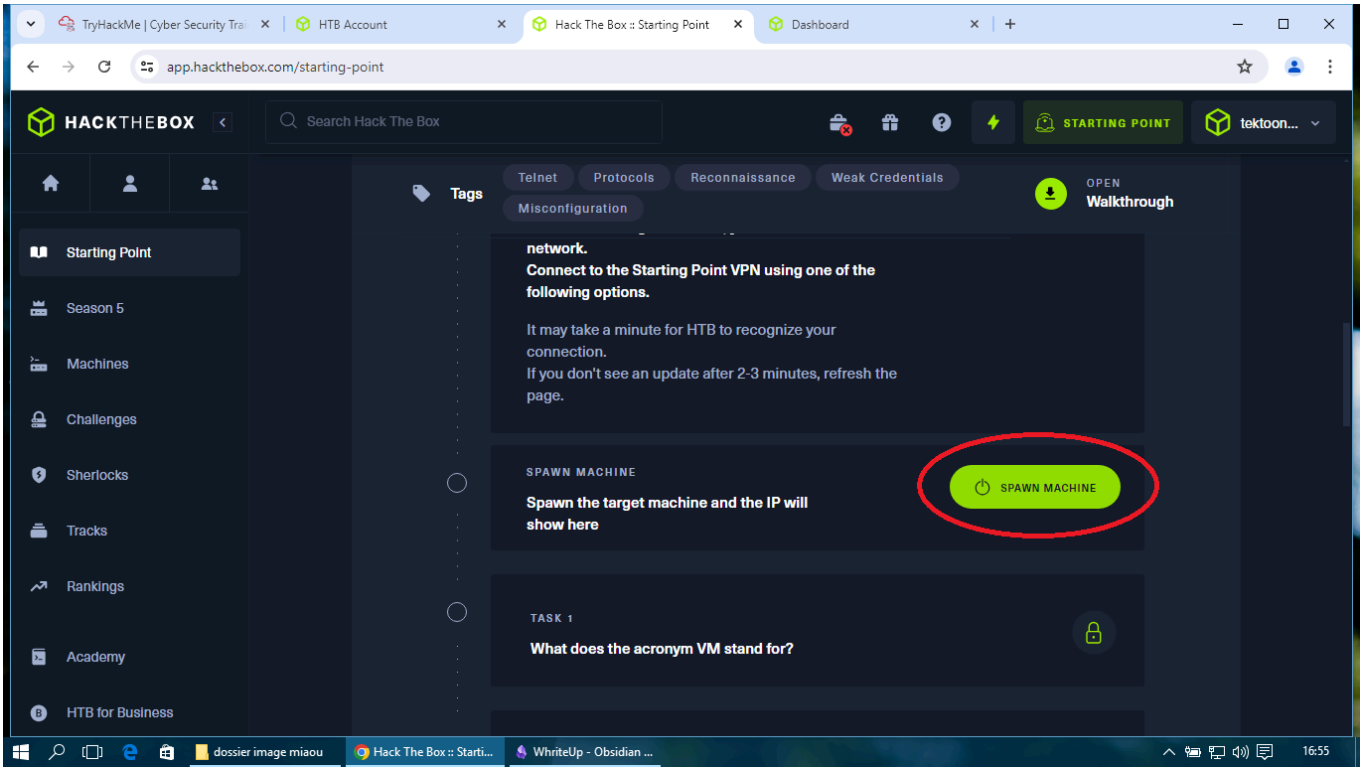
Adresse ip: 10.129.3.31 (celle-ci change a chaque fois)

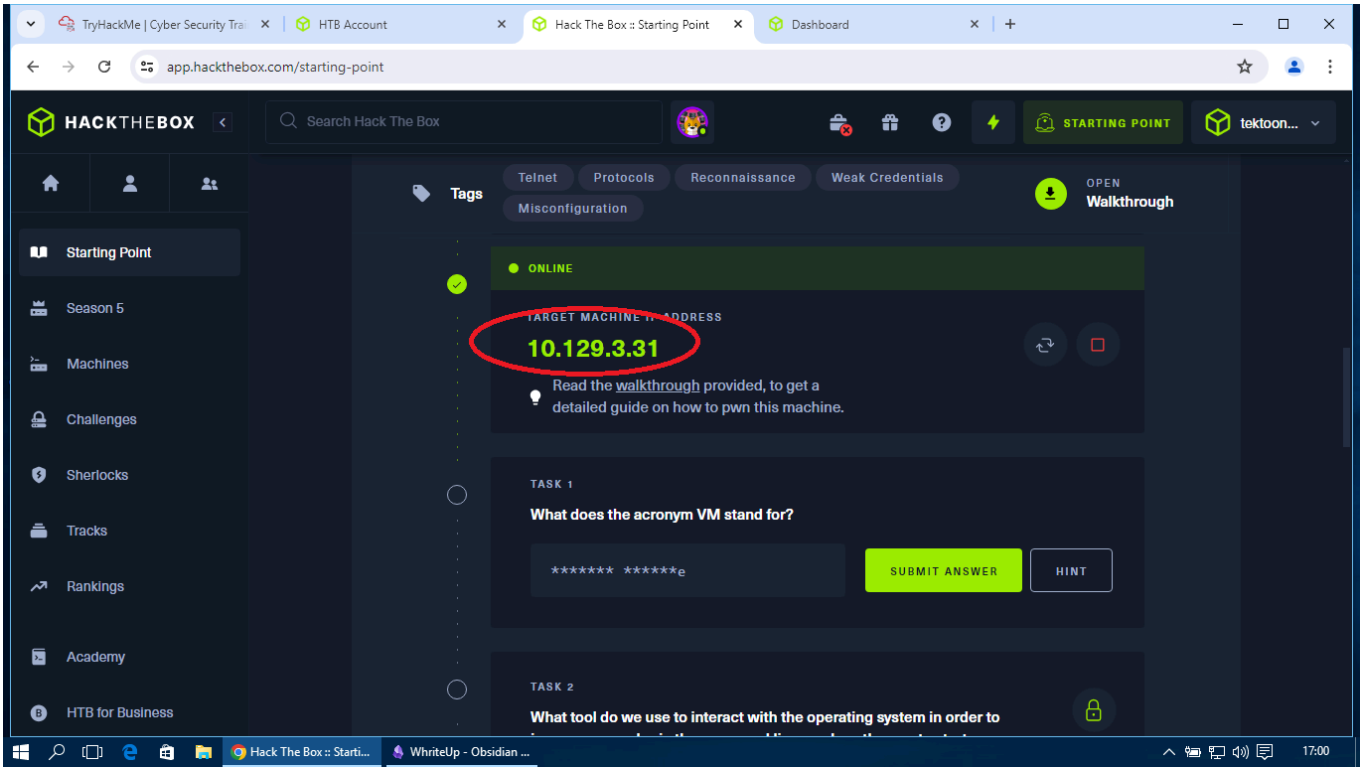
Pour pouvoir se connecter au réseau Hack The Box il nous faut pour cela télécharger le fichier openvpn.

Sur kali lancer la commande "openvp" et lui donner le chemin d'acces au fichier de configuration

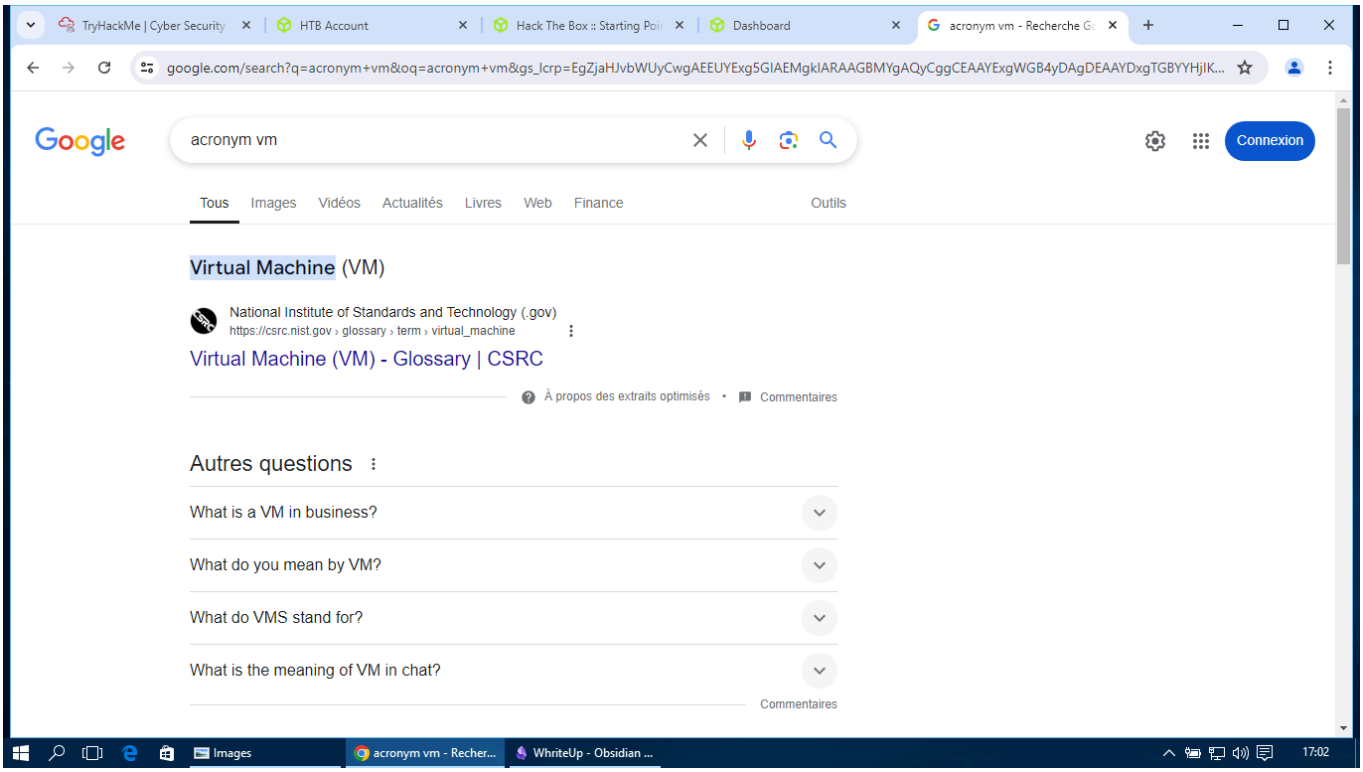
ensuite lancer la machine.



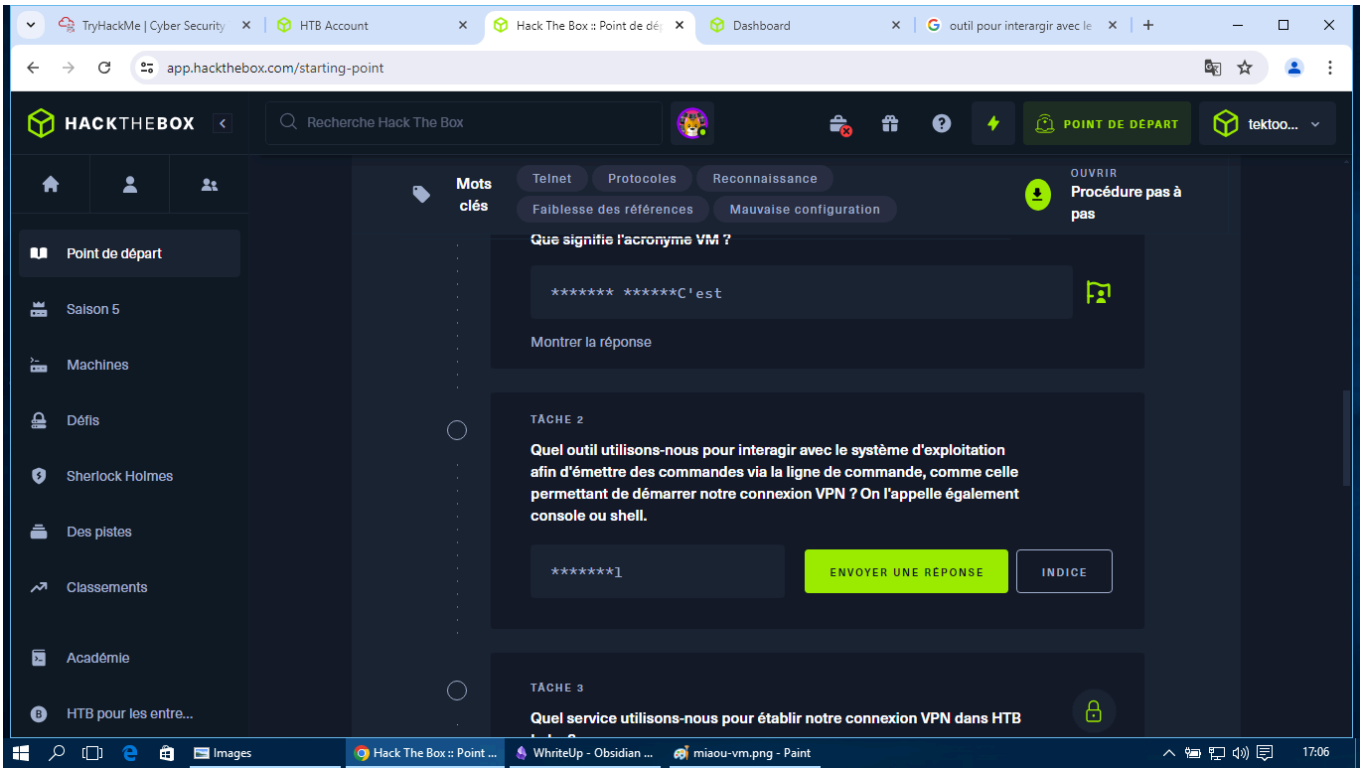
une fois la machine lancer nous obtenons l'adresse IP.



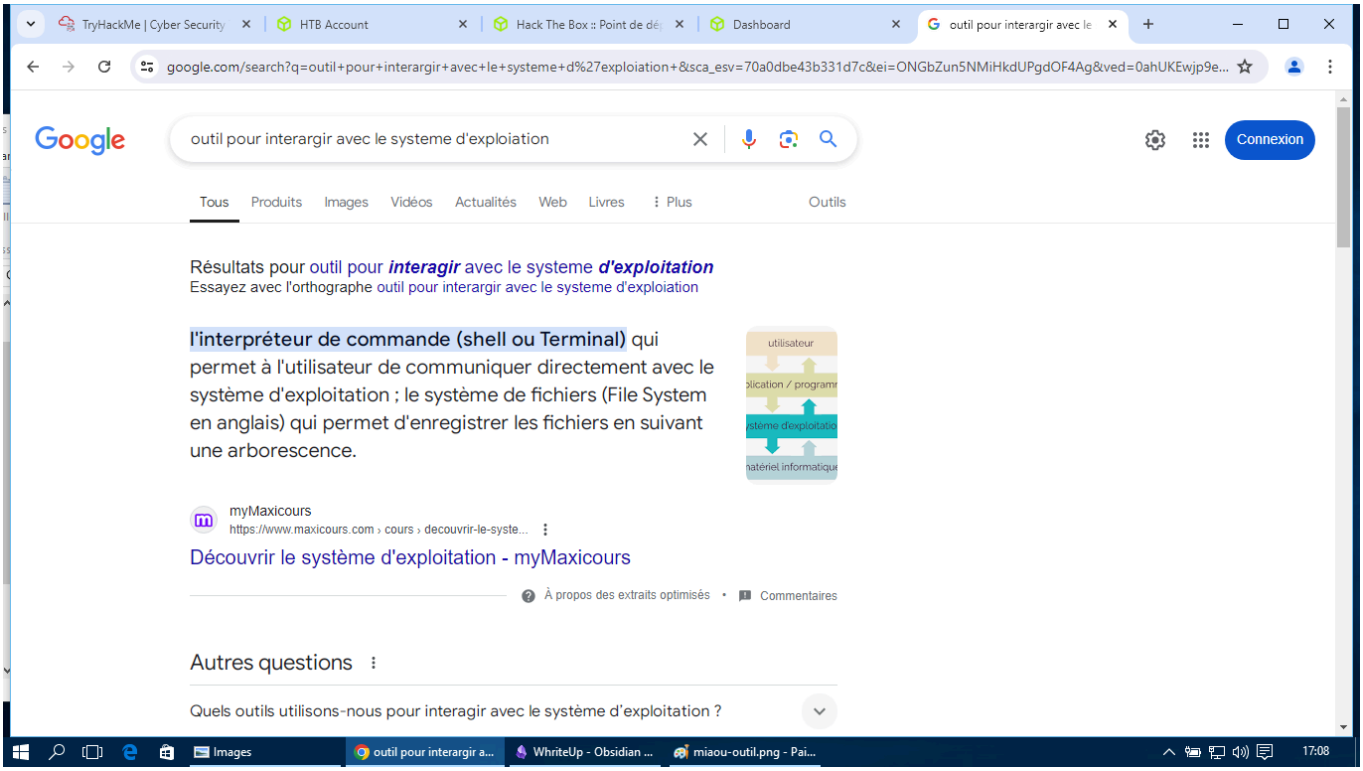
première tache on nous demande ce que signifie l'acronyme VM (petite recherche Google)



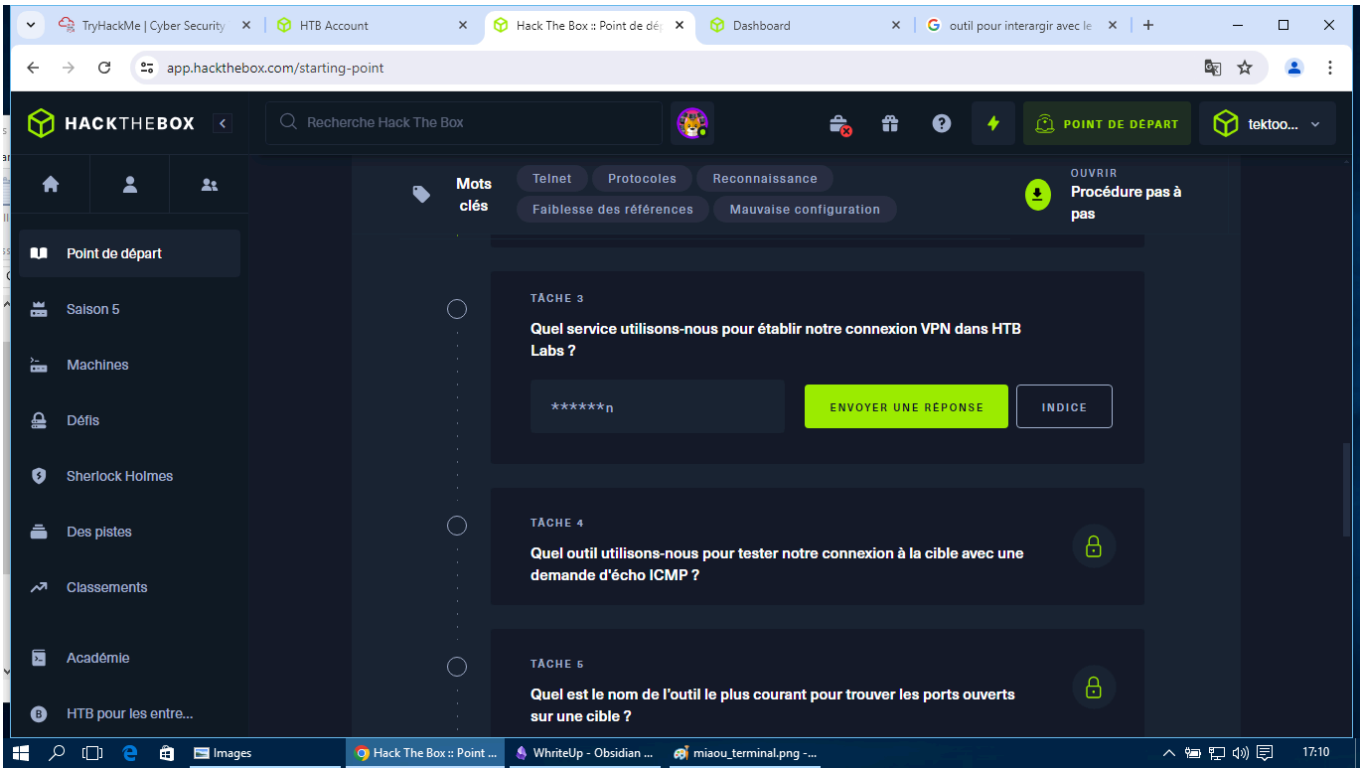
tache numéro 2 on nous demande quel outils utiliser pour interagir avec le systeme d'exploitation en ligne de commande



pour cela petite recherche Google.

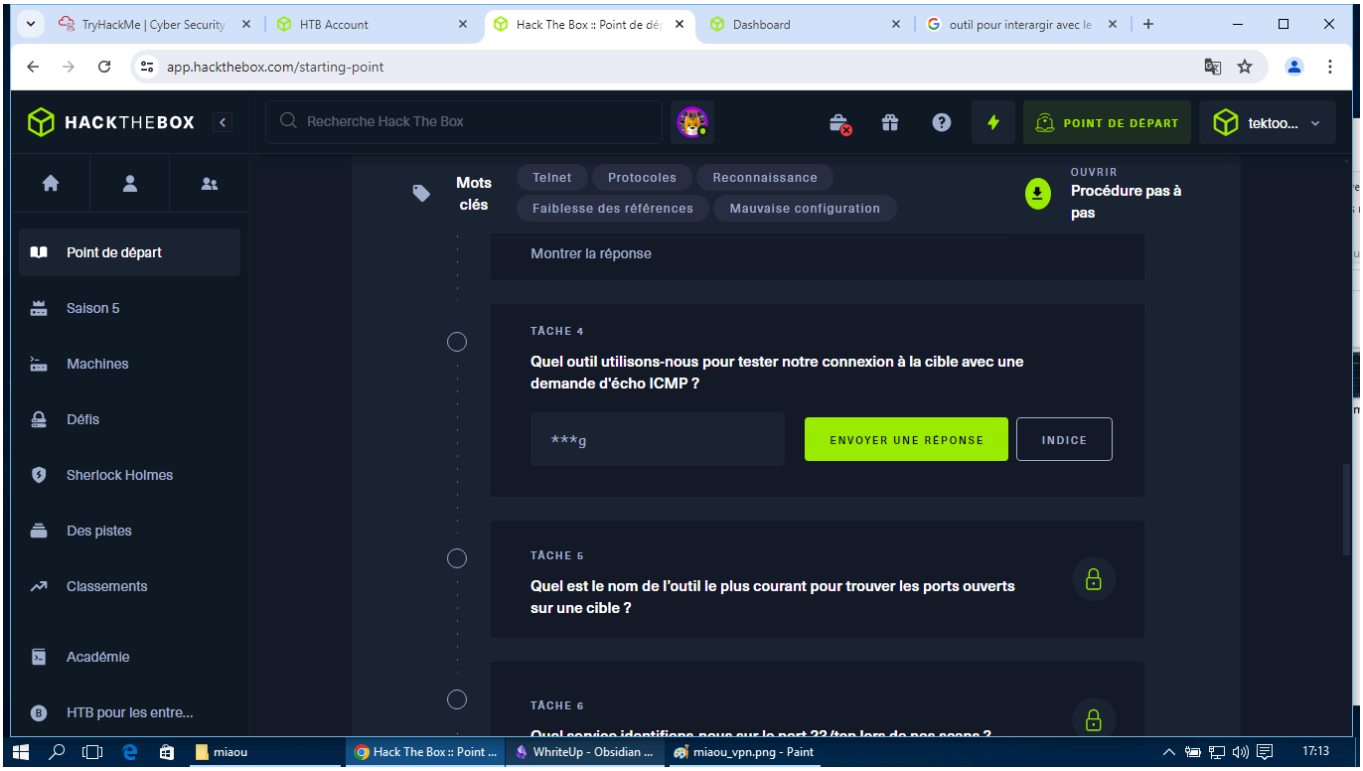


on nous demande ensuite quel service on a utiliser pour établir une connexion VPN avec notre LAB HTB.

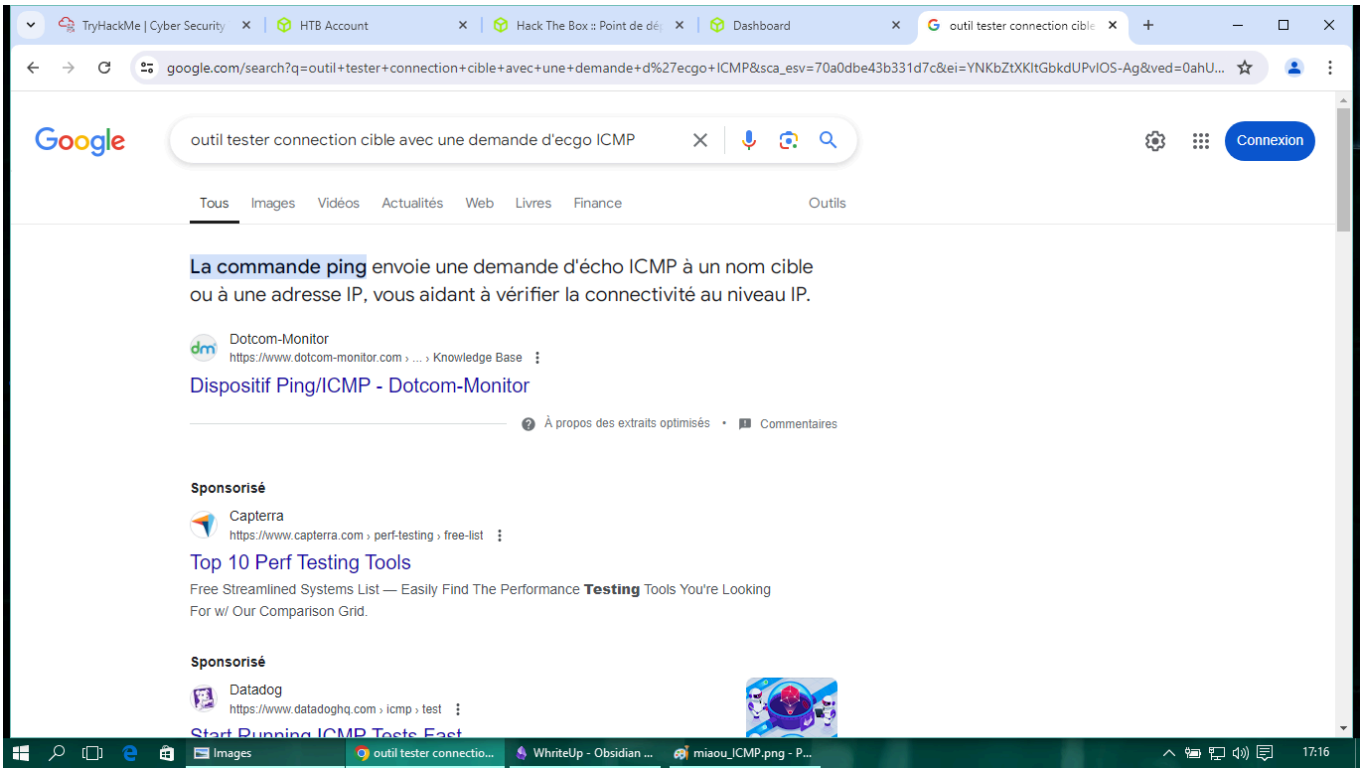


il s'agit d'openvpn comme vue plus haut.

on nous demande ensuite quel outil utiliser pour tester notre connexion a la cible avec une demande d'écho ICMP



pour cela encore une fois petite recherche Google



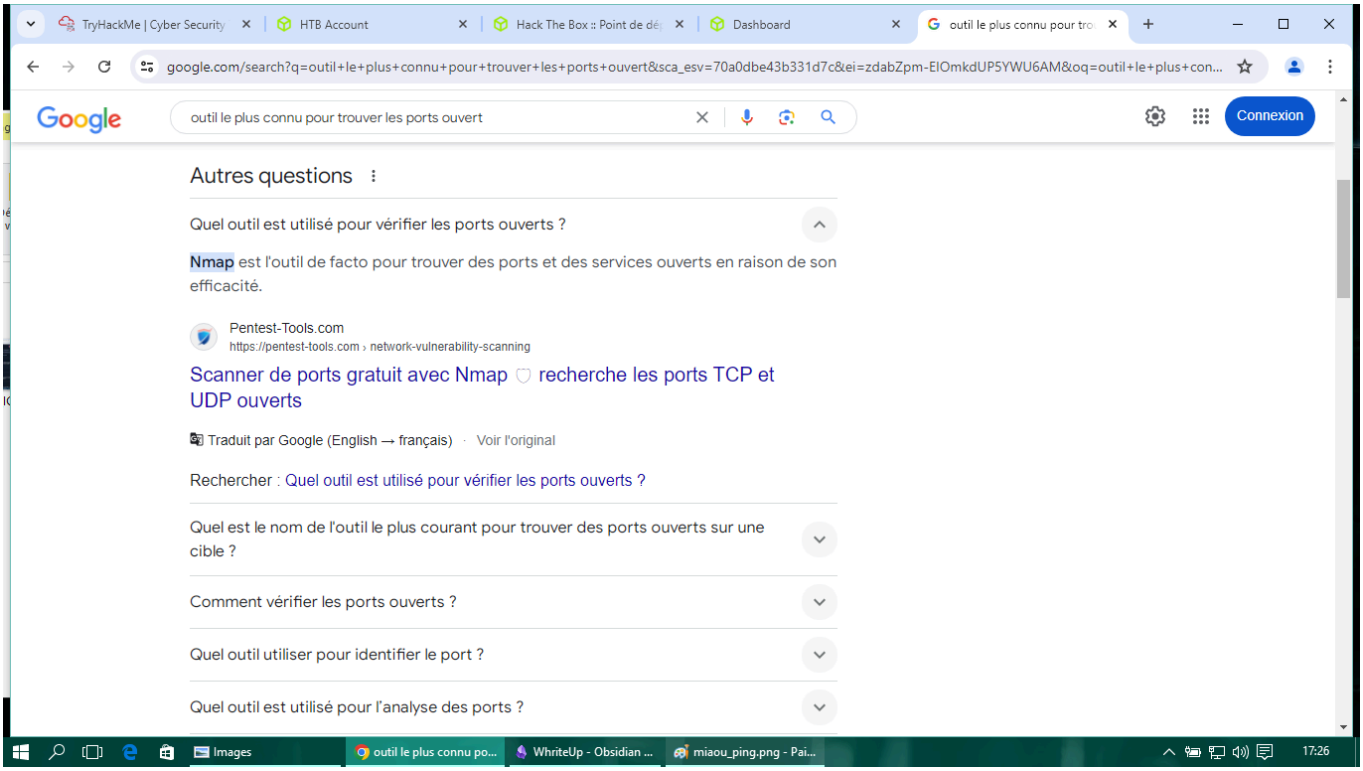
on peut voir ici qu'il s'agit de la commande ping.

on peut également voir grâce a la commande ping que nous somme bien connecté a la machine MIAOU

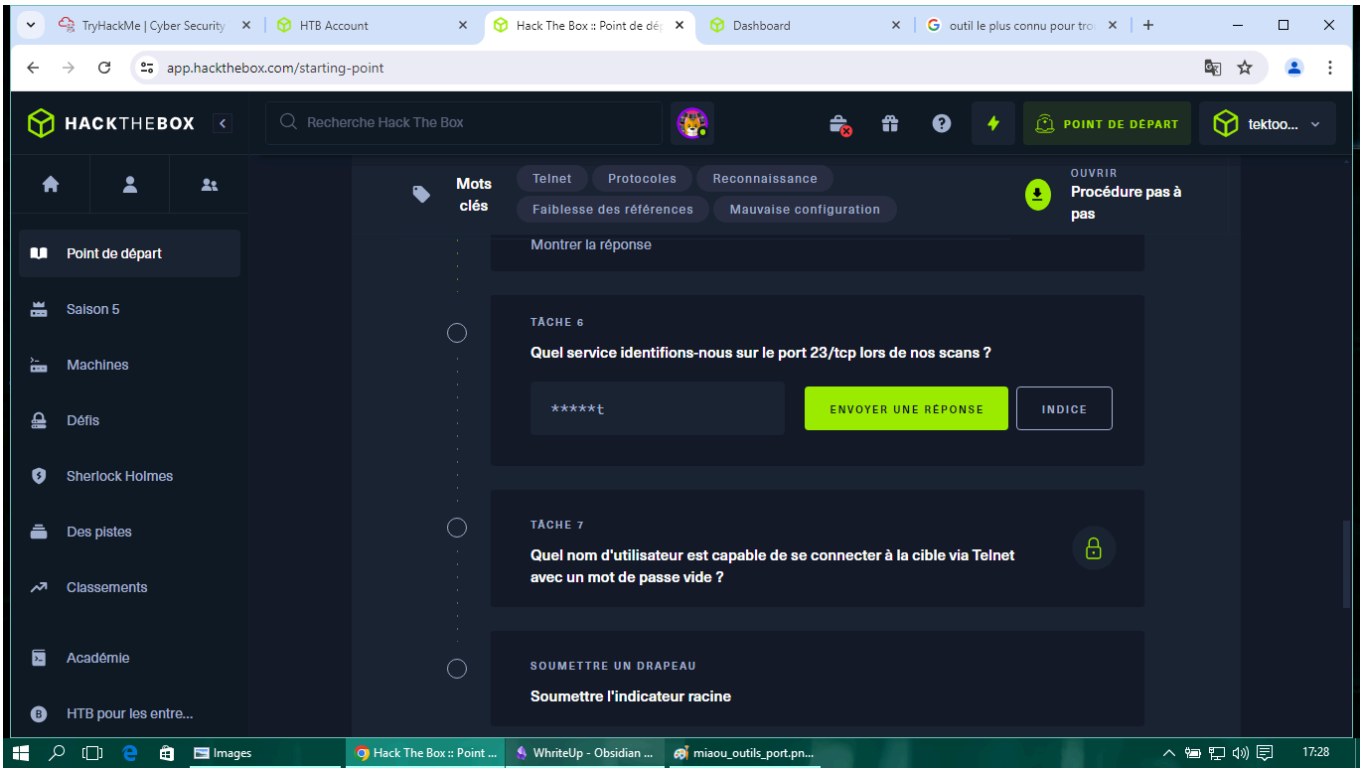
```
┌──(kali㉿kali-raspberry-pi)-[~]
└─$ ping 10.129.3.31
PING 10.129.3.31 (10.129.3.31) 56(84) bytes of data.
64 bytes from 10.129.3.31: icmp_seq=1 ttl=63 time=25.1 ms
64 bytes from 10.129.3.31: icmp_seq=2 ttl=63 time=24.7 ms
64 bytes from 10.129.3.31: icmp_seq=3 ttl=63 time=25.5 ms
64 bytes from 10.129.3.31: icmp_seq=4 ttl=63 time=24.9 ms
64 bytes from 10.129.3.31: icmp_seq=5 ttl=63 time=24.8 ms
^C
--- 10.129.3.31 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 24.695/25.001/25.479/0.276 ms
```

ensuite on nous demande quel outils utiliser pour détecter les ports ouvert sur une cible.

encore une fois Google est ton amie ^^



Ensuite on nous demande quel service est actif sur le port 23 lors de notre scan.



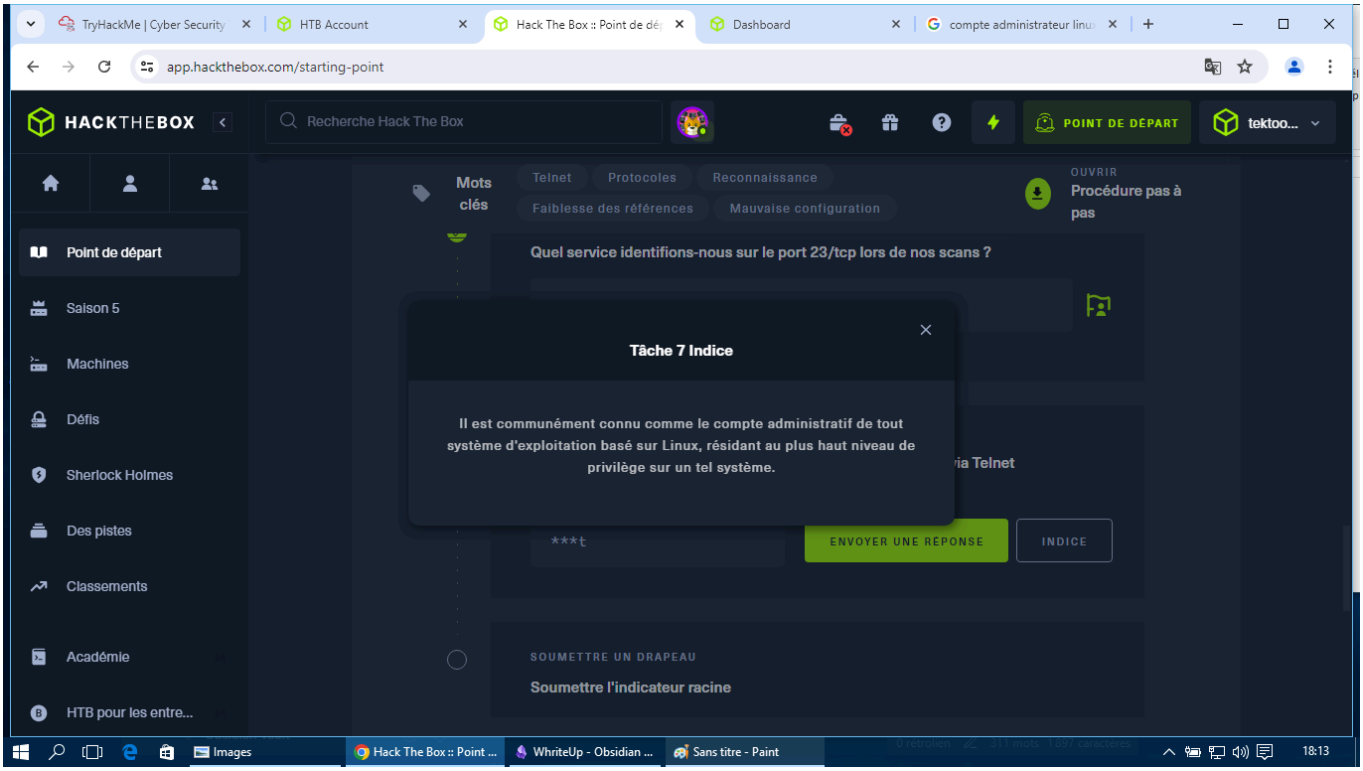
pour cela petit scan avec l'outils NMAP

Apres avoir scanner les ports on peut voir que sur le port 23 il s'agit du service TELNET.

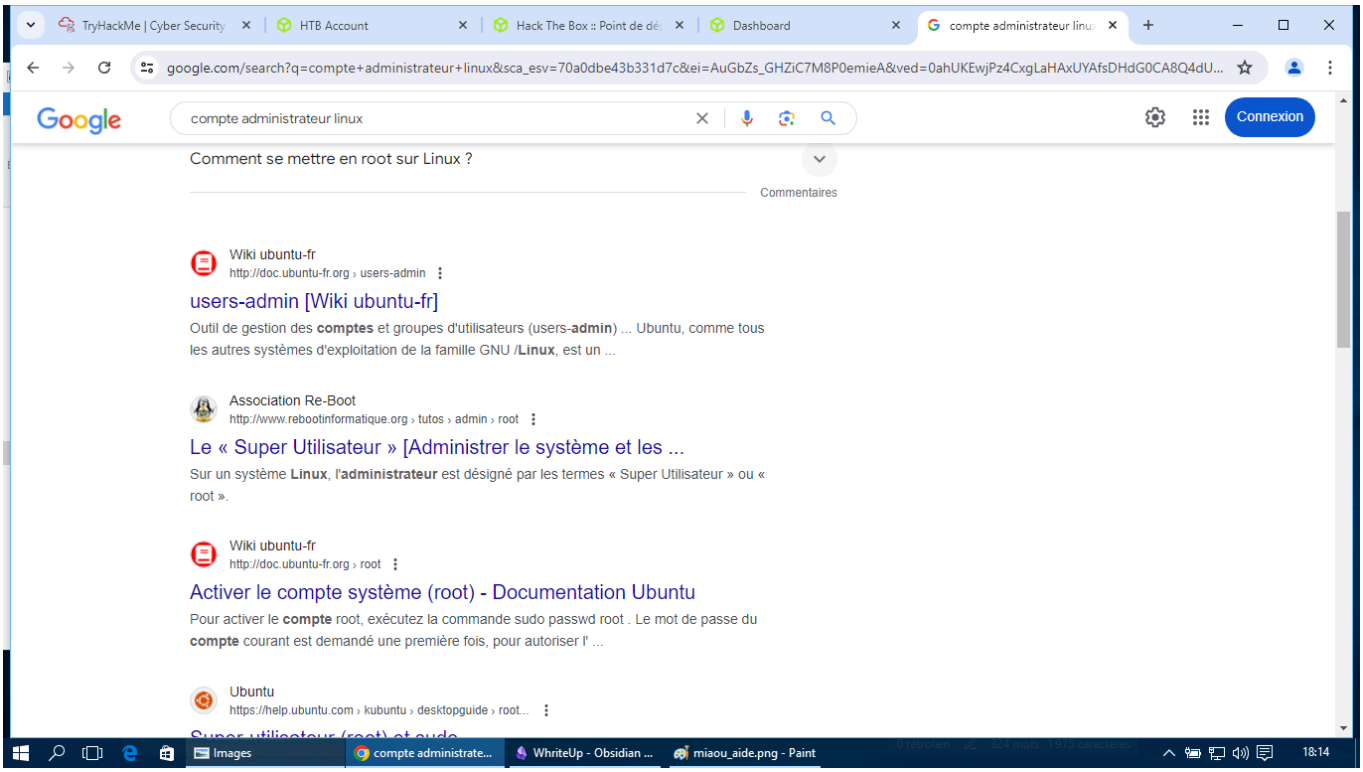
```
┌──(root㉿kali-raspberry-pi)-[/home/kali]
└─# nmap 10.129.3.31
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-20 15:37 UTC
Nmap scan report for 10.129.3.31
Host is up (0.027s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 1.16 seconds
```

ensuite on nous demande quel nom d'utilisateur est capable de se connecter à la cible via Telnet avec un mot de passe vide on peut utiliser l'aide proposer par HTB et par la suite Google

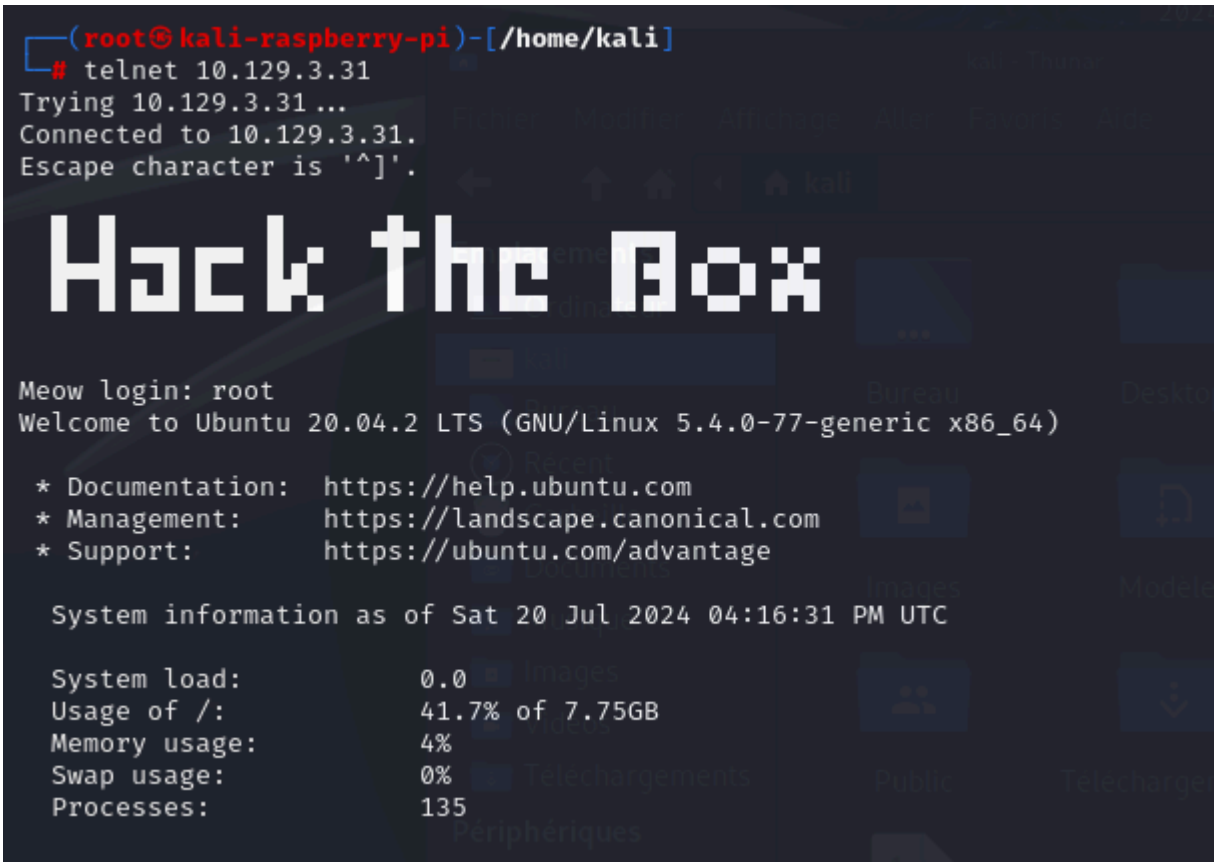


après une petite recherche Google



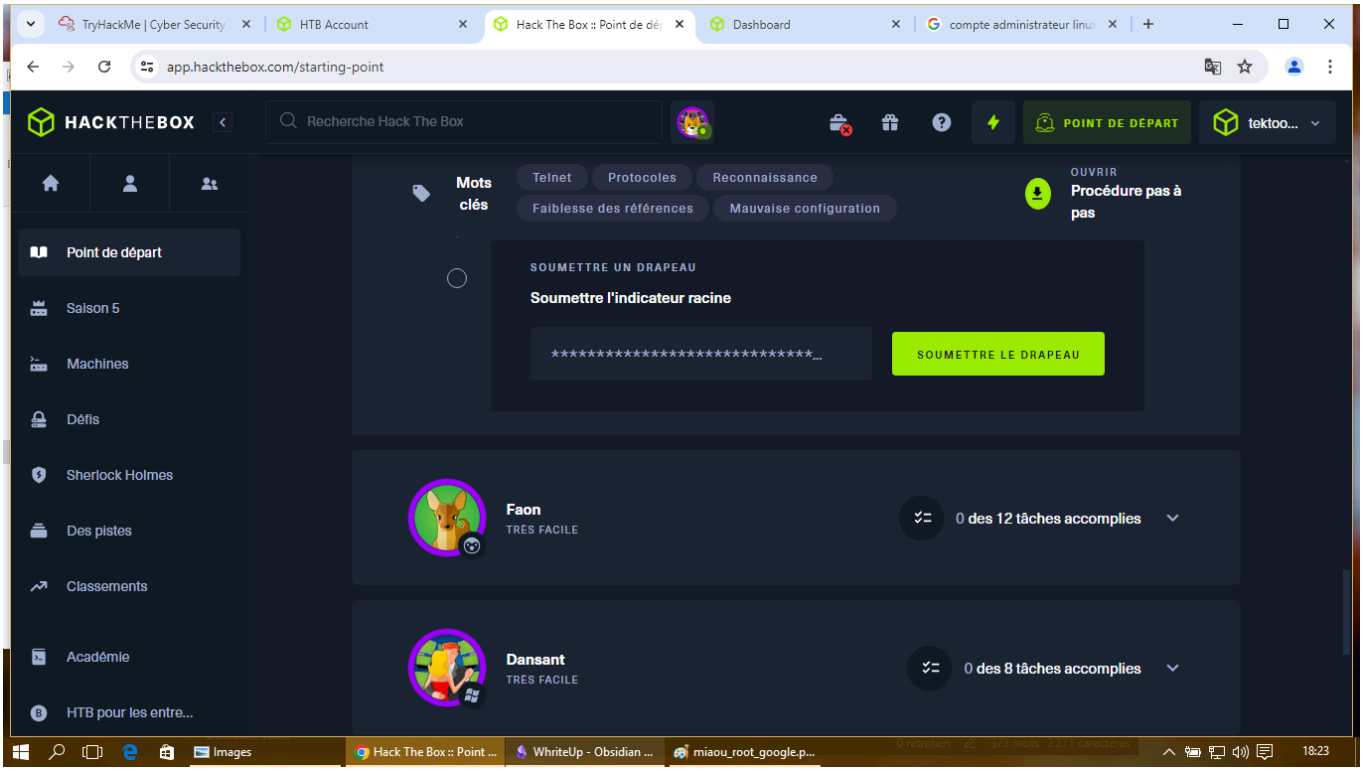
on peut donc voir qu'il s'agit du compte root.

on essaye donc de se connecter avec le compte route en utilisant la commande 'telnet' suivie de l'adresse ip



ici nous sommes donc connecter en root.

on nous demande ensuite le flag.

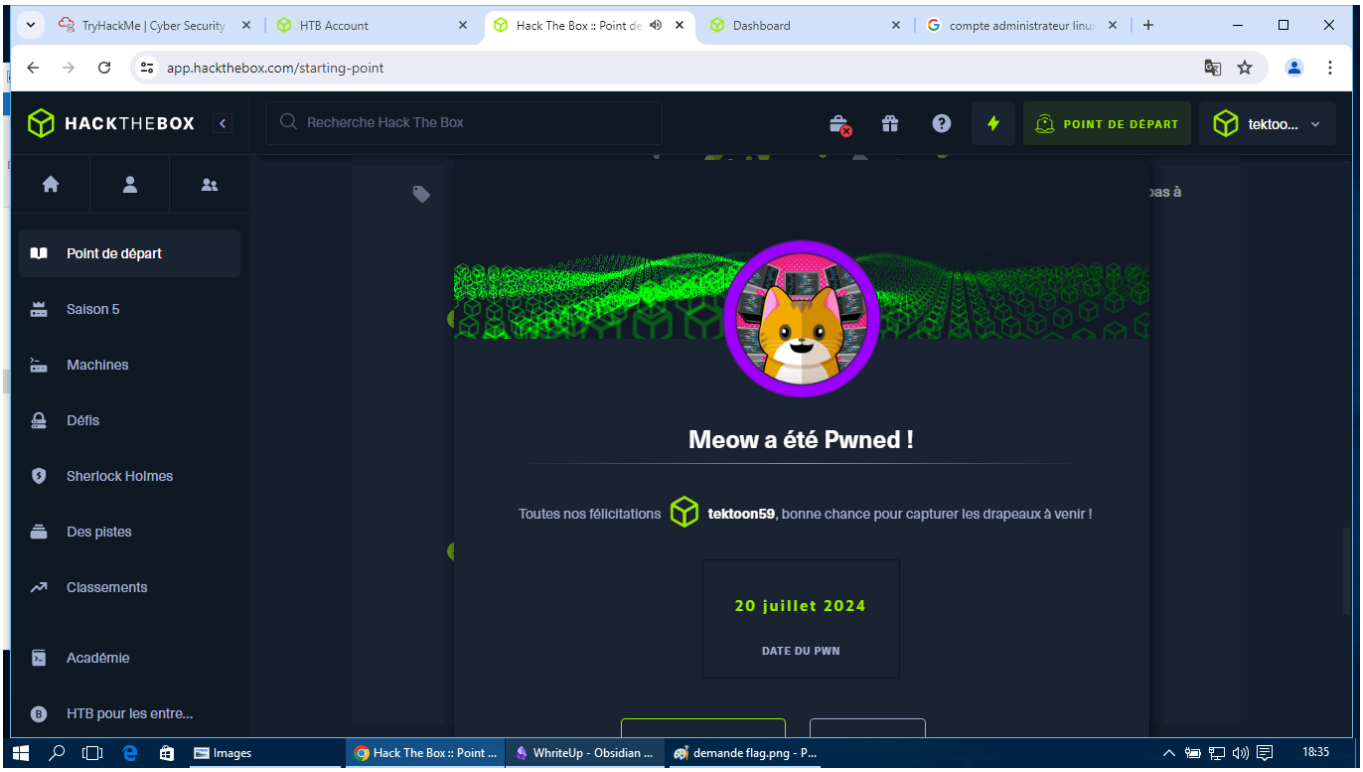


une fois connecter a Telnet avec le compte : root et sans mdp on obtient un shell
il nous suffit donc de faire une 'ls' pour voir qu'il y a un ficher flag.txt

```
root@Meow:~# ls
flag.txt  snap
root@Meow:~#
```

une fois cela fait il ne nous reste plus qu'a utiliser la commande "cat" suivie de flag.txt pour afficher le contenue du fichier flag et pouvoir le renseigner

```
root@Meow:~# cat flag.txt
b40abdfe23665f766f9c61ecba8a4c19
root@Meow:~#
```


TryHackMe | Cyber Security
HTB Account
Hack The Box :: Point de
Dashboard
compte administrateur linu
app.hackthebox.com/starting-point
HACKTHEBOX
Recherche Hack The Box
POINT DE DÉPART
tektoo...
Point de départ
Saison 5
Machines
Défis
Sherlock Holmes
Des pistes
Classements
Académie
HTB pour les entre...
Meow a été Pwned !
Toutes nos félicitations tektoon59, bonne chance pour capturer les drapeaux à venir !
20 juillet 2024
DATE DU PWN
Images
Hack The Box :: Point ...
WhriteUp - Obsidian ...
demande flag.png - P...
18:35