TP2 : Intrusion simple Windows - Bloc 3 - JOBARD Guillaume

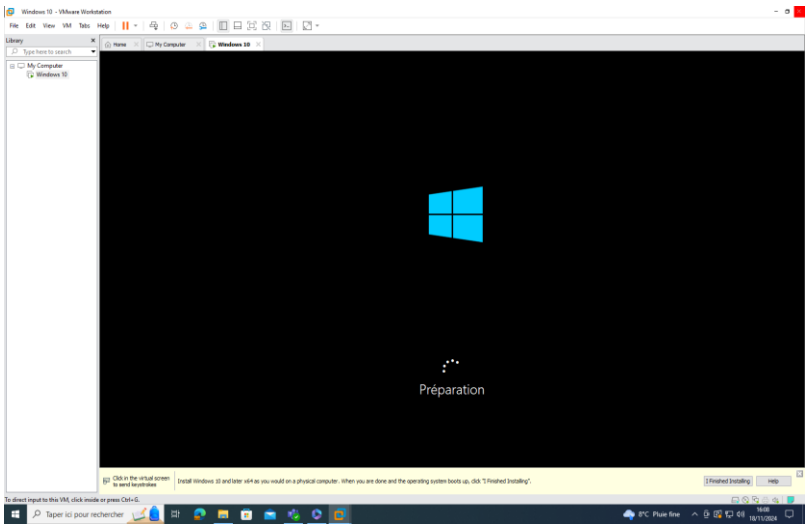
Mouhamed Messaoud HAMOUD SISR-1

INTRODUCTION

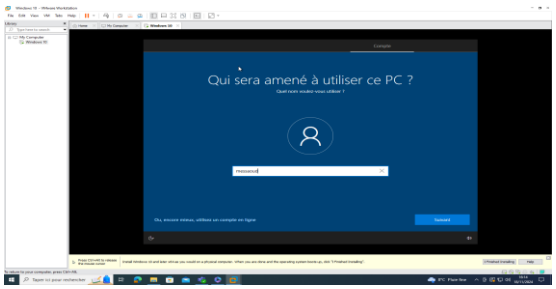
La sécurité des machines sous Windows est essentielle dans un monde où les cyberattaques sont de plus en plus fréquentes. En raison de sa large utilisation, Windows est une cible privilégiée pour les attaquants. Ces derniers peuvent exploiter des failles de sécurité, souvent dues à une mauvaise configuration, des mots de passe faibles ou des logiciels obsolètes.

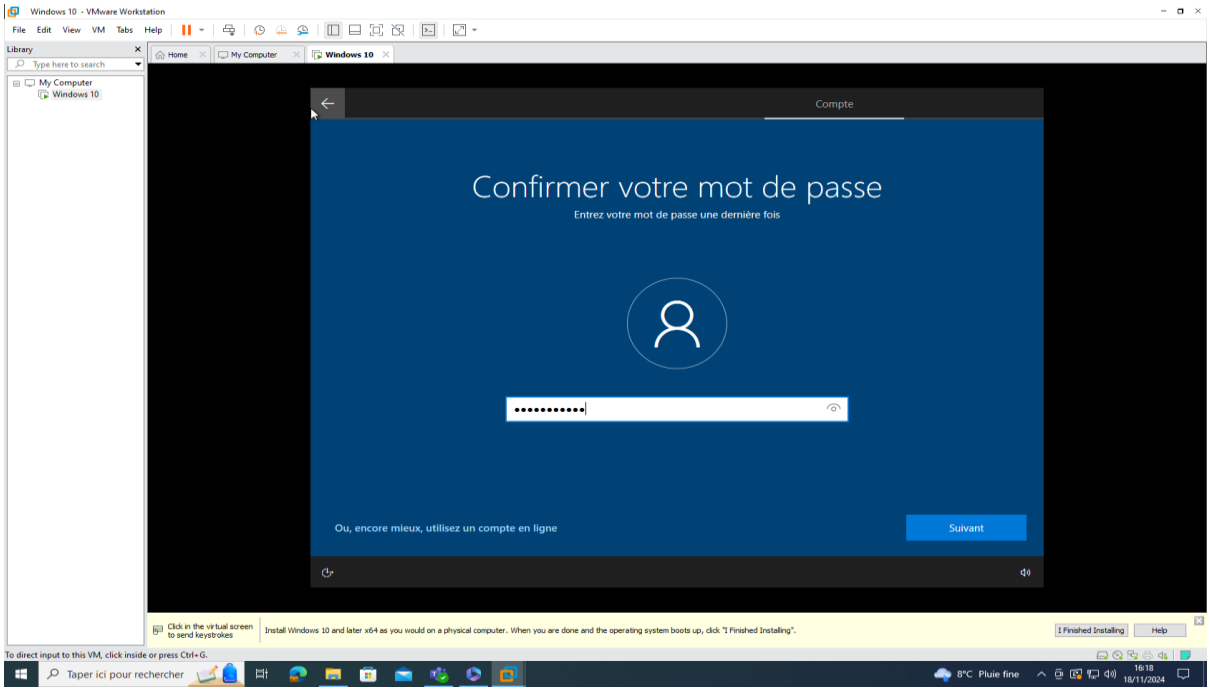
Pour bien sécuriser une machine, il est crucial de comprendre comment un attaquant pourrait l'infiltrer. Se mettre à leur place permet de mieux anticiper les vulnérabilités et d'adopter les bonnes mesures de protection. Il est important de souligner que pénétrer une machine Windows n'est pas aussi difficile qu'il n'y paraît. Avec les outils appropriés et une bonne connaissance du système, un attaquant peut exploiter des failles de manière relativement simple. C'est pourquoi une approche proactive de la sécurité, en anticipant les risques et en renforçant les défenses, est primordiale.

I- Créons une machine virtuelle avec Windows 10 pro dessus

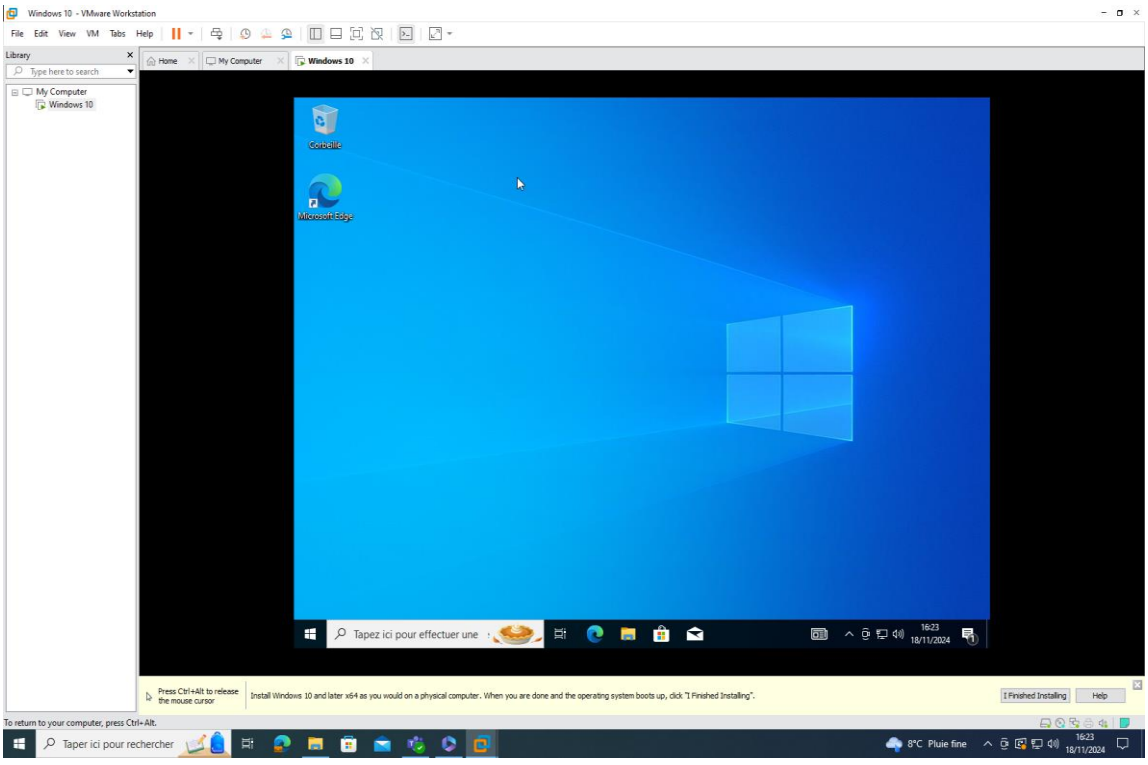


Nous venons de créer Windows 10 pro avec VMware.





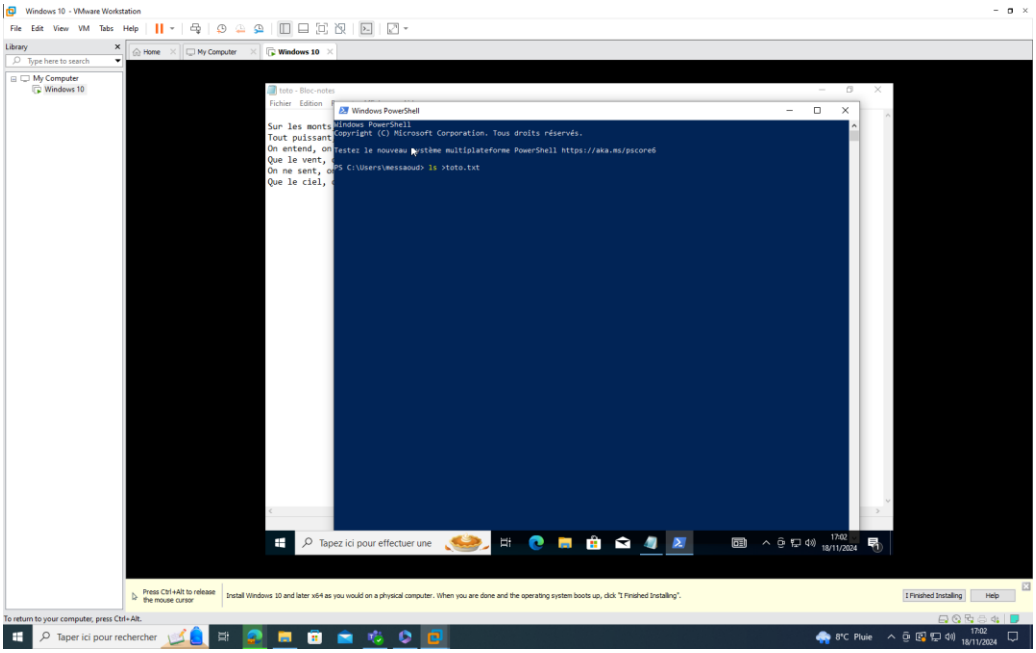
J’ai défini un mot de passe.



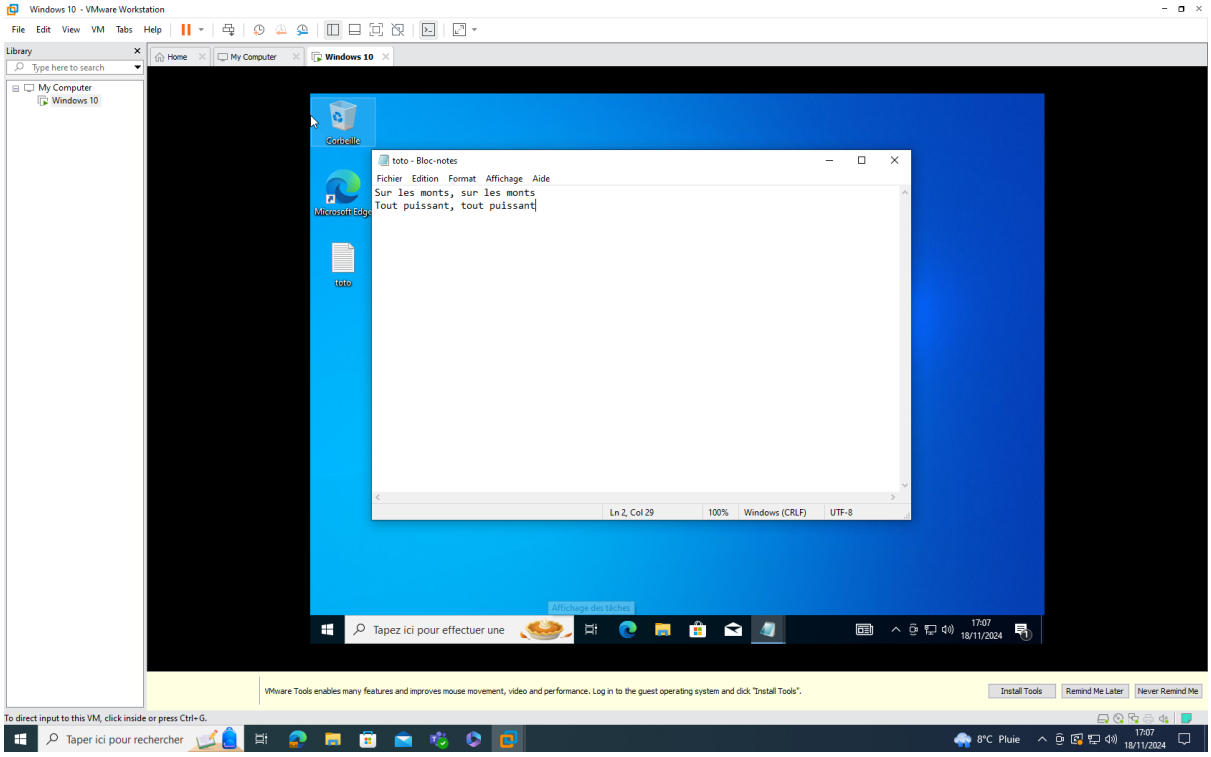
Et nous voilà dans le bureau Windows.

• Créons un fichier toto.txt sur le bureau de Windows

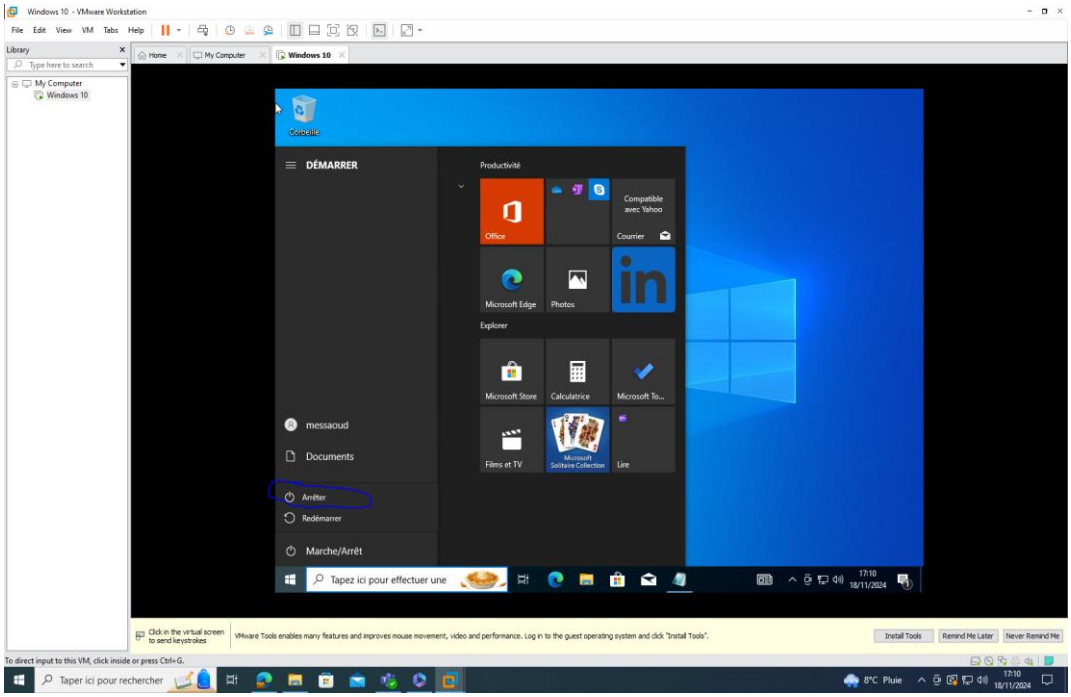
Grace au système Windows PowerShell, j’ai créé un fichier que j’ai nommé toto.txt, il suffit juste de taper ls >toto.txt



Après avoir accéder au fichier, j'ai écrit les paroles de ma chanson préférée et j'ai enregistré le fichier.

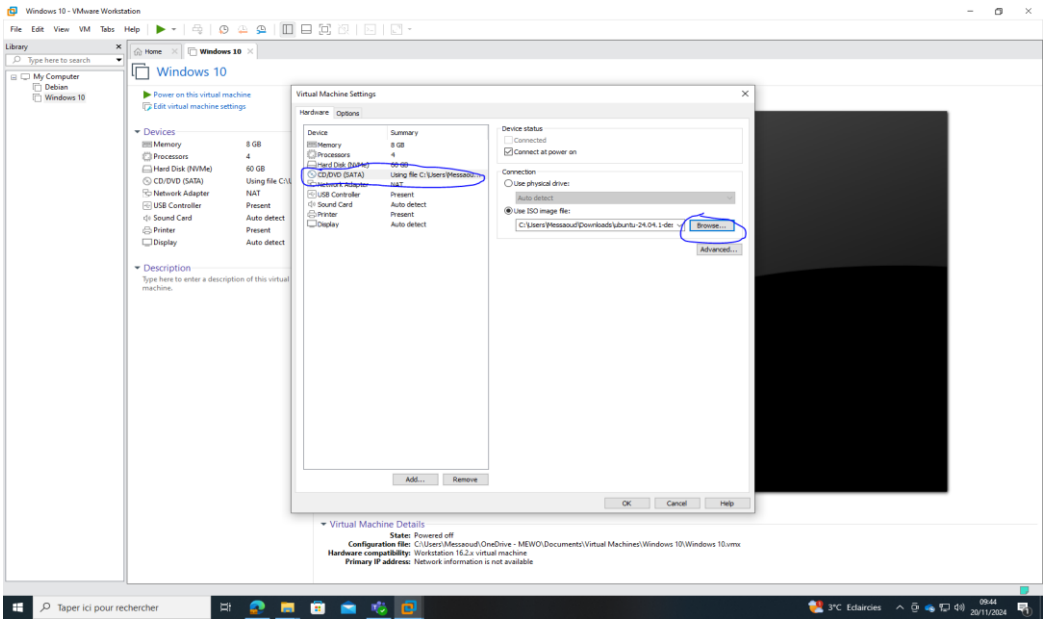


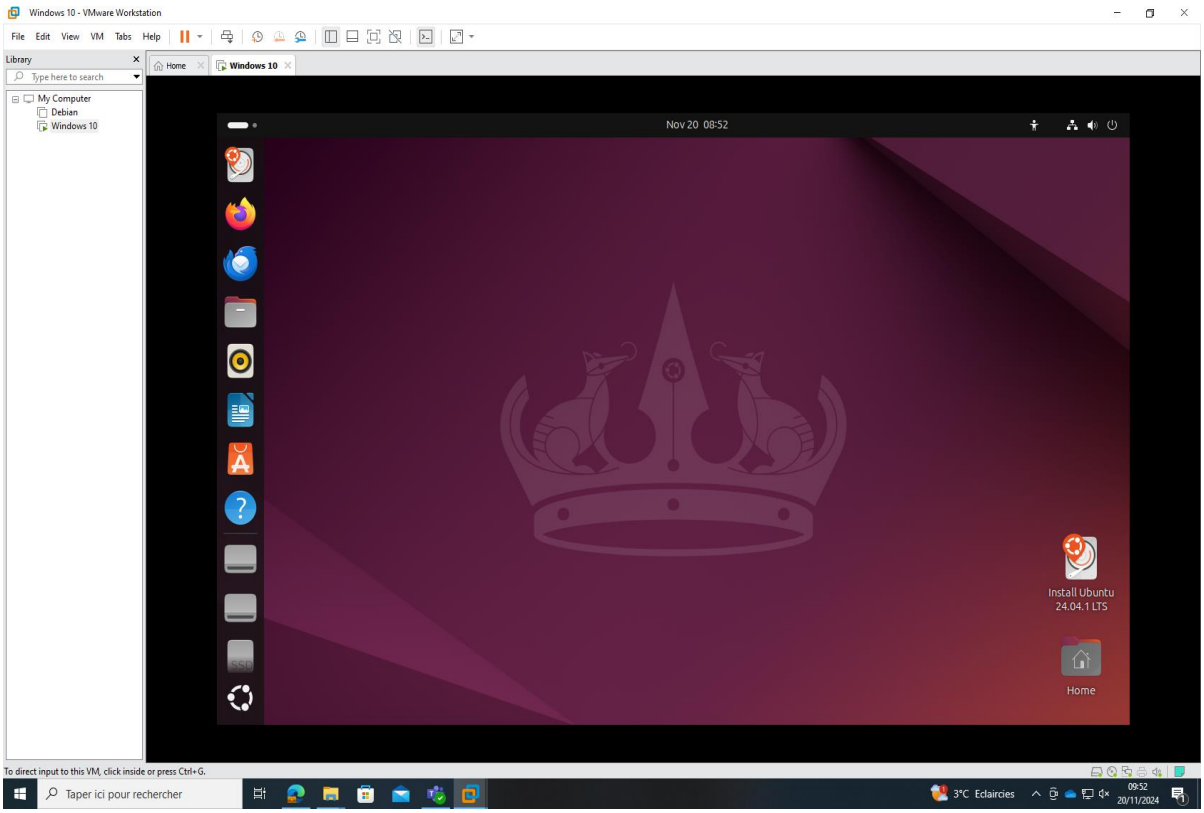
Enfin, au menu démarrer, j'ai arrêté la machine virtuelle Windows 10.



II- Continuons notre expérimentation

J’ai booté sur ma machine virtuelle Windows 10 mais cette fois-ci en utilisant une ISO de Ubuntu Desktop.





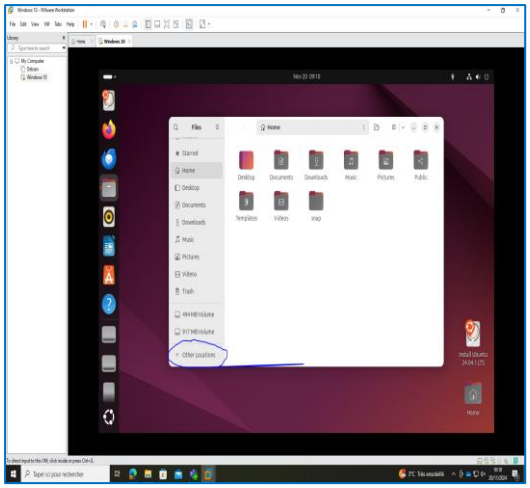
Ainsi, nous sommes dans le bureau de Ubuntu Desktop.

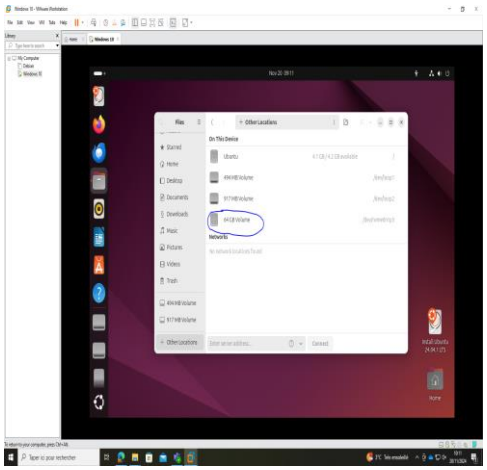
• Est-ce possible de lire le fichier toto.txt ? Est-ce possible de le modifier ?

A- D'abord, cherchons l'emplacement du fichier toto.txt.

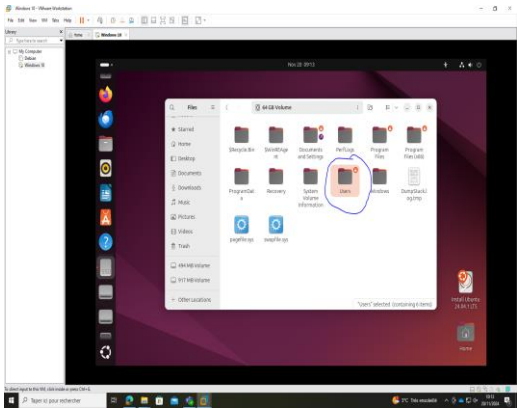
Ce n'était pas du tout difficile car il suffit juste de raisonner. Sachant que nous avons créés le fichier toto.txt dans la machine Windows donc il ne peut être que dans le disque de Windows.

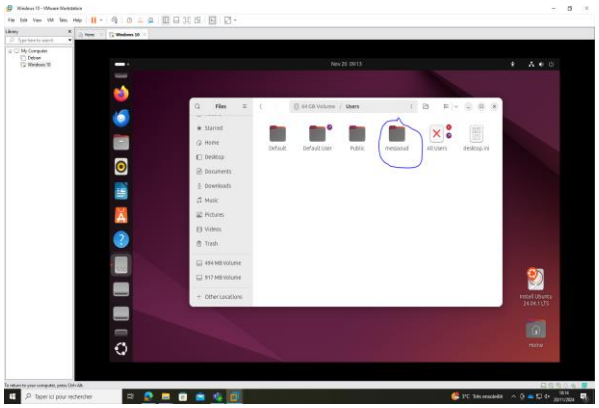
Allons dans Files (fichiers), cliquons sur Other Locations et choisissons le disque SSD 64 GB Volume c'est à dire le disque de Windows 10.



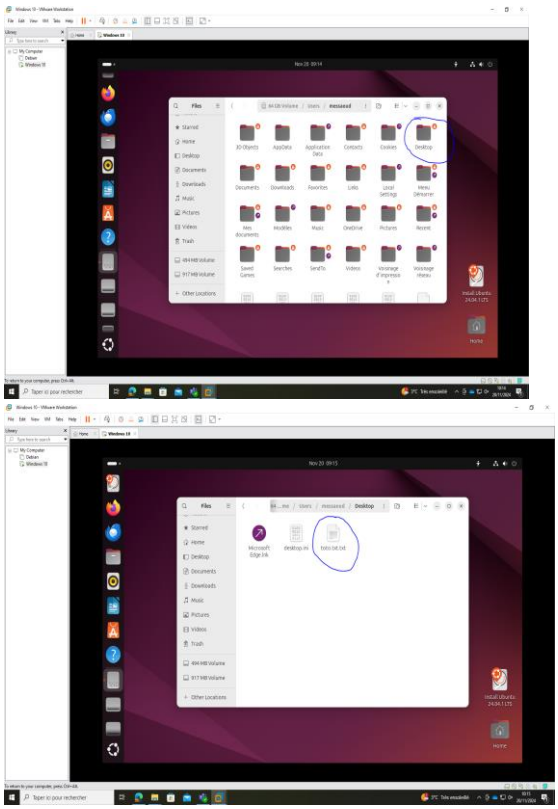


Ensuite cliquons sur Users puis sur messaoud (administrateur Windows)

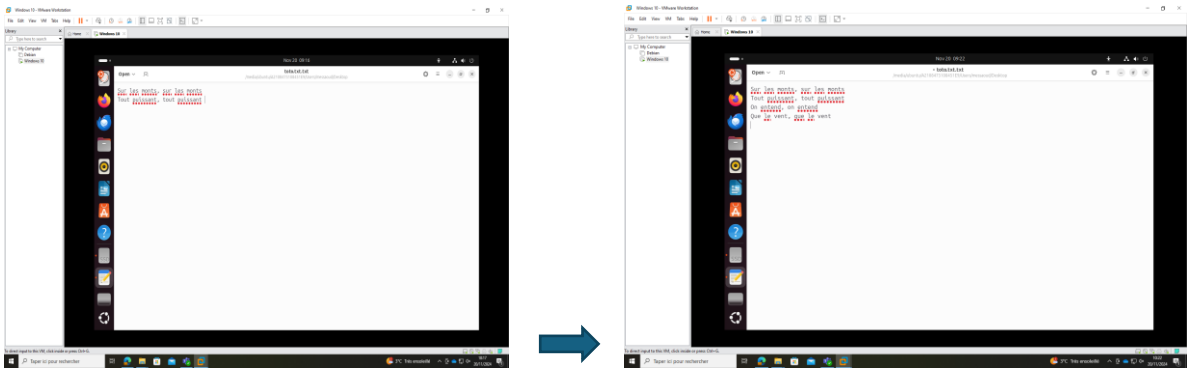




Enfin, cliquons sur Desktop (bureau) car on avait placé le fichier toto.txt dans le bureau Windows



B- Ensuite après avoir ouvert le fichier toto.txt, on constate que les paroles de notre chansons préférées sont présentes et le fichier peut toujours être modifié.



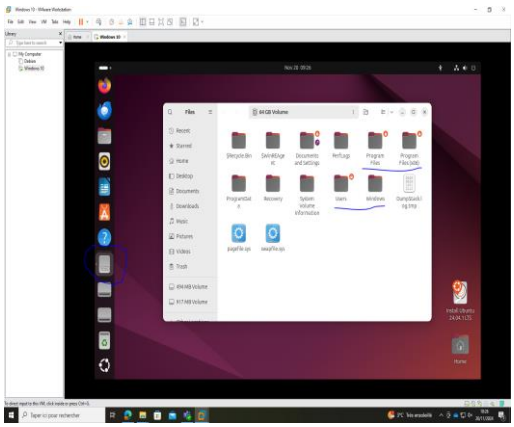
III- Choisissons une technique et expérimentons là

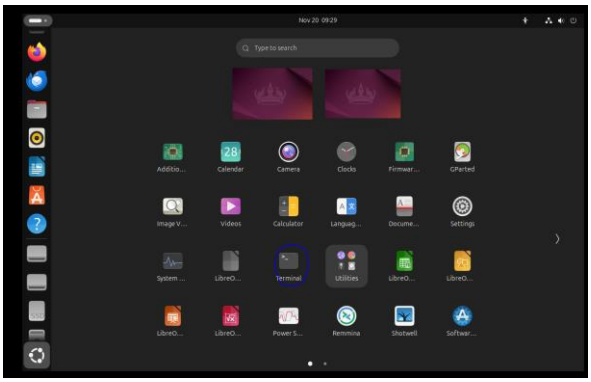
A- D'après les méthodes proposées par https://lecrabeinfo.net/reinitialiser-mot-de-passe-compte-utilisateur-local-windows.html, on choisit la méthode 2-a qui

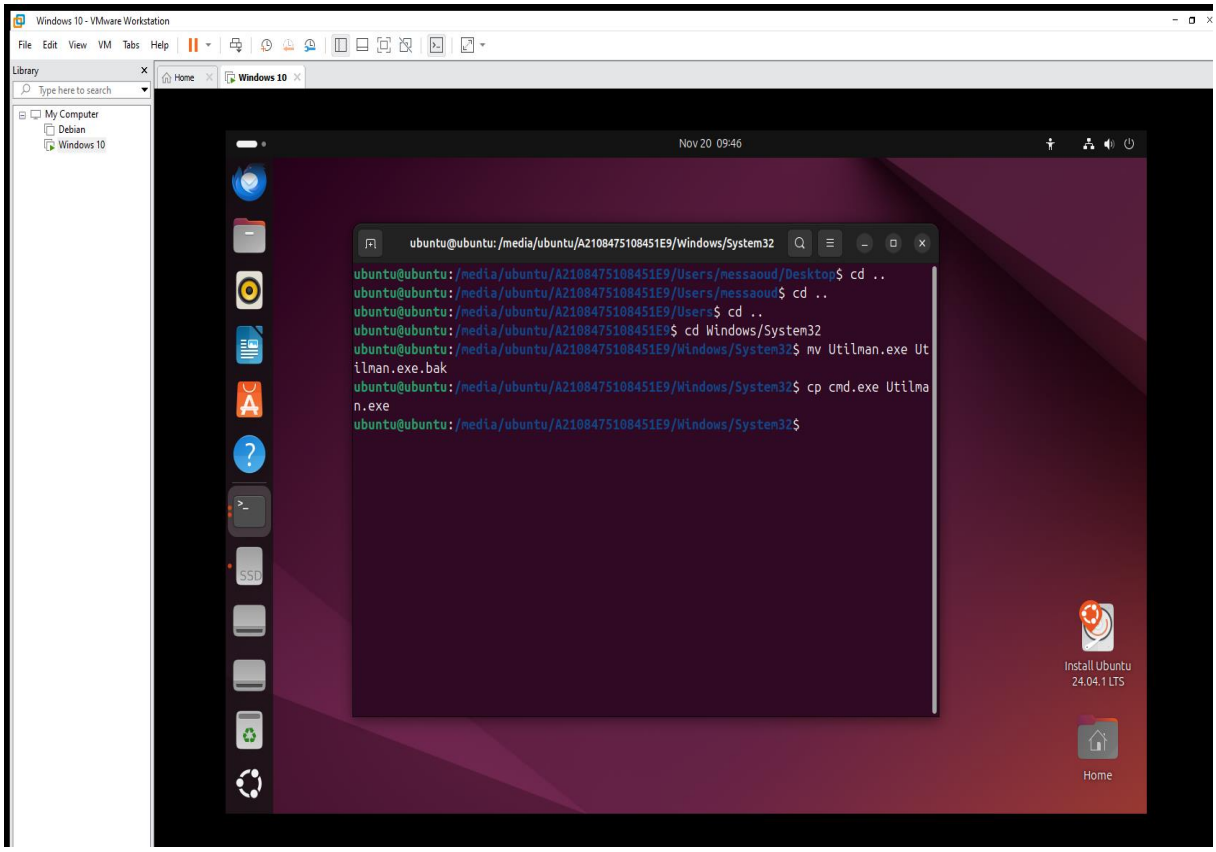
consiste à remplacer les options d'ergonomie par l'invite de commandes et réinitialiser le mot de passe d'un compte utilisateur sur Windows grâce à Ubuntu Desktop, une clé USB/un CD d'une distribution Linux.

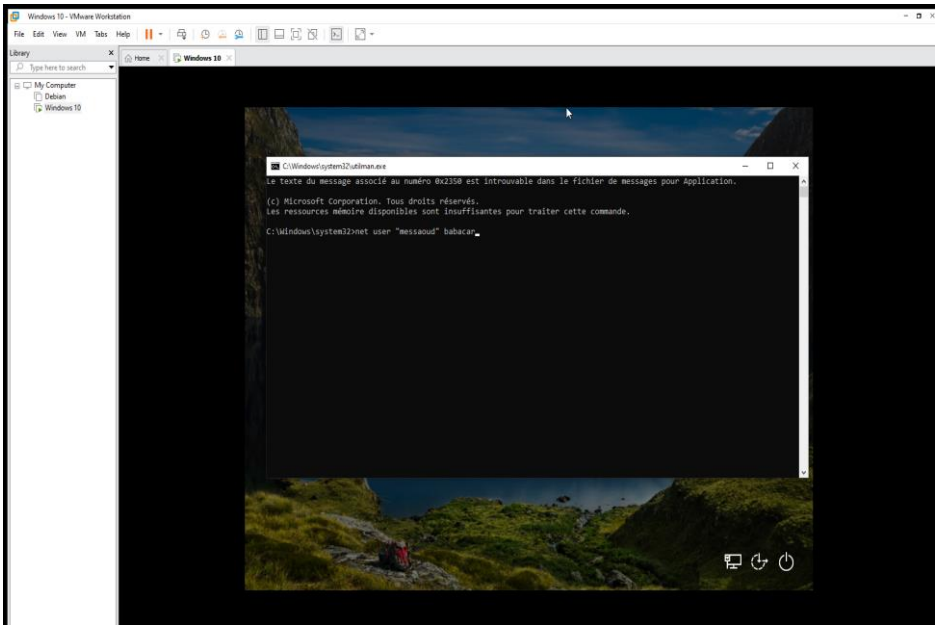
Le principal but est de remplacer Utilman.exe en cmd.exe pour pouvoir modifier le mot de passe. Pour se faire, nous allons ouvrir l'application Terminal sur Ubuntu Desktop et utiliser les commandes du site précédent.

Ex : mv Utilman.exe.bak Utilman.exe pour éviter la destruction du contenu d'Ultiman.exe, cp cmd.exe Ultiman.exe pour copier et coller le contenu de cmd.exe dans Ultiman.exe et rm Ultiman.exe.bak pour éviter les traces.









Comme nous pouvons le voir sur l'image ci-dessus, je viens de changer le mot de passe en mettant au niveau de la commande net user "messaoud" nouveau mot de passe.

B- Quelle méthode s'approche le plus de la vidéo évoquée en introduction ?

La méthode 2-b est la méthode qui se rapproche le plus de la vidéo.

IV- Enfin

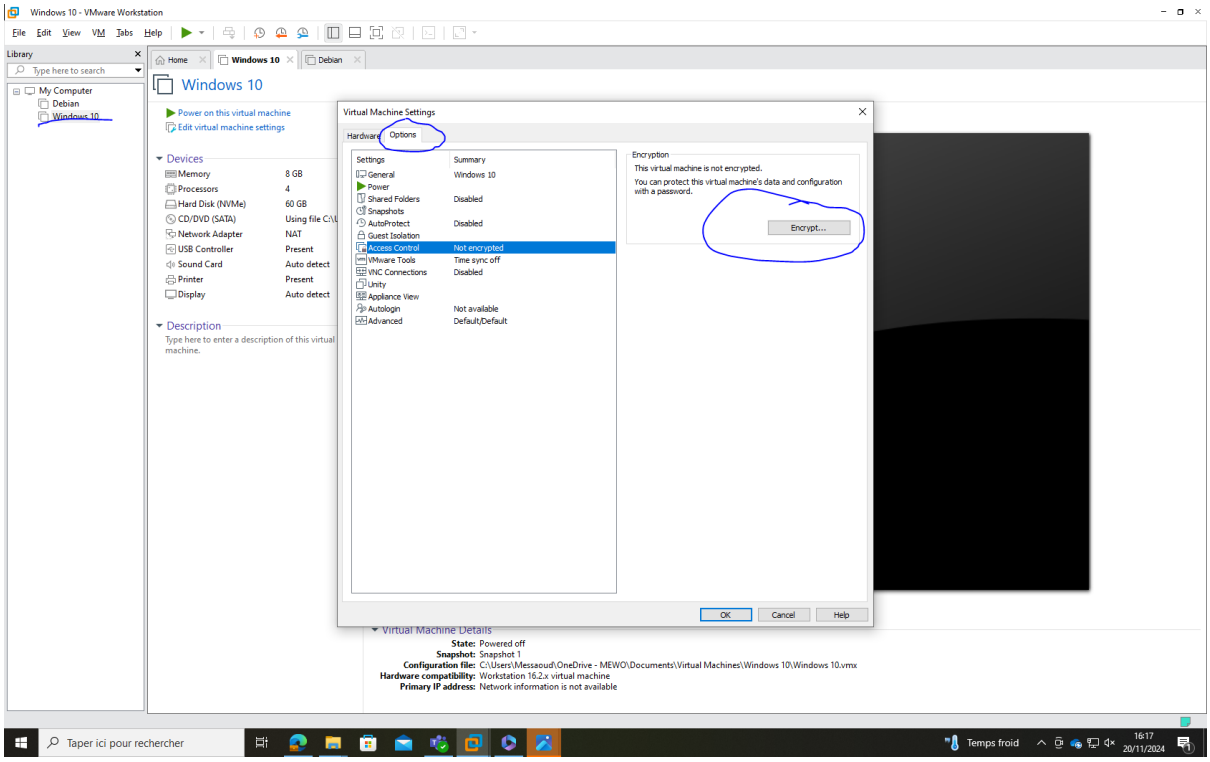
A- Conclusion

En conclusion, la sécurité des systèmes Windows demeure une préoccupation majeure face à l'augmentation des cyberattaques. Comme nous l'avons vu, exploiter des vulnérabilités de Windows n'est pas toujours aussi compliqué qu'il y paraît, surtout lorsque l'attaquant dispose des bons outils et d'une connaissance approfondie du système. Dans le cadre de notre expérience, nous avons démontré comment un attaquant pourrait contourner une sécurité basique en accédant à un compte administrateur via des méthodes simples, comme le démarrage sur un système alternatif tel qu'Ubuntu. Ce type d'intrusion met en lumière l'importance de maintenir une bonne configuration de sécurité, de régulièrement mettre à jour les systèmes et de s'assurer que les méthodes d'authentification sont robustes. Il est essentiel de se mettre dans la peau d'un attaquant pour identifier et corriger ces failles avant qu'elles ne soient exploitées. Cela montre qu'une approche proactive, à travers des tests réguliers et des renforcements de la sécurité, reste la meilleure défense contre les menaces qui pèsent sur nos systèmes. Dans un environnement professionnel ou d'administration, il est impératif de toujours obtenir les autorisations nécessaires avant d'effectuer des modifications sur un système, et de garantir que des pratiques de sécurité robustes sont en place pour prévenir toute intrusion malveillante.

B- Déterminer deux manières de se protéger de ce problème

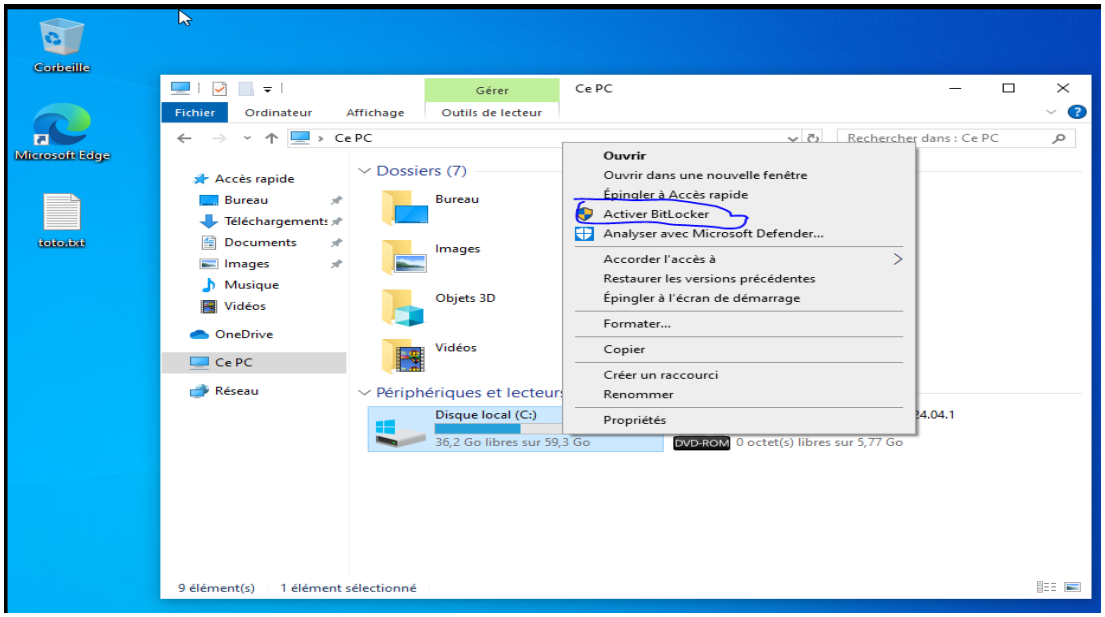
1- Le Cryptage

Le cryptage empêche un attaquant d'accéder aux mots de passe stockés, même s'il accède au fichier de sécurité. Il protège les données sensibles contre l'accès non autorisé, même après des tentatives d'intrusion comme celles que nous avons simulées, en rendant les informations illisibles sans la clé appropriée. Pour crypter la machine virtuelle Windows 10, il suffit de l'éteindre, de faire un clic droit sur Windows 10 au niveau de My computer, aller dans Options et cliquer sur Access control et enfin sur Encrypt.



2- BitLocker

BitLocker offre une protection puissante en chiffrant le disque dur dans son ensemble, ce qui empêche un attaquant d'exploiter les données, même après une tentative d'intrusion sur un système Windows. C'est une défense essentielle contre l'accès non autorisé et les tentatives de vol de données.


Corbeille
Microsoft Edge
toto.txt
Gérer
Ce PC
Fichier
Ordinateur
Affichage
Outils de lecteur
Ce PC
Rechercher dans : Ce PC
Accès rapide
Bureau
Téléchargements
Documents
Images
Musique
Vidéos
OneDrive
Ce PC
Réseau
Dossiers (7)
Bureau
Images
Objets 3D
Vidéos
Périphériques et lecteurs
Disque local (C:)
36,2 Go libres sur 59,3 Go
DVD-ROM
0 octet(s) libres sur 5,77 Go
Ouvrir
Ouvrir dans une nouvelle fenêtre
Épingler à Accès rapide
Activer BitLocker
Analyser avec Microsoft Defender...
Accorder l'accès à
Restaurer les versions précédentes
Épingler à l'écran de démarrage
Formater...
Copier
Créer un raccourci
Renommer
Propriétés
9 élément(s)
1 élément sélectionné