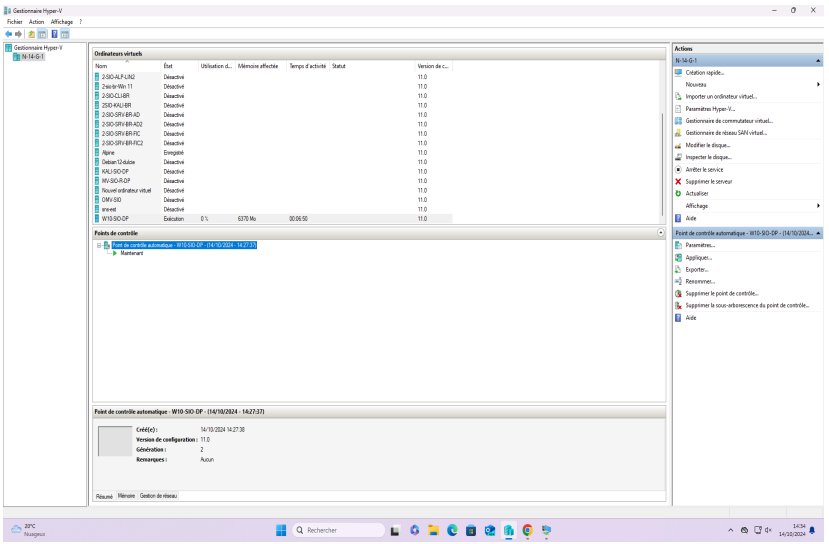
TP2 Intrusion

1) Est-il possible de lire le fichier ?

Oui, en mode Live, il est possible de lire des fichiers présents sur une partition Windows. Une fois la partition montée, Linux permet d'accéder aux fichiers NTFS. On peut ouvrir le fichier .txt en utilisant un éditeur de texte tel que Gedit ou Nano pour en lire le contenu.



2) Est-il possible de modifier le fichier ?

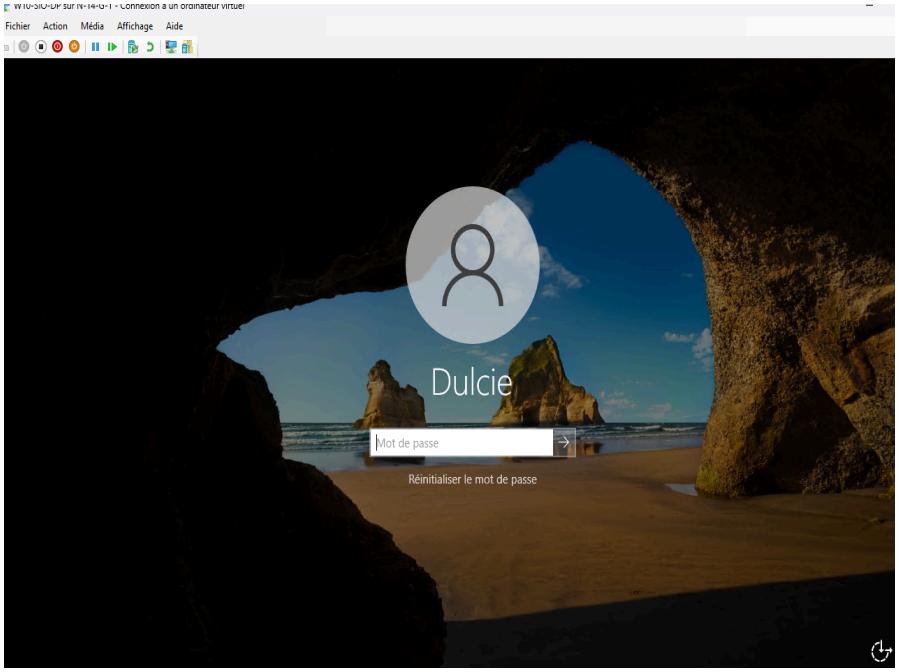
Oui, mais seulement si la partition Windows est en mode lecture-écriture. Si elle est en lecture seule, on ne pourra pas modifier le fichier.

3) Quelle méthode se rapproche le plus de la première étape de la vidéo évoquée en introduction (la 1ère minute)

La méthode qui se rapproche le plus de la première étape de la vidéo est IT Connect, car il explique comment remplacer l'outil d'accessibilité par l'invite de commandes pour changer le mot de passe.

4) Tirez une conclusions sur ce que vous venez de découvrir

J'ai appris que réinitialiser un mot de passe sur Windows peut être simple avec des méthodes comme l'invite de commandes. Cela montre qu'un accès physique permet de contourner des restrictions, ce qui souligne l'importance de sécuriser à la fois les appareils et les mots de passe. Il est essentiel d'être vigilant pour éviter les failles de sécurité liées à l'accès non autorisé.



5) Déterminez 2 manières de se protéger de ce problème et expérimentez les dans votre VM

Pour se protéger contre la réinitialisation non autorisée du mot de passe sur Windows, voici deux méthodes :

- Utiliser un mot de passe fort Choisir un mot de passe complexe qui combine lettres, chiffres et symboles.
- Activer la vérification en deux étapes: Cela nécessite une confirmation supplémentaire, comme un code envoyé par SMS, lors de la connexion.

Dans ma VM, je peux mettre en place ces mesures pour améliorer la sécurité de mes comptes.

6) Pensez vous avoir le même souci sur Linux ? Testez sur votre VM Linux et reprenez le fil de ce TP

Pour tester cela sur ma VM Linux, je vais essayer de démarrer en mode de récupération et voir si je peux réinitialiser le mot de passe d'un utilisateur. Cela me permettra de vérifier si je rencontre le même souci qu'avec Windows.