Margaux TANET
1ère année BTS SIO
18/10/2022

Bloc 3 : TP Intrusion Windows

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

SOMMAIRE

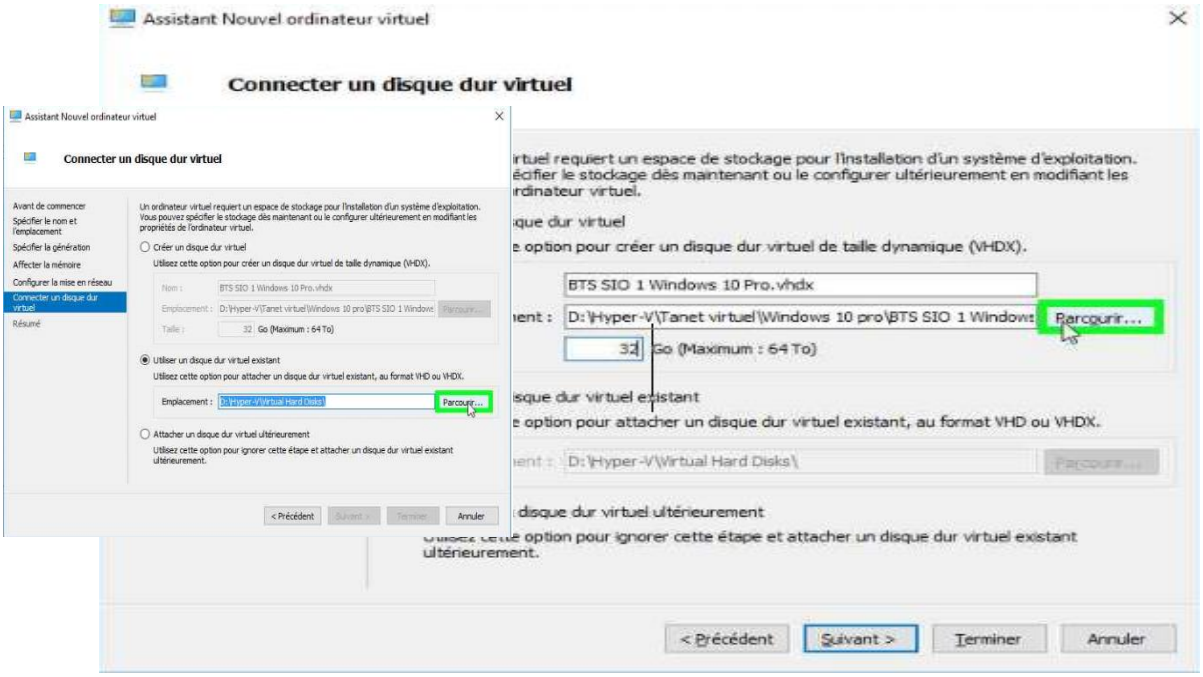
Pour commencer créer une machine virtuelle

- Se rendre dans gestionnaire Hyper-V
- « Nouveau » , « ordinateur virtuel »

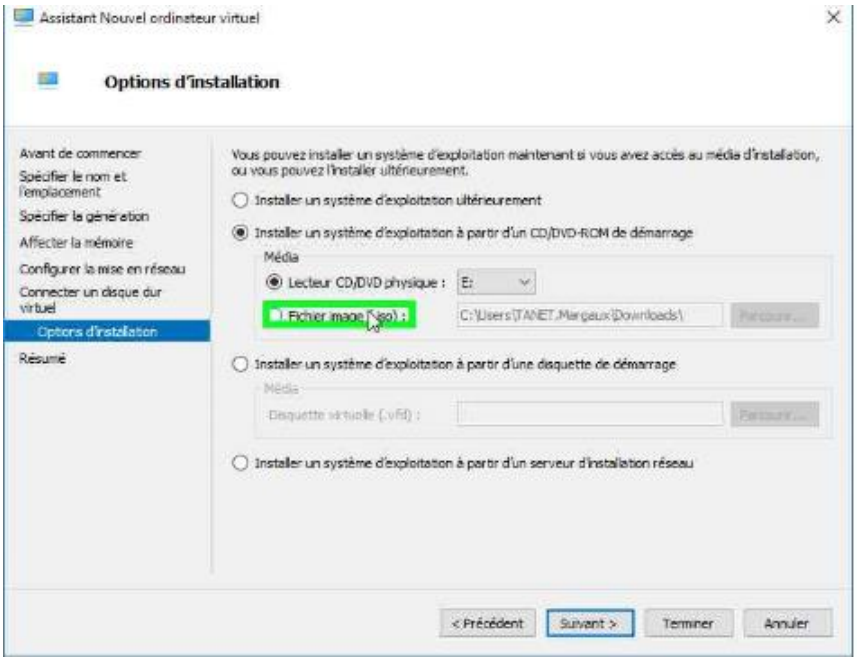
Donnez un nom à votre machine

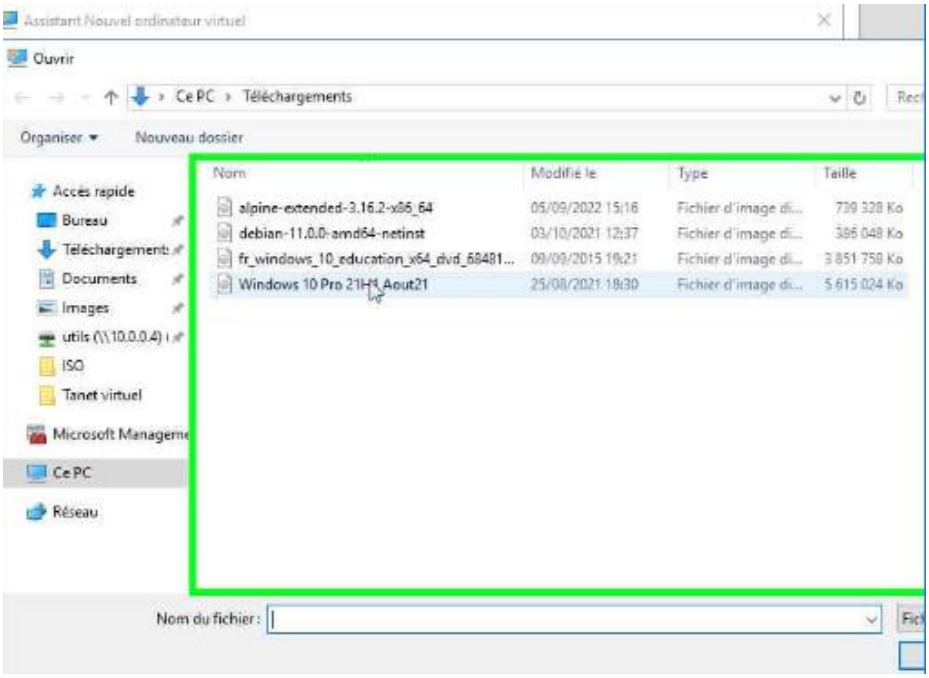
Mettre 2048 Mo au démarrage
Mettre en taille 32 Go pour un système de 64 bits.

Sélectionnez « utiliser un disque dur virtuel ».

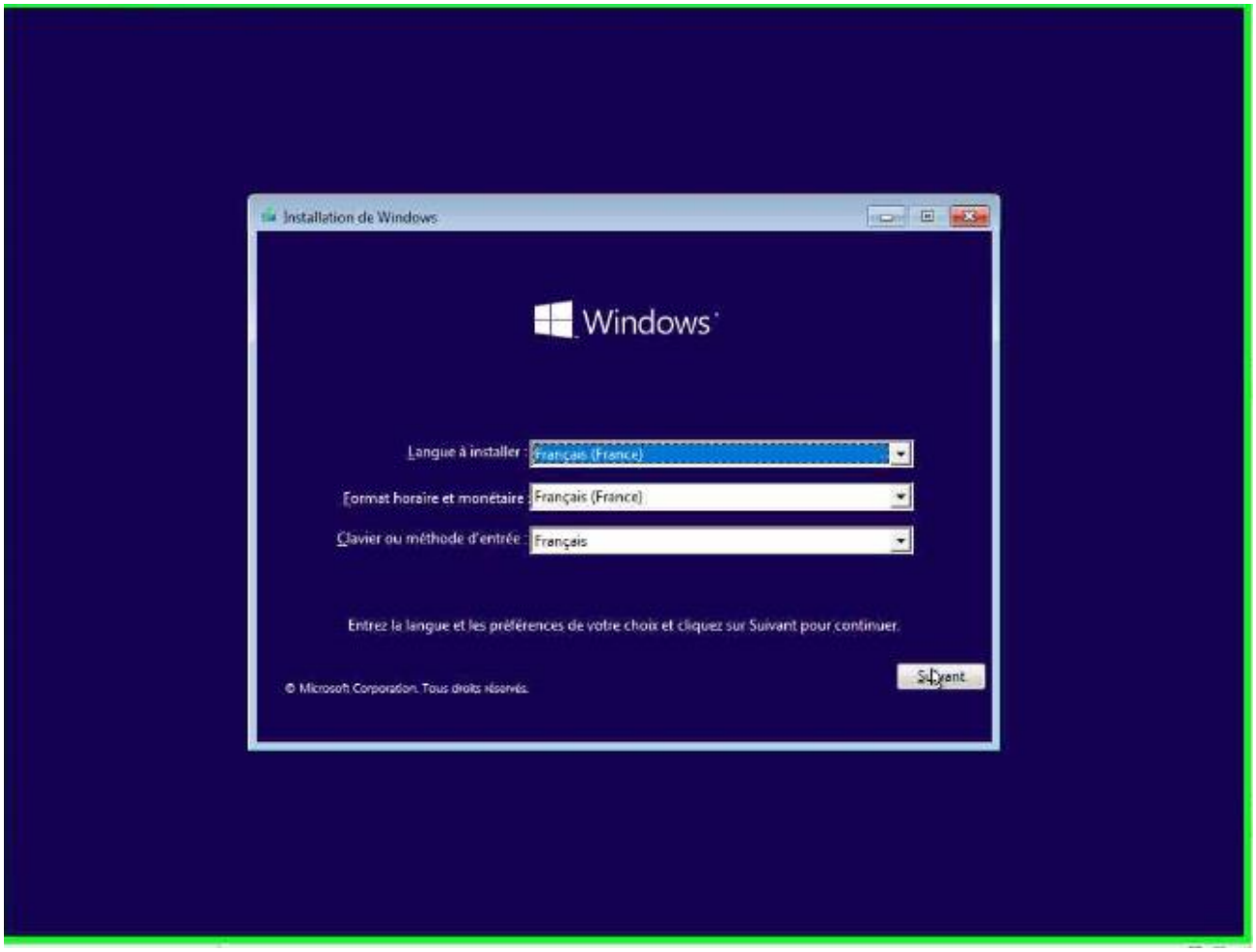


Sélectionnez « fichier image » et joindre le fichier téléchargé précédemment.



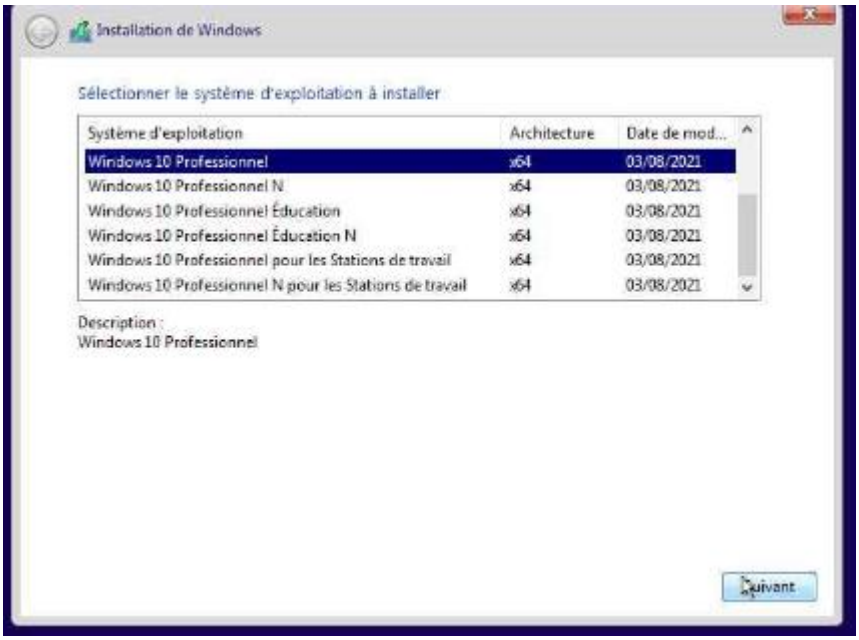


Lancez le démarrage Windows 10 pro en faisant clic droit démarrage et recliquer dessus, suivre l'installation.

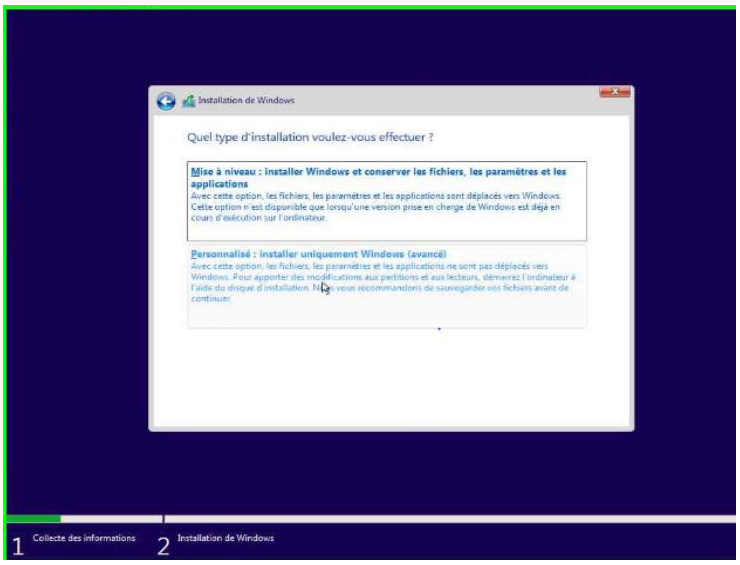


Laissez les paramètres de base.

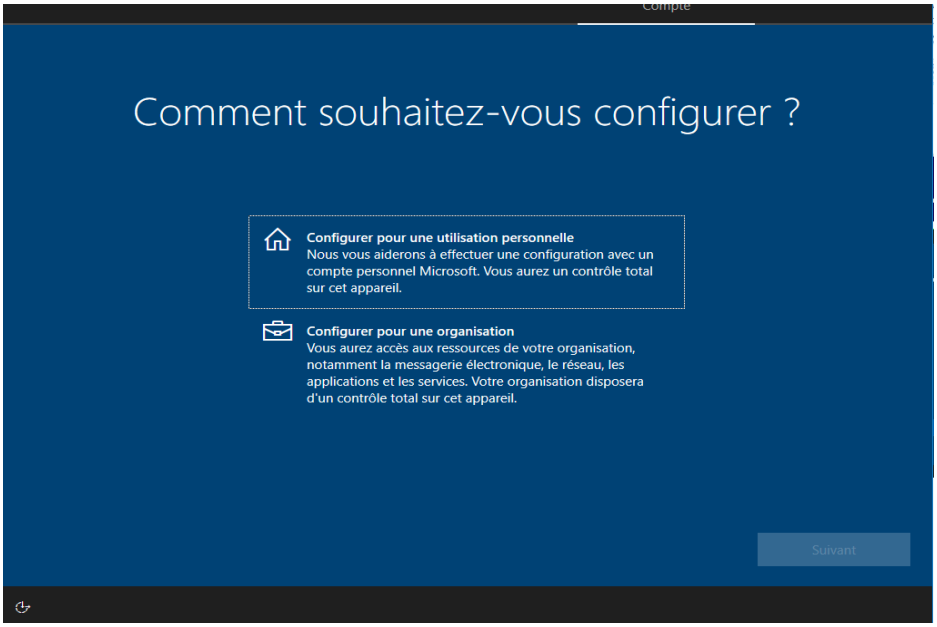
Sélectionnez l'installation Windows 10 Professionnel.



Sélectionnez l'option « personnalisé »



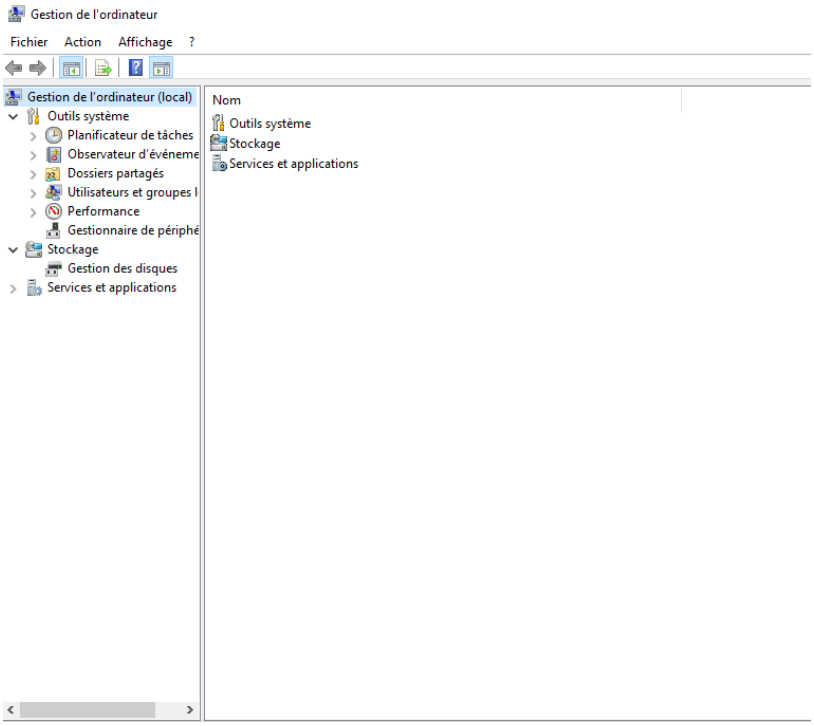
Sélectionnez France, même action pour la disposition du clavier.



Sélectionnez « personnelle » et « hors connexion », Windows 10 Pro est installé.

<u>Pour définir un mot de passe sur votre compte local administrateur :</u>

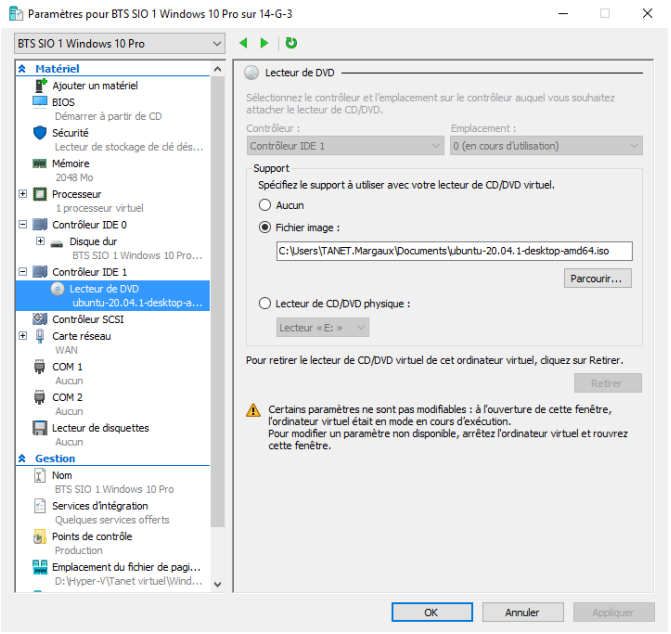
Clic droit sur menu démarrer > « gestion de l'ordinateur »



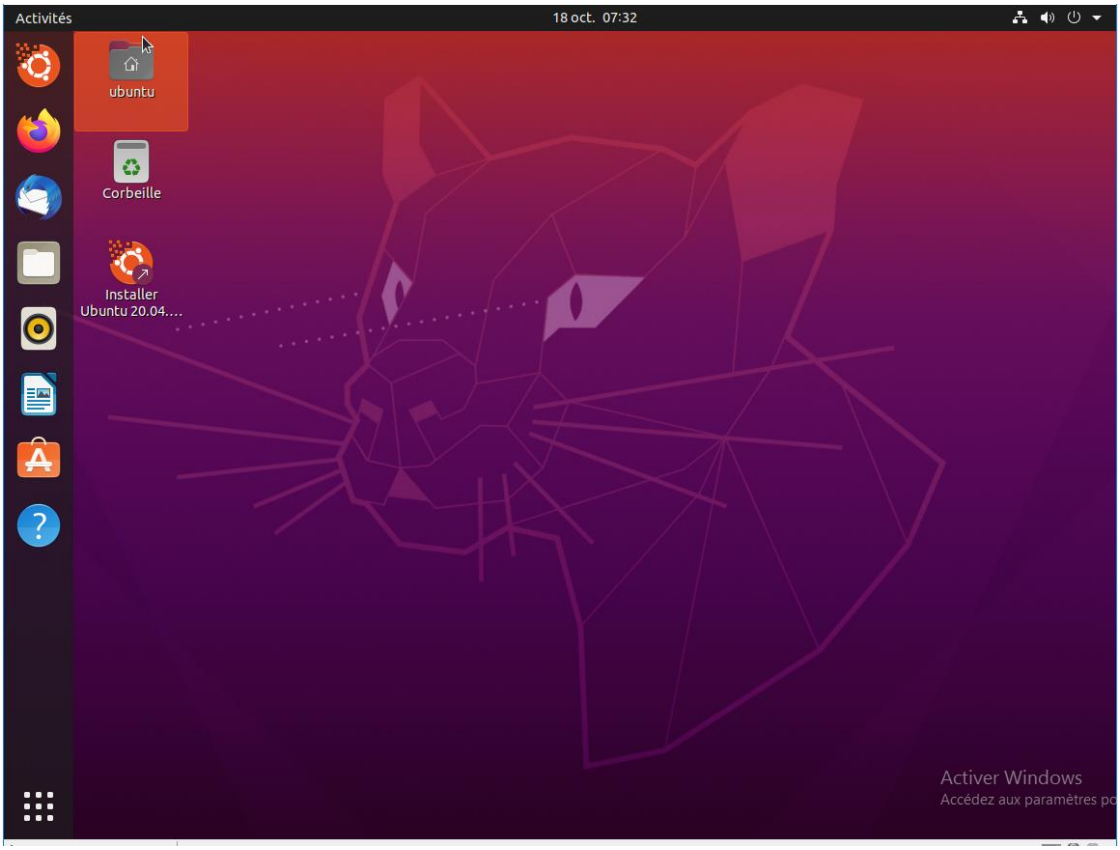
Cliquez sur « utilisateurs et groupes » sélectionnez votre compte utilisateur, clic droit modifiez le mot de passe et choisissez votre mot de passe. Créez un fichier sur le bureau que l'on appellera toto.txt en y renseignant les paroles d'une chanson dedans. Eteindre ensuite la machine.

2) **Bootez sur votre VM en utilisant une ISO de Ubuntu Desktop**

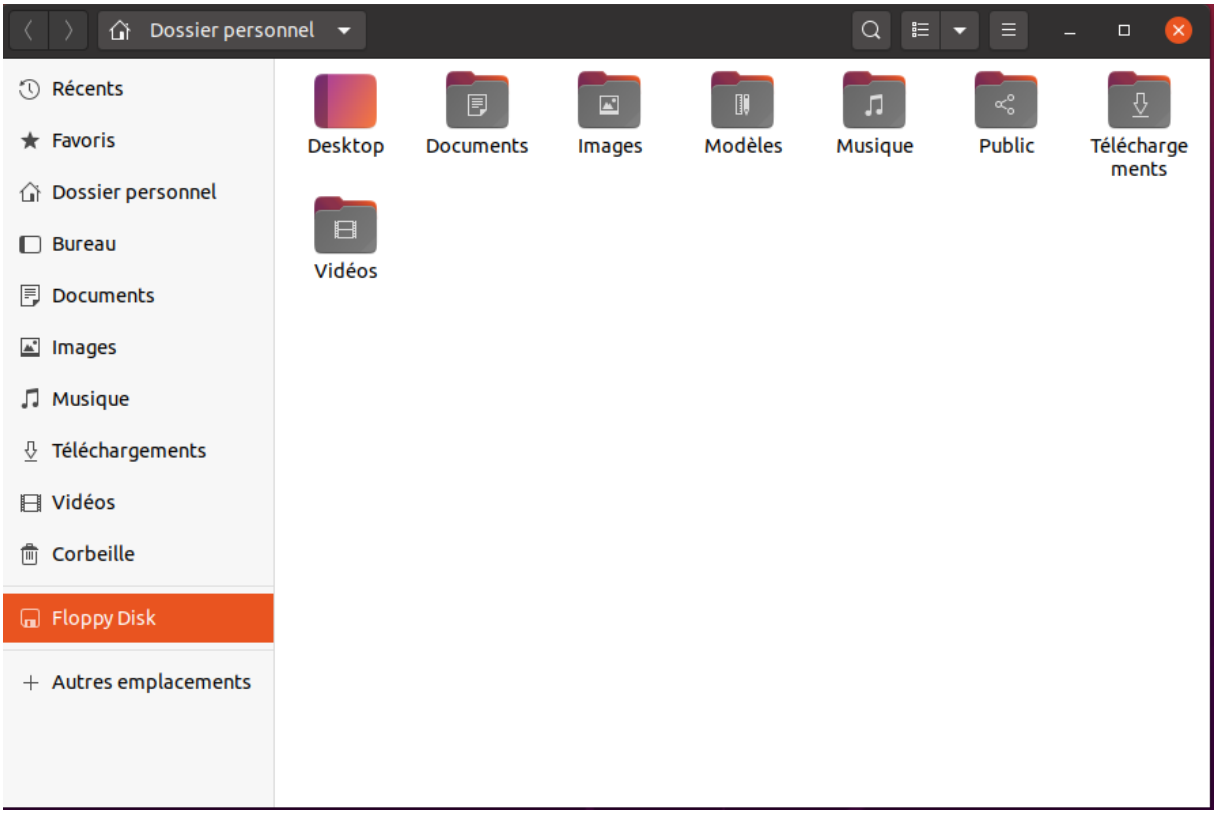
Dans le gestionnaire Hyper-V, prendre l'ISO UBUNTU télécharger au préalable, sélectionnez fichier image et faire parcourir, choisir l'iso Ubuntu et relancez la machine virtuelle :



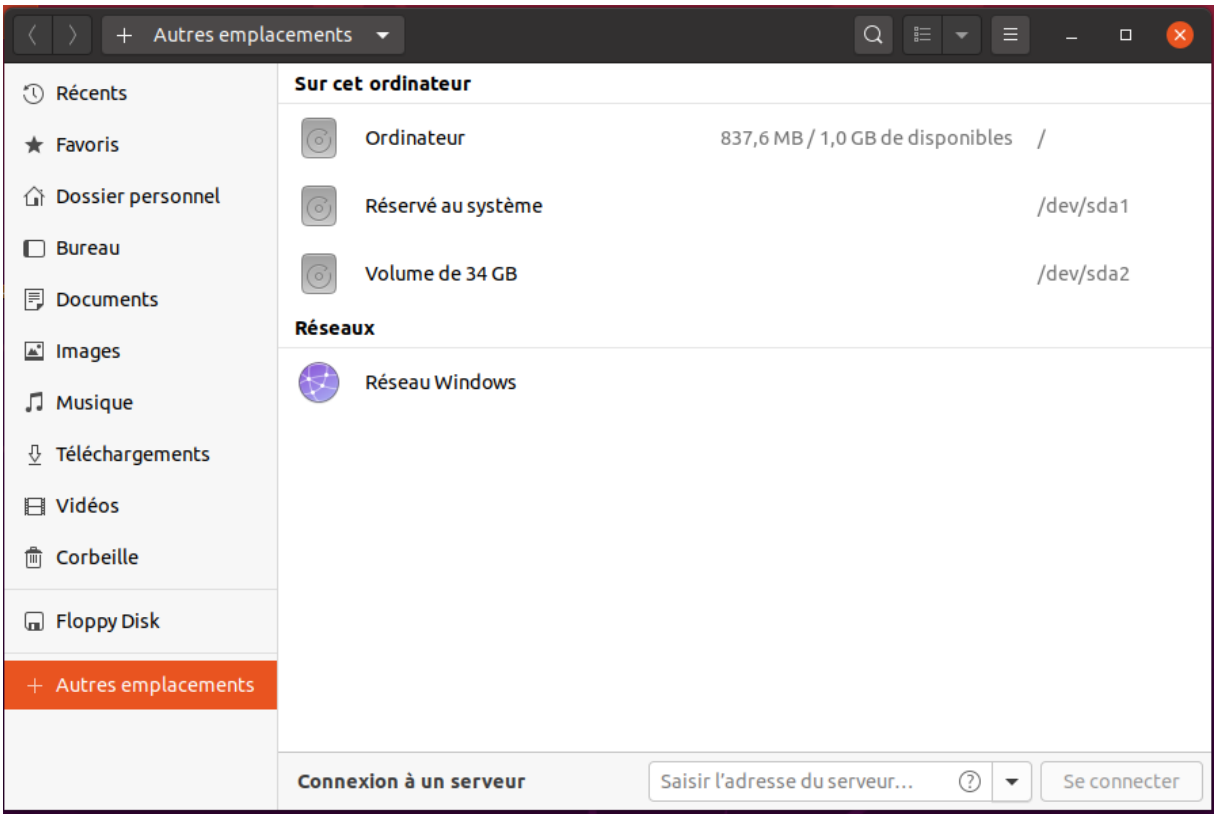
Lors de l'installation d'Ubuntu, sélectionnez la langue et sélectionnez « essayer Ubuntu ». Vous devriez arriver sur cette interface.



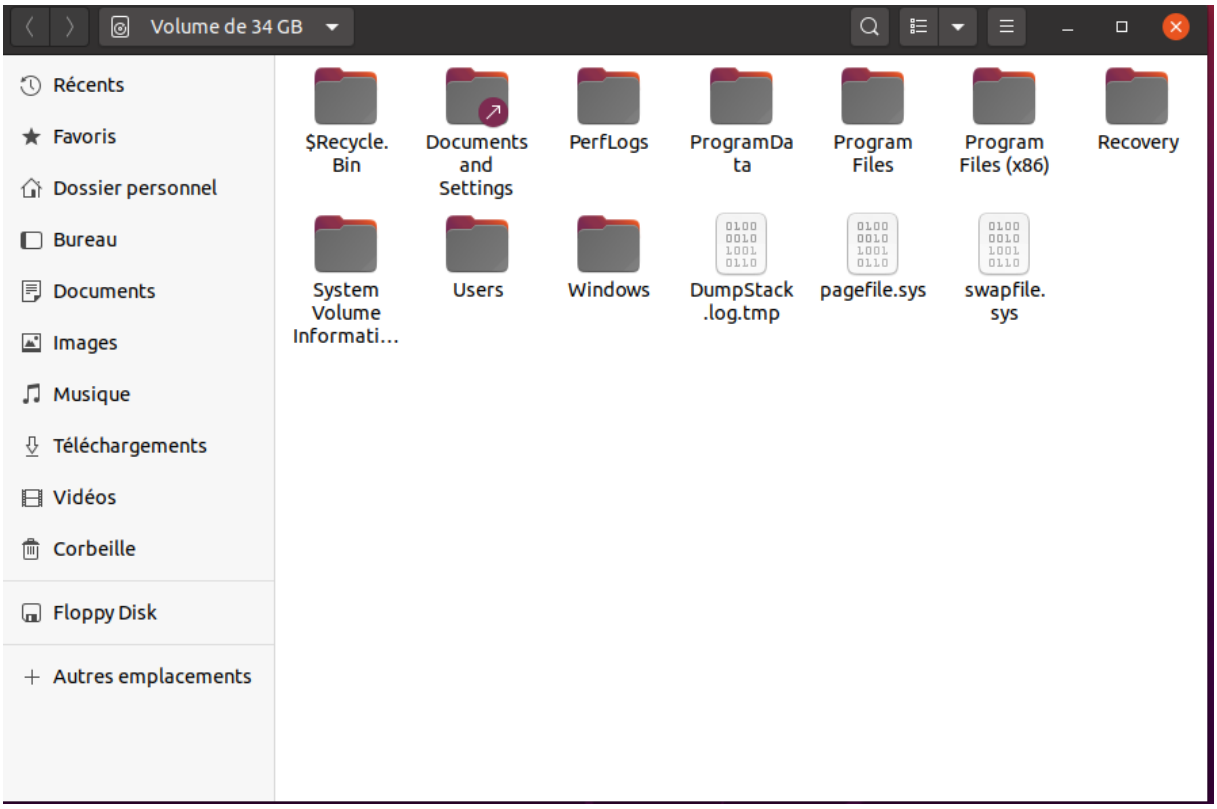
Se rendre dans gestionnaire de fichier :



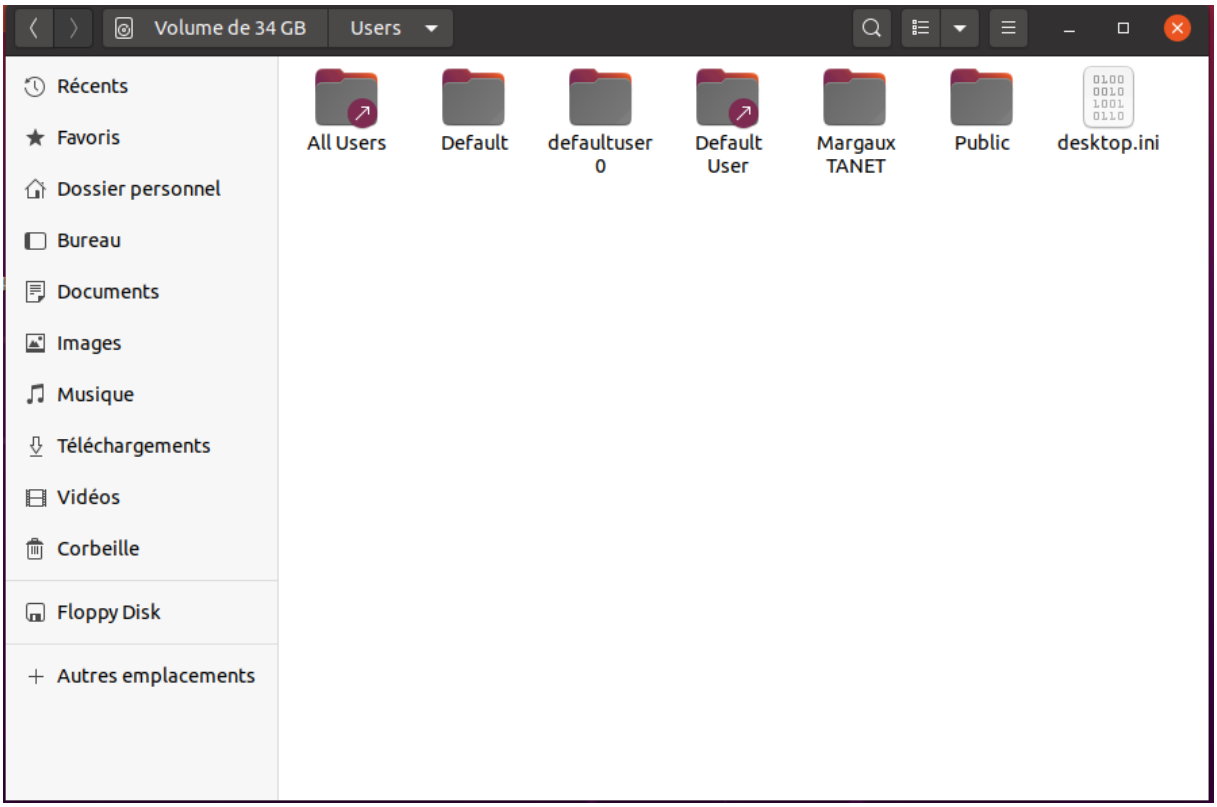
Sélectionnez « autres emplacements » :



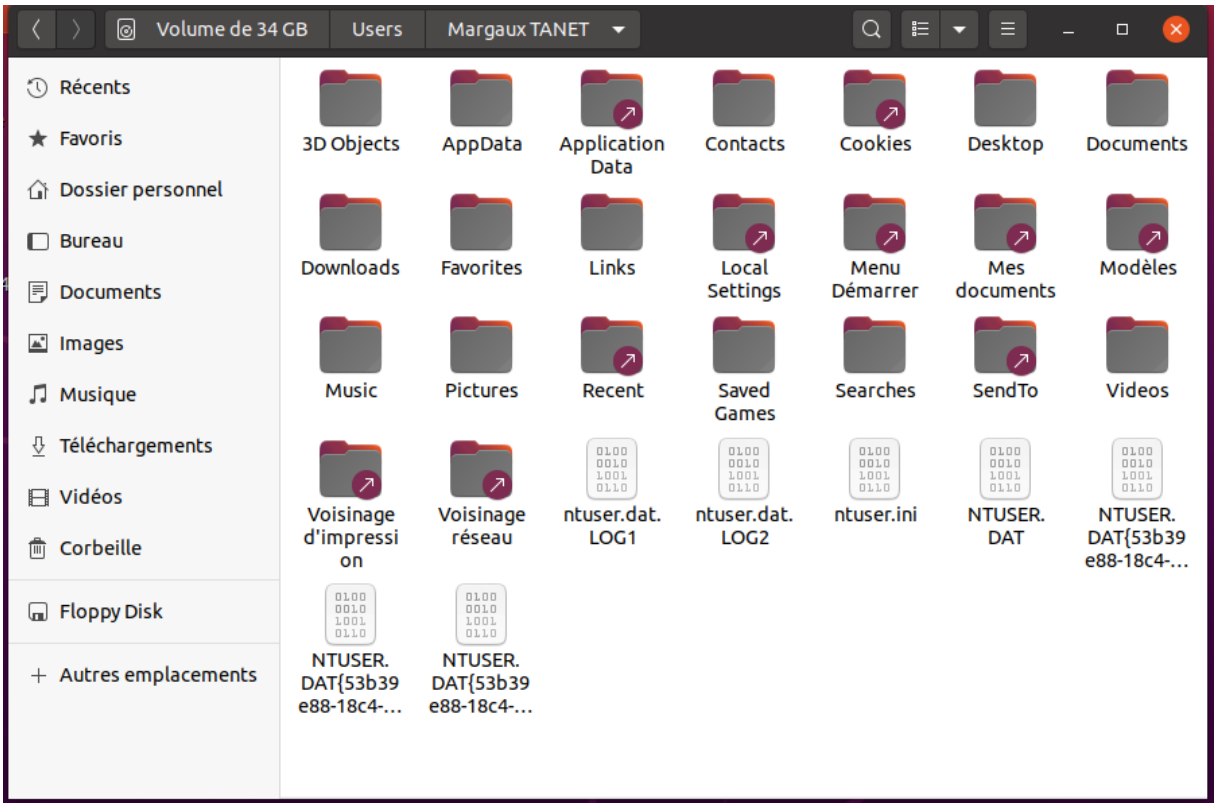
Sélectionnez « Volume de 34 Gb » (disque Windows 10 Pro) :



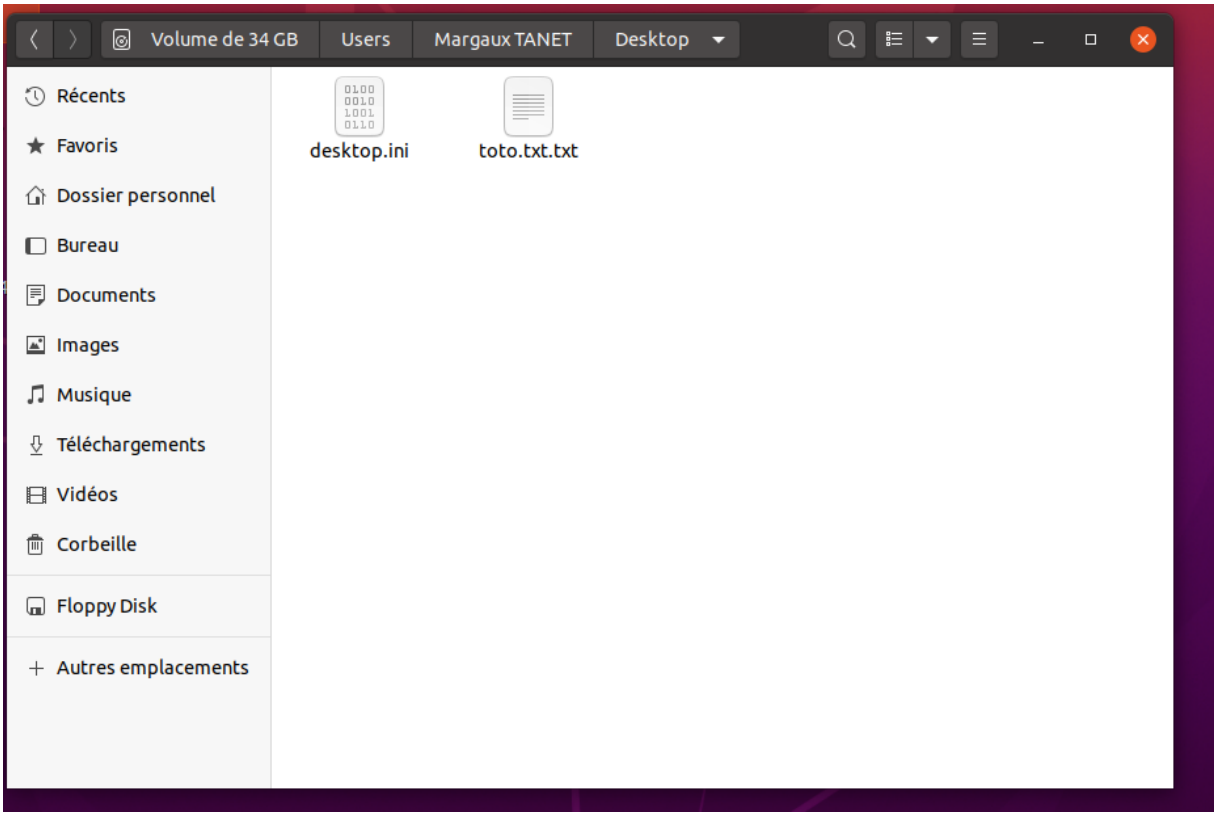
Cliquez sur Users :



Sélectionner notre compte utilisateur :



Et enfin cliquer sur « Desktop » où vous pourrez visualiser le fichier toto.txt :



Le fichier peut être lu mais j'ai rencontré un problème lors de la modification du fichier. Au moment de le modifier il me demandait de l'enregistrer sous, de le remplacer mais le fichier restait impossible à modifier.

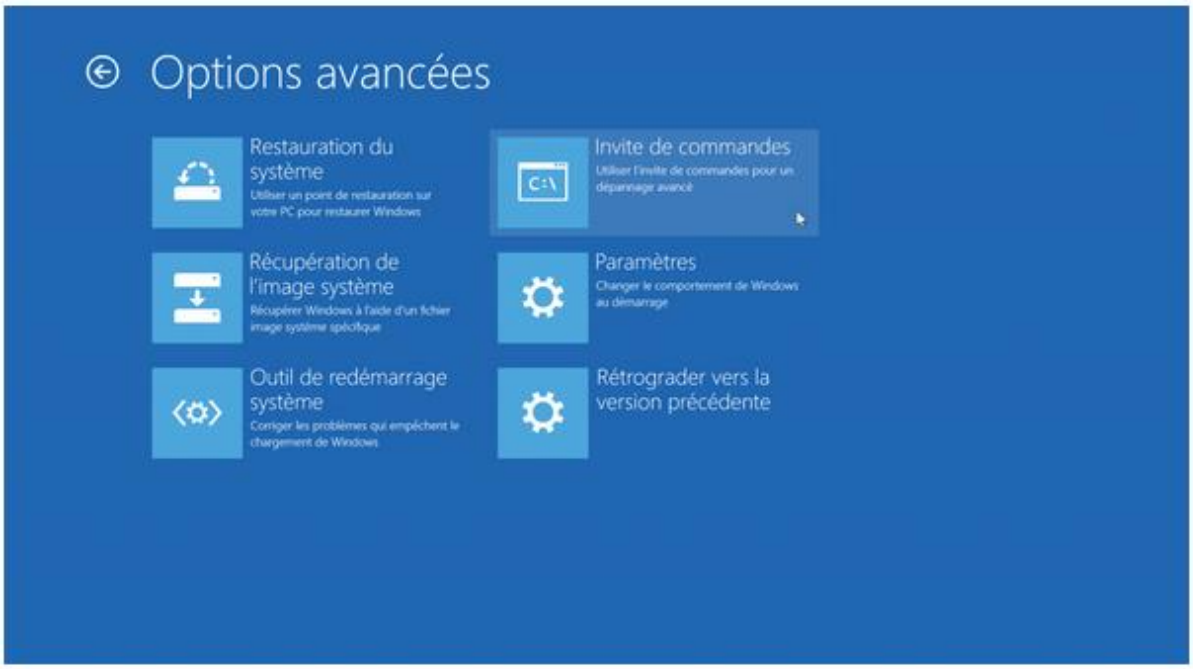
Choix des techniques :

A) Via l'environnement de récupération Windows

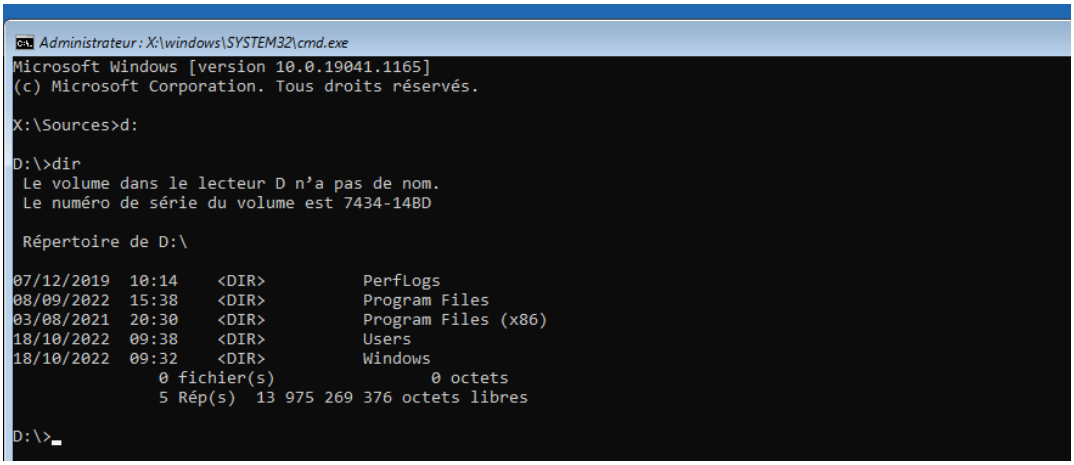
J'ai choisi la méthode via l'Environnement de récupération Windows (WinRE) pour réinitialiser le mot de passe d'un utilisateur grâce à une faille de sécurité de Windows.

Sur Windows 10, se rendre dans les options de démarrage avancées :

Pour cela, mettre l'ISO dans la machine virtuelle Windows 10 : au moment du démarrage appuyer « réparation » sélectionnez « dépannage » > « options avancées » > « invite de commande » et vous tomberez directement sur les options avancées comme ci-dessous :

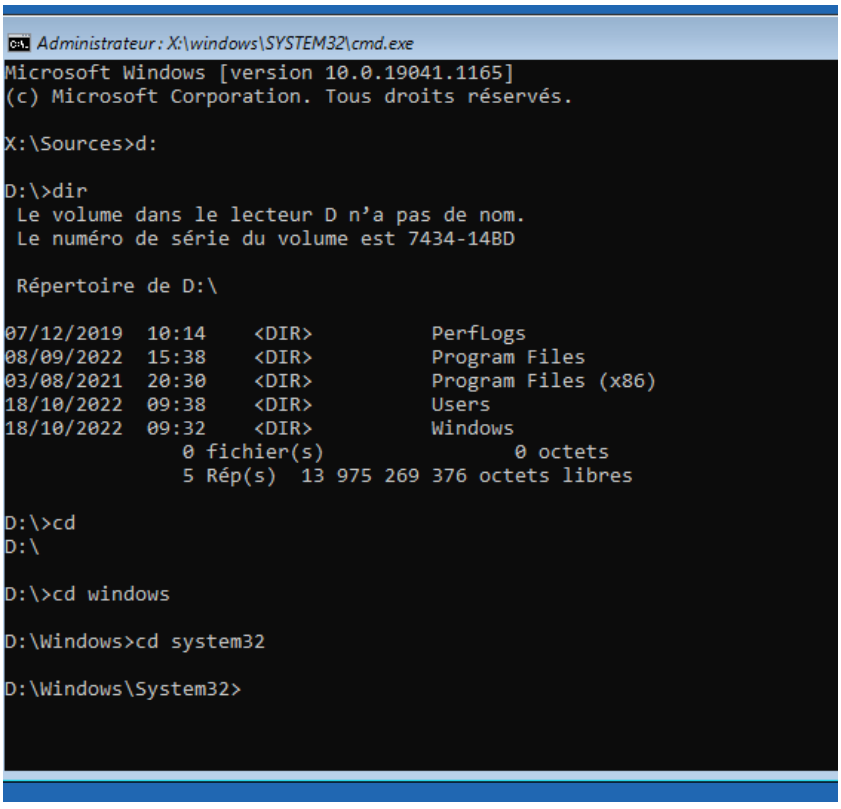


Rentrer « d : » pour votre lettre de lecteur. Faites « dir » après cette commande. Vous obtiendrez les dossiers propres à Windows.

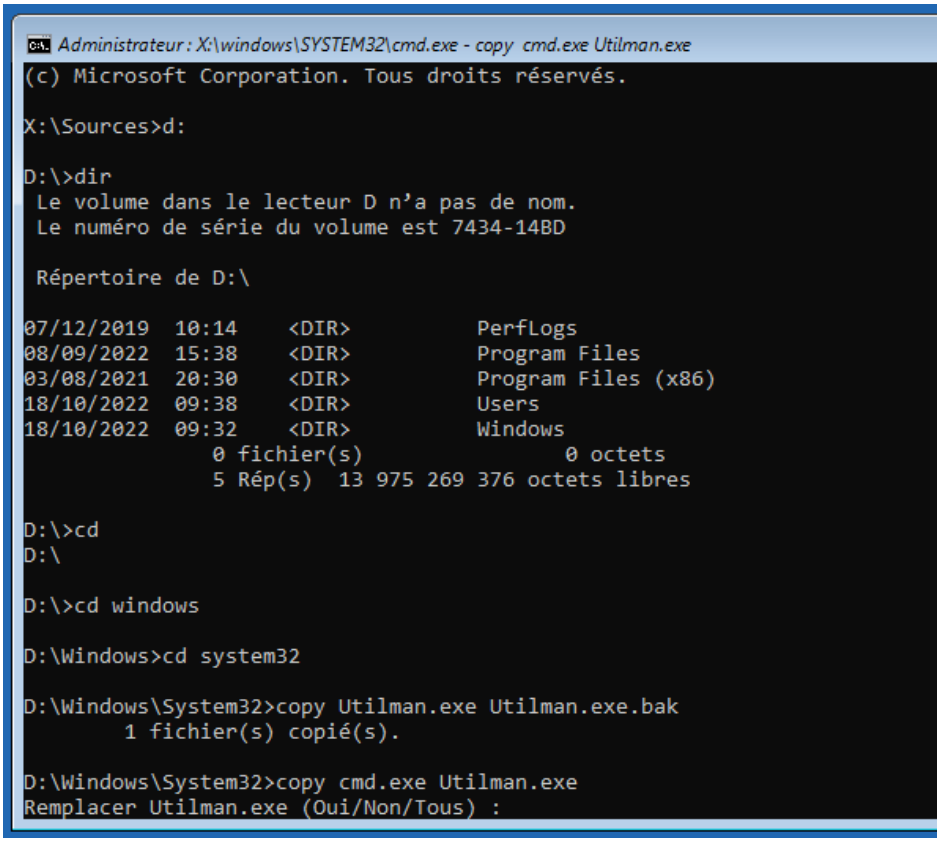


Une fois présent sur le lecteur Windows, se déplacer dans le dossier Windows\system32.

Pour se faire, rentrer ces commandes : *cd Windows* et cd *System32* successivement.



Nous allons créer un fichier de sauvegarde que l'on restaurera lors de la réinitialisation de notre mot de passe. Pour se faire, créer ce fichier se prénommant « utilman.exe » : *copy Utilman.exe Utilman.exe.bak*



Pour remplacer les options d'ergonomie par l'invite de commande :

Nous remplaçons les options d'ergonomie Utilman.exe par l'invite de commande cmd.exe avec la commande : *copy cmd.exe Utilman.exe*

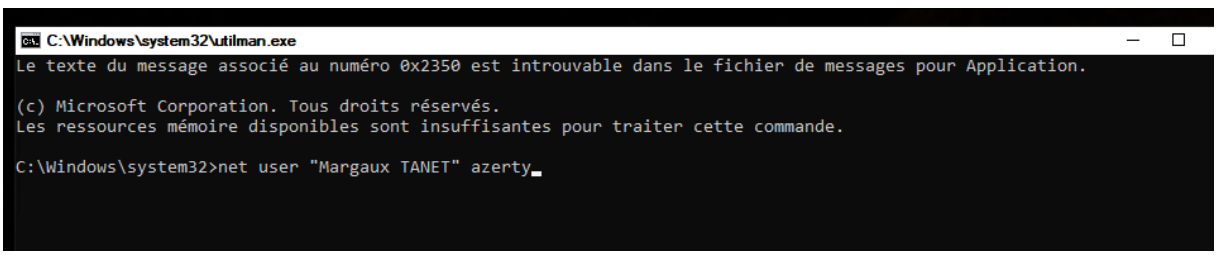
Le fichier a bien été copié, une question vous sera posée, répondez « oui » et redémarrez la machine.

N'oubliez pas d'enlever l'ISO avant le redémarrage.

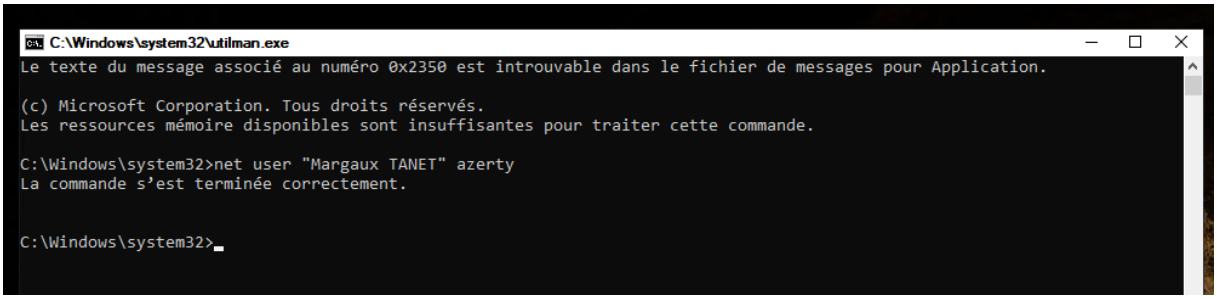
Une fois le redémarrage effectué, sur l'écran de connexion de Windows, appuyez sur les touches Windows + U pour lancer l'invite de commande.

Rentrez la commande suivante pour réinitialiser le mot de passe du compte utilisateur (il vous faudra connaitre le compte utilisateur) : *net user ''compte utilisateur'' nouveau-mot-de-passe*

Dans cette exemple, *net user''Margaux TANET'' azerty*



Un message apparait « la commande s'est terminée correctement » vous pouvez donc relancer la vm en redémarrant avec l'ISO et faire la même instruction que l'étape vu un peu plus au-dessus.



Nous allons restaurer les options d'ergonomie. Faire Windows+U pour ouvrir l'invite de commande :

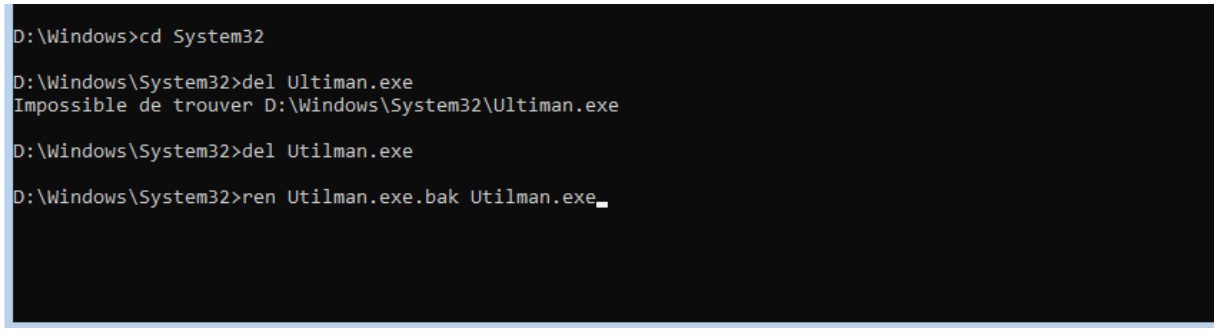
Rentrez les commandes suivantes à la suite :

Cd Windows

Cd System32

Del Utilman.exe

Ren Utilman.exe.bak Utilman.exe

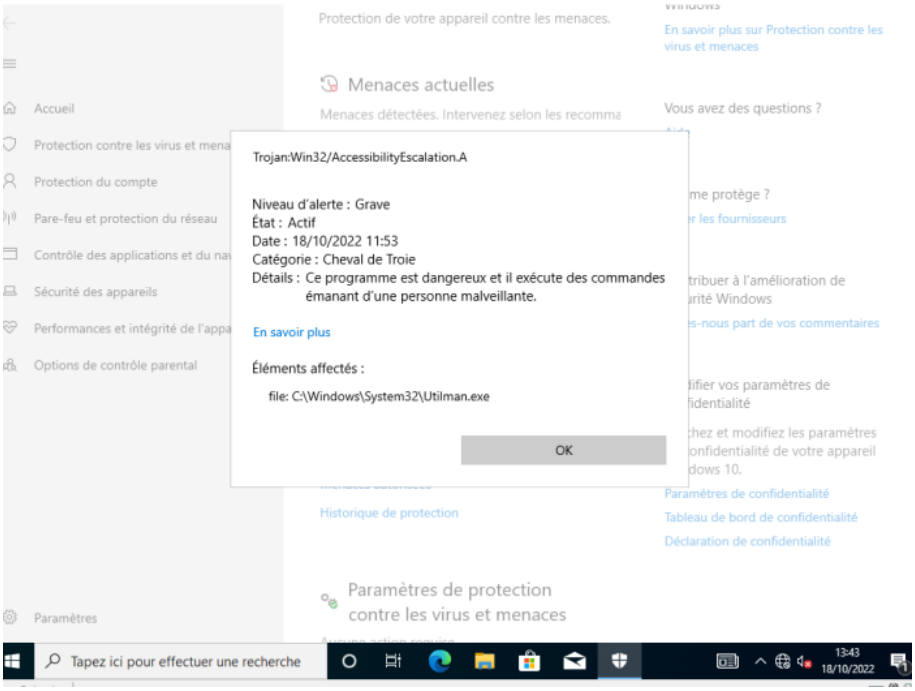


Relancez la machine virtuelle sans l'ISO et tenter de se connecter, normalement vous devriez avoir accès à la session.

Cette méthode est une méthode de contournement que l'on peut faire grâce à une faille de sécurité de Windows.

Dans la vidéo qui nous a été présenté, c'est cette méthode (présentée juste au-dessus) qui se rapproche le plus avec laquelle il a réussi à casser le mot de passe.

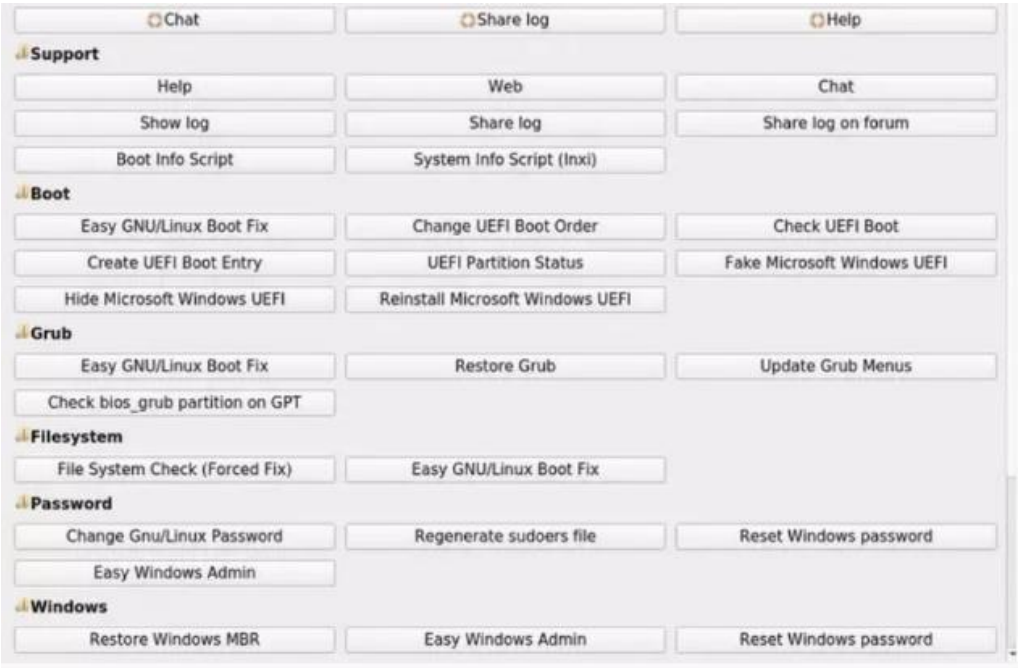
Dans les paramètres de Sécurité Windows un message apparait nous indiquant que le programme est dangereux :



B) Méthode avec Rescatux :

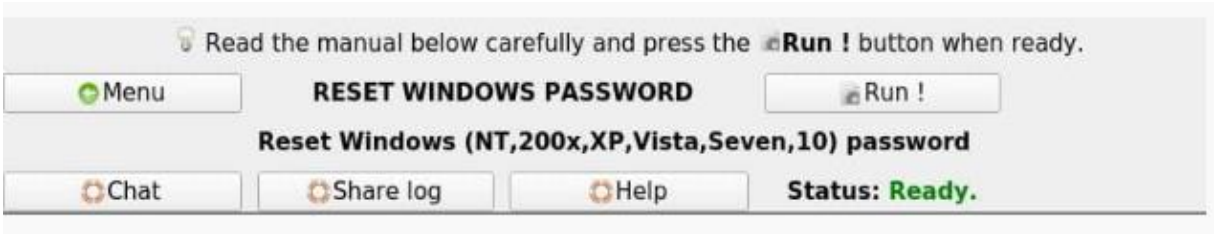
Mettre l'ISO dans la machine virtuelle de la même manière que Ubuntu ou l'ISO Windows 10.

Une fois l'ISO chargée, sélectionnez la langue ainsi que la disposition du clavier et appuyer sur démarrer. Vous arriverez sur ce Menu (en-dessous). A l'aide du curseur descendez jusqu'à la rubrique windows.

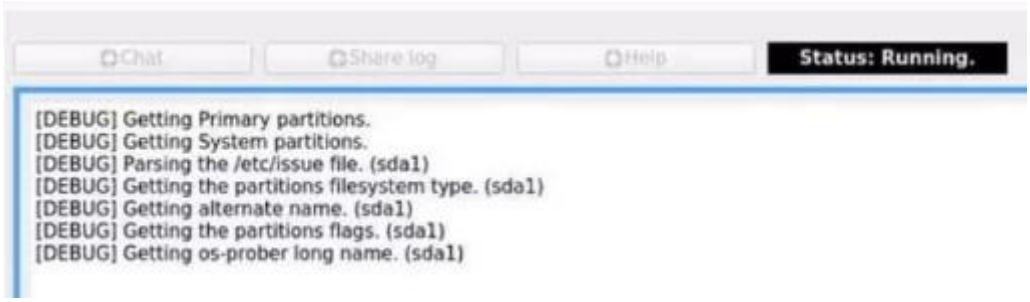


Sélectionnez Blank Windows Password (ancienne version sur la nouvelle elle s'appellera « reset Windows password »). C'est ici aussi que vous pouvez modifier un compte standard en compte Admin (« Windows user to Admin »).

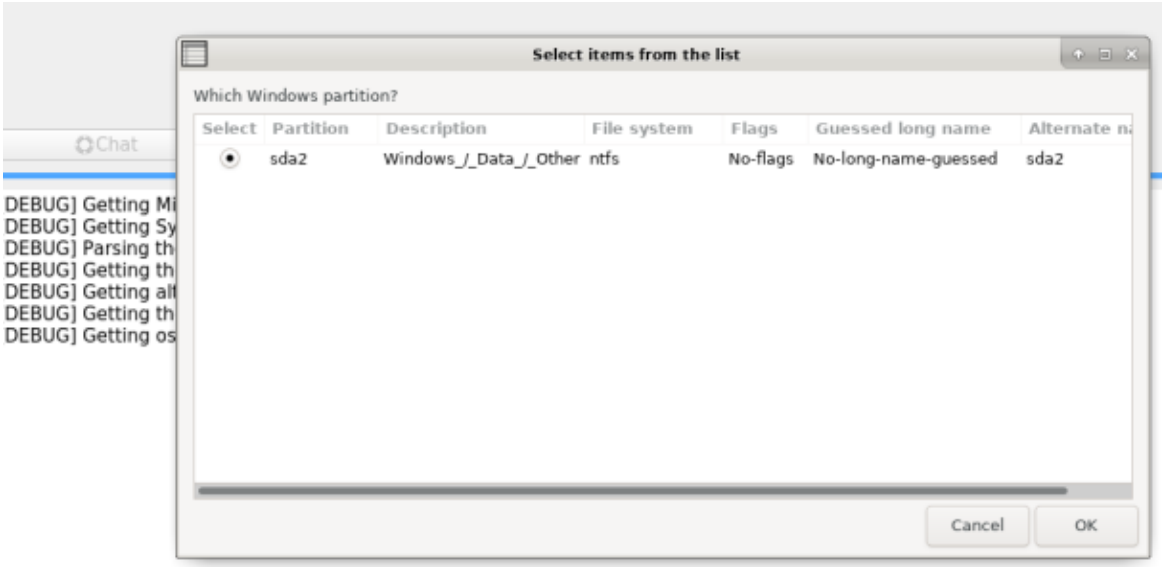
Une fois votre choix d'action effectuée cliquez sur « RUN » en haut à droite du logiciel.



Vous aurez ce message qui apparaitra : (Rescatux commence à travailler)

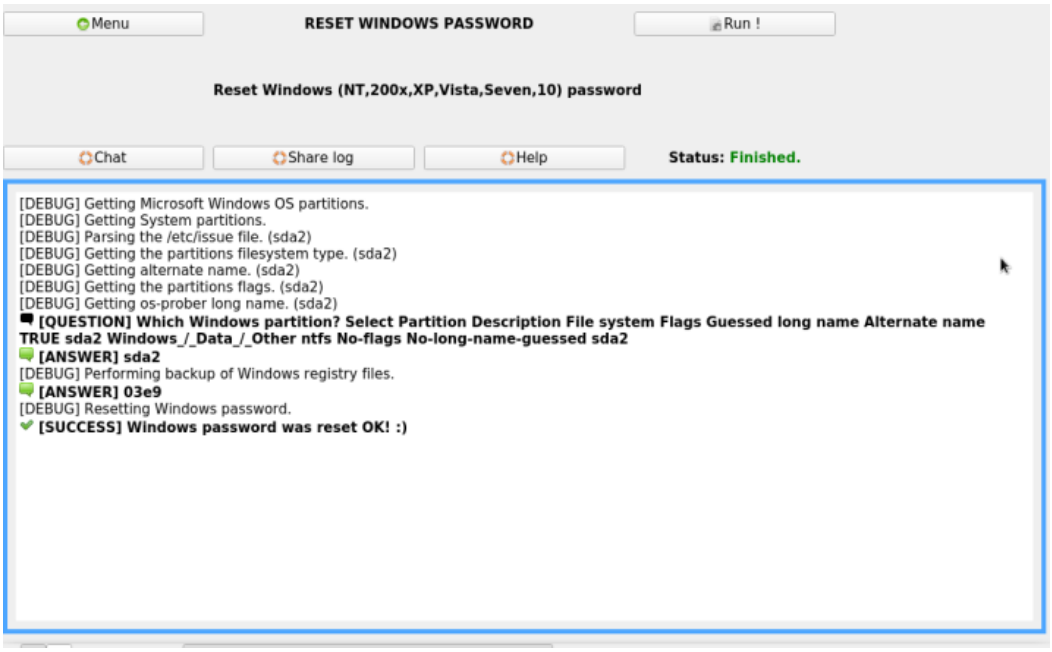


Ensuite il vous proposera de sélectionner la partition sur laquelle est installée Windows.



Il faut par la suite sélectionner le compte visé pour effacer le mot de passe. On choisit donc « administrateur » et OK en bas de page.

Après un petit moment ce message s'affiche. Il vous avertira du succès de l'opération. Il ne reste plus qu'à redémarrer l'ordinateur.



4) Conclusions

Pour la partie Ubuntu : nous venons de découvrir que juste avec une ISO Ubuntu on arrive déjà à récupérer un fichier créer sur Windows sans rencontrer le moindre problème.

Méthode par contournement :

Pour récupérer les mots de passes, sur Windows via l'Environnement de récupération Windows, il est facile mais assez long de changer un mot de passe de compte administrateur avec quelques commandes (comme montrer précédemment). Il faut juste savoir à l'avance le nom du compte administrateur dont on veut le mot de passe. Cette méthode permet de casser un mot de passe grâce à une faille Windows.

Autre méthode qu'on a pu voir, en utilisant une ISO Rescatux il permet d'effectuer différentes tâches et une en particulier : l'effacement de mot de passe d'un compte utilisateur Windows. Rescatux peut fonctionner à la fois sous Linux et Windows. Et a plusieurs autres fonctions (options GRUB (Linux) : Restaurer GRUB, mettre à jour ces menus, mettre à jour les menus GRUB de Debian/Ubuntu ; options Windows : réinitialiser les mot de passes Windows, déverrouiller un utilisateur Windows, réinstaller Microsoft Windows EFI,…)

Il existe d'autres méthodes de cassage de mot de passe dites par « force brute ». Ce sont des tentatives qui sont réalisées successivement jusqu'à trouver la bonne combinaison.

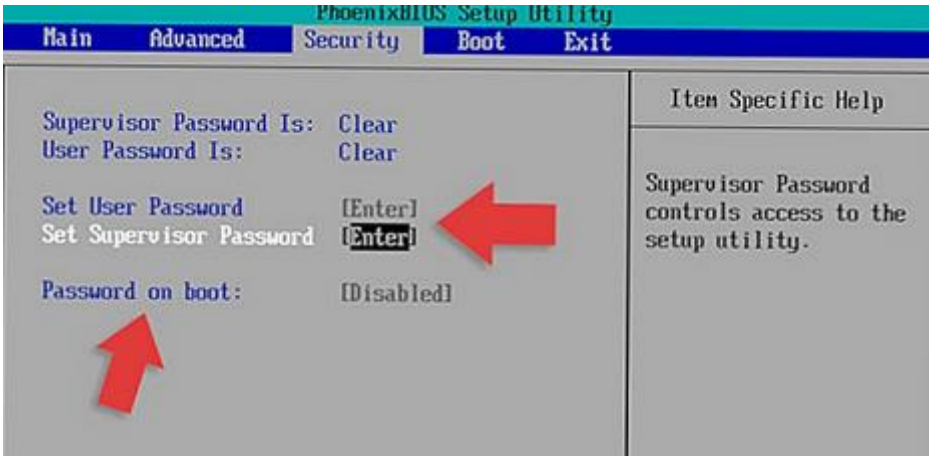
D'autre part, si on connait les lignes de commandes et si on sait où chercher effectivement l'action peut se faire beaucoup plus rapidement.

5) Comment se protéger de ce problème ?

Il existe plusieurs manières de se protéger comme définir un mot de passe au bios ou au UEFI, chiffrer les données ou crypter un disque dur. Désactiver les ports USB dans le BIOS peut être aussi une solution mais comme nous le verrons par la suite (cf. Kon-boot), avec certains logiciels, ils sont capables d'éviter ce blocage. On peut utiliser des outils du système d'exploitation, tels que SysKey, qui crypte le contenu du mot de passe de hachage à l'aide d'un cryptage 28 bits avec une clé de cryptage RC4.

La méthode : mot de passe dans le BIOS :

Redémarrer la machine et dès qu'elle démarre appuyer sur la touche F10 ou F12 selon le fabricant.



Une fois dans le bios aller dans onglet « security » et comme on peut le constater cela indique que le mot de passe du superviseur n'est pas défini. Sélectionner « set supervisor password » et appuyer sur la touche entrée.

Une fenêtre va s'ouvrir et il va falloir définir un mot de passe mais aussi définir le mot de passe utilisateur.

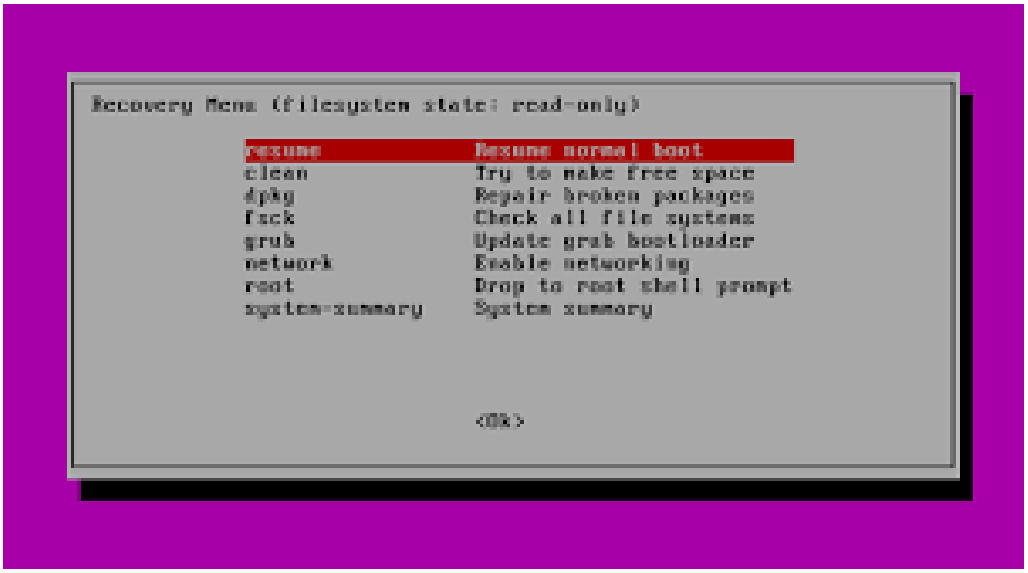
Normalement un statut « set » doit avoir changé, il apparaissait avant « clear ». Redémarrer Windows 10.

6) Casser un mot de passe sur Linux

Pour se faire créer une nouvelle machine virtuelle avec comme ISO Ubuntu.

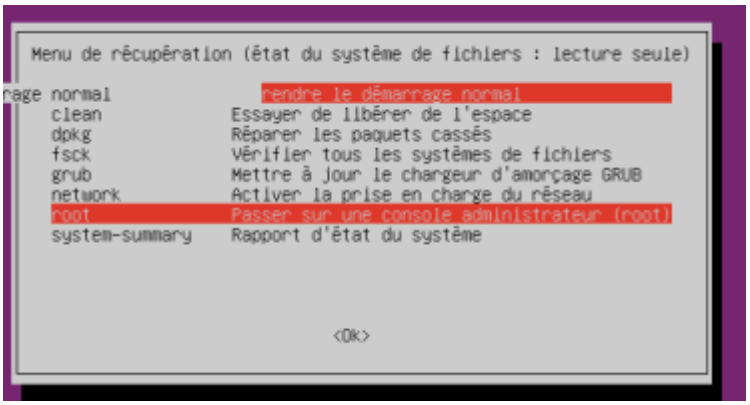
Nous allons utiliser le mot de passe en utilisant Grub. Une fois l'installation terminée, redémarrer l'ordinateur et maintenez appuyée la touche Maj pour accéder au menu Grub.

Appuyer sur la flèche vers le bas pour sélectionner la ligne « mode de récupération » et appuyer sur « entrée ».

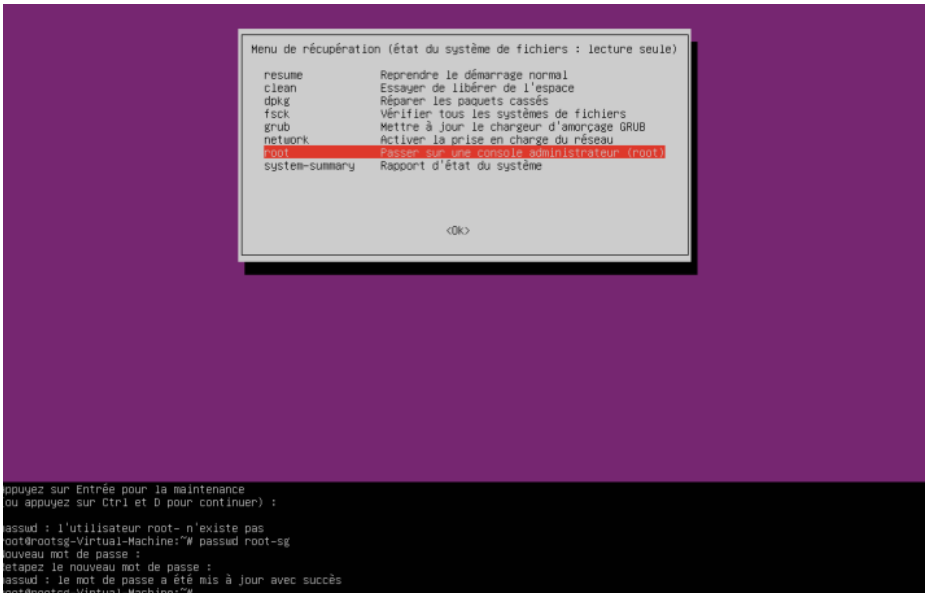


Le processus de démarrage est lancé, après quelques instants, un menu de récupération va apparaitre.

Avec les touches allez sur root et faites entrée. A ce symbole #, saisir « *passwd username* ». (Où *username* est le nom du compte)



Ils demanderont ensuite à mettre un nouveau mot de passe et à confirmer le nouveau mot de passe. Puis tapez *reboot*.



Conclusion :

Il est encore plus facile de casser un mot de passe sous Linux en quelques commandes et le mot de passe est déjà changé.

7) Autre méthode pour casser un mot de passe : Kon-Boot

Kon-Boot est un outil qui permet de passer outre les mots de passes dans Windows et MacOS.

Ce qui est différent avec cet outil c'est qu'il contourne certains BIOS même si on désactive les ports USB. Il fonctionne en court-circuitant le mot de passe mais ne le supprime pas. Le logiciel peut être copié sur un disque, une clé USB.

(La capture suivante vient de ce site : https://www.malekal.com/ouvrir-session-windows-10-sans-mot-de-passe-kon-boot/)

Se rendre sur le menu boot, sélectionner la clé USB. Un message *Kon-Boot driver loaded* apparait, appuyez sur la touche Entrée.

Windows 10 se charge et le bureau de Windows 10 s'ouvre sans mot de passe.