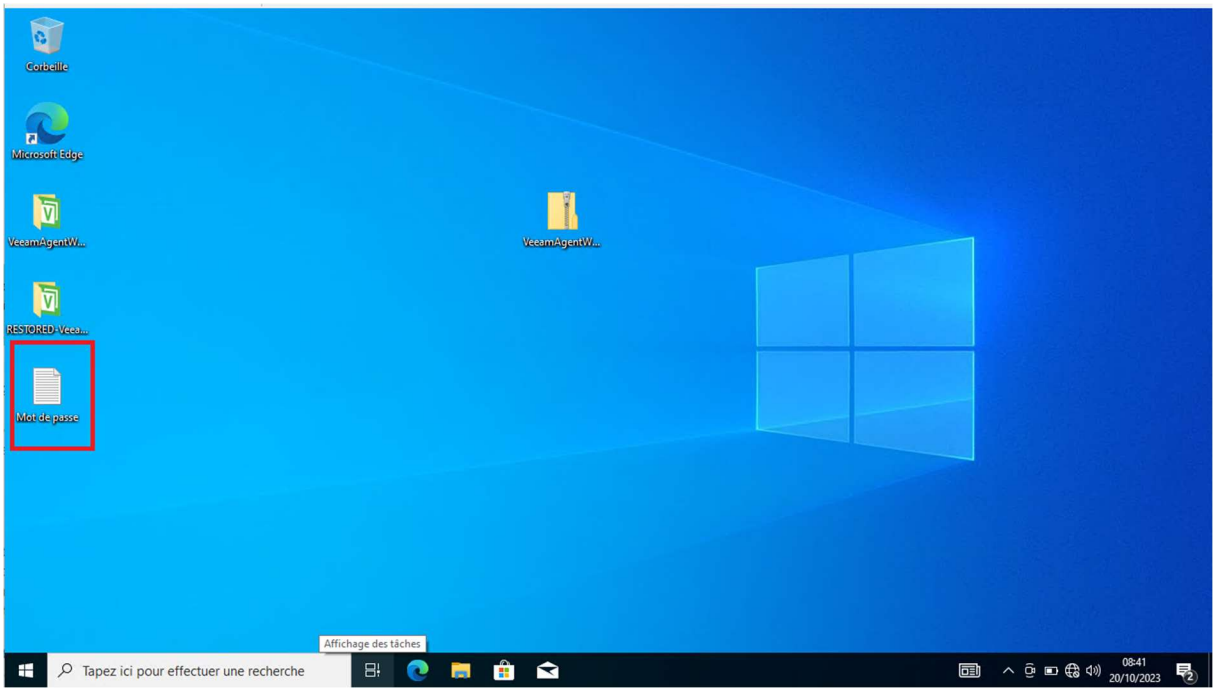
Compte rendu TP intrusion : Mots de passe (TEWES Arnaud)

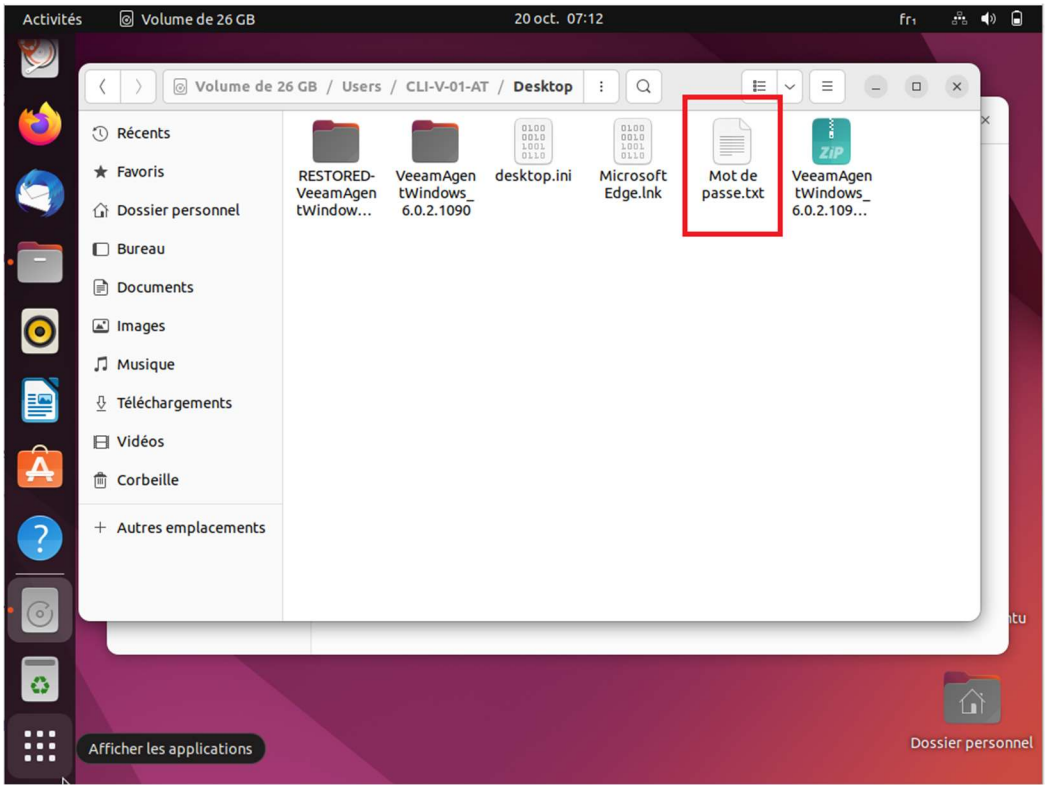
Dans ce TP, nous allons tenter de nous introduire dans une session Windows sans mot de passe et de lire et modifier un fichier que nous avons créé au préalable. Dans un premier temps, nous allons essayer de lire le fichier en mode Live ou Essai sous Ubuntu. Dans un second temps, nous allons supprimer le mot de passe d'une session Windows grâce à certains outils disponibles sur Internet. Ensuite, nous allons expérimenter tout ce que nous avons vu, mais cette fois sous Linux pour vérifier si les mêmes problèmes peuvent nous arriver.

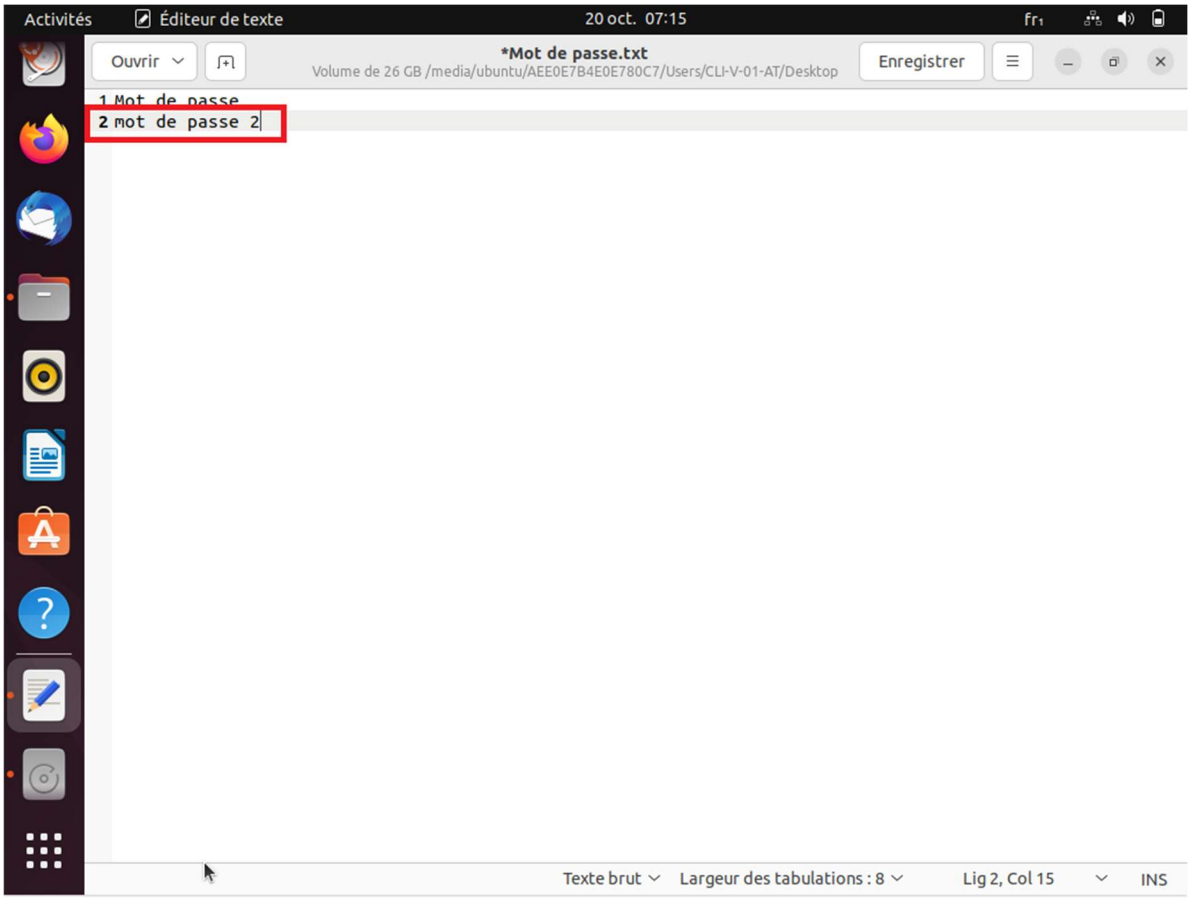
Création d'une machine virtuelle sous Windows, définition d'un mot de passe, création d'un fichier texte et tentative de lecture en mode Live ou Essai sous Ubuntu.

Tout d'abord, j'ai ouvert une machine virtuelle sous Windows 10 qui a un mot de passe, puis j'ai créé un document texte nommé « Mots de passe » avec comme contenu « Mot de passe 1 »

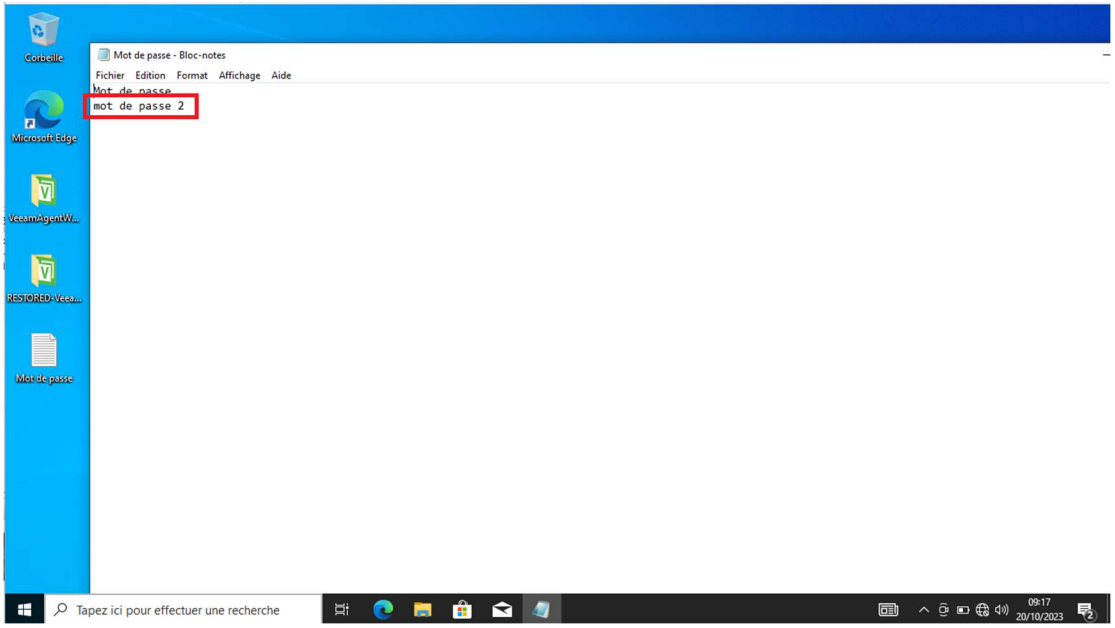


Ensuite, en démarrant à partir d'un ISO Ubuntu qui a un mode « Test », j'ai essayé de lire le fichier et de le modifier en ajoutant « Mot de passe 2 » en dessous.





Grâce à cette technique, j'ai bien pu ouvrir le fichier que j'avais créé sans utiliser le mot de passe de la session, et même le modifier. Je vais maintenant essayer de le lire en me reconnectant sur ma session avec mon mot de passe habituel.



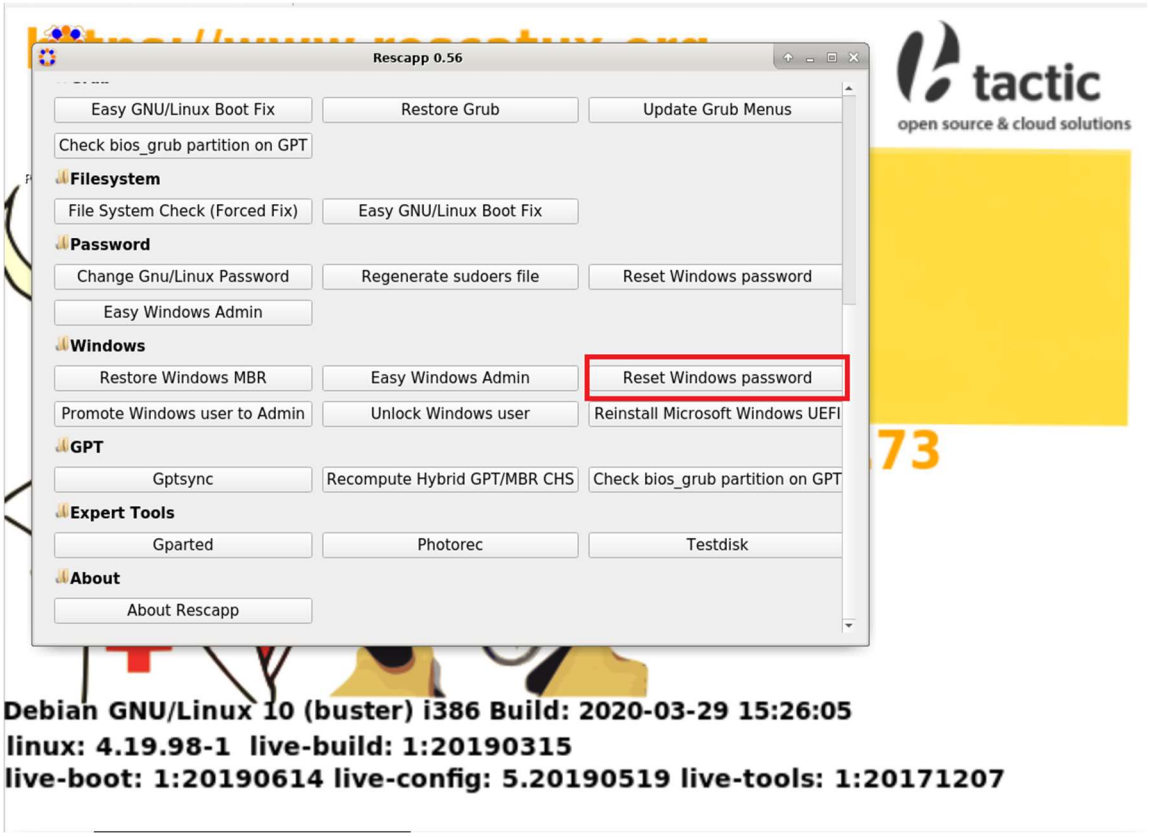
Tout a fonctionné, nous avons pu ouvrir, lire et modifier un fichier qui avait été créé sous Windows, et tout cela sans connaître le mot de passe de la session.

Question 1 et 2 :

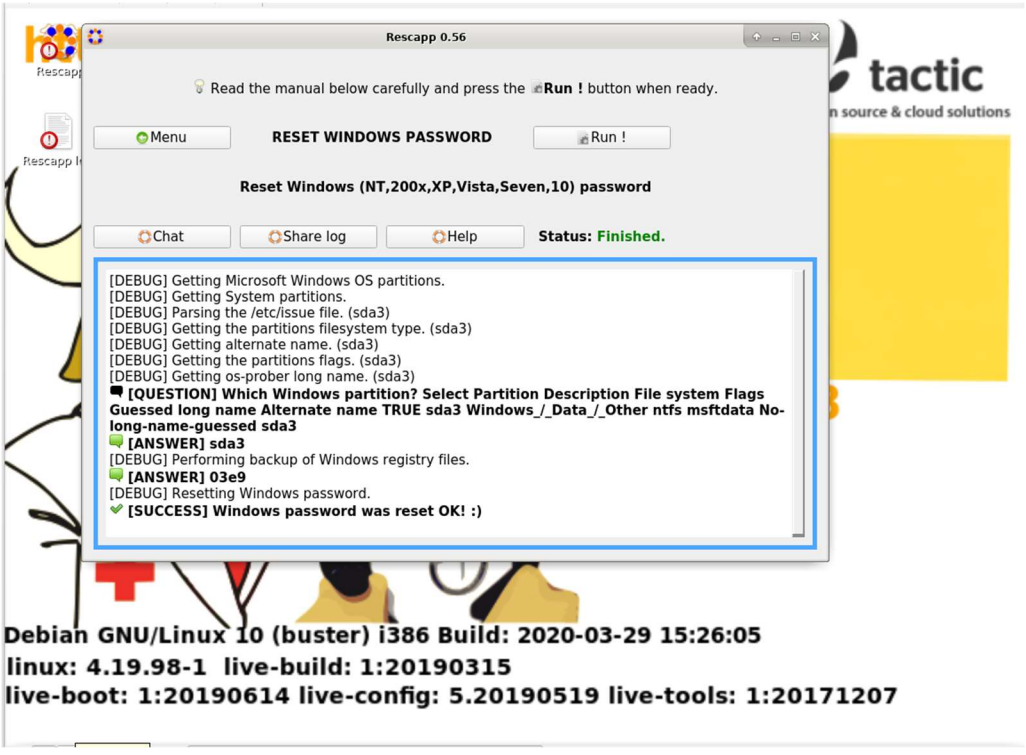
Il est donc bien possible de lire et de modifier un fichier en démarrant simplement à partir d'un ISO Linux, et nous pouvons d'ailleurs accéder à tout le disque dur de la machine.

Maintenant, nous allons essayer, grâce à l'outil Rescatux, de supprimer le mot de passe de ma session Windows.

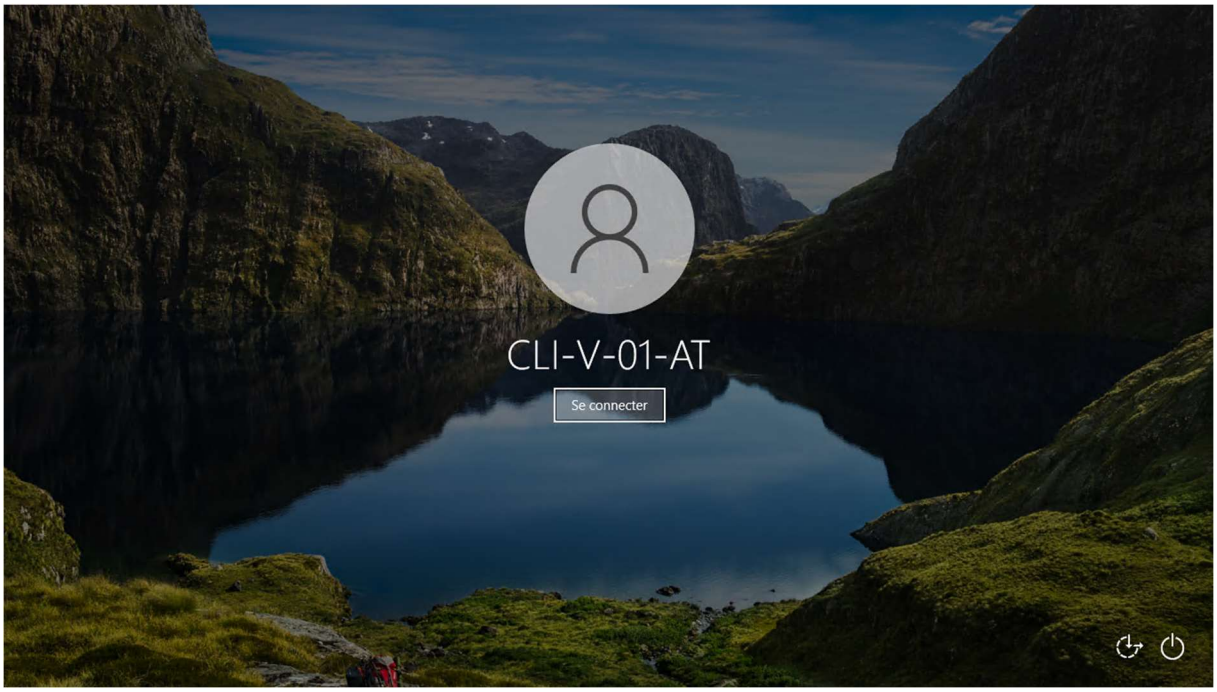
Tout d'abord, il faut démarrer sur l'iso de Rescatux et ouvrir la console Rescapp. Ensuite, nous avons plusieurs choix, dont celui de supprimer le mot de passe Windows « Reset Windows password ».



La console nous demande sur quelle partition se trouve l'utilisateur et de quel utilisateur il faut supprimer le mot de passe. Ensuite, le programme démarre.



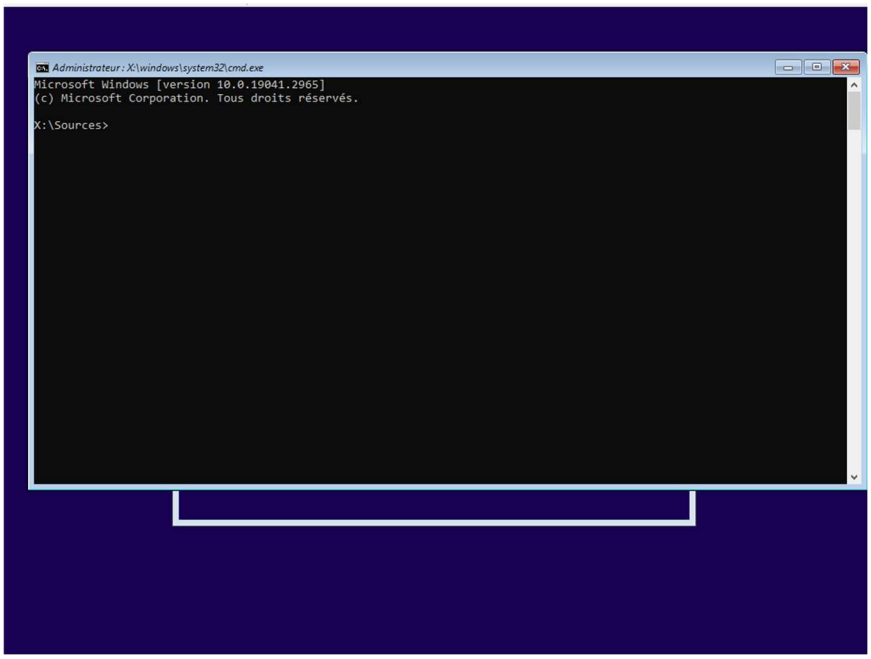
La console a terminé, nous essayons donc de nous connecter sur notre session Windows.

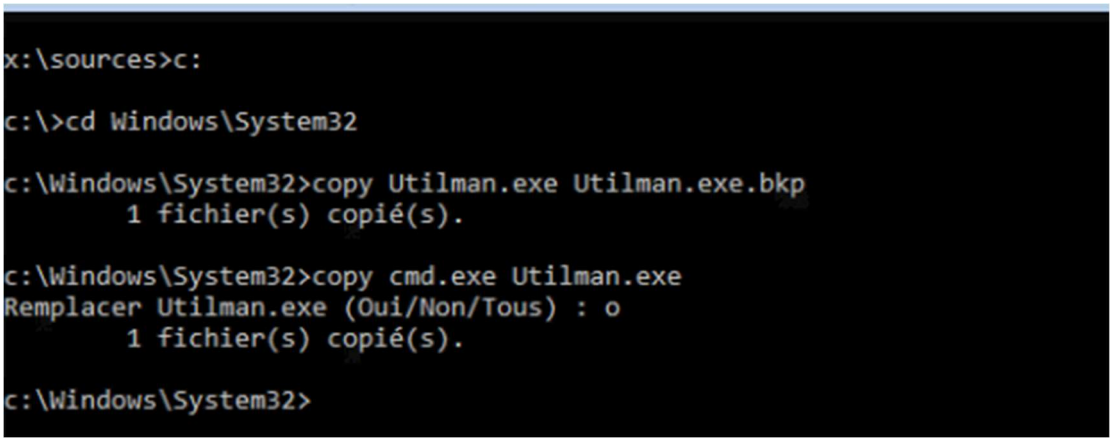


Le mot de passe a bien été supprimer.

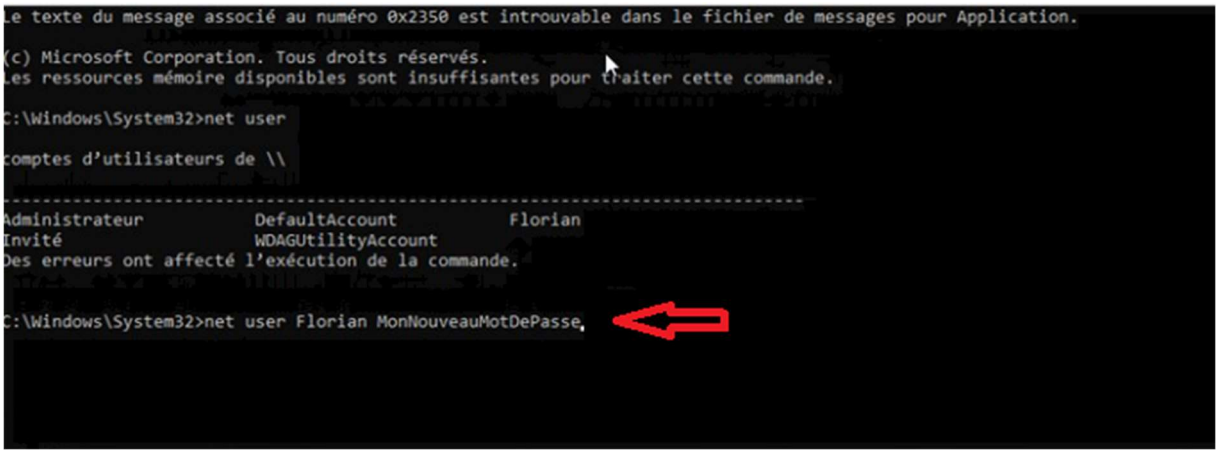
Question 3

La méthode qui se rapproche le plus de la vidéo de Mr Robot est la méthode n°2 qui consiste à démarrer sur un ISO Windows 10, ouvrir une invite de commande et modifier le fichier Utilman.exe en cmd.exe pour ensuite pouvoir modifier ou supprimer le mot de passe d'une session Windows. Voici quelques captures d'écran :





Il suffit ensuite de redémarrer le PC, les outils d'ergonomie sont désormais une invite de commande. Maintenant, nous pouvons écrire la commande « net user NomDeSession NouveauMotDePasse », en remplaçant NomDeSession par le nom de l'utilisateur, et NouveauMotDePasse par le nouveau mot de passe. Nous pouvons ensuite nous connecter avec le nouveau mot de passe.



Question 4

En conclusion, un mot de passe Windows ne suffit pas à protéger ses données et son disque dur. Nous avons vu plusieurs méthodes simples qui permettent, soit d'accéder directement au dossier du disque dur, soit de modifier le mot de passe. D'autres méthodes permettent aussi de le contourner sans le modifier et d'accéder à la session. Une personne lambda ne pourra pas y accéder, mais pour une personne qui se renseigne, toutes les sources disponibles sur internet permettent effectivement, sans trop de recherche, de réussir à passer outre ce mot de passe. Un mot de passe Windows n'est donc pas quelque chose de sûr et il faut mettre d'autres choses en place pour assurer la sécurité des données comme un chiffrement du disque dur ou une double authentification.

Question 5

Pour se protéger de ce problème, plusieurs solutions sont possibles comme :

- Activer le chiffrement du disque dur (avec BitLocker par exemple) sera très utile si une intrusion a lieu. Le cryptage intégral garantit que seules les personnes possédant la bonne clé de cryptage pourront décrypter et accéder aux fichiers et informations du disque dur crypté.

- Utilisez un mot de passe fort et complexe pour votre compte utilisateur local. Évitez d'utiliser des mots courants ou des informations personnelles dans votre mot de passe. Un mot de passe fort est essentiel pour protéger votre ordinateur contre les attaques par force brute. Comme nous l'avons vu en cours et selon les recommandations de la CNIL, un mot de passe fort doit être long et complexe, avec une combinaison de lettres majuscules et minuscules, de chiffres et de symboles. Un tel mot de passe peut mettre plusieurs mois voire plusieurs années a se faire demasquer.

- Nous avons la possibilité de mettre un mot de passe sous Windows pour accéder à nos fichiers. Mettre un mot de passe pour accéder à ses fichiers est une méthode courante pour protéger ses données contre les accès non autorisés. Cependant, il est important de noter que cela ne garantit pas une sécurité absolue.

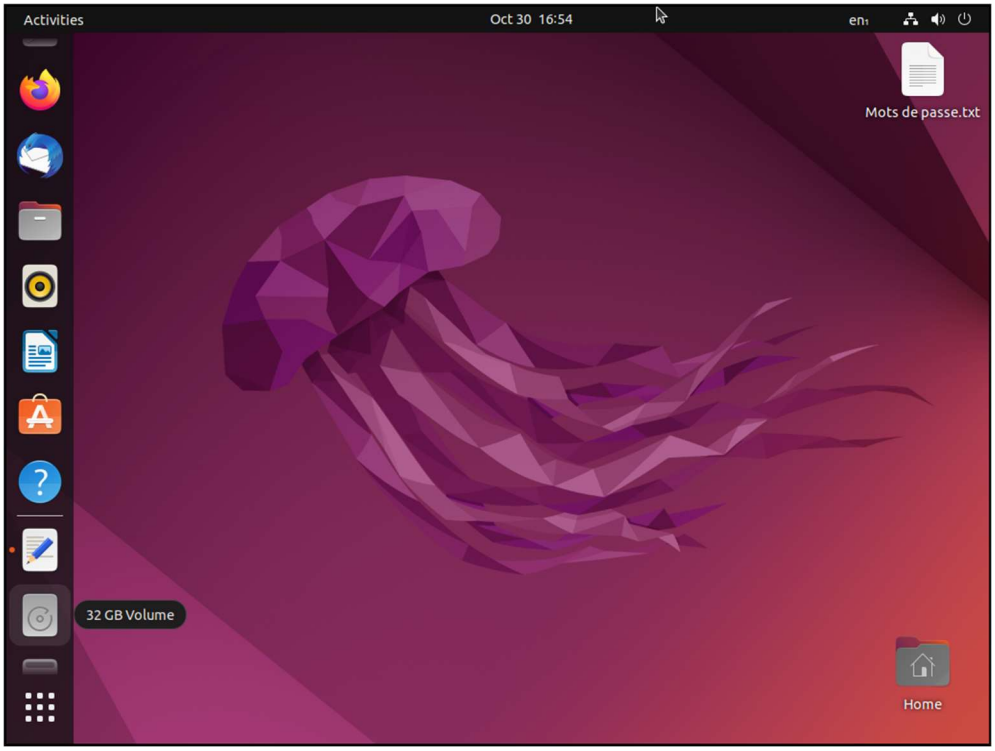
- Si l'on a un ordinateur portable, ne jamais le laisser à portée d'un inconnu (comme sur le siege de sa voiture par exemple) lorsqu'on s'absente, ou sur son bureau au travail lorsqu'on y est pas. Au vu de tous les moyens possible qu'il existe de contourner le mot de passe, ce n'est pas sécurisé de laisser un PC a portée.

- Prévoir une sauvegarde de notre disque dur en suivant la méthode du 3-2-1. Cela permet, en cas de soucis, de vol, ou d'attaque de ransomware, de pouvoir toujours récupérer nos données.

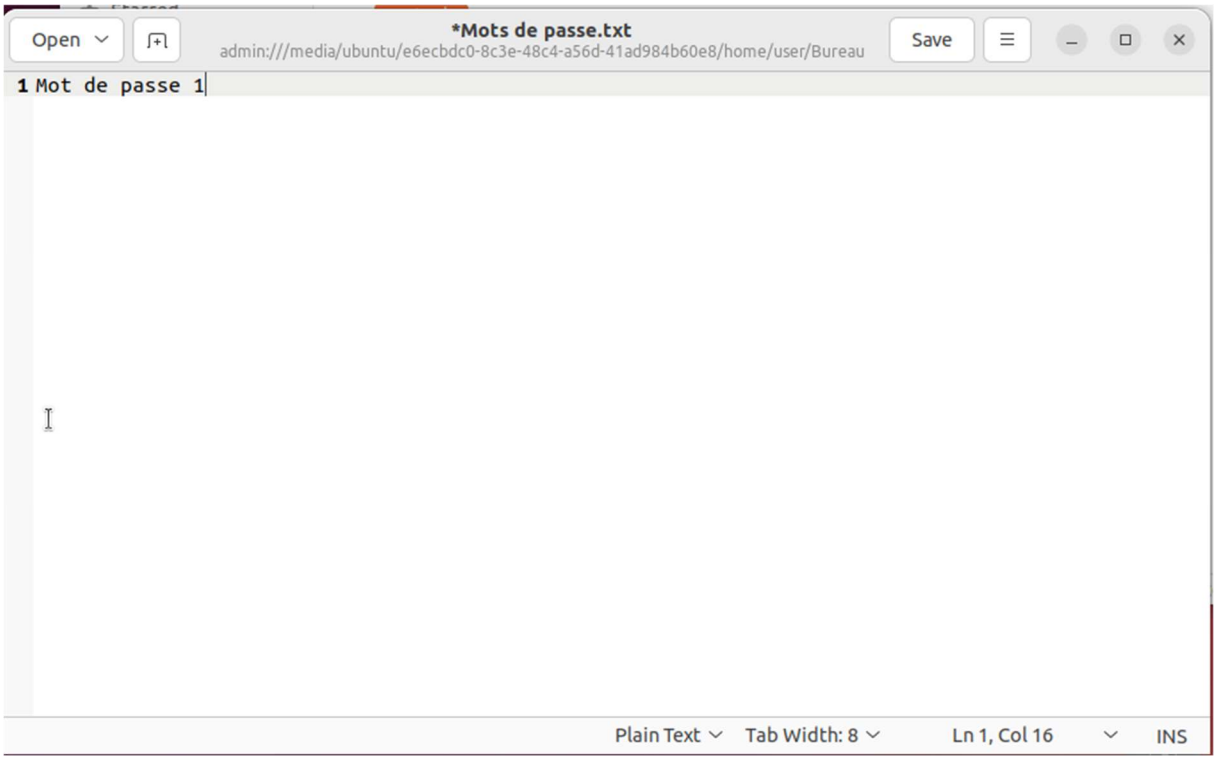
Question 6

Nous allons maintenant reprendre le fil de ce TP pour vérifier si nous rencontrons les mêmes problèmes avec une distribution Linux. Kali Linux ne fonctionnant pas sur mon PC, j'ai fait le test avec une VM sous Ubuntu, et en bootant également sur Ubuntu en version « essai » pour essayer de lire le fichier mot de passe.

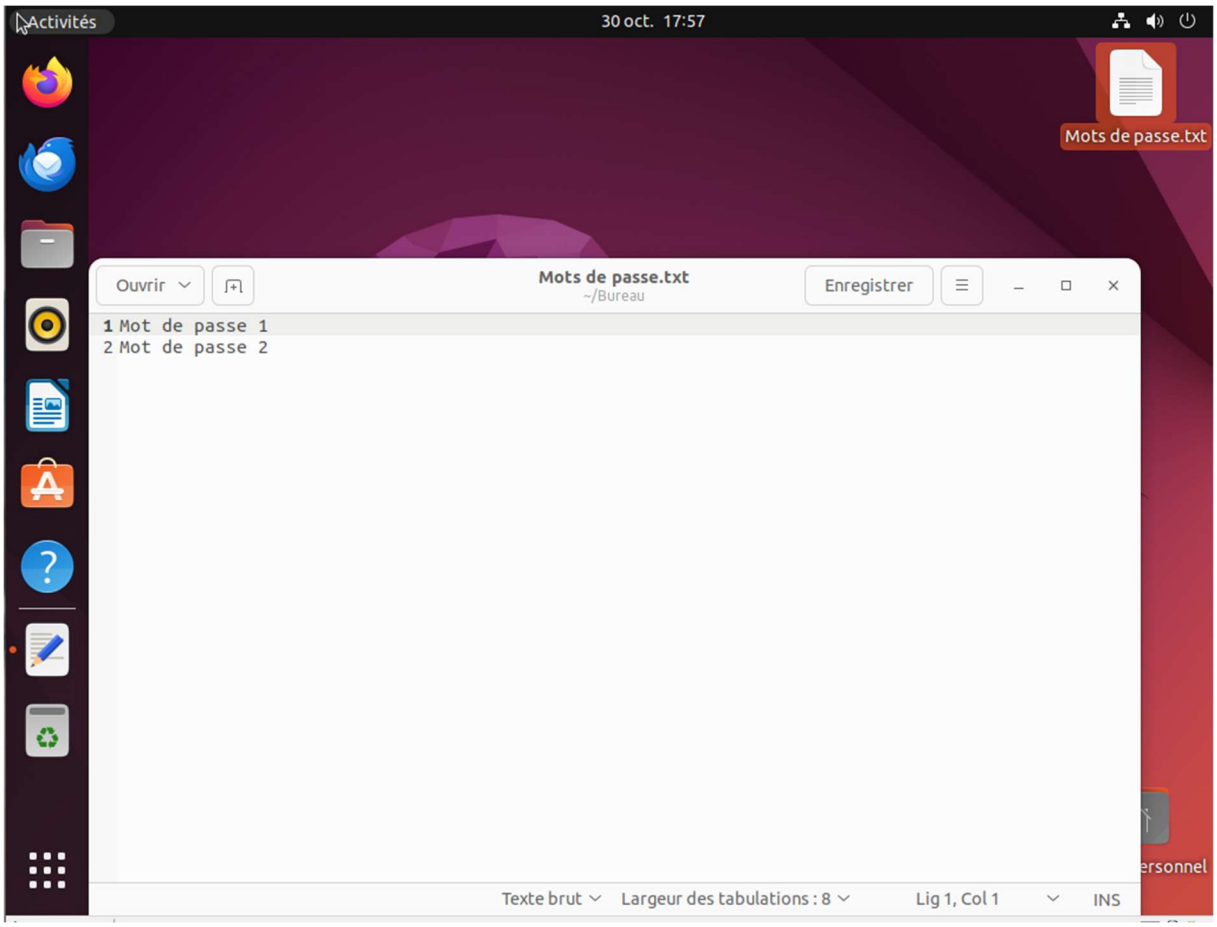
Dans un premier temps, j'ai créé un fichier mot de passe sur mon bureau.



J'ai ensuite demarré ma VM sur la version d'essai d'Ubuntu et j'ai essayé de lire le fichier.



J’ai ajouté une ligne « Mot de passe 2 » dans le fichier, et j’ai essayer de le lire avec mon Ubuntu installé sur ma VM.



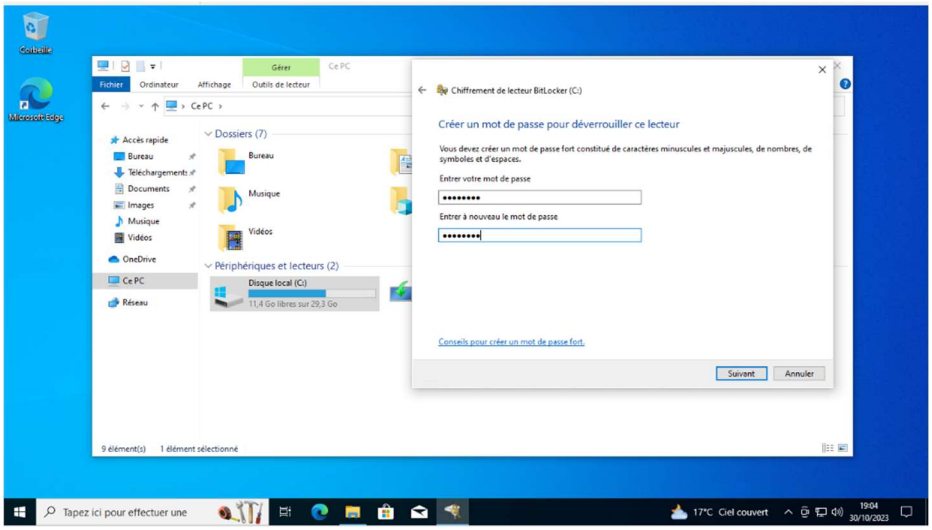
J’ai réussi à lire le fichier texte « Mots de passe » avec les deux lignes inscrites a l’interieur. J’ai donc bien pu lire et modifier le fichier, et ca, sans mot de passe…

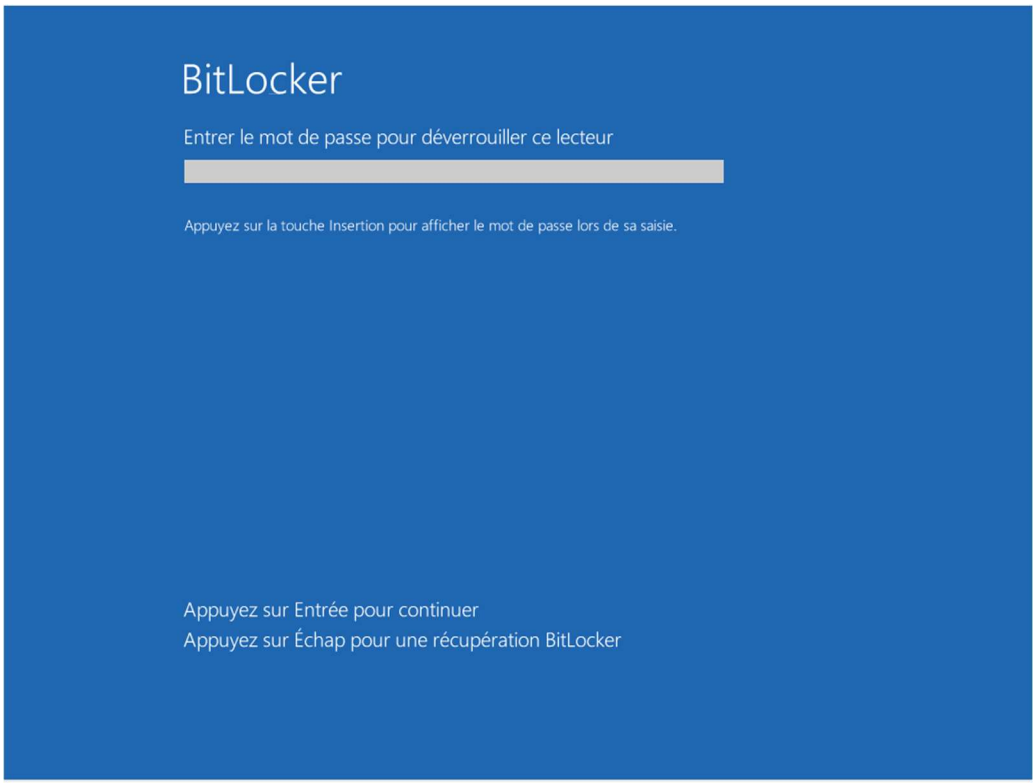
Pour résumer, il faut donc d’autres alternatives, que l’on soit sous Linux ou sous Windows pour protéger ses données comme vu plus haut à la question 5…

Pour aller plus loin :

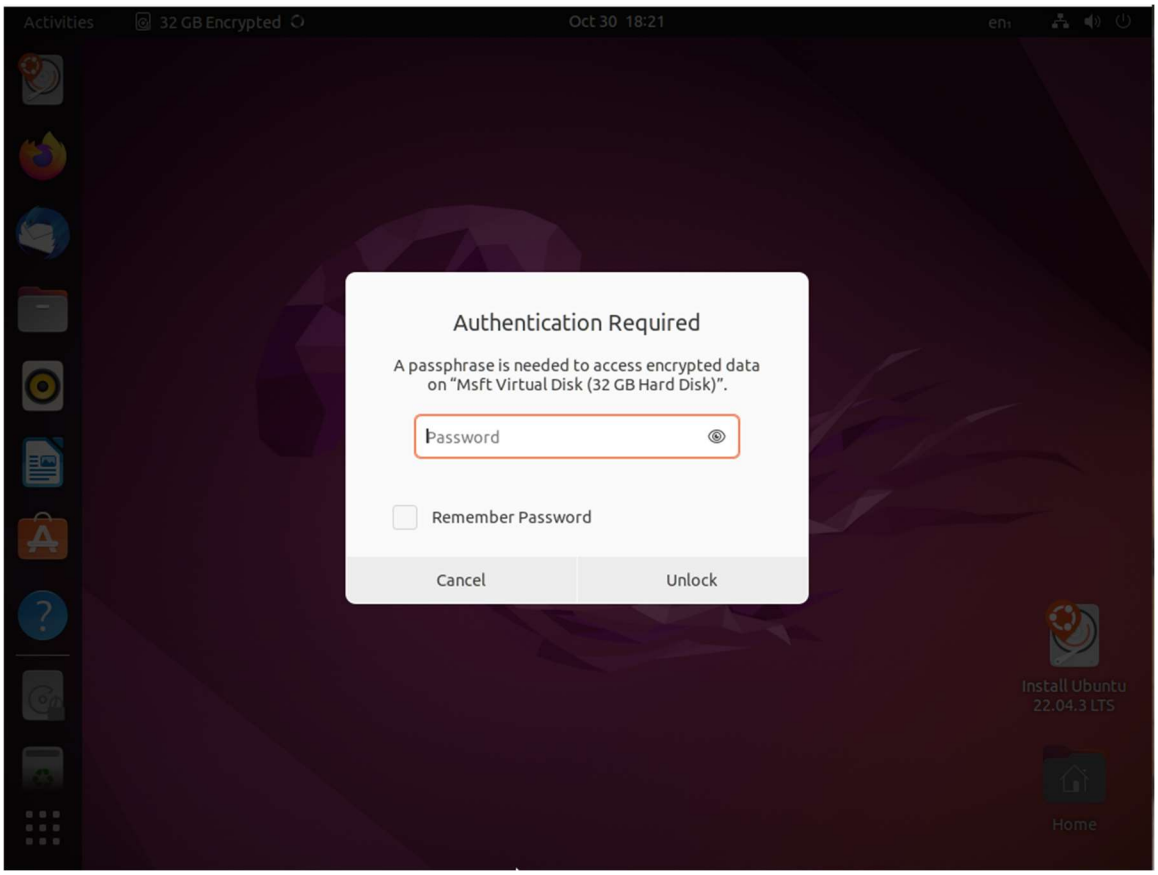
Je vais maintenant essayer de lire le fichier texte « Mots de passe » de ma VM sous Windows 10 en ayant activé BitLocker au préalable et en ayant chiffré mon disque dur.

J'ai donc activé BitLocker sur ma VM Windows 10.





J’ai ensuite démarré sur Ubuntu version « test » et j’ai essayé d’ouvrir le disque dur ou Windows est installé.



Le disque dur est correctement chiffré et il nous est impossible d’y accéder, même en utilisant les techniques mentionnées précédemment.

Conclusion

La méthode de chiffrement du disque dur est une méthode fiable qui permet de sécuriser les données de son disque dur. Il est nécessaire de prendre des précautions lorsqu’on traite des données sensibles et de rester vigilant, car les attaques malveillantes peuvent survenir de n’importe où !