2024.11.19 - Bloc 3 - TP2 Intrusion Windows

**

1. Préparation

J’ai créé ma VM, mon nom d’utilisateur est YohanVM

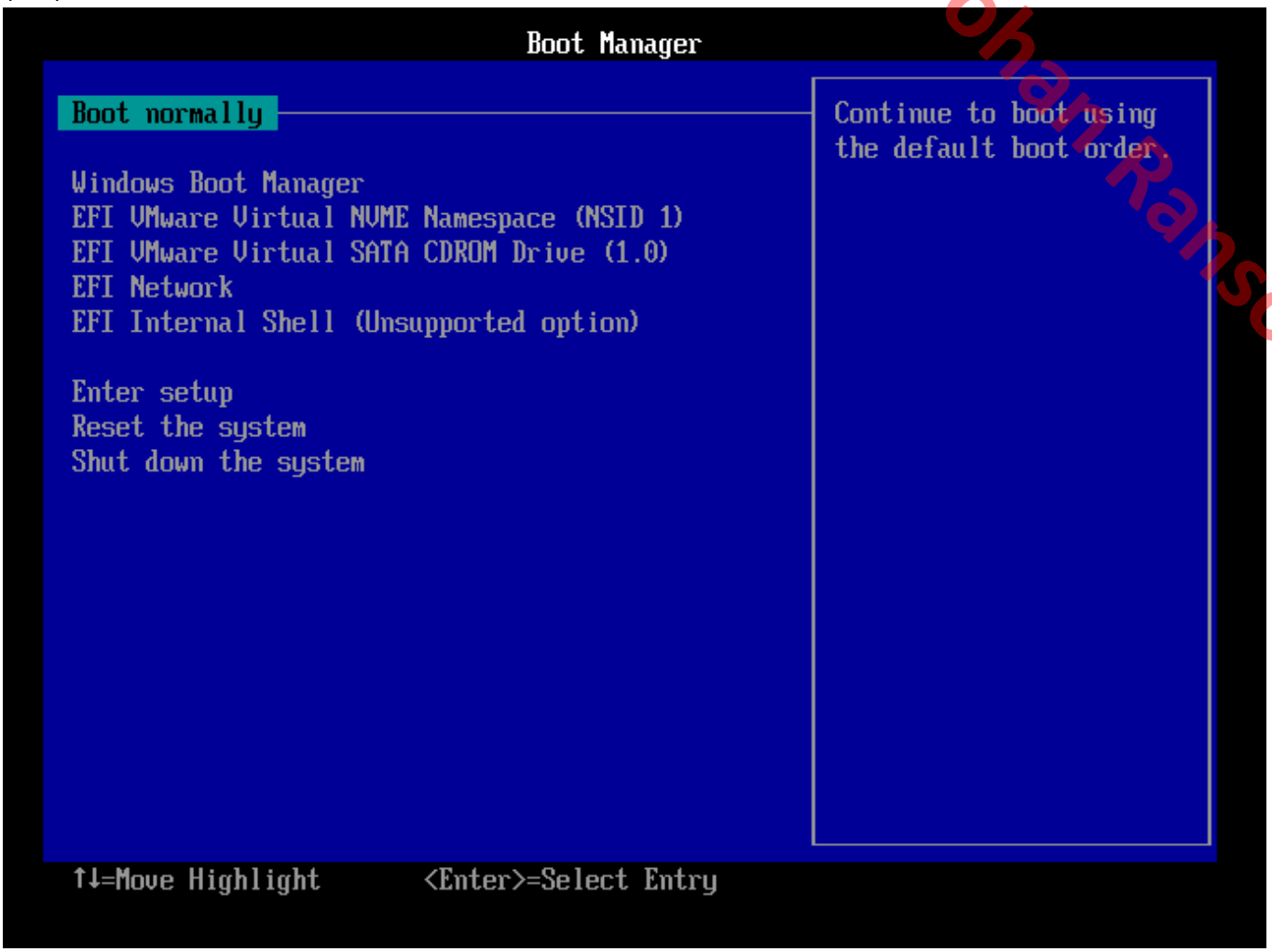
Je vais donc créer maintenant un fichier toto.txt sur mon bureau avec les paroles “Viens voir le docteur non n’aies pas peur”

Maintenant j’éteins ma VM et je télécharge Ubuntu (https://ubuntu.com/download/desktop/thank-you?version=24.04.1&architecture=amd64<s=true)

2. Booter Ubuntu

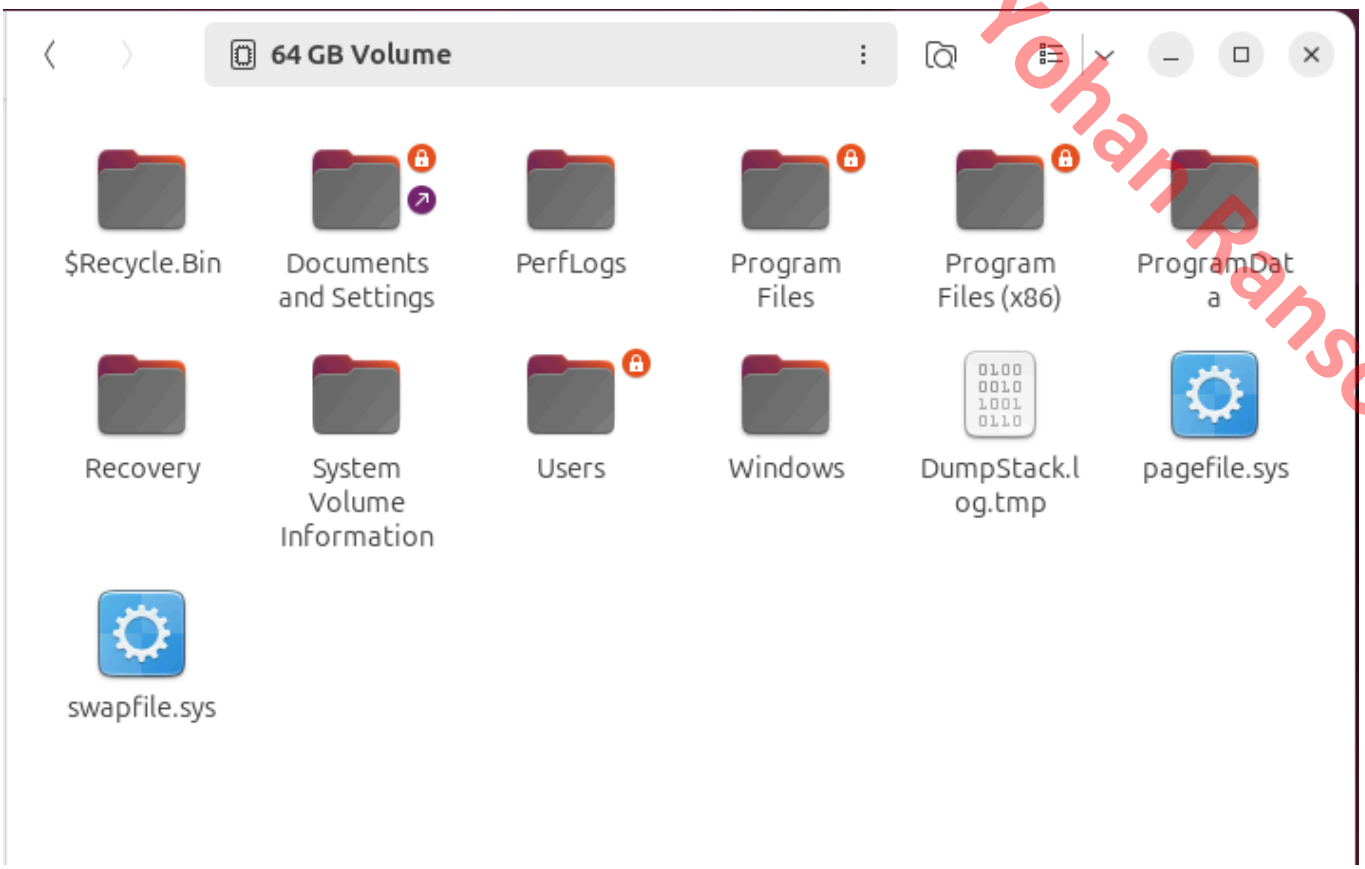
Je place l’iso Ubuntu dans “Edit virtual machine settings”, mais n’ayant pas réussi à démarrer avec Ubuntu j’ai dû m'aider de Google pour pouvoir acquérir cette page. J’ai donc dû accéder au BIOS pour pouvoir configurer l’ordre de démarrage et sélectionner “EFI SATA CDROM Drive

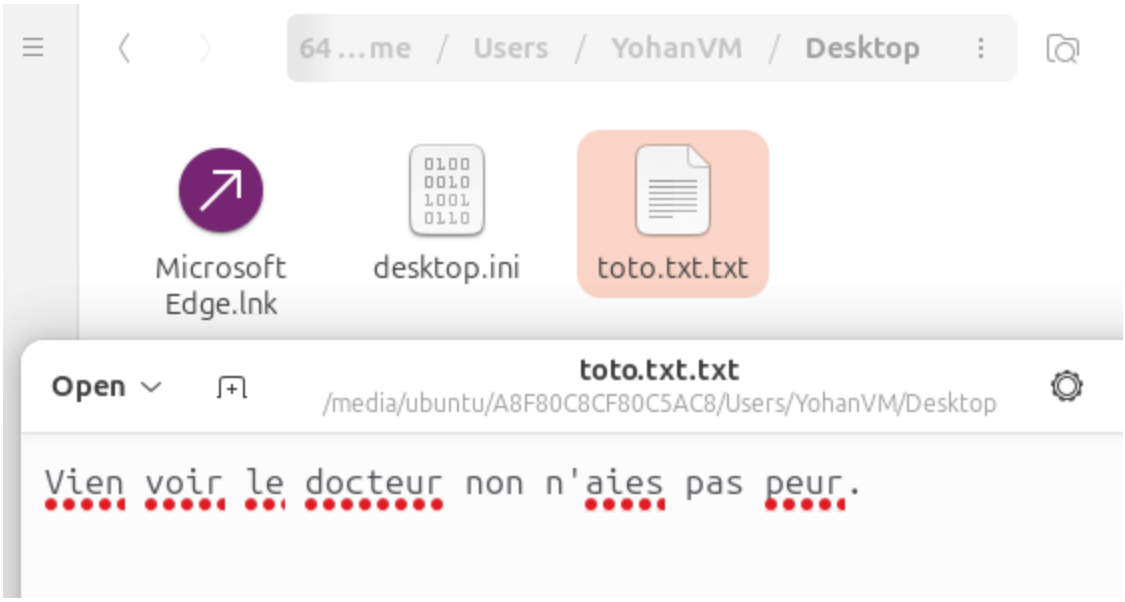
(1.0)



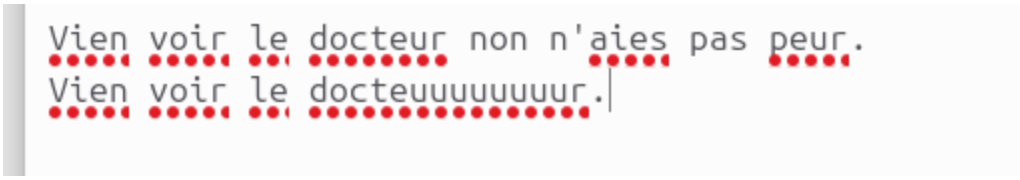
Pour retrouver le fichier “toto.txt” je vais sur l’onglet : Files

Une fois dessus j’ai recherché le fichier le plus “gros” pour accéder au disque principal de Windows.





J’ai pu ouvrir et lire le fichier.



Et même le modifier, et l’enregistrer. Je constate qu’il est bien modifié sur Windows.

Récapitulatif :

J’ai démarré la VM en mode live avec Ubuntu, ensuite j’ai accédé au disque dur de Windows en montant le volume principal de 64 GB.

Une fois le volume monté, j’ai pu accéder aux répertoires du système d’exploitation.

En allant chercher le dossier toto.txt (User > YohanVM > Desktop) J’ai pu l’ouvrir, lire son contenu, et même modifier le texte. Après avoir fait des modifications, j’ai réussi à enregistrer le fichier sans problème.

En finalité, cette expérience démontre une faiblesse importante de la sécurité par mot de passe de Windows.

Choisissez l’une des techniques et expérimentez là

J’ai choisi la méthode WinRE (l’environnement de récupération Windows) avec l’invite de commandes.

Je redémarre ma VM et j’appuie rapidement sur F8 pour accéder au mode de récupération de Windows et sélectionner Windows boot Manager

Ensuite je force l’accès à WinRE en fermant brutalement Windows deux ou trois fois. Ensuite, Windows détecte une tentative de démarrage défectueuse et on me propose automatiquement un écran de récupération.

Dépannage > Options avancées > Invite de commandes.

En entrant les commandes dites sur le site “le chemin d’accès spécifié est introuvable” sûrement une mauvaise manipulation de ma part.

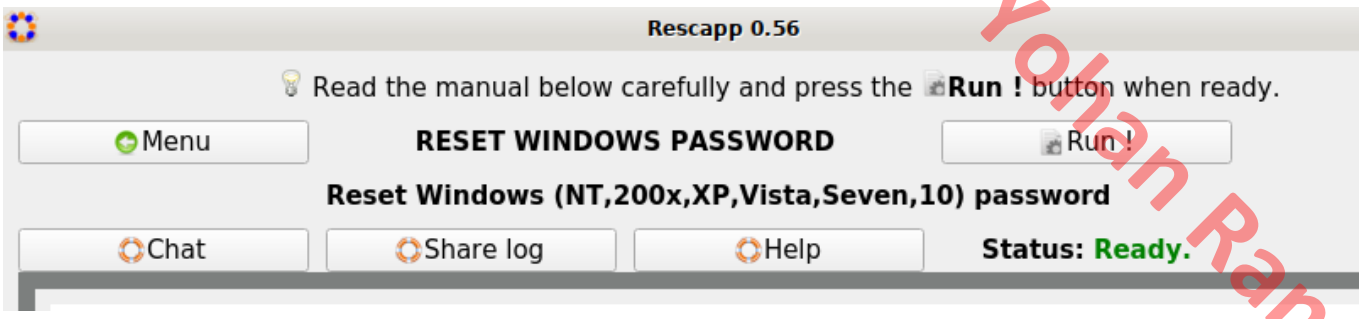
Cependant, pour pouvoir récupérer mon mot de passe je dois le connaitre (sachant qu’il n’y a qu’une session admin) S’il y avait plusieurs sessions, il me faudrait connaître au moins l’un des mots de passe de session.

Maintenant testons avec Rescatux

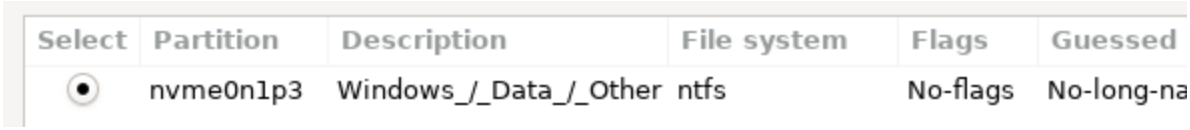
J’ai téléchargé l’iso de Rescatux sur sourceforge.net

Une fois l’iso monté j’ai du ré-accéder au BIOS pour changer l’ordre de démarrage des iso.

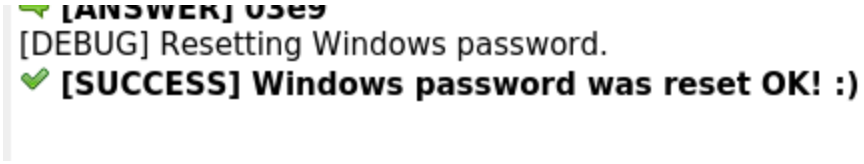
Rescatux est maintenant lancé, j’ai donc été sur le fichier “Rescapp” ensuite “Reset Windows Password”



Je sélectionne la partition Windows



Et j'ai ensuite effacer le mot de passe



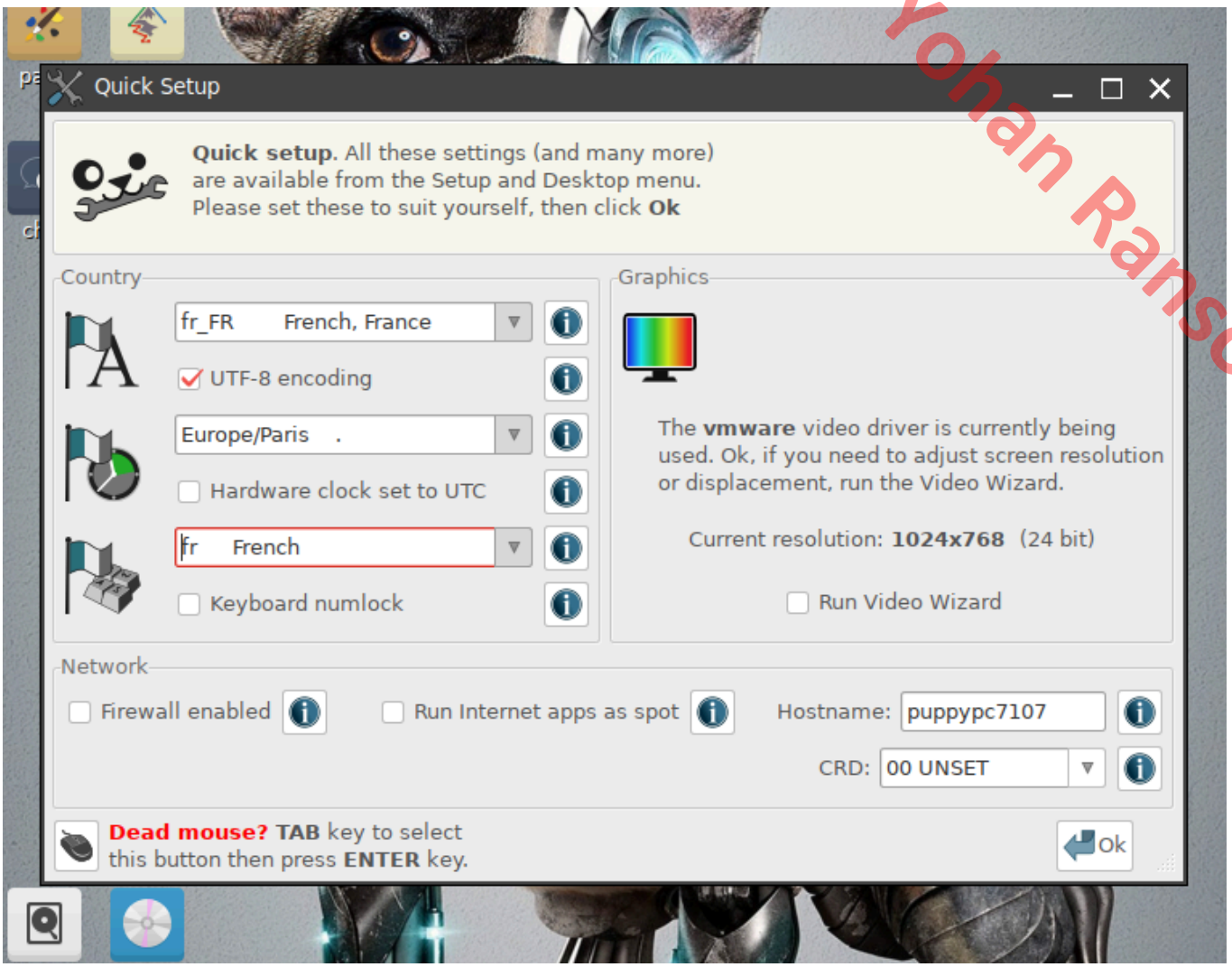
En redémarrant ma VM que je constate que le mot de passe à bien été réinitialisé

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

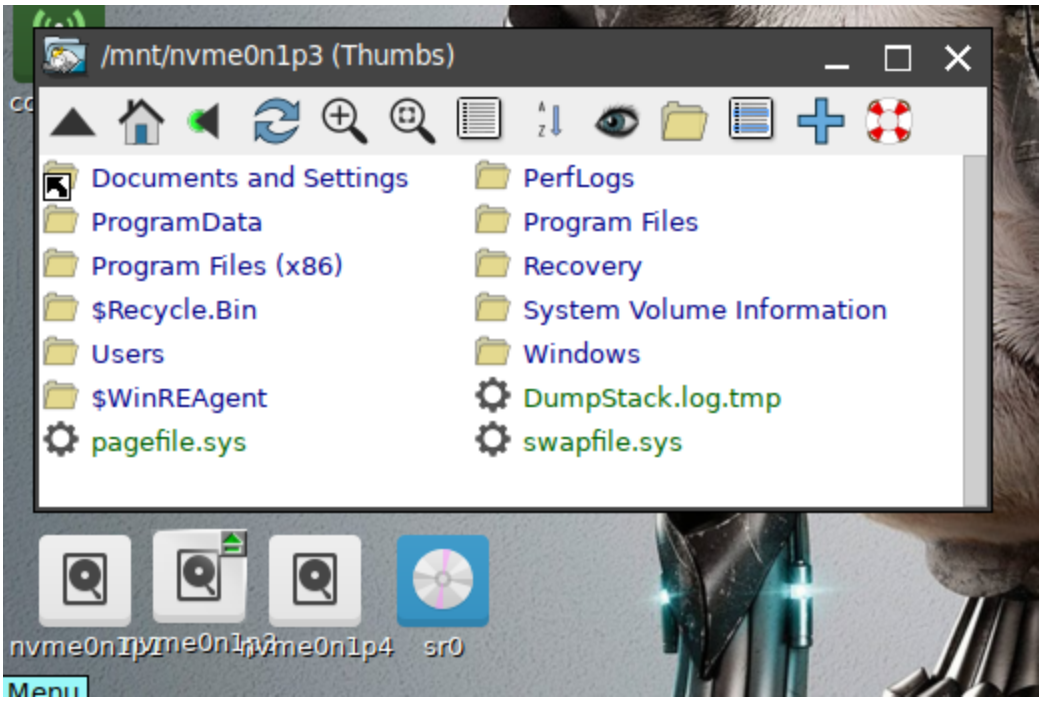
En ayant bien regardé la vidéo et en regardant les tutos je constate que la méthode qui s'approche le plus de la vidéo évoquée est celle avec Puppy Linux.

L'idée est qu'en remplaçant un fichier système , on peut ouvrir une session de commande au moment de l'écran de connexion de Windows.

Une fois Puppy Linux ouvert nous devons choisir la langue ainsi que la disposition du clavier.



Je cherche ensuite ma partition Windows : (nvme0n1p3)



Ayant eu des difficultées à faire les manipulations, j'ai du m'aider de ChatGPT pour choisir les bonnes commandes pour être en lecture-écriture

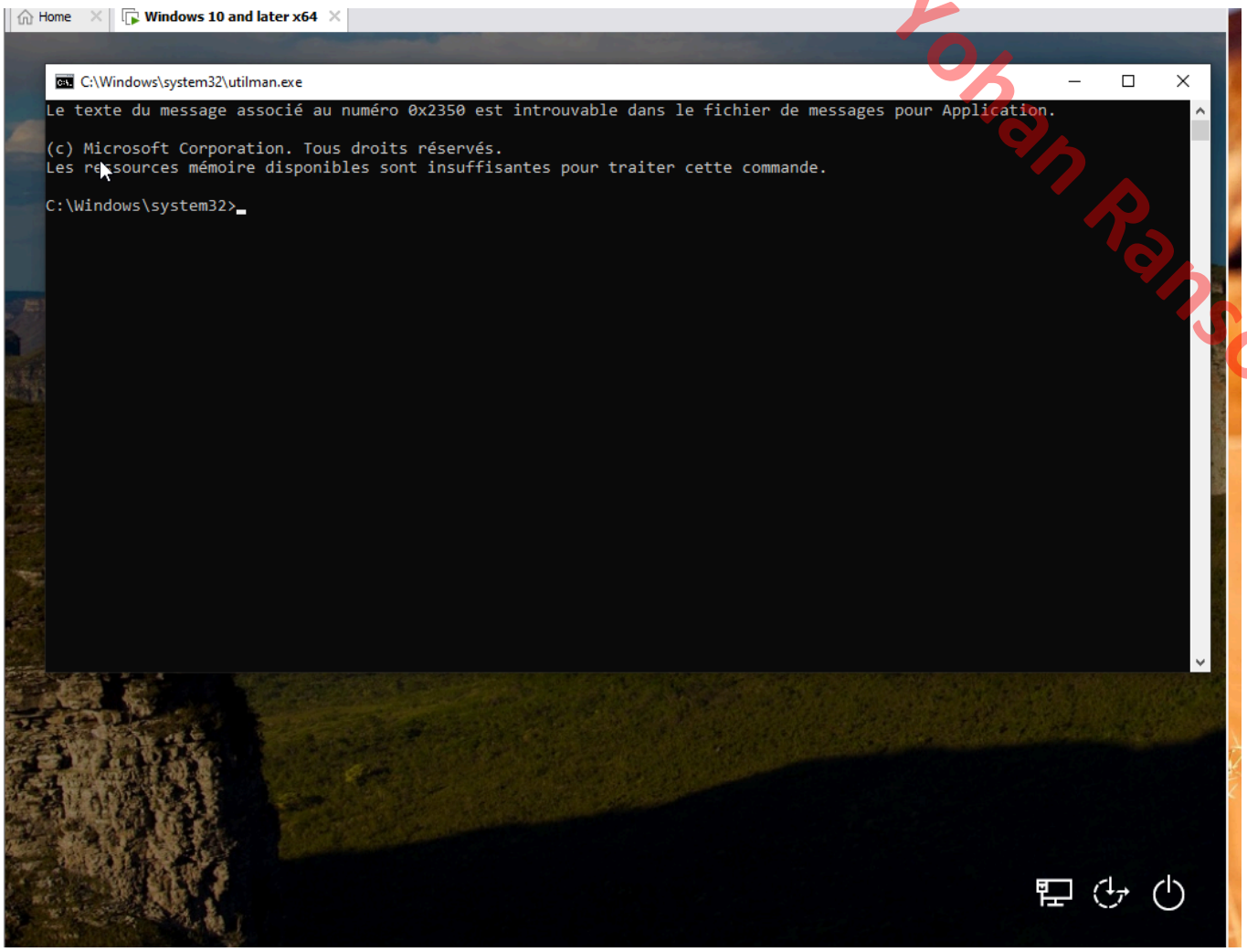

```
root# umount /mnt/windows
nvm: invalid drive

** (ROX-Filer:13193): WARNING **: 23:29:00.814: Existing ROX-Filer process is not respon
ding! Try with -n
root# killall ROX-Filer
root# umount /mnt/windows
umount-FULL: /mnt/windows: not mounted.
root# ntfs-3g /dev/nvme0n1p3 /mnt/windows
root# _
```

```
root# mount | grep /mnt/windows
/dev/nvme0n1p3 on /mnt/windows type fuseblk (rw,relatime,user_id=0,group_id=0,allow_othe
r,blksize=4096)
root#
```

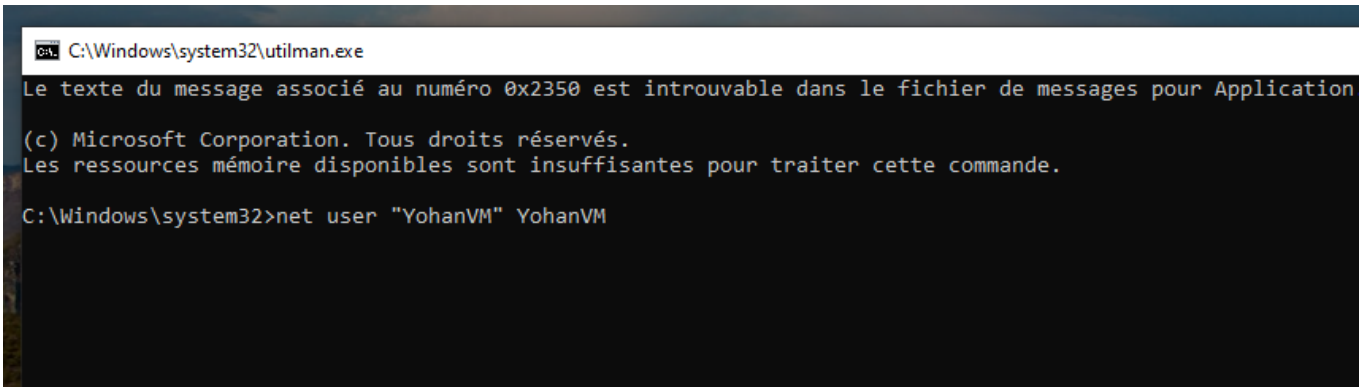
Après de nombreuses péripéties ….

```
root# cd /mnt/windows/Windows/System32
root# mv Utilman.exe Utilman_old.exe
root# cp cmd.exe Utilman.exe
root# _
```

J'ai pu réussir à accéder à l'invite de commande sur la page de connexion windows :



Et ainsi modifier le mot de passe :



J'en conclus qu'avec simplement quelques manipulations il reste plutôt simple de contourner la sécurité Windows. Il suffit juste d'avoir les bons logiciels et nous pouvons récupérer, réinitialiser et contourner les mots de passe.

L'exemple même avec Ubuntu, le fait de pouvoir modifier des fichiers sur un Windows protégé par un mot de passe, sans avoir ce mot de passe est plutôt pas mal. Cela peut permettre de pouvoir récupérer des documents importants et sensibles lorsque nous perdons notre mot de passe.

Ou bien avec Puppy Linux, pouvoir réinitialiser le mot de passe en mettant quelques commandes dans la console (comme sur la vidéo).

Ces techniques sont fort pratique certe, mais celà n'empêche qu'entre de mauvaises mains elles s'avèrent risqué car n'importe qui d'assez compétent peut accéder à vos données (perso comme pro).

Pour se protéger de celà nous pouvons :

- Désactiver le démarrage sur des supports externes dans le BIOS et mettre un mot de passe dans le BIOS.

Celà pourrait limiter les options d'intrusion en empêchant un démarrage alternatif. Cependant, cette méthode n'est efficace que si elle est combinée avec un mot de passe BIOS pour

empêcher quelqu'un de modifier les paramètres de démarrage.

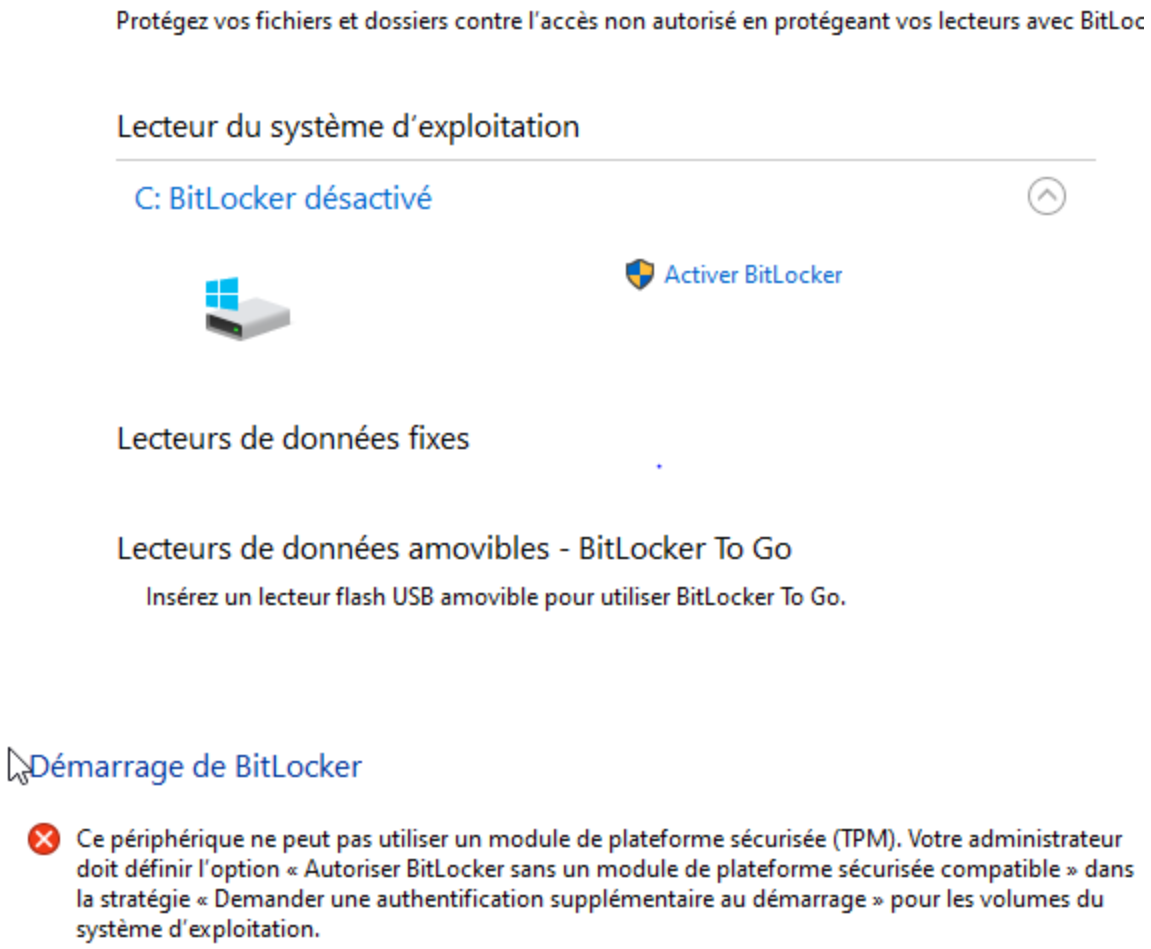
- Activer le chiffrement du disque avec BitLocker

L'avantage est que celà rend l'accès aux données quasiment impossible (sauf pour monsieur Jobard) même si le disque dur est physiquement retiré de la machine.

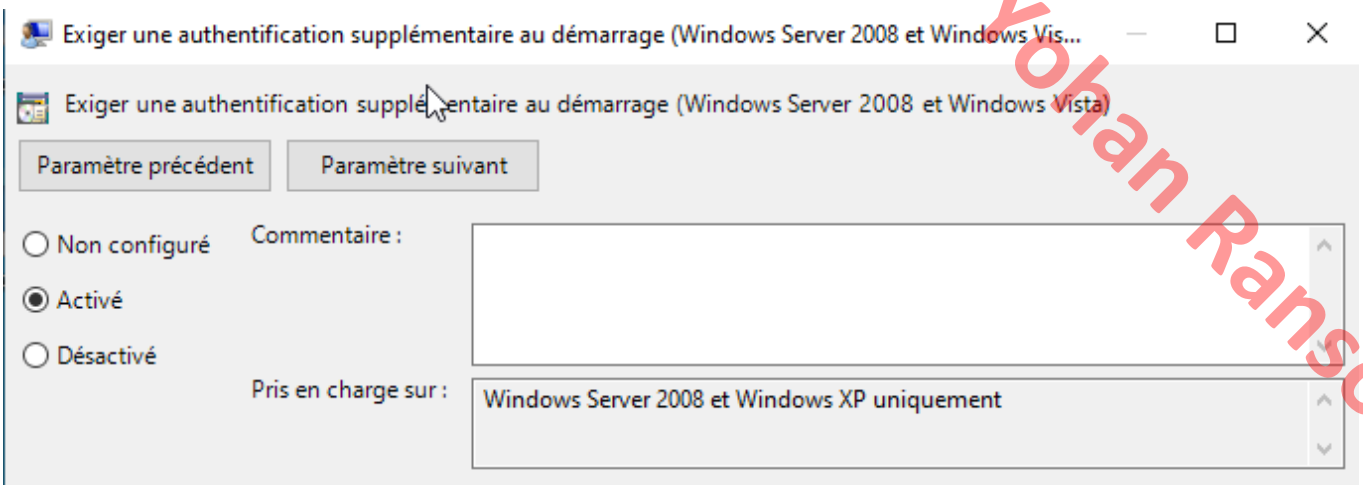
Cependant, il faut bien s'assurer d'avoir sauvegarder la clé de récupération BitLocker. En cas de perte, il peut être impossible de récupérer les données (sauf, encore une fois, pour monsieur Jobard)

Pour Linux le résultat est le même malgré qu'il soit stricte en matière de permission. Si le disque n'est pas chiffré, un accès avec un autre système d'exploitation peut permettre de contourner les protections.

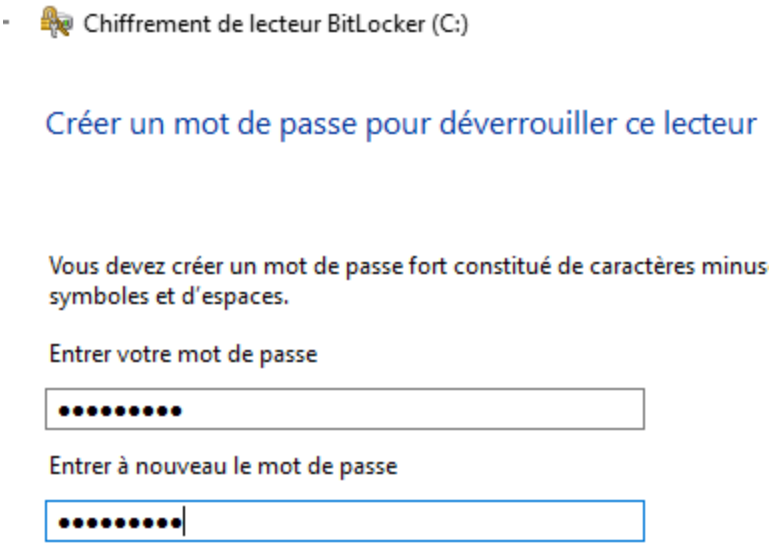
Je vais maintenant essayer de chiffrer avec BitLocker :

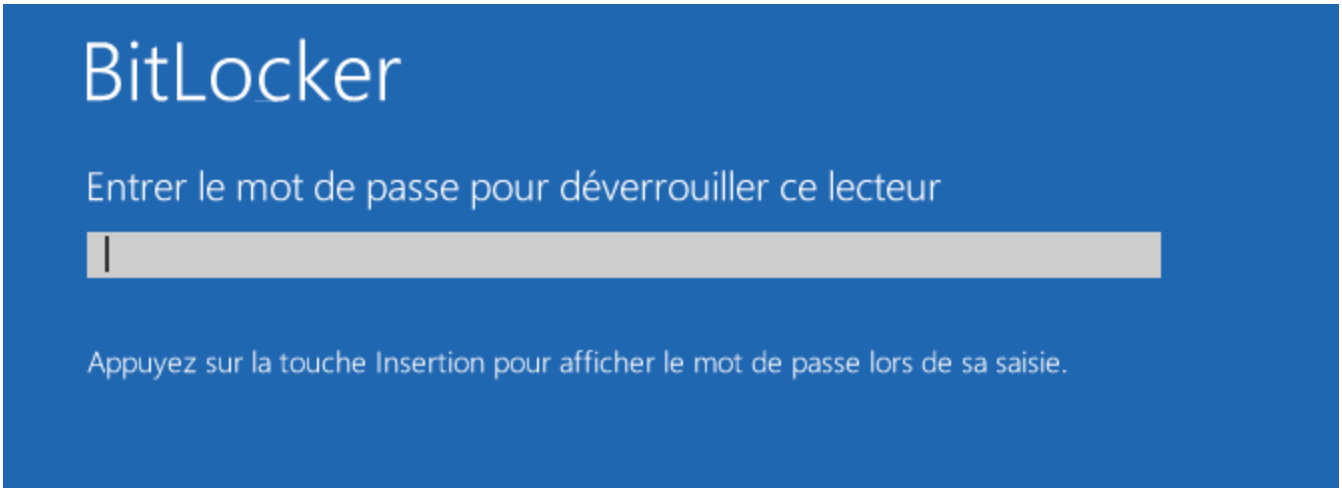


BitLocker ne peut pas être activé, je vais devoir le configurer pour qu'il fonctionne sans TPM en ouvrant l'éditeur de Stratégie.



Une fois la manipulation faite, j'ai pu choisir mon mot de passe et le confirmer.





Pour conclure;

Chiffré avec BitLocker peut énormément aider à la sécurisation de nos données.

Suite à des difficultés techniques liées à mon matériel, j'ai eu recours à l'assistance de ChatGPT pour suivre les procédures nécessaires et pour formuler certaines phrases. Cet accompagnement m'a permis de compléter ce TP en respectant les consignes malgré les obstacles rencontrés.

**