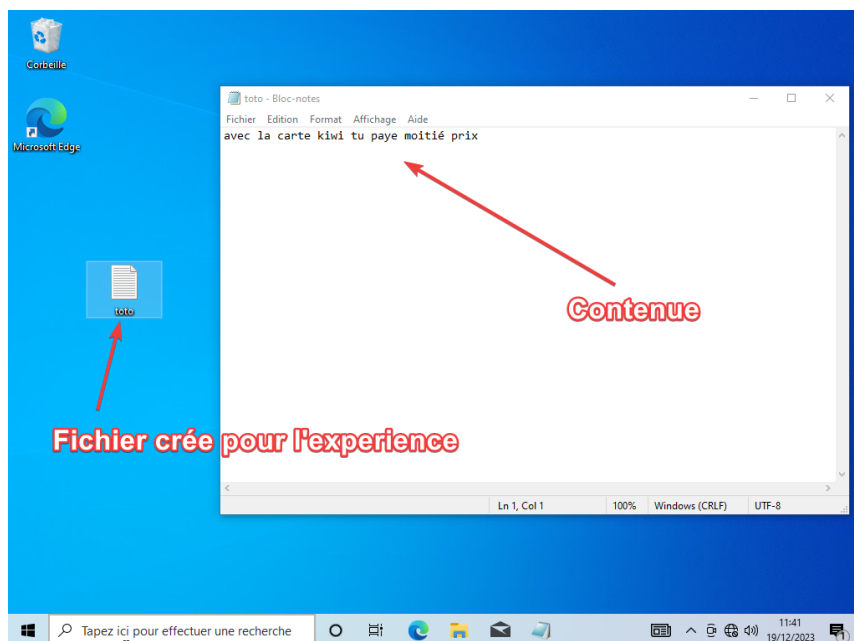


Compte rendue TP 2

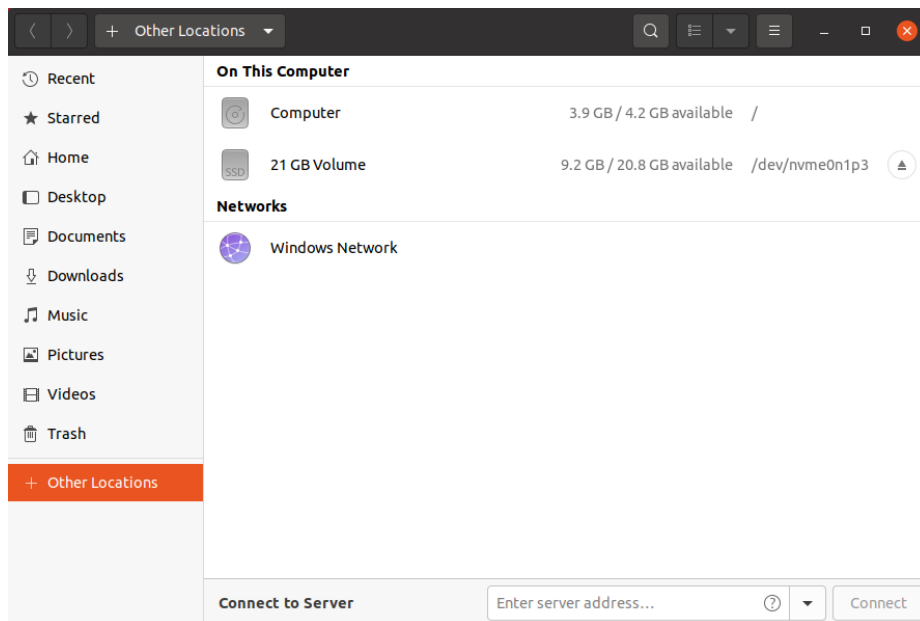
Dans le cadre de ce court TP, nous avons exploré la simplicité d'accéder aux fichiers d'un utilisateur ayant installé un compte local administrateur sur son ordinateur. Pour illustrer cette vulnérabilité, j'ai utilisé VMware, bien que ces manipulations puissent être réalisées sur n'importe quel ordinateur, qu'il soit portable ou non.

Pour cette expérience, j'ai créé une machine virtuelle basée sur Windows 10 Famille. Le mot de passe configuré (0909) est arbitraire, car l'objectif est d'obtenir un fichier sans se connecter en tant qu'utilisateur. Une fois l'installation de Windows terminée et l'accès au bureau obtenu, j'ai créé un fichier texte à des fins de démonstration.



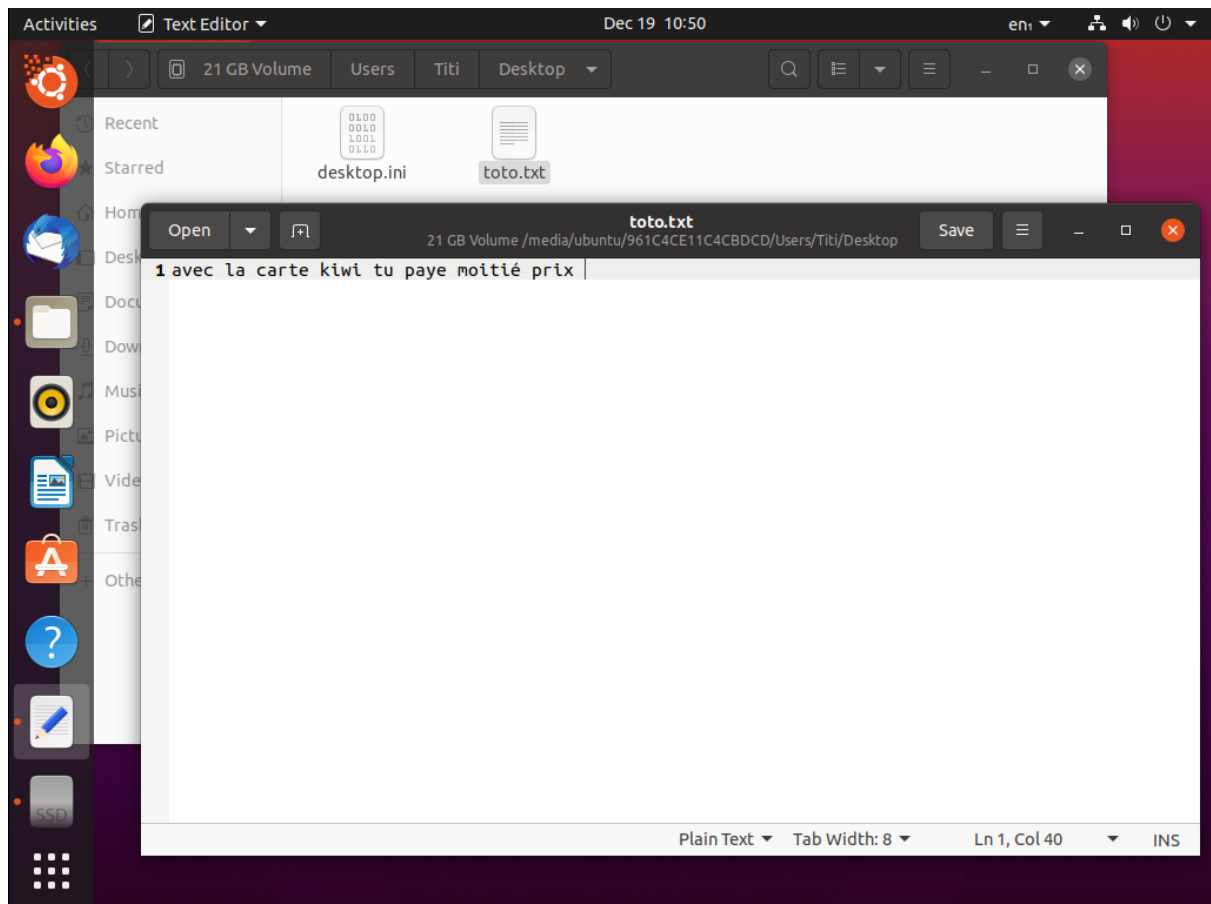
Le fichier en question (<https://i.imgur.com/0GbOLUq.png>)

Pour la suite de notre manipulation j'éteins l'ordinateur et insère un disque virtuel contenant un iso d'ubuntu. La prochaine étape consiste tout simplement à démarrer l'ordinateur sur le disque contenant notre image et accéder à l'interface d'essai d' Ubuntu. Une fois sur celle-ci on accède à l'explorateur de fichier.



Explorateur de fichier Ubuntu

Sur celui-ci on observe deux disques l'un contenant notre windows 10 et l'autre hébergent notre ubuntu.



Accès au dossier cible

Pour finir nous accédons à notre fichier fraîchement créé sur votre windows via le chemin montré sur l'image. Comme on peut le voir, on possède tous les droits dessus comme écrire, lire et copier le fichier txt.

On comprend par cet exercice que si aucune manipulation est faite, les données que l'on stock via notre user sur votre disque dur reste accessible malgré la mise en place d'un mot de passe utilisateur. Donc toute personne sachant lire un article peut accéder à vos données si bien sûr les conditions de cet exercice sont réunies.

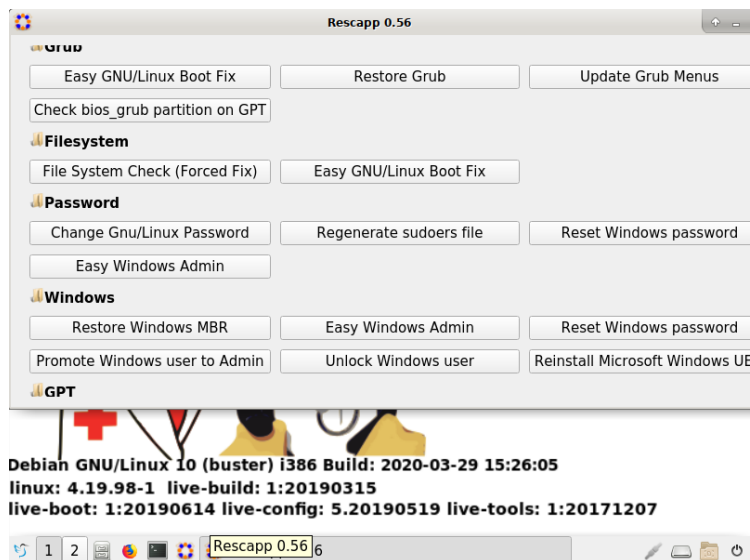
Il existe à ce jour des solutions pour pallier ce problème, une très connue est le système de chiffrement fournis par Windows appelé Bitlocker. Celui-ci chiffre toutes vos données en générant une clé qui vous permettra d'accéder au données de votre disque dur. Cette option reste disponible que pour les versions pro de Windows. Pour mon exemple je vais utiliser 7zip qui peut crypter un fichier ou un dossier seulement qui ne pourra être ouvert que par le bon interpréteur ou par le logiciel même.

Je fournis ici un lien vers un fichier qui montre les manipulations avec 7zip dans le but de chiffrer un fichier mais aussi d'observer ce qu'il se passe quand on essaye de l'ouvrir sans autorisation : [Fonctionnement de 7zip](#)

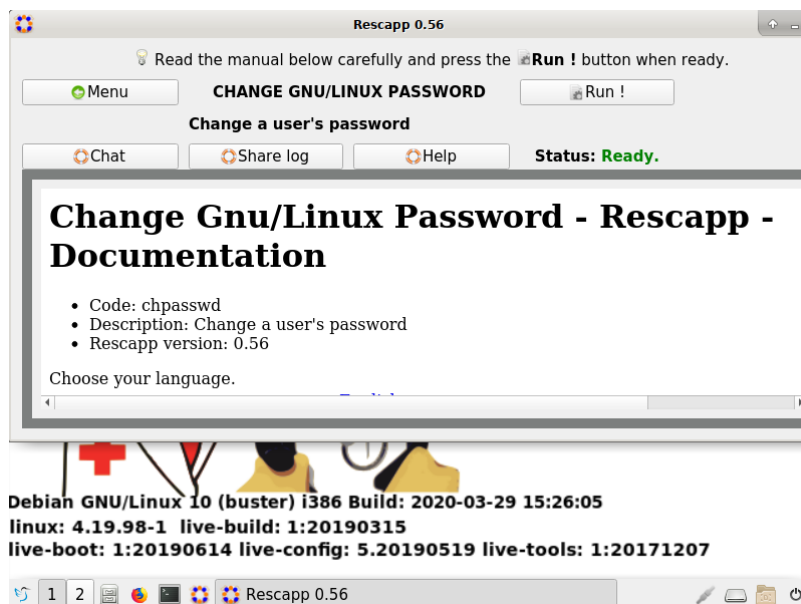
Essayant plusieurs fois de lire les données d'une machine ubuntu via un windows to go insérer dans celle-ci, sans réussir à accéder aux données. Et suite à une discussion avec le professeur j'ai compris que le formatage des disques étant différent windows ne peut lire les fichier situé sur la partition ubuntu, qui ne sera même pas visible d'ailleurs.



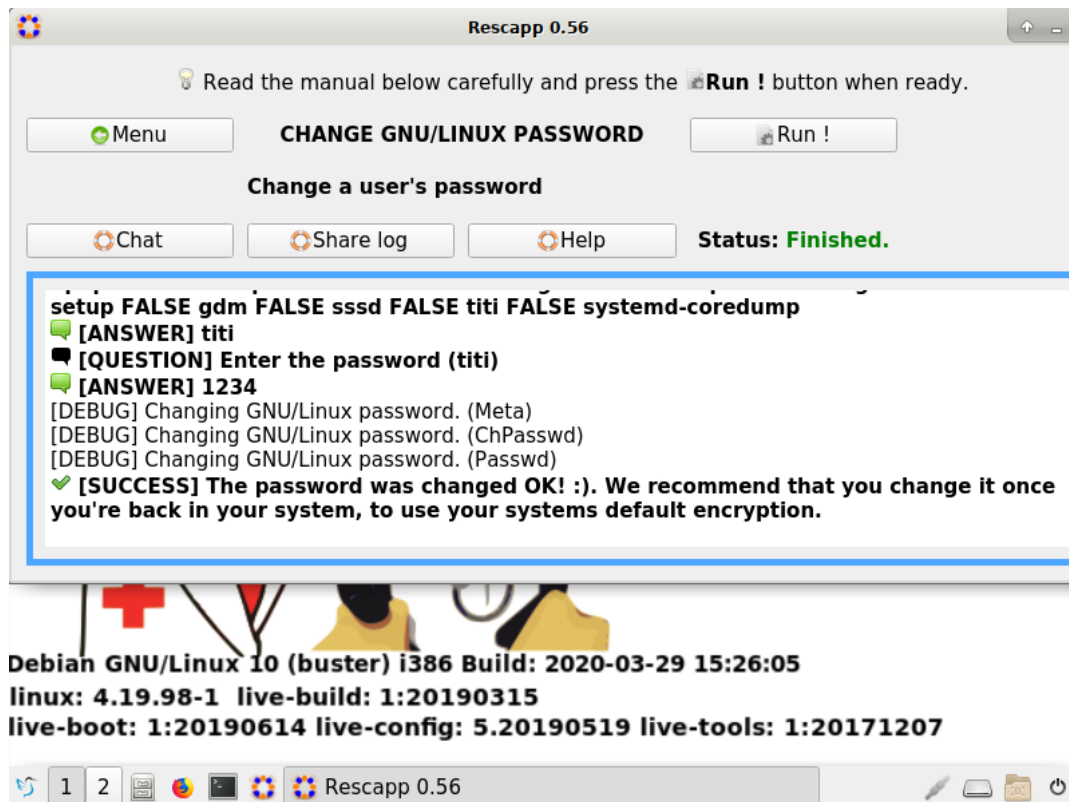
Pour compléter ce rendu, j'ai essayé de modifier le mot de passe de mon utilisateur dans ma machine ubuntu fraîchement créée, je sais qu'il existe une manière directement intégré au software d'Ubuntu/Grub pour modifier le mot de passe. Cependant, j'ai préféré utiliser un logiciel dédiée à la récupération de données appelé Rescatux.



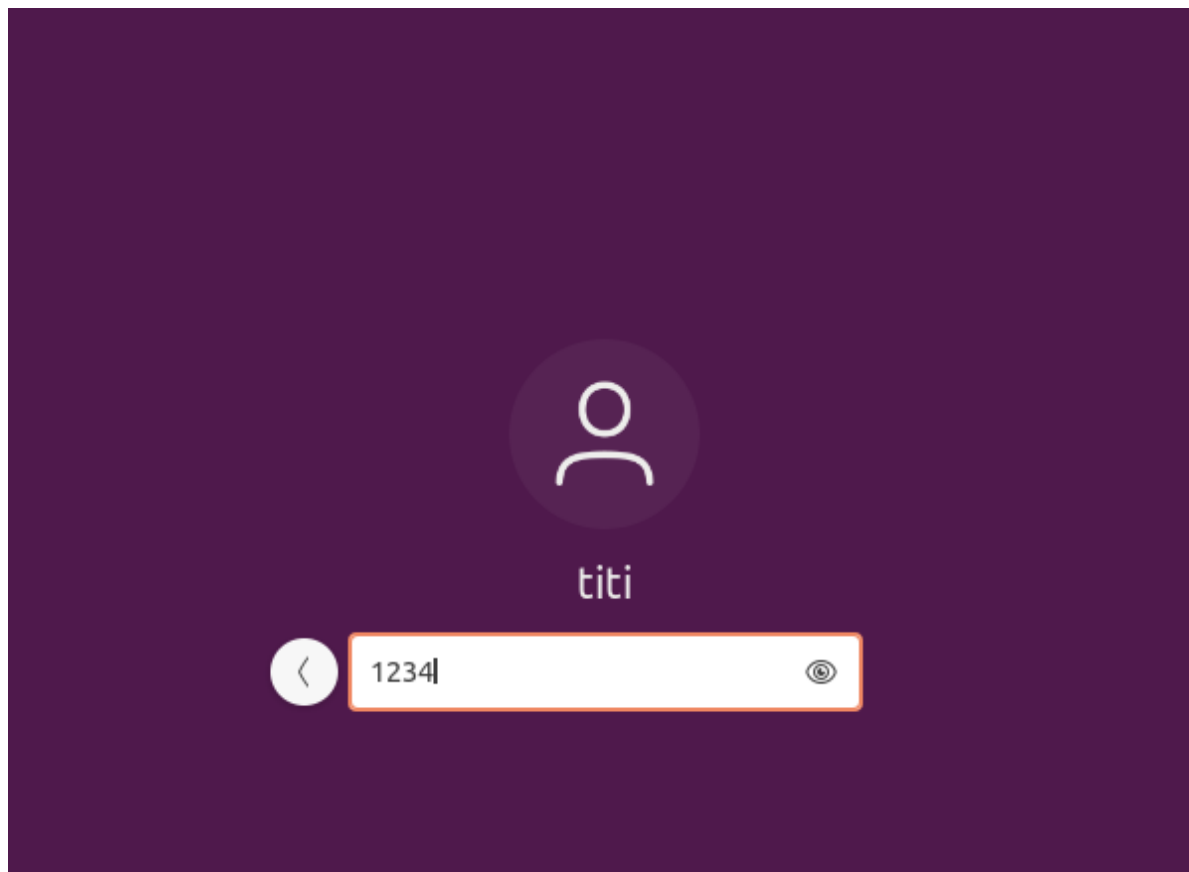
Dans l'image précédente j'accède directement au menu proposée par ce petit système portable et me dirige sur l'option changer le mot de passe linux/grub.



Une fois que le logiciel me signale que le changement est effectué avec succès, j'éteint la machine avec pour but de relancer ubuntu.



Sur cet écran je rentre le mot de passe configuré au préalable sur Rescatux. Et celui-ci fonctionne. La manipulation est terminée, nous reprenons la main sur l'ordinateur.



Le processus est assez similaire pour le système d'exploitation Windows. En revanche, pour mac OS, la seule technique qui fonctionne est celle basée sur le chargeur d'amorçage (OS) GRUB, dont j'ai parlé un peu plus tôt, car mac OS fonctionne sur le noyau Linux et possède donc les mêmes failles. Cela est vrai uniquement pour les anciennes versions et anciens ordinateurs.

En conclusion, ce compte rendu met en lumière la vraie sécurité que nous apporte un mot de passe windows ou linux. De meilleures solutions existantes telles que BitLocker, VeraCrypt et d'autres alternatives qui offrent des moyens réellement plus efficaces de protéger les informations sensibles, mais ce choix doit être guidé par les besoins spécifiques de chaque utilisateur. En adoptant des pratiques robustes de chiffrement et en restant attentif aux évolutions technologiques, il est possible de renforcer significativement la sécurité des données informatiques.

Source :

<https://www.7-zip.org/>

<https://chat.openai.com/> (pour correction et inspiration)

<https://lecrabeinfo.net/> (pour certain tutoriel)

<https://getsharex.com/> (pour les screenshots)

Tiago Gomes

Synthèse en cas d'incompréhension :  Synthès 1.1