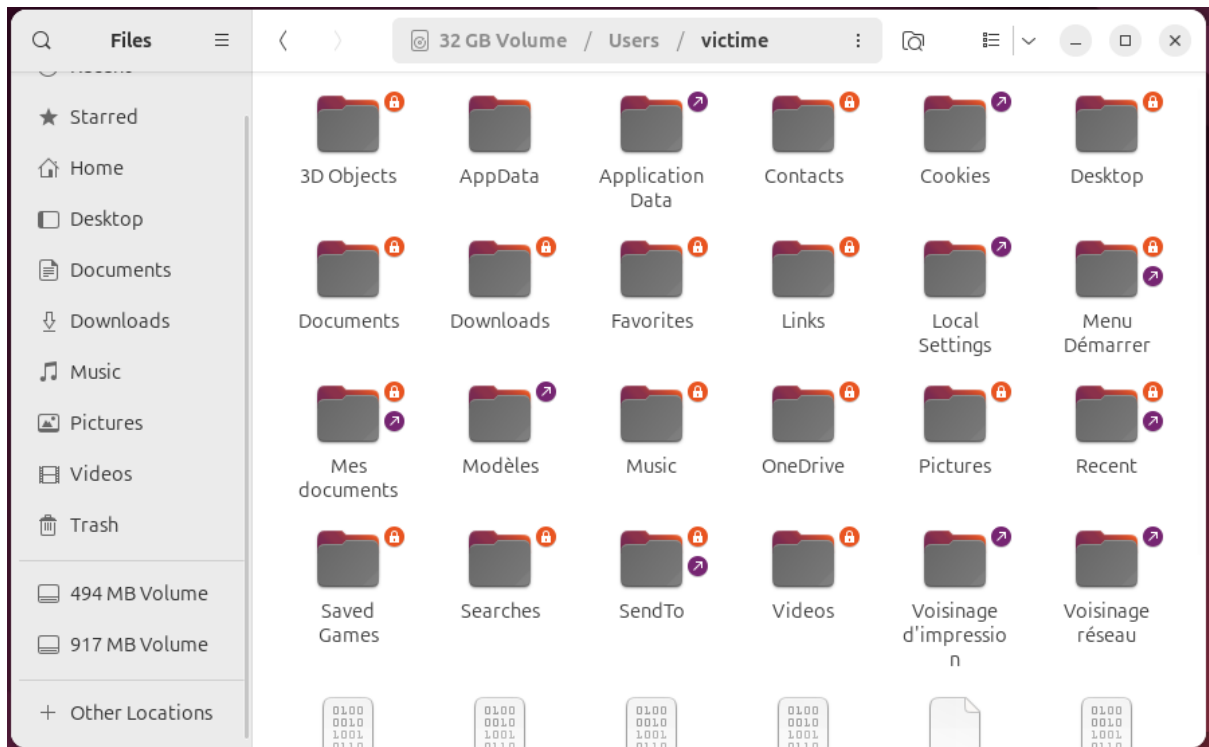
Users

Dans ce même dossier, nous allons sélectionner notre victime, l'utilisateur victime :

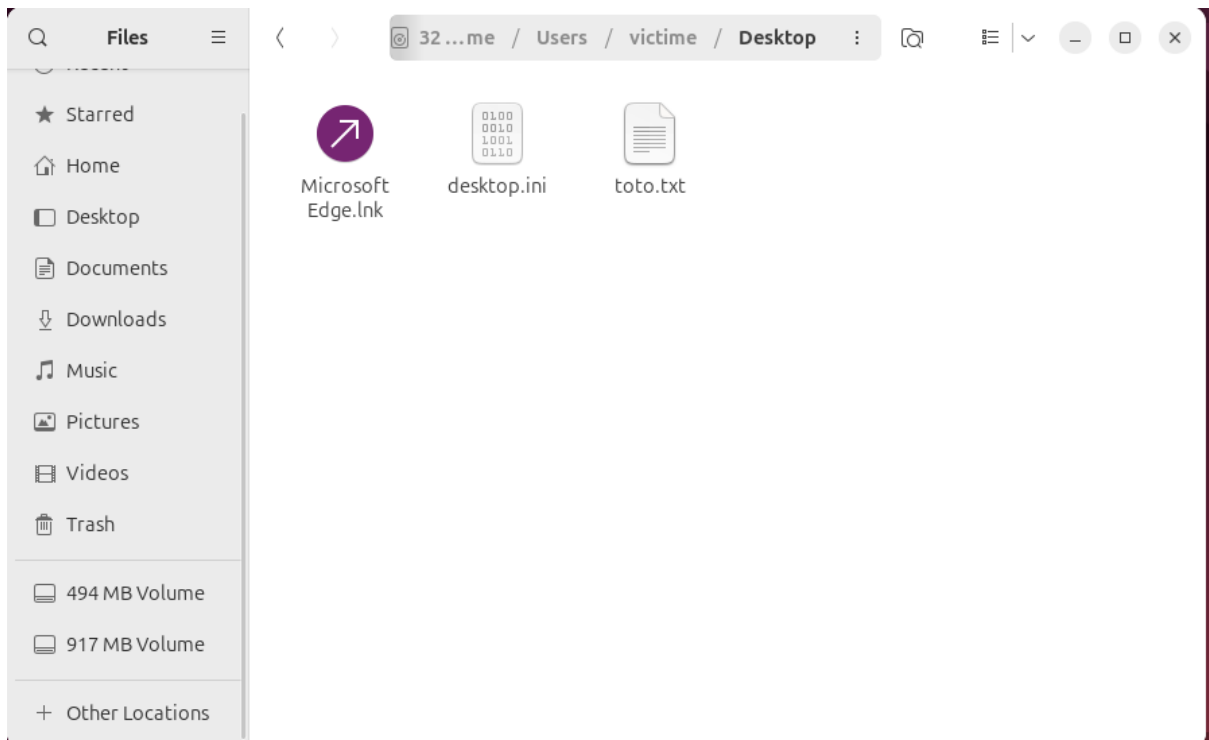


victime

Voici le contenu de l'utilisateur victime:

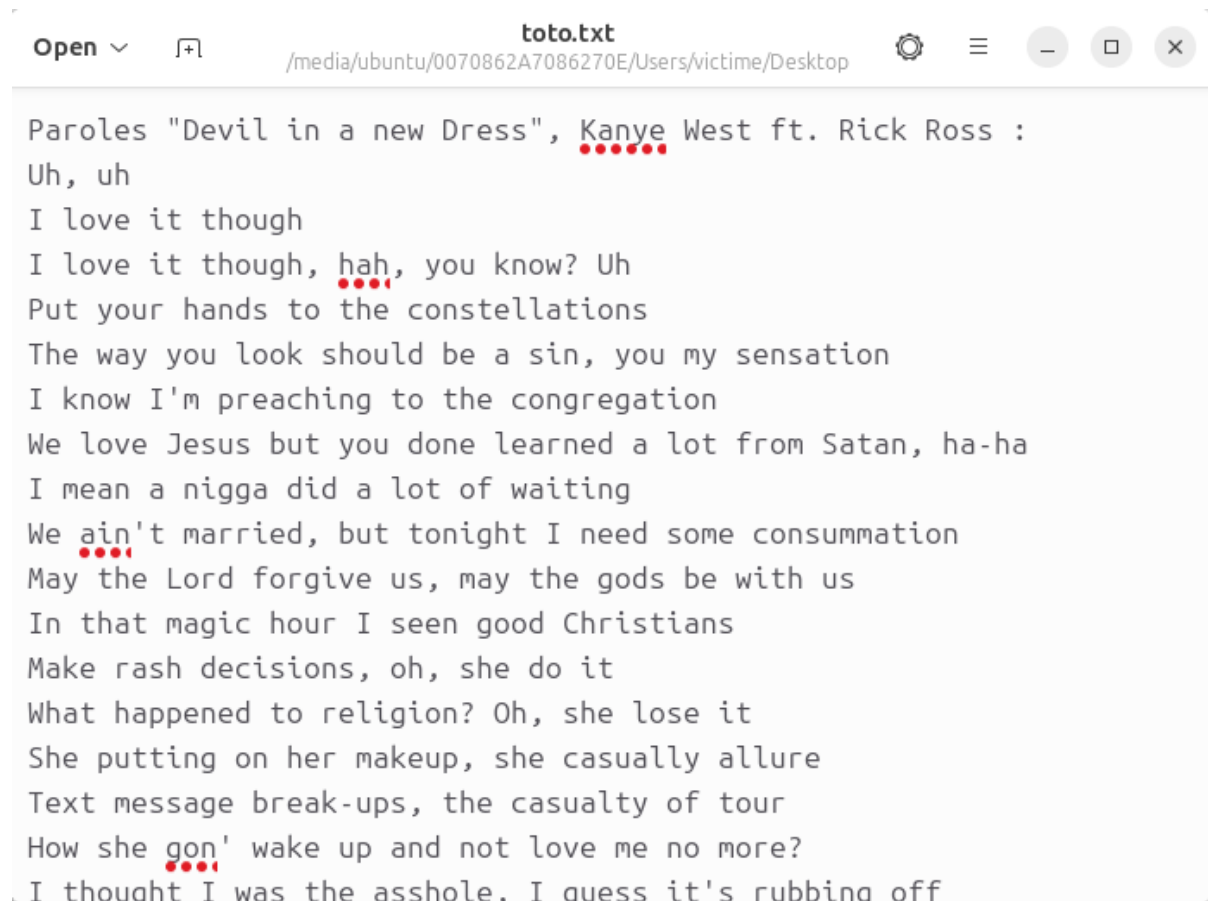


Lorsque nous avons créé le fichier toto.txt (cf l'étape 3), nous l'avons stocké sur le bureau. Nous allons donc rechercher dans le dossier Desktop.



Bingo ! Nous avons retrouvé notre fichier toto.txt contenant, pour rappel, les paroles de l'une des meilleures musiques jamais produite par l'humain.

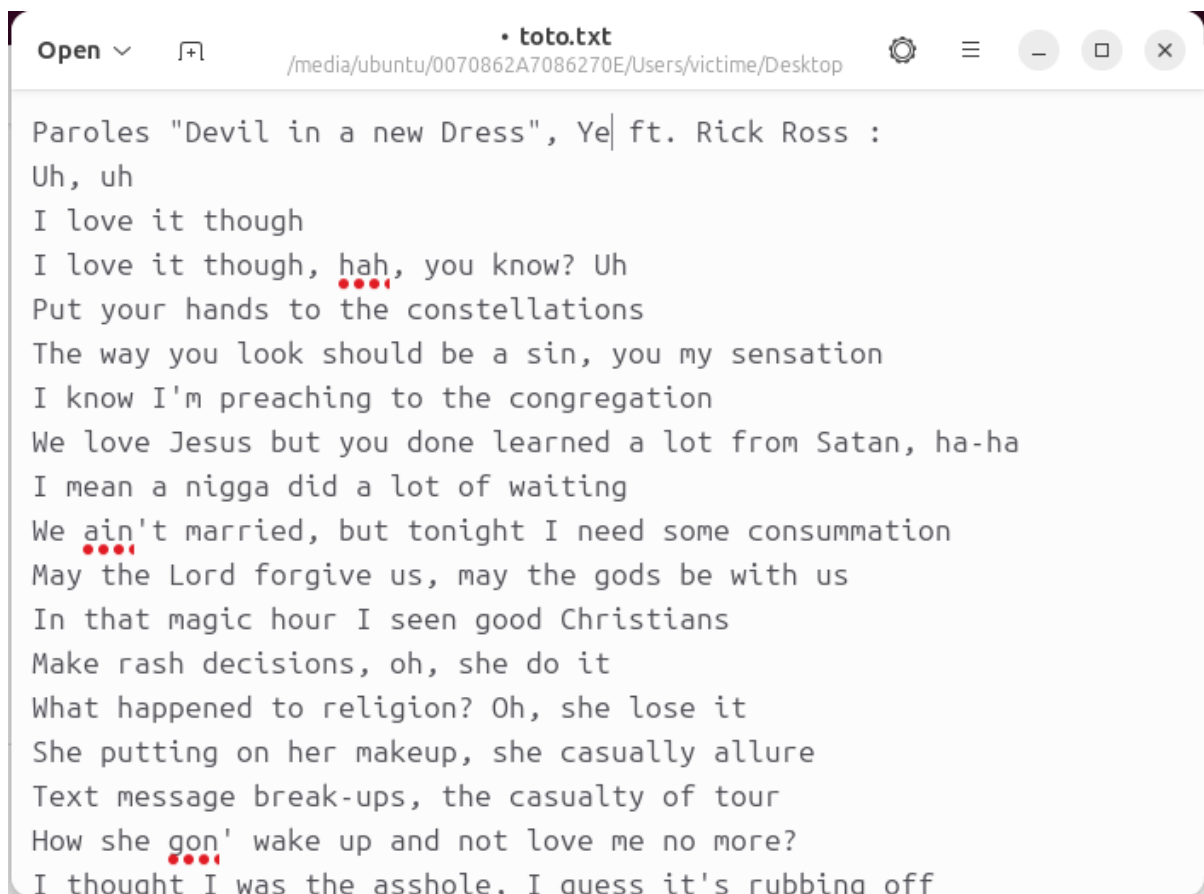
Vérifions maintenant si l'on peut l'ouvrir:



The image shows a screenshot of a text editor window. The title bar at the top reads 'toto.txt'. Below the title bar, the file path is visible: '/media/ubuntu/0070862A7086270E/Users/victim/Desktop'. The main area of the window contains the following text:

```
Paroles "Devil in a new Dress", Kanye West ft. Rick Ross :  
Uh, uh  
I love it though  
I love it though, hah, you know? Uh  
Put your hands to the constellations  
The way you look should be a sin, you my sensation  
I know I'm preaching to the congregation  
We love Jesus but you done learned a lot from Satan, ha-ha  
I mean a nigga did a lot of waiting  
We ain't married, but tonight I need some consummation  
May the Lord forgive us, may the gods be with us  
In that magic hour I seen good Christians  
Make rash decisions, oh, she do it  
What happened to religion? Oh, she lose it  
She putting on her makeup, she casually allure  
Text message break-ups, the casualty of tour  
How she gon' wake up and not love me no more?  
I thought I was the asshole, I guess it's rubbing off
```

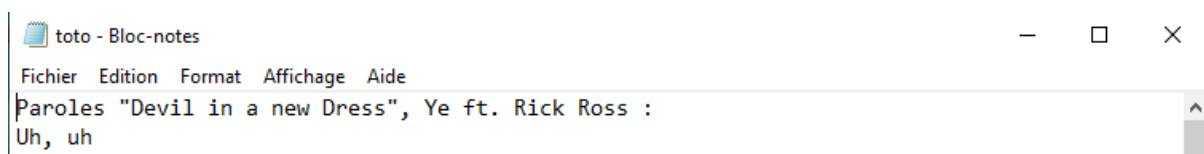
Nous pouvons l'ouvrir, vérifions maintenant la possibilité de modifier ce même fichier:



```
Open ▾ /media/ubuntu/0070862A7086270E/Users/victim/Desktop • toto.txt
Paroles "Devil in a new Dress", Ye ft. Rick Ross :
Uh, uh
I love it though
I love it though, hah, you know? Uh
Put your hands to the constellations
The way you look should be a sin, you my sensation
I know I'm preaching to the congregation
We love Jesus but you done learned a lot from Satan, ha-ha
I mean a nigga did a lot of waiting
We ain't married, but tonight I need some consummation
May the Lord forgive us, may the gods be with us
In that magic hour I seen good Christians
Make rash decisions, oh, she do it
What happened to religion? Oh, she lose it
She putting on her makeup, she casually allure
Text message break-ups, the casualty of tour
How she gon' wake up and not love me no more?
I thought I was the asshole, I guess it's rubbing off
```

Nous pouvons modifier le fichier ainsi que lire, ce qui pose évidemment de gros soucis au niveau sécurité car nous avons évité le mot de passe Windows en passant par un autre OS tout en restant sur un disque dur commun.

Nous allons tout de même vérifier que le fichier toto.txt a lui aussi était modifié.



```
toto - Bloc-notes
Fichier Edition Format Affichage Aide
Paroles "Devil in a new Dress", Ye ft. Rick Ross :
Uh, uh
```

La modification a bien été appliquée.

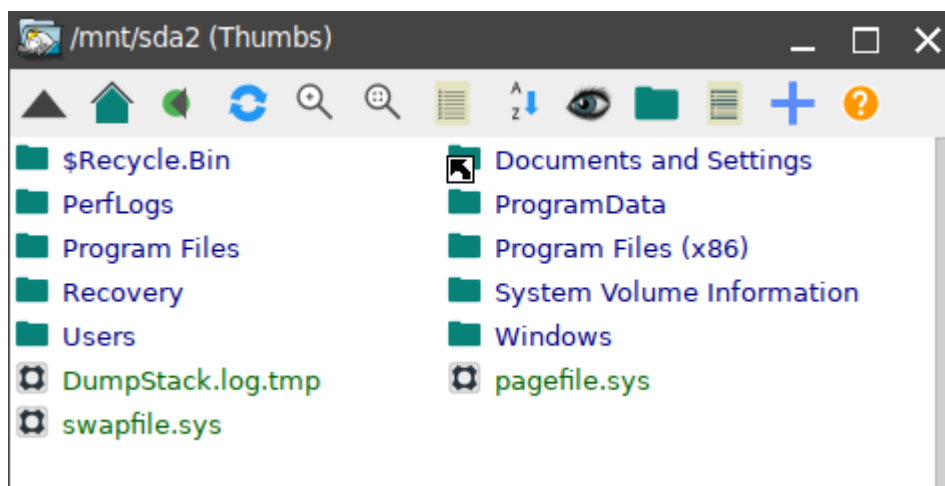
Essayons maintenant une autre méthode

La prochaine méthode consiste a repasser par un Linux mais cette fois pour intervertir deux fichiers au démarrage à savoir le fichier utilman.exe, qui charge au démarrage les paramètres d'accessibilité tels que la loupe, par le cmd.exe qui nous permettra de modifier le mot de passe. Le linux que nous allons utiliser est le Puppy Linux, très léger (400mb).

Après avoir boot sur notre linux , on arrive sur cet écran d'accueil



Nous allons maintenant rechercher dans les 3 lecteurs en bas à gauche lequel contient notre partition de windows.

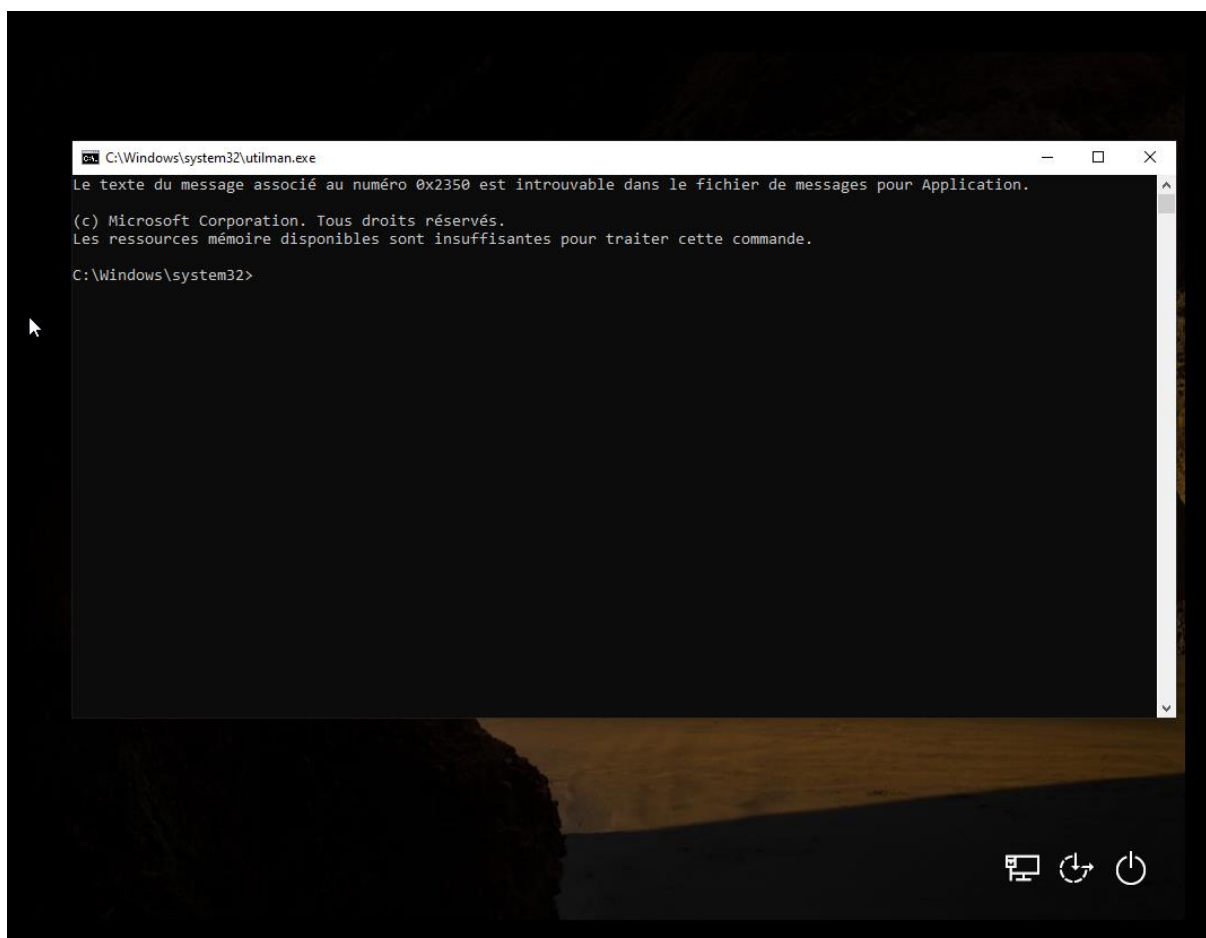


Une fois trouvé, nous allons entrer une commande afin de pouvoir inverser les deux fichiers comme expliquer au dessus.

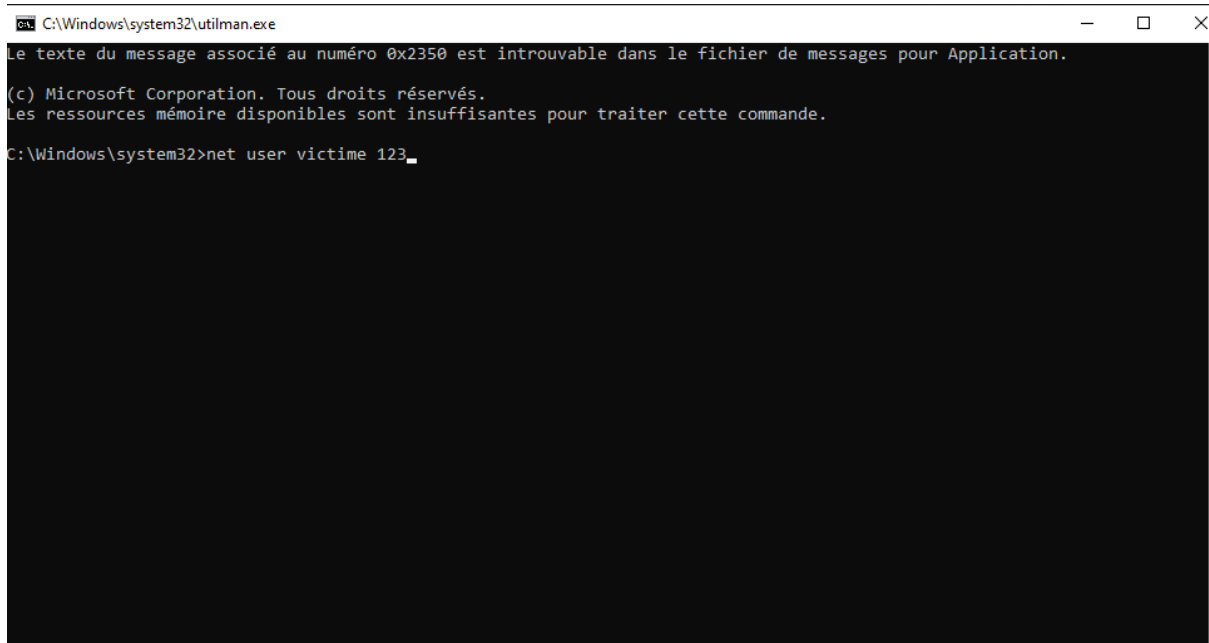
```
# cd /mnt/sda4
# cd Windows/System32
# mv Utilman.exe Utilman.exe.bak
# cp cmd.exe Utilman.exe
```

Grace a cette suite de commande (en remplaçant sda4 par sda2). Nous remplaçons sda4 par sda2 car c'est celui-ci qui contient notre partition de Windows.

Les commandes ont bien fonctionnée comme le montre la capture d'écran suivante:



Afin de modifier le mot de passe, nous allons utiliser la commande : `net user "nom_compte_utilisateur" nouveau_mot_de_passe avec victime` pour le nom d'utilisateur.



```
C:\Windows\system32\utilman.exe
Le texte du message associé au numéro 0x2350 est introuvable dans le fichier de messages pour Application.
(c) Microsoft Corporation. Tous droits réservés.
Les ressources mémoire disponibles sont insuffisantes pour traiter cette commande.
C:\Windows\system32>net user victime 123
```

En entrant ceci, le mot de passe est maintenant 123, la commande a bien fonctionné.

On a choisi de remplacer cmd et Utilman.exe car cette application se lance directement au démarrage et on peut l'utiliser dans l'écran d'accueil.

Dans notre épisode de Mr. Robot, c'est la méthode 2b WinRE, environnement de récupération windows. Il inverse les fichiers cmd et les fichiers sethc. Il ouvre donc son invite de commande grâce à la combinaison de touche Ctrl + A.

Nous venons de découvrir qu'il est possible d'utiliser une faille permettant d'accéder au disque dur de l'ordinateur via un autre OS afin de modifier le mot de passe sur un autre OS via l'accès aux partitions de celui-ci. On pourrait éviter ce genre de faille en interdisant l'accès aux autres partitions de disque dur par les OS entre eux. Cela fermerait ce pont entre les différentes "faces" de l'ordinateur et éviterait de se faire voler des données comme dans l'épisode de Mr. Robot sur son ordinateur de chez soi.

Une solution pour une configuration sans virtualisation, on pourrait mettre un mot de passe à notre bios afin que le voleur de données ne puisse même pas changer le bios.

On pourrait aussi chiffrer les données du disque dur. On peut protéger les données du premier OS en interdisant aux autres partitions de communiquer

Pour l'exemple de Mr. Robot, on remarque qu'utiliser la double authentification pour protéger ses différents comptes. Il est aussi grandement recommandé de ne pas sauvegarder ses mots de passe sur le navigateur, ne pas utiliser de gestionnaire de mot de passe et aussi de ne pas utiliser plus d'une fois un même mot de passe.

