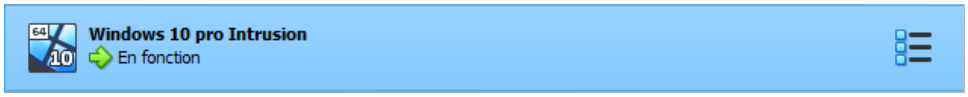
DERRUAU ROMÉO

TP Intrusion simple Windows

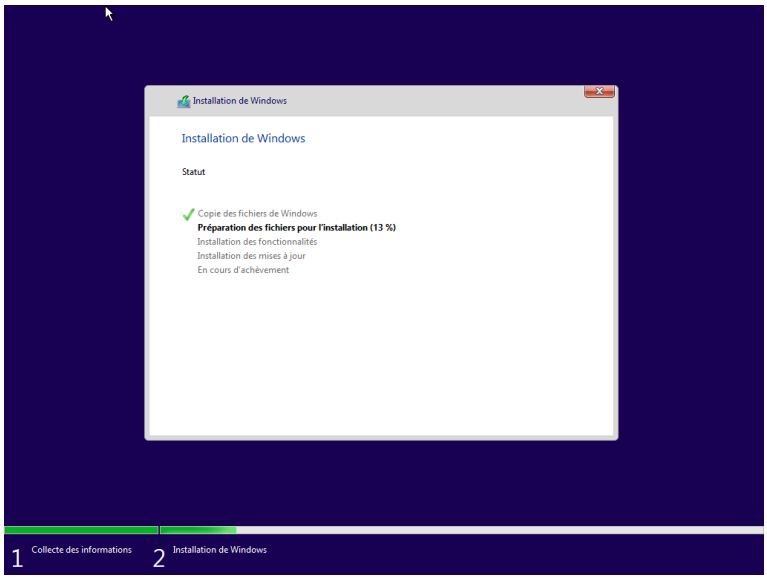
1- Création de la VM Windows 10

Dans un premier temps, j'ai créé une VM Windows 10 avec la configuration suivante :

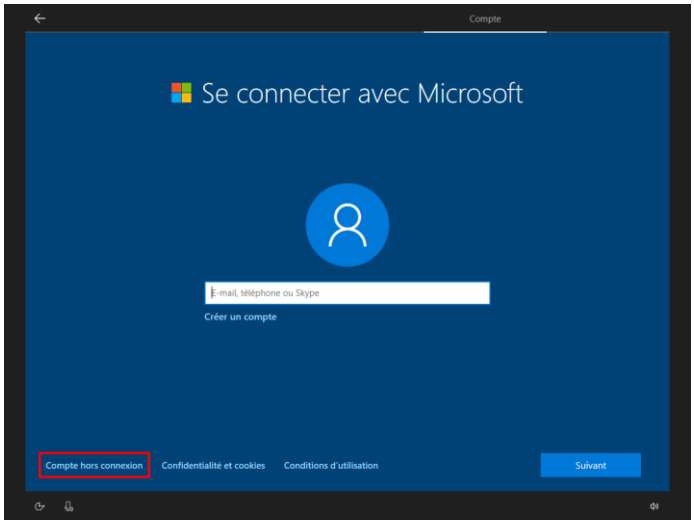
- 2 cœurs de processeur
- 20 GO de stockage
- 8 GO de RAM
- ISO Windows 10



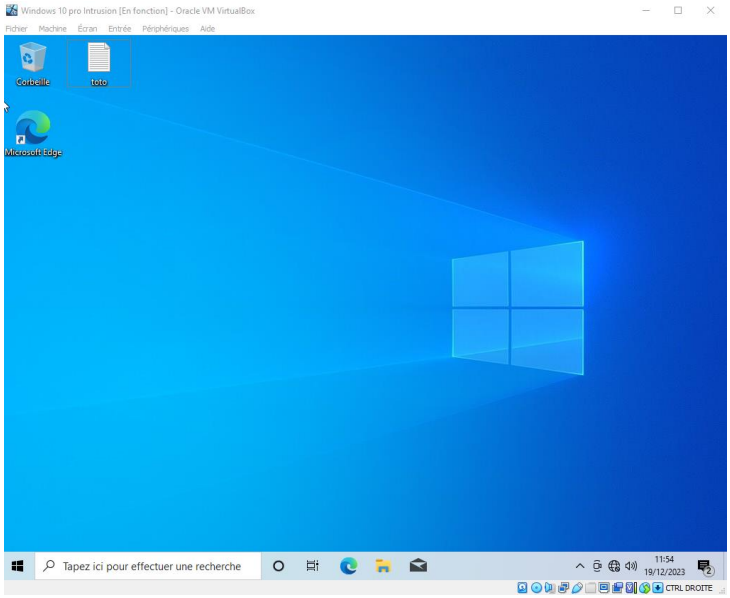
Dans un second temps, je procède à l'installation standard de Windows

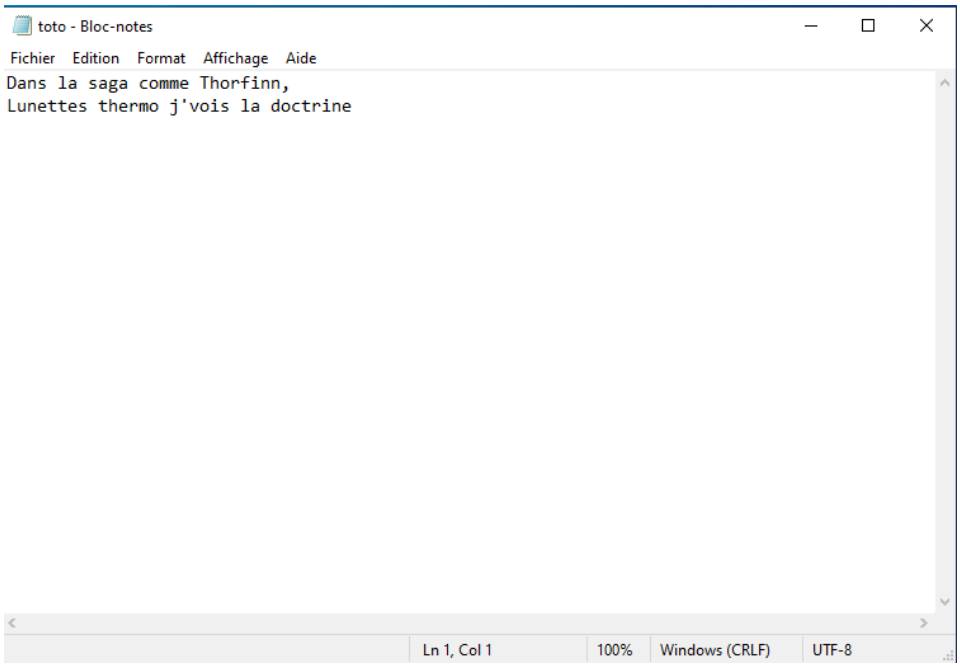


Je créé un compte Administrateur et lui attribue un mot de passe.



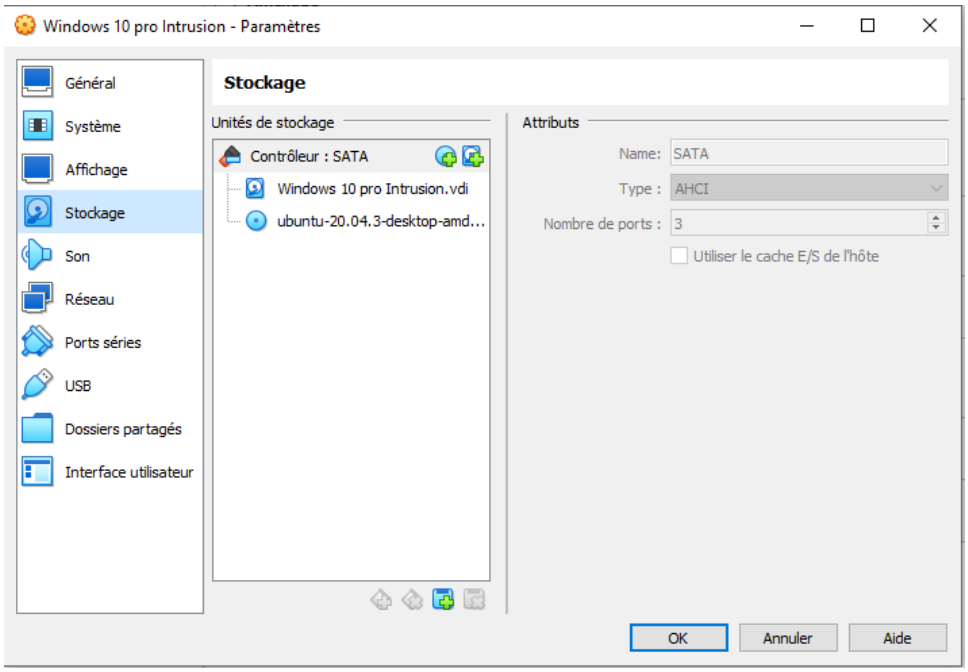
Une fois arrivé sur le bureau, je créé un nouveau fichier texte et je le nomme “Toto”, j’écris des paroles de chanson dans ce dernier.

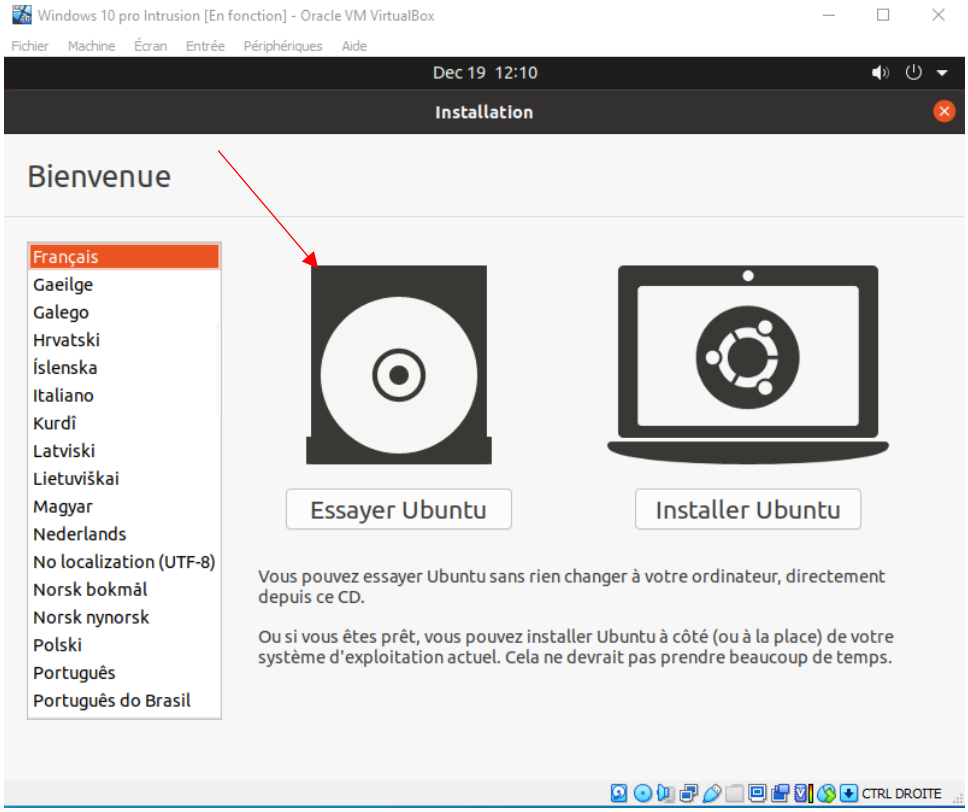




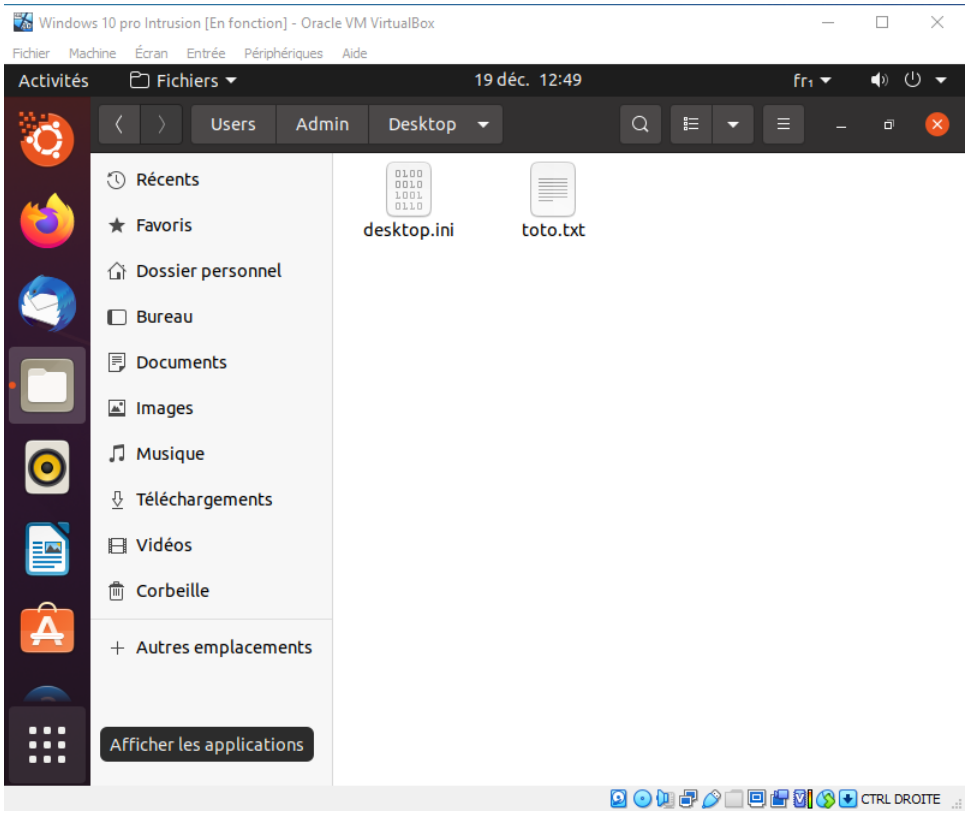
2- Passage sur l'ISO de Ubuntu

Premièrement on passe sur l'ISO de Ubuntu (20.4.3)

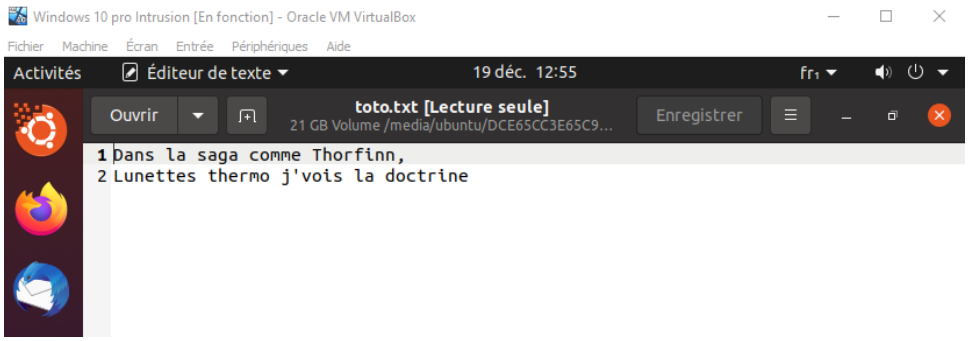




En ayant boot avec Ubuntu et en allant dans les fichiers et dans “Autre emplacement”, il faut suivre le chemin “Users/Admin/Desktop”



On peut avoir accès en lecture et en écriture au fichier “toto” que j’ai créé sur Windows 10.



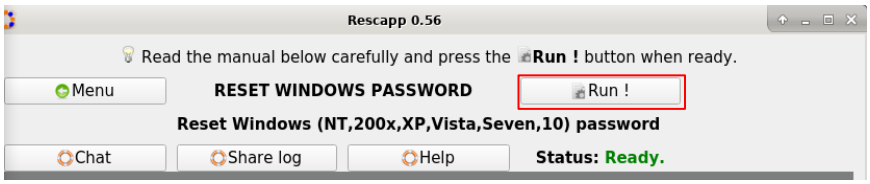
3- Choisissez l'une des techniques et expérimentez là pour voir si effectivement ce serait aussi simple que cela.

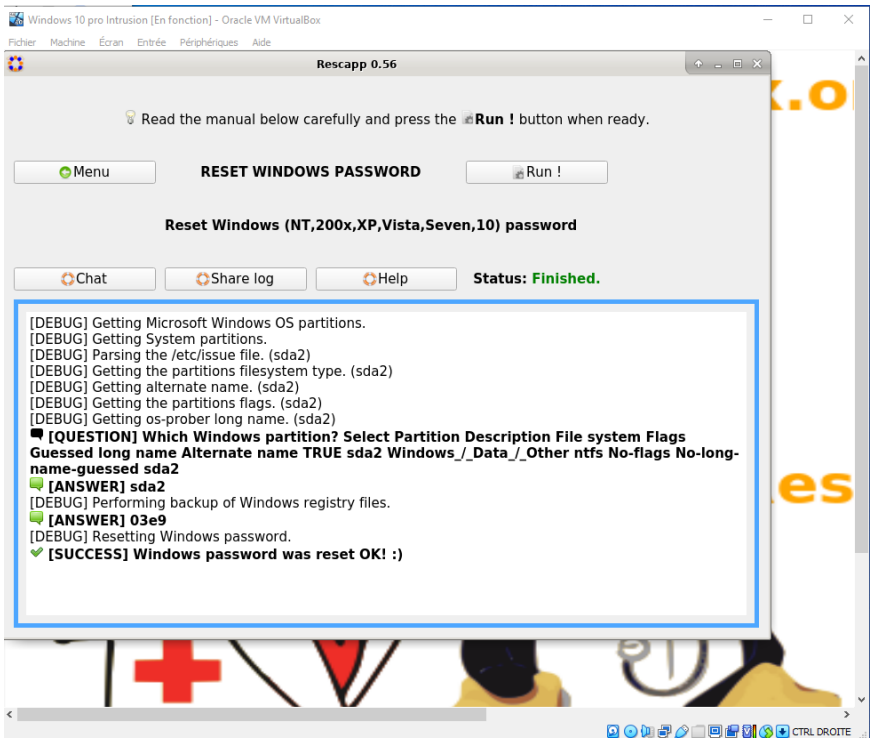
Je choisi la méthode Rescatux.

Je commence par boot avec l'iso Rescatux, puis je sélectionne le boot en mode auto.

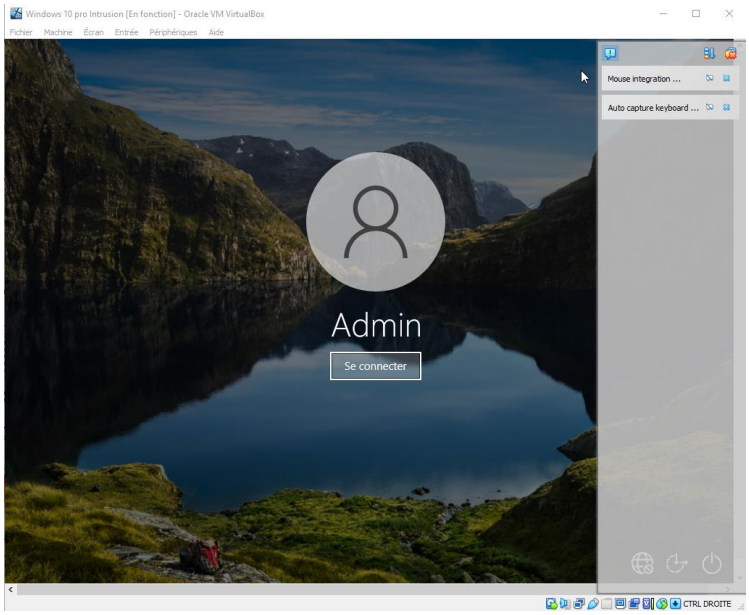
Par la suite, il faut ouvrir le fichier Recapp, puis cliquez sur Reset Windows password.

Cliquer sur RUN pour exécuter le reset du mot de passe.





Une fois le message “password was reset OK” affiché, il faut redémarrer la machine sur Windows 10 pour vérifier qu’il n’y a plus de mot de passe.



Il n’y a effectivement plus de mot de passe sur le compte “admin”.

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

En prenant en compte, toutes les méthodes présentent sur le site évoqué dans le sujet, la méthode Utilman qui semble se rapprocher le plus de celle utilisée dans la vidéo de Mr Robot.

Elle contient comme dans la vidéo le lancement du système tiers, le contrôle du CMD et la possibilité de renommer les fichiers.

5- Conclusion

Tirez des conclusions sur ce que vous venez de découvrir.

> En conclusion, on comprend que la sécurité apporter par un mot de passe n'est pas optimal et présente beaucoup de faille et de méthode pour passer outre l'identification.

Déterminez deux manières de se protéger de ce problème et expérimentez-les toujours dans votre machine virtuelle.

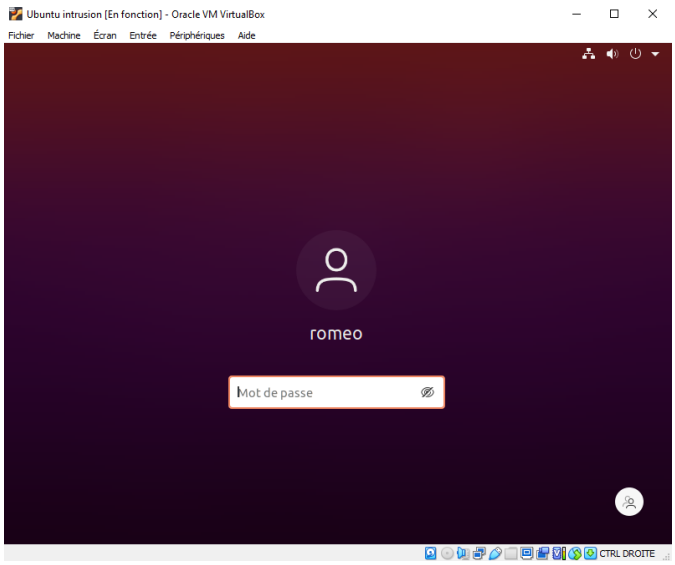
> D'après ChatGPT et mes expériences.

- Activez la double authentification : Si possible, activez la double authentification sur vos comptes. Cela ajoutera une couche de sécurité supplémentaire en demandant un code de vérification au-delà du mot de passe lors de la connexion.

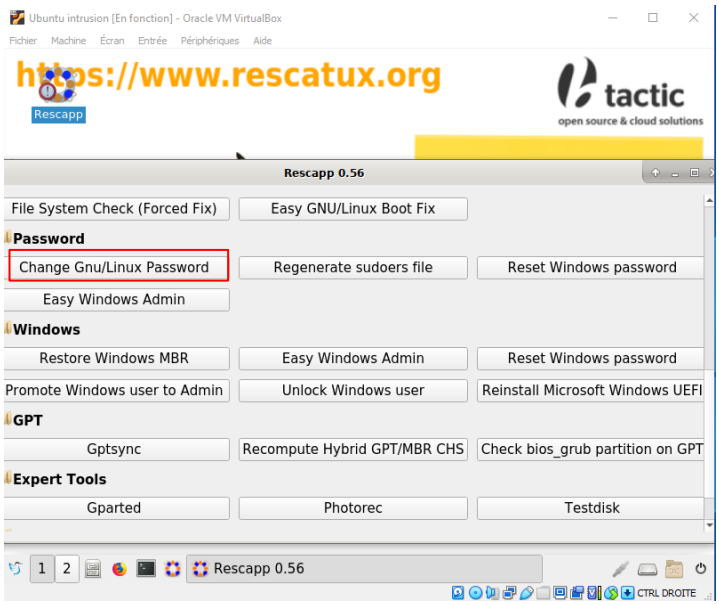
- Sachez qui a accès à votre appareil : Évitez de laisser votre appareil sans surveillance et assurez-vous que seules des personnes de confiance ont accès à votre ordinateur ou à votre téléphone.

Pensez-vous qu'on a le même souci sur Mac ou Linux ? Testez sur une VM Linux fraîchement créé par vos soins, reprenez le fil de ce TP

> Je recommence comme dans les premières étapes, je créé une VM Ubuntu, j'installe l'OS avec un compte admin et un mot de passe.

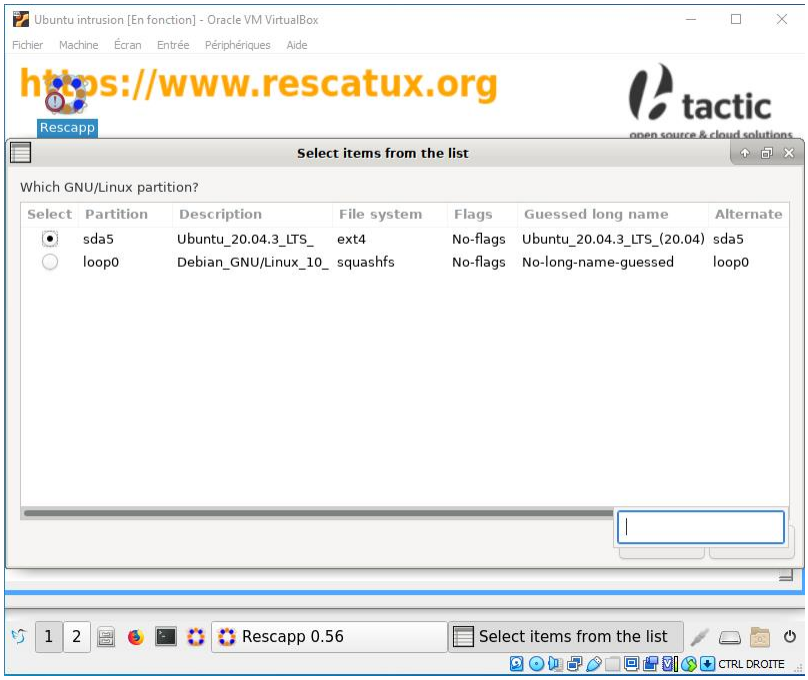


Je reprends la méthode Rescatux.

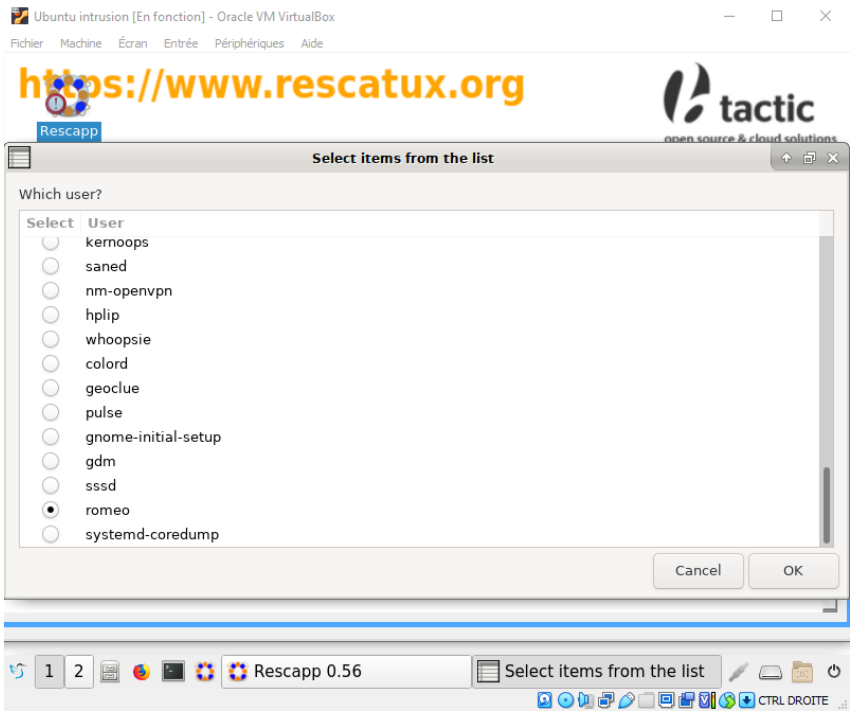


Je clique sur Change Gnu/Linux Password, pour modifier le mot de passe à ma guise car je ne peux pas le reset.

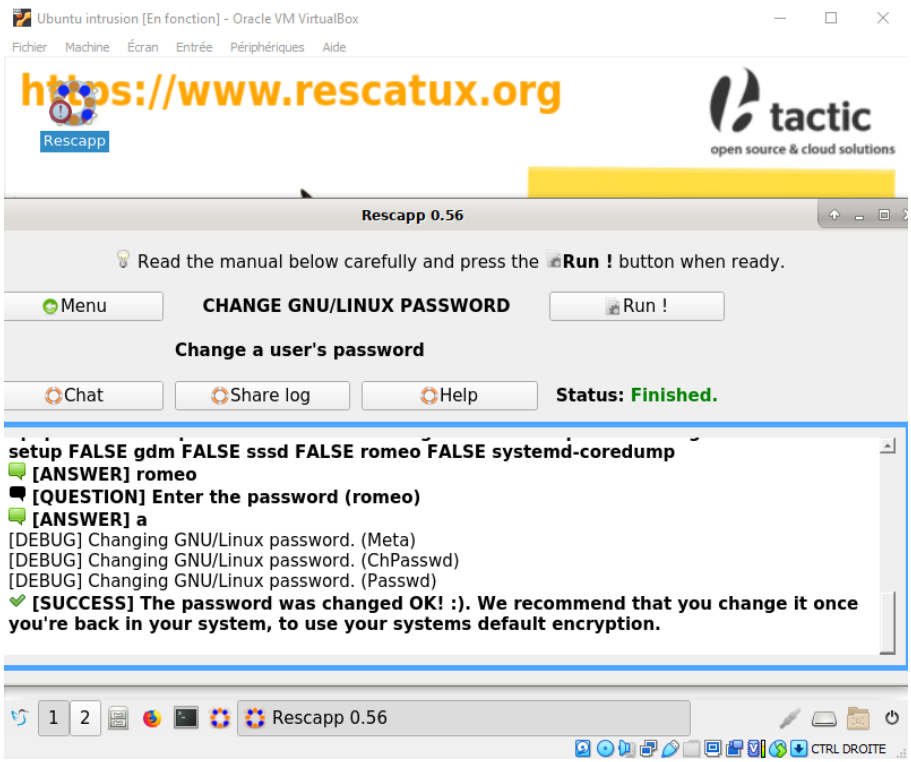
Je sélectionne la partition disque souhaité.

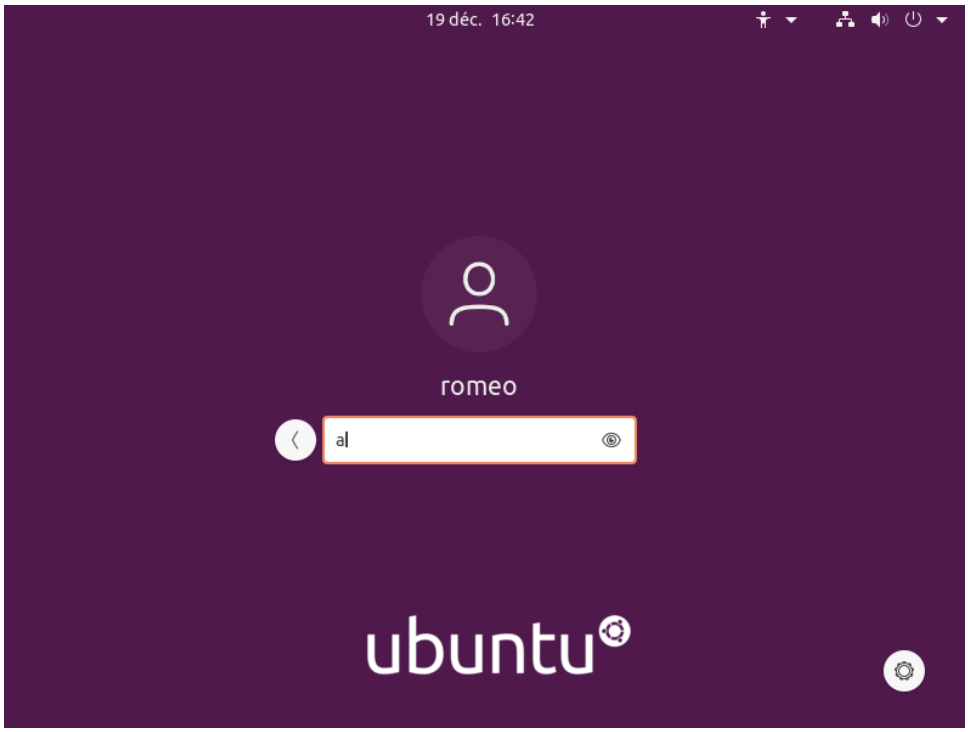


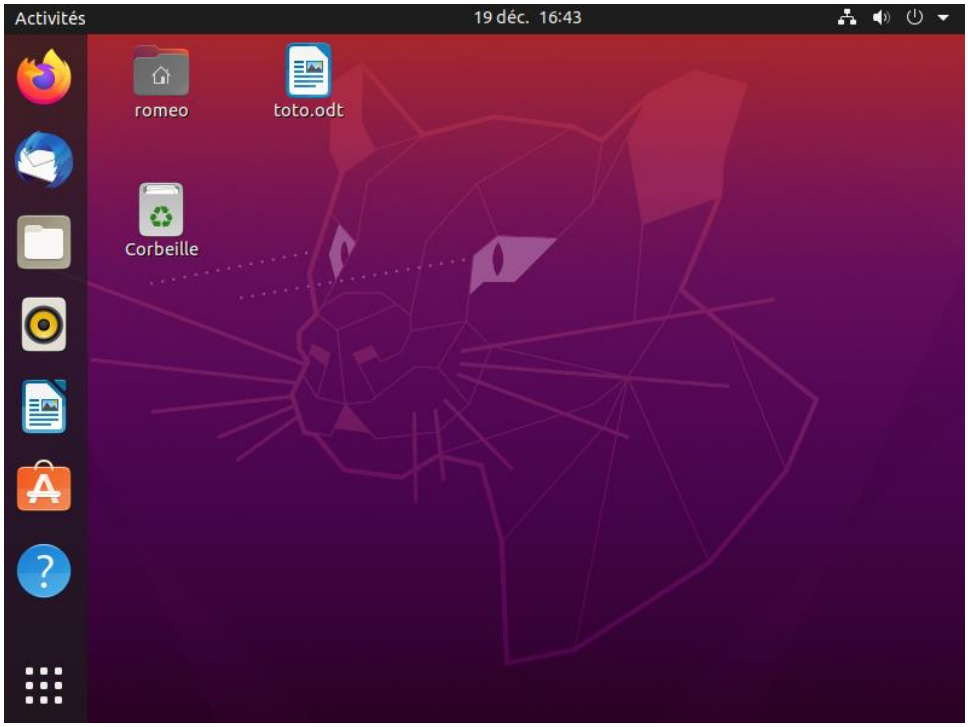
Je sélectionne l'utilisateur souhaité concerné par le changement de mot de passe.



Félicitation, le mot de passe vient d’être changé sans problème.






Activités
19 déc. 16:43
romeo
toto.odt
Corbeille