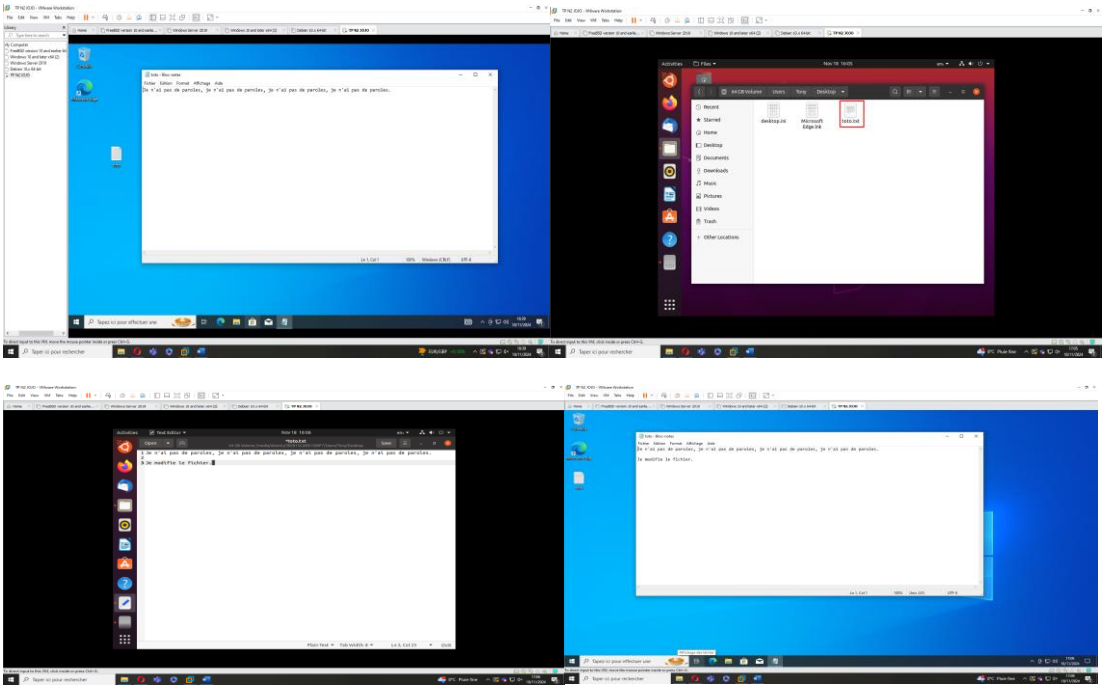
# TP N°2 :  Intrusion simple Windows :

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

*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. Chaque étudiant assume devant la justice ses actes. Ma responsabilité ne pourra être engagée, vous voilà prévenus.*

1/ J'ai créé une machine virtuelle sous W10 ainsi qu'une session « Tony » avec un mot de passe, sur le bureau de cette session j'ai créé un fichier .txt (toto) avec une phrase dedans.

Ensuite j'ai booté ma VM sur un nouvel ISO « Ubuntu » via le mode CD-ROM, j'ai donc essayé de retrouver mon fichier .txt (toto) sur Ubuntu, ainsi que de le modifier.



Effectivement je peux retrouver mon fichier .txt via le chemin :

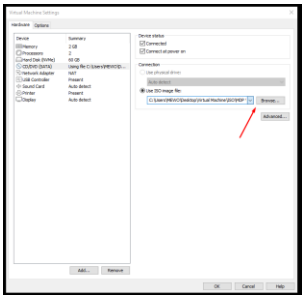
« Other Locations -> 64GB Volume -> Users -> Tony -> Desktop -> toto.txt »

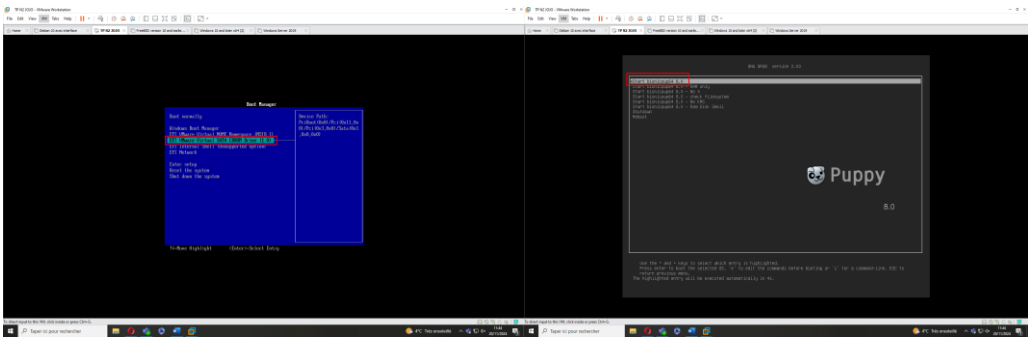
Je peux aussi constater que si je modifie mon fichier depuis Ubuntu et que je l'enregistre, si je suis capable de le retrouver modifié sur ma session Windows.

2/ Sur le site : https://lecrabeinfo.net/reinitialiser-mot-de-passe-compte-utilisateur-local-windows.html je peux choisir une méthode pour m'aider en cas d'oublie de mon mot de passe, je choisis donc la méthode n°2a via Puppy Linux.

Je télécharge donc un ISO Puppy Linux, j'éteins ma VM et je change mon ISO dans les settings. Pour pouvoir démarrer sur Puppy Linux suivez ces méthodes :

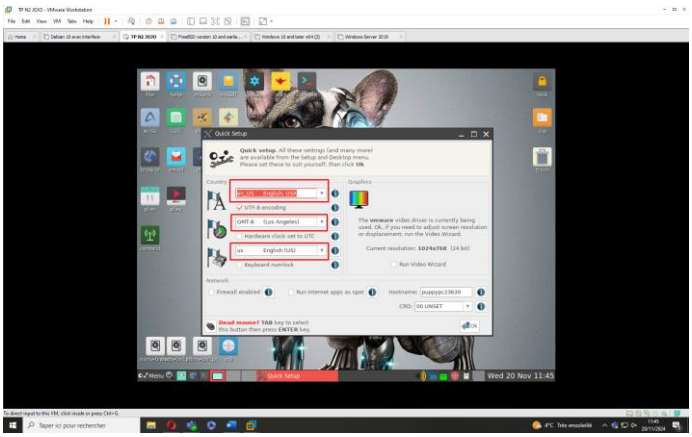
- Démarrez la VM et appuyez sur F9 pour accéder au BOOT menu
- Sélectionnez **Find /grub.cfg** puis **Start bionicpup64**.





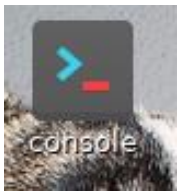

Une fois Puppy Linux démarrer, une page « Quick Setup » s'ouvre, il faut changer alors ouvrir les 3 volets concernant la langue / l'heure / disposition clavier et les configuré en Français / Europe -Paris / fr Français.

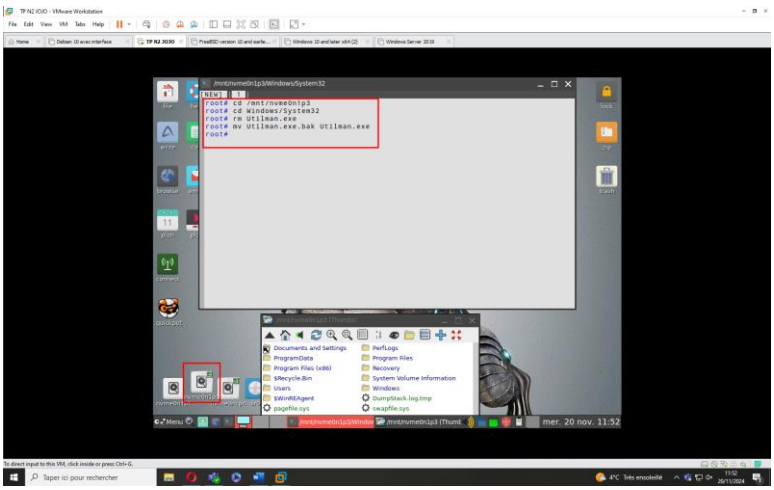
Appliquez les paramètres modifier en cliquant sur OK, puis RESTART pour restart la machine.



Une fois la VM redémarrer sur Linux Puppy, il y a 3 dossiers en bas à gauche, suivez ces étapes :

- Ouvrez-les et trouvez ou est installer Windows
- Une fois le nom repérer, ouvrez un terminal de commande (Console sur le bureau)
- Tapez les commandes ci-dessous une à une, ces commandes permettent de remplacer **Utilman.exe** par **cmd.exe**

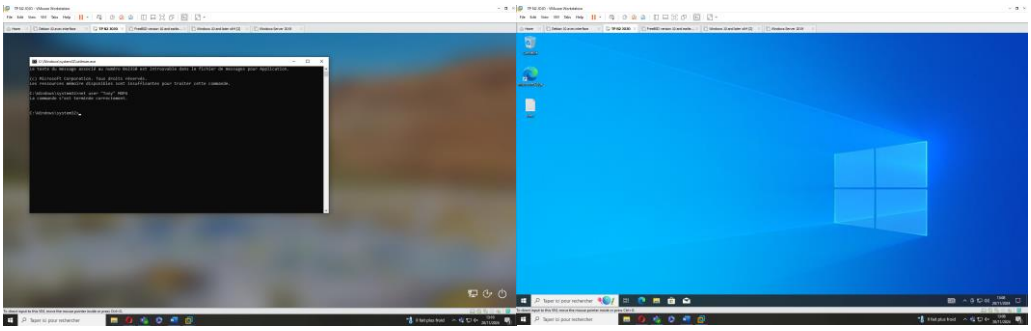



Vous pouvez maintenant redémarrer votre VM normalement (sur votre Windows10).

Une fois arriver sur l'écran de déverrouillage, au lieu d'entrer votre mot de passe, faites le raccourci **Windows + U,** ce qui va ouvrir votre terminal de commande, en suite taper la commande **« user "Votre_Utilisateur" nouveau_mdp »**.

Bravo vous venez de récupérez votre session Windows, vous pouvez fermer votre CMD et écrire votre nouveau mot de passe afin d'accéder à votre session.

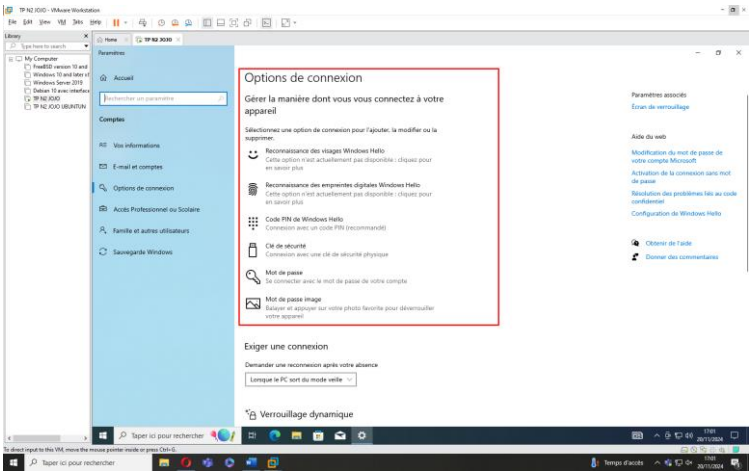


3/ En suivant ces procédures, j'ai pu constater qu'il est très facile d'accéder à une session Windows non protégée, il suffit d'avoir une clef USB préparer à l'avance avec un logiciel disponible gratuitement en ligne et d'avoir connaissance de quelques commandes seulement.

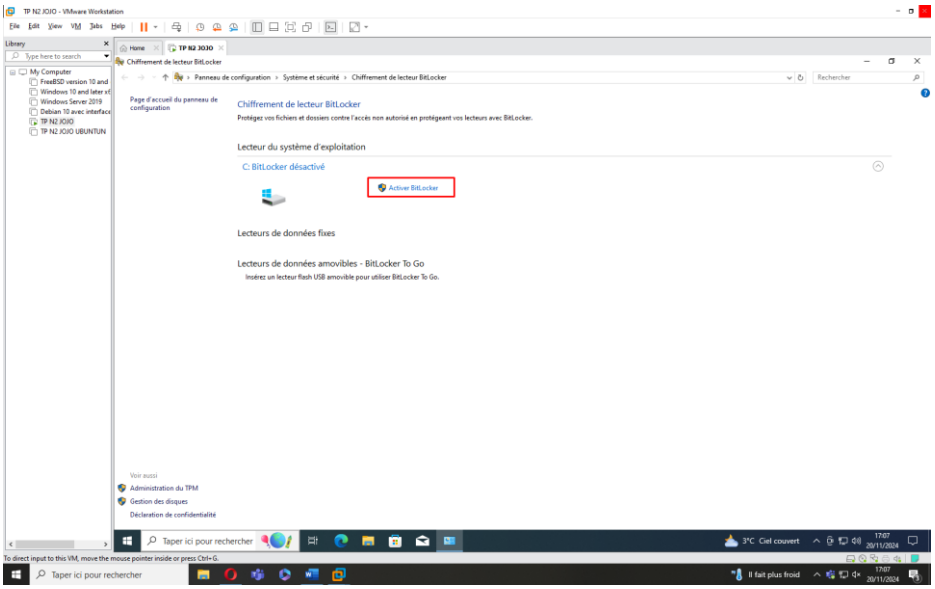
Afin de protéger notre session Windows il existe plusieurs moyens différents :

- Chiffrement BitLocker
- Authentification à 2 facteurs
- Protégé physiquement vos machines, (ne pas laisser trainer son PC portable)

A/ Pour **l'authentification à 2 facteurs**, il suffit d'aller dans **Options de connexion** et de choisir une méthode puis **la configuré**, cela fera un mot de passe supplémentaire lié à votre compte Microsoft pour un peu plus sécurisé votre session Windows.



B/ Concernant la méthode **BitLocker**, il suffit de rechercher **Gérer BitLocker** dans la barre de recherche et de l'activer, attention à bien sauvegarder vos clefs BitLocker afin de pouvoir récupérer vos données en cas de chiffrement BitLocker.

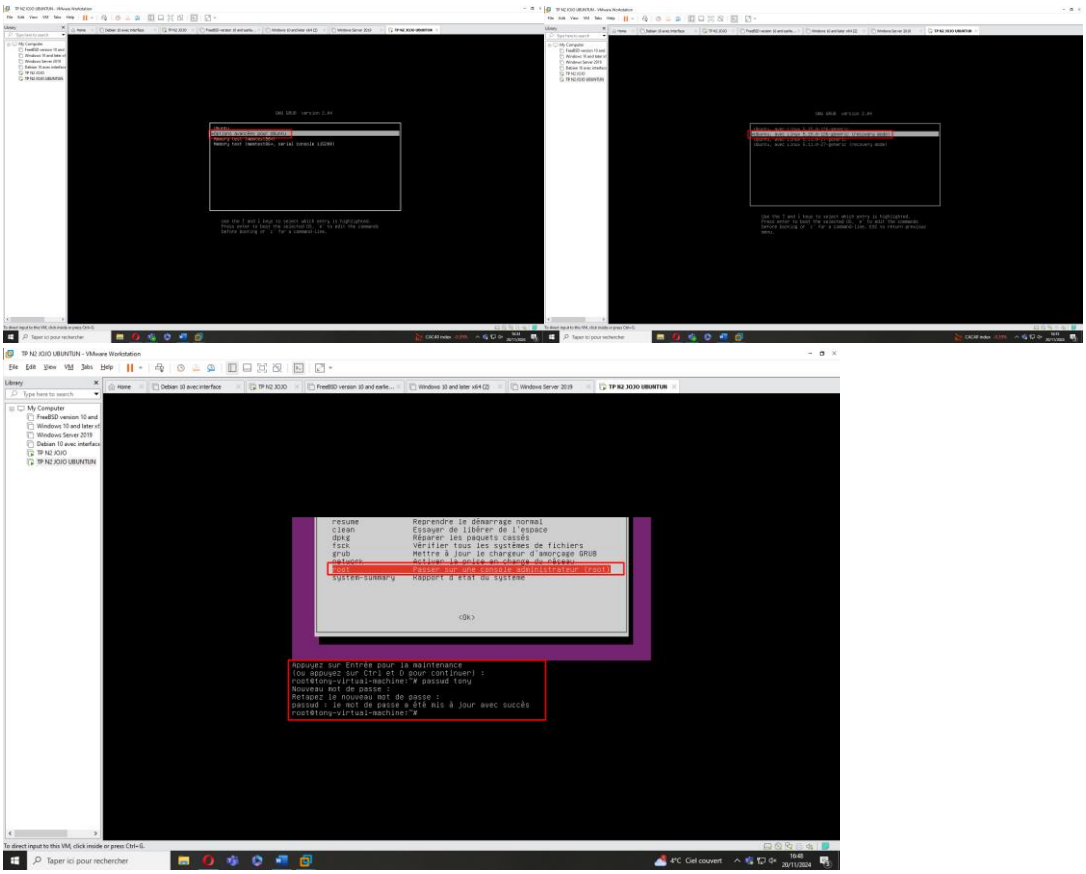



4/ Maintenant nous allons essayer de « récupérer » notre mot de passe sur une VM Linux, pour comparer avec notre méthode pour Windows.

J'ai donc installé une VM Ubuntu, je l'ai configuré avec un utilisateur et mot de passe de session.

Pour récupérer son mot de passe sur Linux Ubuntu il faut :

- Premièrement éteindre sa VM, puis la redémarrer en restant appuyer sur la **touche MAJ**
- Sélectionnez « **Options avancées pour Ubuntu** »
- Puis la version **d'Ubuntu suivis de (Recovery Mode)**
- Avec la flèche du bas sélectionnez « **root** », faites entrer, puis écrivez la commande **passwd VOTRE_NOM_DE_SESSION**
- Vous pouvez maintenant changer votre mot de passe et redémarrer votre session, **finito pipo.**




Pour conclure, nous pouvons constater qu'il est encore plus facile de changer son mot de passe sur Linux Ubuntun que Windows, ce n'est vraiment pas bien sécurisé.

DISCLAIMER 2 : Si vous n'avez pas lu le premier disclaimer, lisez le sinon relisez le ! ☺