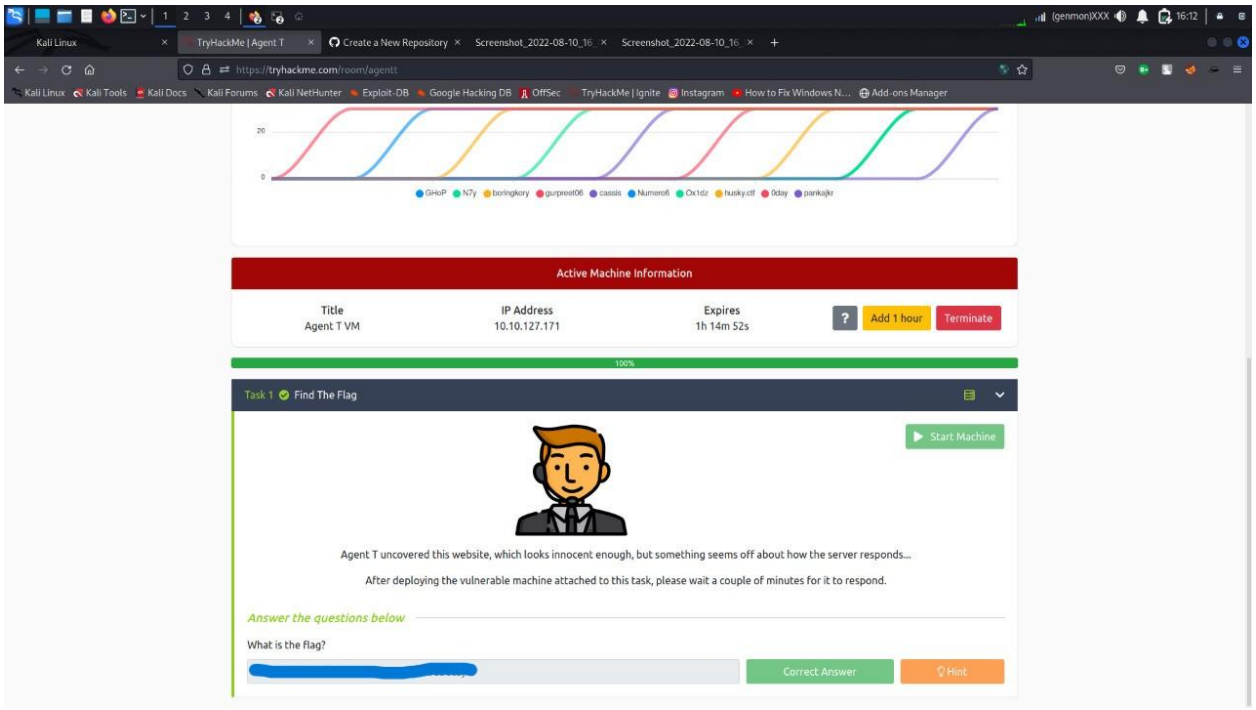
Agent-T writeup

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.

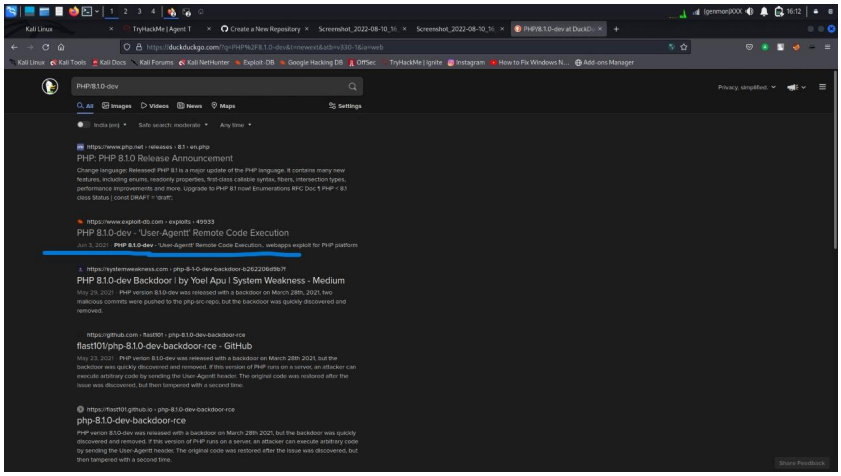
Nmap -sV(service version) ip address.

```
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-Agentt Remote Code Execution on exploit.db`

NOw copy the code and paste it in notepad and save it with xyz.py (in python formet)

Taske 4

Now run the code

Python3 xyz.py

Paste url

Run id

Result: uid=0(root) gid=0(root) groups=0(root)

RUN cat/;ls

Cd /;cat flag.txt

See the flag