Welcome to my walkthrough for the TryHackMe CTF - Agent T by John Hammond

This was definitely the most doable room I have done on the website so far, so this won't be a long drawn-out walkthrough - just a simple step-by-step of how I approached the task.
I was using a modified Kali VM for this task.

First off - enumeration.

I scanned the machine with Threader3000 for speed, however it is probably just as quick to run an nmap scan for this room. (Threader3000 - https://github.com/dievus/threader3000)
export ip=10.10.219.18
nmap -Pn $ip -p- -T5 (if you're really in a hurry, you can leave out the -p- for all ports - although I wouldn't recommend this as it is a bad habit to get into and you may miss things in other scenarios)

If you do want to get started without waiting for a long scan, you can also run
nmap -Pn $ip -T4
and then if that finds anything interesting, you can get started on that while running
nmap -Pn $ip -p- -T5
in the background and if your initial efforts are futile, you can come back to anything else the second scan produces.

With the results of the first scan:
PORT STATE SERVICE
80/tcp open http

We now know that port 80 is open. I like to run a more specific scan in the background and save the output results, while I go and visit this on my browser:
nmap -sC -sV -Pn -oN nmap-$ip.out $ip -p80 -T4

and I am visiting
http://10.10.219.18/ (obviously insert your own target machine IP here)
in your browser of choice.

When the page is loaded, we are presented with an admin dashboard, seemingly logged in as admin, with a search bar for text input. I always check the source code for a target web page when I first land on it, and in this case with only port 80 to work with, I like to capture the page request in Burp Suite too for more information.

Using Burp Proxy with intercept on, I refreshed the web page to inspect it. I couldn't see anything on the initial request worth looking at, so I deicded to inspect the response as well.

In the response headers, we are told a few things:
HTTP/1.1 200 OK
Host: 10.10.219.18
Date: Mon, 08 Aug 2022 04:04:36 GMT
Connection: close
X-Powered-By: PHP/8.1.0-dev
Content-type: text/html; charset=UTF-8

Next - Exploitation

On a hunch, I decided to check Exploit-DB for the "X-Powered-By:" Entry - PHP/8.1.0-dev
The first entry for PHP 8.1.0-dev is a User-Agentt Remote Code Execution. This seemed like something worth checking out! (https://www.exploit-db.com/exploits/49933)

This exploit contains a python script that gives us access to a backdoor and provides us with a shell on the host - by sending the User-Agentt header. I copied this code to a file on my machine called exploit.py, and ran the file with:
python3 exploit.py

The script asks us for the full host URL, in my case:
http://10.10.219.18/ (don't forget the http:// or it won't work properly)

Hitting enter, I was granted a very basic shell which I tried to upgrade with
python3 -c 'import pty; pty.spawn("/bin/bash")'

However this failed, so I just proceeded with normal enumeration.

$ whoami
root – (No PrivEsc needed here!)

$ pwd
/var/www/html

$ ls
404.html
…
vendor

This showed me nothing interesting, so I tried to navigate to the / drive

```
$ cd /

$ pwd
/var/www/html
```

Finally - Post Exploitation

Being unable to traverse drives, I changed tact and decided to just search for any files containing the word flag in the name.

```
$ find / -name *flag*
/proc/sys/kernel/acpi_video_flags
...
/flag.txt
```

This showed me flag.txt, so I opened it with

```
$ cat /flag.txt
```

And that's it!

I know this is the most basic walkthrough imaginable - no pictures or anything. It's the first one I've ever written, and I plan on learning more about GitHub and will be upgrading my walkthrough quality as time goes on. However, if this helps you, I'm glad! I had a lot of fun with this room, and although I'm really new to the Cyber Security and Hacking world, I found I was able to do this room quite quickly without any real issues (on my first run through, I modified the exploit script a few times before realising it could be run without any modification at all.)
This room really reinforced some basics for me: mainly, check anything unusual-looking for known exploits. PHP 8.1.0-dev just sounds like something exploitable, however in other situations it might not be quite so obvious, so trial and error can really pay off. Also, Burp Suite is a great tool if you have to analyse a website. It should be a go-to option straight away. I definitely recommend this room for anyone at beginner level, to just reinforce the absolute basics of exploiting a vulnerable machine.

Until next time.

Cheers!