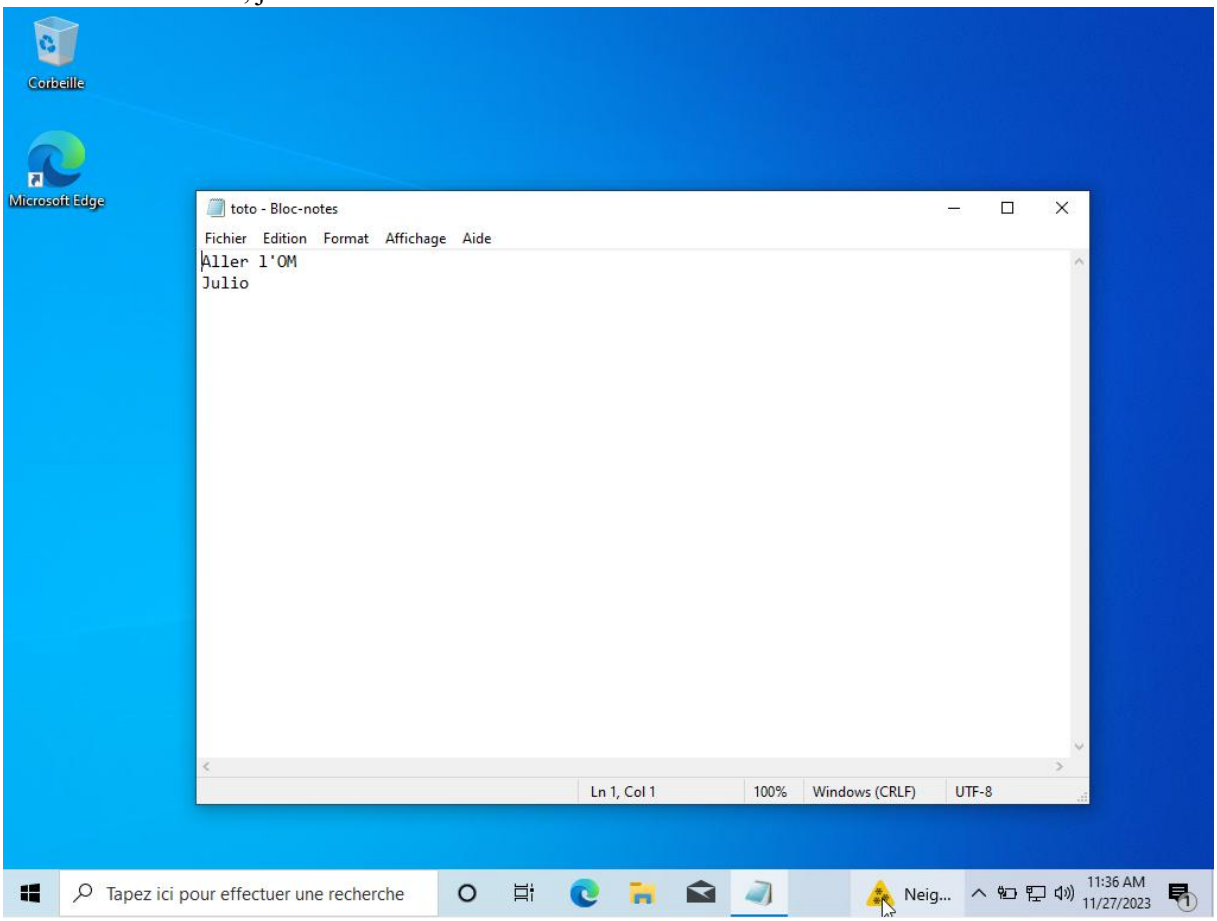
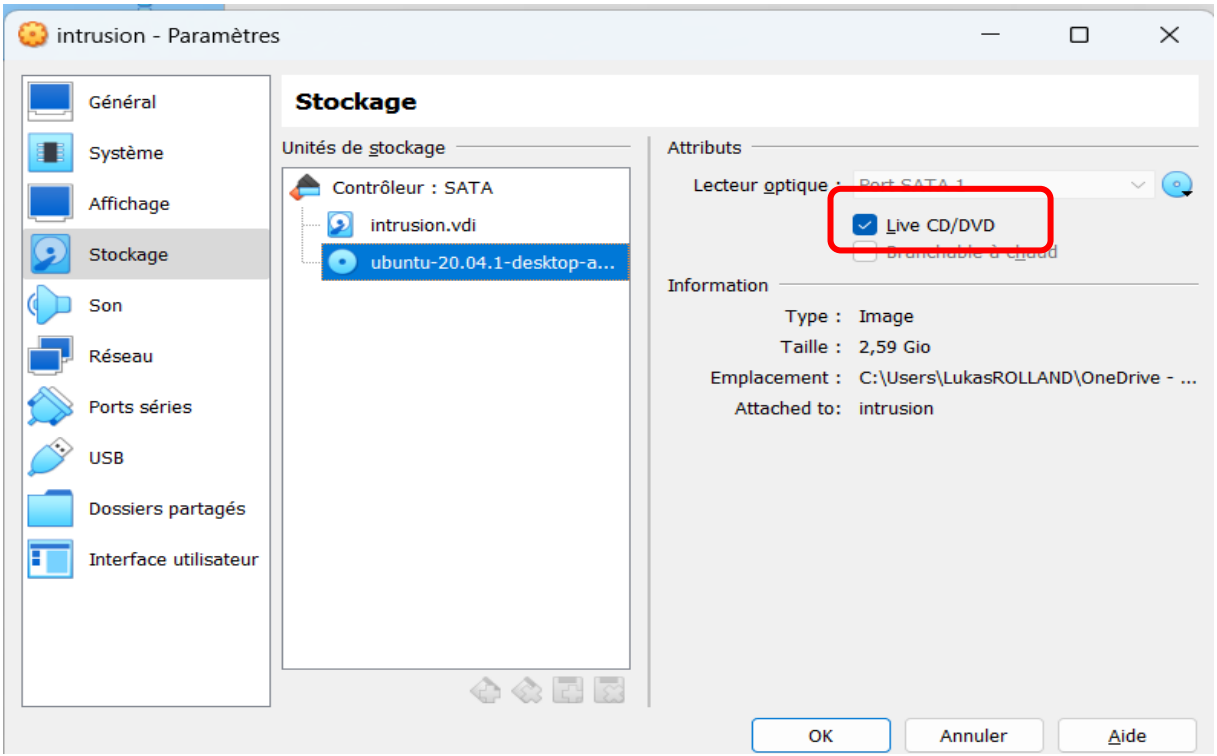
TP2 : Intrusions

Tout d'abord, nous avons installée l'ISO de Windows 10, puis nous avons donc créée une Machine Virtuel sous Windows 10.

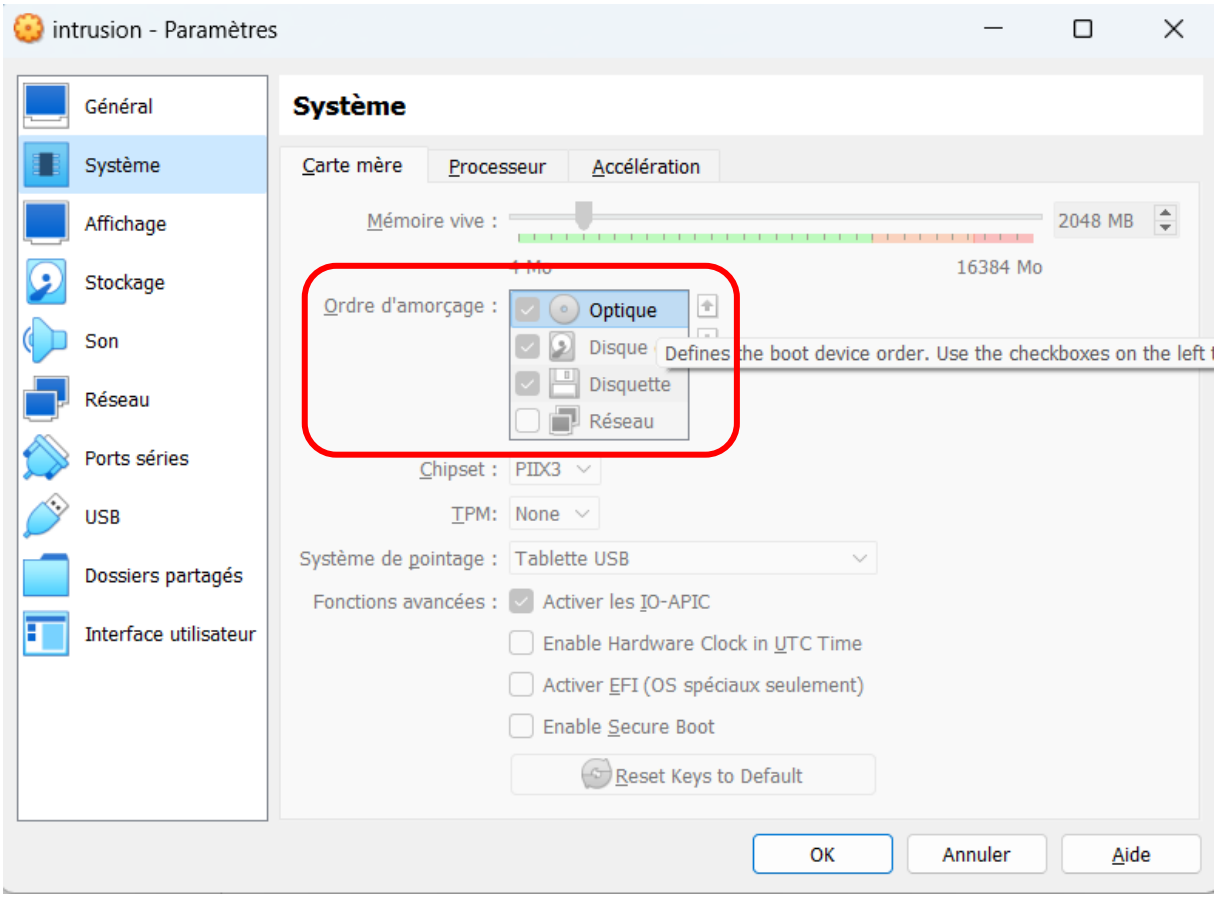
Une fois la VM crée, j'ai créé un document toto.txt



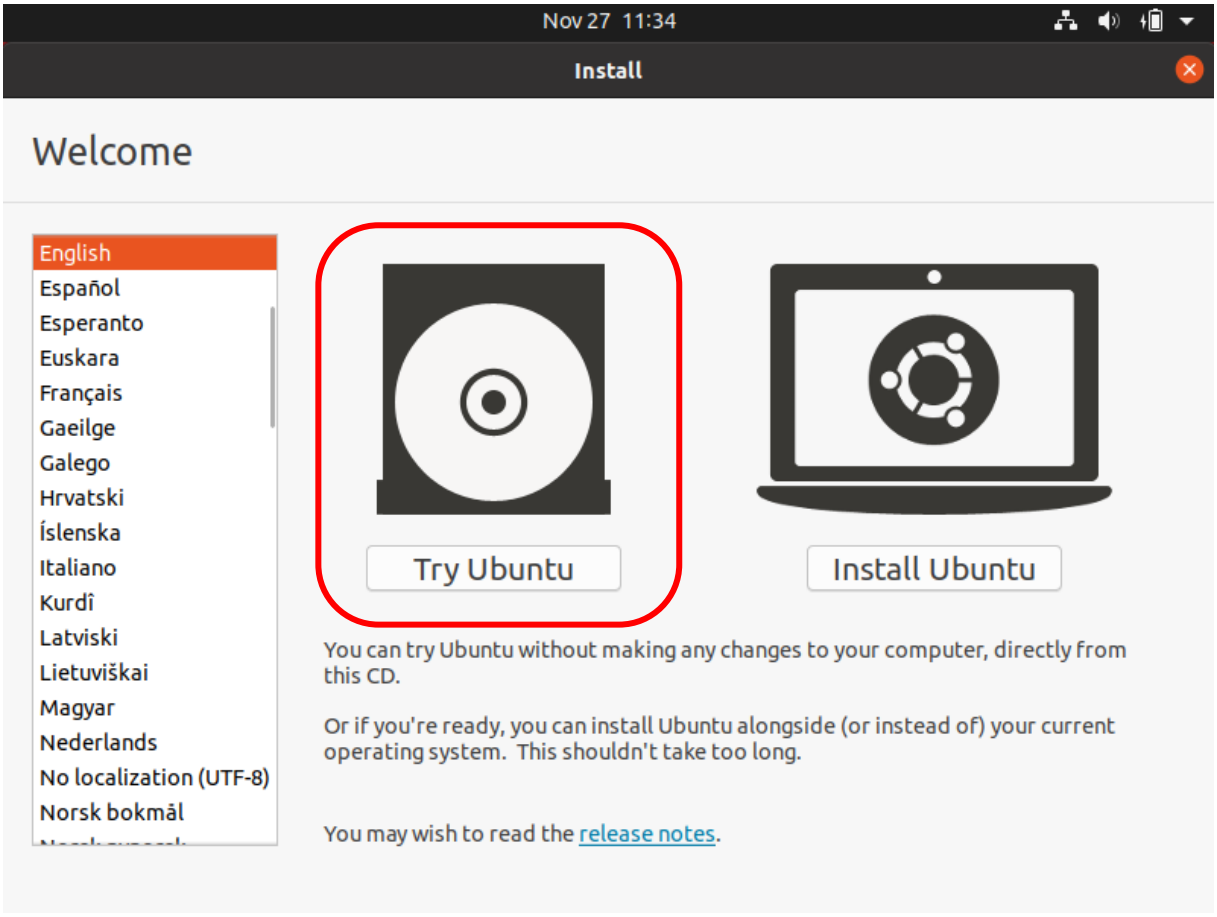
Après cela, j'ai éteint la VM pour ensuite la booter avec une ISO Ubuntu Desktop, et j'ai cocher « Live CD/DVD »



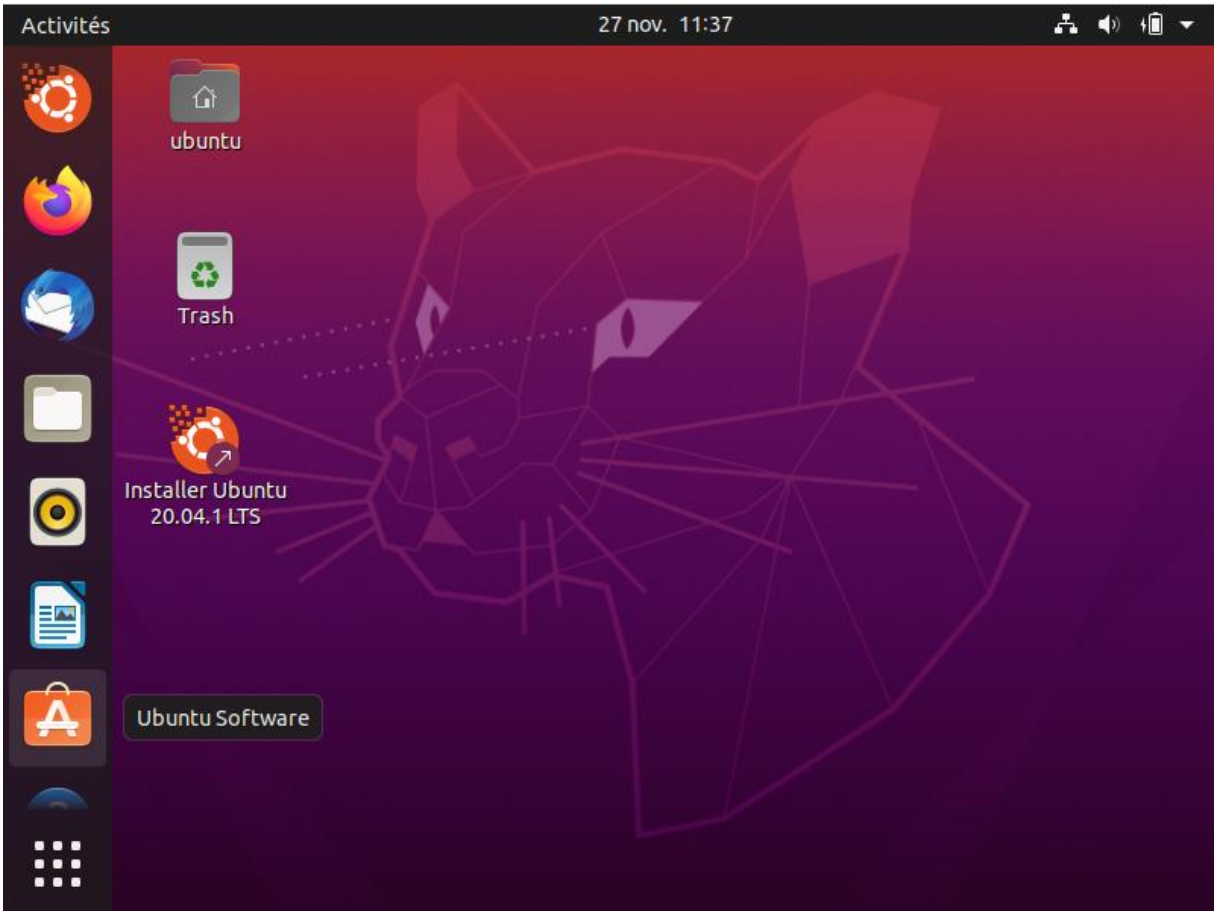
En suite j'ai dû forcer l'ordre de démarrage des disques pour que l'ISO Ubuntu se lance en premier.



Une fois Ubuntu lancé, il faut lancer et non installer.



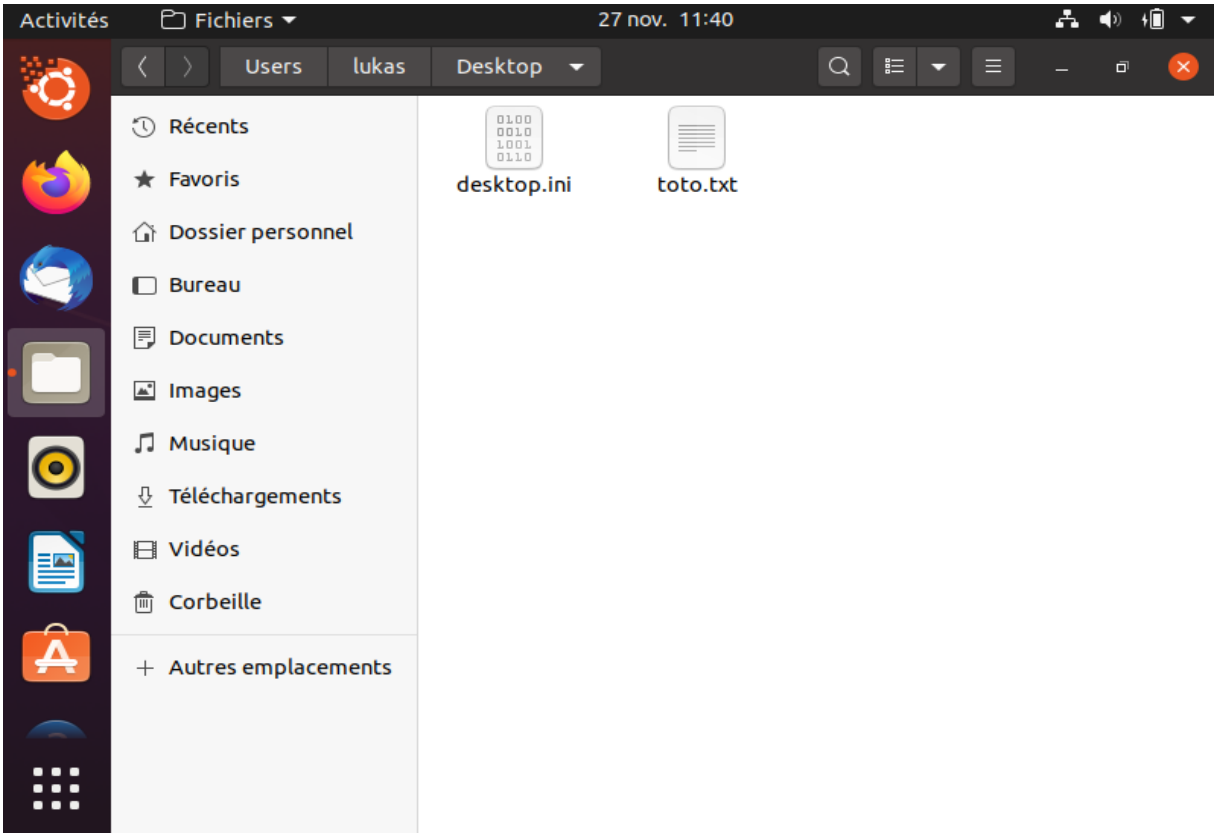
Après, il faut chercher le fichier toto.txt



Pour trouver le fichier j'ai suivi le chemin suivant :

Autre Emplacements/30GB volumes/User/Lukas/Desktop

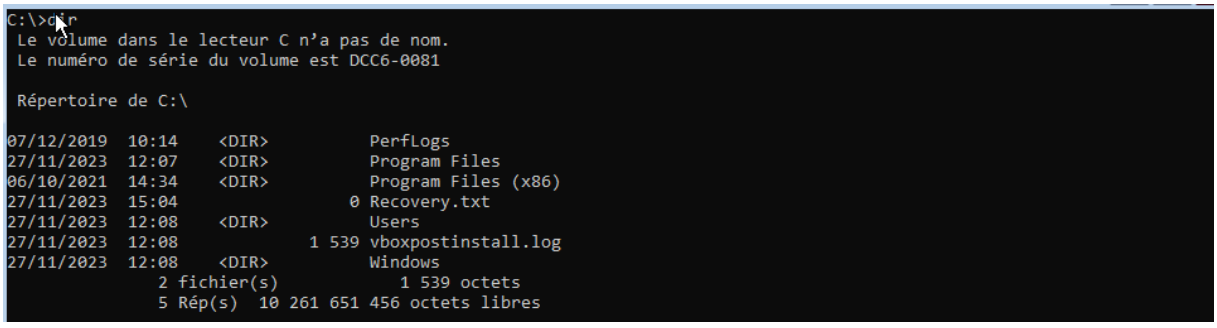
Nous avons donc accès au fichier créé depuis Windows au début.



Et il est aussi possible de l'ouvrir pour voir son contenu.

Maintenant essayons de changer le mot de passe du compte :

Une fois dans l'invite de commande, je suis aller dans le lecteur C : en faisant « C : » puis j'ai fait un « dire » pour voir si c'était le bon lecteur, et comme vous pouvez le voir c'était le bon puisqu'il y a les répertoires Windows.



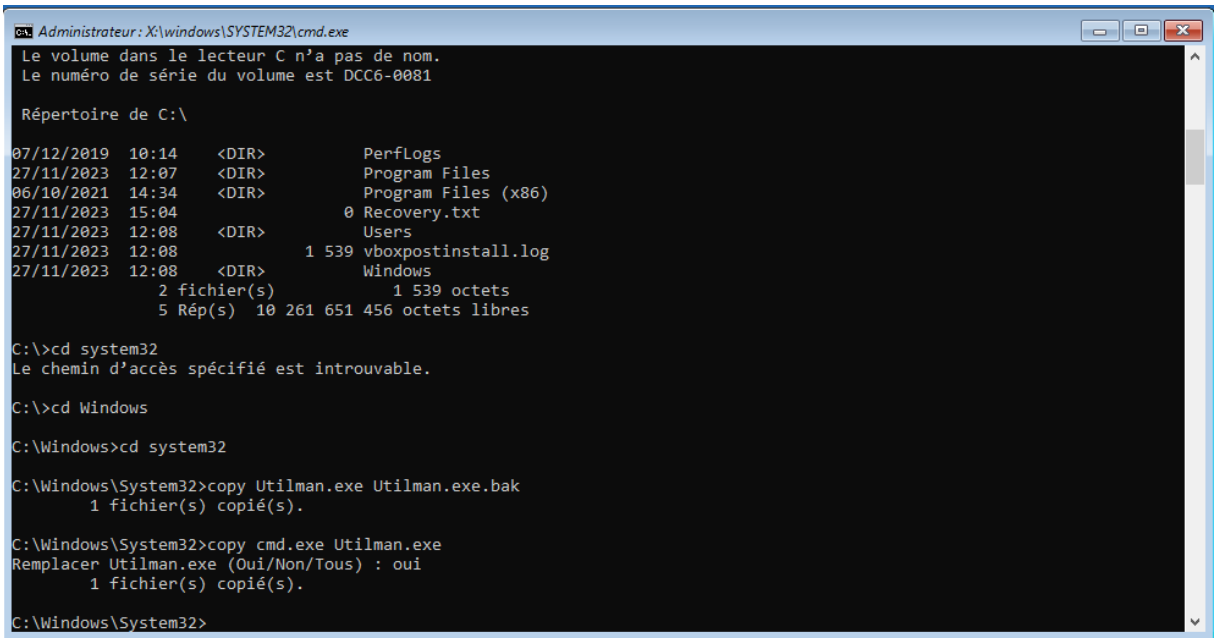
En suite j’ai fait les commandes donner dans le site internet lecrabinfo :

Cd system32 (sert à se rendre dans le fichier system32)

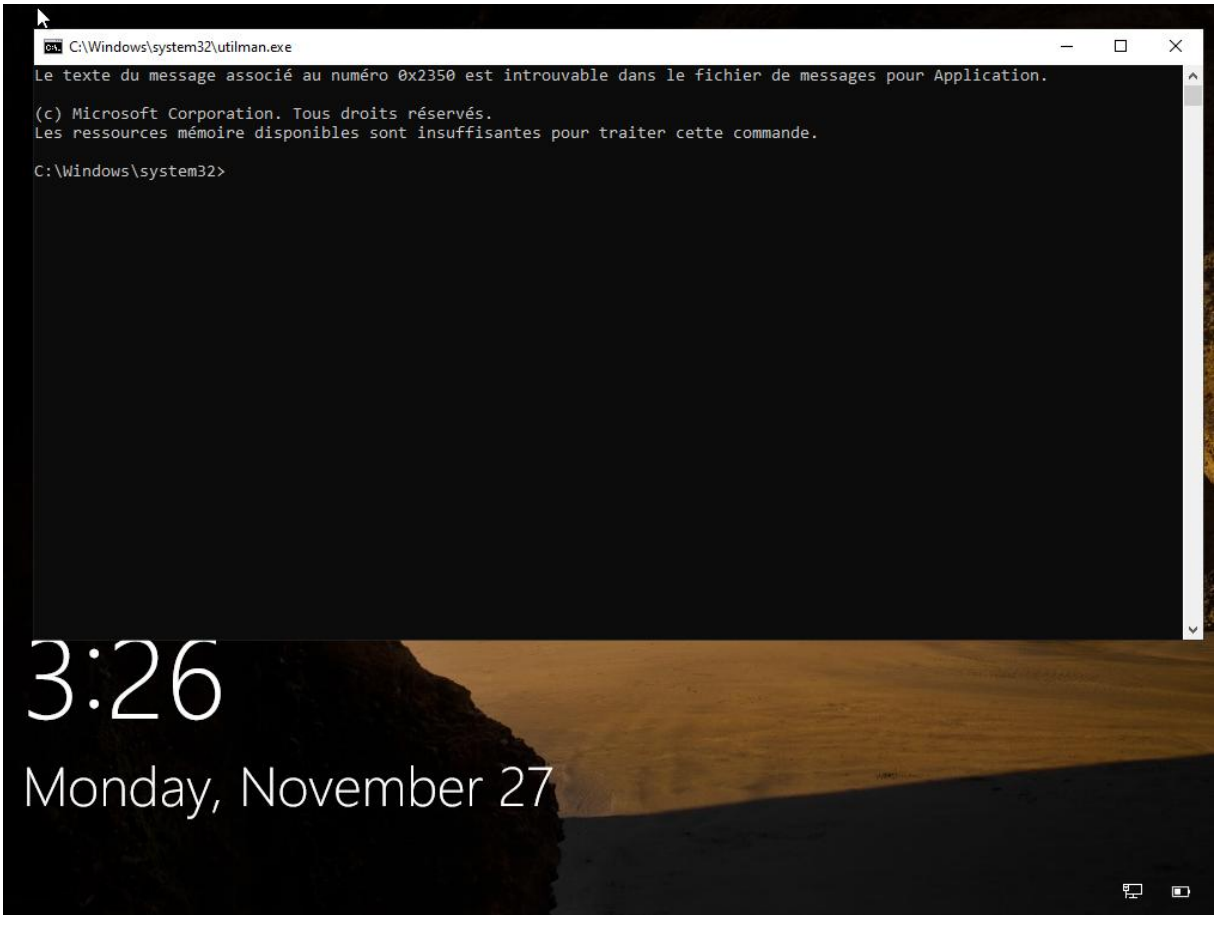
Cd Windows (sert à se rendre dans le fichier Windows)

Copy Utilman.exe Utilman.exe.bak (crée une sauvegarde du fichier Utilman.exe)

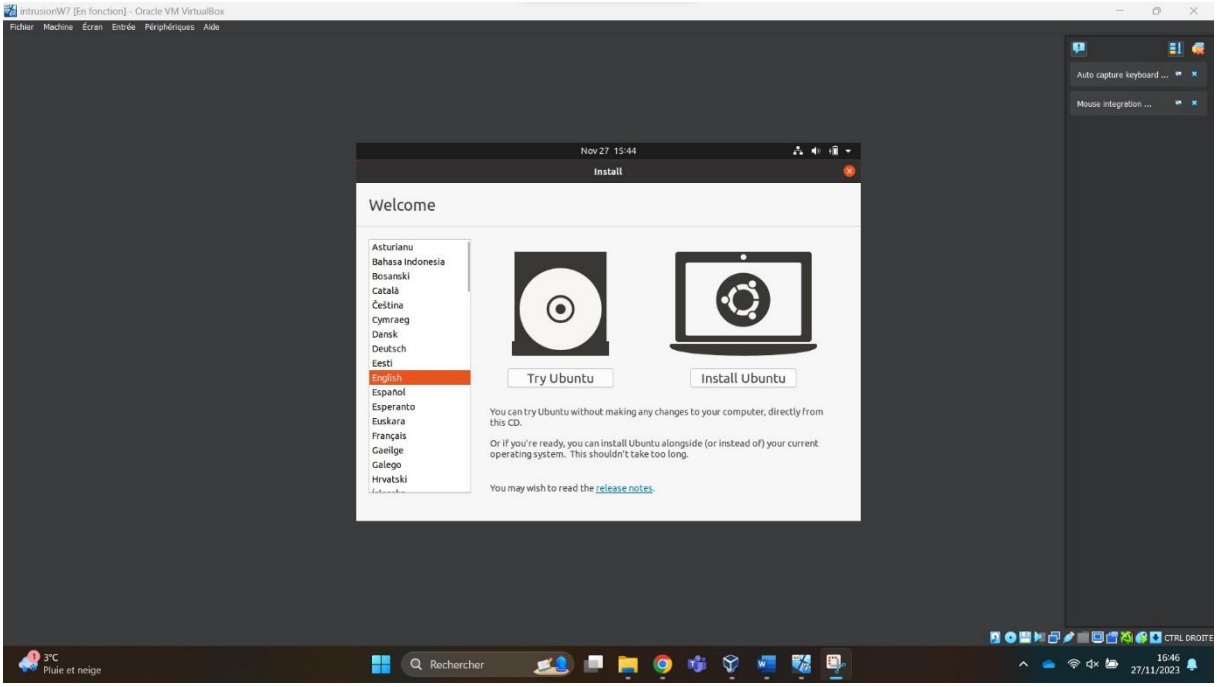
Copy cmd.exe Utilman.exe.bank (remplace les options d’ergonomie utilman.exe par l’invite de commandes cmd.exe)



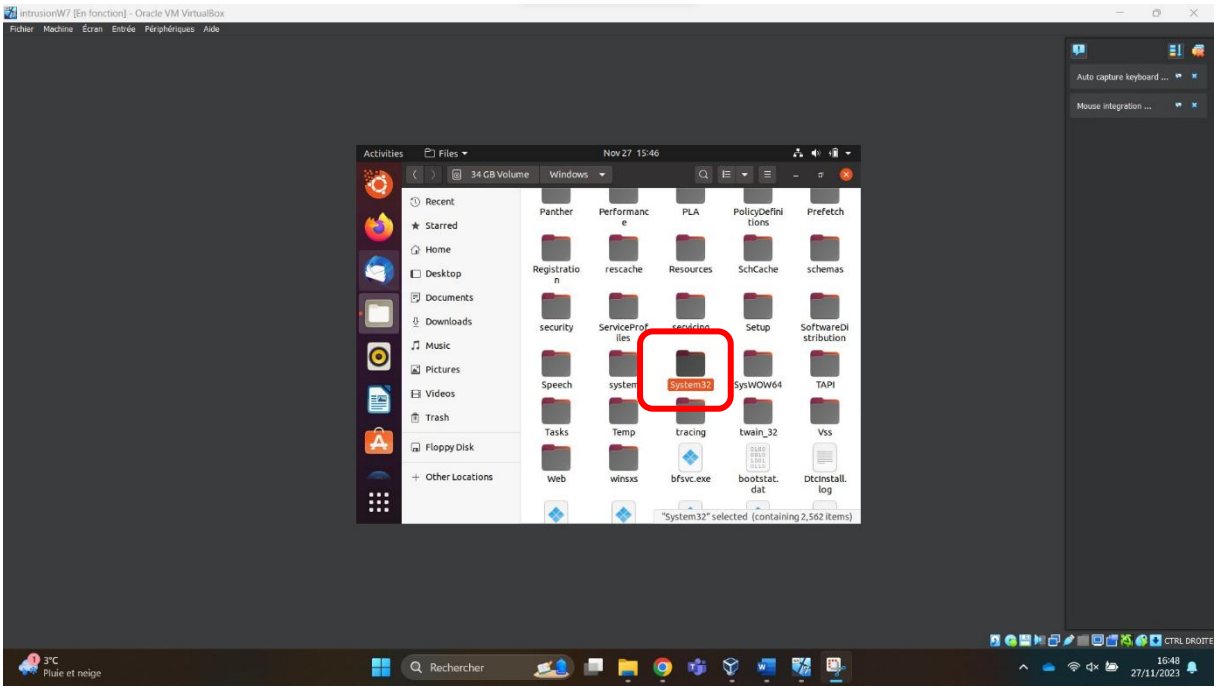
En suite j’ai dû redémarrer ma VM plusieurs fois pour pouvoir accès à l’invit de commande en faisant WIN+U



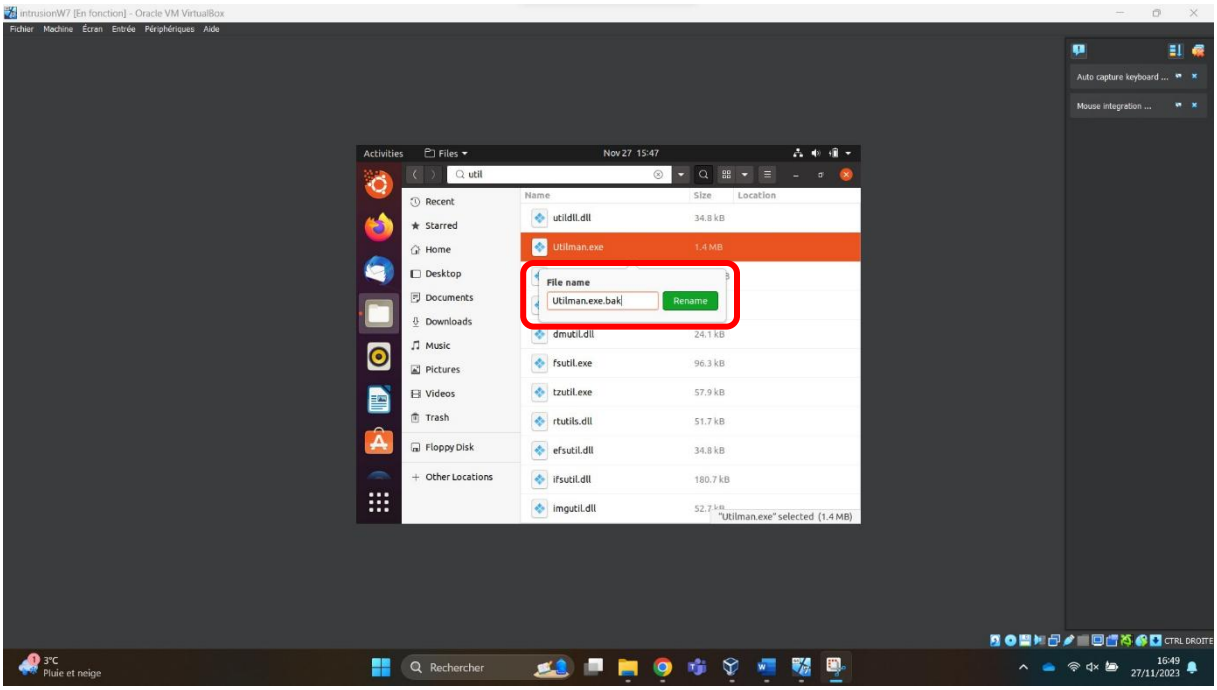
A chaque fois que le cmd se lancé, il se referme directement après dû à Windows defender. Donc nous allons re essayer avec Windows 7. Donc j'ai installé une ISO pour Windows 7, j'ai créé une VM. Pour cette version de Windows, il faut mettre un ISO ubuntu et le lancer :



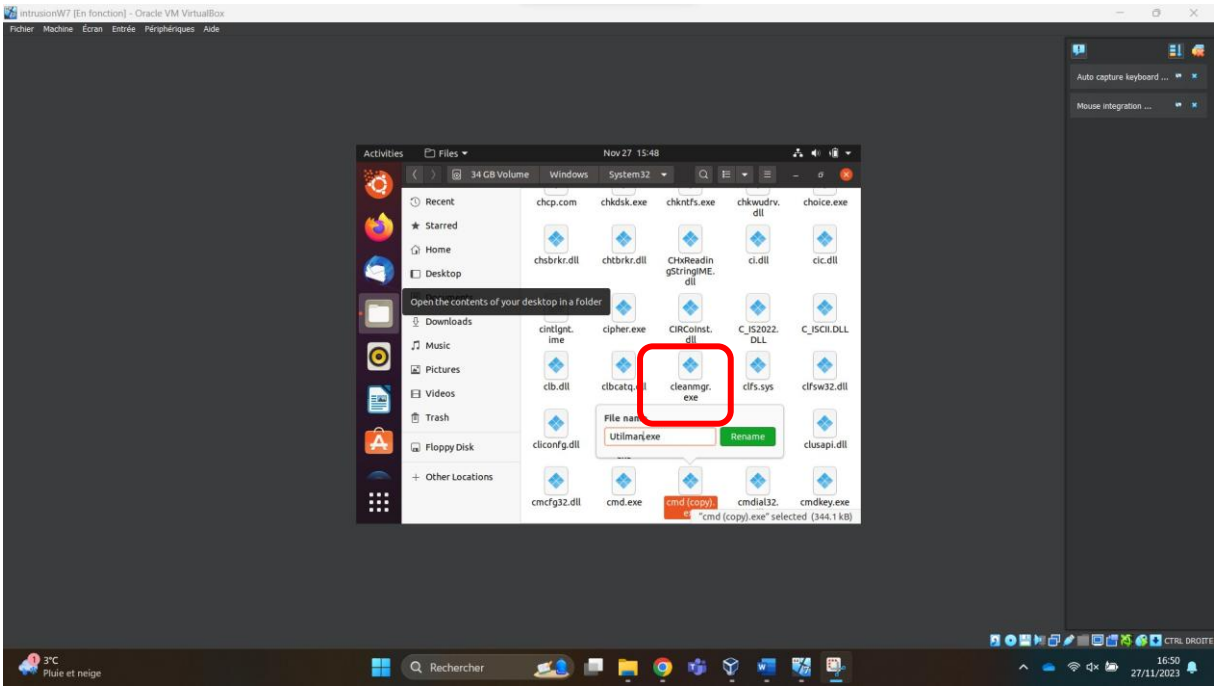
En suite aller dans le fichier « Windows » puis « system32 »



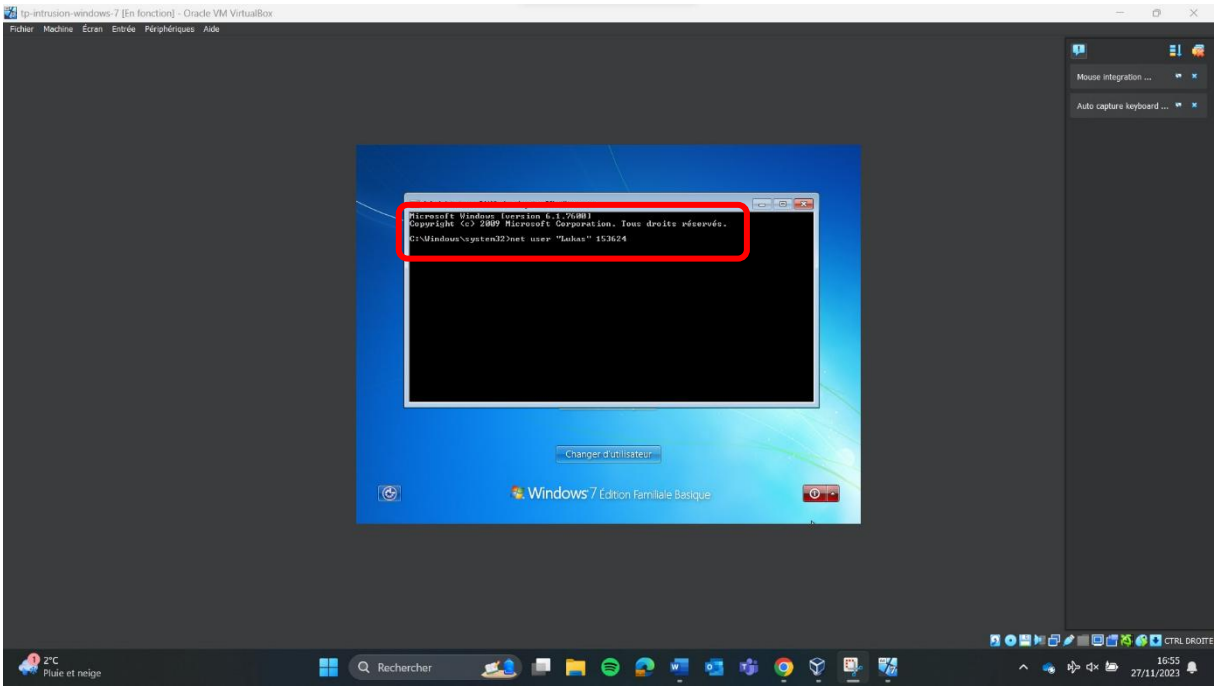
En suite chercher le fichier « Utilman.exe » et renommer le « Utilman.exe.bak »



En suite il faut renommer « cmd.exe » par « Utilman.exe »



Après cela, retourner sous Windows puis allez dans le terminal et tapez « net user nom d'utilisateur » avec le nouveau mot de passe de l'utilisateur



C'est donc la méthode 1 qui s'approche le plus de la vidéo, mais je n'ai pu la faire car je n'avais pas de machine physique ni de clef USB.

Cette faille consiste a utilisé un fichier nécessaire au lancement de Windows, Utilman.exe est un fichier pour les personnes malvoyantes qui leurs permet d'utiliser un ordinateur et qui est donc indispensable pour eux. Cela consiste donc à remplacer Utilman.exe par le cmd pour qu'une fois sur l'écran de veille, il suffit d'ouvrir Utilman et ce sera le cmd qui s'affichera.

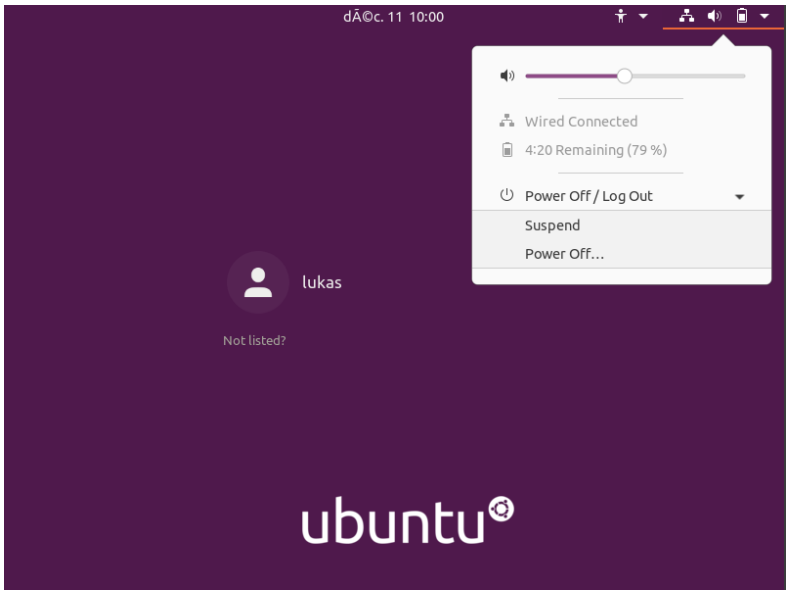
Cette faille de sécurité a été résolu sur les versions à partir de Windows 1o, mais elle a été simplement décalée puisqu'il est possible de faire la même chose simplement avec un fichier diffèrent. De plus il est possible grâce au Rubber Ducky qui est une clef USB qu'il suffit de brancher, d'outrepasser le mot de passe Windows sans même toucher à l'ordinateur.

Il y a plusieurs manières pour se protéger de cela :

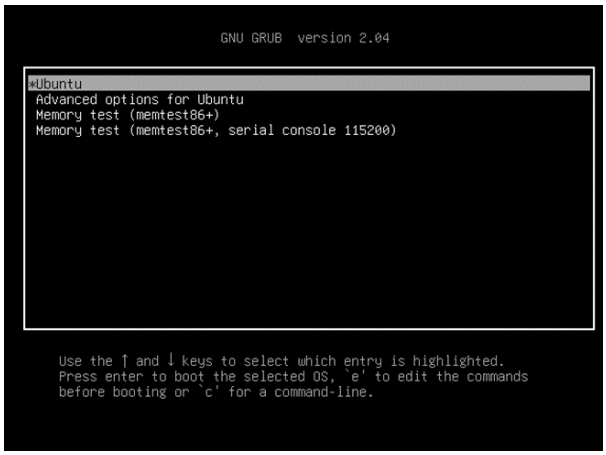
- Protéger ses répertoires/fichiers en les chiffrant
- Ne pas utiliser le compte administrateur comme compte de tous les jours
- Mettre un mot de passe sur le BIOS

Nous allons maintenant tenter de modifier le mot de passe d’un système linux grâce a la méthode « Bin bash » :

s

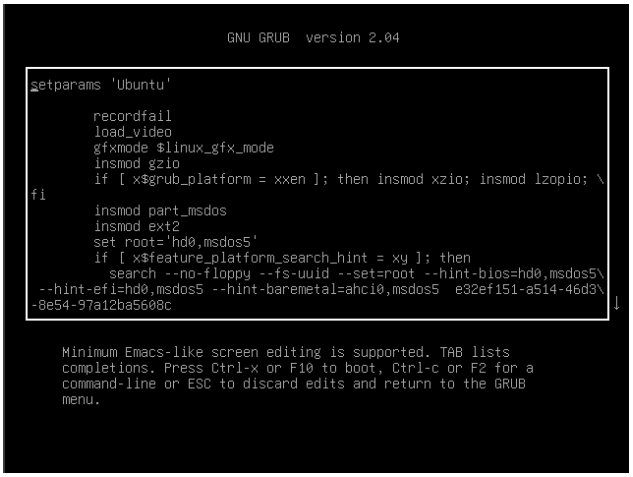


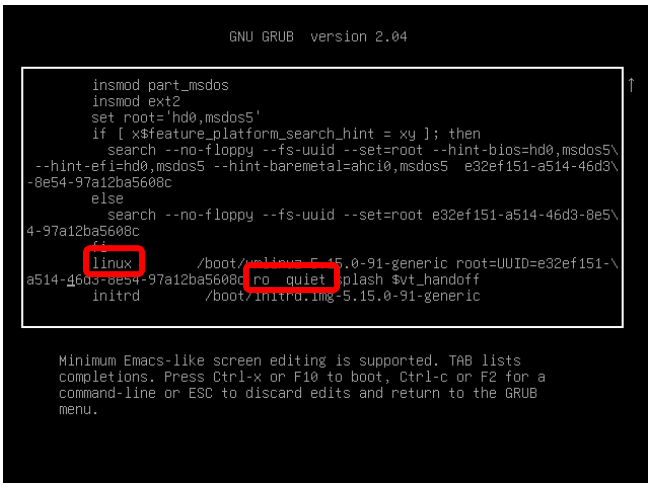
Tout d’abord, il faut redémarrer la machine



Appuyez sur maj pendant le redémarrage de votre machine

Maintenant appuyez sur « e » pour avoir ce menu



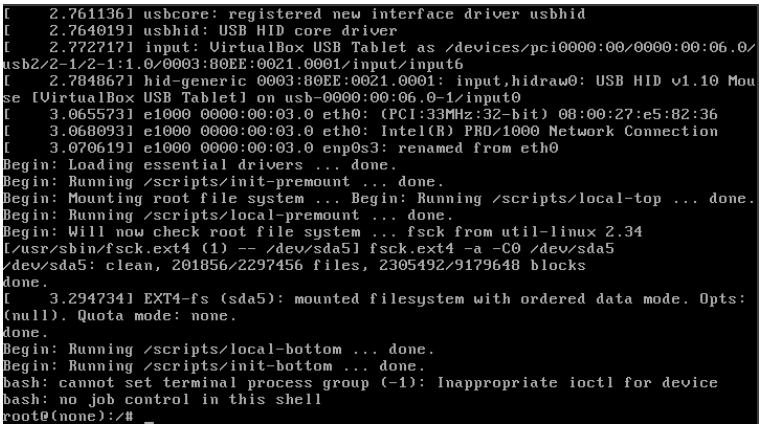


Descendez sur la ligne ou il y a écrit linux, puis déplacez-vous vers la droite pour trouver « ro quiet »

Remplacez « ro quiet… » par « rw=/bin/bash »

En suite appuyez sur CTRL+X ou F10

pour démarrer.

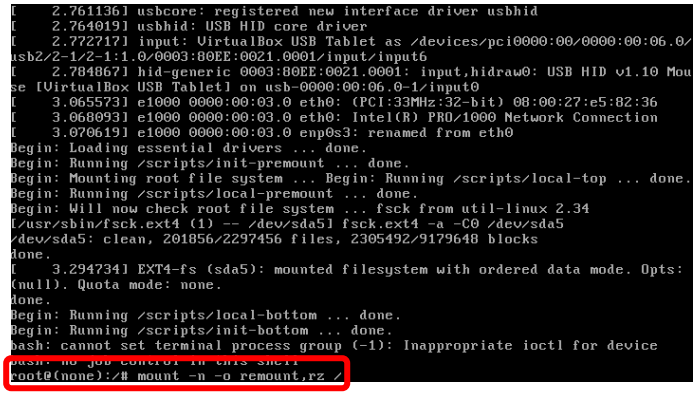


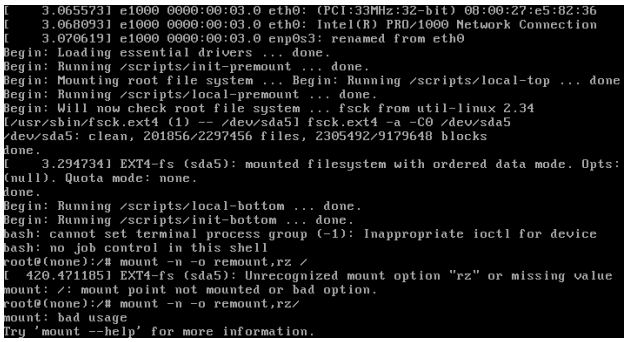
Puis vous vous retrouvez logiquement avec cette écran :

Taper “ mount -n -o remount,rw / “

Cela montera le système en lecture et en écriture

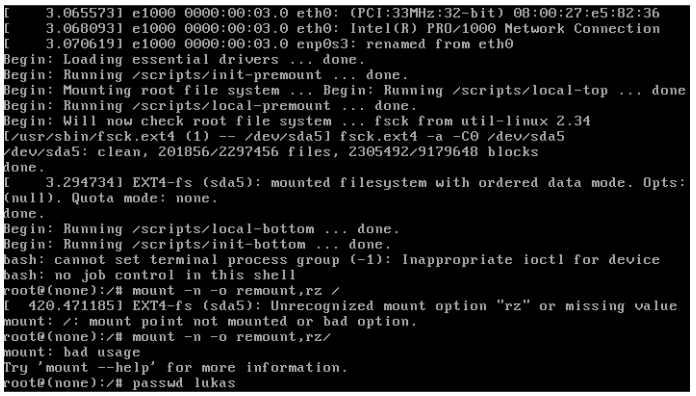
(Au lieu de la lecture seule, qui est la valeur par défaut.)

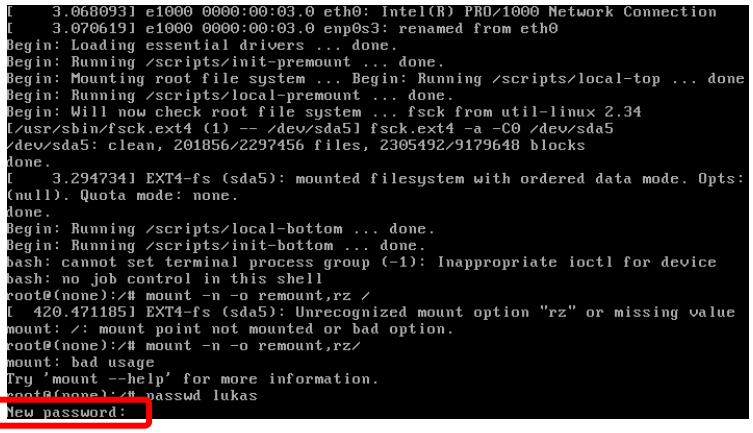




Si vous avez un message d’erreur similaire, cela veut dire que votre lecteur est déjà monté, passez à la prochaine étape comme si cela avait fonctionné.

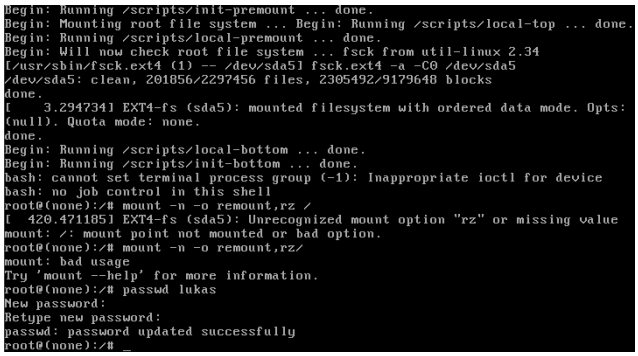
En suite tapez « passwd NomUtilisateur »

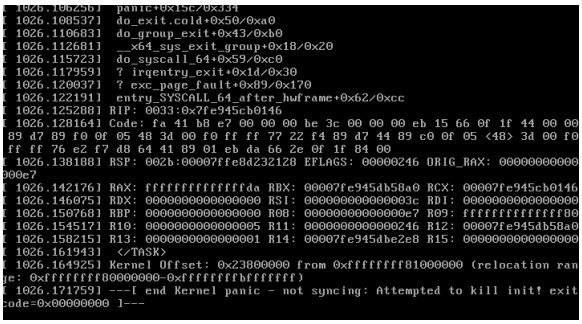




Vous pouvez maintenant définir un nouveau mot de passe

Vous avez donc bien changé le mot de passe, vous pouvez maintenant appuyez sur CTRL+D ou CTRL+ALT+SUPPR pour quitter





En suite redémarrer avec "Reboot -f"

Rentrez simplement votre nouveau mot de passe et

Le tour et joué !!