

TP B3 : Identifier 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 à adopter 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 garantit 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 Authenticator

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.

Oracle VM VirtualBox - Gestionnaire de machines

Fichier Machine Aide

Outils

Nouvelle Ajouter Configuration Oublier Démarrer

 Ubuntu type Éteinte	Général Nom : TP4 B3 Système d'exploitation : Windows 10 (64-bit)	Prévisualisation 
 Kali Linux Éteinte	System Mémoire vive : 12030 Mo Processeurs : 4 Ordre d'amorçage : Disquette, Optique, Disque dur Accélération : Pagination imbriquée, Paravirtualisation Hyper-V	
 Debian graphique type Éteinte	Affichage Mémoire vidéo : 128 Mo Contrôleur graphique : VBoxSVGA Serveur de bureau à distance : Désactivé Enregistrement : Désactivé	
 Debian Type Éteinte	Stockage Contrôleur : SATA Port SATA 0 : TP4 B3.vdi (Normal, 50,00 Gio) Port SATA 1 : [Lecteur optique] Win10_21H1_French_x64.iso (5,46 Gio)	
 Windows Server 2016 Éteinte	Audio Pilote hôte : Par défaut Contrôleur : Intel Audio HD	
 FTP2 Éteinte	Réseau Interface 1: Intel PRO/1000 MT Desktop (Interface pont enp1s0f0)	
 Windows 10 XAMP Éteinte	USB Contrôleur USB : xHCI Filtres de périphérique : 0 (0 actif)	
 Server 2016 Éteinte	Dossiers partagés Aucun	
 Windows 10 Type Éteinte	Description Aucune	
 Windows 10 Pro Éteinte		
 TP4 B3 Éteinte		

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.

Qui sera amené à utiliser ce PC ?

Quel nom voulez-vous utiliser ?



Créer un mot de passe facile à retenir

Vérifiez que vous choisissez quelque chose dont vous vous souviendrez sans faute.

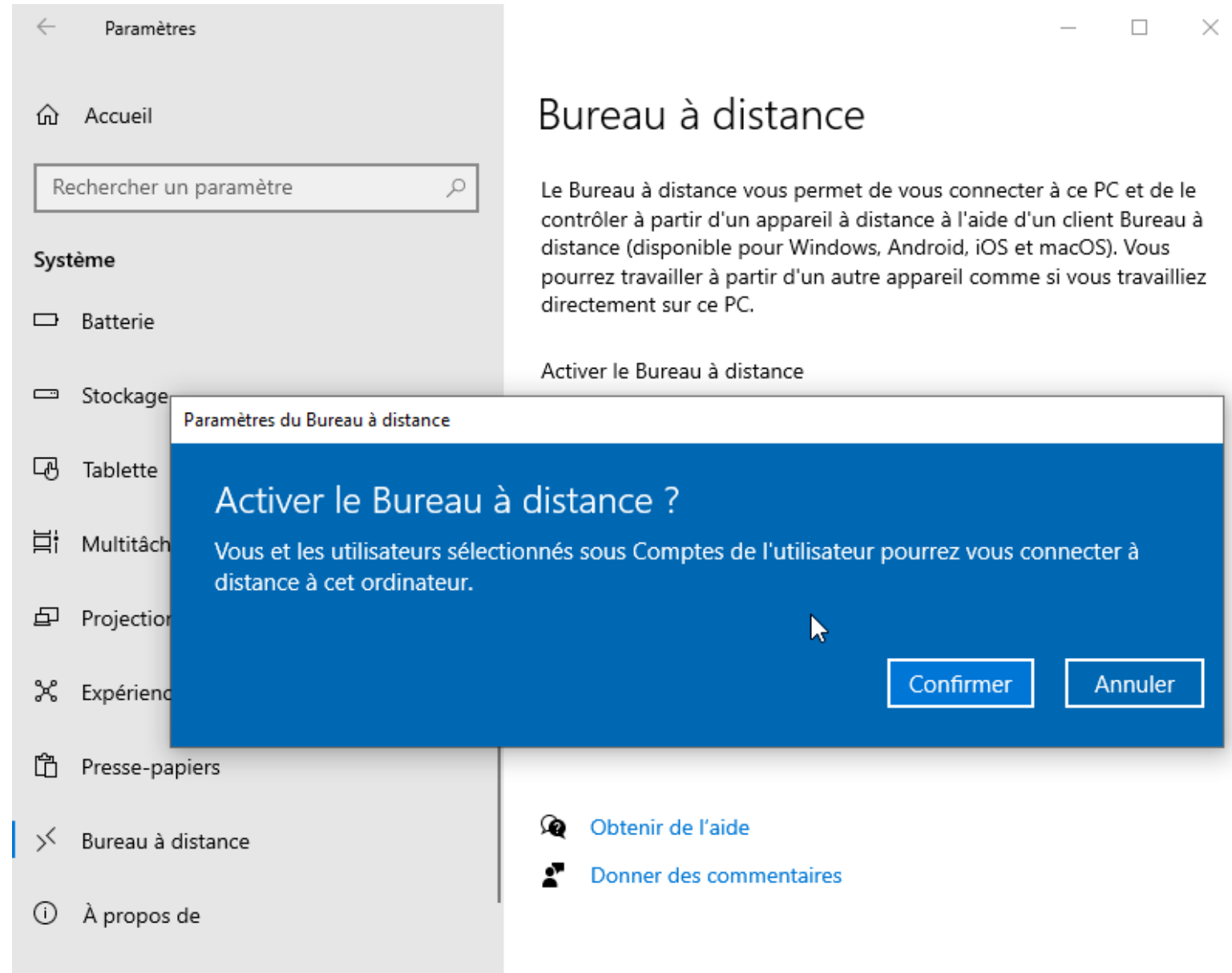


Configuration du bureau à distance :

Pour utiliser le bureau à distance :

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

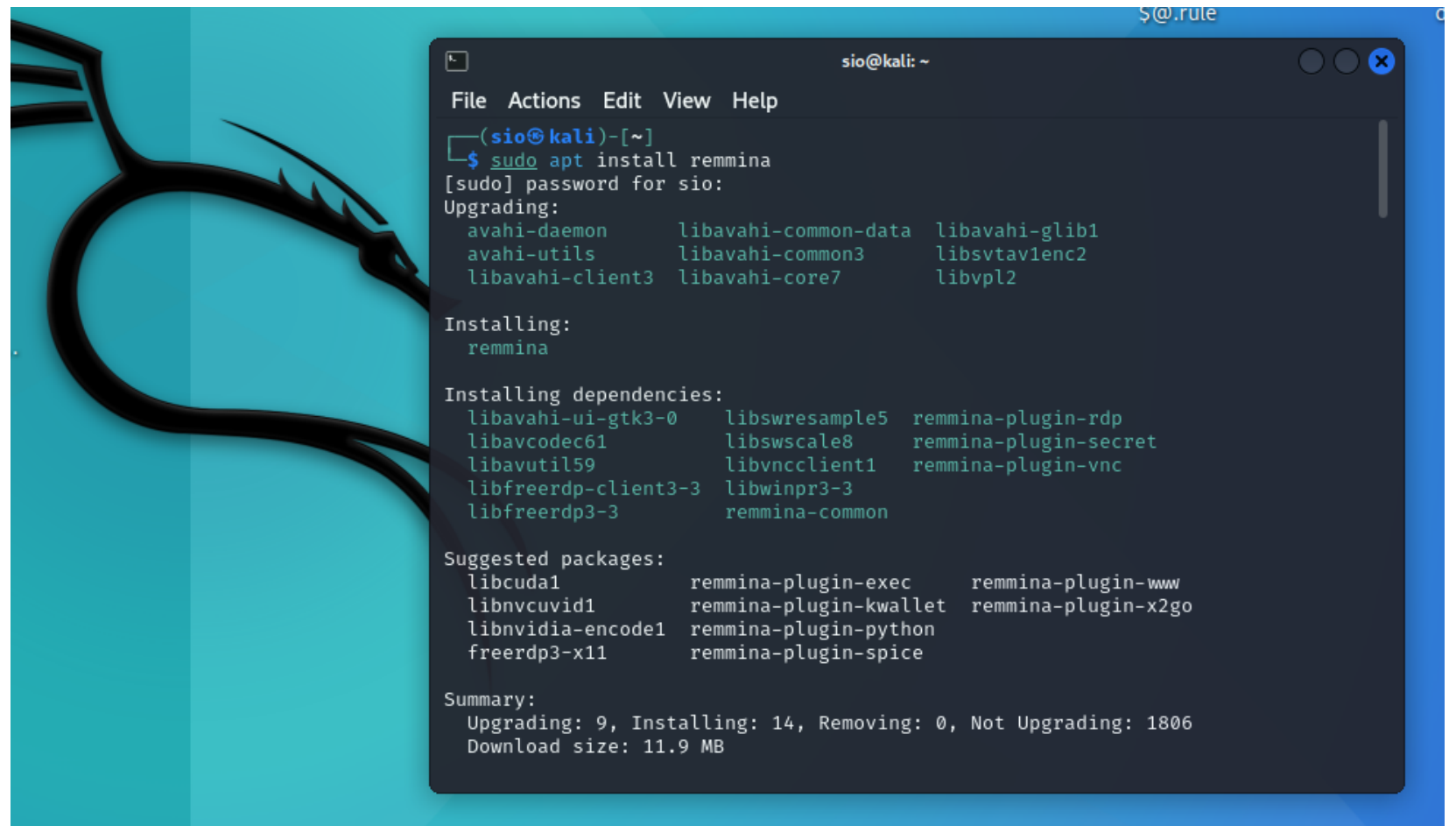
Le bureau à distance est configuré, on va pouvoir se connecter.



Machine de l'assaillant :

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

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

A terminal window titled 'sio@kali: ~' is shown against a blue background with a black dragon silhouette. The terminal displays the command to install remmina, the password prompt, the upgrade of dependencies, the installation of remmina, the installation of its dependencies, a list of suggested packages, and a summary of the operation.

```
sio@kali: ~  
File Actions Edit View Help  
(sio@kali)-[~]  
$ sudo apt install remmina  
[sudo] password for sio:  
Upgrading:  
  avahi-daemon      libavahi-common-data  libavahi-glib1  
  avahi-utils       libavahi-common3      libsvtav1enc2  
  libavahi-client3  libavahi-core7        libvpl2  
  
Installing:  
  remmina  
  
Installing dependencies:  
  libavahi-ui-gtk3-0  libswresample5  remmina-plugin-rdp  
  libavcodec61       libswscale8     remmina-plugin-secret  
  libavutil59        libvncclient1   remmina-plugin-vnc  
  libfreerdp-client3-3 libwinpr3-3  
  libfreerdp3-3      remmina-common  
  
Suggested packages:  
  libcuda1          remmina-plugin-exec  remmina-plugin-www  
  libnvcuvid1       remmina-plugin-kwallet remmina-plugin-x2go  
  libnvidia-encode1 remmina-plugin-python  
  freerdp3-x11      remmina-plugin-spice  
  
Summary:  
  Upgrading: 9, Installing: 14, Removing: 0, Not Upgrading: 1806  
  Download size: 11.9 MB
```

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.

```
(sio@kali)-[~]  
$ nmap 192.168.60.54  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 09:44 CET  
Nmap scan report for 192.168.60.54  
Host is up (0.00027s latency).  
Not shown: 996 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
3389/tcp  open  ms-wbt-server  
  
Nmap done: 1 IP address (1 host up) scanned in 10.60 seconds
```

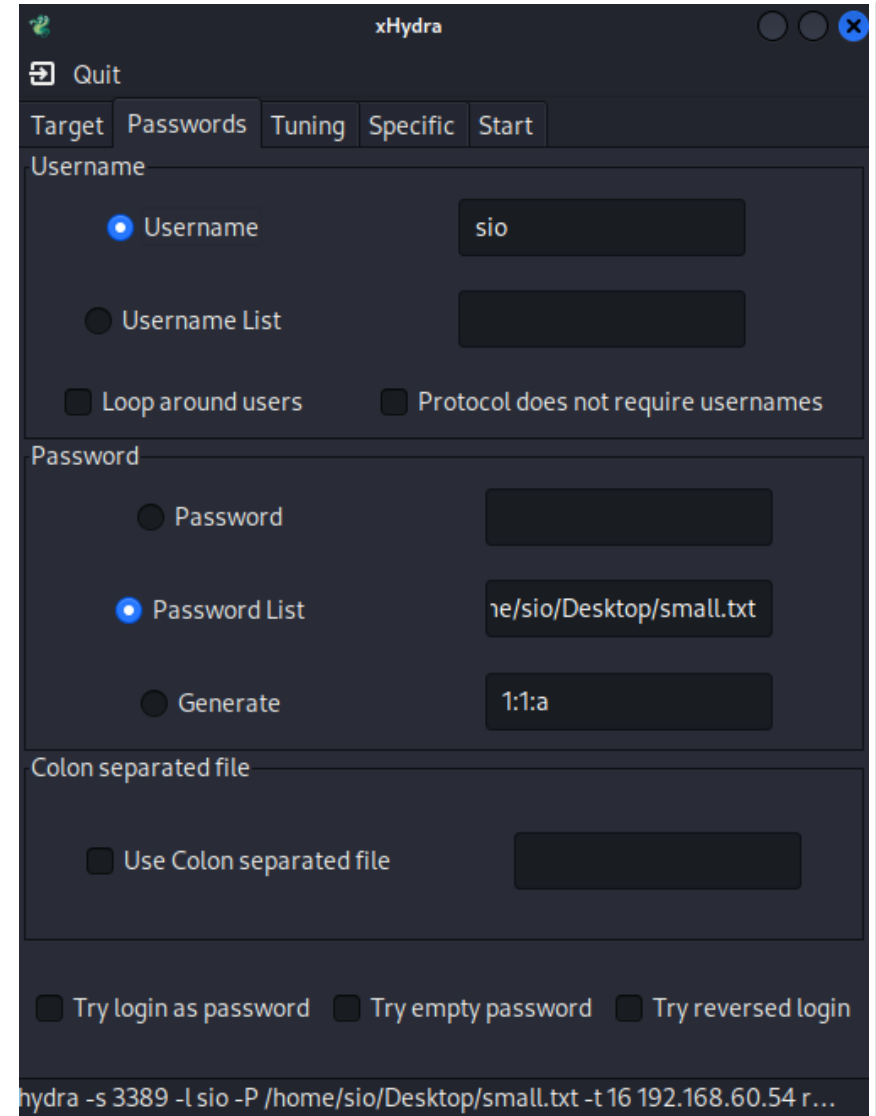
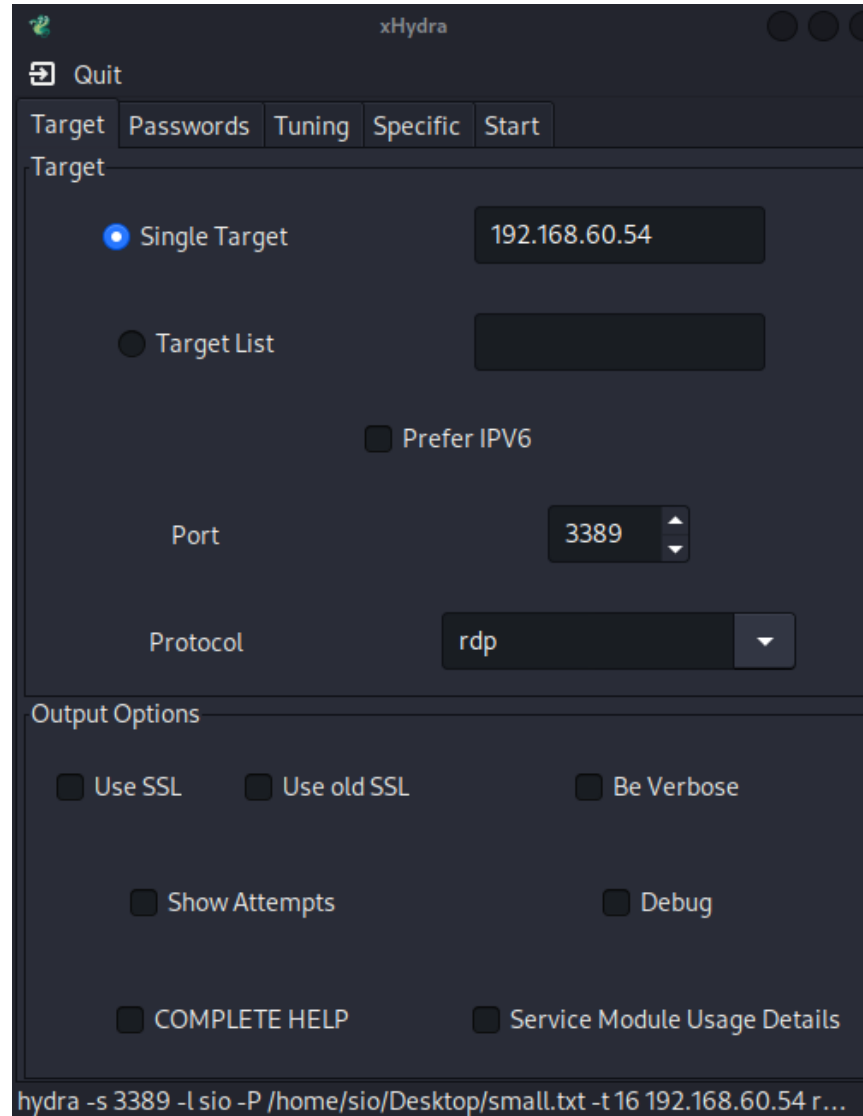
Xhydra :

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.

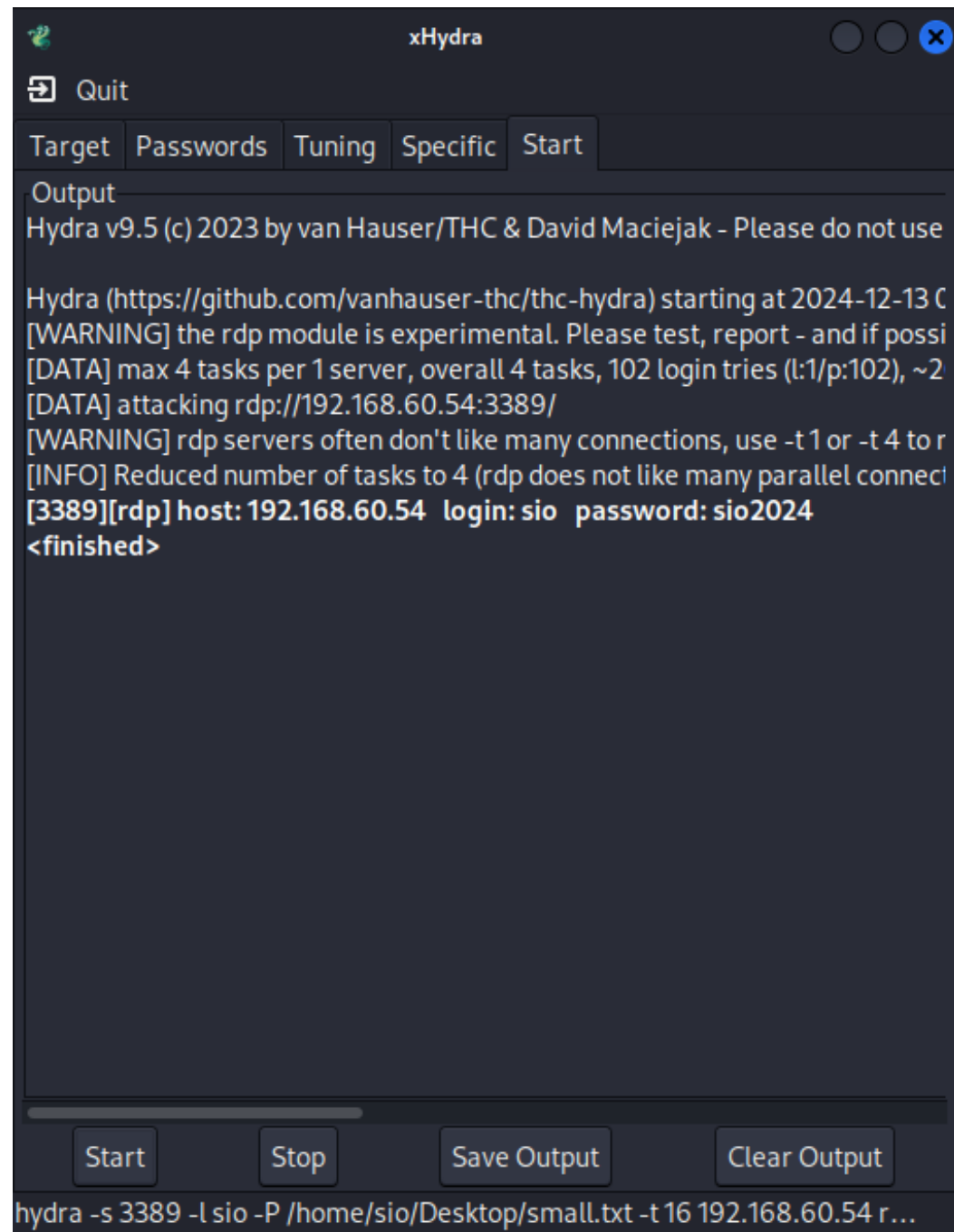


Mot de passe trouvé :

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.



The screenshot shows the xHydra application window. At the top, there's a title bar with the name 'xHydra' and standard window controls. Below the title bar is a menu bar with a 'Quit' option. A tabbed interface is visible with tabs for 'Target', 'Passwords', 'Tuning', 'Specific', and 'Start'. The 'Start' tab is currently selected. The main area is labeled 'Output' and contains the following text:

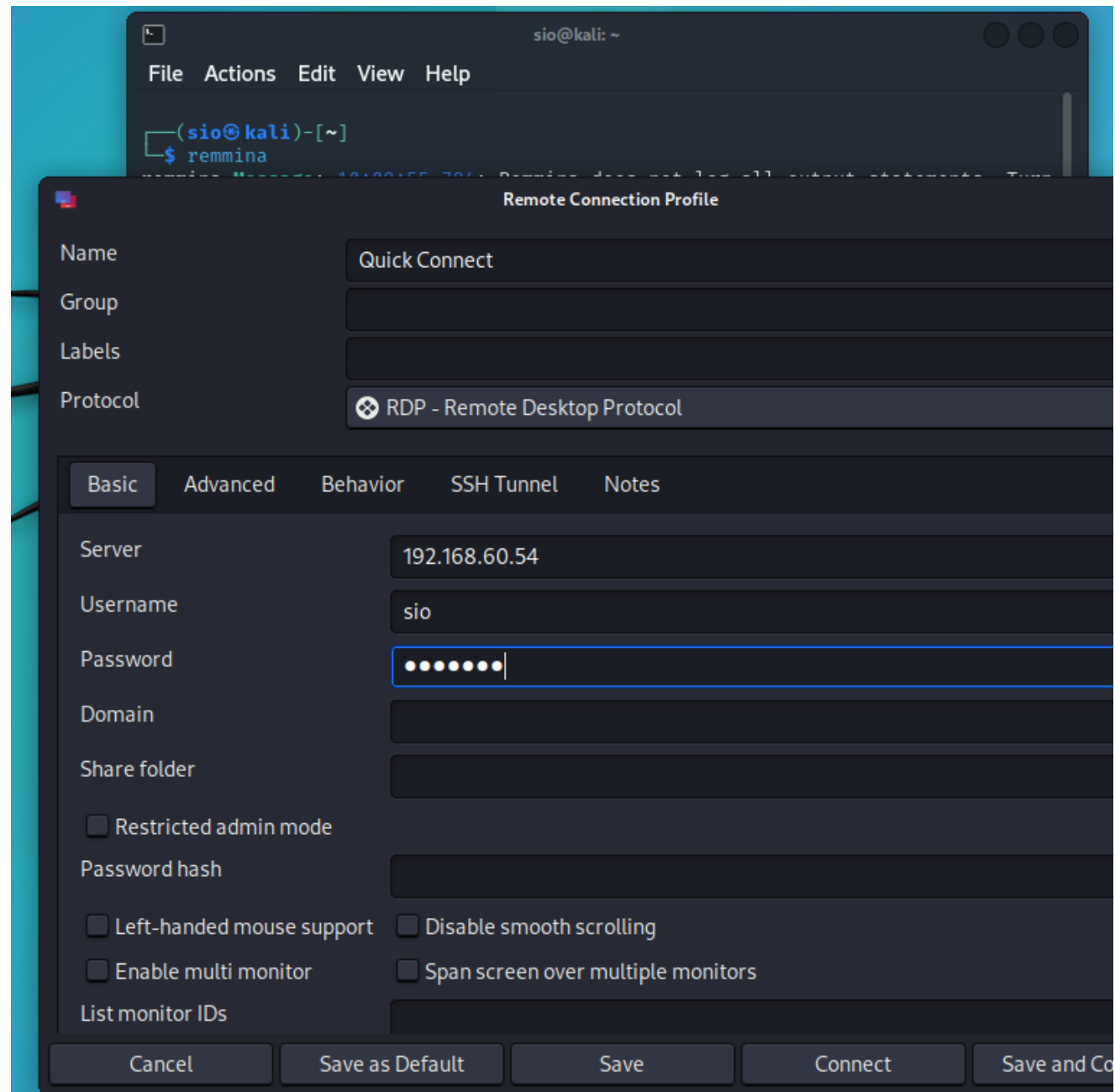
```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-13 C  
[WARNING] the rdp module is experimental. Please test, report - and if possi  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 102 login tries (l:1/p:102), ~2  
[DATA] attacking rdp://192.168.60.54:3389/  
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to r  
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connect  
[3389][rdp] host: 192.168.60.54 login: sio password: sio2024  
<finished>
```

At the bottom of the window, there are four buttons: 'Start', 'Stop', 'Save Output', and 'Clear Output'. Below these buttons, a command line is visible: `hydra -s 3389 -l sio -P /home/sio/Desktop/small.txt -t 16 192.168.60.54 r...`

Connexion à distance :

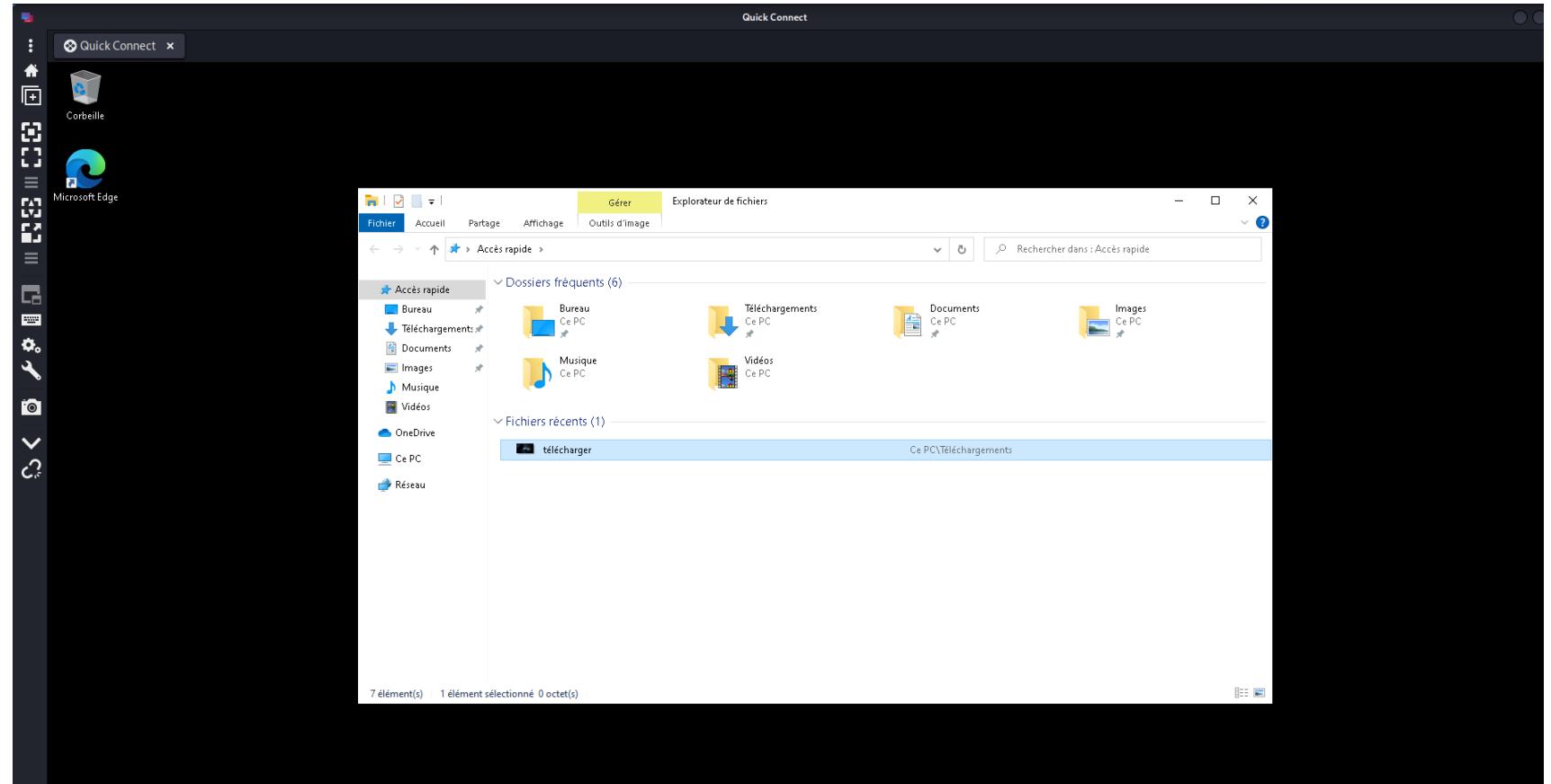
On utilise remmina pour se connecter à distance depuis la VM Kali.

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 télécharger un rançongiciel à la place d'une image et faire fermer votre entreprise.

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

