

TP CYBERSÉCURITÉ : Intrusion simple Windows

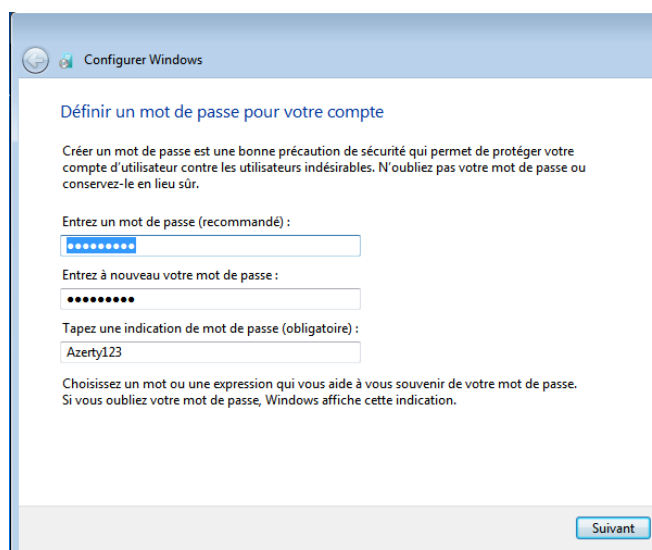
Objectif du TP : découvrir l'intérêt de sécuriser correctement une machine sous Windows et savoir se protéger en se mettant à la place de l'attaquant.

1) Pour la création d'une machine virtuelle sous Windows 7 Pro

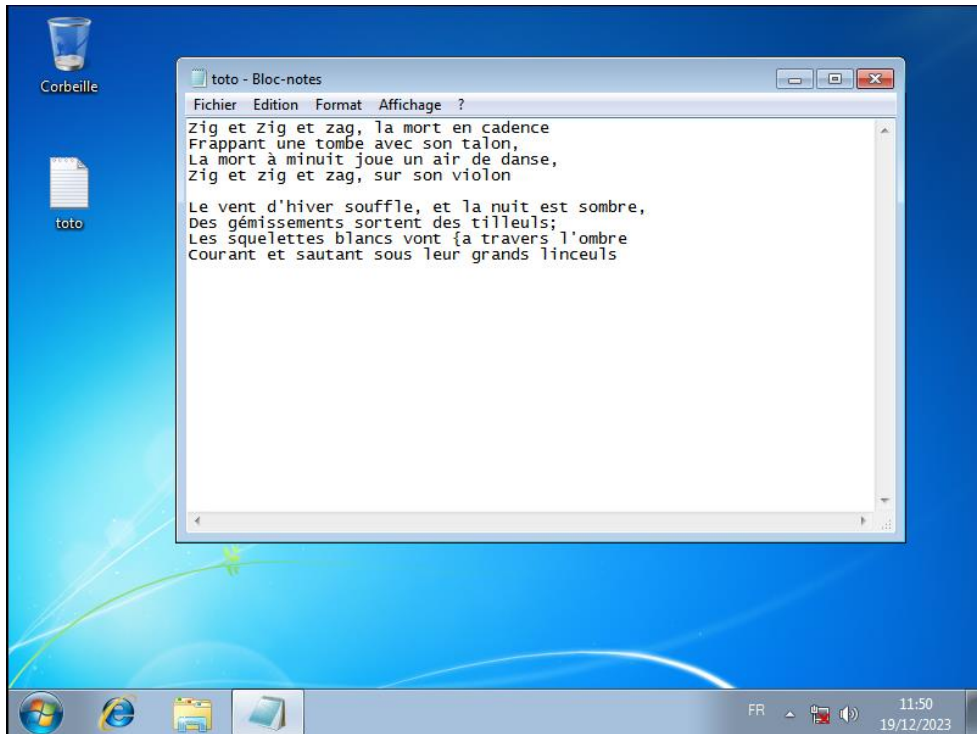
Dans un premier temps j'ouvre VM Ware,
Je crée une nouvelle machine virtuelle avec le minimum de spécificité.
J'utilise l'ISO de Windows 7 du lecteur réseau de MEWO \\10.10.0.5



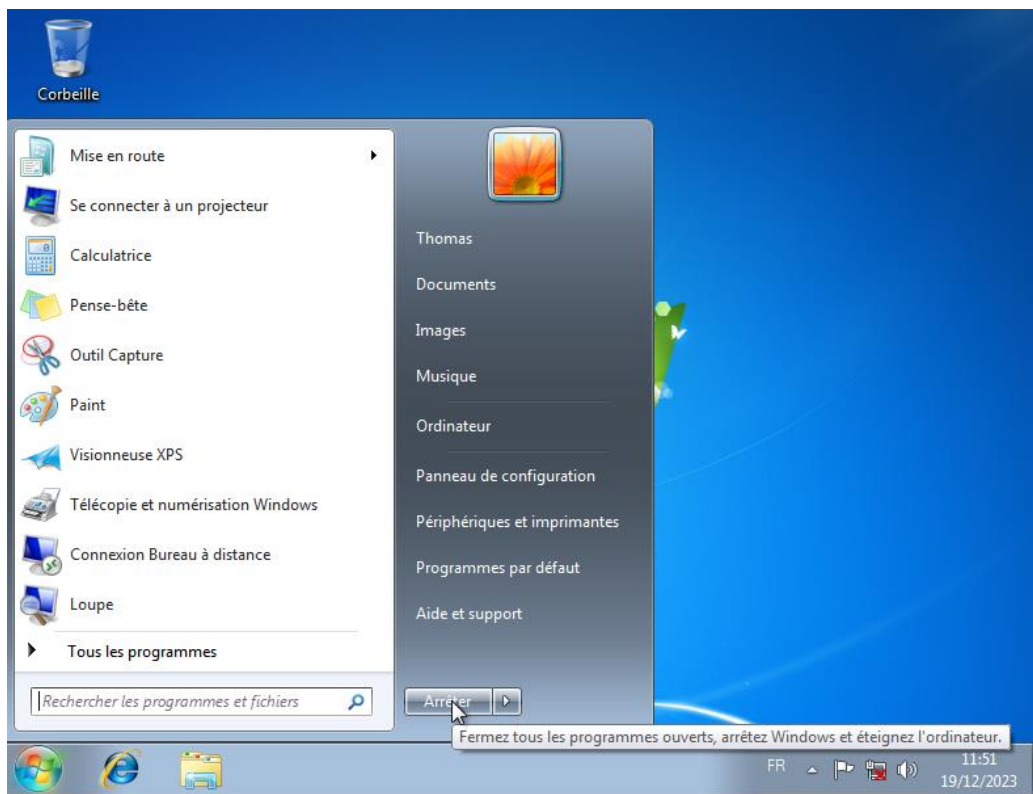
J'installe Windows 7
Ensuite je rentre un mot de passe



Une fois Windows 7 démarré, je crée un fichier txt avec les paroles d'une musique



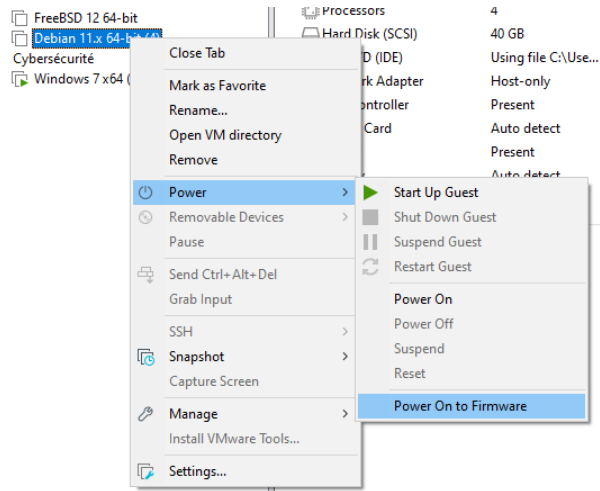
J'arrête la VM



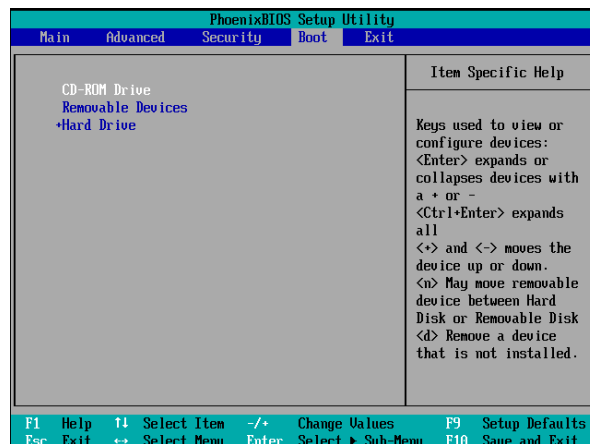
2) Booter sa VM Windows 7 avec Ubuntu

Pour ce faire, dans les paramètres de VMware j'enlève l'ISO de Windows 7 et je place l'ISO d'Ubuntu

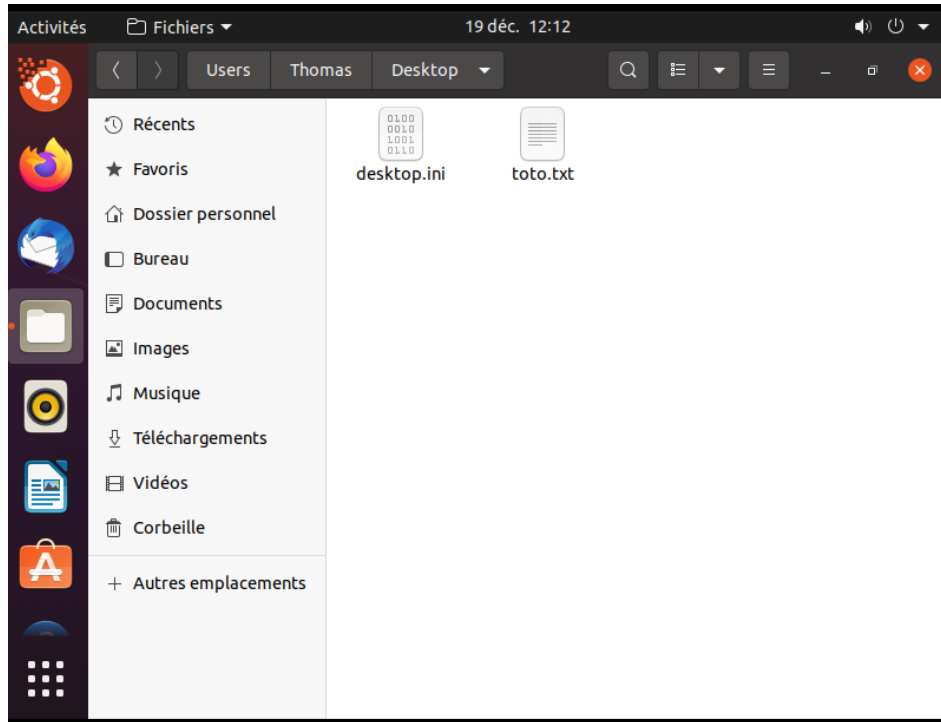
Ensuite je fais clic droit sur la VM, je vais dans Power puis power On to Firmware pour démarrer sur le BIOS.



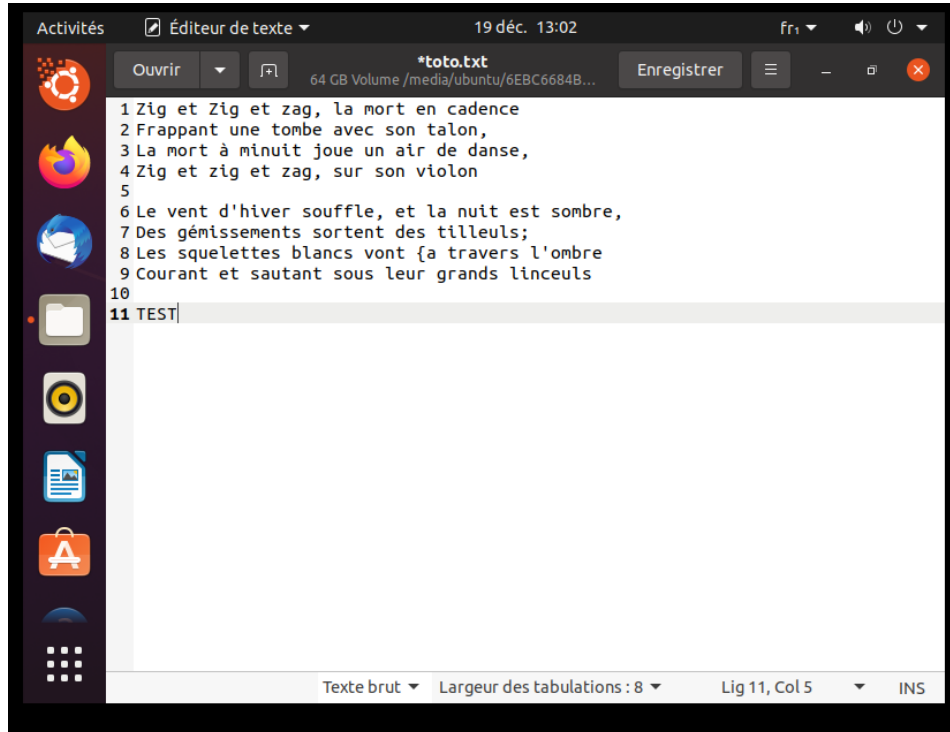
Sur le BIOS je change l'ordre de BOOT en plaçant le DVD/CD disque en premier



Une fois ubuntu démarré, je vais dans fichier puis dans Volume de 64 GB / User / Thomas et enfin Desktop



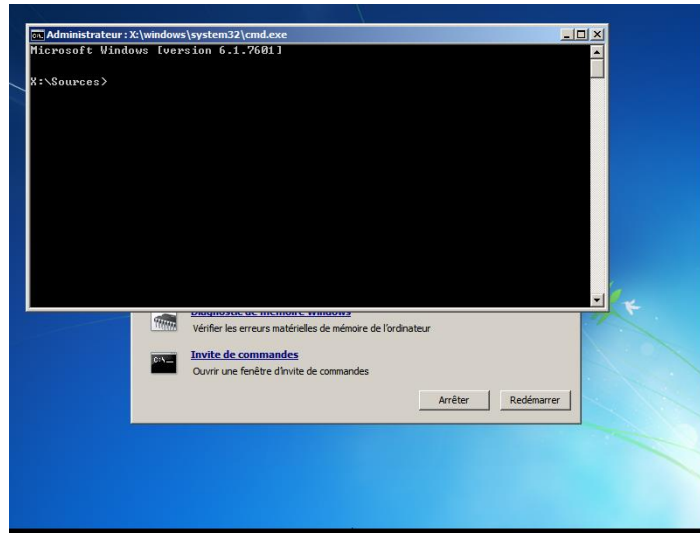
Oui je peux lire et modifier le fichier txt



3) Expérimentation de la [Méthode n°2b : via l'Environnement de récupération Windows](#)

En suivant le tutoriel du site « [Réinitialiser le mot de passe d'un compte utilisateur sur Windows – Le Crabe Info](#) »

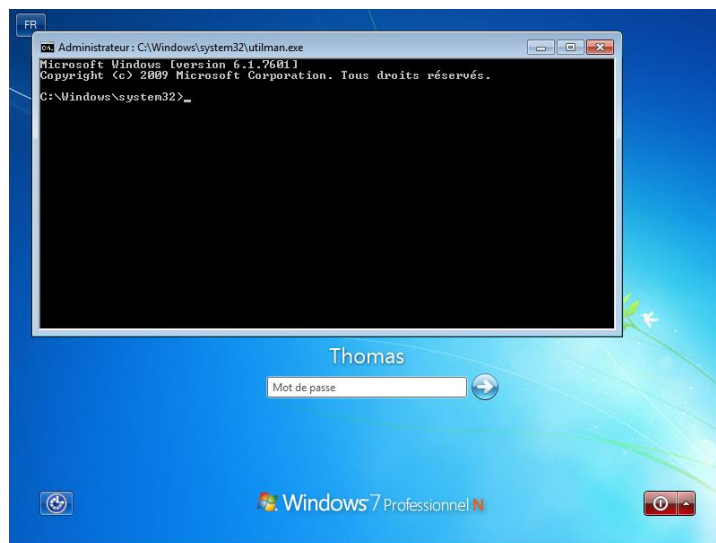
Je démarre ma VM en mode démarrage avancée en appuyant sur F8 puis je clique sur invite de commande



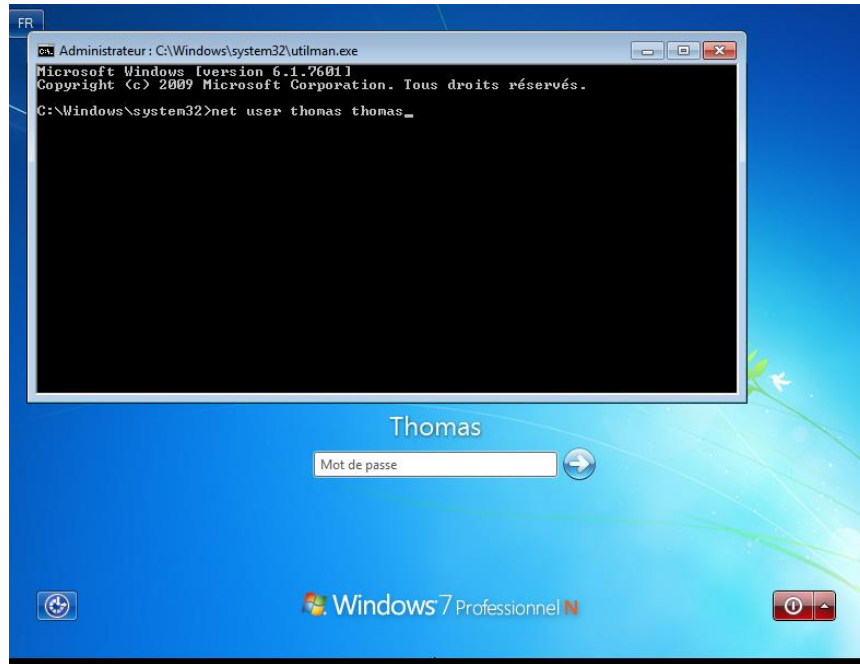
Dans l'invite de commande je tape

- D : pour aller sur le disque D
- dir pour vérifier que c'est bien le lecteur de windows
- cd Windows\system32 pour me déplacer dans le fichier system32
- copy Utilman.exe Utilman.exe.bak
- copy cmd.exe Utilman.exe

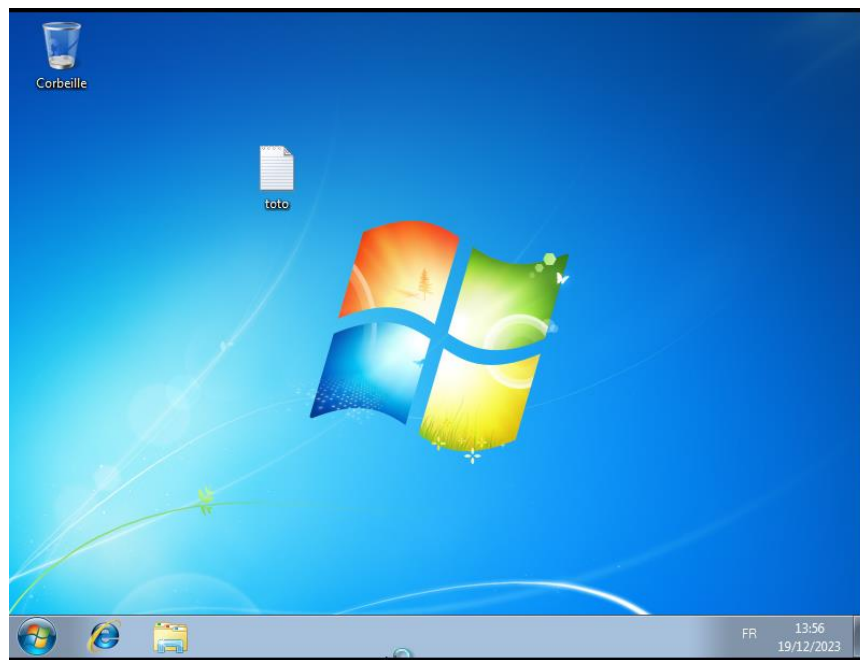
Je redémarre le pc et effectue la combinaison Windows + U pour ouvrir les options d'ergonomie mais grâce à l'intervention ci-dessus c'est cmd qui s'ouvre



J'exécute ensuite la commande
net user "nom_compte_utilisateur" nouveau_mot_de_passe



Avec le nouveau mot de passe thomas je peux accéder au bureau

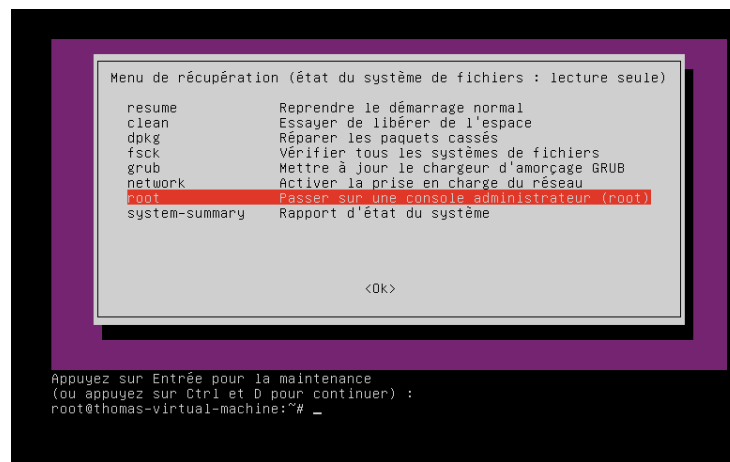


La méthode utilisée dans la vidéo ressemble beaucoup à la Méthode n°2b : via l'Environnement de récupération Windows
Car le personnage lance l'outil Operating system pour ensuite changer cmd avec sethc pour que cmd s'ouvre à la place de celle-ci pour ensuite faire netuser et changer le mot de passe

4) Enfin

- Conclusion et méthode de protection : La plupart des utilisateurs ne se satisfont que d'un mot de passe pour protéger leur pc, mais on la bien vu grâce à ce TP, qu'un mot de passe seul est une méthode de protection trop faible pour sécuriser ses données.
Il existe plusieurs méthodes pour protéger ses données.
Crypter les données de son disque dur (cf : image ci-dessous)
Utiliser une authentification à deux facteurs ou un compte Microsoft connecté
Ou encore directement protégé son BIOS avec un mot de passe
- Pensez-vous qu'on a le même souci sur Mac ou Linux ?
Je pense que tout comme Windows, Linux a aussi ses vulnérabilités et pour ce faire je vais tester le tutoriel ci-dessous
- Je crée une VM sur Linux (Ubuntu) je configure un mot de passe
Puis je suis le tutoriel de [J'ai oublié mon mot de passe ! \(ubuntu-fr.org\)](http://ubuntu-fr.org)

Je redémarre Ubuntu en maintenant la touche Maj pour accéder au menu de récupération
Je lance root

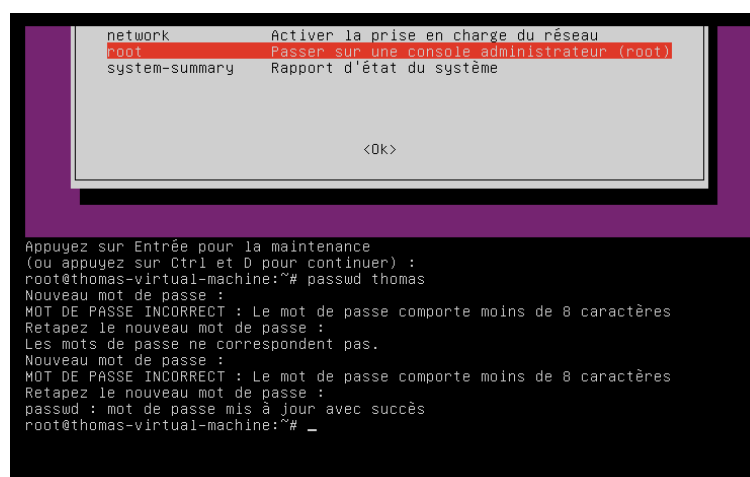


```
Menu de récupération (état du système de fichiers : lecture seule)
resume          Reprendre le démarrage normal
clean           Essayer de libérer de l'espace
dpkg            Réparer les paquets cassés
fsck            Vérifier tous les systèmes de fichiers
grub            Mettre à jour le chargeur 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@thomas-virtual-machine:~# _
```

En root je tape la commande passwd thomas
Ensuite je tape un nouveau mot de passe

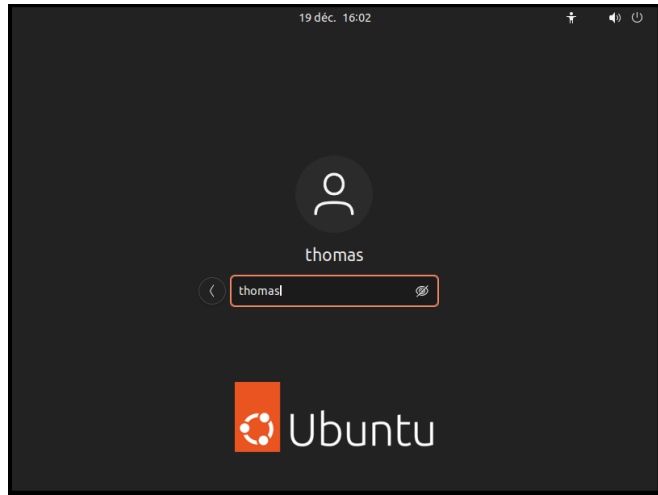


```
network          Activer la prise en charge du réseau
root           Passer sur une console administrateur (root)
system-summary  Rapport d'état du système

<Ok>

Appuyez sur Entrée pour la maintenance
(ou appuyez sur Ctrl et D pour continuer) :
root@thomas-virtual-machine:~# passwd thomas
Nouveau mot de passe :
MOT DE PASSE INCORRECT : Le mot de passe comporte moins de 8 caractères
Retapez le nouveau mot de passe :
Les mots de passe ne correspondent pas.
Nouveau mot de passe :
MOT DE PASSE INCORRECT : Le mot de passe comporte moins de 8 caractères
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
root@thomas-virtual-machine:~# _
```

Je redémarre Ubuntu et dans la case mot de passe, je mets le nouveau de passe crée précédemment



J'arrive bel et bien à rentrer sur le bureau

