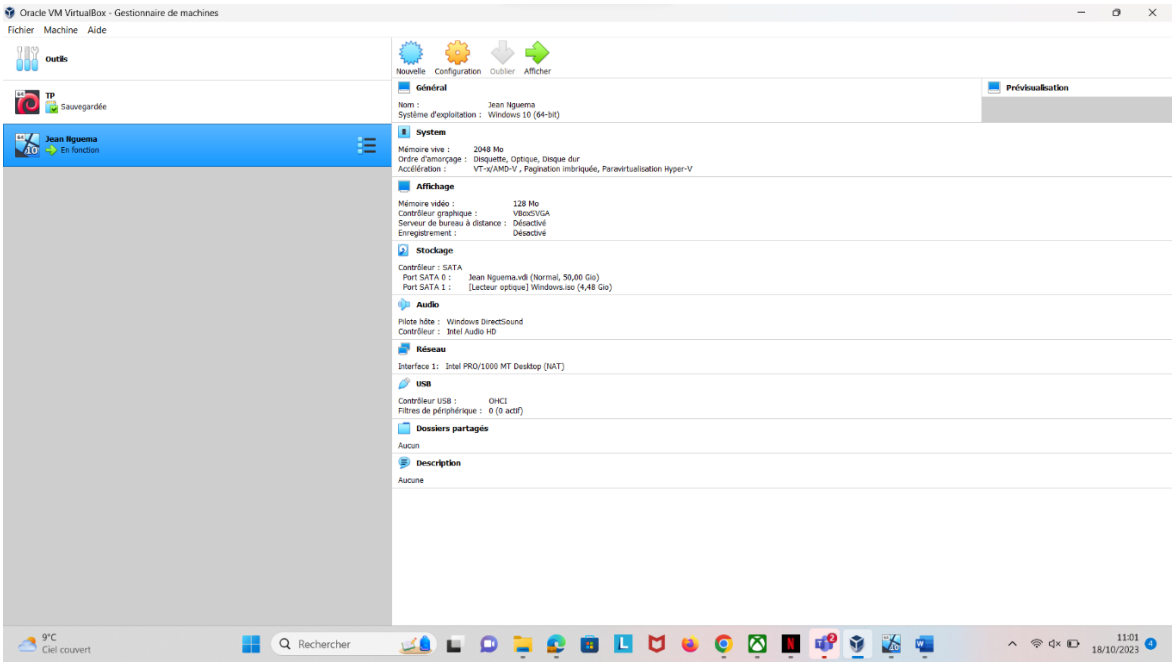
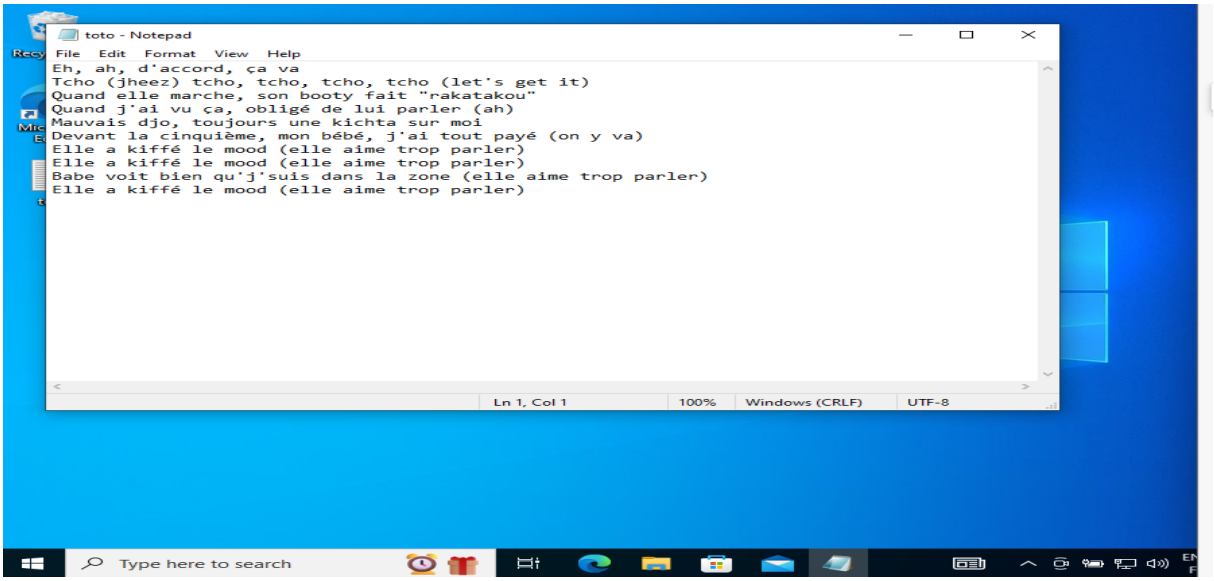
TP Intrusion simple Windows-Bloc3

Objectif : découvrir l'intérêt de sécuriser correctement une machine sous Windows et savoir se protéger en se mettant à la place de l'attaquant.

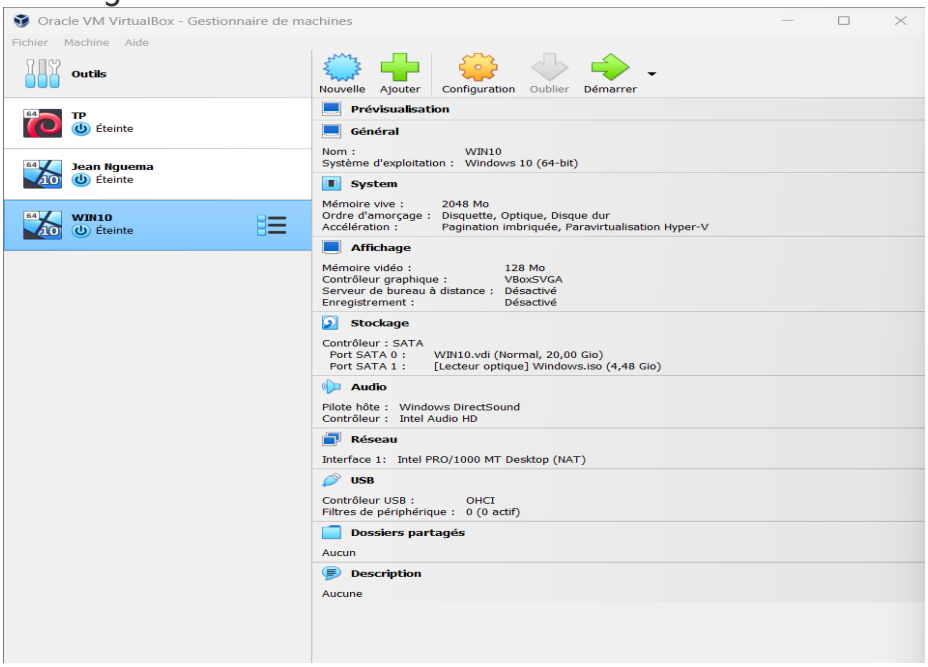
- Mettons-nous en condition ;
  - Créons une VM avec Windows 10 Pro dessus.



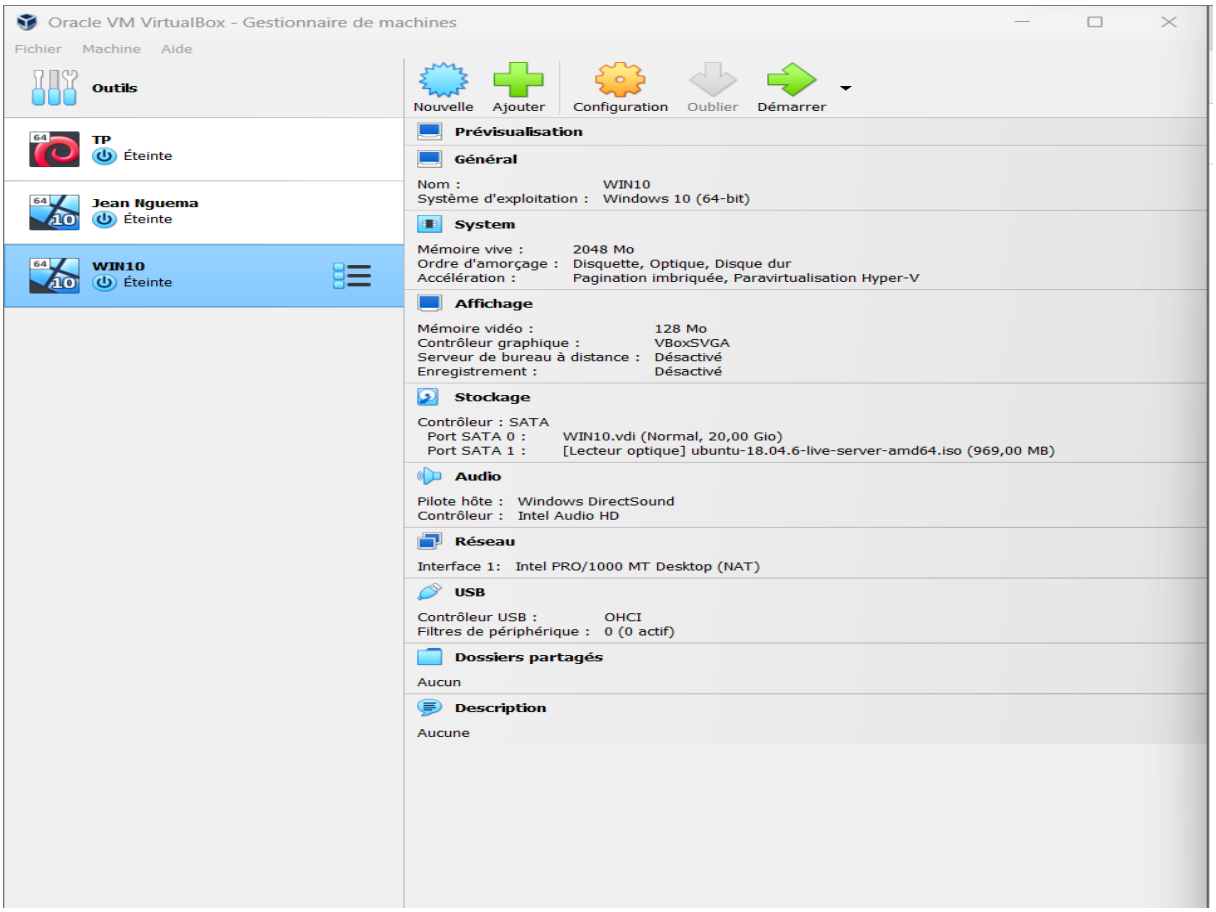
  - Nous avons bel et bien mis un mot de passe sur notre compte local administrateur et avons créer un fichier << toto.txt>> sur le bureau nous avons inséré les paroles de notre chanson préférée.



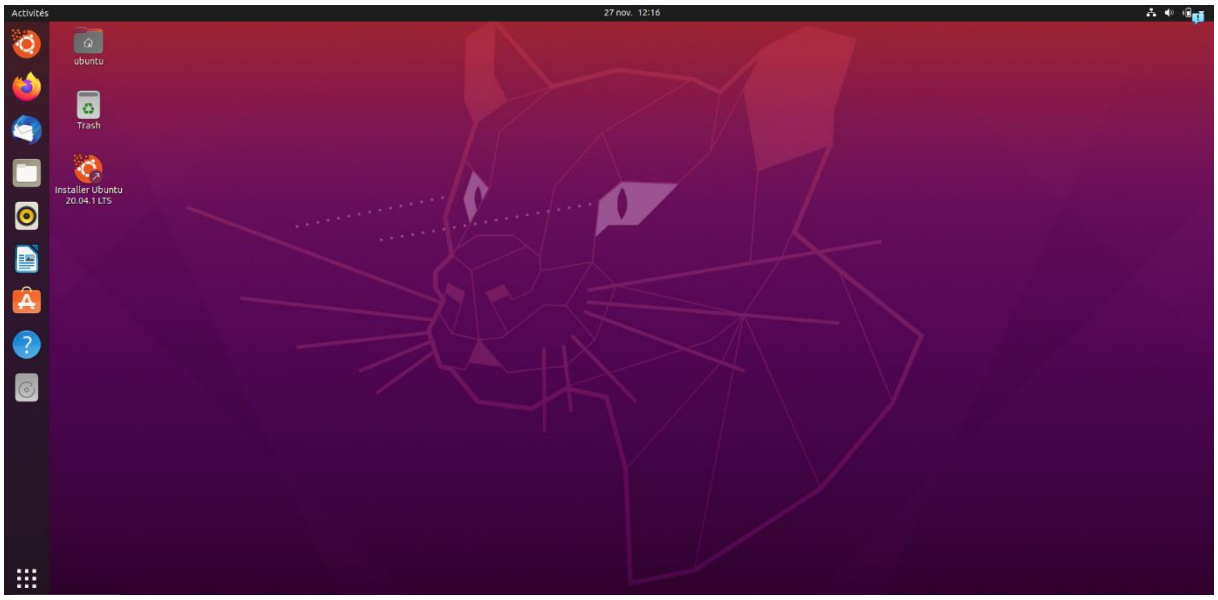
-Eteignons notre VM.

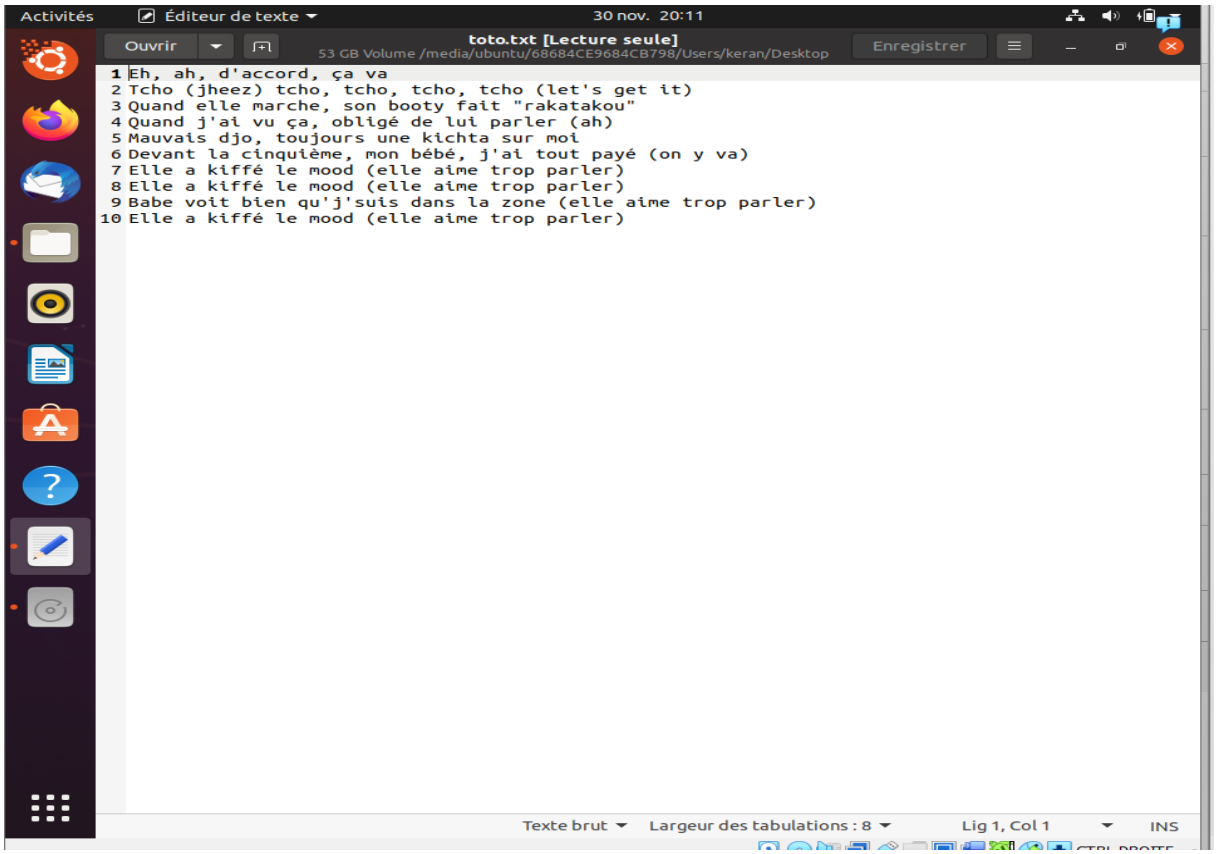


- Continuons notre expérimentation ;
  -Bouttons sur notre VM mais en utilisant une ISO de Ubunto Desktrop cette fois.



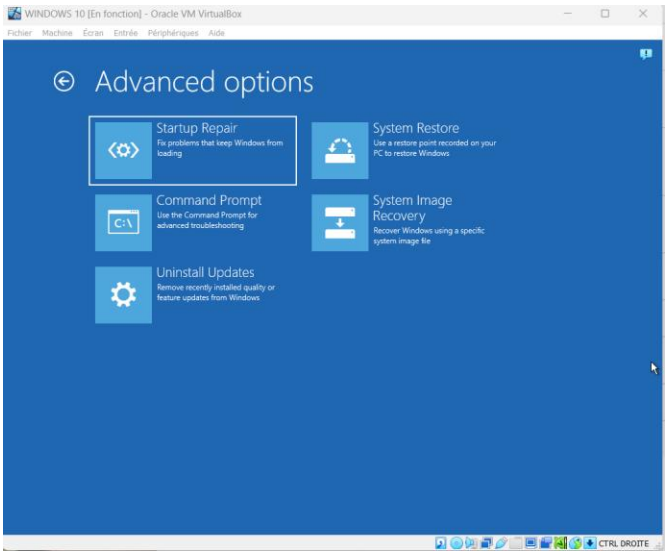
-Démarrons en mode live-DVD (<<essayer Ubuntu>>) et tentons d'accéder au fichier <<toto.txt>>



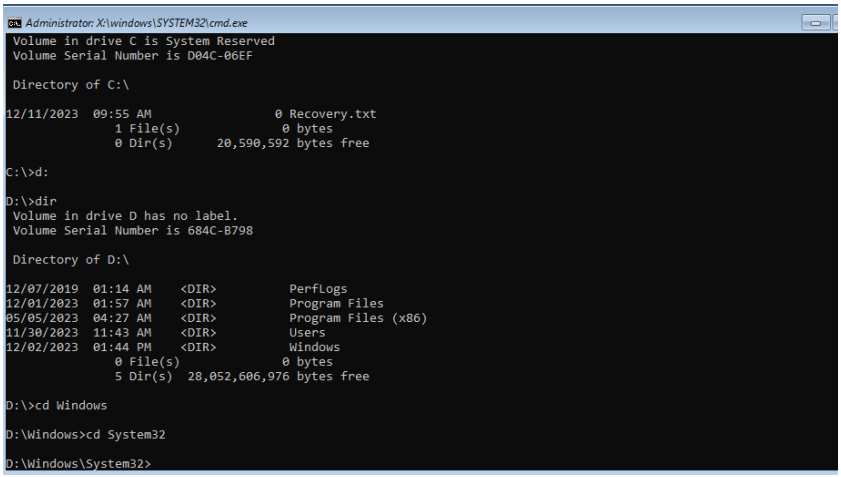


- A l'aide de l'ISO Ubuntu nous avons démarré en mode live DVD (<<Essayer Ubuntu>>) et nous avons pu accéder à notre fichier toto et il est également possible de modifier le fichier.

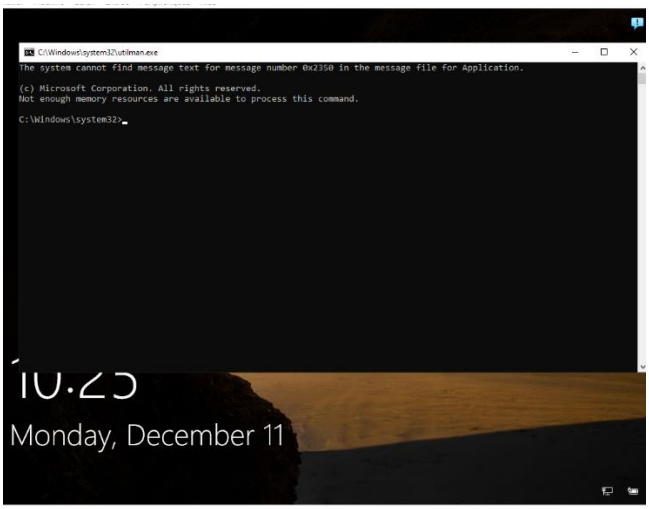
- Essayons autre chose ;
  -A l'aide de ce lien https://lecrabeinfo.net/reinitialiser-mot-de-passe-compte-utilisateur-local-windows.html choisissons l'une des techniques et expérimentons là pour voir si effectivement ce serait aussi simple que cela.

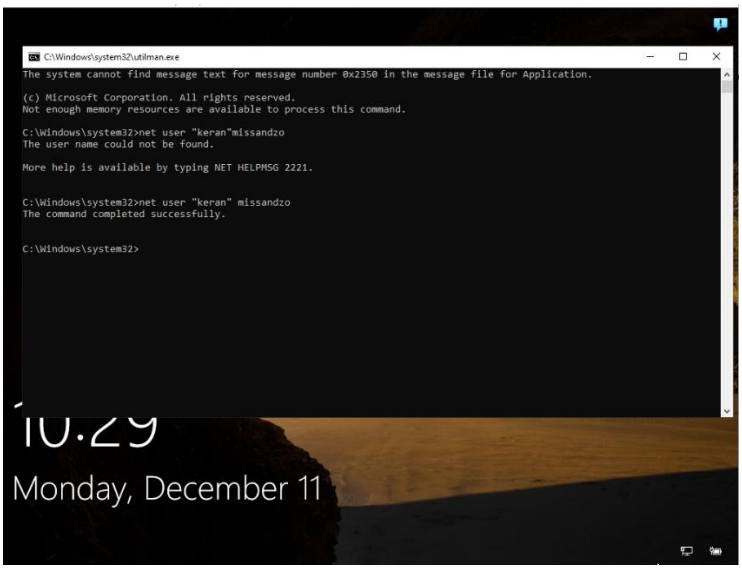


*A ce niveau nous rentrons dans les commandes avancées afin de pouvoir indiquer des commandes.

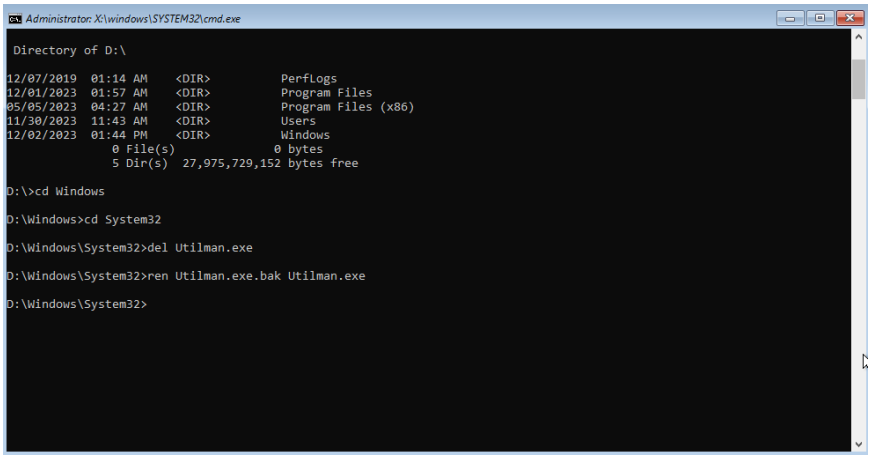


-Nous suivons le cheminement en introduisant des commandes.





-A ce niveau nous pouvons alors modifier le mot de passe de l'utililsateur.



_Chose faite, nous pouvons redémarrer la machine et introduire le nouveau mot de passe.

- Alors après avoir expérimenter la méthode 2b, nous pouvons donc en déduire qu'elle est très similaire à celle de la vidéo évoquée en introduction.

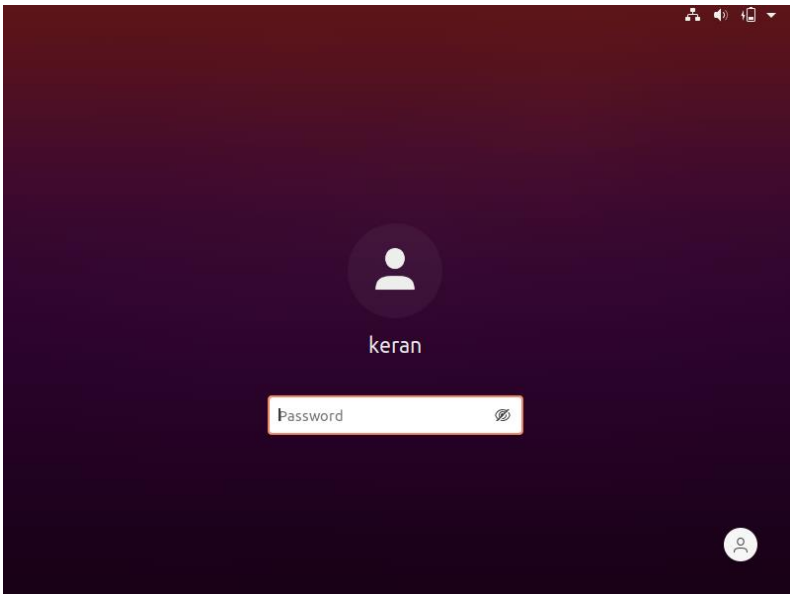
- Enfin ;

- En vue de la facilité avec laquelle nous avons pu enfreindre Nous la sécurité dans un Windows, de ce fait, on peut en conclure que la sécurité avec un system Windows reste toujours un souci majeur et doit être une des priorités pour ces derniers afin de mieux à point ce souci.

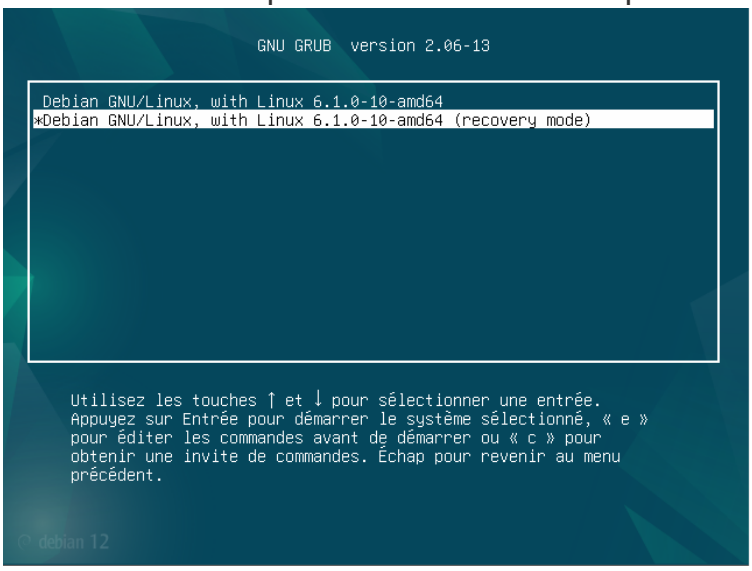
- Nous pouvons se protéger de ce problème tout d'abord en faisant fréquemment nos mises à jour, puis éviter des virus.

- Reprenons le fil de ce TP avec une machine linux et voyons ensemble si nous avons la même défaillance.

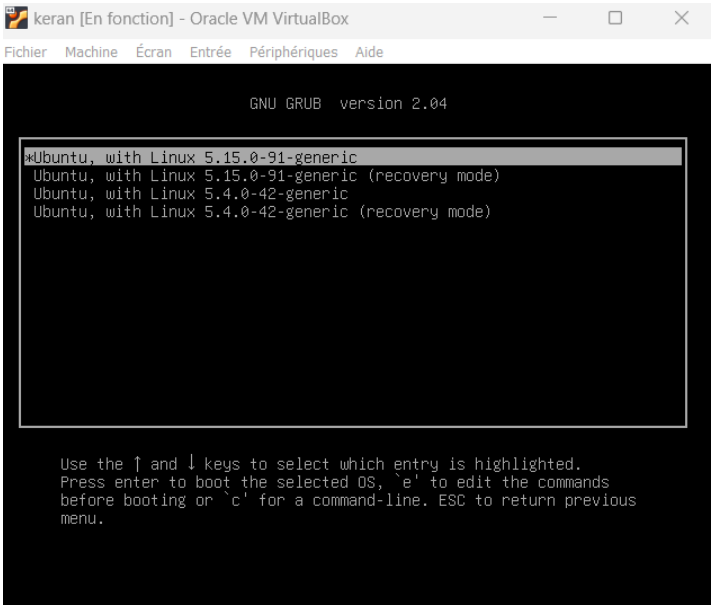
*Commençons par créer une machine virtuelle Linux .



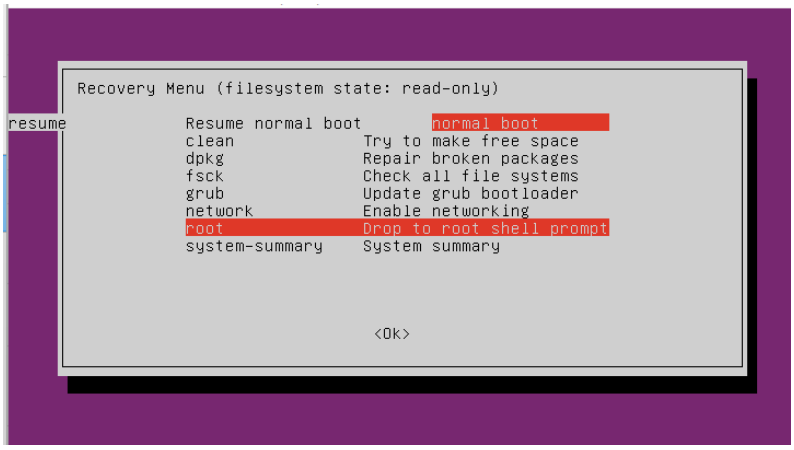
*Puis utilisons le touche MAJ ou Echap au démarrage de la VM, cela ouvre le menu Grub et va nous permettre d'accéder aux options avancées.



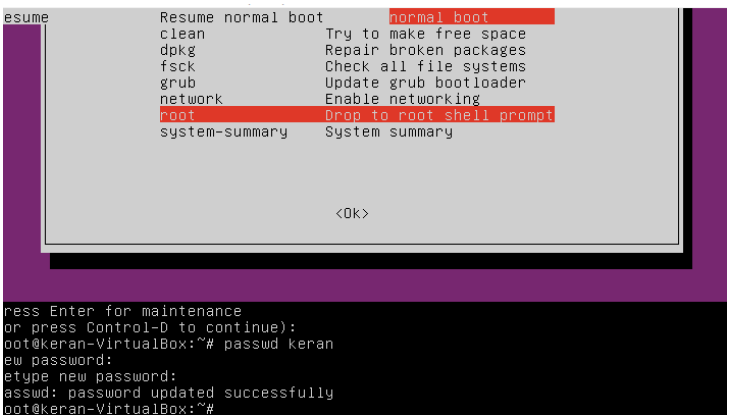
*Puis rentrer dans le mode de reécupération.

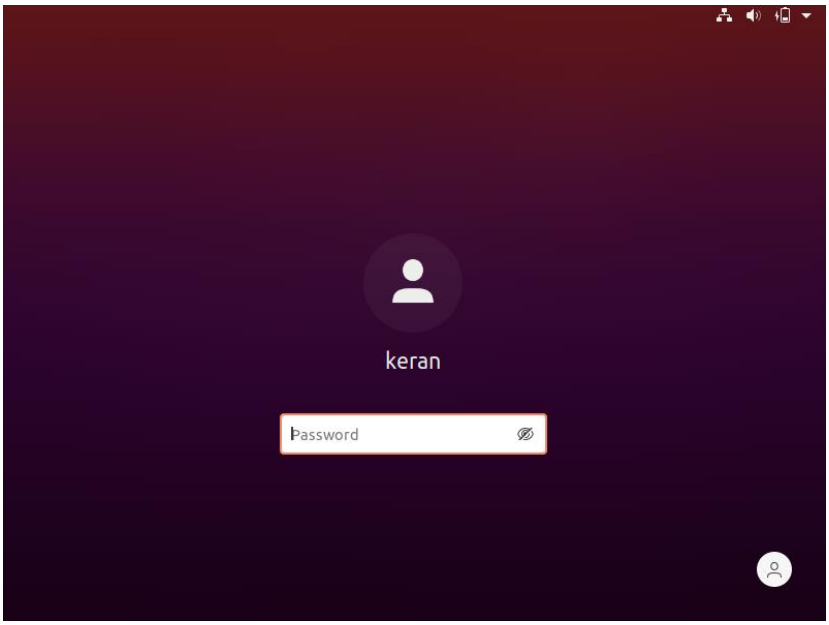


*Puis on arrive on se met en root pour ouvrir la console en administrateur.



*A ce niveau on va utiliser la commande **passwd** suivi de l'utilisateur pour changer son mot de passe. Et pour finir taper la commande reboot pour redémarrer la machine virtuelle.





- Par conséquent, nous pouvons constater que nous retrouvons le même souci sur un Linux.