

TP 2 : Intrusion simple

Guillaume Jobard

Table des matières

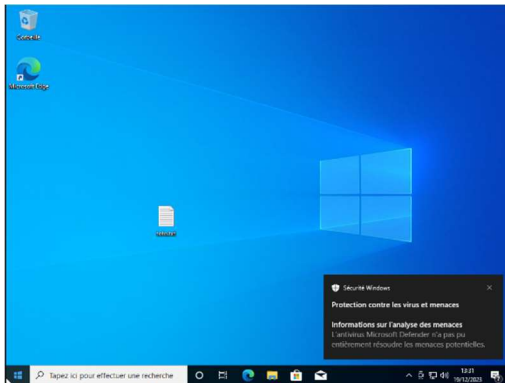
Test d'intrusion	3
Étape 1 :	3
Étape 2 :	3
Étape 3 :	4
Étape 4 :	5
Conclusion et protection	7
Procédure BitLocker	8
Essai avec une distribution Linux.....	12

Test d'intrusion

Étape 1 :

Création de la VM sur VMWare, avec un iso Windows 10 pro avec un compte local en administrateur (lgm).

Une fois démarré, je crée un fichier texte sur le bureau (toto.txt). Ensuite j'éteins la VM.



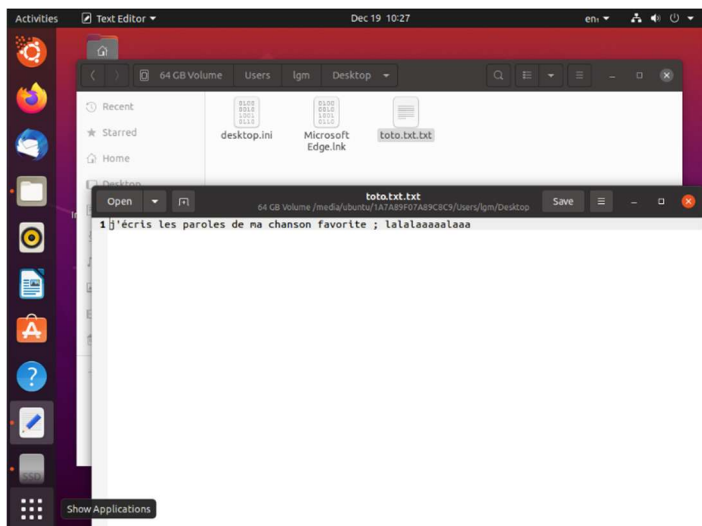
Étape 2 :

Je remplace l'iso dans les paramètres de la VM avec celle de Ubuntu Desktop 20.04.3 en version d'essai.

Lorsque je démarre la VM, j'accède au BIOS en martelant la touche Échap afin de boot en LiveDVD.

Une fois ouvert je réalise qu'en allant dans *l'explorateur de fichier*, *other location*, *SSD*, *user*, « *lgm* », puis dans le fichier *desktop* ; je retrouve mon fichier créer plus tôt sur mon Windows 10.

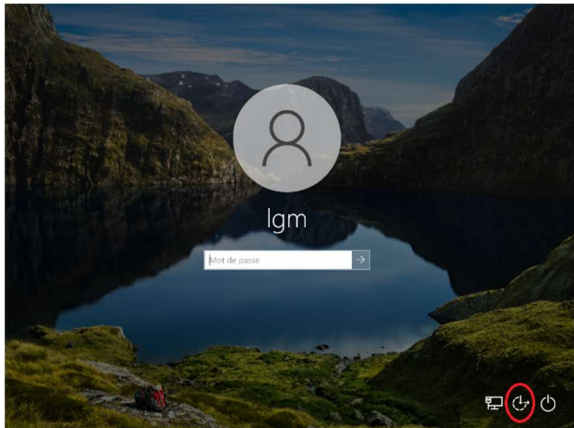
Je peux y accéder en lecture mais aussi en modification.



Étape 3 :

Premièrement j'ai essayé de réaliser la technique de la méthode 2 avec Utilman.exe ([Article](#))

Le but étant de remplacer le fichier Utilman.exe qui permet d'ouvrir les options d'ergonomie sur l'écran de verrouillage Windows. Afin de le remplacer par un cmd.exe.



Voici les notes que j'ai pu en tirer en réalisant la procédure.

« J'essaye la technique du fichier utilman.exe à remplacer par un cmd.exe grâce à une faille de sécurité Windows

Sur ma VM j'accède au bios et je lance l'Install du setup, puis sur l'interface graphique je clique sur "réparer l'ordinateur" ainsi une fenêtre avec plusieurs options s'ouvre

Je clique sur "dépannage" et "invite de commande"

Ensuite sur l'invite de commande je vais aller dans le fichier système de Windows en suivant ces commandes

"C :"

"cd Windows\System32"

Ensuite on procède à une copie du fichier utilman.exe en utilman.exe.old

"copy Utilman.exe Utilman.exe.old"

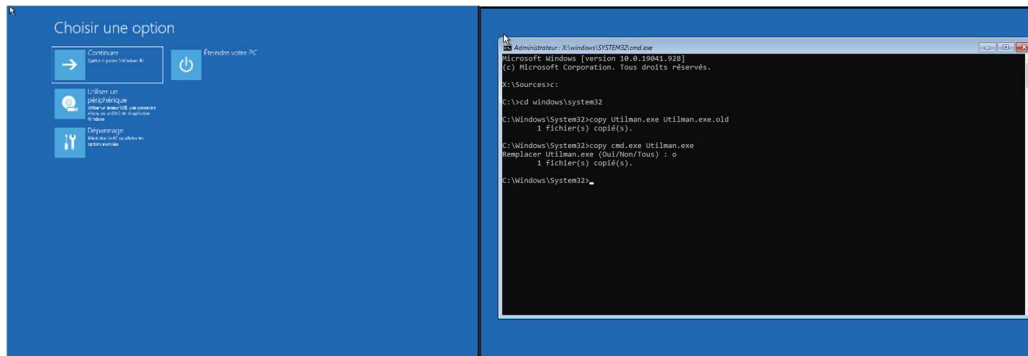
Puis on remplace le fichier utilman.exe en cmd.exe grâce à la commande

"copy cmd.exe Utilman.exe"

"Exit" puis entrée

De retour sur ma fenêtre me demandant de choisir une option

Je clique sur "continuer" pour lancer le redémarrage de mon Windows »



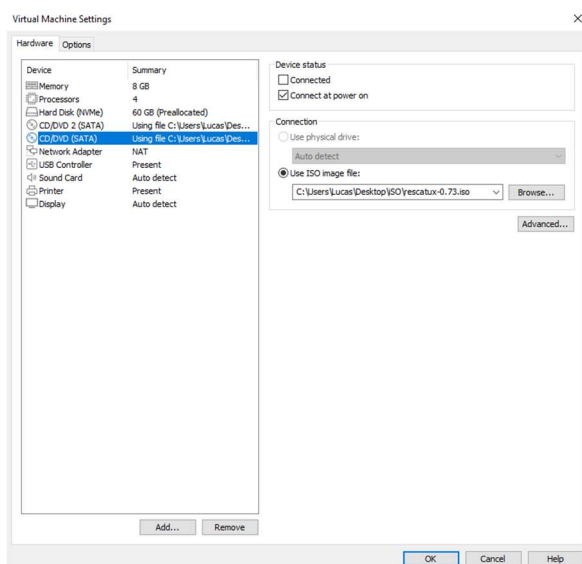
Malheureusement je me suis retrouvé bloqué car la version de mon Windows 10 était trop récente par conséquent Windows Defender détectait l'anomalie du fichier et m'empêchait d'ouvrir un cmd à la place des options d'ergonomie sur l'écran de verrouillage.

J'ai donc pensé à désactiver Windows defender via un PowerShell, exécuter par le cmd ou encore désactiver Windows defender via l'éditeur du registre. Malheureusement là aussi, ça n'a pas fonctionné. Manque de temps je n'ai pas pu fouiller davantage.

Étape 4 :

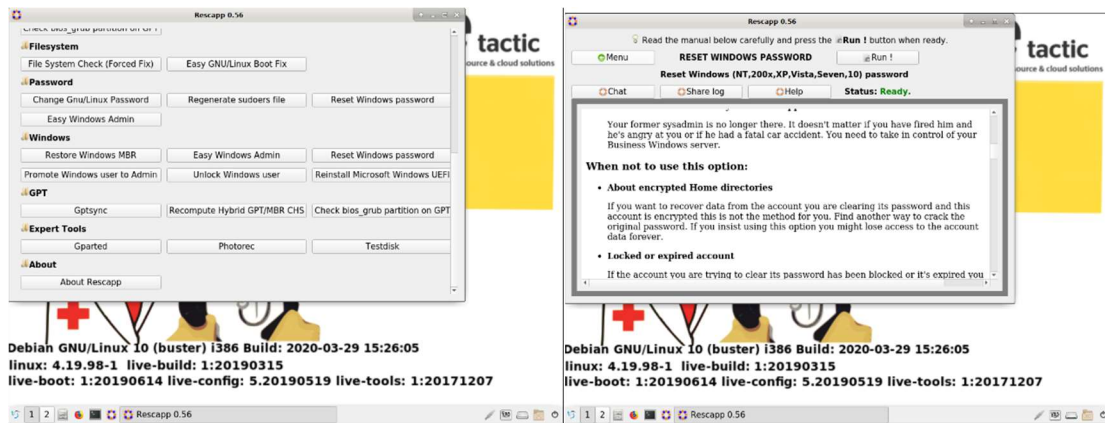
J'ai donc essayé la méthode numéro 1 avec Rescatux. ([Article](#)). Cette fois-ci ça été beaucoup plus rapide et intuitif.

Avec cette même VM Windows 10 j'ai créé un deuxième CD/DVD Drive dans les paramètres de la VM sur VMWare avec l'ISO de Rescatux.

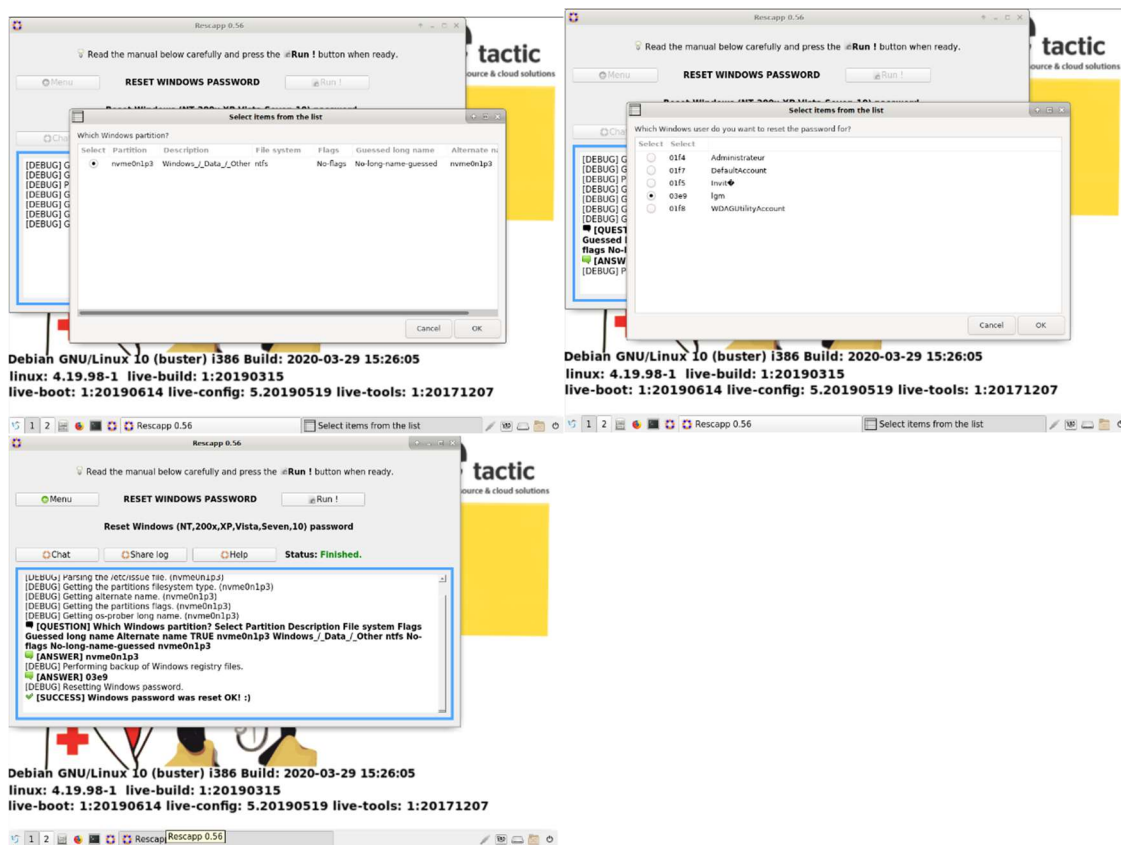


Ici également je démarre la VM et j'accède au BIOS, cette fois-ci je boot sur le CD/DVD Drive 2 avec Rescatux.

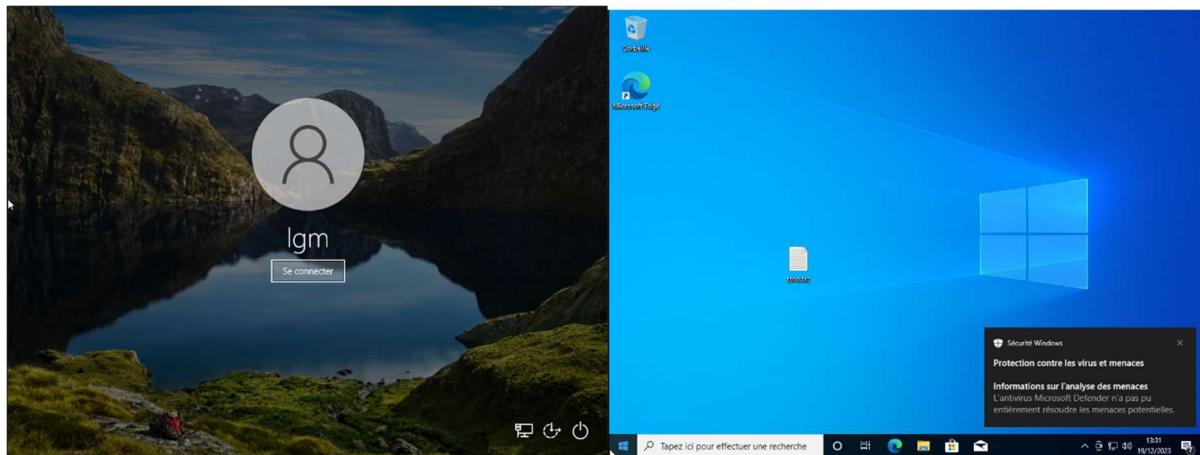
Une fois l'OS démarré je vais cliquer sur « Reset Windows password » puis sur « Run ».



Ensuite je choisis ma partition, mon compte utilisateur, et j'attends que ça mouline.



Une fois que c'est « OK », je redémarre ma VM. Cela va lancer mon Windows 10. Et je vois bien que je n'ai plus de besoin de mot de passe sur ma session.



Et voilà j'ai pu faire sauter le mot de passe et accéder au profil.

Cependant la méthode qui s'approcherait le plus de l'extrait de MrRobot serait la méthode de Utilman.exe.

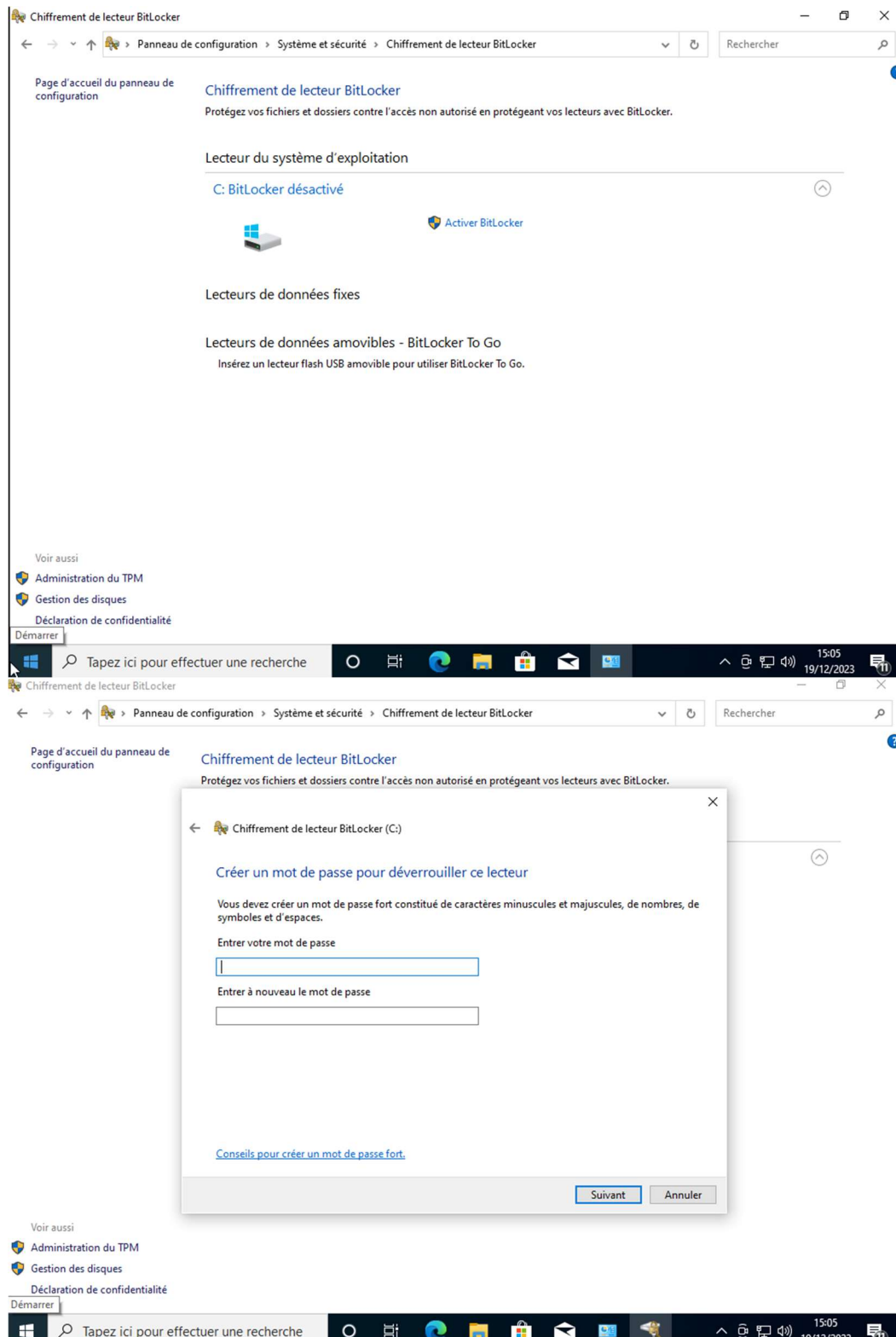
Conclusion et protection

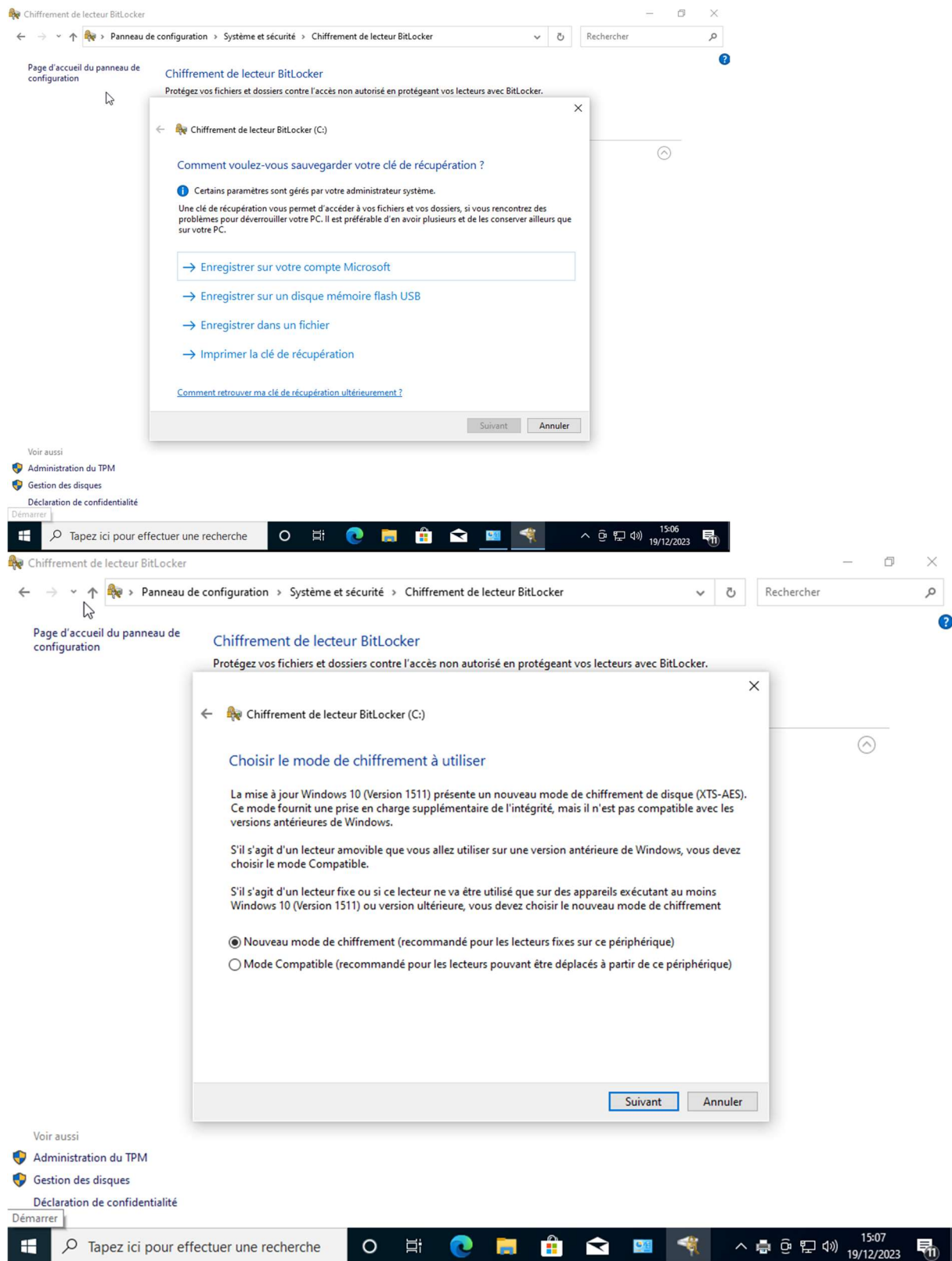
Ce que je peux conclure de ce travail, c'est que faire sauter un mot de passe d'une session Windows est très facile et je dirais même accessible à n'importe qui. On comprend donc très vite qu'un mot de passe de session est très important à renforcer. Effectivement la plupart des utilisateurs lambda, professionnel ou personnel, juge que le mot de passe de session est « inutile », par conséquent cela procure une des principales failles surtout dans le cadre professionnel. On va donc pouvoir s'intéresser à comment se protéger face à ceci et quelles solutions mettre en place.

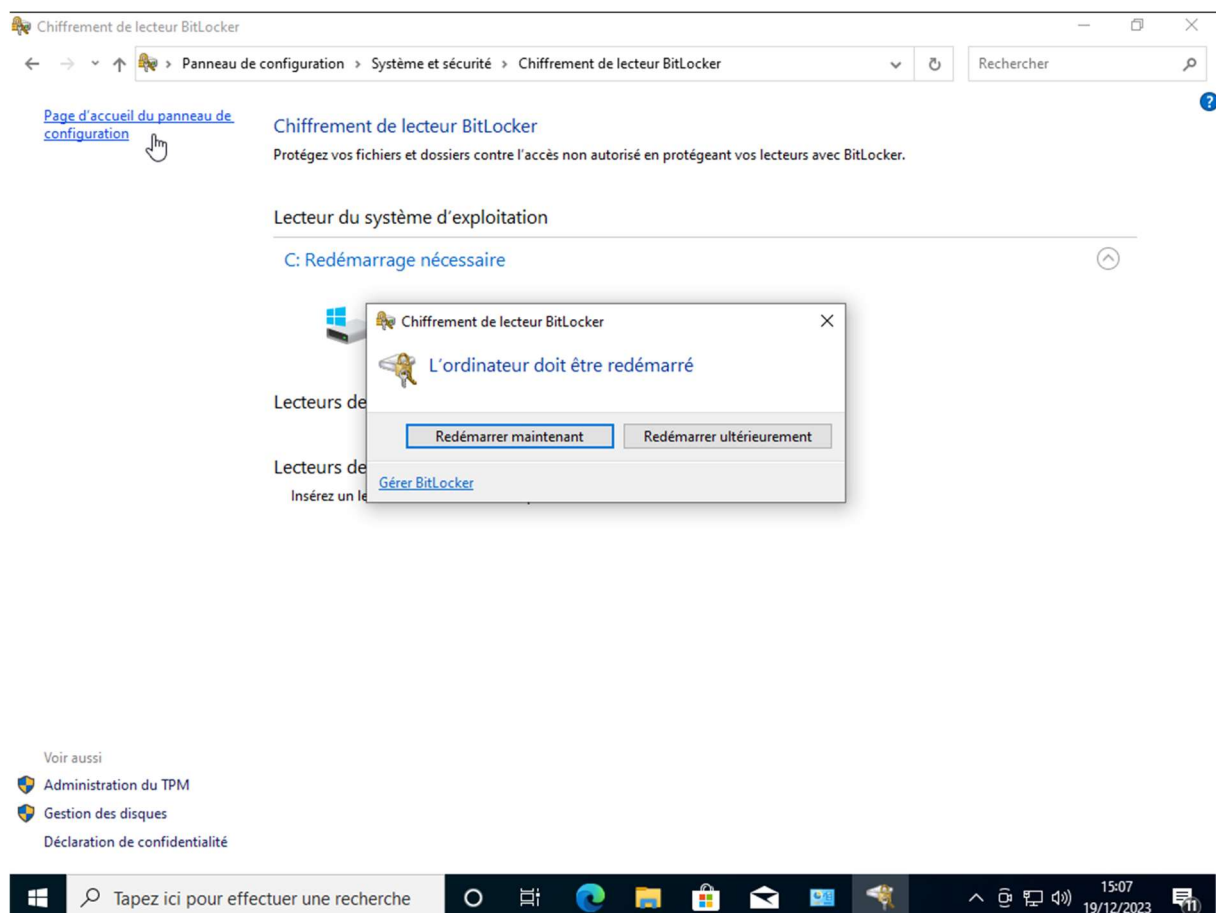
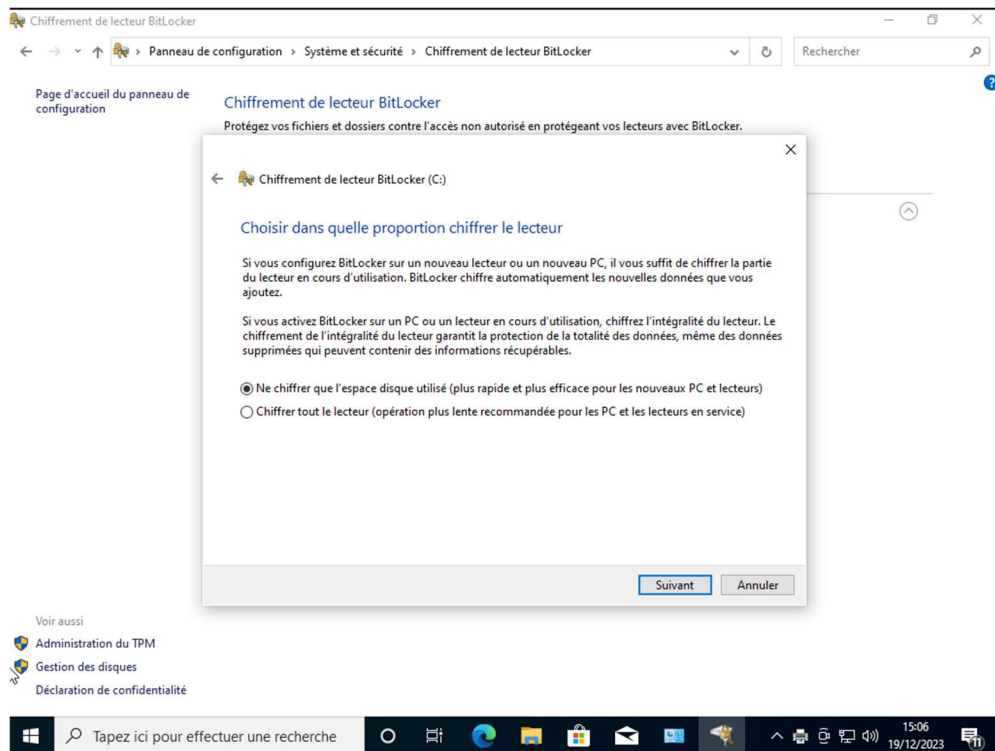
Premièrement, vérifier son bios ; les mises à jour, l'ordre de démarrage soit bien établi en sorte que ce soit son OS principal qui démarre toujours en premier. MAIS surtout un mot de passe administrateur pour accéder à son BIOS. Cela rajouterait une couche de protection face à une tentative d'intrusion par le bios. (Pour cela il faut accéder au bios puis dans sécurité, ajouter un mot de passe administrateur.) A tester sur une machine (J'ai pu expérimenter ça dans le cadre de mon alternance.)

Deuxièmement, BitLocker ; Activer et mettre en place BitLocker afin de chiffrer les données de son disque. Pour cela on va faire Windows + R, taper control, aller dans système et sécurité et chiffrement de lecteur BitLocker puis activer BitLocker. (Une clé de récupération sera fournie et un mot de passe unique demandé également.) Cela va permettre qu'avant chaque démarrage de Windows, un mot de passe supplémentaire sera demandé et les données du disque seront chiffrés. (J'ai pu également expérimenter cela avec mon entreprise.)

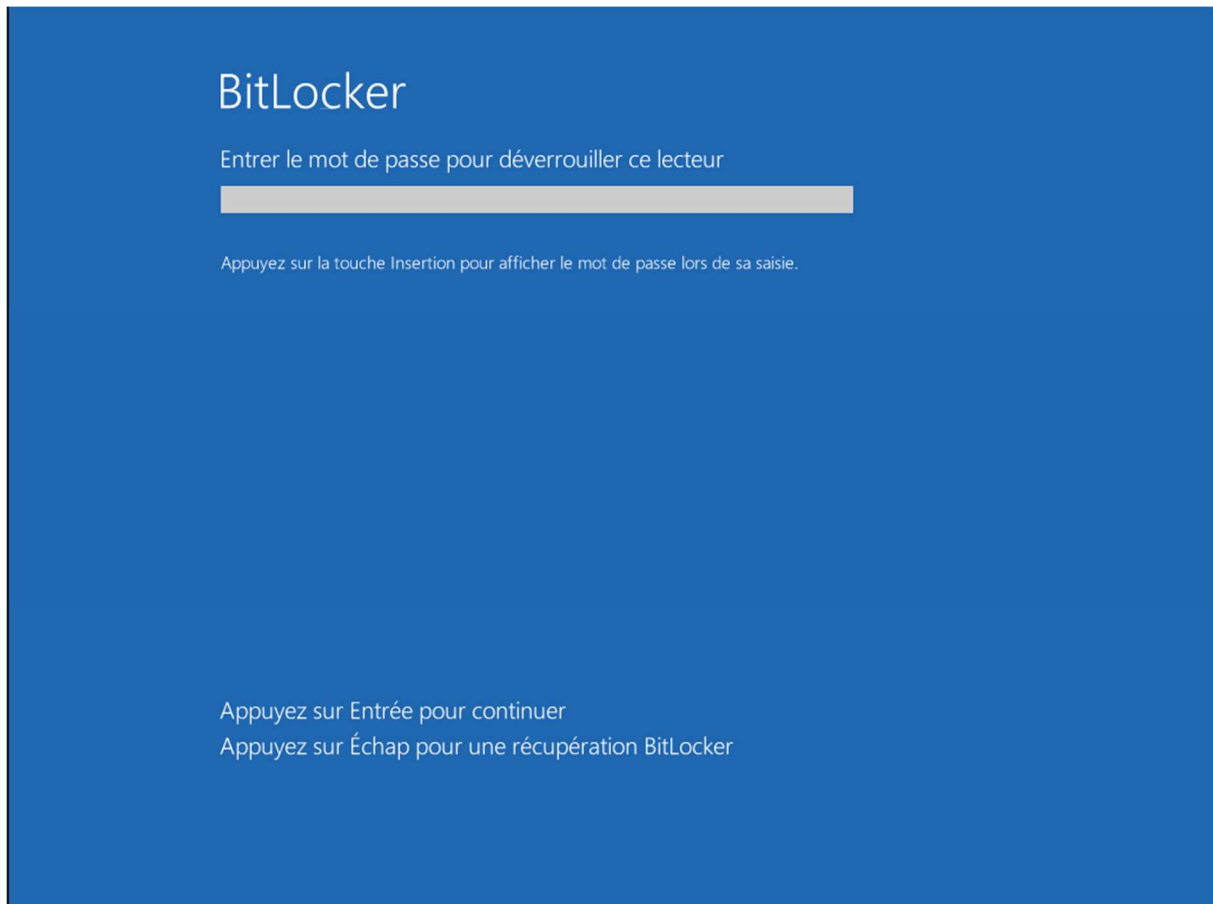
Procédure BitLocker







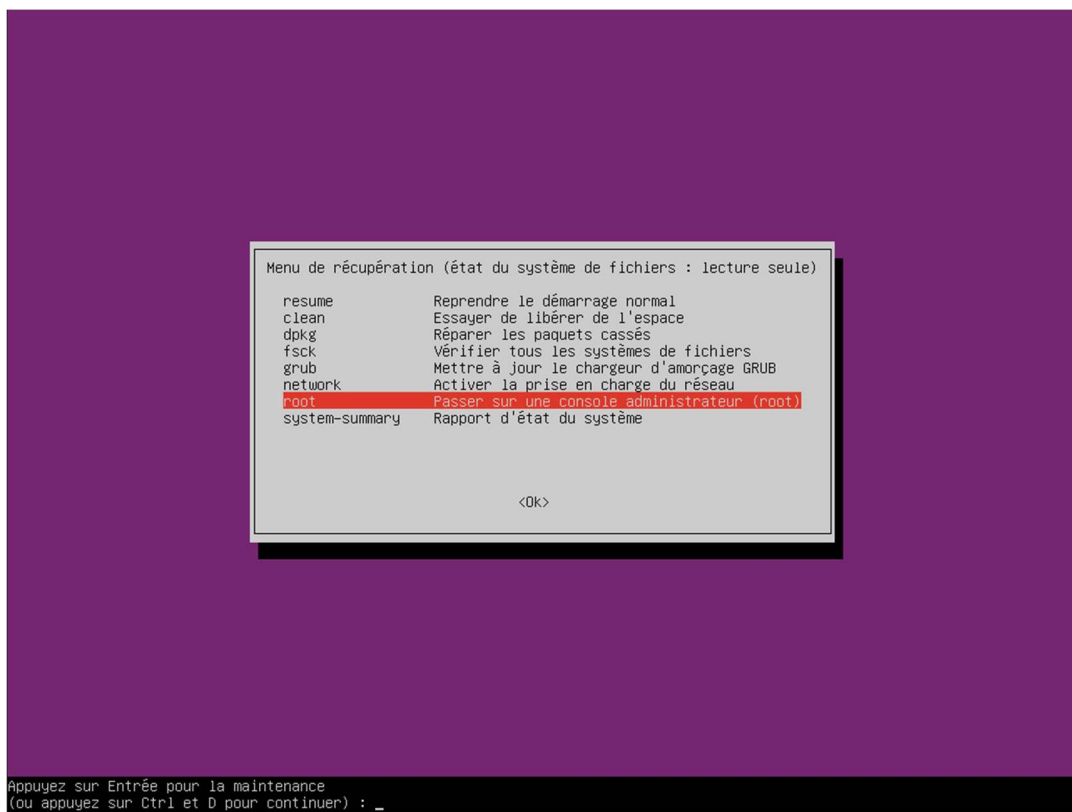
Une fois redémarré, notre mot de passe sera alors demandé.

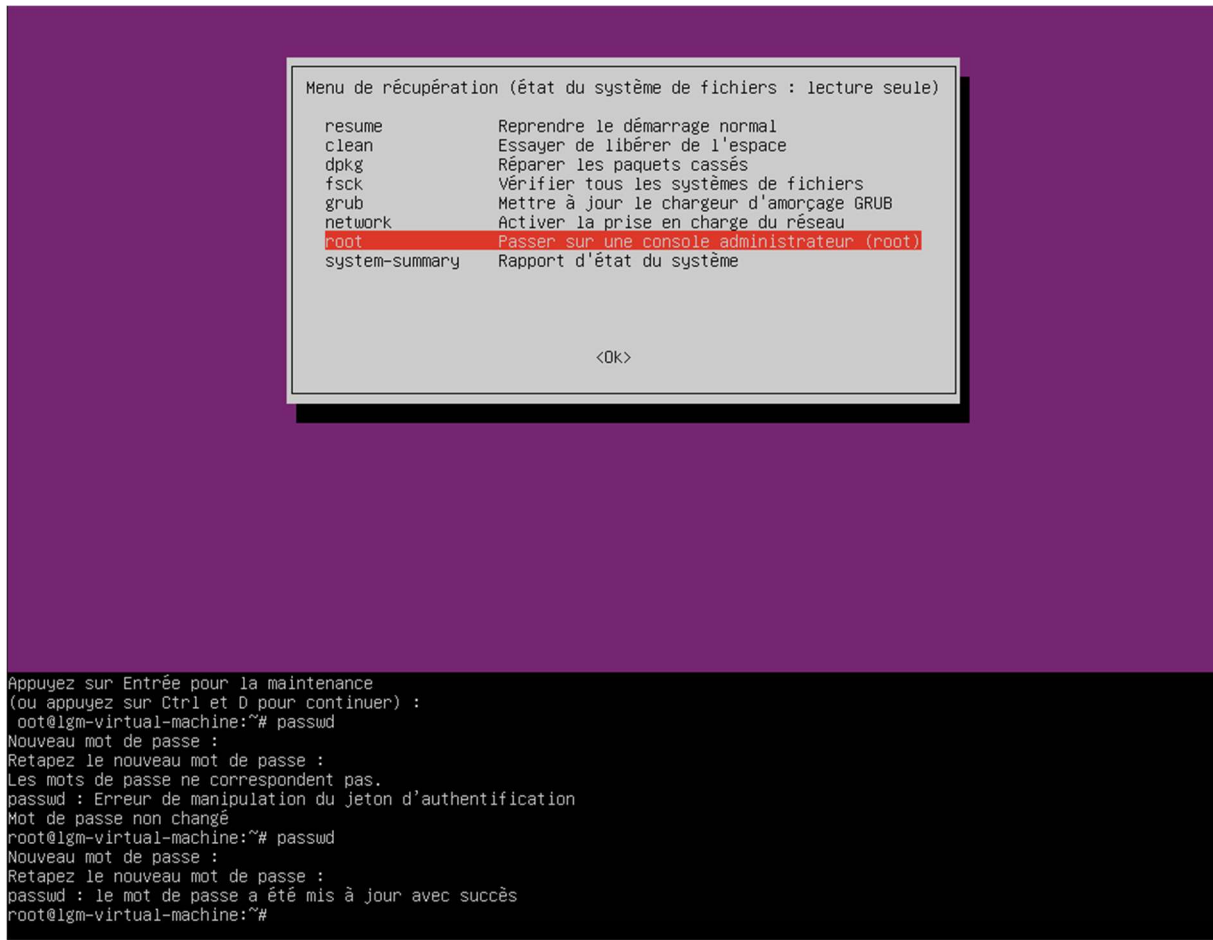


Essai avec une distribution Linux

J'ai installé un Ubuntu 20 sur une machine virtuelle avec VMWare. Effectivement le problème est bien présent aussi avec une version linux en accédant directement au Grub (mode avancé de Linux) nous pouvons changer le mot de passe d'un utilisateur. Voici comment y procéder ;

```
Ubuntu, avec Linux 5.15.0-91-generic
*Ubuntu, avec Linux 5.15.0-91-generic (recovery mode)
Ubuntu, avec Linux 5.11.0-27-generic
Ubuntu, avec Linux 5.11.0-27-generic (recovery mode)
```





The image shows a Linux recovery menu and a terminal session. The menu is titled "Menu de récupération (état du système de fichiers : lecture seule)" and lists several options. The "root" option is highlighted in red. Below the menu, a terminal session shows the user pressing Enter to enter maintenance mode, then using the "root" option to become root. The user then attempts to change the password using "passwd", but the first attempt fails due to a mismatch. The second attempt is successful, and the password is updated.

```
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@lqm-virtual-machine:~# passwd
Nouveau mot de passe :
Retapez le nouveau mot de passe :
Les mots de passe ne correspondent pas.
passwd : Erreur de manipulation du jeton d'authentification
Mot de passe non changé
root@lqm-virtual-machine:~# passwd
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : le mot de passe a été mis à jour avec succès
root@lqm-virtual-machine:~#
```

Et voilà, le mot de passe a bien pu être changé sans s'être connecté sur l'utilisateur.