Cybersécurité des services informatiques

PROFESSEURS : MR JOBARD

TP N°2 : Intrusion simple 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.

Introduction :

Microsoft prend la sécurité au sérieux. Les comptes Microsoft, le système d'exploitation Windows et les autres produits Microsoft incluent des mots de passe pour sécuriser nos informations. Cependant dans certaines séries télévisées cela semble à un jeu d'enfant, de contourner ce dispositif. C'est dans l'exemple du série MR Robot S04E03.

Cette procédure de sécurité qui est de mettre un mot de passe à l'allumage de sa machine. Est-ce vraiment efficace et infaillible ?

Pour répondre à ces questions on va se mettre en pratique.

En premier lieu, on va créer une VM avec un Windows 10 Pro dessus. Puis créer un document texte dans le bureau qui s'appelle toto.text

En deuxième lieu on va essayer d'accéder sur le document en supposant de ne pas savoir le mot de passe du compte administrateur.

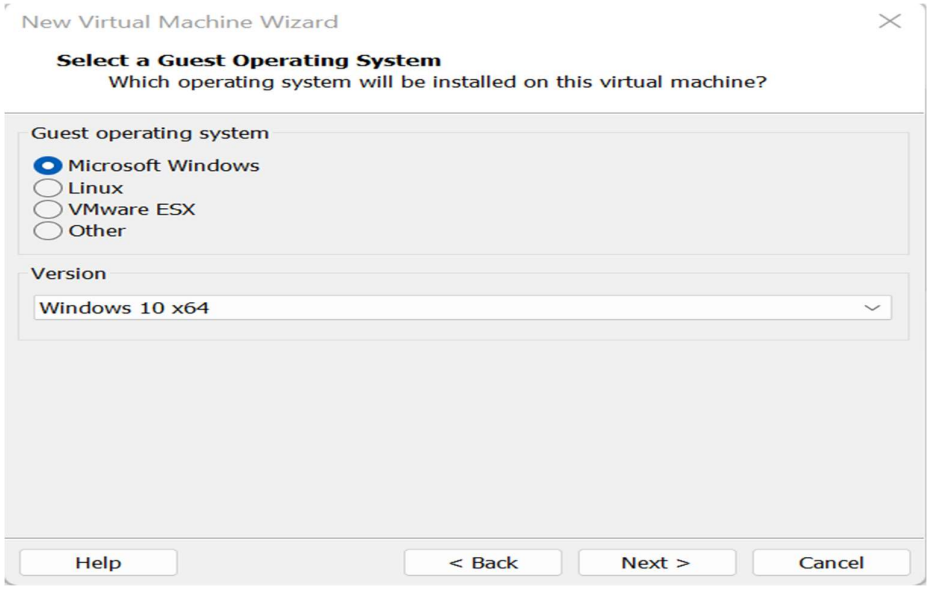
En troisième lieu on va procéder autrement pour avoir accéder au compte administrateur en changeant son mot de passe.

Et enfin on va faire le même procédé sur un VM Linux.

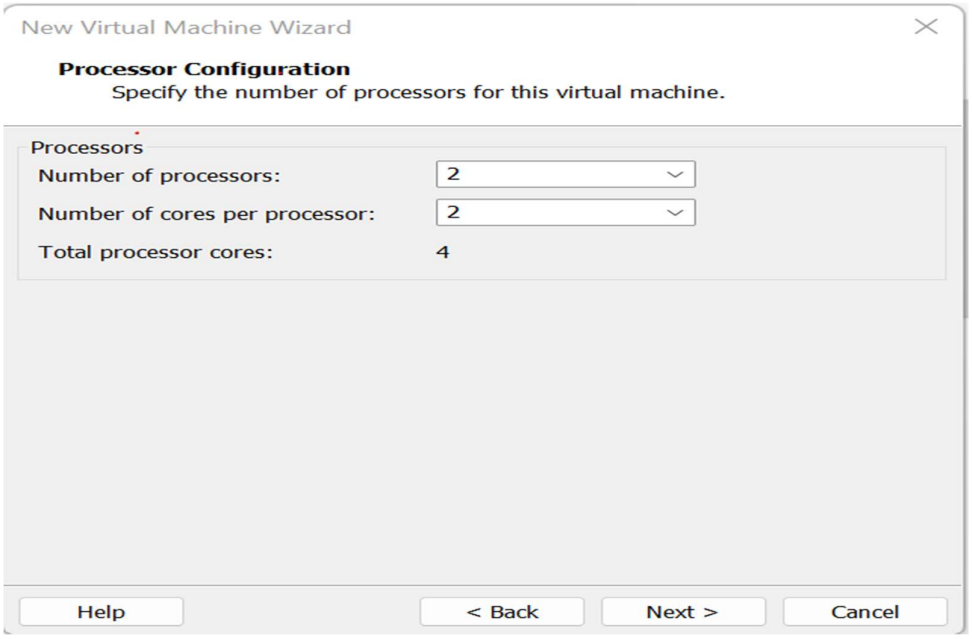
I. La création du VM

1.1. Les quelques différentes étapes de la création de notre VM

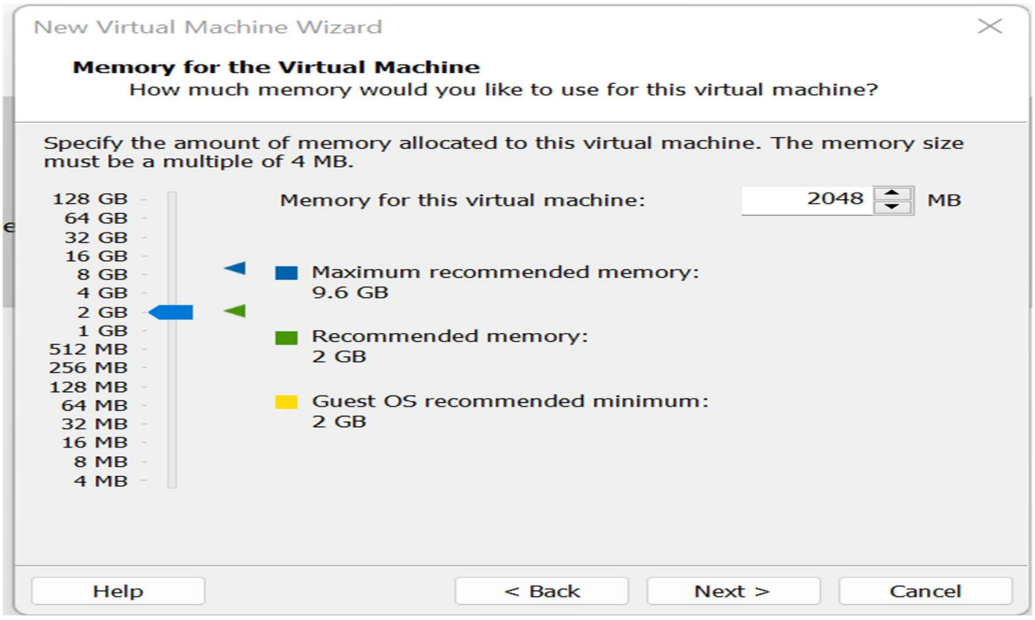
Je choisis d'abord le système opération du VM



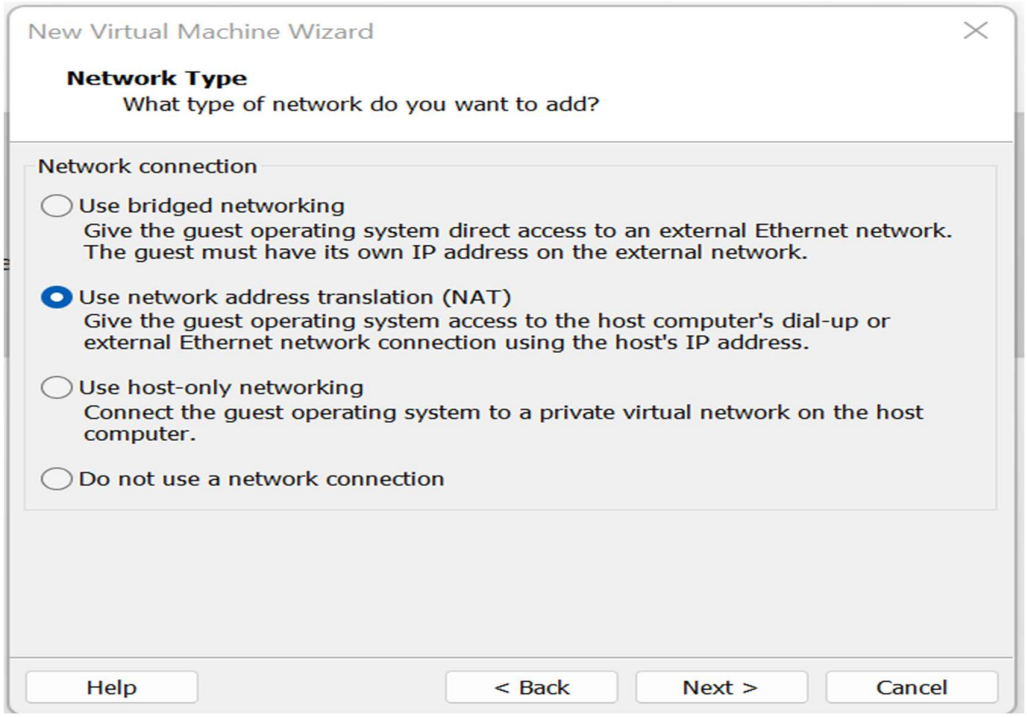
Cette étape correspond à la spécification du nombre de processeurs du VM.
Je choisis cores 4 pour permettre la machine d'être un peu plus rapide à la suite de notre procédure.



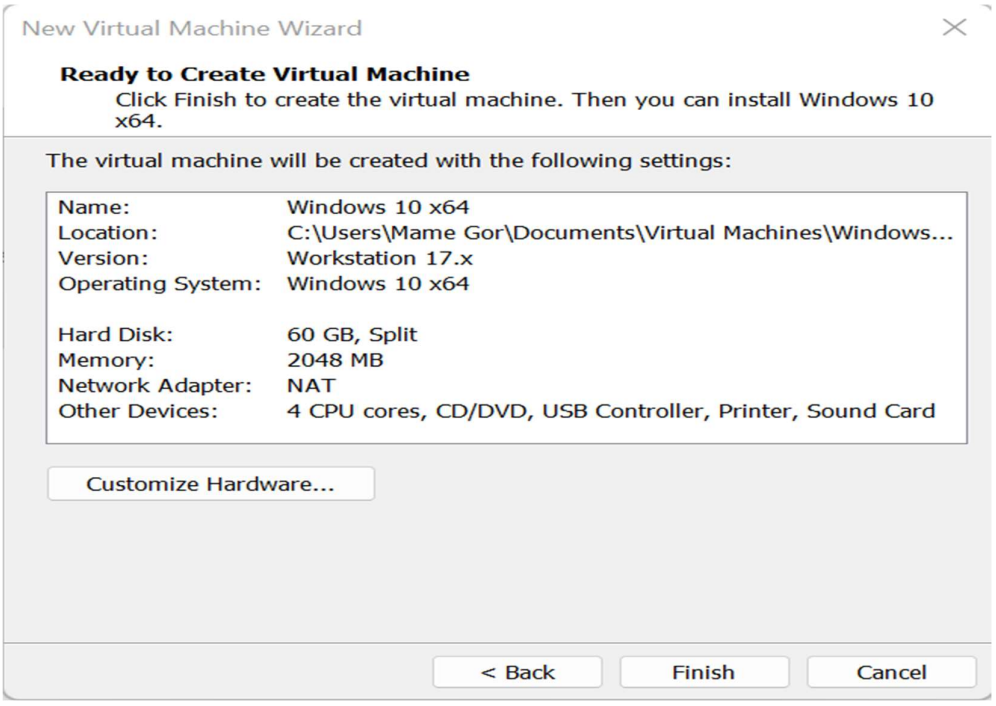
Dans cette étape on choisit le nombre de RAM du VM.



A ce niveau on sélectionne le type du réseau. J'ai sélectionné le NAT pour que mon VM n'interfère pas au réseau externe.

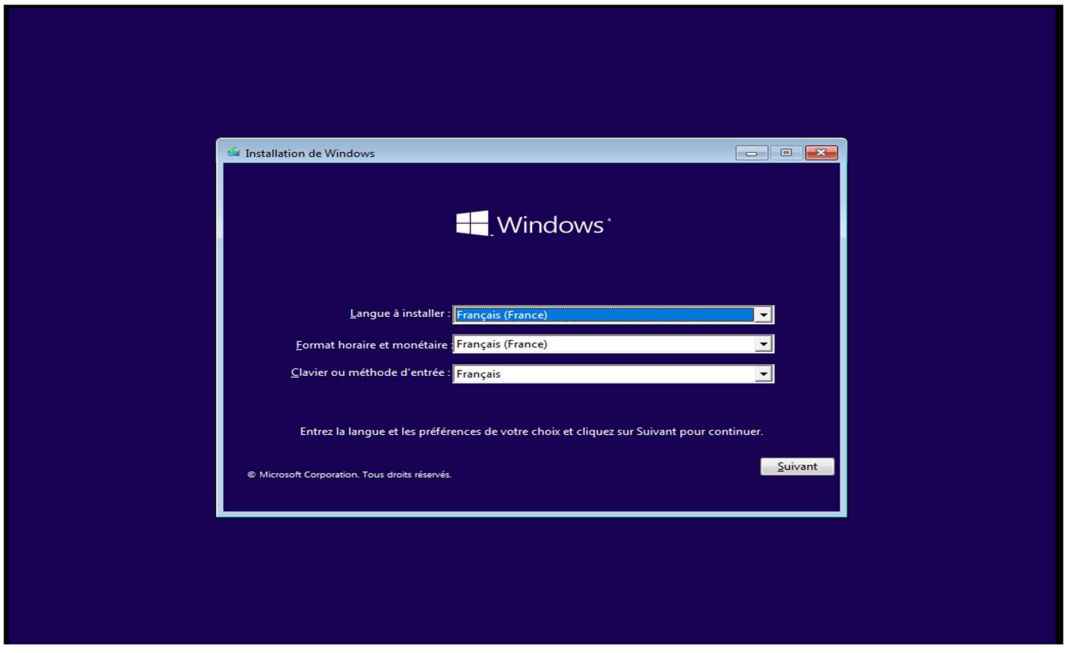


Et enfin une Récapitulatif de de notre futur VM

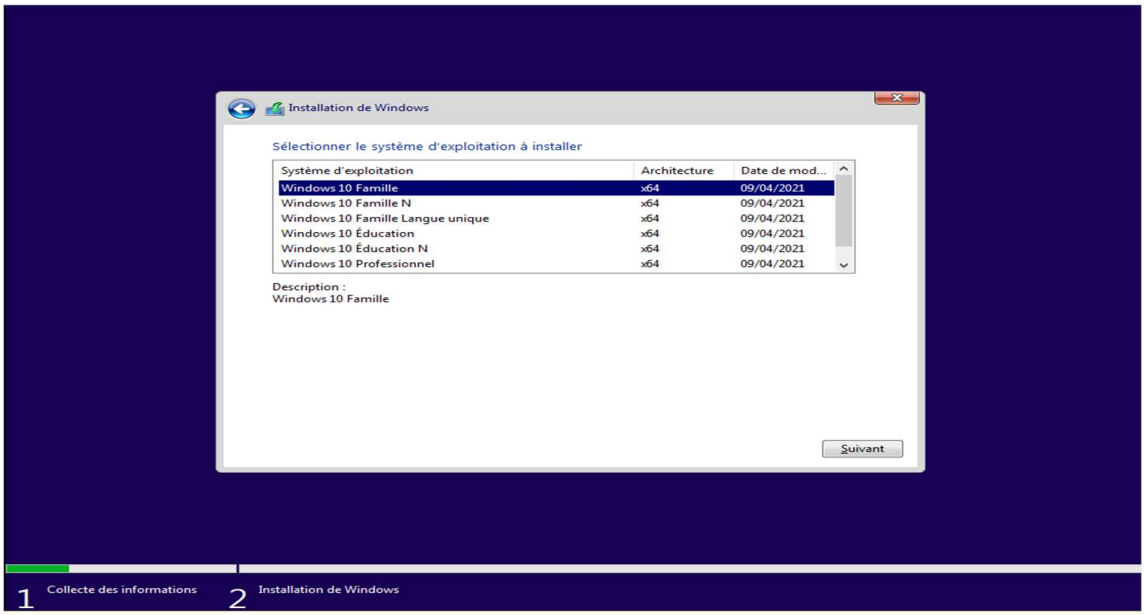


Après avoir insérer l'ISO, on démarre le VM pour finaliser la dernière partie. C'est-à-dire :

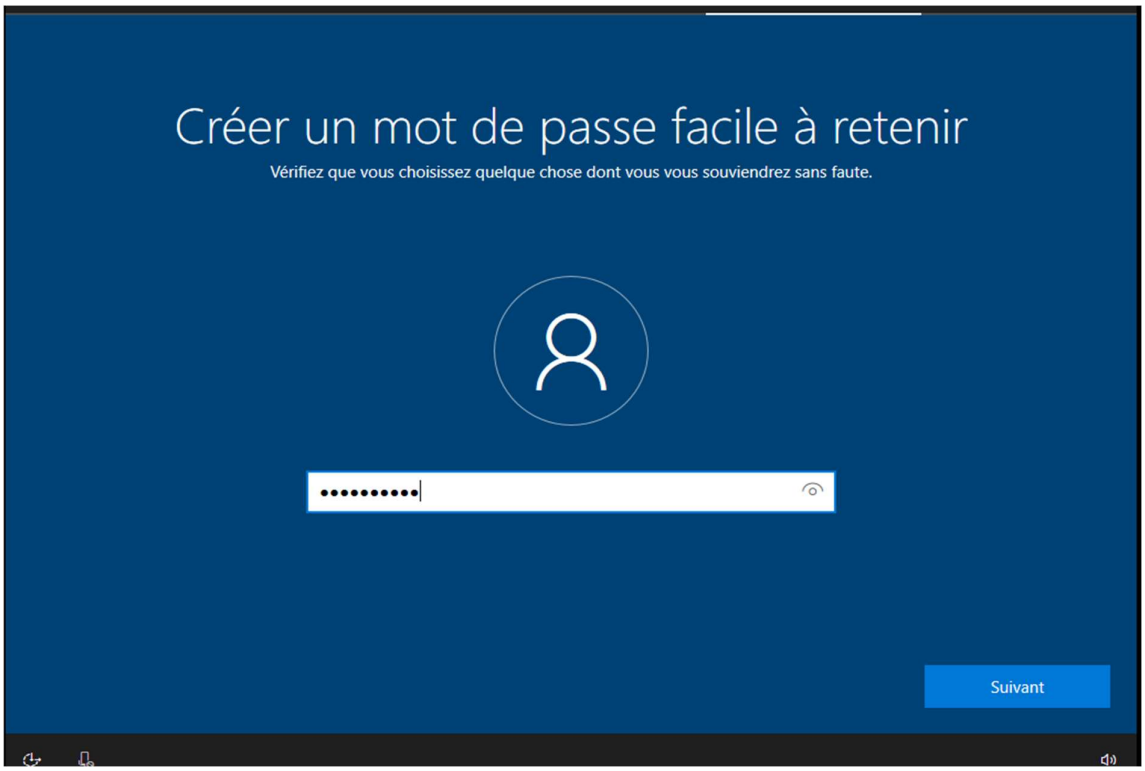
- ✓ Choisir :la langue, le format horaire et la langue du clavier.



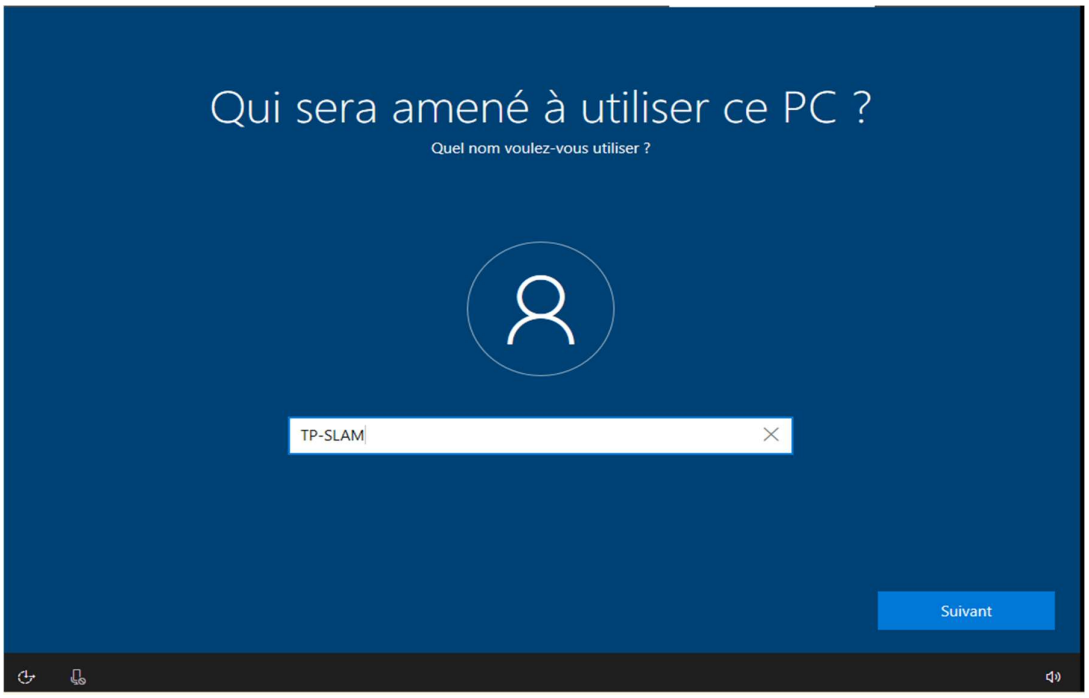
✓ Le système d’exploitation. J’ai choisi Windows 10 famille



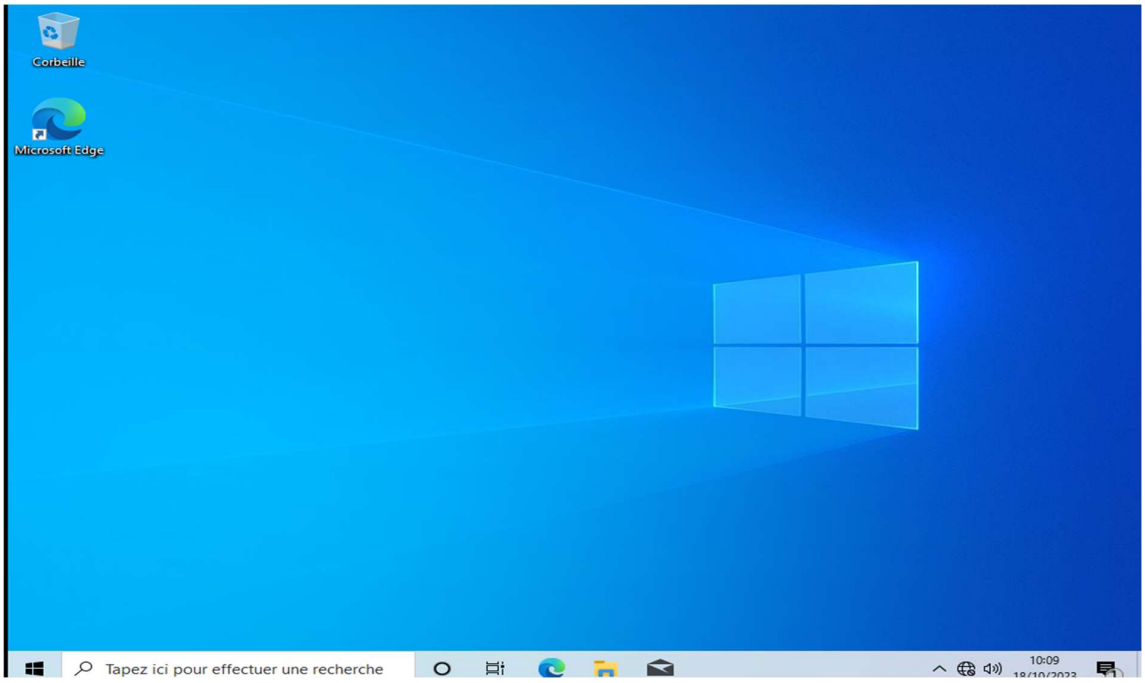
✓ Crée un mode de passe « compte administrateur »



✓ Définir le nom du compte administrateur

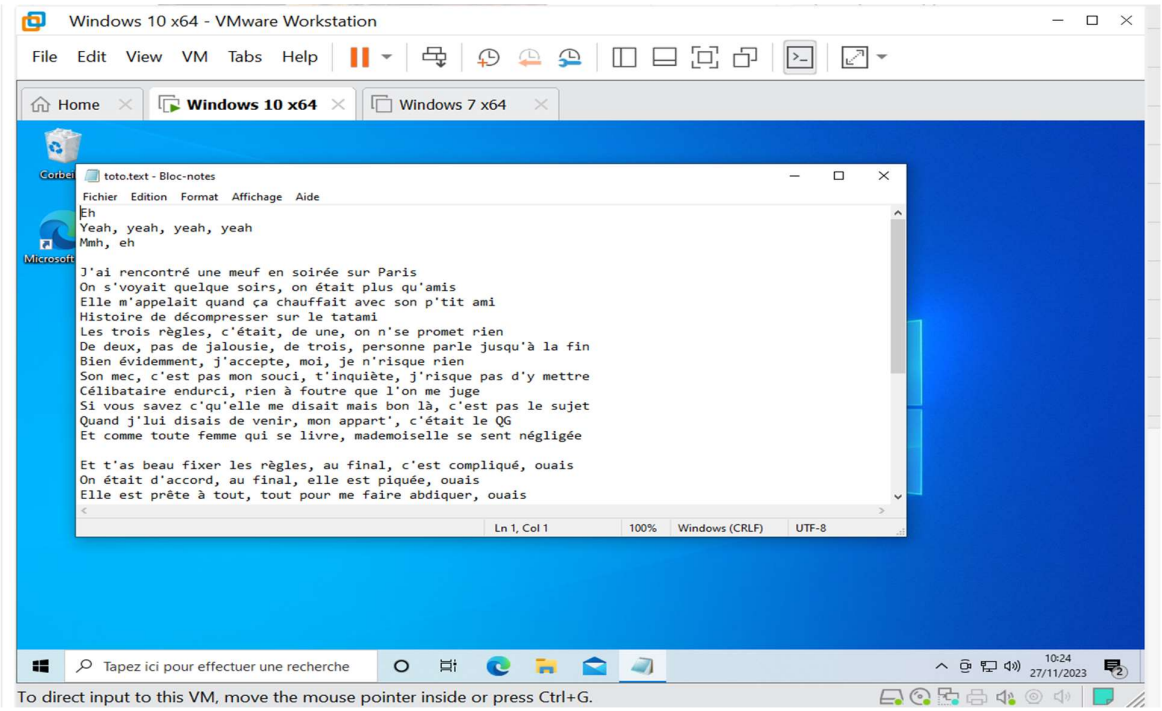


✓ Et voila notre VM est prêt



1.2 La création du document texte

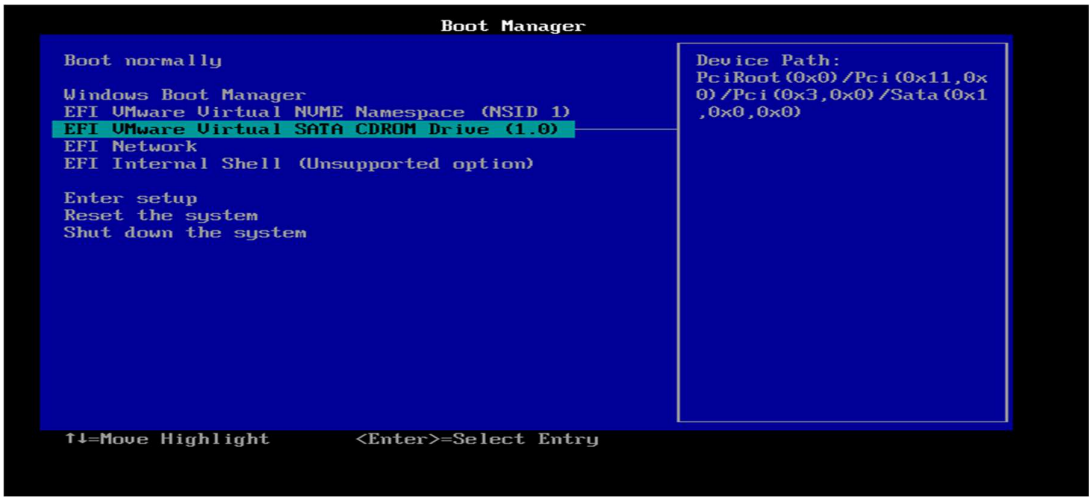
Dans mon VM, je crée dans le bureau un document : toto.text puis j'écris les paroles du chanson Dadju « compliqué » dans le fichier toto. Après j'éteins la machine.



II. Accéder sur le document texte : toto.text

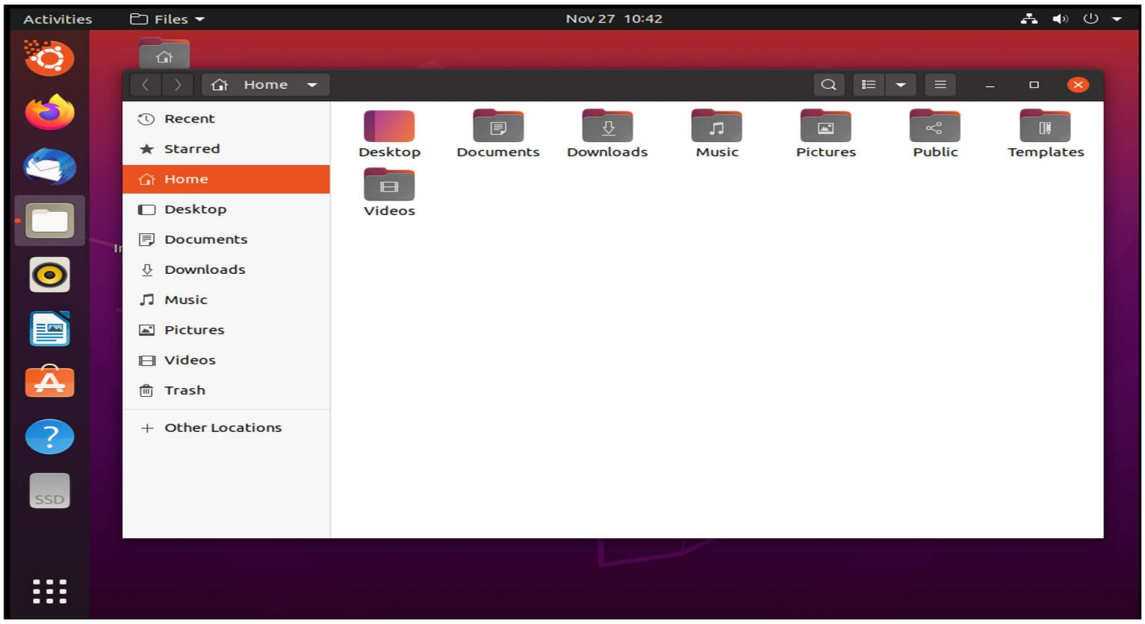
Dans la suite je vais essayer d'accéder sur le fichier toto.text pour lire et modifier le contenu sans oublier que l'utilisateur avais mis un mot de passe qui respecte les normes. En autre terme on va se mettre à la place de l'attaquant.

Pour ce faire, je vais utiliser l'ISO de UBUNTU et booter dessus.

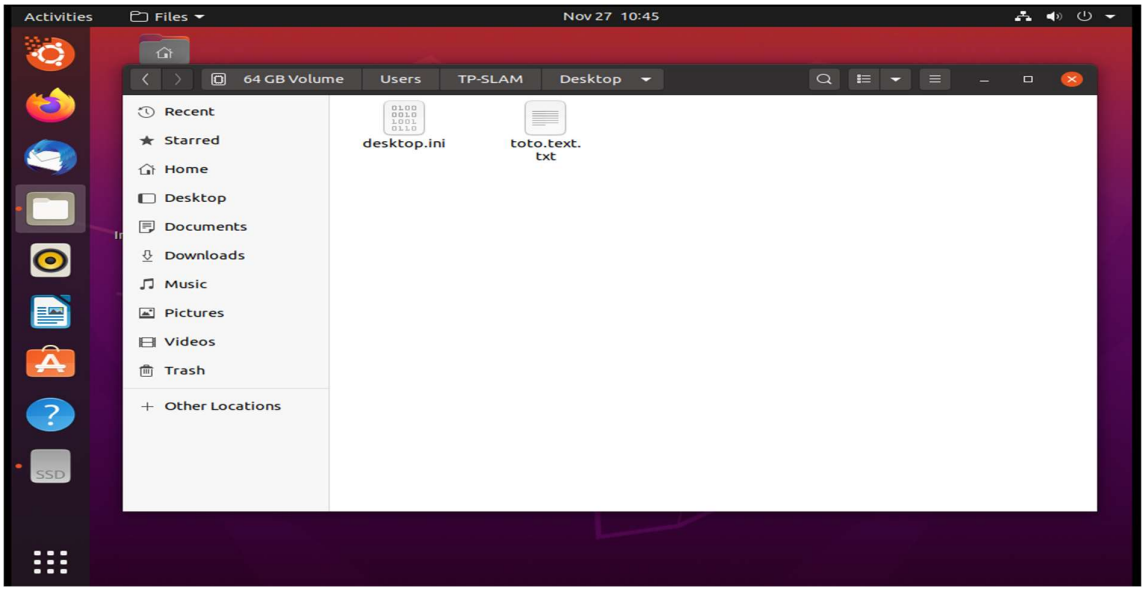


On démarre en mode live-DVD. Pour l'installation et choisis « Essayer Ubuntu »

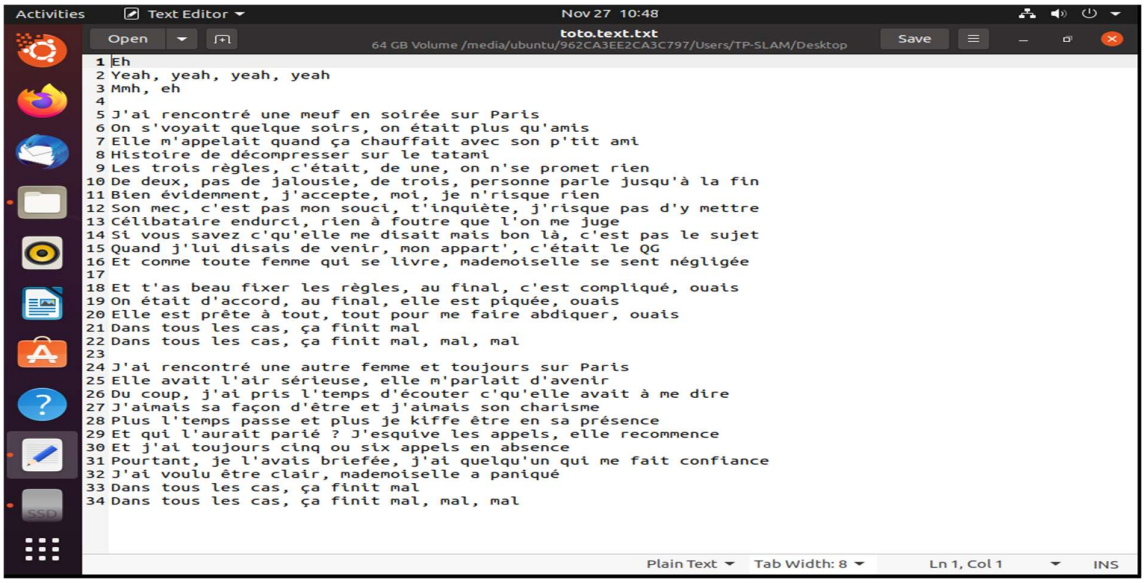
2.1. Trouvons notre fichier toto.text



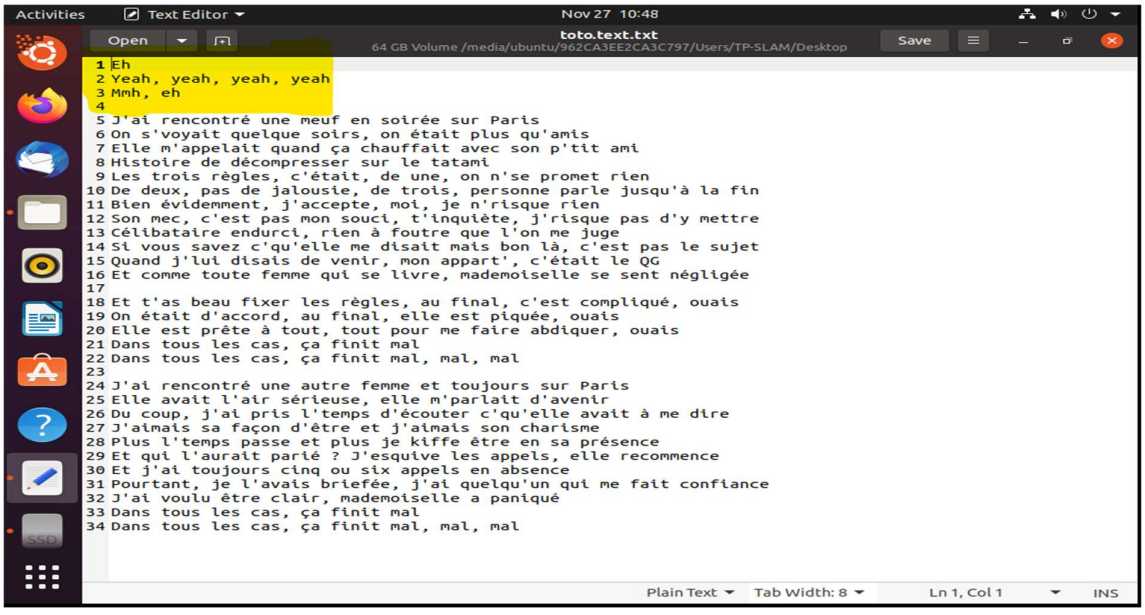
Apparemment le fichier toto.text est dans le VM Ubuntu. Dans le chemin d'accès suivant : fils/other locations/users/TP-SLAM /Desktop.
Et maintenant pour répondre à la question est-il possible de lire le fichier. Je vais faire un clic droit /open.



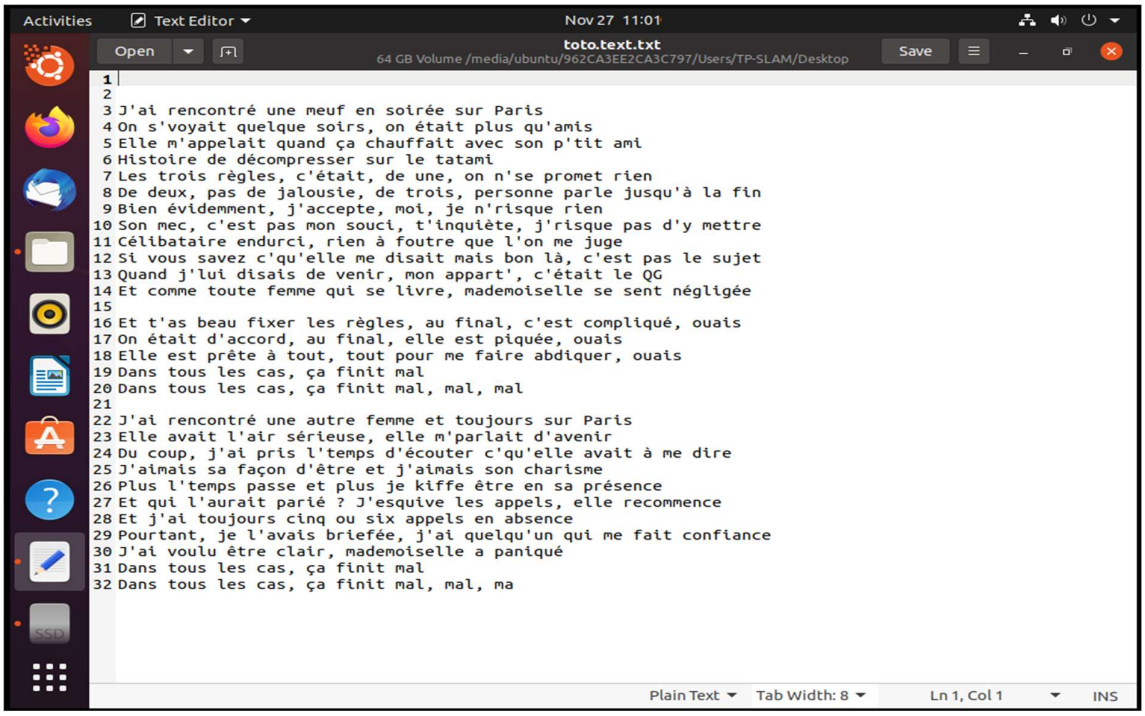
- Bien sûr on peut lire le fichier toto.text, je vois le contenu : les paroles de la chanson de Dadju. Vue que on a accès sur le fichier. Est-il possible de le modifier ? Autrement dit est ce que on a les droits administrateurs pour le modifier. Pour répondre à cette question je vais essayer de supprimer les trois premières lignes du texte puis fais une sauvegarde.



Voici les lignes (colores en jaune) qu'on va supprimer.



Lorsque que j'ai ouvert le fichier de nouveau après la sauvegarde, on ne voie plus les trois premières lignes. Donc on a modifié le fichier toto.text



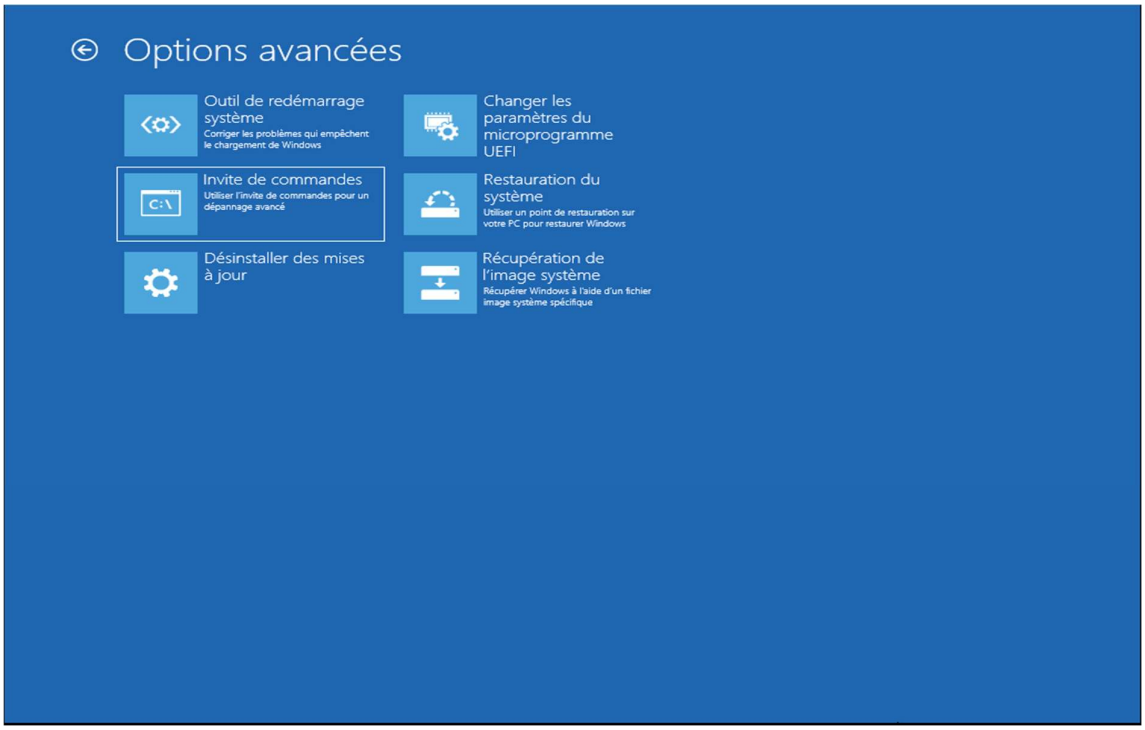
III. Accéder au compte administrateur en changeant son mot de passe.

Dans cette partie, on va réinitialiser le mot de passe Administrateur de Windows 10, en appliquant une méthode parmi les cinq qui sont proposés par le prof

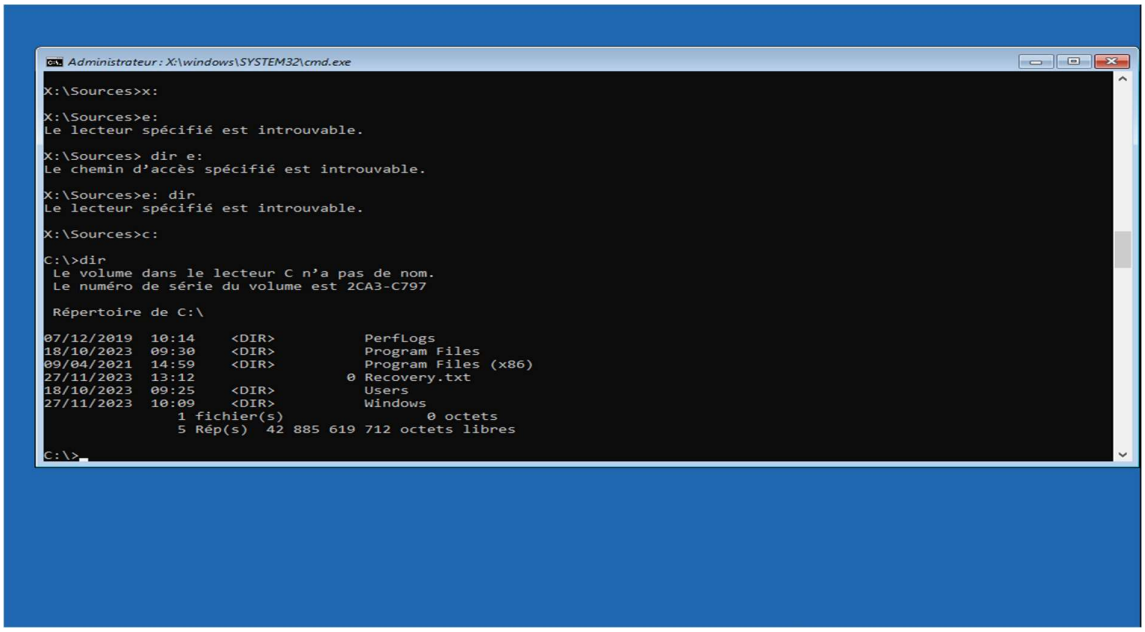
3.1 Méthode n°2b : via l'Environnement de récupération Windows (WinRE)

Cette méthode consiste à remplacer l'exécutable "Utilman.exe" par "Cmd.exe" (Invite de commandes) dans les fichiers système de Windows.

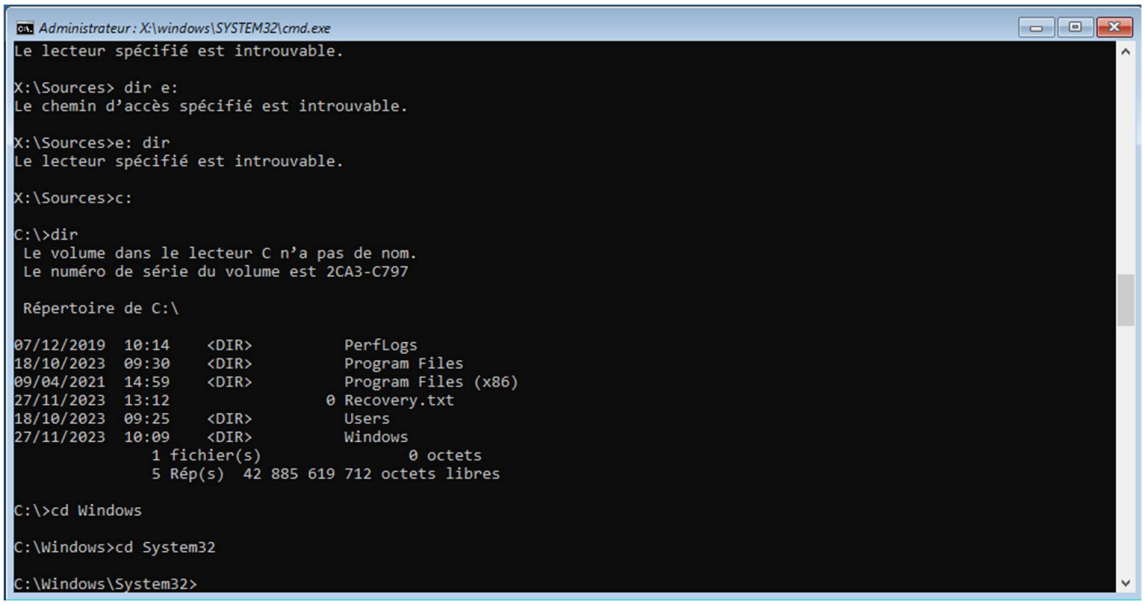
1. D'abord je vais **Lancez l'invite de commandes.** Notre VM est un Windows 10, donc je vais aller dans le bios en appuyant sur F4 (NB : sa peut être différent selon les machines) lors du démarrage. Après on choisit Options de démarrage avancées puis sélectionnez Dépannage ensuite Options avancées et en fin Invite de commandes.



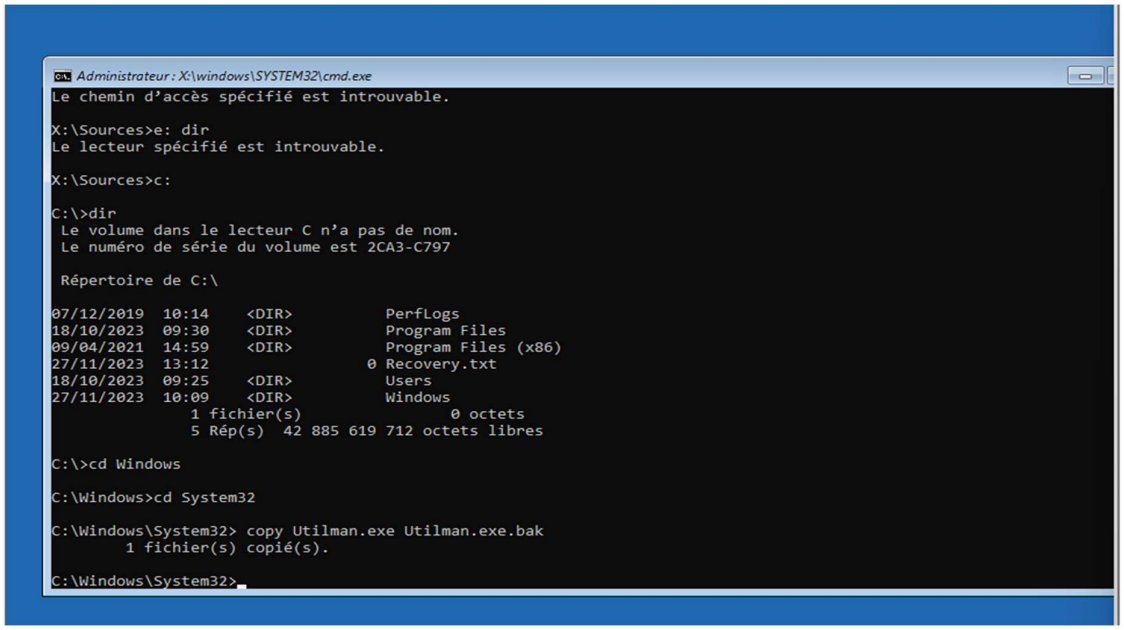
2. Une fois dans le cmd on cherche notre lecteur qui correspond à notre installation. Pour savoir quelle lettre correspondant à notre installation de Windows, on entre une lettre (par exemple C:) puis saisisse la commande « dir » pour lister son contenu. Si on retrouvez les dossiers propres à Windows (Program Files, Users, Windows…), c'est que on y est.



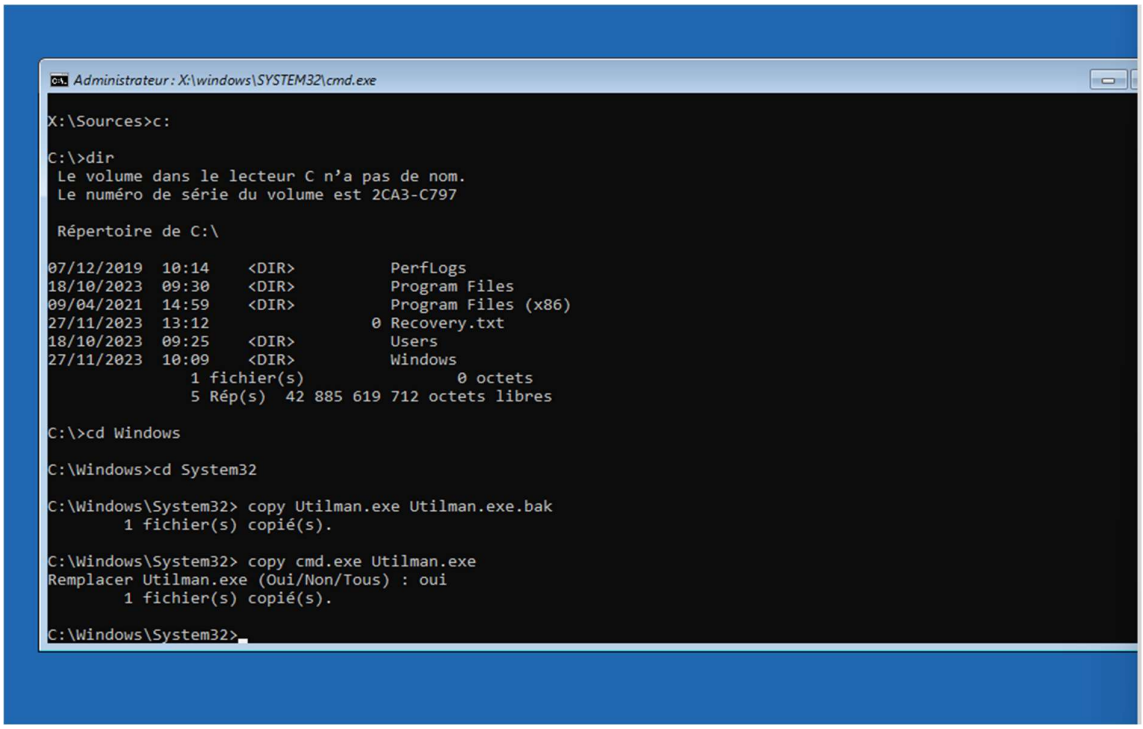
3. Maintenant on est sur le lecteur contenant Windows. J'utilise le commande « cd » pour se déplacer dans le dossier Windows\System32.



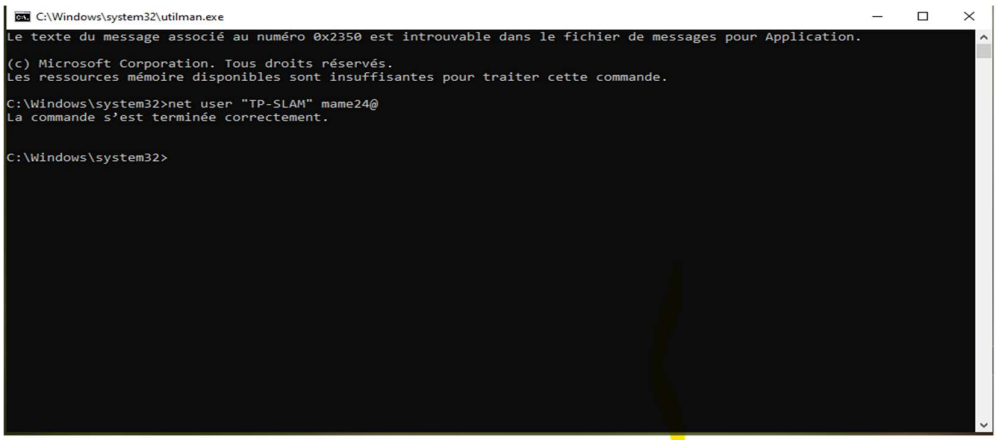
4. Après on crée une sauvegarde du fichier utilman.exe, en utilisant le ligne de commande suivant : Copy Utilman.exe Utilman.exe.bak



5. Par la suite on remplace les options d'ergonomie utilman.exe par l'invite de commandes : copy cmd.exe Utilman.exe

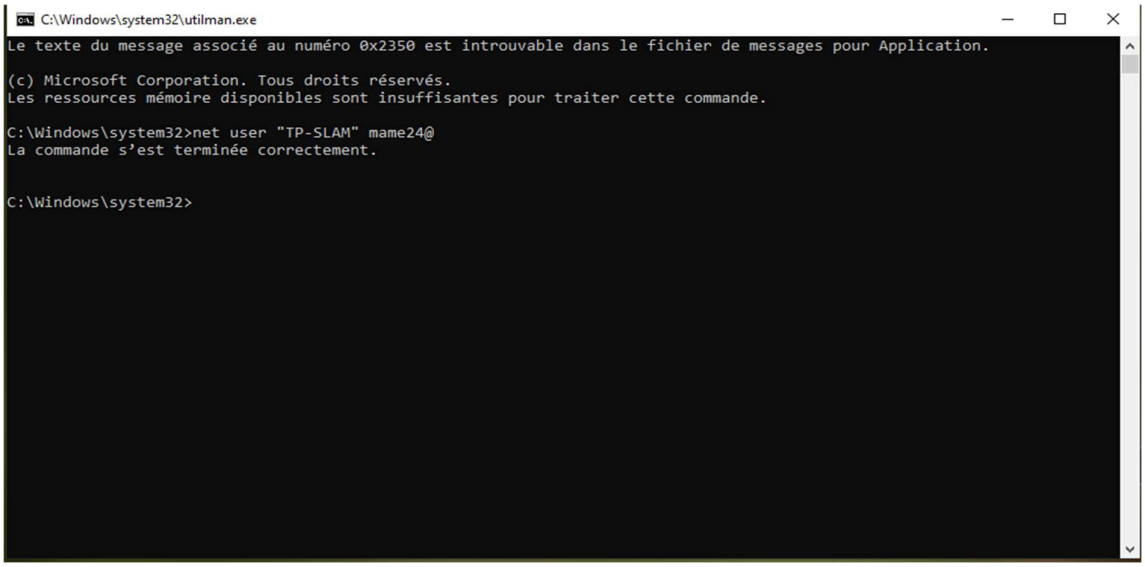


6. A ce point on va redémarrer notre VM. Et Sur l'écran de connexion de Windows, on appuie sur les touches Win + U pour lancer l'invite de commandes (en lieu et place des options d'ergonomie).



7. Maintenant on peut changer le mot de passe Pour réinitialiser le mot de passe d'un compte utilisateur, on tape la commande suivante : « net

user "nom_compte_utilisateur" nouveau_mot_de_passe » (net user ‘’TP-SLAM’’ 4321Azerty@)



C’est fait on a changé le mot de passe du compte utilisateur TP-SLAM.

- Cette même méthode est utilisée par Elliot dans la série Mr Robot S04E03

Une petite conclusion

D'après ce qu'on vient de découvrir, il est possible de réinitialiser le mot de passe d'un compte utilisateur en exploitant une faille de sécurité de Windows. La méthode que je viens d'utiliser en ai une preuve. En gros il s'agit de renommer le fichier utilman.exe en cmd.exe afin qu'en pressant les touches Windows + U nous puissions avoir l'Invite de commande Windows à la place des options d'ergonomie

3.2 Deux manières de se protéger de ce problème :

On peut utiliser BitLocker pour protéger le lecteur système. En effet il ne sera pas possible de réinitialiser le mot de passe Administrateur avec la méthode employée ci-dessus ! Sauf si la personne connaît le mot de passe de déverrouillage (sur un PC sans puce TPM) ou la clé de récupération pour déverrouiller manuellement le lecteur chiffré.

Ou en utilisant LAPS Legacy ou Windows LAPS. De ce fait Windows ne nous permettra pas de réinitialiser le mot de passe par ce que le compte est contrôlé par une stratégie externe.

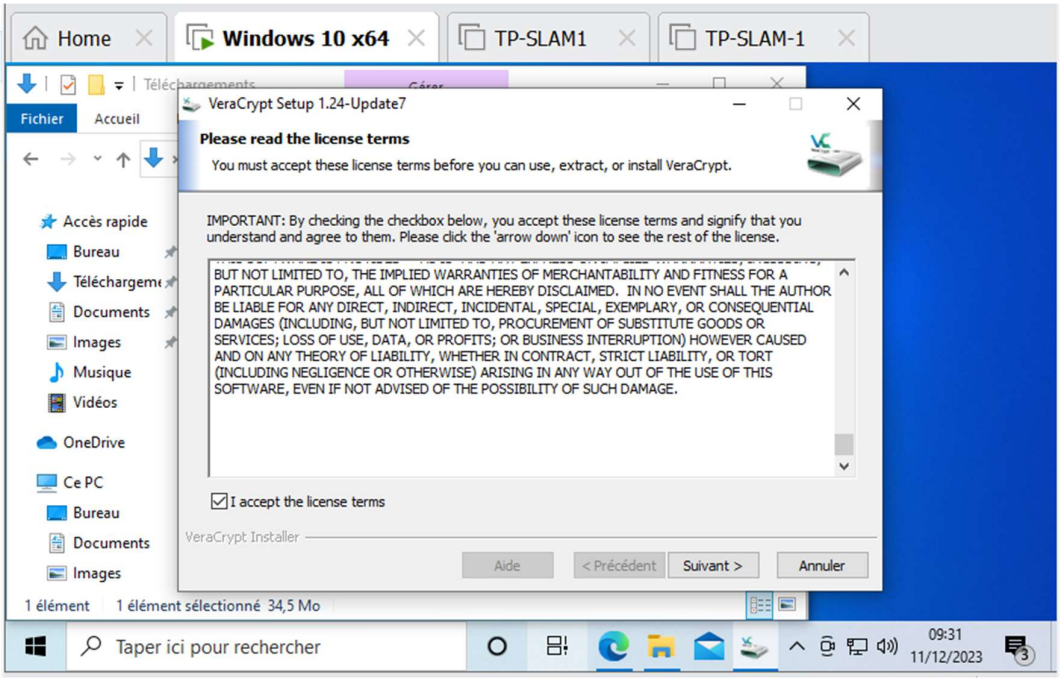
Ou encore VeraCrypt.

3.3 Exprimons les dans noter VM

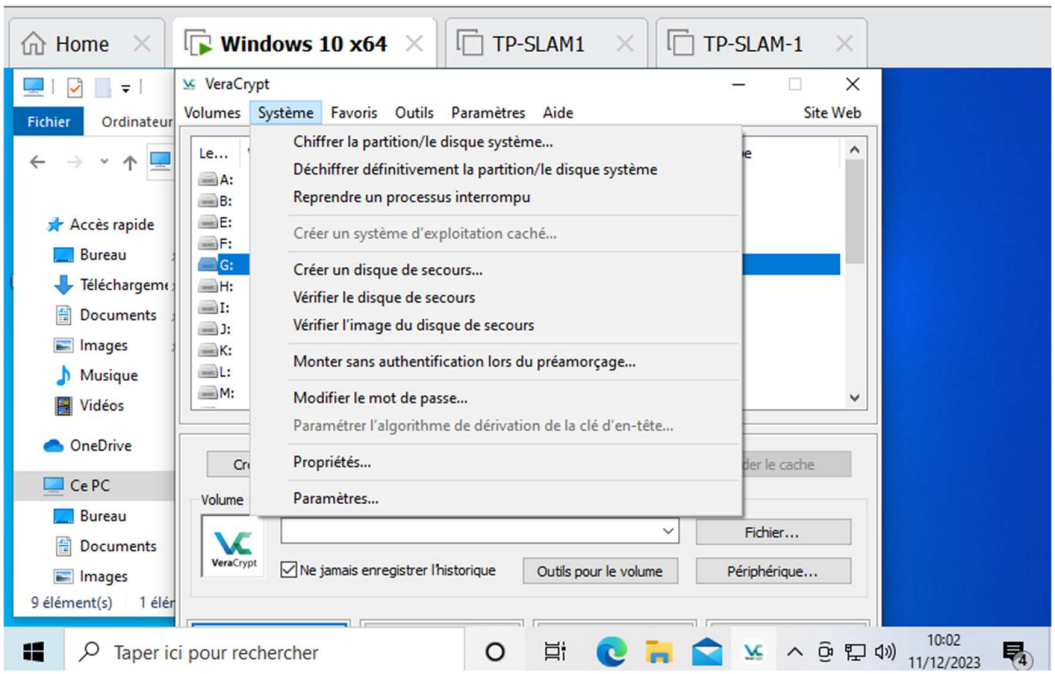
Pour notre cas on va utiliser VeraCrypt pour chiffrer notre lecteure. Ce logiciel est une alternative à BitLocker, le logiciel de chiffrement de Microsoft. Vue que on utilise Windows 10 home on ne peut pas utiliser BitLocker. Par contre VeraCrypt peut être utiliser sur n'importe quelle version (Windows 10, 8, 7, Vista, XP) et n'importe quelle édition de Windows.

On va passer à l'installation de VeraCrypt et le chiffrèrent de notre disque système.

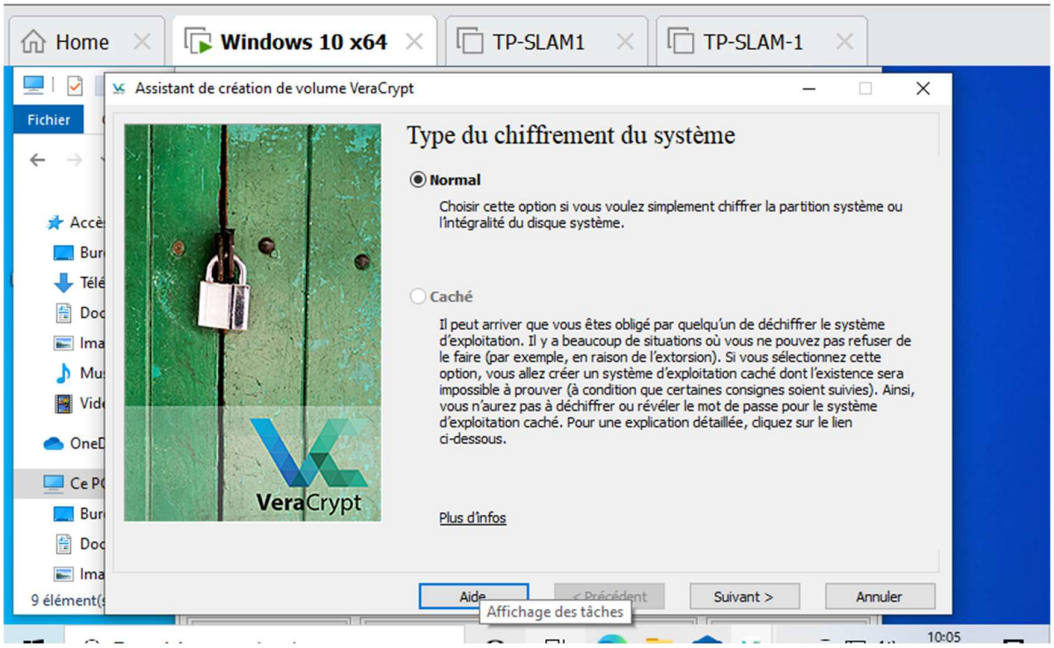
D'abord je vais installer veraCrypt



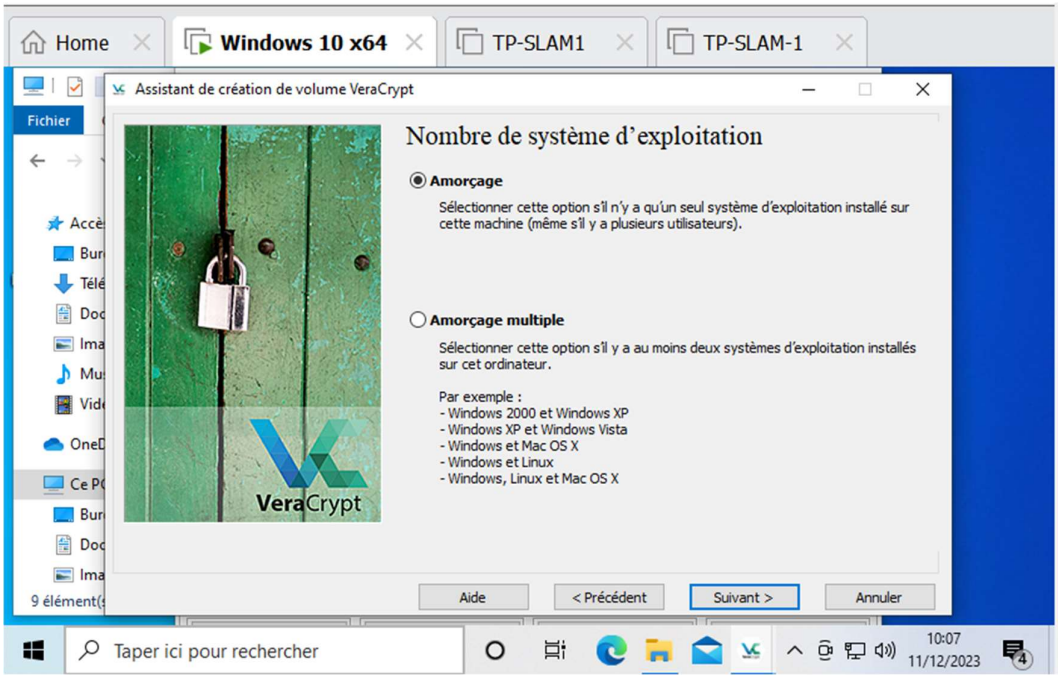
Je vais ouvrier VeraCrypt puis sélectionner système /chiffrer la pation/le disque système



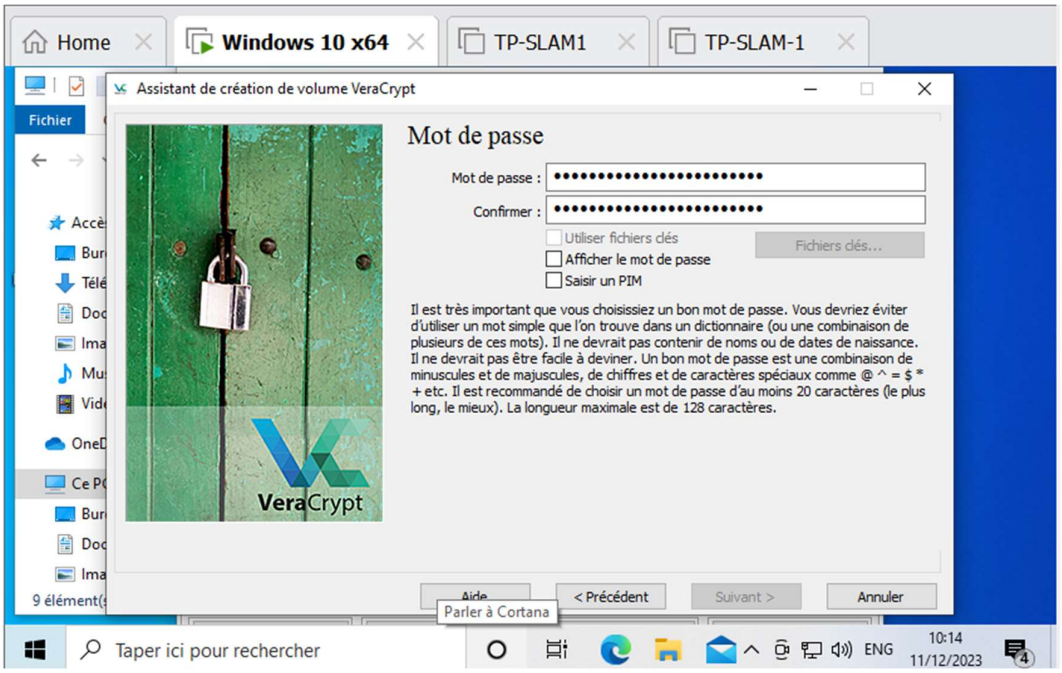
Je sélectionne normal



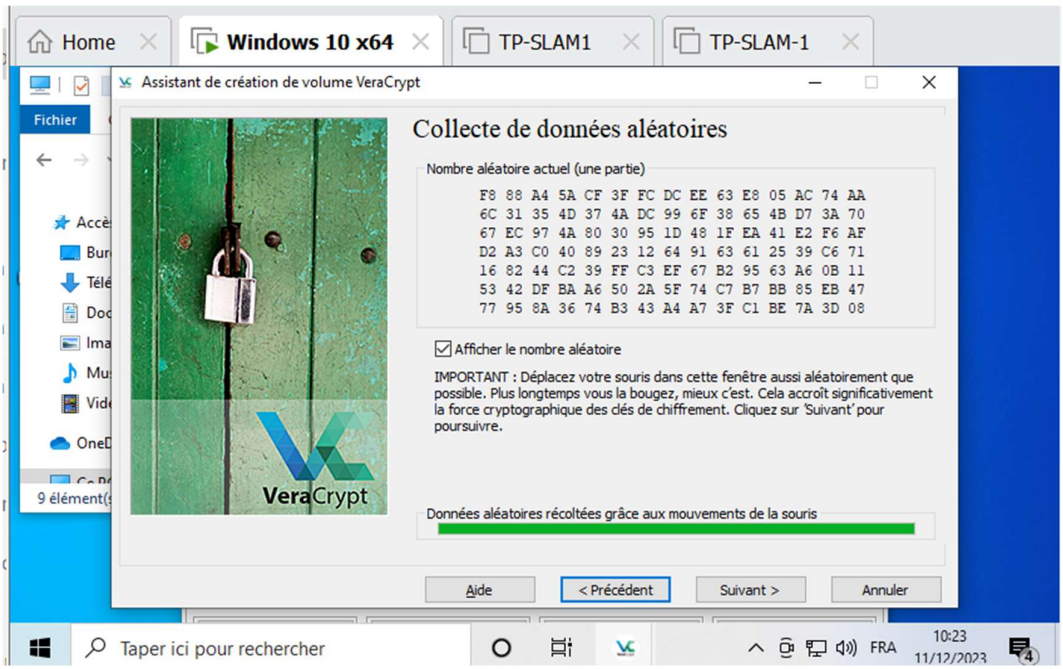
Dans Nombre de système d'exploitation, je vais sélectionner Amorçage parce que on a qu'une seule installation sur notre vm



Dans cette partie je choisis le mot de passe

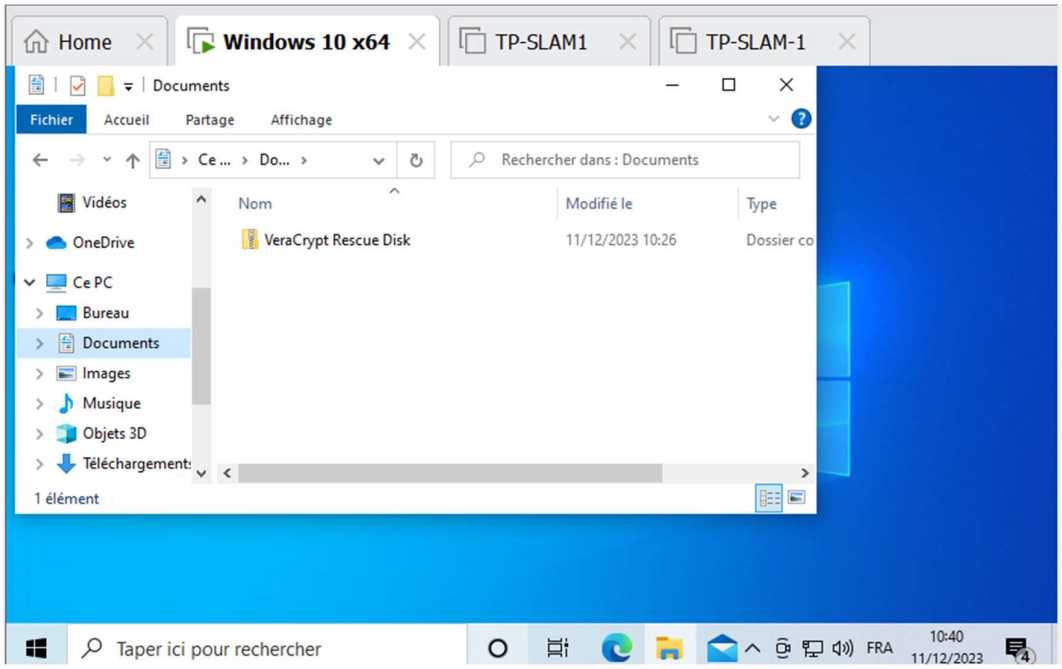


VeraCrypt utilise ces mouvements de souris pour augmenter la force des clés de chiffrement. Une fois la barre de progressio est remplie, je clique sur Suivant.



Pour la suite il faut une clé USB pour Décompresser le fichier ZIP. Malheureusement on n'a pas de clé USB pour continuer les manipulations.

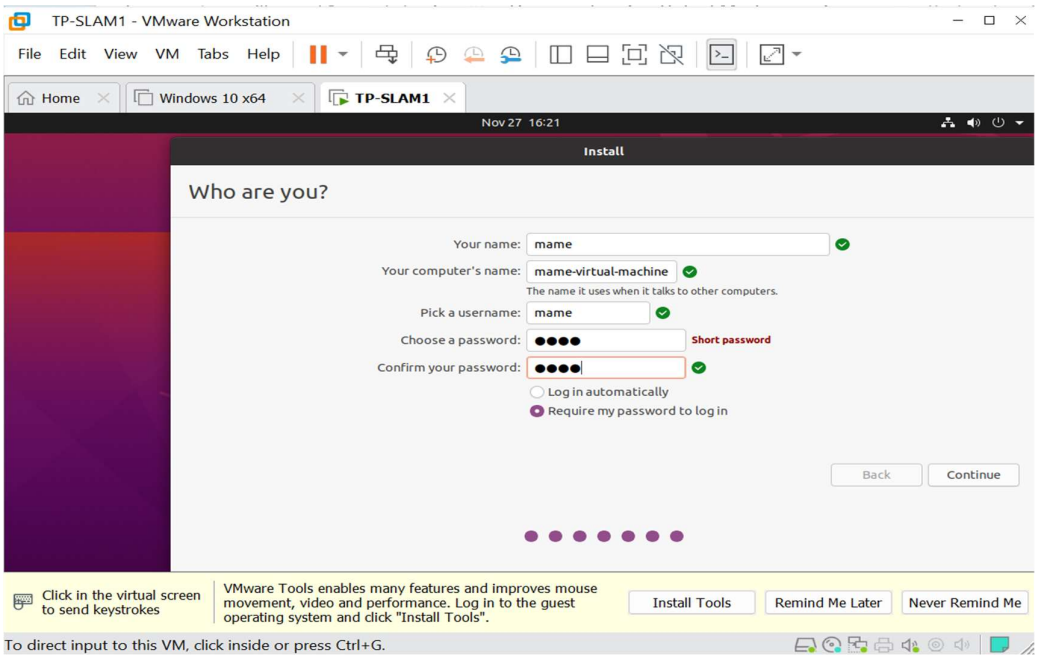
Voici le dossier veraCrypt qu'on devait décompresser



IV. Le même procédé sur un VM Linux

Dans cette partie je vais créer un VM Ubuntu dont le compte administrateur contient un mot de passe. Par la suite on va essayer de se connecter sur ce même compte en supposant de ne pas connaitre le mot de passe du compte administrateur. Autrement dit on va faire la même chose qu'on a fait sur Windows.

4.1 La création du VM Ubuntu



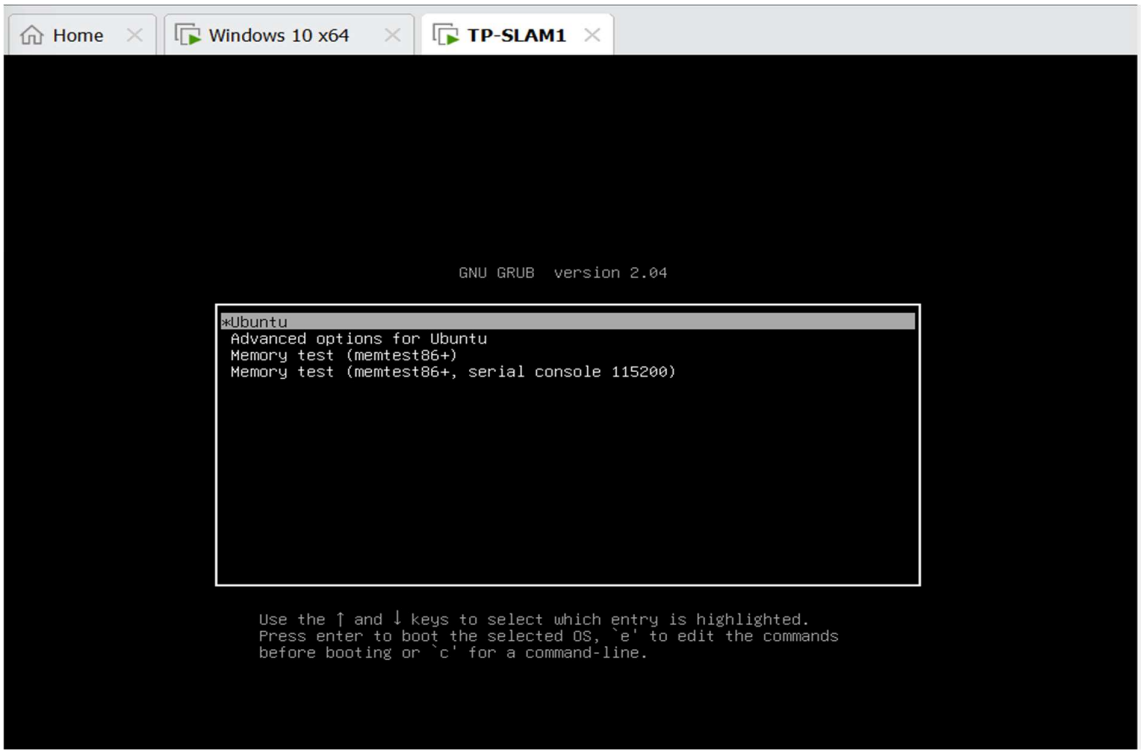
Accéder sur le compte admis sans connaître le mot de passe ?

Pour ce faire on va démarrer notre VM en mode rescue.

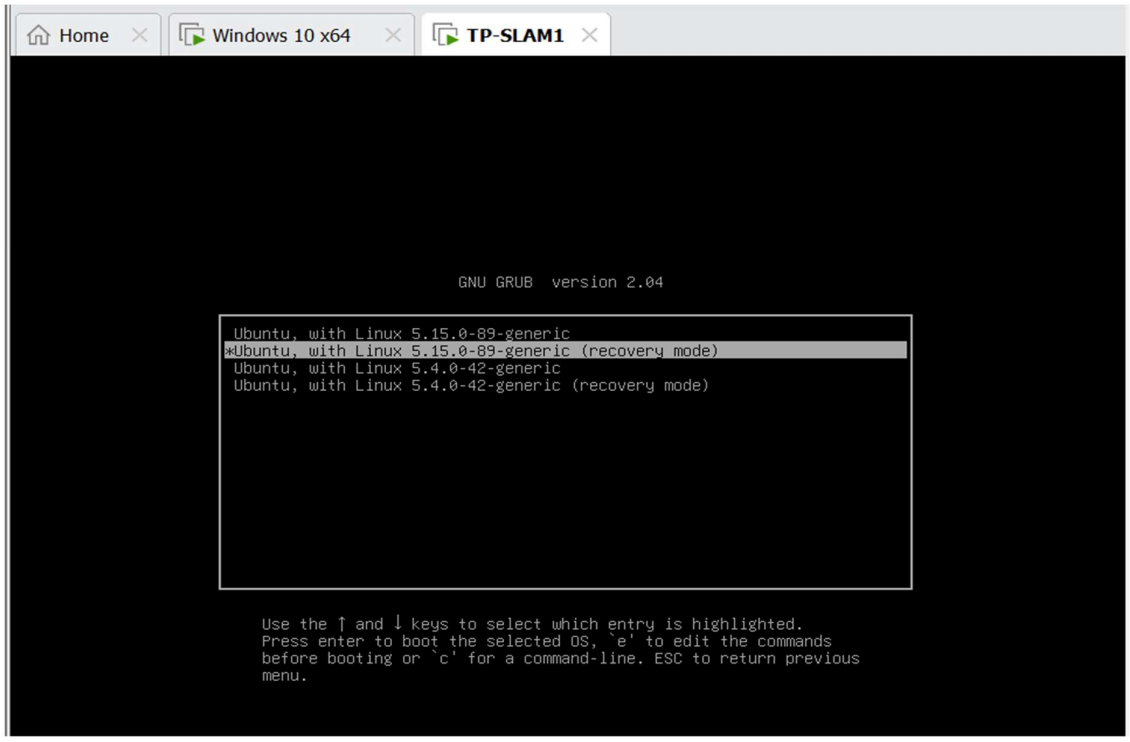
Le mode rescue est un mode de récupération que l'on peut activer au démarrage du PC. Cela permet d'accéder à des outils de dépannage intégré à la distribution Linux.

Pour ouvrir le mode rescue, j'ai appuyé sur la touche **ESC** au démarrage.

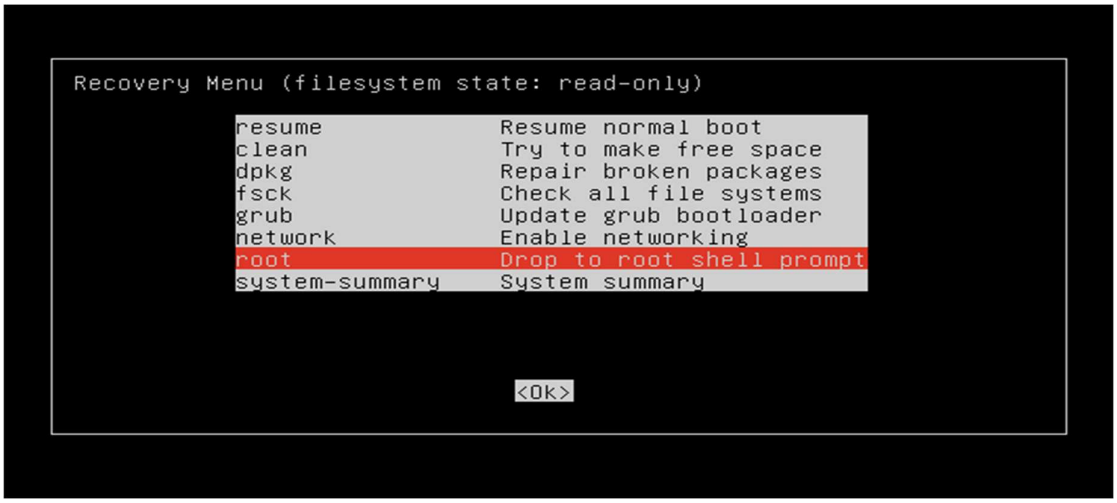
Ensuite on choisit Options avancées pour Ubuntu (Advanced option for Ubuntu).



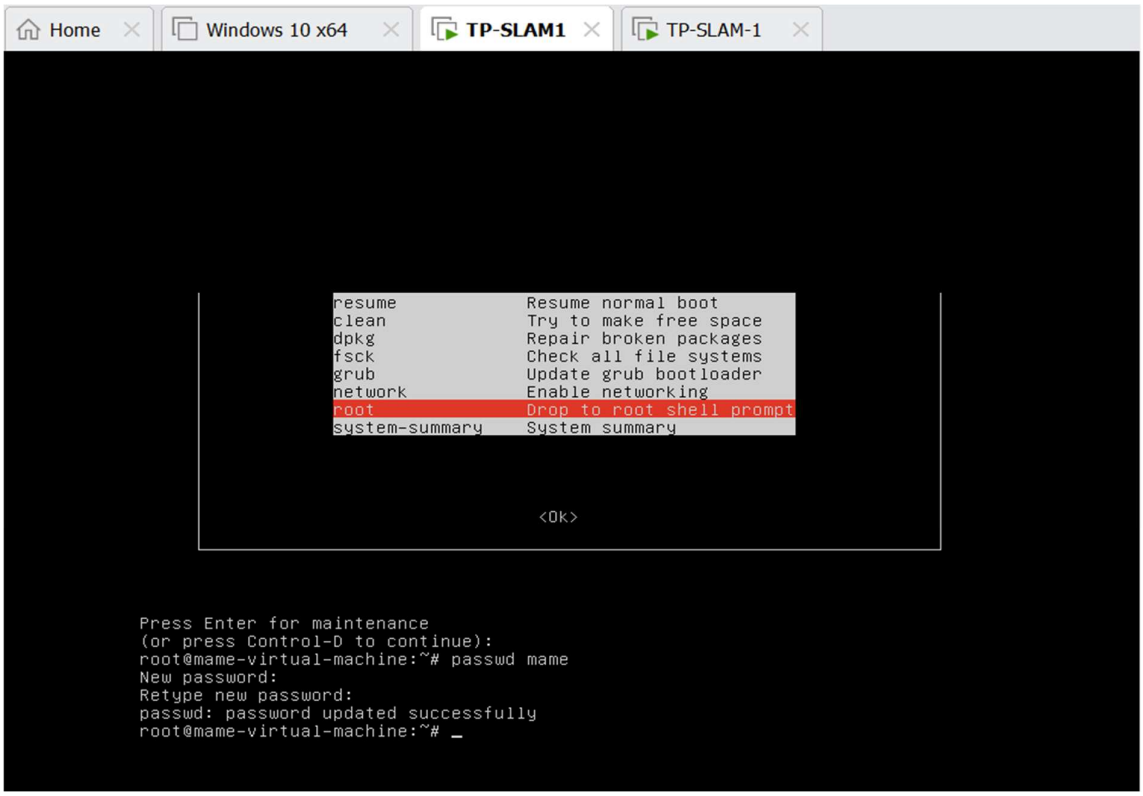
Après on sélectionne la deuxième option (recovery mode)



Dans le menu de récupération, on sélectionne Root puis appuie sur entrée

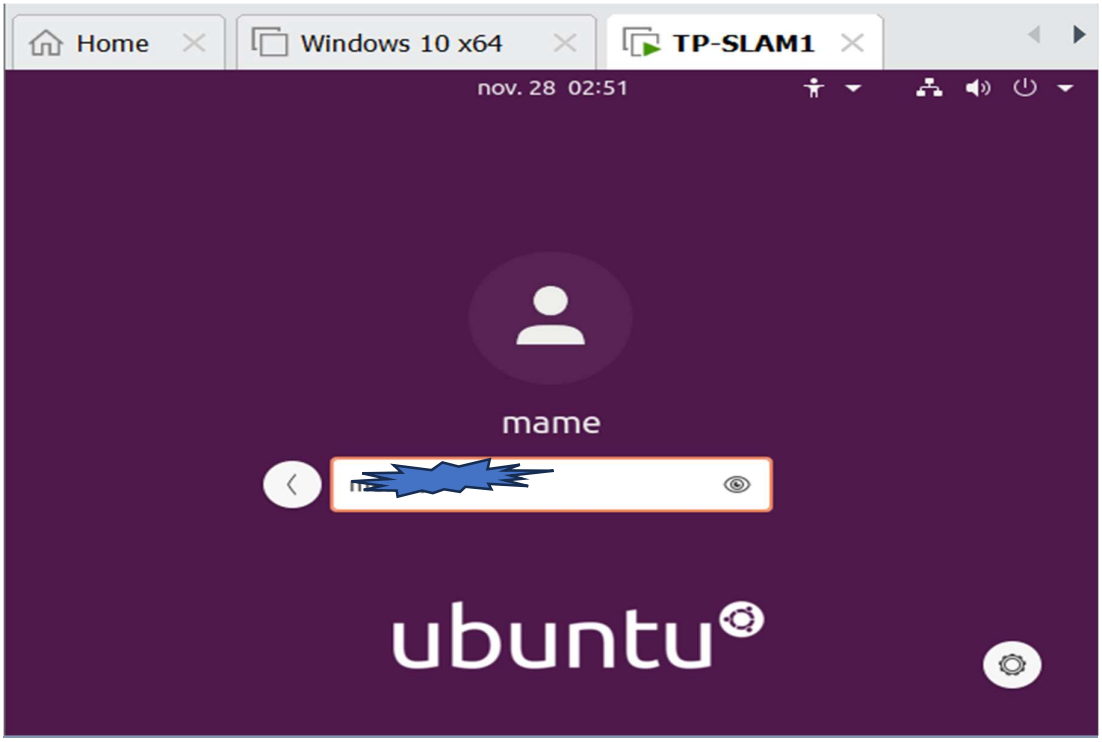


Ainsi on appuie sur la touche entrée du clavier. Puis pour réinitialiser le mot de passe de l'utilisateur, on utilise la commande passwd ex passwd mame et taper le nouveau mot de passe.



Et en fin il ne reste qu'a saisi exit pour revenir au menu de récupération, sélectionné Résume et ok

Maintenant essayons de se connecter avec le nouveau mot de passe qu'on a créer



Conclusion :

Grâce à ce TP, je suis capable de réinitialiser le mot de passe administrateur d'une machine sous Windows mais aussi comment se protéger à ce problème.