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

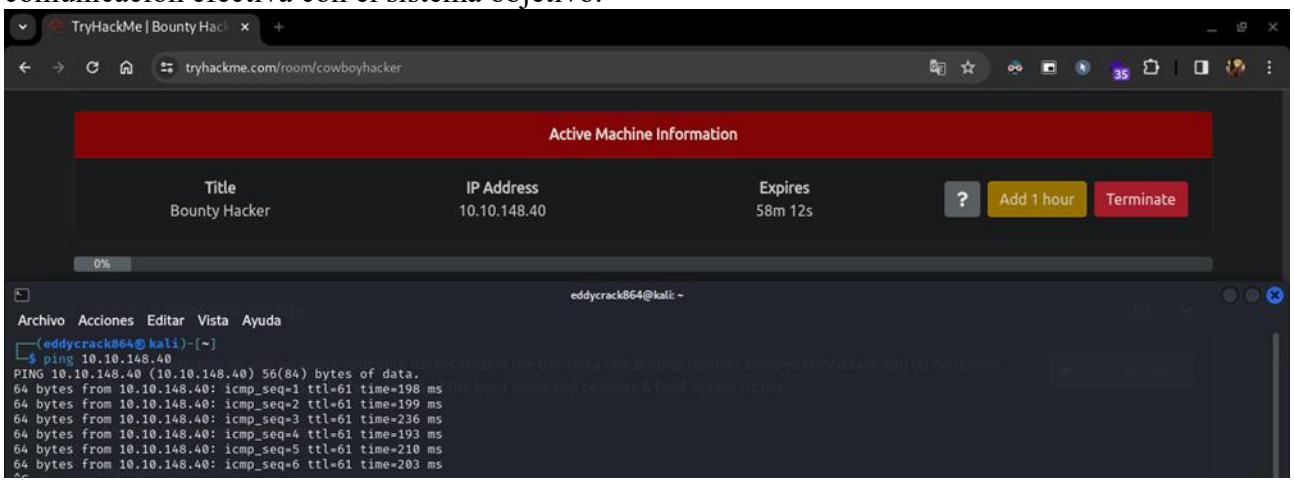
Parámetro	Descripción
-sC	Permite ejecutar scripts personalizados para obtener información adicional sobre los servicios en ejecución en el host objetivo.
-sV	Determina las versiones de los servicios que se están ejecutando en los puertos abiertos del host objetivo.

Hydra

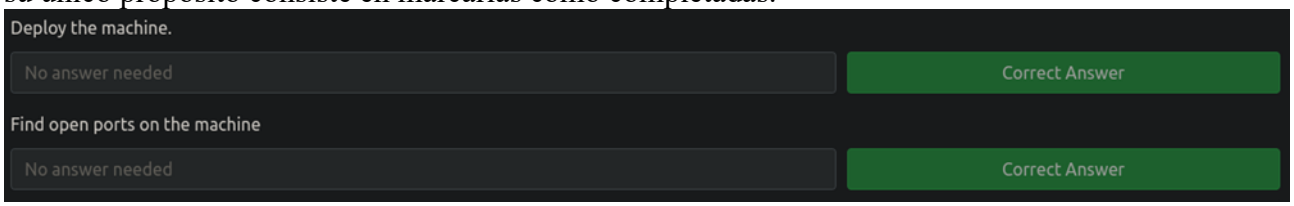
Parámetro	Descripción
-L	Se utiliza para especificar un archivo que contiene una lista de nombres de usuario
-P	Se utiliza para especificar un archivo que contiene una lista de contraseñas.

Desarrollo:

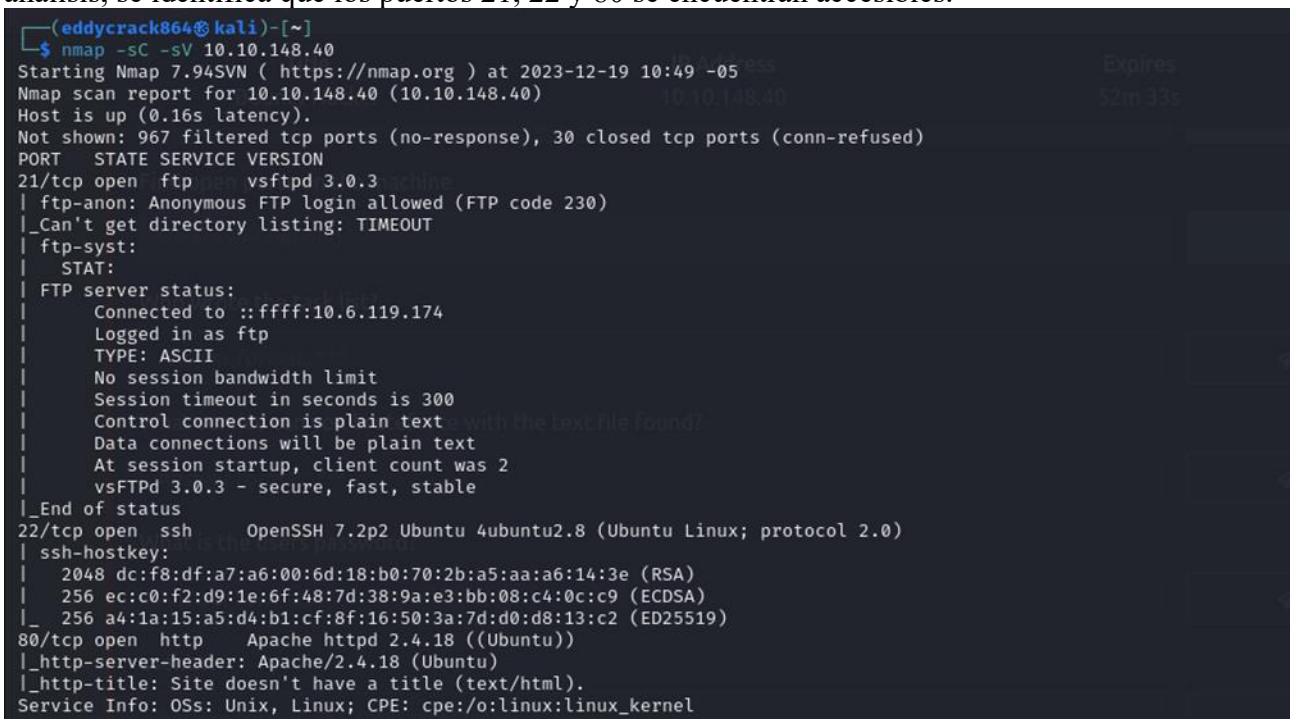
1. Se procedió a verificar la conectividad con la máquina objetivo mediante la ejecución de un comando ping dirigido a su dirección IP. Este paso inicial es fundamental para establecer la comunicación efectiva con el sistema objetivo.



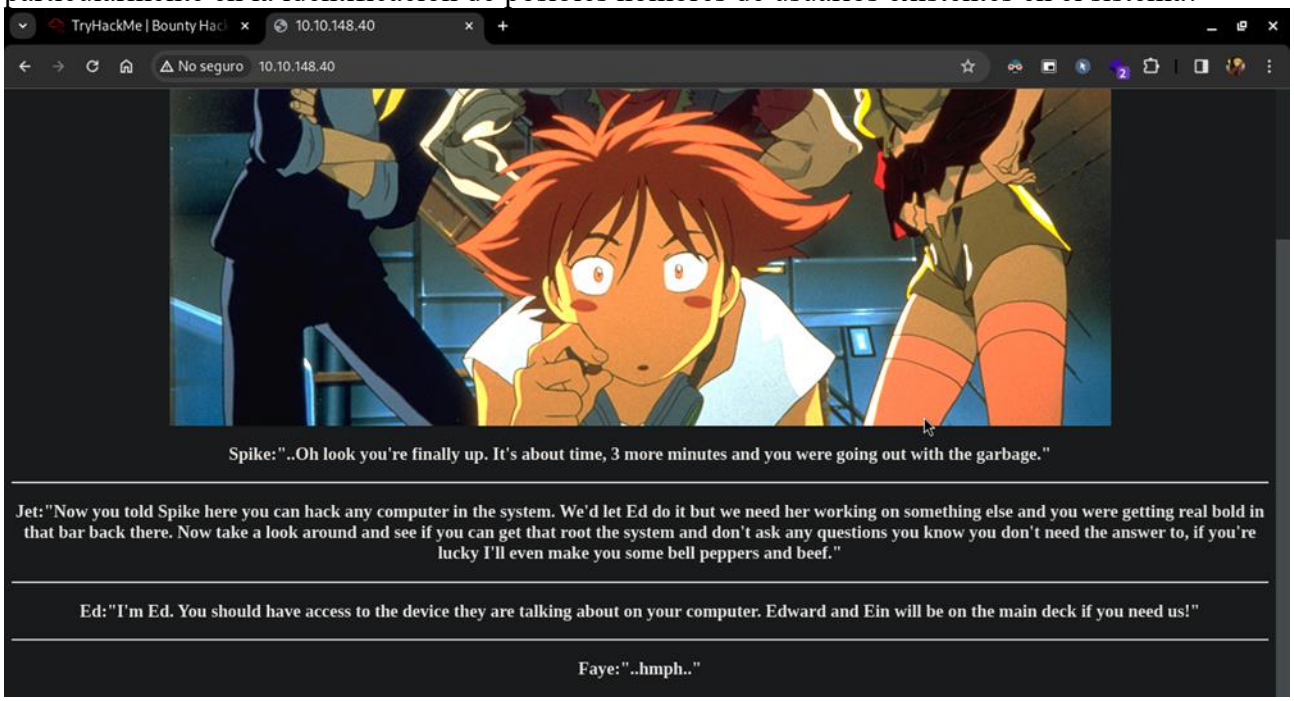
2. Las dos primeras interrogantes en la plataforma TryHackMe no requieren una respuesta sustantiva; su único propósito consiste en marcarlas como completadas.



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.

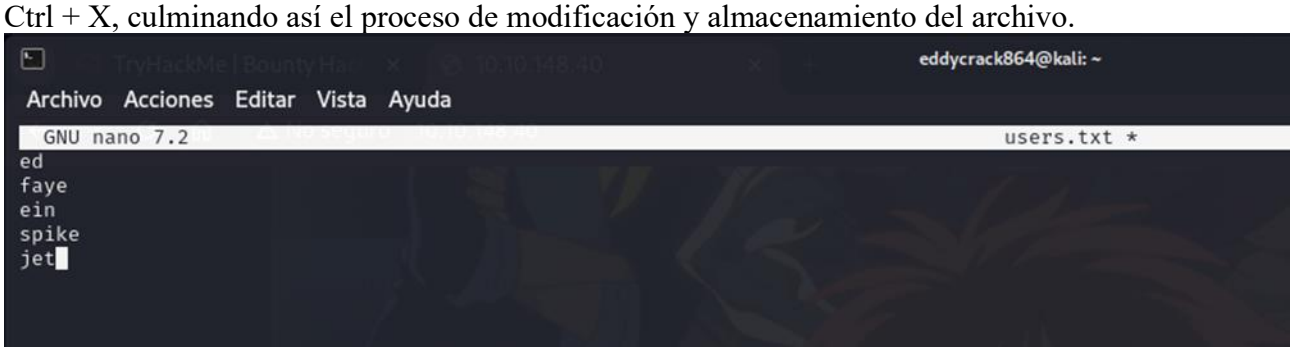


4. Subsecuentemente, se procede a la interacción con el servicio HTTP alojado en el puerto 80 mediante la introducción de la dirección IP de la máquina objetivo en el navegador web. Al efectuar este acceso, se visualiza un breve diálogo entre personajes de anime, en el cual se halla un conjunto de textos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

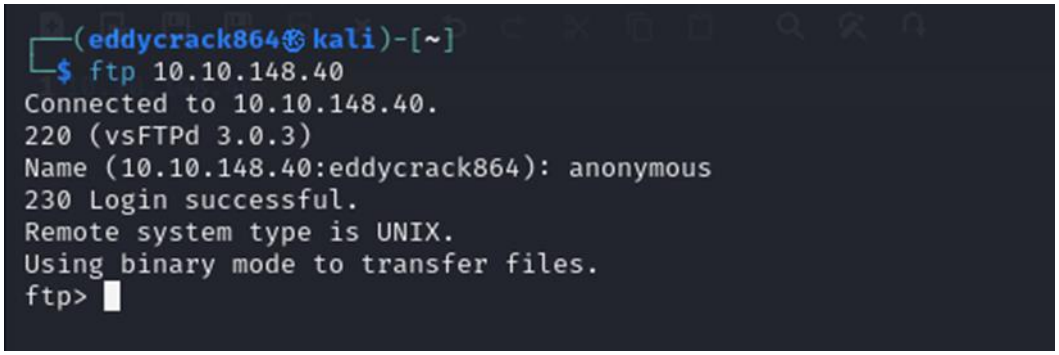


5. Posteriormente, basándose en los datos extraídos de la página web, se procede a la creación de un archivo de texto destinado a almacenar dicha información. Con tal propósito, se emplea el comando "nano" para iniciar el editor de texto y generar el archivo correspondiente.

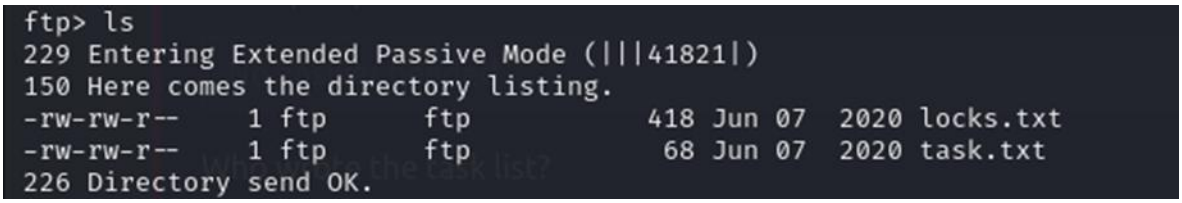
6. Dentro del entorno del editor de texto, se procede a la inclusión de los nombres previamente identificados en el diálogo mencionado. Para preservar los cambios realizados, se ejecuta la combinación de teclas Ctrl + O, seguido por la confirmación de dichos cambios mediante la tecla Enter. Posteriormente,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



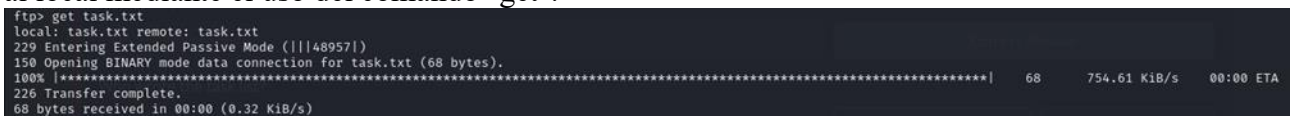
7. Como se observó durante la fase de escaneo con Nmap, se identificó que el puerto 21 correspondiente al servicio FTP permite el acceso anónimo. Aprovechando esta configuración, se procederá a la autenticación utilizando las credenciales de acceso anónimo.



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.

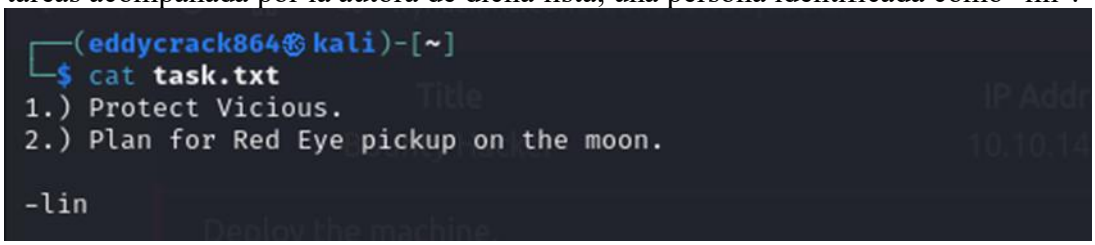


9. Subsecuentemente, se procederá a la transferencia del archivo "tasks.txt" desde el sistema remoto al local mediante el uso del comando "get".

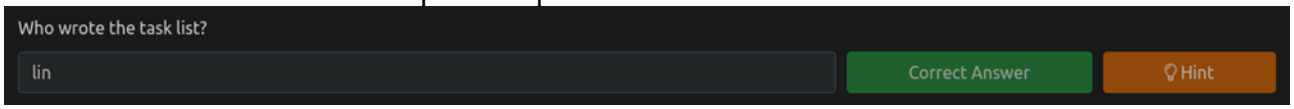


10. Se repite el procedimiento para la transferencia del archivo "locks.txt" mediante el comando "get".

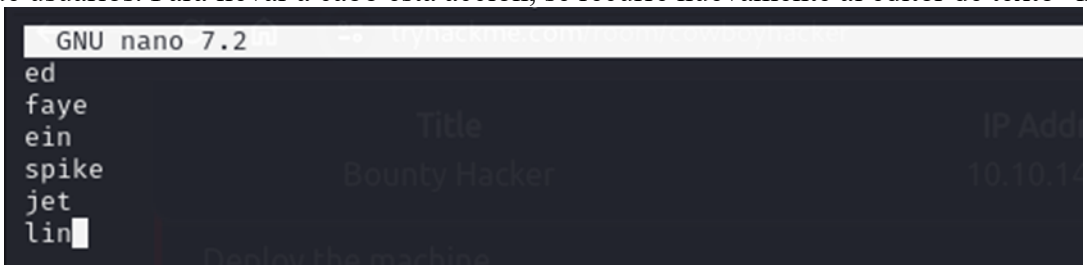
11. Una vez completada la transferencia de los archivos al entorno local, se emplea el comando "cat" para examinar el contenido del archivo "tasks.txt". Dentro de este archivo, se identifica una lista de tareas acompañada por la autora de dicha lista, una persona identificada como "lin".



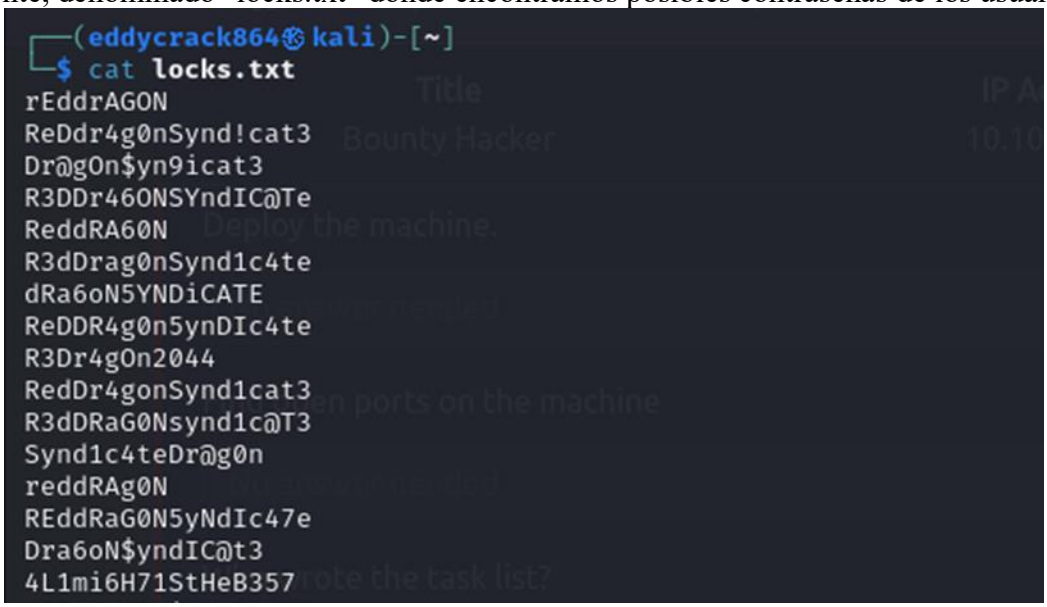
12. La lectura del archivo en el paso anterior proporciona la respuesta a la interrogante actual, relacionada con el nombre de la persona que elaboró la lista.



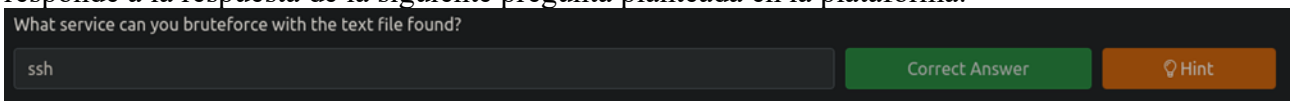
13. Se procede a la inclusión de la nueva usuaria, "lin", en el archivo de texto que contiene la lista previa de usuarios. Para llevar a cabo esta acción, se recurre nuevamente al editor de texto "nano".



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

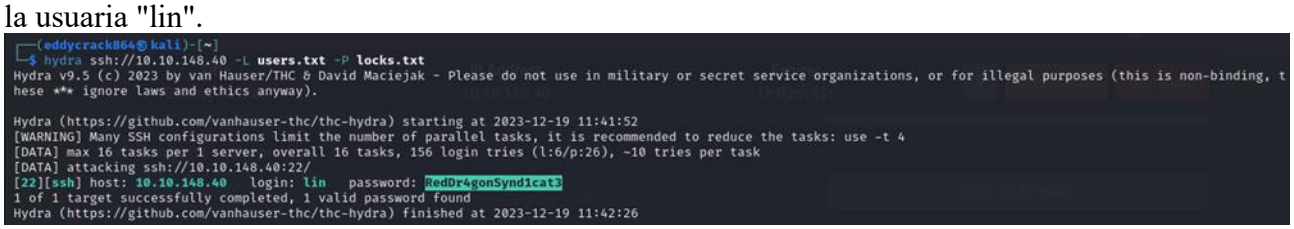


15. Con los nombres de usuario recopilados y las posibles contraseñas, se puede proceder a realizar un intento de inicio de sesión mediante fuerza bruta en el servicio SSH alojado en el puerto 22. Esto responde a la respuesta de la siguiente pregunta planteada en la plataforma.



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.

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

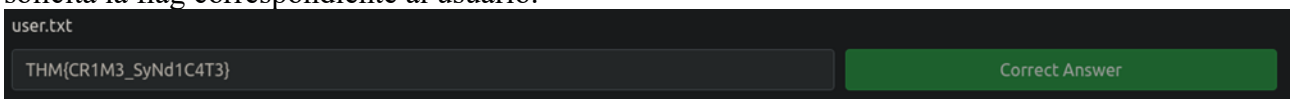


18. Con la contraseña obtenida mediante la ejecución de Hydra, se dispone ahora de la información necesaria para responder a la pregunta planteada por la plataforma.

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.

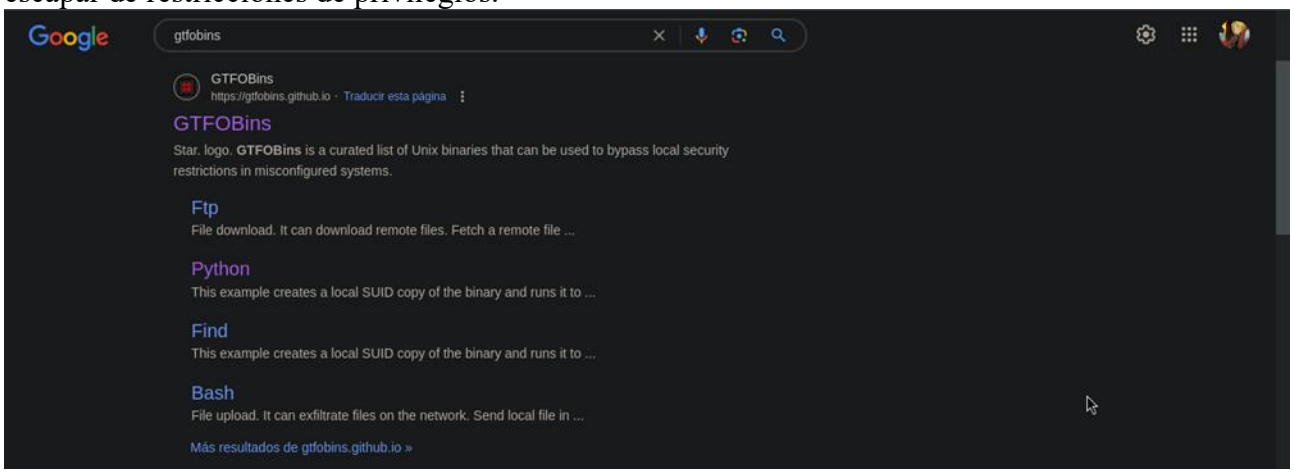
20. Una vez que se ha accedido al sistema a través de SSH utilizando las credenciales adquiridas, se procede a la exploración del escritorio. Al utilizar el comando "ls" para listar los archivos disponibles, se identifica la presencia de la primera flag denominada "user.txt". Posteriormente, se visualiza el contenido de esta flag mediante el comando "cat".
Flag: ***THM{CR1M3_SyNd1C4T3}***

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

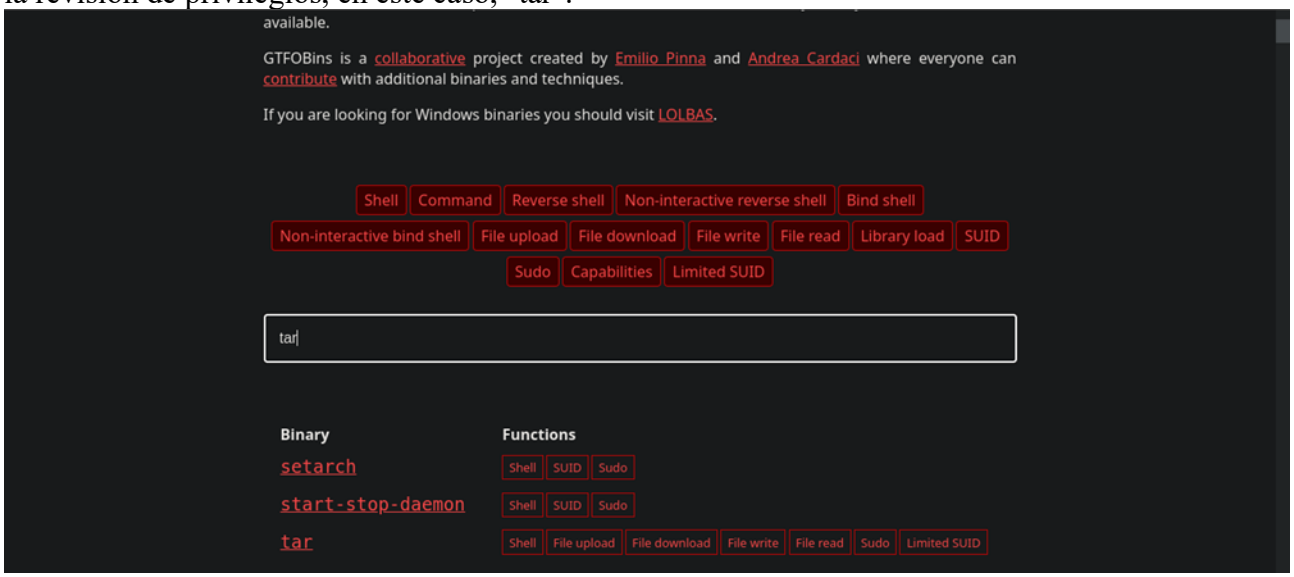


22. Posteriormente, se ejecuta el comando "sudo -l" para verificar los privilegios que el usuario posee para la ejecución de comandos con elevados privilegios. El resultado de esta operación revela que el usuario tiene la capacidad de ejecutar el comando "tar" con privilegios elevados. Cabe destacar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

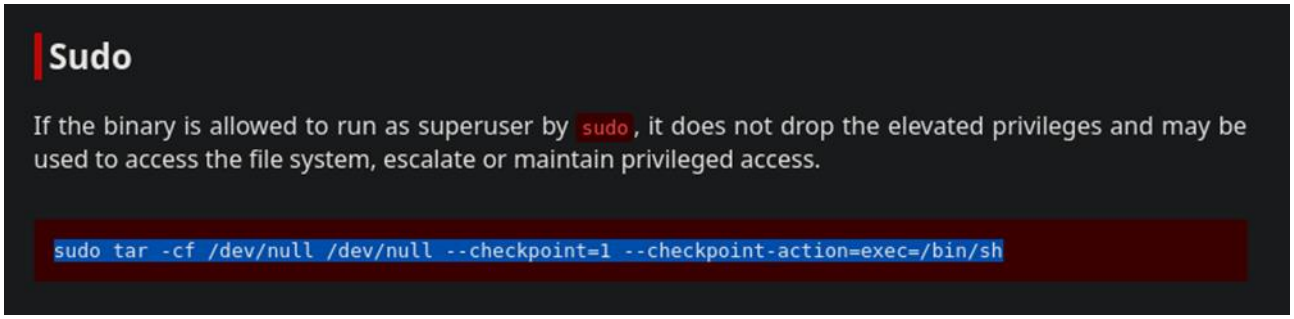
23. Con el objetivo de escalar los privilegios, se inicia la búsqueda de un binario que facilite la elevación de privilegios. Para llevar a cabo esta tarea, se realiza una consulta en la página web de GTFOBins, una fuente confiable que cataloga binarios y comandos susceptibles de ser utilizados para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



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

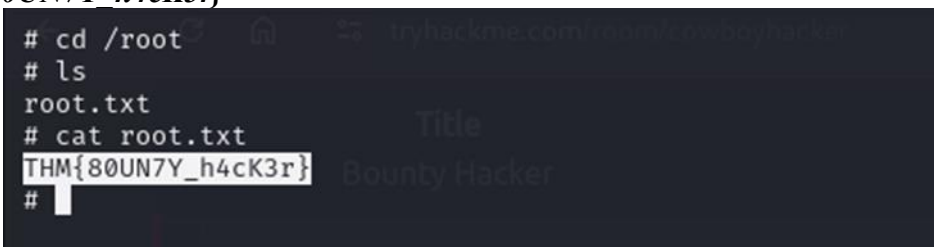


25. Dentro de la lista de binarios disponibles en GTFOBins, se procede a buscar el correspondiente al superusuario o "sudo". Una vez identificado, se copia el comando proporcionado para su ejecución en la terminal.

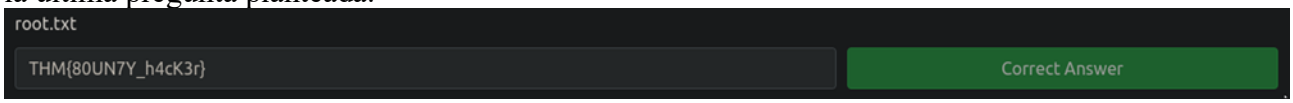


26. Tras la ejecución del comando proporcionado, se procede a verificar el usuario actual mediante la ejecución del comando "whoami". La terminal confirma que el usuario ha sido escalado exitosamente a "root".

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}***



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



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