TryHackMe - Year of the Rabbit 🐇

1. Starting Off

I connected to the machine using the IP address provided in the task.

---

2. Scanning the Target

I started with an Nmap scan:

```
nmap -sV -sC <IP>
```

Only port 80 (HTTP) was open. So I opened it in the browser and saw a website saying “Year of the Rabbit.”

---

3. Enumerating the Website

There wasn’t much on the main page, so I ran **gobuster** to find hidden directories:

```
gobuster dir -u http://<IP> -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

I found a few interesting directories:

- `/assets/`
- `/images/`
- `/r`
- `/rabbit`
- `/hidden/`

---

4. Digging Deeper

Inside `/r` and `/rabbit`, I found a message that hinted at hidden users and possible credentials.

In the `/hidden/` directory, there was a file called `.htpasswd` and `.htaccess`. These are usually used to protect directories with usernames and passwords.

---

5. Cracking the Password

I copied the hash from `.htpasswd` and used **john** to crack it:

```
john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

It gave me the password: `pinkfluffyunicorns`

---

6. Logging In

I went back to the `/hidden/` folder, entered the username (found earlier in one of the directories) and the cracked password. I got access to a note mentioning another user: `cronos`.

There was also a hidden folder containing a private SSH key.

---

7. SSH Access

I saved the key and set the right permissions:

```
chmod 600 id_rsa
ssh -i id_rsa cronos@<IP>
```

I got access to the machine!

---

8. Privilege Escalation

Once inside, I looked for ways to escalate my privileges. I used:

```
sudo -l
```

It showed I could run a Python script as root. I edited the script or used Python to spawn a root shell.

---

9. Got the Flag 🏁

After becoming root, I navigated to `/root` and found the final flag!