TP B3 : Identifer les menaces

Hego Maxence

Audit sur mot de passe :

Au cours de cette présentation nous allons voir l'importance d'utiliser un mot de passe fort pour vos sessions.

Voici un rappel sur les bonnes pratiques a adopté pour votre mot de passe :

Mot de passe fort : Selon votre préférence, vous pouvez choisir parmi ces trois recommandations de la CNIL pour avoir un mot de passe sécurisé :

- 12 caractères avec majuscules, minuscules, chiffres et caractères spéciaux
- 14 caractères comprenant des majuscules, des minuscules et des chiffres
- Une phrase avec au minimum 7 mots.

Gestionnaire de mots de passe : Plutôt que modifier très légèrement le mot de passe que vous avez retenu, utiliser cet outil peut vous permettre de retenir plusieurs mdp fort. Ex ZeniPass

Authentification à deux facteurs : L'authentification à deux facteurs garanti une meilleure sécurité et est recommandé par la CNIL. Il s'agit le plus souvent d'un code à renseigner que vous avez reçu par mail ou SMS après avoir entré votre mot de passe. Ex : Microsoft Authentificator

Présentation de la formation :

Au cours de cette formation un **hacker éthique ou White hack** va cracker le mot de passe d'une session Windows.

Cette formation est à **caractère éducatif,** elle est réalisée avec l'**accords de la direction et des personnes présentes**.

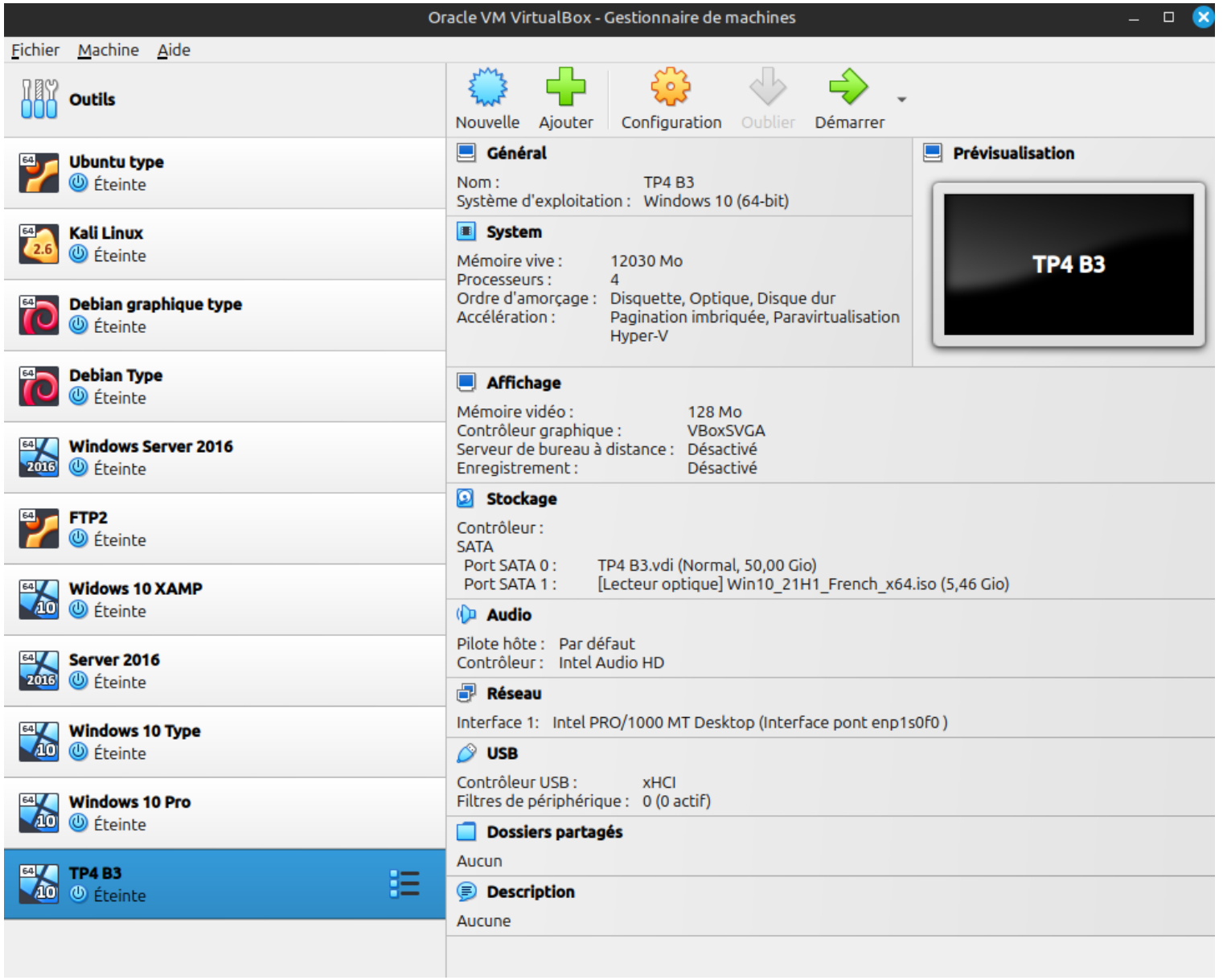
La session Windows que l'on va cracker a été **créé spécialement pour l'occasion sur une VM,** ce n'est pas celle d'un employé.

Cependant, les méthodes présentées lors de cette formation sont les mêmes utilisées par un **black Hat, un hacker malveillant**.

Avertissement : reproduire ces méthodes sans les autorisations nécessaires vous exposent à des risques juridiques.

Création de la VM :

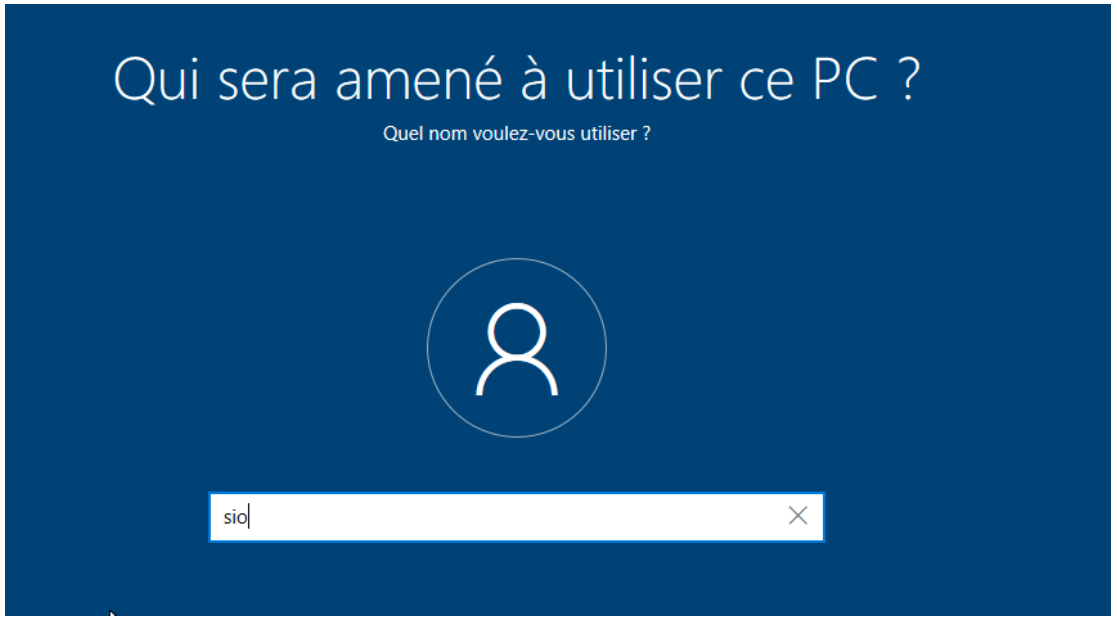
On utilise le logiciel Virtual Box et l'on crée une VM Windows 10 Pro, en accès par pont.

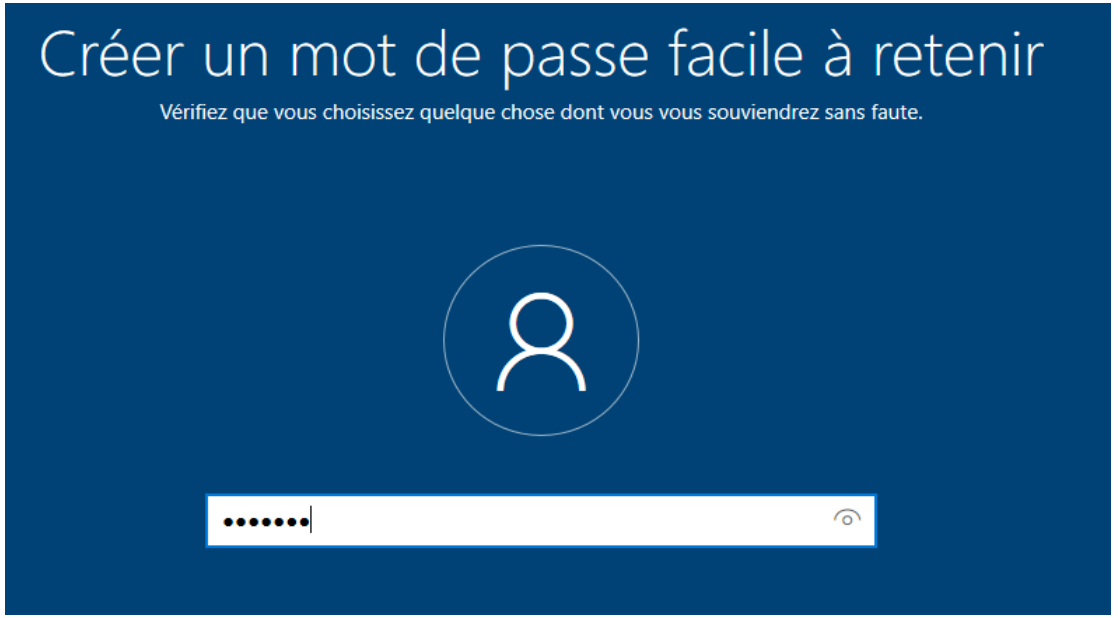


Création du login et mot de passe :

On définit un **login et un mot de passe** pour simuler une session d'un utilisateur.

Dans cette formation on ne cherche que le mot de passe mais un hacker peut également reprouver votre login avec les mêmes méthodes.



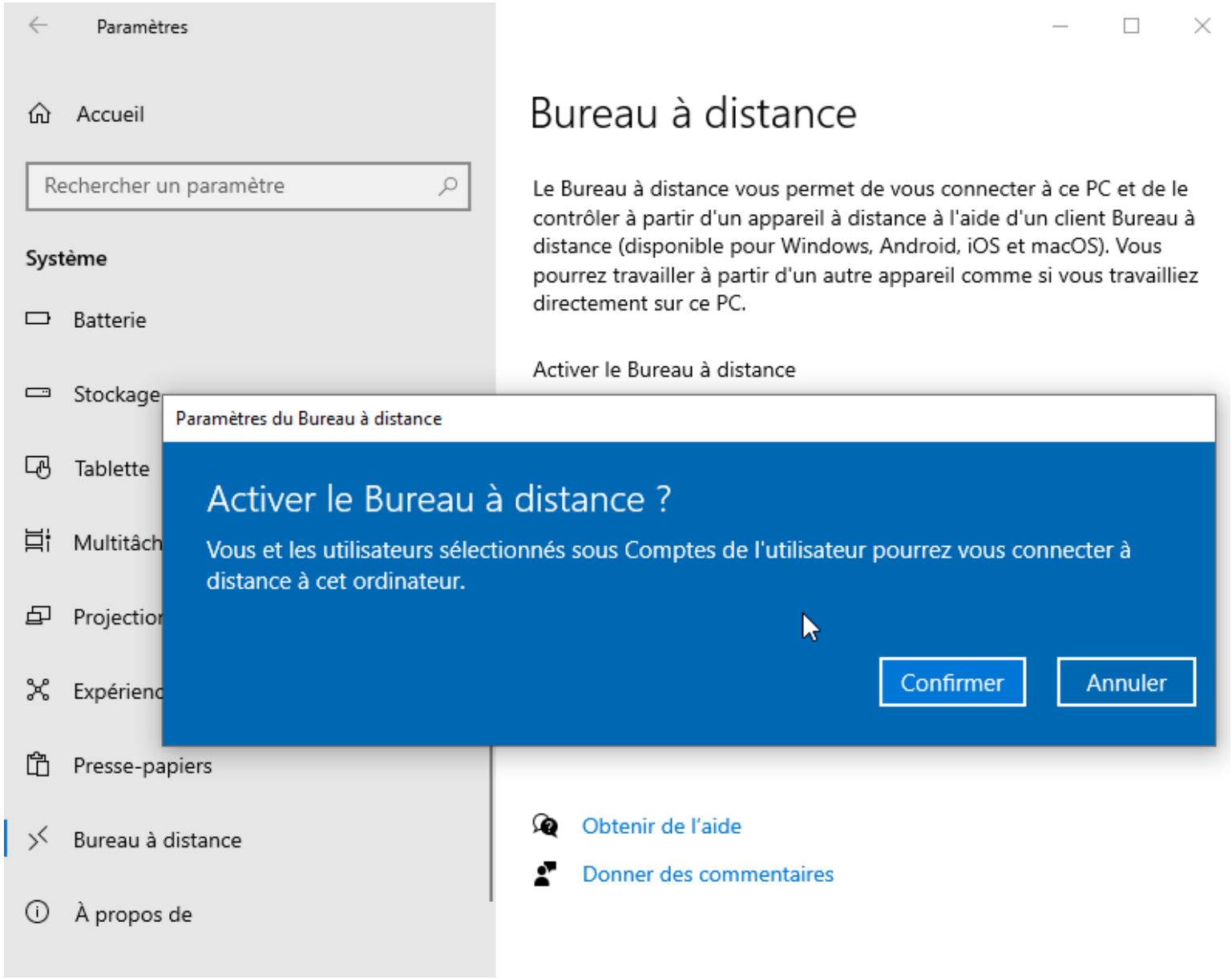


Configuration du bureau à distance :

Pour utiliser le bureau à distance :

- Paramètre
- Système
- Bureau à distance
- Activer le bureau à distance
- Confirmer

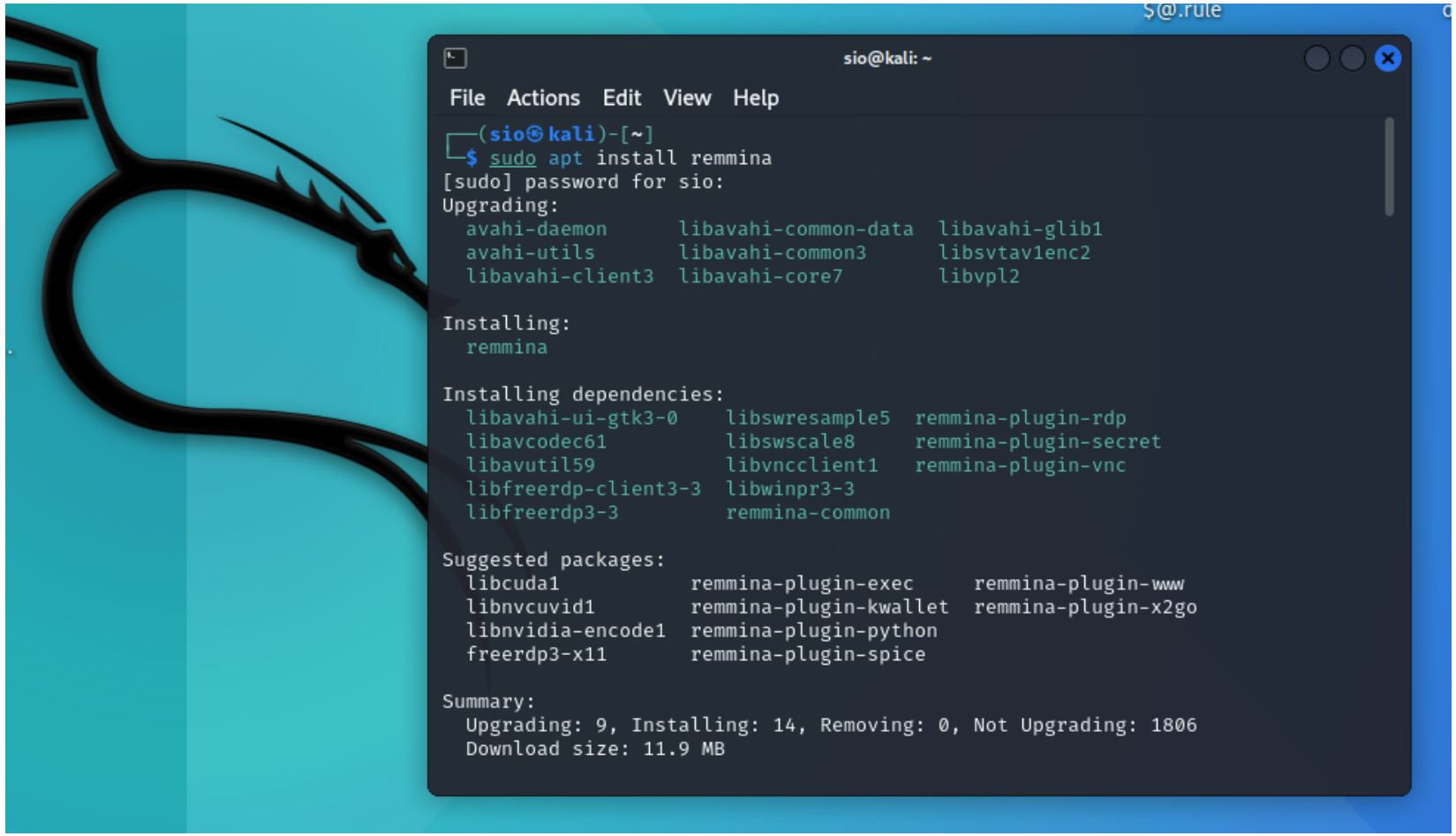
Le bureau à distance est configuré, on va pouvoir se connecter.



Machine de l'assaillant :

Le hacker va utiliser une VM Kali, c'est une distribution Linux spécialisé dans la cybersécurité.

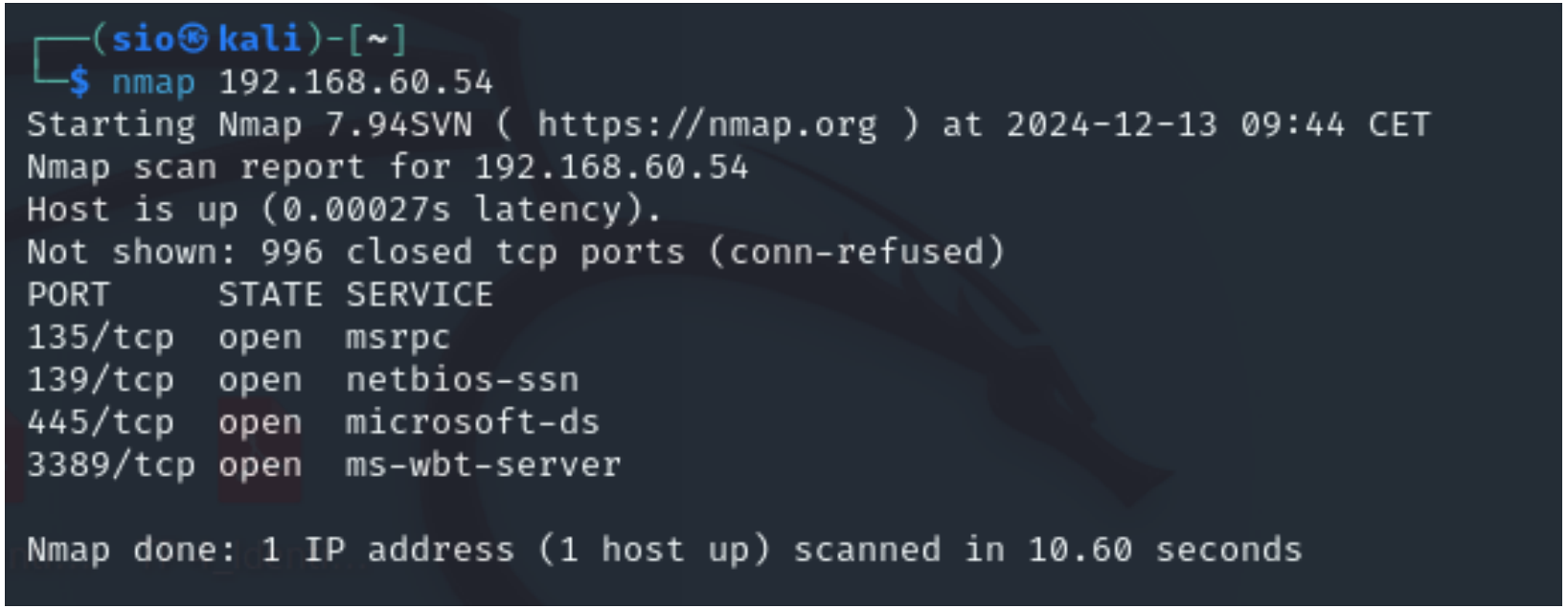
On installe remmina qui permet de se connecter à distance à la VM Windows.



Scan des failles :

On utilise la commande nmap avec l'IP de la VM Windows pour connaître les ports ouverts sur la machine.

Le protocole 3389 pour le RDP (accès au bureau à distance) est bien ouvert.



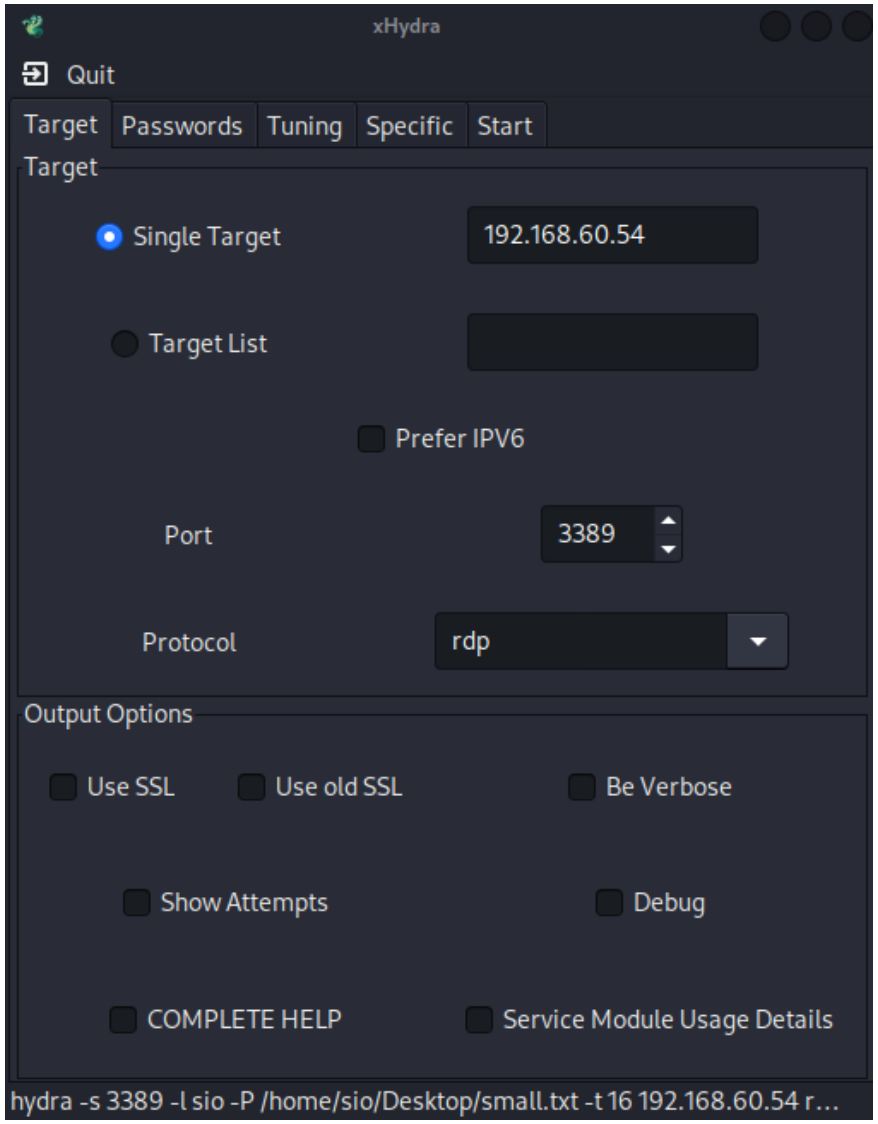
Xhydra :

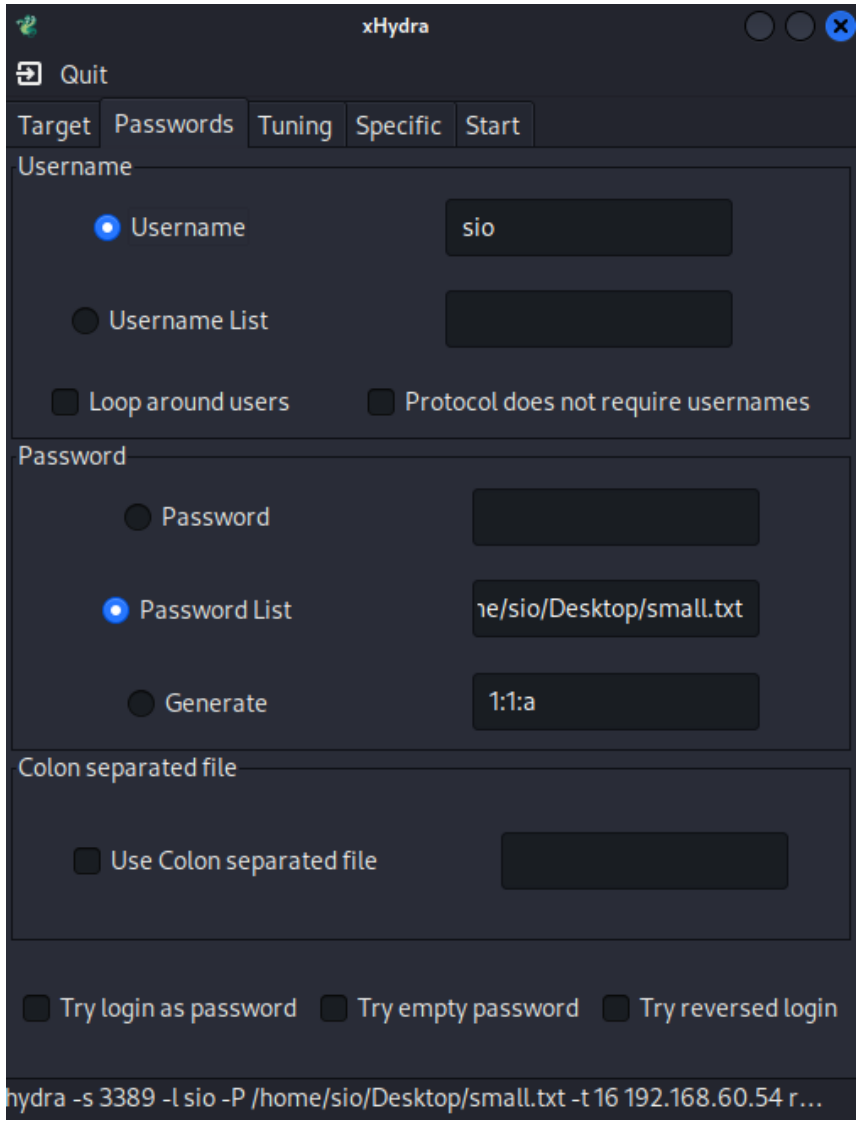
On utilise xhydra pour brute force le mot de passe de la session de l'utilisateur.

On définit l'adresse IP de la VM windows, le protocole (détecté par nmap), le login et le chemin d'une wordlist.

Une wordlist correspond à une liste des mots de passes les plus utilisées.

Une wordlist personnalisé peut être crée par OSINT.



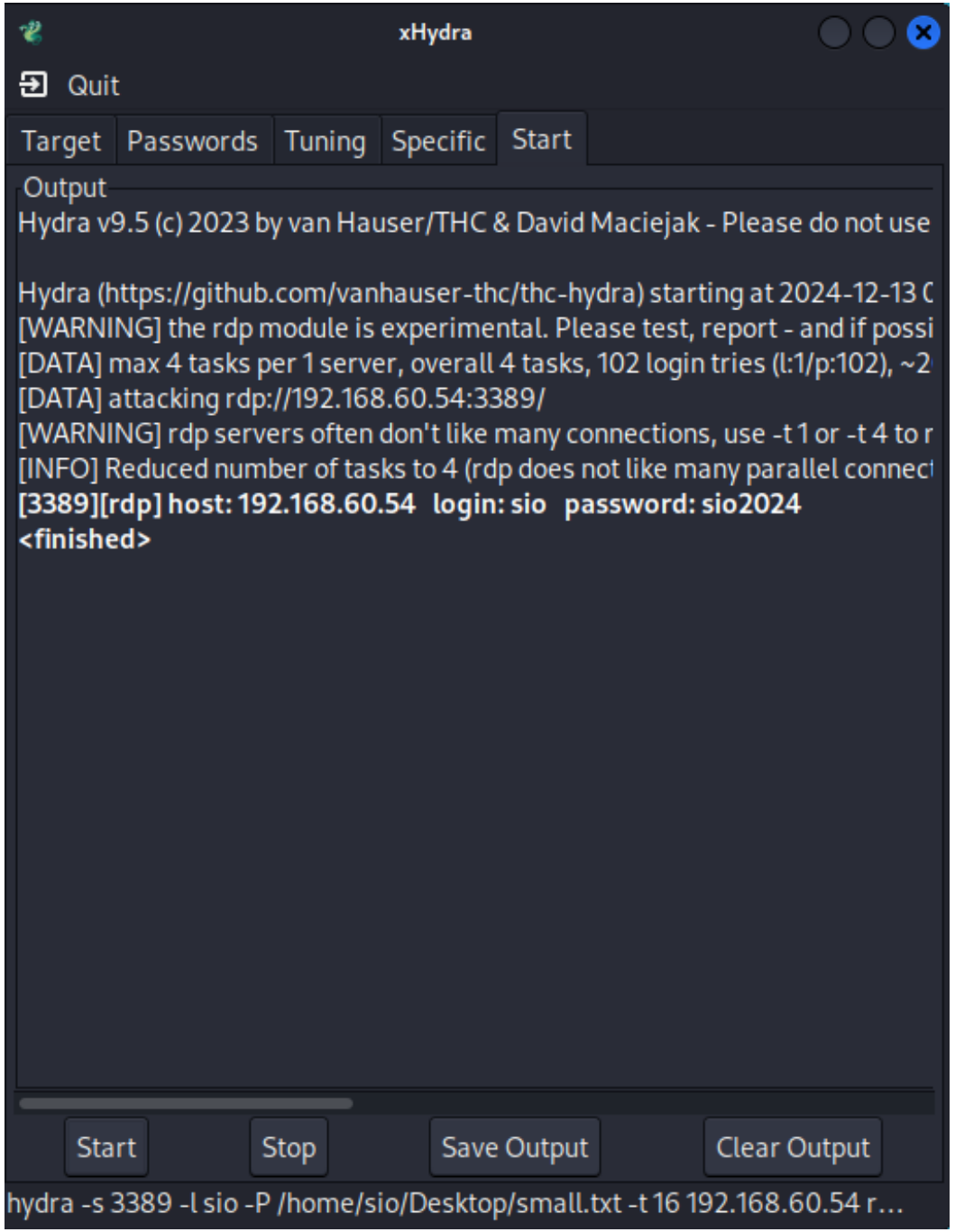


Mot de passe trouvé :

On a trouvé le mot de passe !!!

Ce mot de passe faible a été trouvé en moins de quelques secondes.

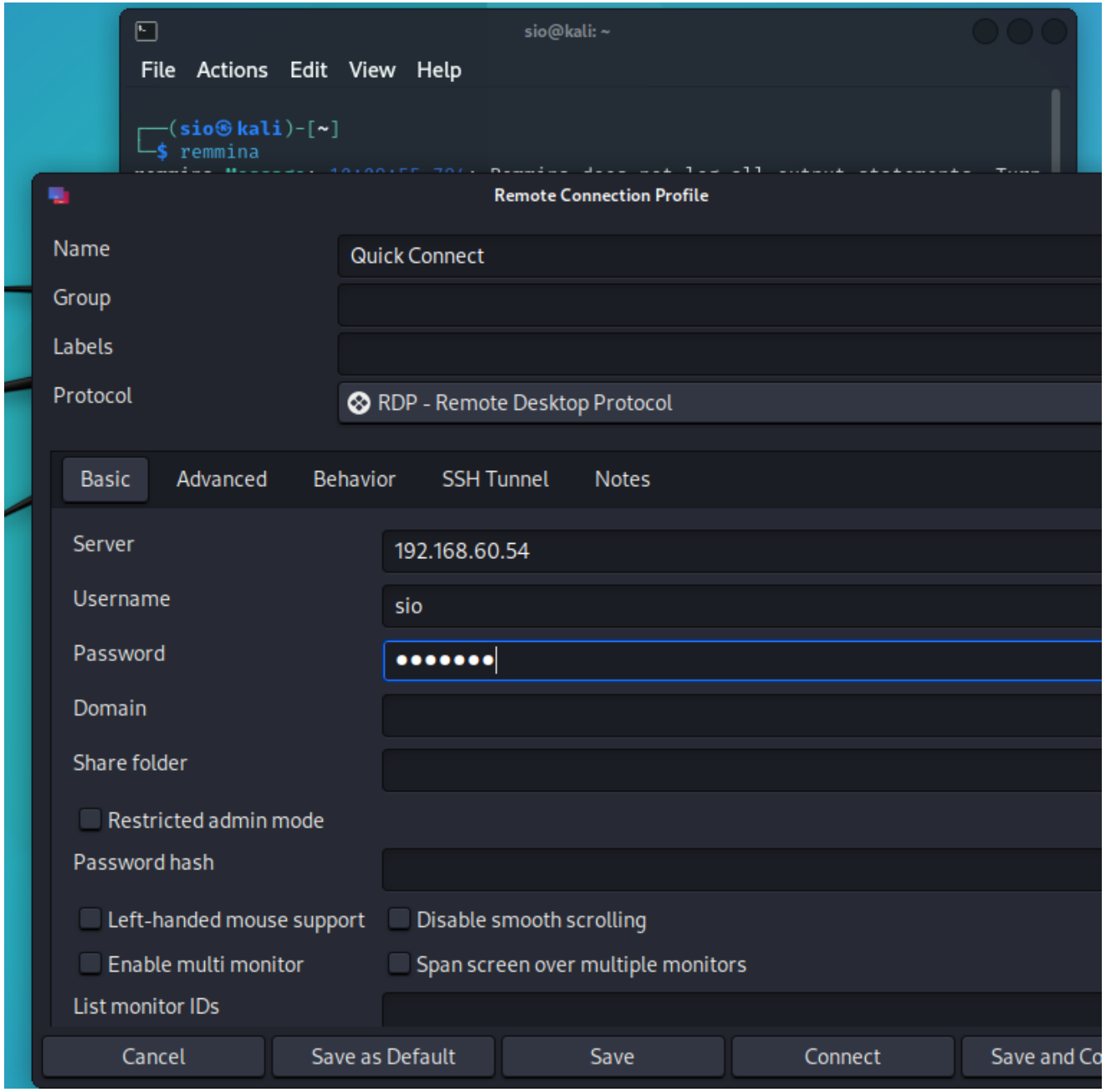
Un mot de passe fort (voir ANSSI) peut prendre plusieurs dizaines d'années avant d'être trouvé.



Connexion à distance :

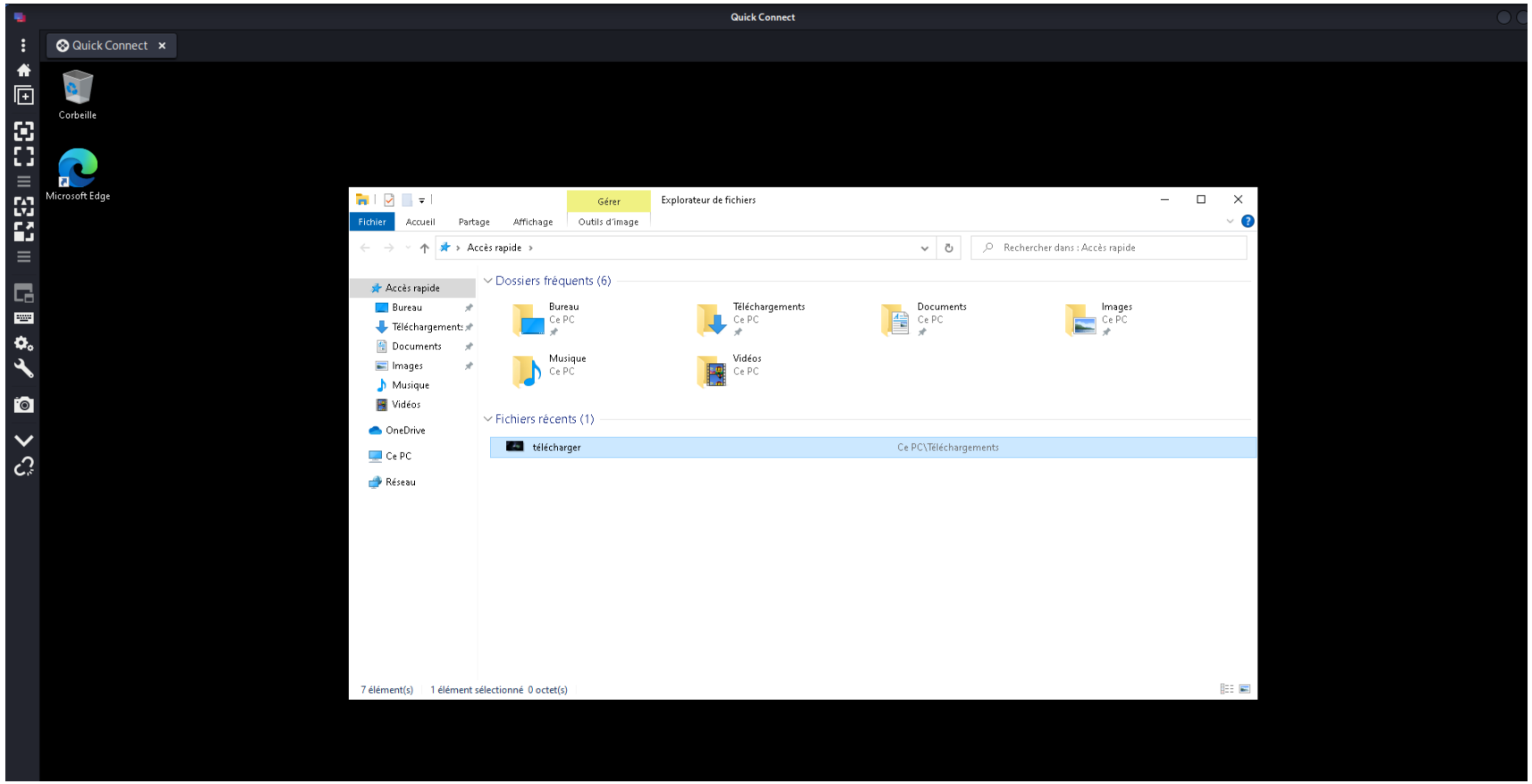
On utilise remmina pour se connecter à distance depuis la VM Kali.

On renseigne l'adresse IP de la VM Windows, le login et le mot de passe.



Contrôle à distance :

Depuis la VM Kali on télécharge une image et on change le fond d'écran.



Windows est tombé :

Oh mon dieu ! Quelqu'un a changé le fond d'écran !!!

Un vrai hacker pourrait télécharge un rançongiciel à la place d'une image et faire fermer votre entreprise.

Utiliser un mot de passe fort pour vos sessions !!!