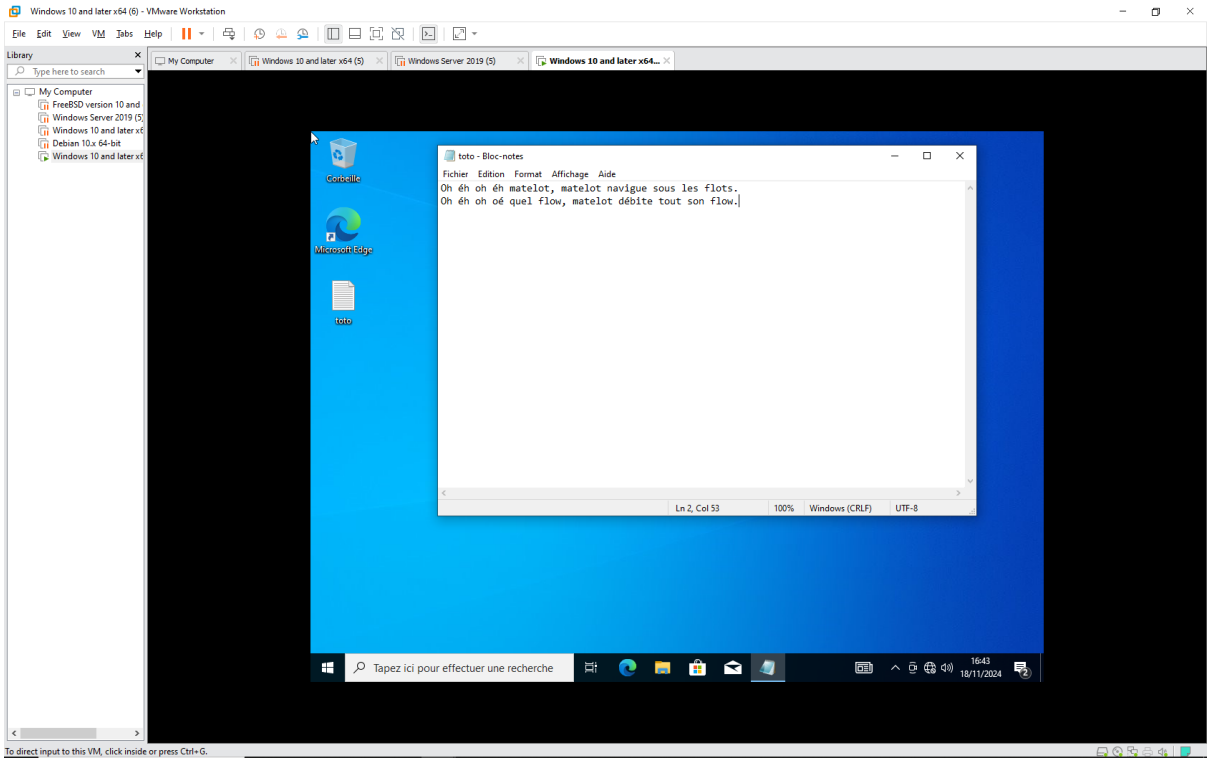
TP Intrusion

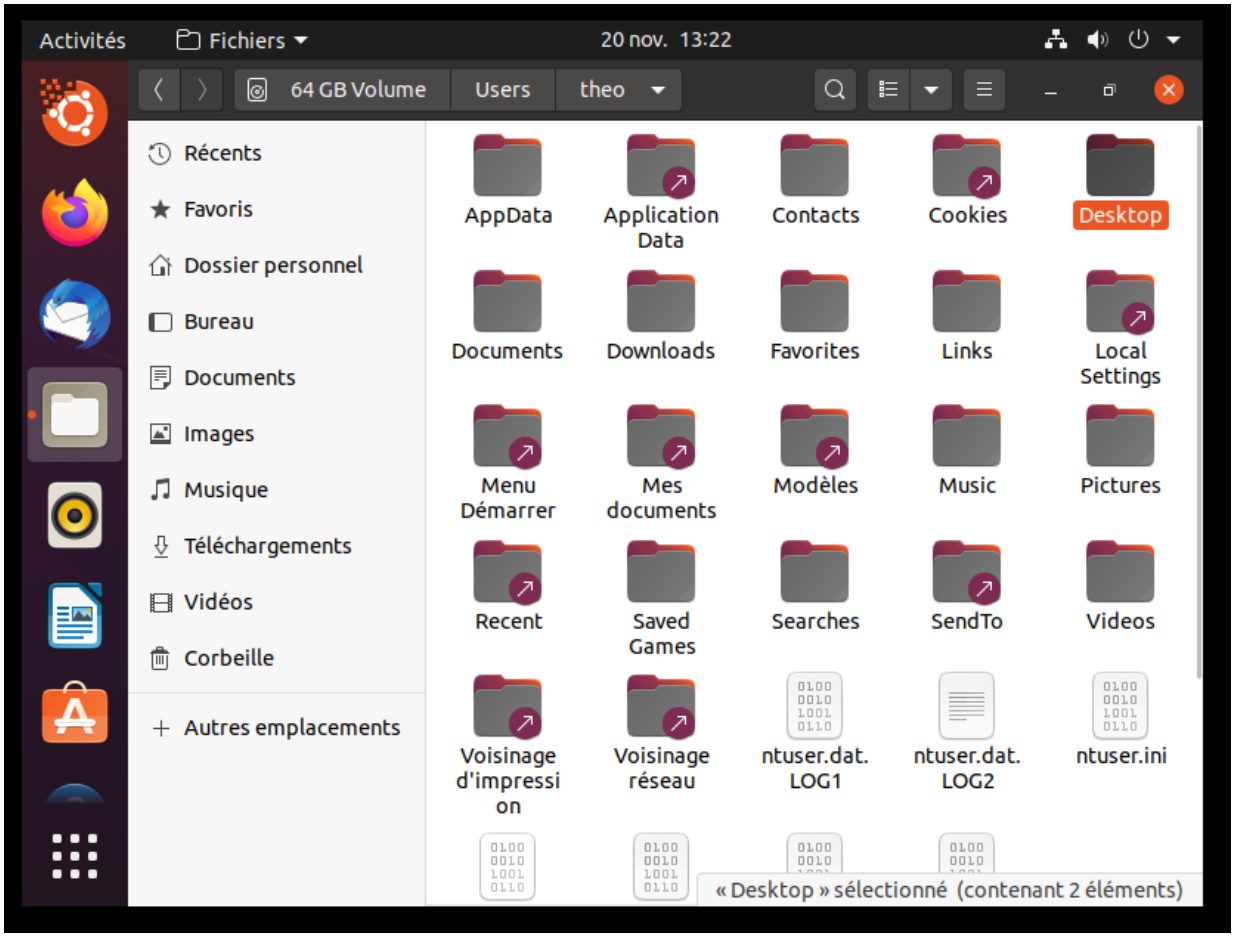
1) Une Machine virtuelle a été créée avec une iso Windows 7 pro.

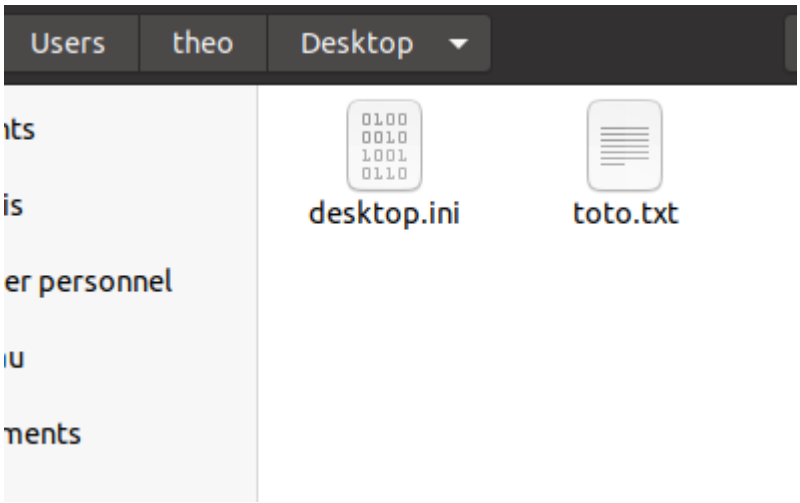
Le fichier toto.txt a été ajouté au bureau.



2) Passons sur Linux Ubuntu, avec cette iso : ubuntu-20.04.1-desktop-amd64.

Ensuite tentons de chercher ce fichier texte toto.txt dans les dossiers au sein d'Ubuntu





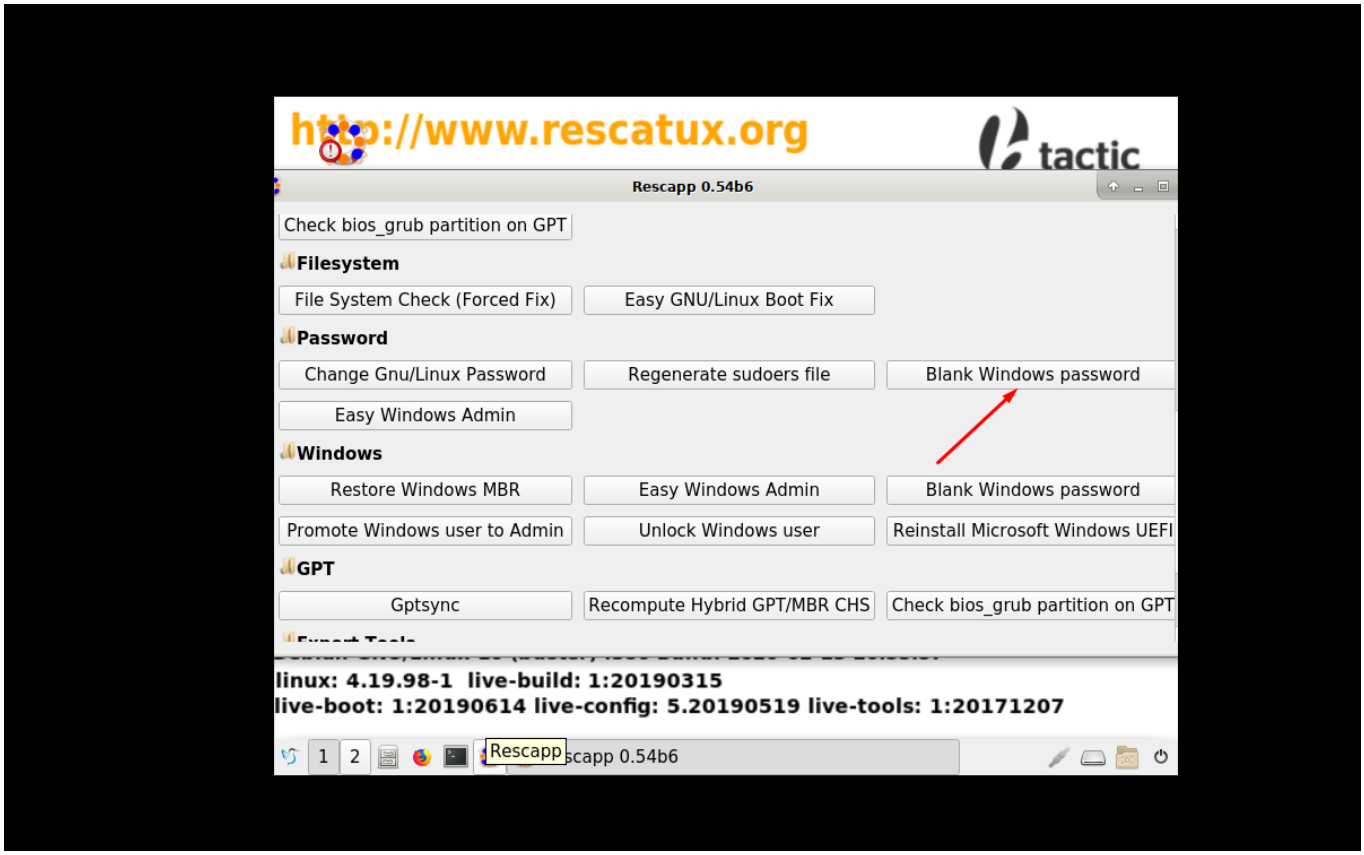
Le chemin d'accès est si dessus, le fichier toto.txt y est bien présent.

Il est possible de le lire et de le modifier, que ce soit sur Windows ou sur Ubuntu.

3) La méthode correspondant à l'extrait vidéo est la 2a avec utilman.exe.

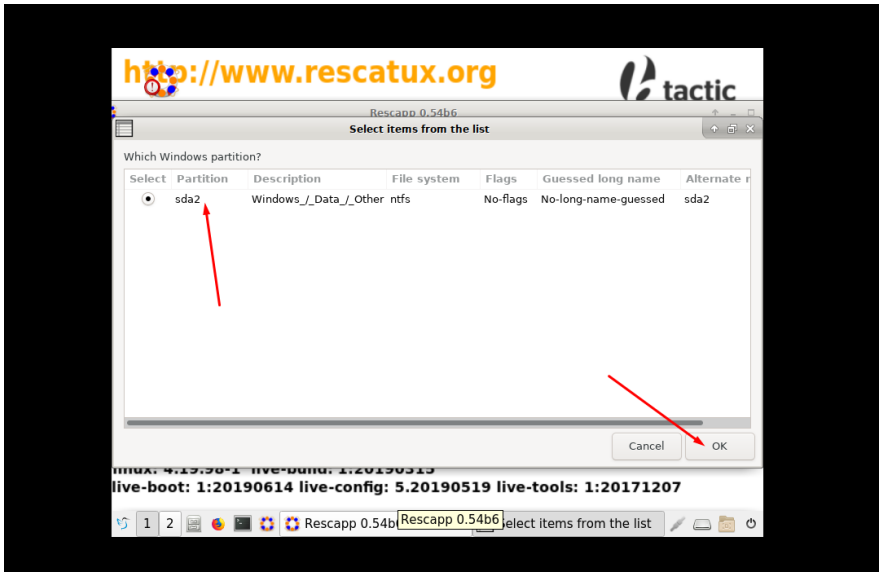
Pour la suite de la procédure je m'aiderai de la méthode 1 : Rescatux.

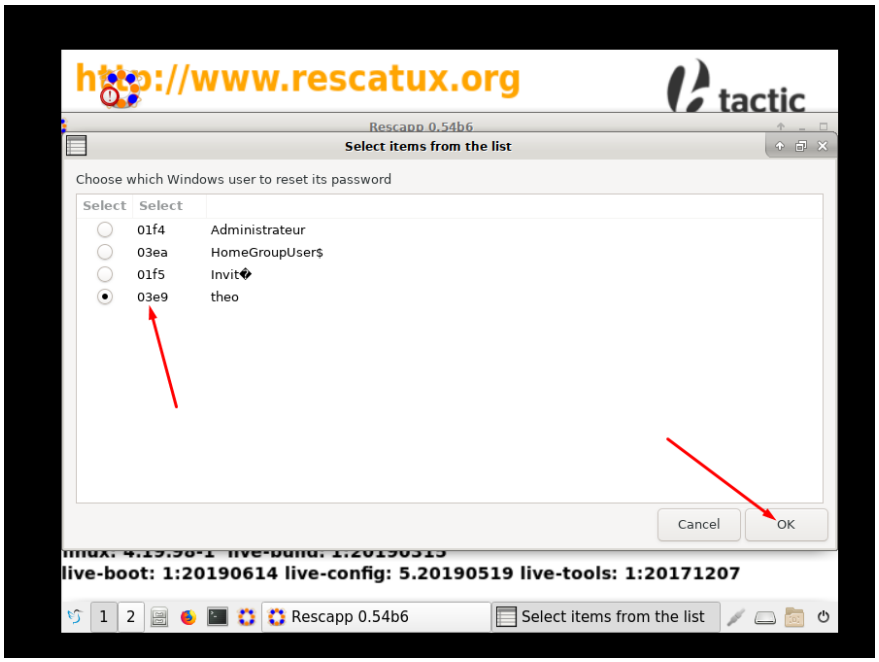
Après avoir boot sur Rescatux avec l'iso "rescatux-0.72-beta8" je trouve cette page où il suffira d'appuyer sur Blank Windows password.

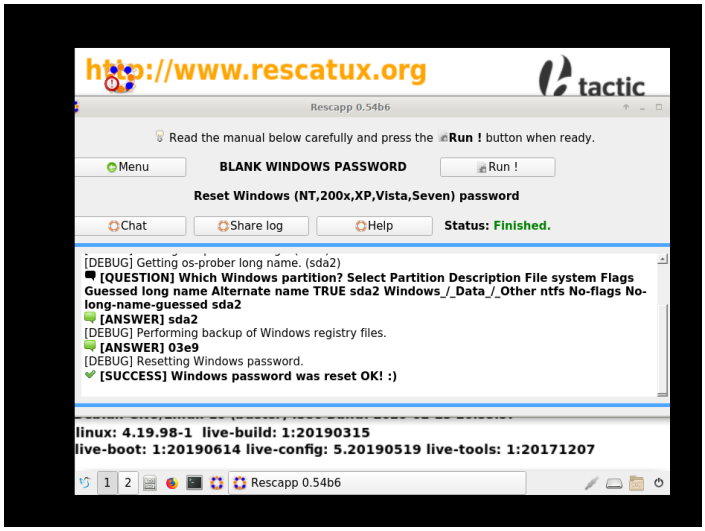


Puis sur Run !

Enfin il suffit de passer par le chemin sda2 -> session du mot de passe à modifier (ici theo).


http://www.rescatux.org
tactic
Rescapp 0.54b6
Select items from the list
Which Windows partition?
Select
Partition
Description
File system
Flags
Guessed long name
Alternate n
sda2
Windows_/_Data_/_Other
ntfs
No-flags
No-long-name-guessed
sda2
Cancel
OK
live-boot: 1:20190614 live-config: 5.20190519 live-tools: 1:20171207
Rescapp 0.54b6
Select items from the list

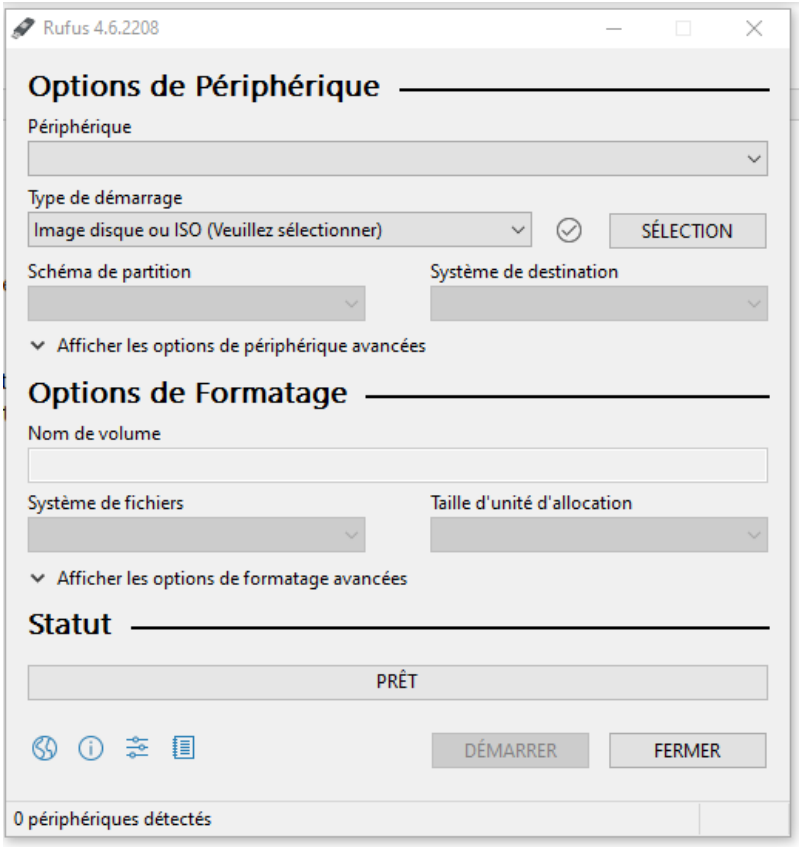

http://www.rescatux.org
tactic
Rescapp 0.54b6
Select items from the list
Choose which Windows user to reset its password
Select
Select
01f4
Administrateur
03ea
HomeGroupUser$
01f5
Invit
03e9
theo
Cancel
OK
live-boot: 1:20190614 live-config: 5.20190519 live-tools: 1:20171207
Rescapp 0.54b6
Select items from the list


http://www.rescatux.org
tactic
Rescapp 0.54b6
Read the manual below carefully and press the Run ! button when ready.
Menu
BLANK WINDOWS PASSWORD
Run !
Reset Windows (NT,200x,XP,Vista,Seven) password
Chat
Share log
Help
Status: Finished.
[DEBUG] Getting os-prober long name. (sda2)
[QUESTION] Which Windows partition? Select Partition Description File system Flags Guessed long name Alternate name TRUE sda2 Windows_/_Data_/_Other ntfs No-flags No-long-name-guessed sda2
[ANSWER] sda2
[DEBUG] Performing backup of Windows registry files.
[ANSWER] 03e9
[DEBUG] Resetting Windows password.
[SUCCESS] Windows password was reset OK! :)
linux: 4.19.98-1 live-build: 1:20190315
live-boot: 1:20190614 live-config: 5.20190519 live-tools: 1:20171207
Rescapp 0.54b6

Le mot de passe a été réinitialisé avec succès.

DISCLAIMER : Il est rappelé que les techniques et propos tenus en cours restent dans un cadre pédagogique et ne doivent être en aucun cas utilisés à des fins malveillantes.

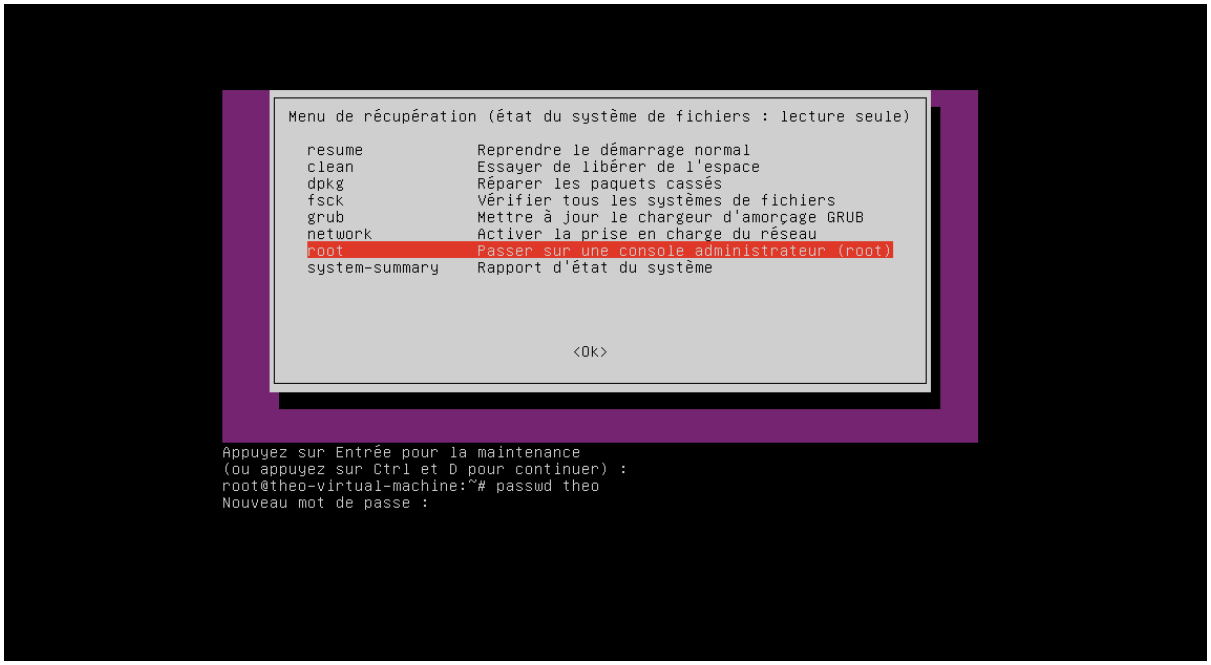
4) Conclusion : Cette modification a été effectuée directement dans la machine virtuelle, mais il est également possible de l'exécuter avec le logiciel Rufus dans une clé USB bootable comme ci-dessous. En plaçant l'iso rescatux dans le champ "type de démarrage". Puis dans "Périphérique" la clé USB préalablement formatée.



Afin de solutionner à la réinitialisation de mot de passe nous pourrions déjà passer sur Windows 10 ou 11 et ensuite se connecter via une connexion Microsoft, car les sessions locales ont des limites de sécurité.

La procédure Linux est toute autre, afin de modifier le mot de passe via le menu Grub > options avancées > menu de récupération ensuite taper le nom de la machine et enfin le mot de passe.

Ce qui nous prouve que la réinitialisation des mots de passe de session Linux est aussi simple pour des attaquants voir même encore moins sécurisé que sur Windows.


Menu de récupération (état du système de fichiers : lecture seule)
resume Reprendre le démarrage normal
clean Essayer de libérer de l'espace
dpkg Réparer les paquets cassés
fsck Vérifier tous les systèmes de fichiers
grub Mettre à jour le chargeur d'amorçage GRUB
network Activer la prise en charge du réseau
root Passer sur une console administrateur (root)
system-summary Rapport d'état du système
<Ok>
Appuyez sur Entrée pour la maintenance
(ou appuyez sur Ctrl et D pour continuer) :
root@theo-virtual-machine:~# passwd theo
Nouveau mot de passe :