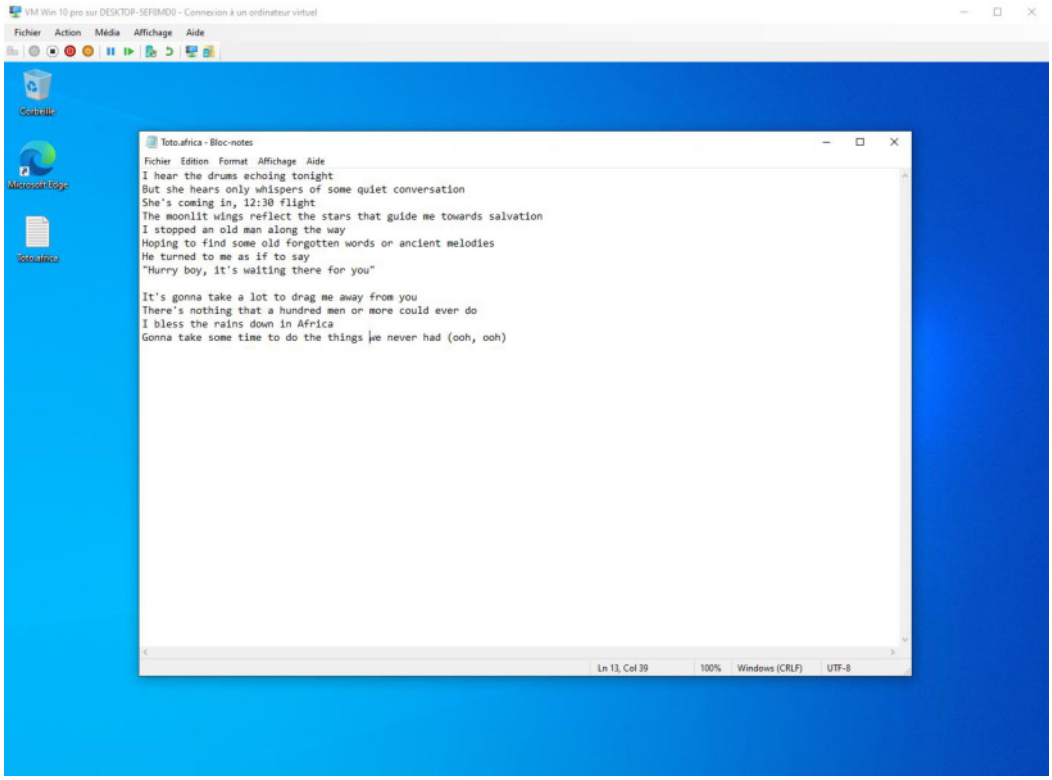
CASALE Pierre 18/10/2022

Compte rendu TP intrusion Windows

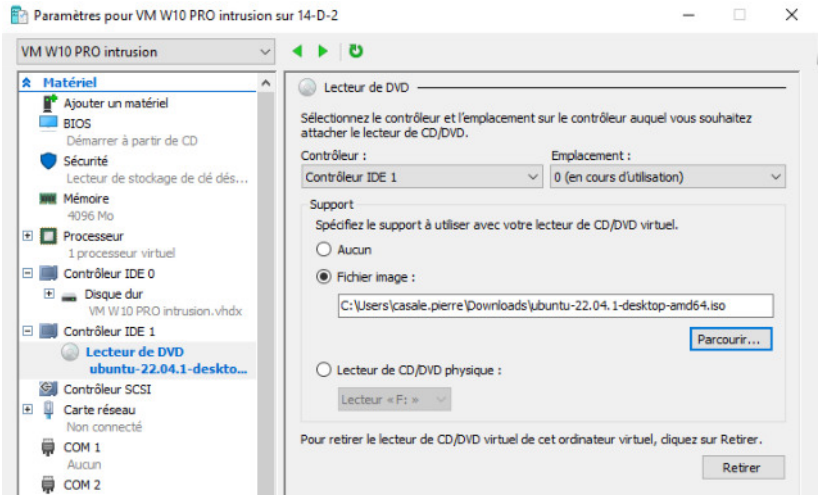
Première partie

Nous allons voir comment accéder à un fichier sur le bureau d'un utilisateur sans démarrer sa session.

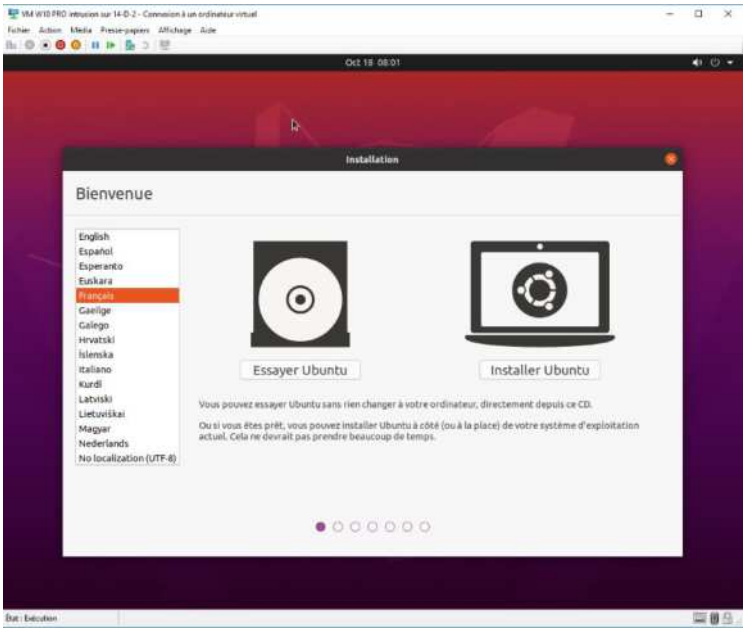
Tout d'abord on crée une VM Windows 10 pro, puis on choisit un mot de passe utilisateur avant de lancer Windows. On crée un fichier Toto en txt avec des paroles de chanson.



Une fois le fichier enregistré on éteint la VM et on ajoute l'iso d'Ubuntu.

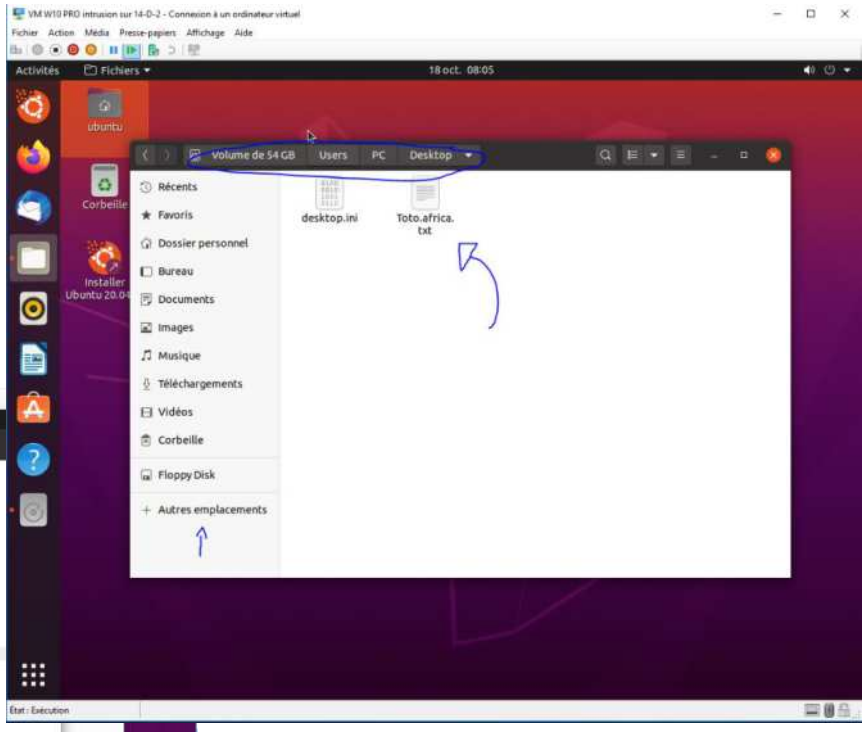


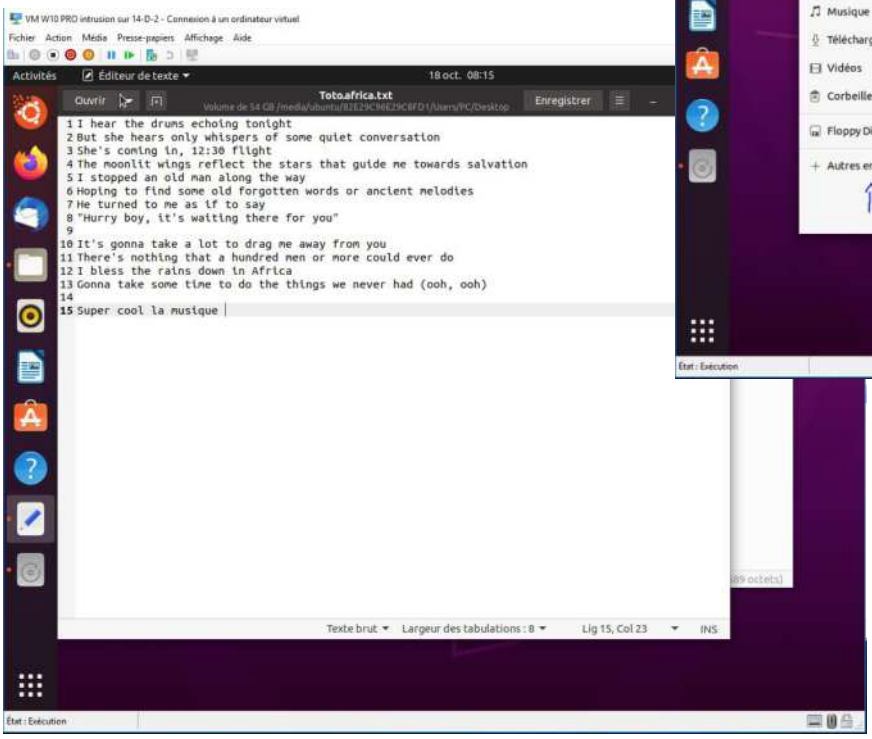
Puis on relance la VM en choisissant « essayer Ubuntu »



Maintenant on va essayer d'accéder à notre fichier Toto.

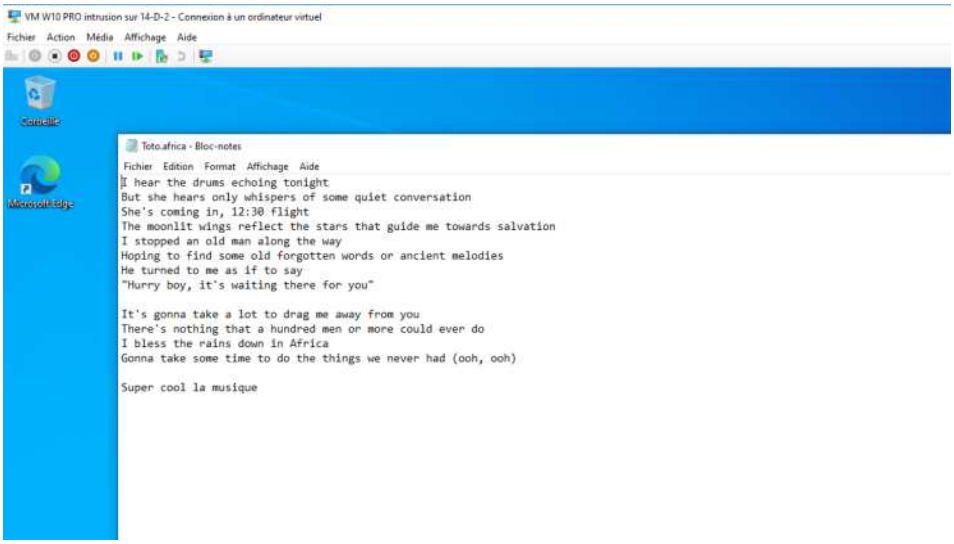
Une fois Ubuntu lancé on va aller dans l'explorateur de fichier (cliquer sur Ubuntu), choisir « un autre emplacement », sélectionner le disque ou est installé Windows, cliquer sur « user » puis sur le nom d'utilisateur (ici PC) et enfin aller sur le bureau.





De là on a accès au fichier toto, il suffit de l'ouvrir et nous pouvons le modifier.

Après avoir redémarré notre VM (en éjectant l'iso au préalable) on peut ouvrir notre fichier toto et voir qu'effectivement les modifications ont été enregistrées.



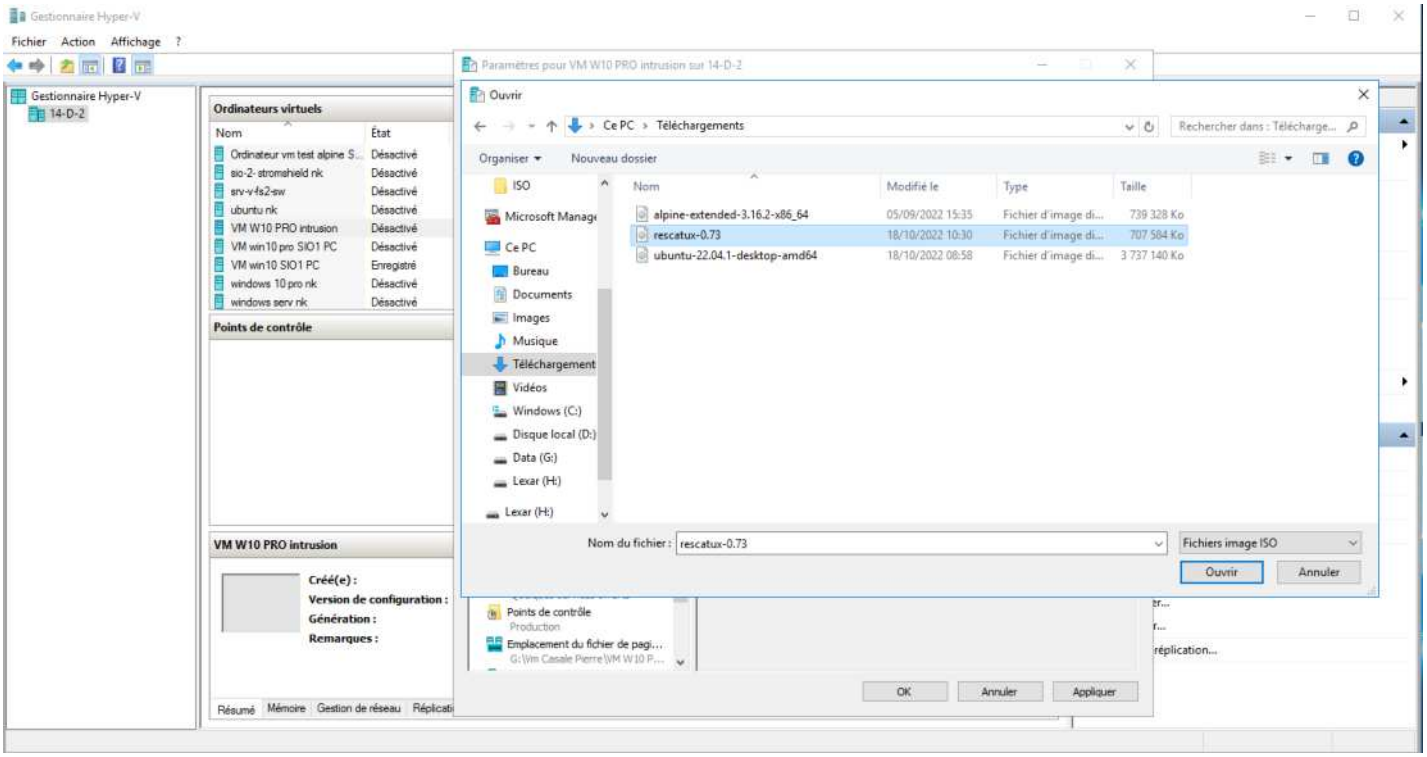
Par conséquent on peut en déduire qu'en démarrant sur Ubuntu par exemple on peut avoir accès au reste de l'ordinateur sans rencontrer de sécurité.

Deuxième partie

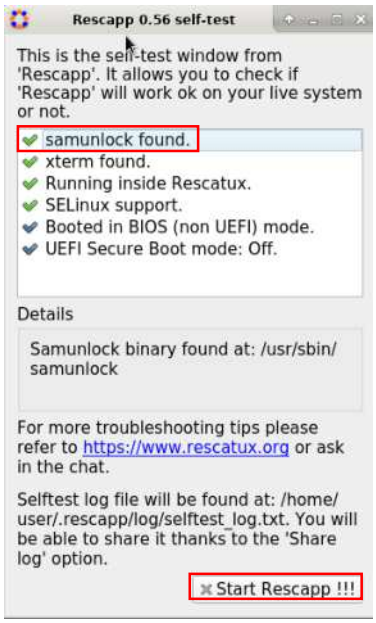
Nous allons voir comment nous connecter à notre session Windows sans avoir à saisir le mot de passe, pour cela il y a énormément d'outils sur internet dont trois que l'on va tester dans ce tp.

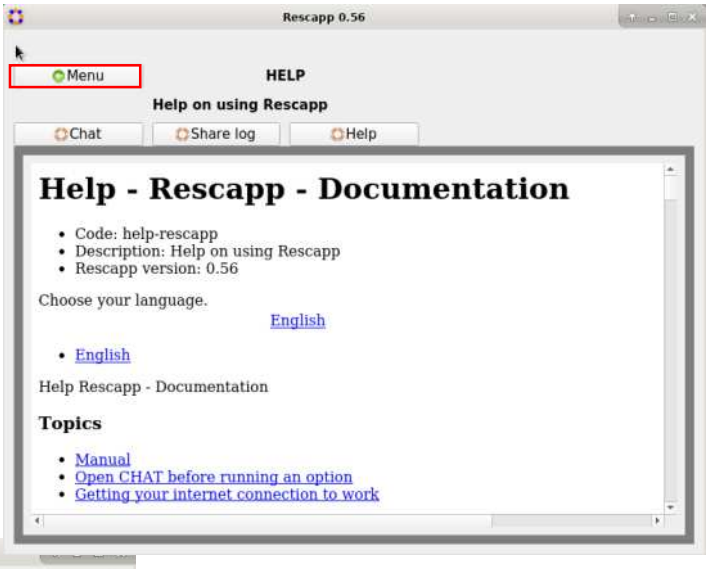
1/ Rescatux

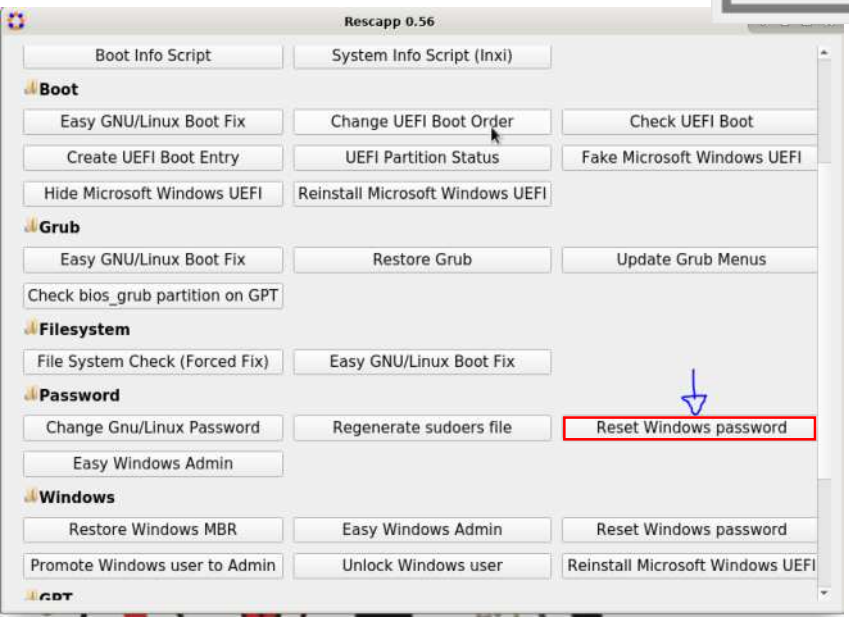
Après avoir téléchargé l'iso de rescatux (trouvé sur Google en quelques clics) il suffit de l'ajouter dans notre VM comme précédemment avec Ubuntu.



La VM va donc démarrer sur l'outil rescatux, une fois sur ce qui s'apparente à un bureau, on clique sur rescatux.app, « execute », dans la fenêtre suivante on sélectionne « samunlock found » puis on clique sur « Start Rescapp !!! » et sur « Menu ».

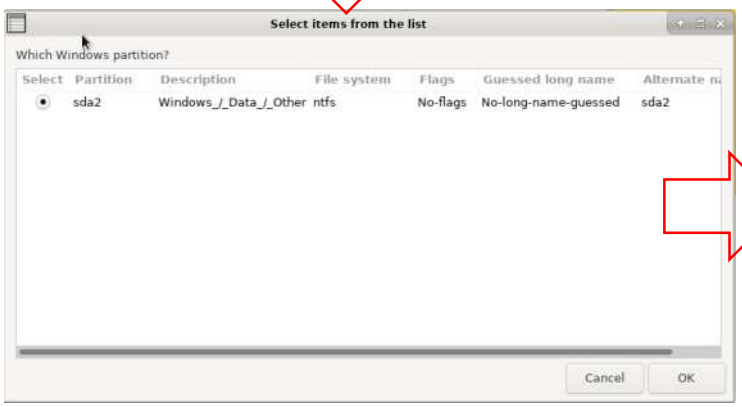


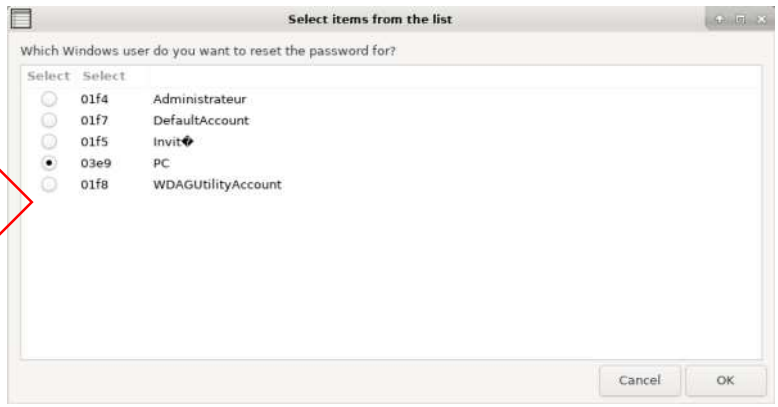




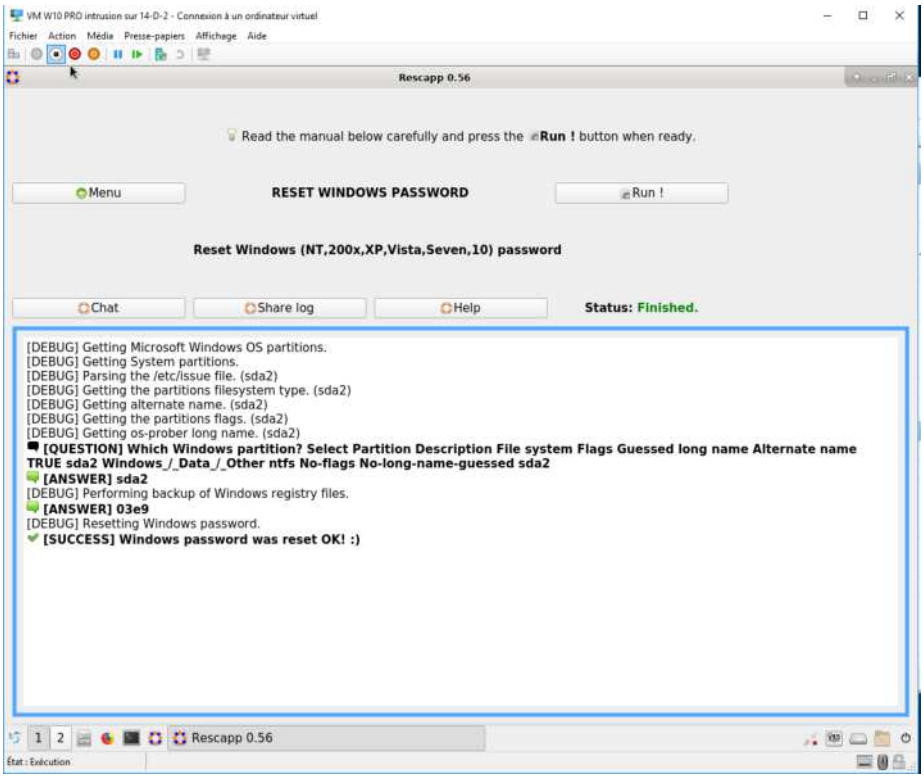
Ici on clique sur « Reset Windows password »

On commence la procédure en cliquant sur « Run », on sélectionne le disque concerné (sda2), puis l'utilisateur.

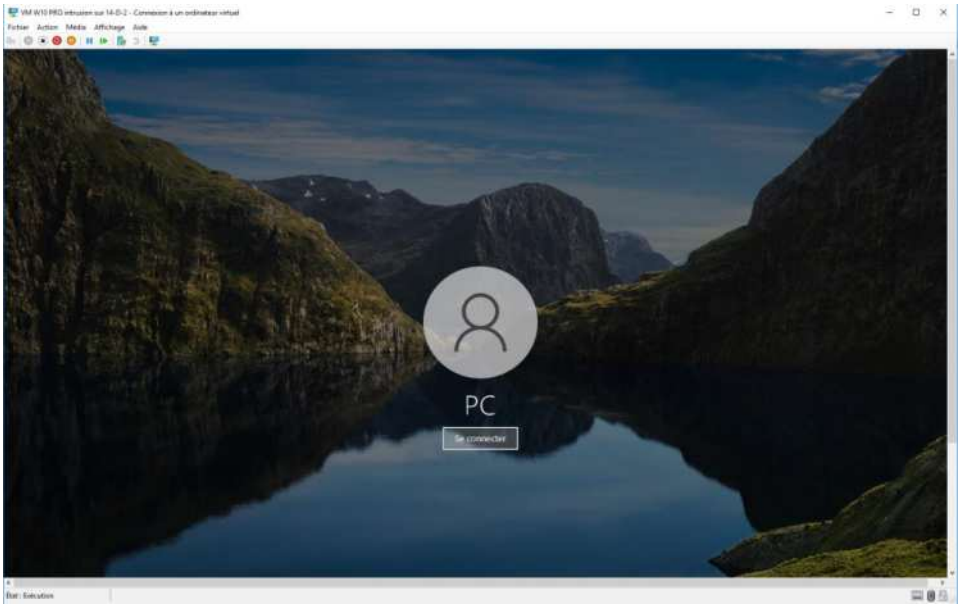




Le mot de passe a maintenant été réinitialisé, il suffit donc d'éteindre la VM et la relancer pour qu'elle démarre sous Windows et on peut s'apercevoir qu'on peut se connecter sans entrer de mot de passe.



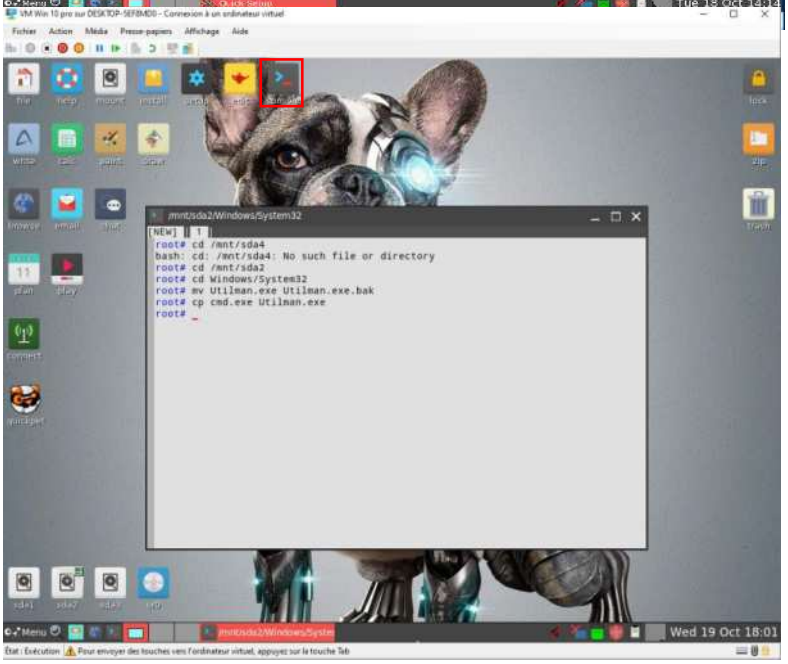
On voit qu'aucun mot de passe n'est demandé, on a donc pu accéder à la session utilisateur sans passer par le mot de passe.



2/ Puppy linux

Comme précédemment on ajoute l'iso désirée dans notre VM, pour cet exemple puppy linux.

Une fois démarré nous pouvons changer la langue pour le français, dans l'onglet qui s'ouvre automatiquement, pour faciliter les étapes suivantes.



On ouvre la console et on tape les commandes suivantes :

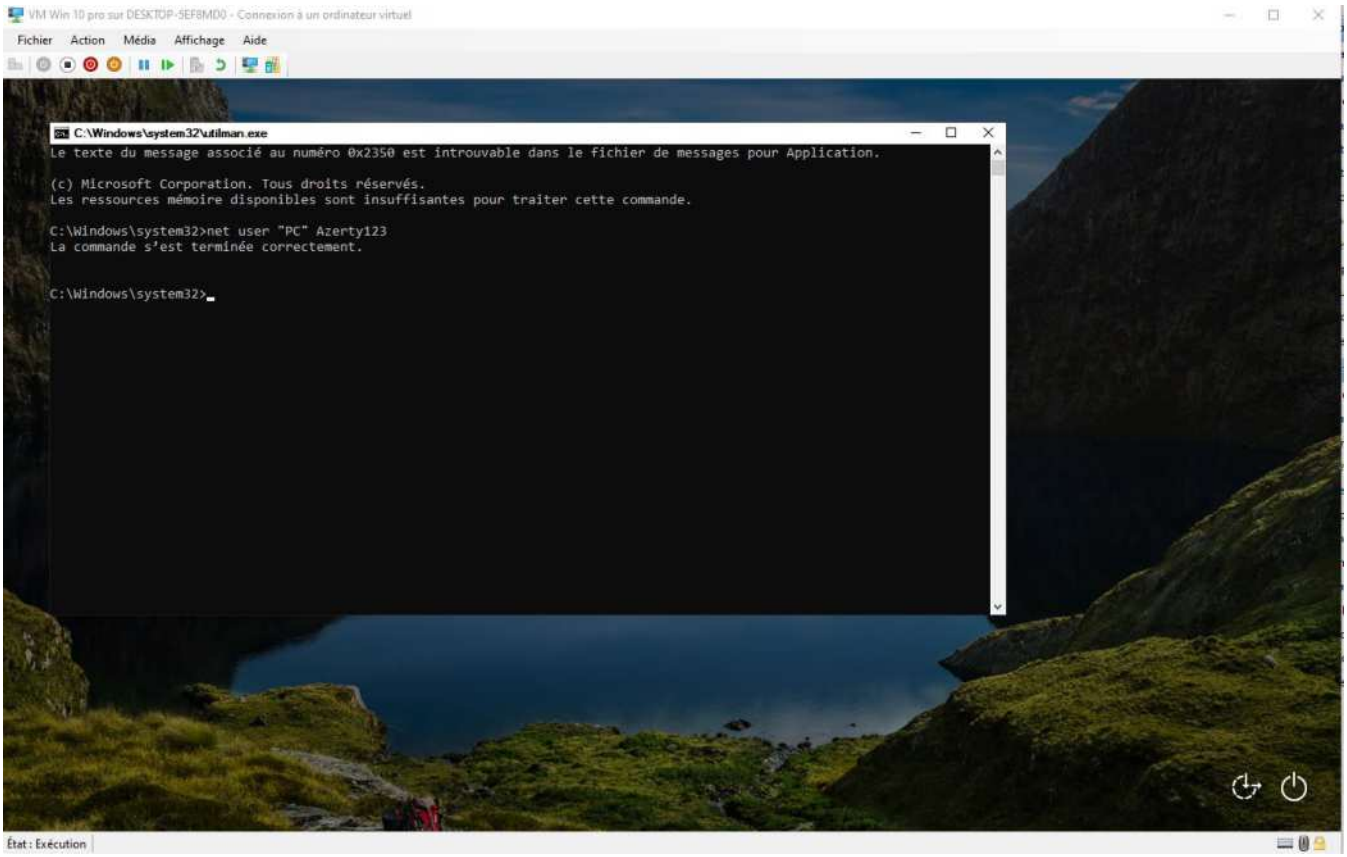
« cd /mnt/sda2 » > pour aller dans le répertoire 'sda2'

« cd Windows/System32 » pour aller dans 'System32'

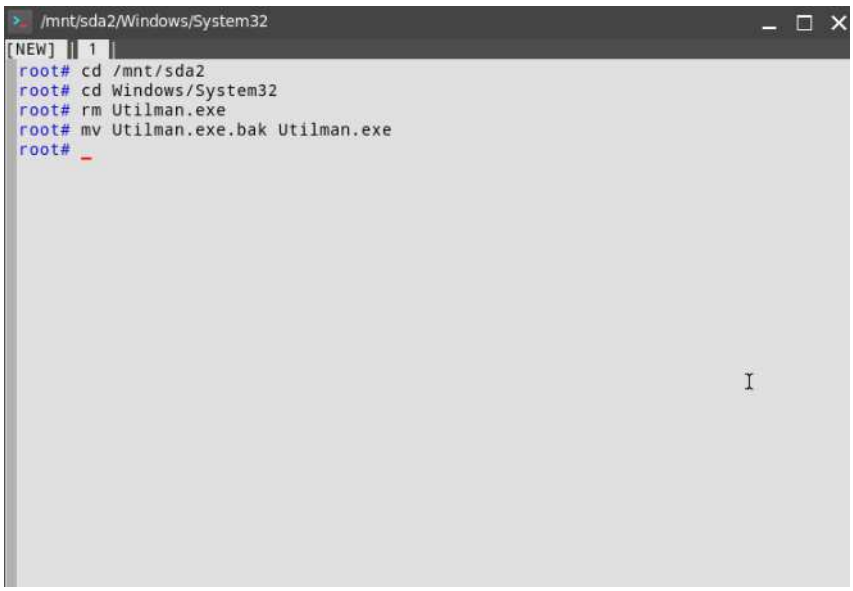
« mv Utilman.exe Utilman.exe.bak » crée 'Utilman.exe.bak' et y place 'Utilman.exe'

« cp cmd.exe Utilman.exe » copie 'cmd.exe' dans Utilman.exe.

Ceci fait on peut redémarrer notre machine et sur l'écran d'accueil appuyer sur 'ctrl + u' qui au lieu d'ouvrir l'utilitaire va ouvrir le cmd. Dans le cmd on va écrire net user « nom_d'utilisateur » (PC) nouveau_mot_de_passe (Azerty123).



Le mot de passe est maintenant changé pour celui qu'on a choisi, il ne nous reste plus qu'à remettre en place l'interface de base en repassant par puppy linux.



On ouvre la console et on écrit :

« cd /mnt/sda2 »

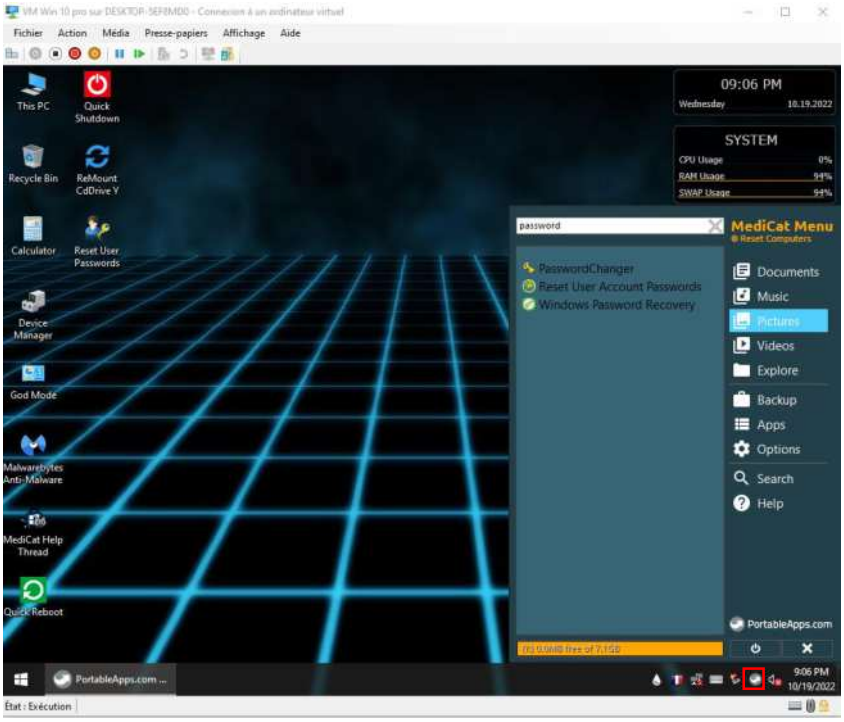
« cd Windows/System32 »

« rm Utilman.exe » supprime 'Utilman.exe'

« mv Utilman.exe.bak Utilman.exe » déplace 'Utilman.exe.bak' dans 'Utilman.exe'

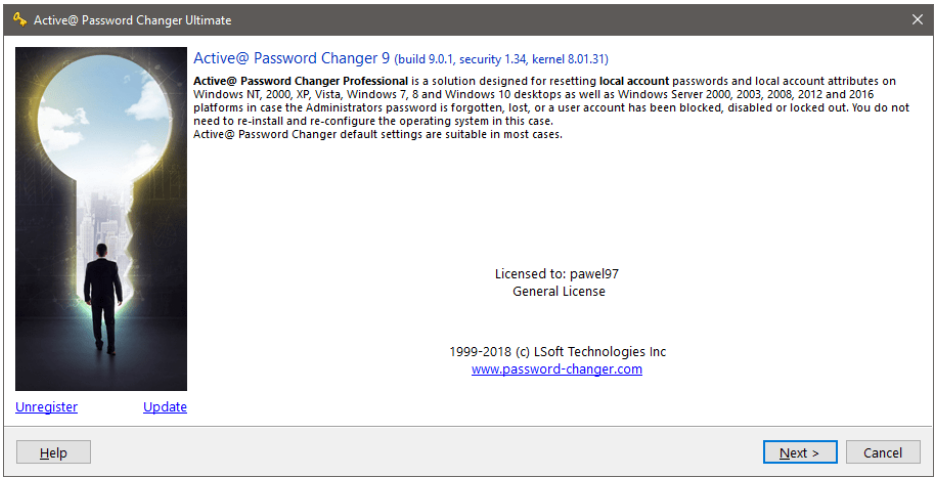
3/ Medicat

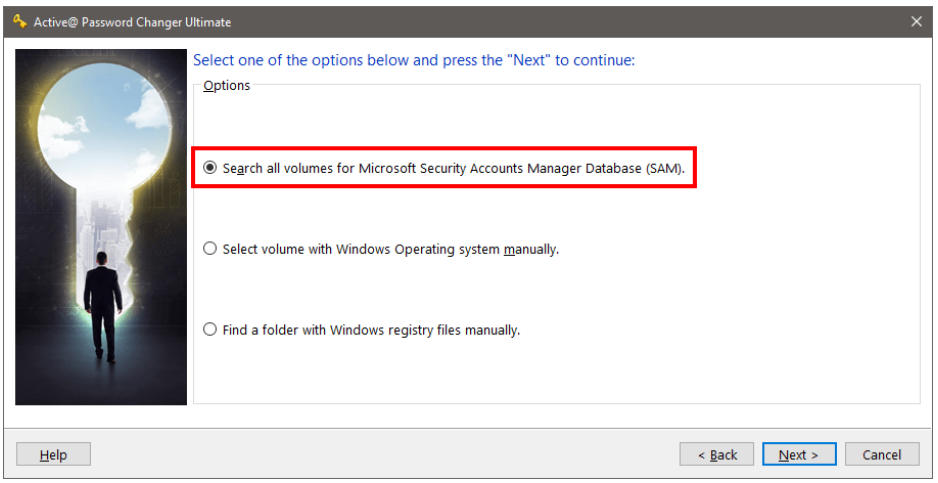
On remplace l'iso précédente par celle de Medicat puis on lance la VM.



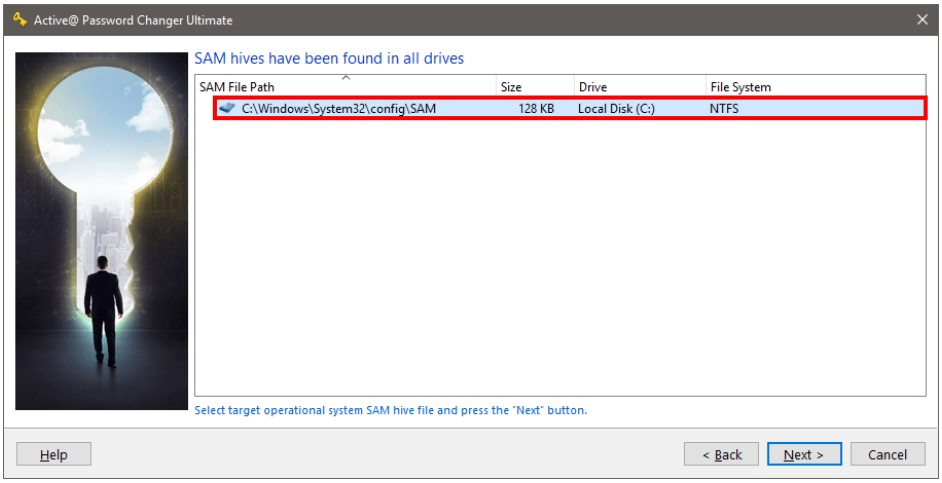
On ouvre l'utilitaire et on écrit « password » pour trouver plus rapidement les outils nécessaires au changement de mot de passe.

J'ai choisis PasswordChanger, on va donc suivre les étapes de ce logiciel.

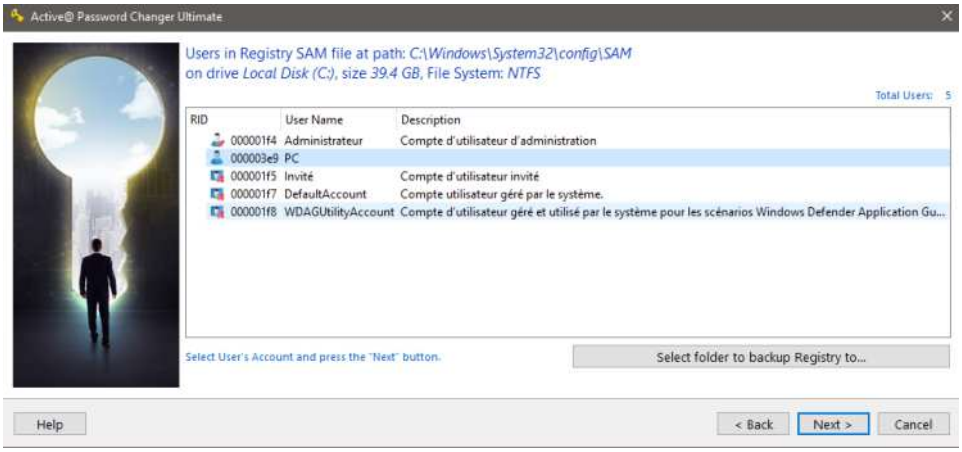




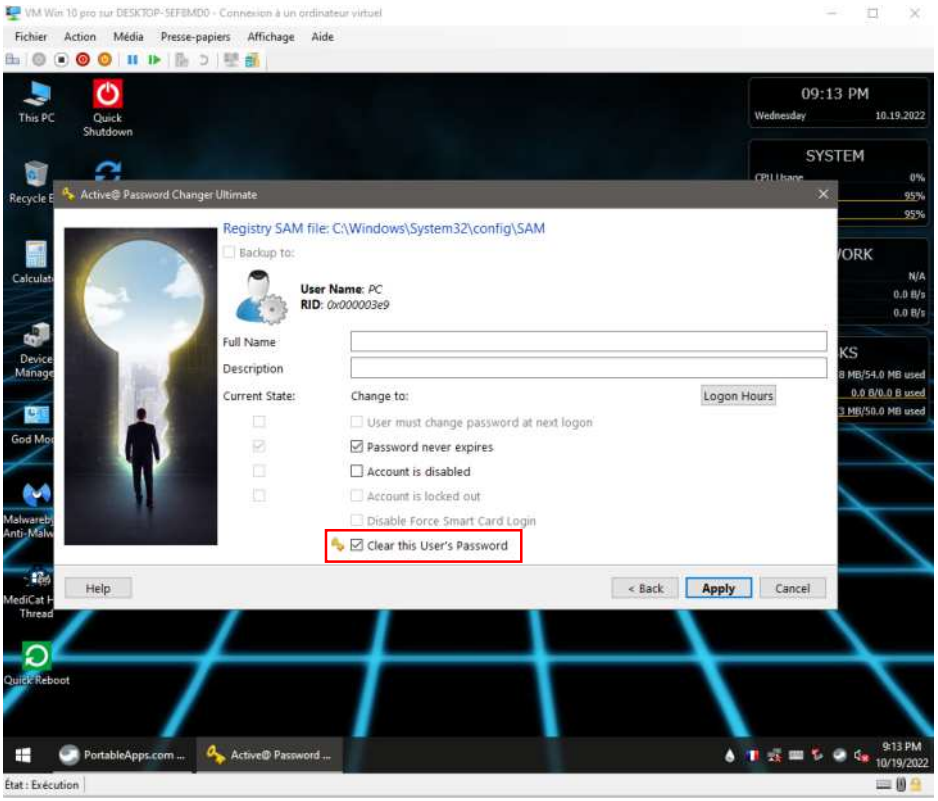
On coche la première case pour rechercher tous les volumes SAM (Security Accounts Manager).



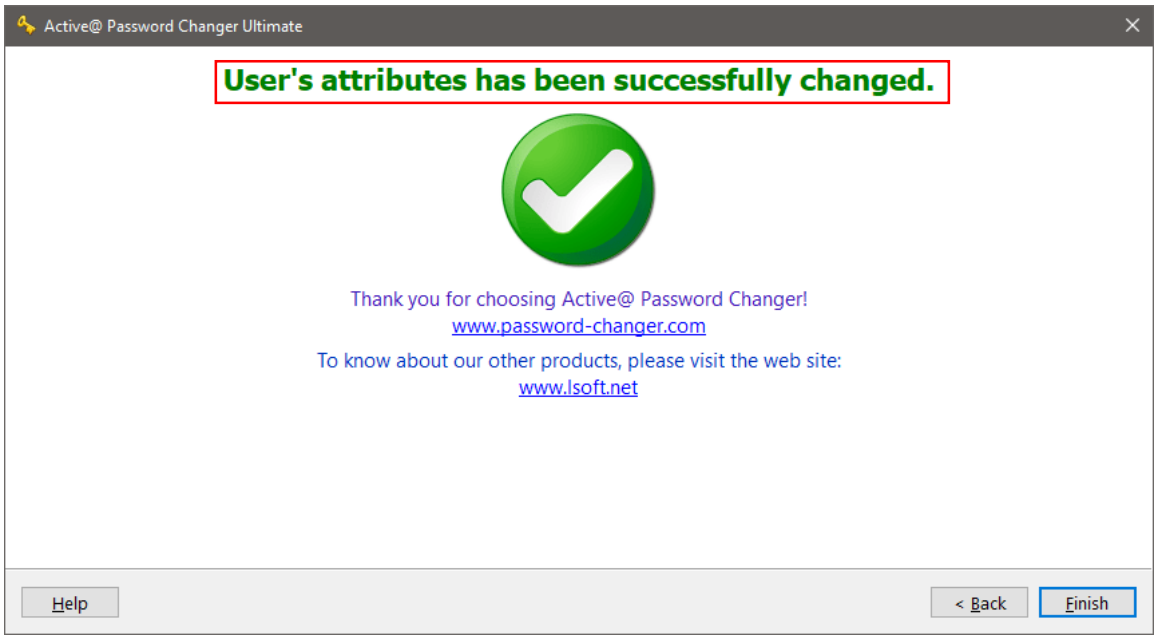
On sélectionne notre disque.



Puis notre utilisateur.



On coche « Clear this Users's Password » pour réinitialiser le mot de passe.



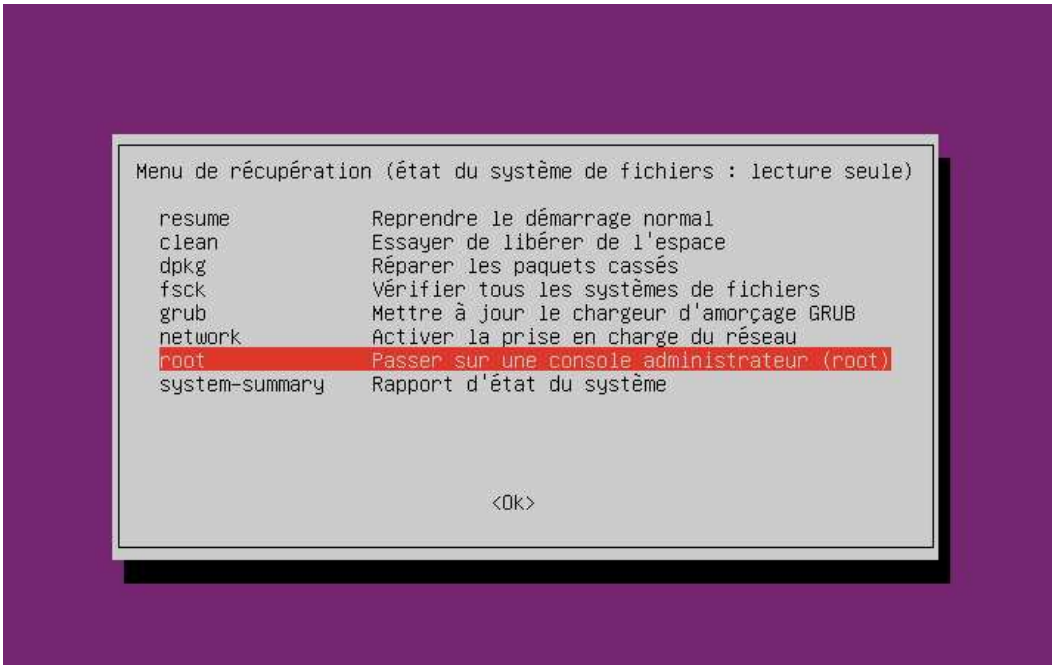
Avec ce logiciel aussi le mot de passe a pu être modifié.

Dernière partie

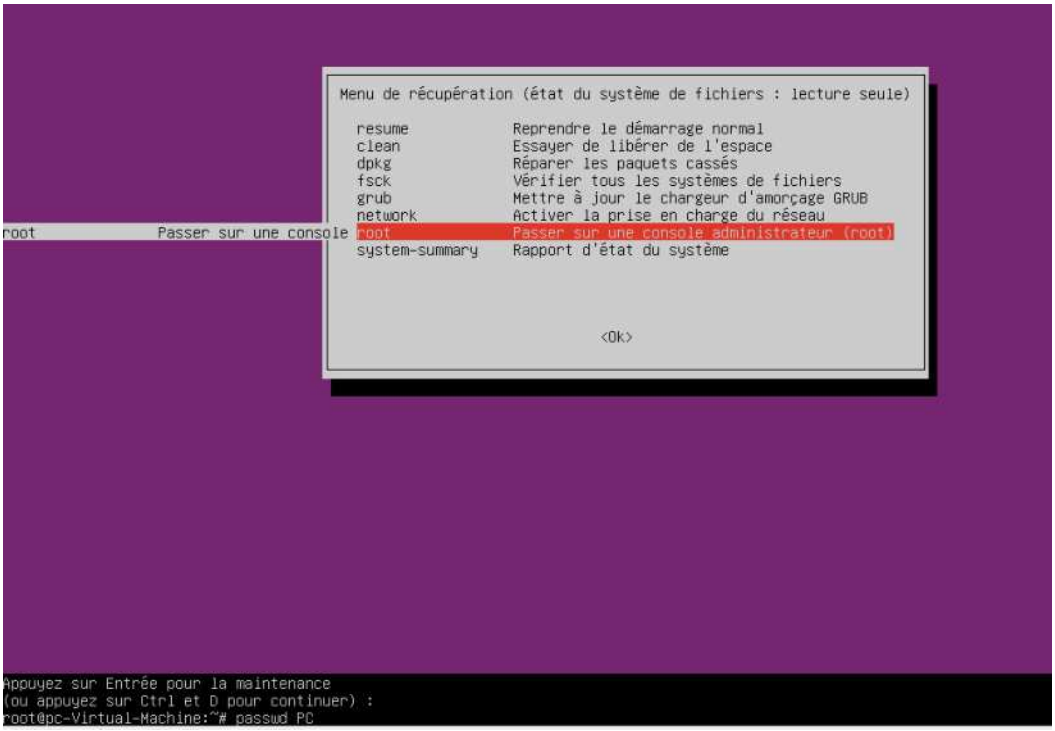
Nous avons vu qu'il était possible d'accéder assez facilement à notre session Windows en contournant le mot de passe à l'aide de différents outils, qu'en est-il de linux ?

On crée une VM avec Ubuntu (dans cet exemple Ubuntu 20.04).

Après avoir créé un utilisateur on redémarre la machine et on appuie sur « MAJ » pour entrer dans le menu grub, après avoir sélectionné « boot options » puis « restore mode » on arrive sur cette fenêtre.

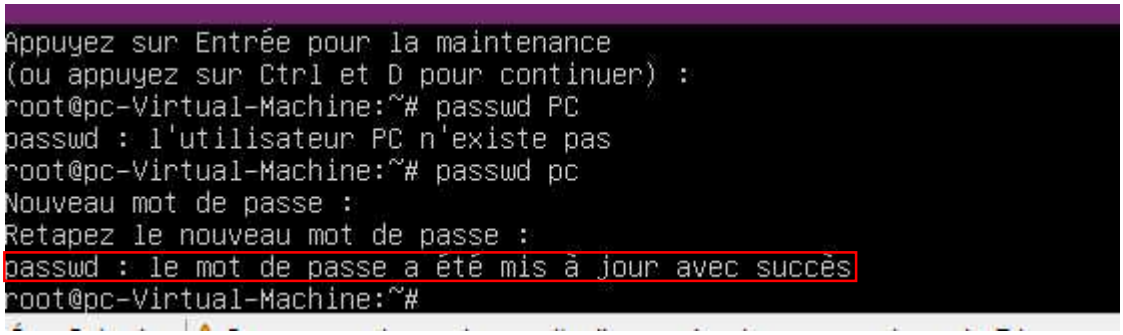


Ici on choisit « root »



On appuie sur entrée jusqu'à voir « # ».

Ensuite on écrit « passwd 'nom_d'utilisateur' » pour changer le mot de passe.



Sous linux également le mot de passe peut donc facilement être contourné.

Conclusion

On a vu au cours de ce TP qu'il était relativement simple de passer outre un mot de passe quelques soit le système en place, cependant il existe des moyens de se protéger des personnes malveillantes qui voudraient s'introduire dans votre pc, dans la vidéo d'exemple (Mr Robot) Eliott utilise la méthode deux en remplaçant le mot de passe grâce au cmd qui a pris la place l'utilitaire.

Pour se prémunir de ses dangers on peut d'abord envisager de chiffrer son ou ses disques durs pour rendre les rendre plus difficile d'accès, mais aussi choisir un mot de passe BIOS pour éviter la modification de séquence de démarrage (clé usb), et pour les attaque qui serait en mesure de contourner cette défense on peut encore désactiver les ports usb de la machine concernée pour empêcher n'importe qui de brancher une clé usb sur la machine.