🏝️ TryHackMe - Lian_Yu Writeup

@Chris Noble

> Difficulty: Easy
>
> **IP**: `<IP>`
>
> **Skills**: Enumeration, Web Recon, Privilege Escalation

🔍 1. Nmap Scan

```
nmap -sC -sV -oN nmap.txt <IP>
Ports found:
```

- 22 (SSH)
- 80 (HTTP)

🌐 2. Web Enumeration

Visit `http://<IP>` in your browser.

🔎 Gobuster

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

Found:

- `/island`
- `/green_arrow`

- `/notes.txt`

📝 Read notes.txt

It might give hints about usernames or files to check.

🧍 3. User Discovery

Visit `/green_arrow` — it might be password-protected.

Use **Hydra** or **basic login fuzzing** if credentials are hinted:

```
hydra -l admin -P rockyou.txt <IP> http-post-form "/green_arrow:username=^USER^&password=^PASS^:Invalid"
```

🐚 4. Getting a Shell

If credentials are found, try SSH:

```
ssh <username>@<IP>
```

⚙️ 5. Privilege Escalation

Check for sudo permissions:

```
sudo -l
```

Look for:

- Sudo rights without password
- Writable scripts in `/etc`
- Cron jobs

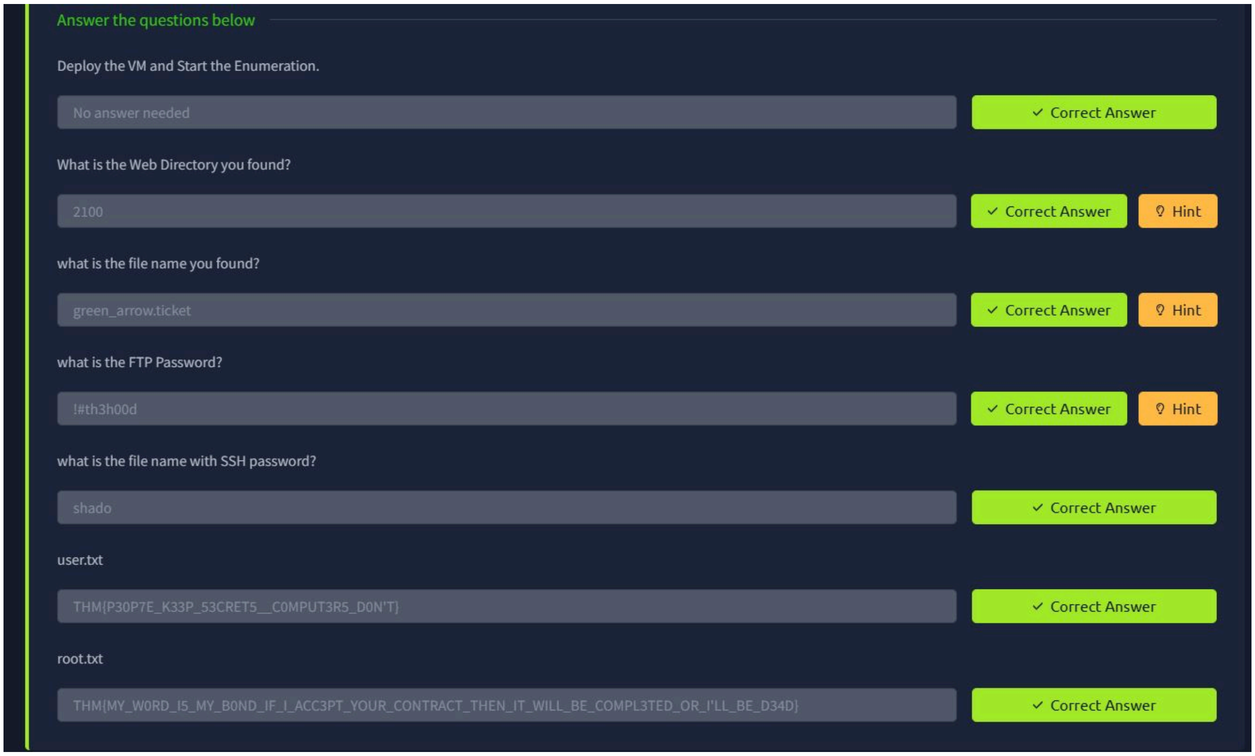
🏁 6. Capture the Flag(s)

Use `cat` to read the user and root flags:

```
cat /home/<user>/user.txt
cat /root/root.txt
```

✅ Flags

- **User flag:** 🎯 Found after login
- **Root flag:** 🎯 Found after privilege escalation



Answer the questions below

Deploy the VM and Start the Enumeration.

No answer needed

What is the Web Directory you found?

2100

what is the file name you found?

green_arrow.ticket

what is the FTP Password?

!#th3h00d

what is the file name with SSH password?

shado

user.txt

THM{P30P7E_K33P_53CRET5__C0MPUT3R5_D0N'T}

root.txt

THM{MY_W0RD_I5_MY_B0ND_IF_I_ACC3PT_YOUR_CONTRACT_THEN_IT_WILL_BE_COMPL3TED_OR_I'LL_BE_D34D}