THM – Simple CTF

Objetivo del laboratorio:

- Descubrir servicios, puertos abiertos y versiones de software.
- Utilizar una inyección SQL para obtener información crítica de la base de datos.
- Descubrir y explotar una debilidad en la configuración de Vim para escalar privilegios.

Requisitos:

- Sistema Operativo Kali Linux
- Software Gobuster

Categoría:
Web, Linux, SQL Inyection, Exploiting, 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.
cd	Se utiliza para cambiar el directorio actual, esencial para navegar por el sistema de archivos.
cat	Se utiliza para concatenar y mostrar el contenido de archivos.
ls	Lista los archivos y directorios en un directorio específico.
sudo	Se utiliza para ejecutar comandos con privilegios de superusuario o de otro usuario.

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.

Gobuster

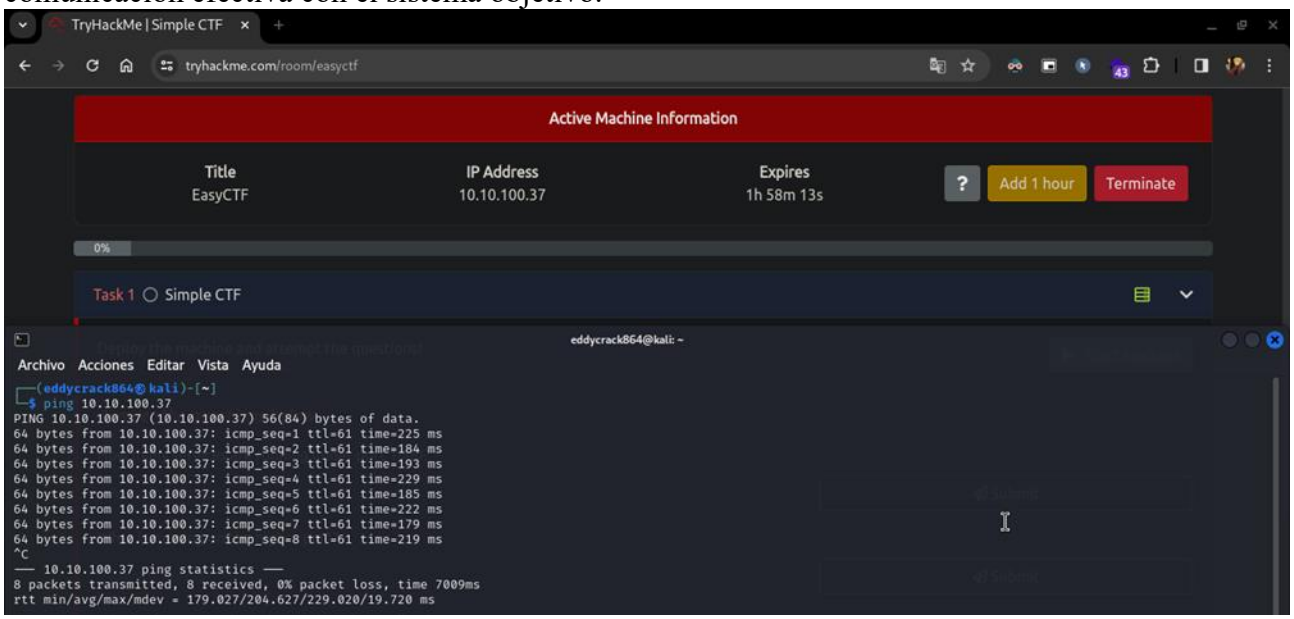
Parámetro	Descripción
-u	Se utiliza para especificar la URL de destino.
-w	Se utiliza para especificar el archivo de palabras clave o diccionario.

Hashcat

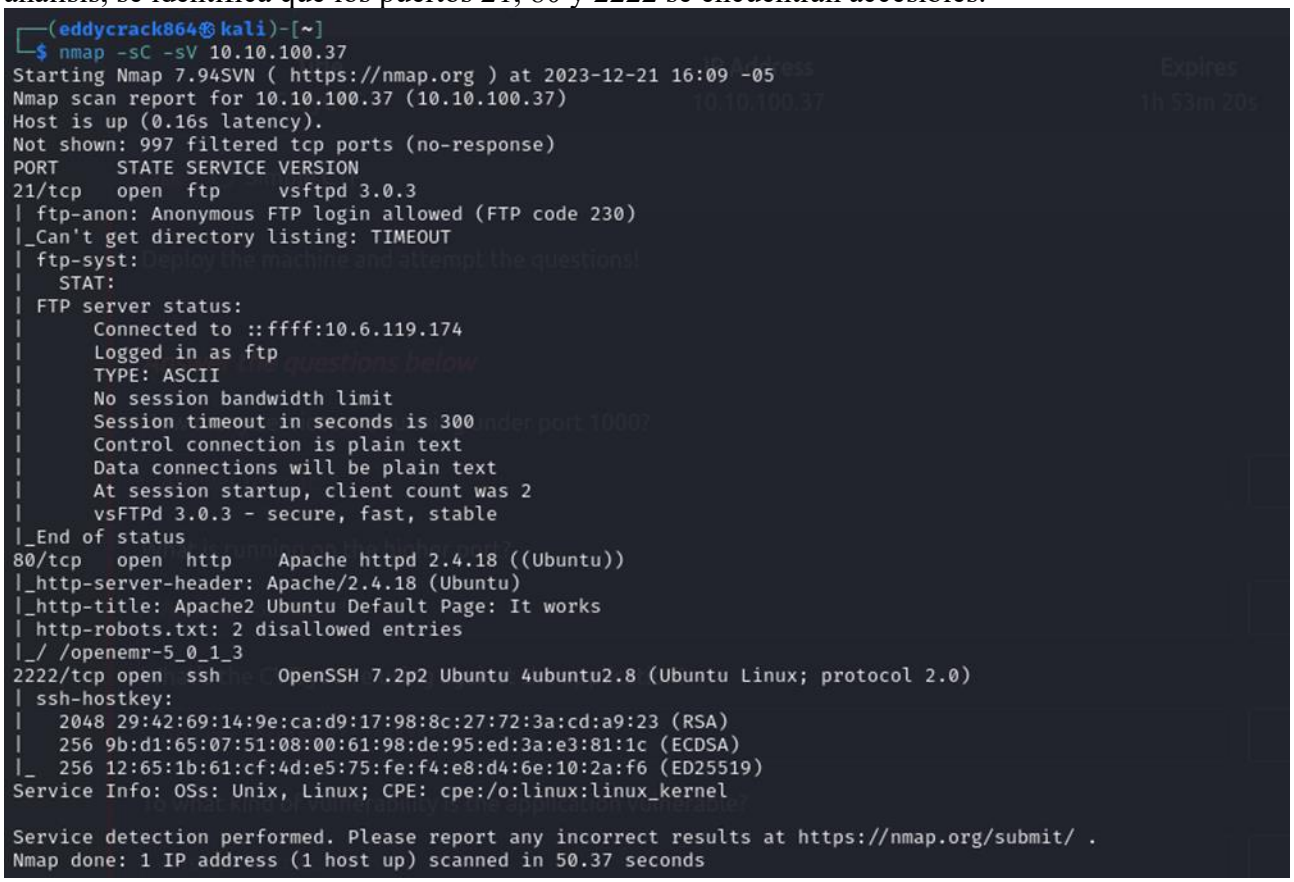
Parámetro	Descripción
-O	Se utiliza para seleccionar el modo de ataque.
-a	Se utiliza para seleccionar el algoritmo de ataque.
-m	Se utiliza para seleccionar el formato del hash.

Desarrollo:

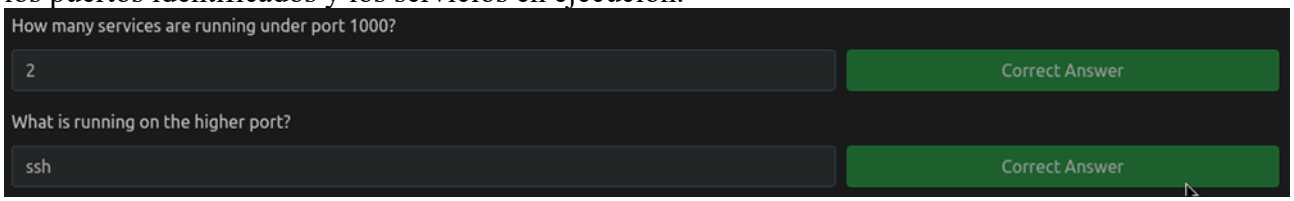
1. Se procedió a verificar la conectividad con la máquina objetivo mediante la ejecución de un comando ping dirigido a su dirección IP. Este paso inicial es fundamental para establecer la comunicación efectiva con el sistema objetivo.



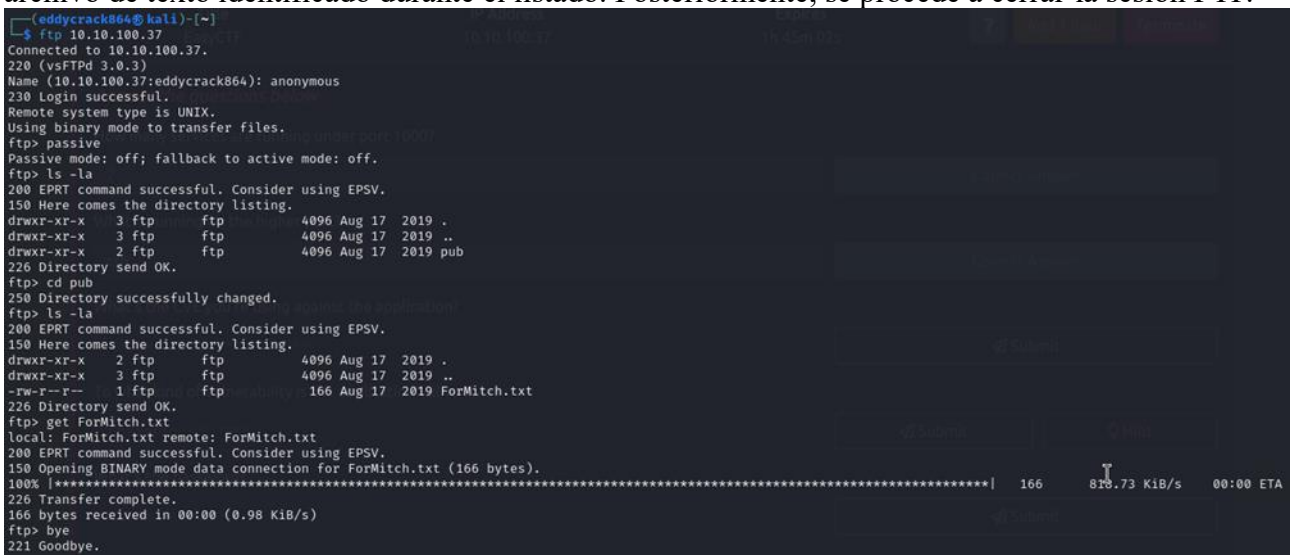
2. Se inicia el análisis mediante la aplicación de la herramienta de escaneo de red Nmap para sondear los puertos de la máquina objetivo. Se emplean los parámetros de escaneo "-sC" y "-sV" con el propósito de recabar información exhaustiva sobre los servicios en ejecución. Como resultado de este análisis, se identifica que los puertos 21, 80 y 2222 se encuentran accesibles.



3. Posterior a la ejecución del escaneo Nmap y valiéndose de la información derivada de los resultados obtenidos, se procede a abordar las interrogantes planteadas por TryHackMe en relación a los puertos identificados y los servicios en ejecución.



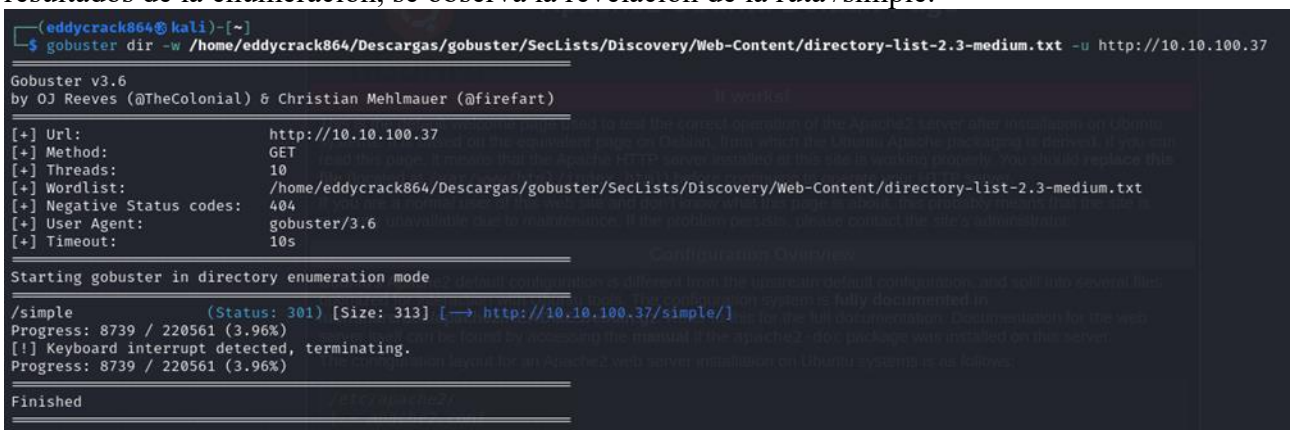
4. Dado que el escaneo Nmap reveló la habilitación del acceso anónimo en el puerto 21, se procede a ingresar a través de FTP con el objetivo de listar el contenido y realizar la transferencia de un archivo de texto identificado durante el listado. Posteriormente, se procede a cerrar la sesión FTP.



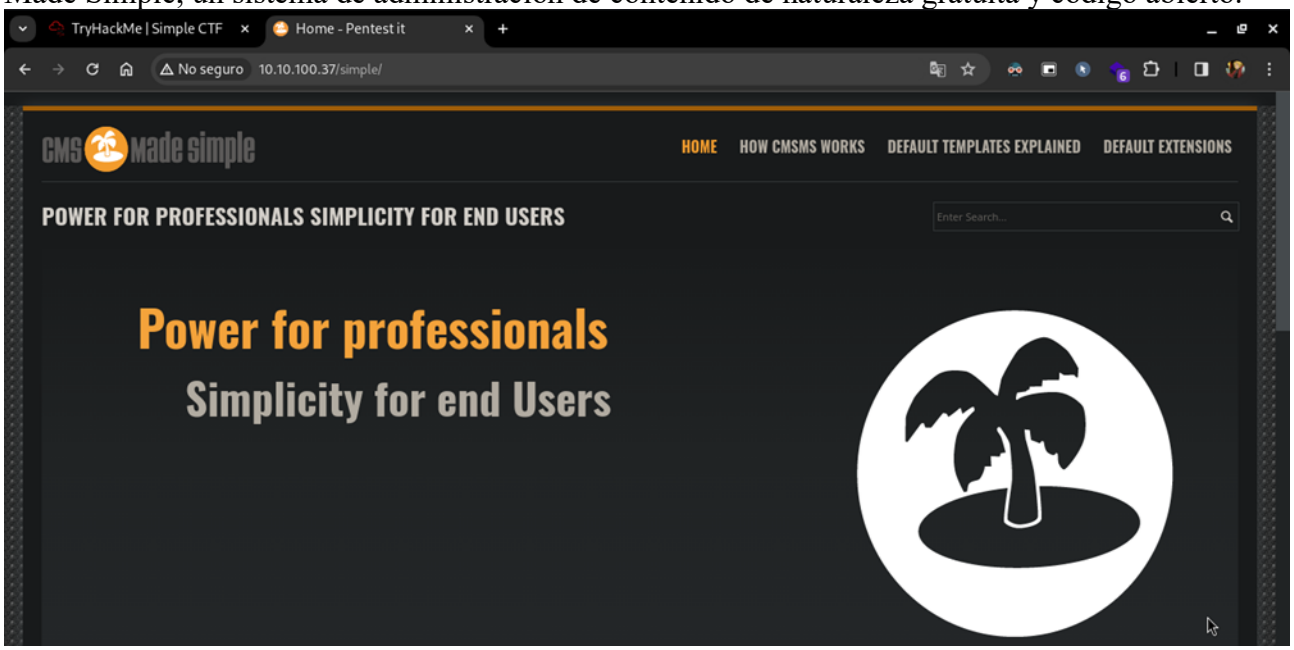
5. Ahora se procede a examinar el archivo de texto transferido mediante el comando 'cat', revelando un mensaje que señala la extraordinaria debilidad de la contraseña asociada al usuario denominado Mitch.

6. Ahora se procede a introducir la dirección IP de la máquina objetivo en el navegador. Dado que el puerto 80 se encuentra habilitado, se visualiza la página por defecto de Ubuntu; no obstante, esta exploración inicial no aporta indicios sustanciales para avanzar en el análisis.

7. Dado que no se obtuvieron indicios significativos al explorar la página web principal, se opta por realizar una enumeración de directorios mediante la herramienta Gobuster. Se configura la herramienta con el diccionario correspondiente y la dirección IP objetivo como parámetros. En los resultados de la enumeración, se observa la revelación de la ruta /simple.

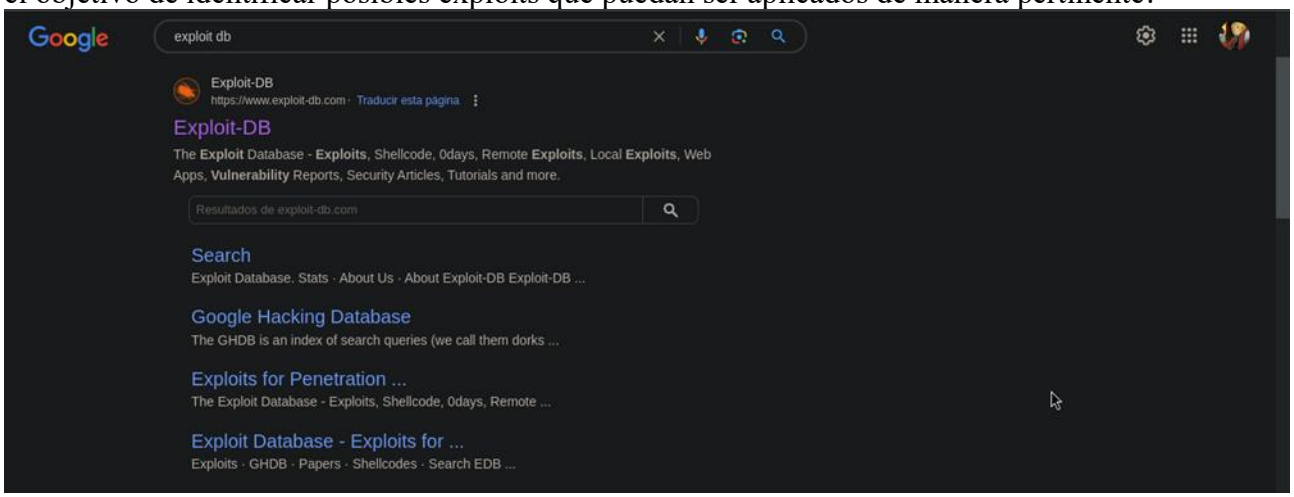


8. Una vez se accede a la ruta previamente descubierta, se visualiza una página web que utiliza CMS Made Simple, un sistema de administración de contenido de naturaleza gratuita y código abierto.

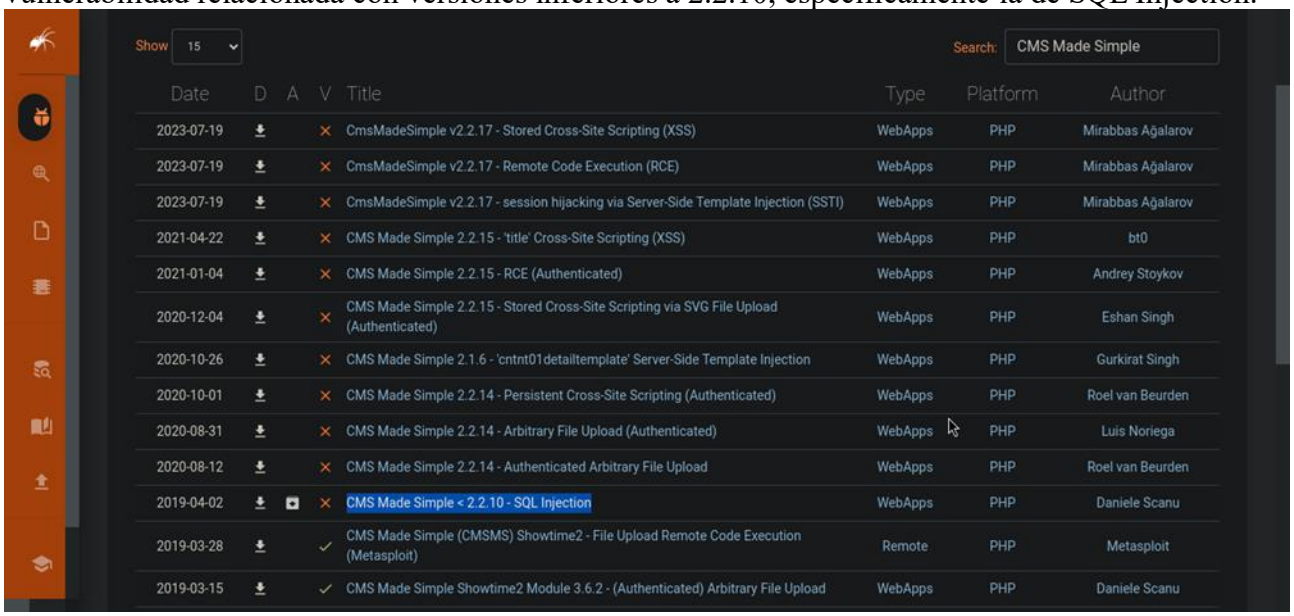


9. Al examinar el pie de página de la página web, se revelan detalles adicionales, destacando, entre ellos, el empleo de CMS Made Simple en su versión 2.2.8.

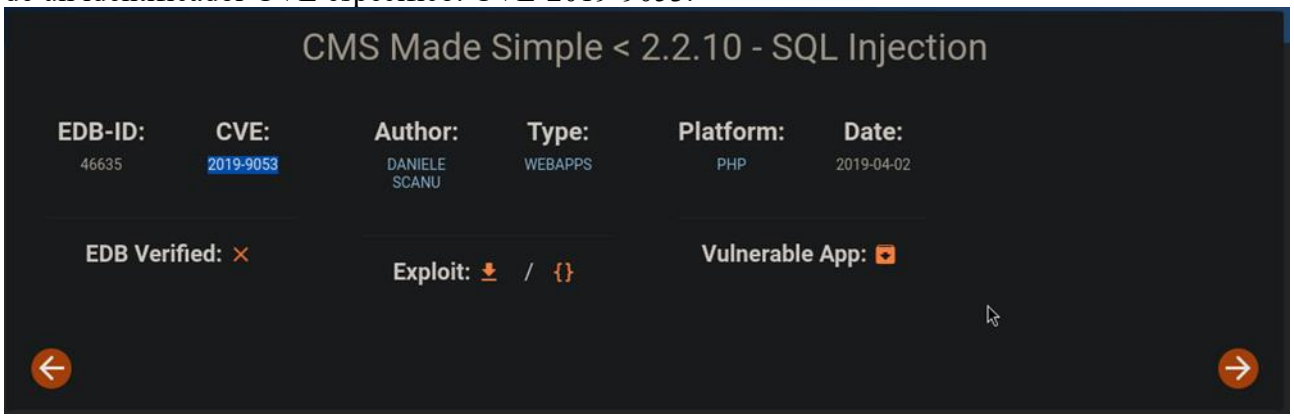
10. En esta fase, se procederá a realizar una búsqueda en la página de Exploit Database en la web con el objetivo de identificar posibles exploits que puedan ser aplicados de manera pertinente.



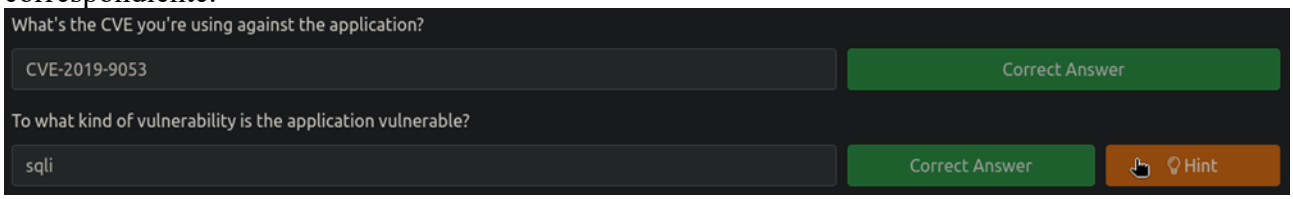
11. En la interfaz de Exploit DB, se realiza una búsqueda específica para CMS Made Simple, revelando múltiples opciones de vulnerabilidades. En este contexto, se opta por explorar la vulnerabilidad relacionada con versiones inferiores a 2.2.10, específicamente la de SQL Injection.



12. Al optar por el exploit seleccionado, se accede a información detallada que incluye la asignación de un identificador CVE específico: CVE-2019-9053.

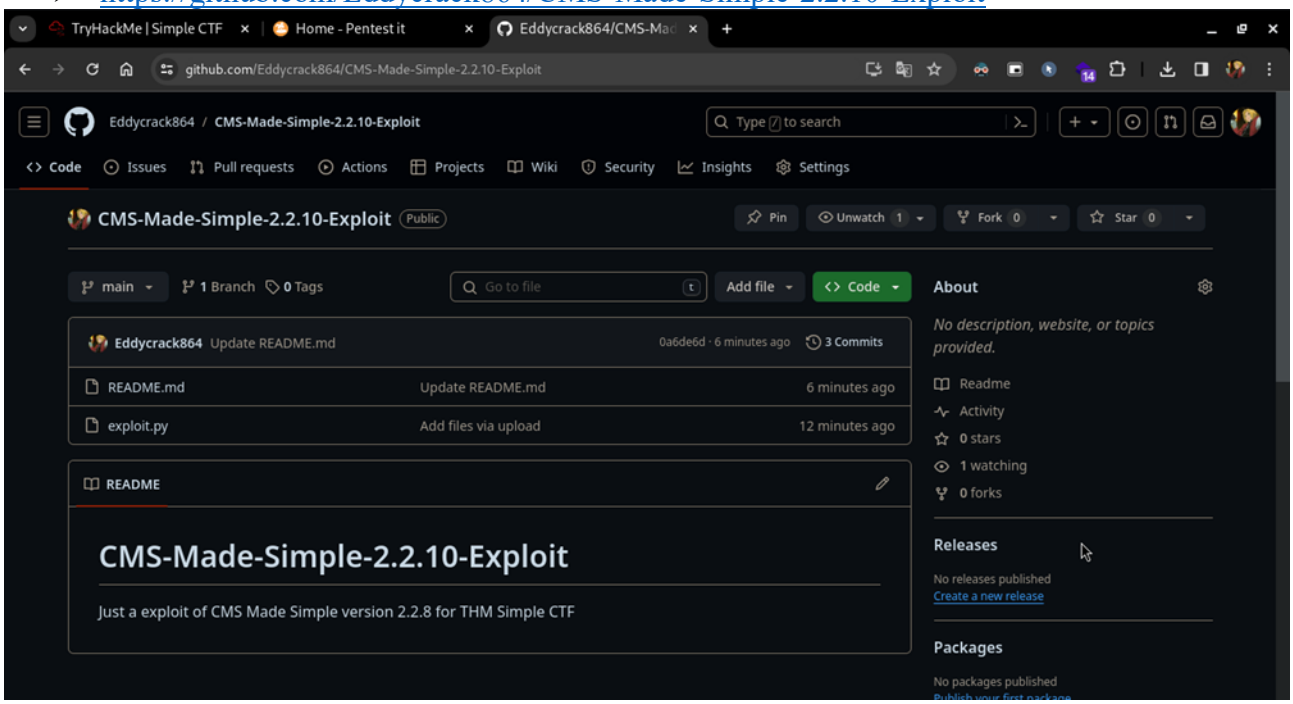


13. Con la información recopilada en Exploit DB, se está en posición de responder a las preguntas planteadas, donde se requiere proporcionar el CVE asociado y el tipo de vulnerabilidad correspondiente.

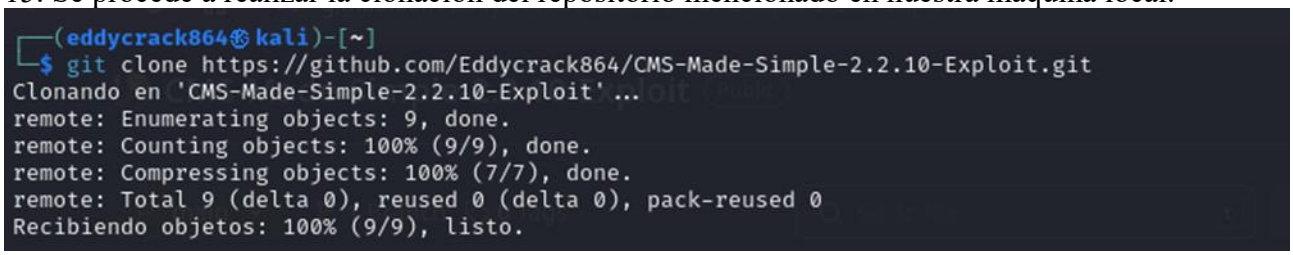


14. El exploit diseñado para aprovechar la vulnerabilidad identificada se encuentra disponible en el repositorio de GitHub con la siguiente URL:

- https://github.com/Eddycrack864/CMS-Made-Simple-2.2.10-Exploit



15. Se procede a realizar la clonación del repositorio mencionado en nuestra máquina local.



16. Una vez completada la clonación del repositorio, se procede a navegar hacia el directorio recién creado con el fin de listar su contenido y localizar el script que contiene el exploit.

17. Se procede a ejecutar el script mediante el siguiente comando, proporcionándole como parámetros la ruta de la página objetivo y el diccionario correspondiente

```
┌──(eddycrack864㉿kali)-[~/CMS-Made-Simple-2.2.10-Exploit]
└─$ python3 exploit.py -u http://10.10.100.37/simple --crack -w /usr/share/wordlists/rockyou.txt
```

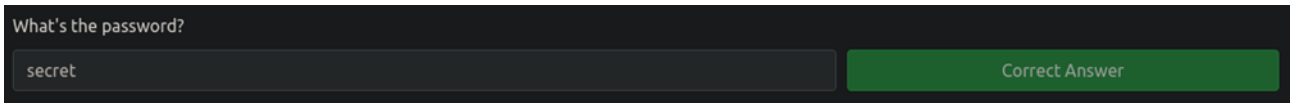
18. Al ejecutar el script, iniciará el proceso de obtención de la "sal" de la contraseña, que consiste en un conjunto de bits aleatorios utilizados como una de las entradas en una función derivadora de claves. Asimismo, el script recopilará información clave como el nombre de usuario, el correo electrónico y la propia contraseña. Es importante destacar que este procedimiento puede demandar varios minutos para su conclusión, ya que implica operaciones intensivas en términos computacionales.

```
[+] Salt for password found: 1dac0d92e9fa6bb2
[+] Username found: mitch
[+] Email found: admin@admin.com
[+] Password found: 0c01f4468bd75d7a84c7eb73846e8d96
```

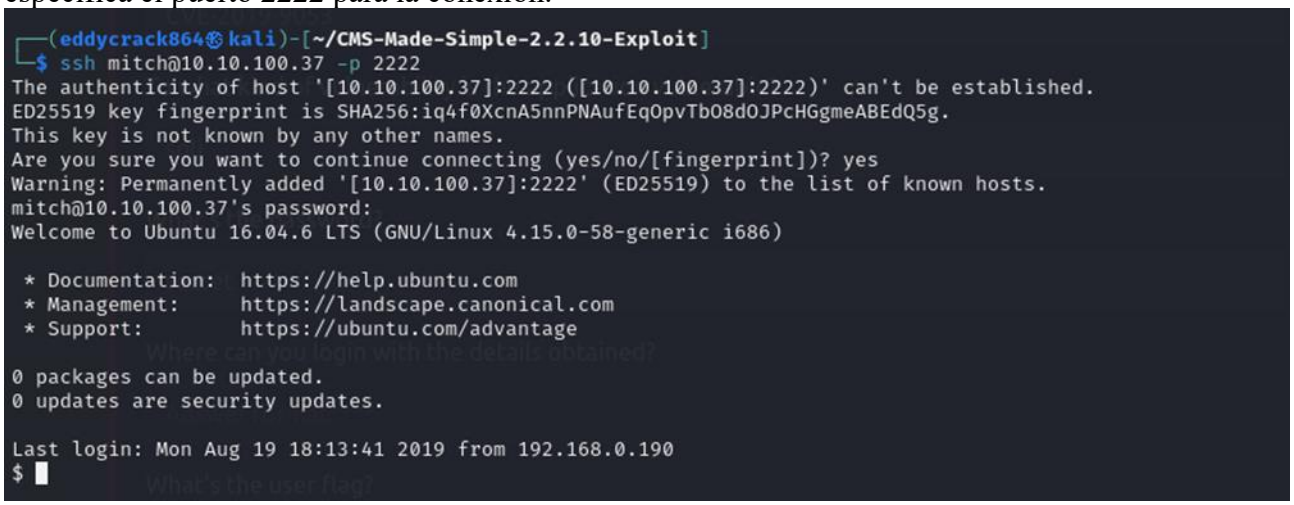
19. Con los datos adquiridos tras la ejecución del exploit, el siguiente paso implica descifrar el hash de la contraseña utilizando la "sal" identificada. Para llevar a cabo este proceso, se empleará la herramienta netcat, especificando los siguientes parámetros: El tipo de ataque, El formato del hash, el algoritmo del hash, la contraseña unida con ":" a la sal de la contraseña y finalmente especificamos el diccionario. Como resultado de esta operación se obtiene que la contraseña para el usuario Mitch es "secret."

```
┌──(eddycrack864㉿kali)-[~/CMS-Made-Simple-2.2.10-Exploit]
└─$ hashcat -O -a 0 -m 20 0c01f4468bd75d7a84c7eb73846e8d96:1dac0d92e9fa6bb2 /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i3-2120 CPU @ 3.30GHz, 1402/2868 MB (512 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 31
Minimim salt length supported by kernel: 0
Maximum salt length supported by kernel: 51

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Precompute-Init
* Early-Skip
* Not-Iterated
* Prepended-Salt
* Single-Hash
* Single-Salt
* Raw-Hash

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

0c01f4468bd75d7a84c7eb73846e8d96:1dac0d92e9fa6bb2:secret
```

20. Con la conclusión exitosa del proceso de descifrado del hash de la contraseña, se está en posición de responder a la pregunta planteada por la plataforma, la cual requiere la introducción de la contraseña revelada.

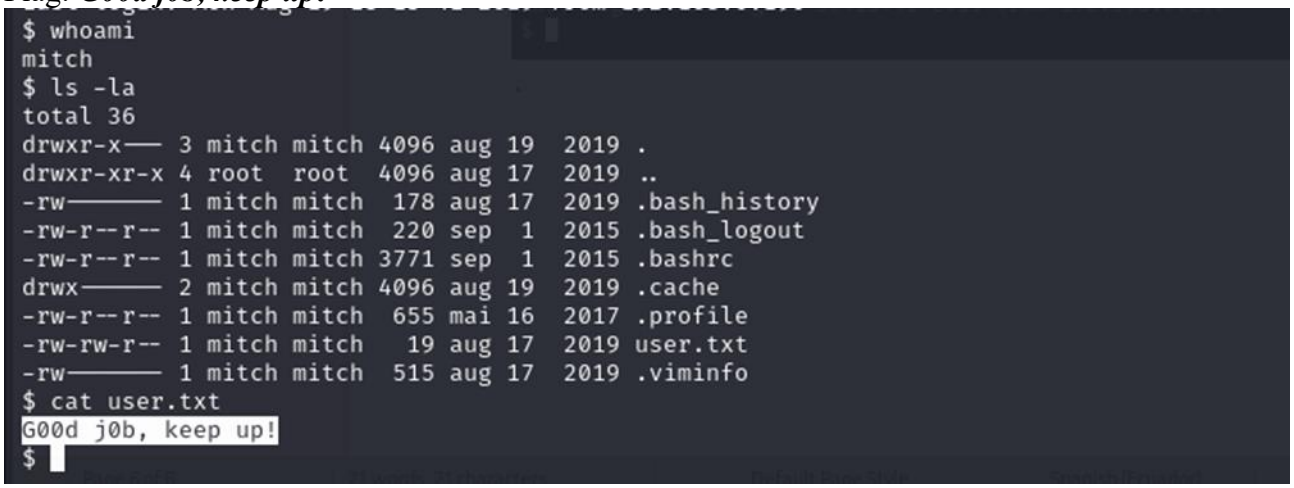


21. Con las credenciales descifradas en nuestro poder, ahora se procede a iniciar sesión a través de SSH utilizando el nombre de usuario y la contraseña correspondientes al usuario "Mitch". Se especifica el puerto 2222 para la conexión.

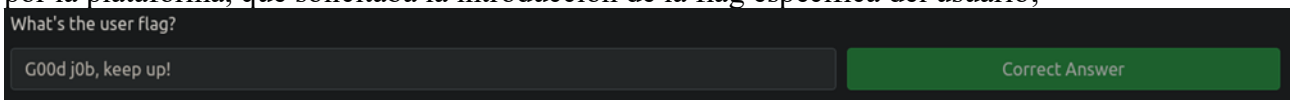


22. Posterior a la exitosa autenticación mediante SSH con las credenciales de "Mitch", se procede a verificar el nombre de usuario actual mediante el comando "whoami". Con la confirmación de que se ha ingresado como "Mitch", se procede a listar el contenido del directorio actual mediante el comando "ls". Este paso revela la presencia de la flag del usuario en dicho directorio, y para visualizar su contenido, se utiliza el comando "cat".

Flag: ***G00d j0b, keep up!***



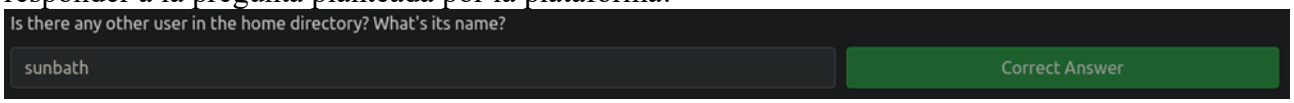
23. Con la exitosa visualización de la flag del usuario se procede responder a la pregunta formulada por la plataforma, que solicitaba la introducción de la flag específica del usuario,



24. La exploración del directorio /home revela la presencia de otro usuario en el sistema.

```
$ cd /home
$ ls -la
total 16
drwxr-xr-x  4 root    root    4096 aug 17  2019 .
drwxr-xr-x 23 root    root    4096 aug 19  2019 ..
drwxr-x---  3 mitch   mitch   4096 aug 19  2019 mitch
drwxr-x--- 16 sunbath sunbath 4096 aug 19  2019 sunbath
$
```

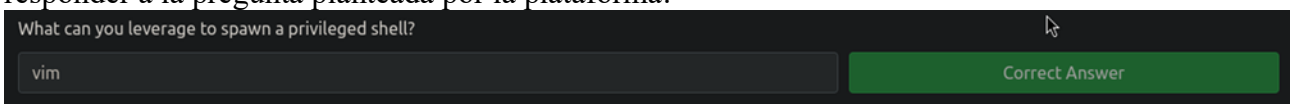
25. Con la identificación de este nuevo usuario en el directorio /home, se está en posición de responder a la pregunta planteada por la plataforma.



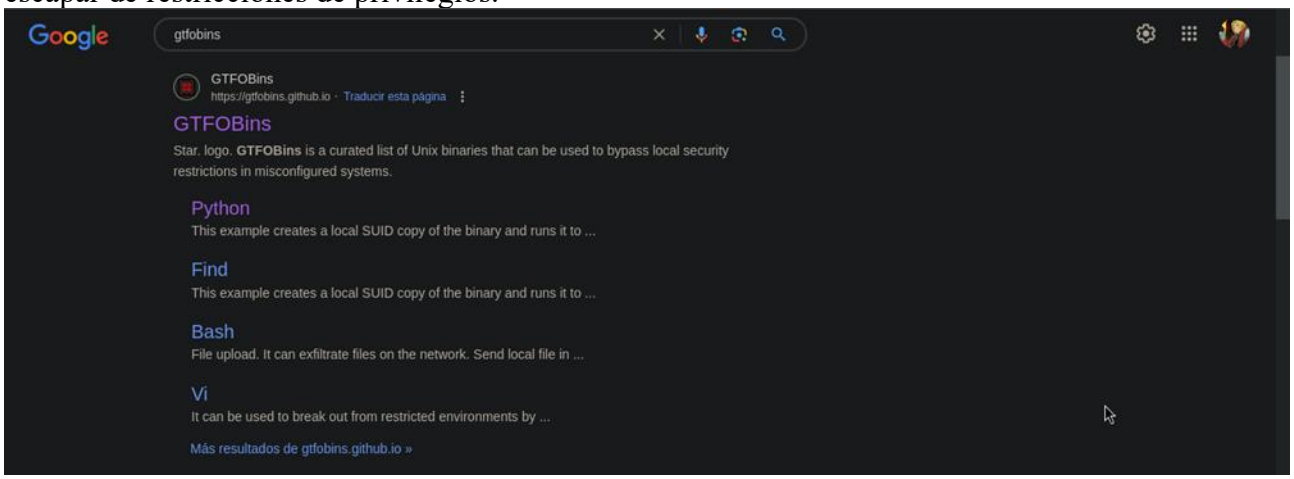
26. Al ejecutar el comando sudo -l, se obtendrá una lista de los comandos que el usuario actual tiene permitido ejecutar como root sin necesidad de ingresar una contraseña, en este caso se tiene acceso a la ejecución de vim.

```
$ sudo -l
User mitch may run the following commands on Machine:
    (root) NOPASSWD: /usr/bin/vim
$
```

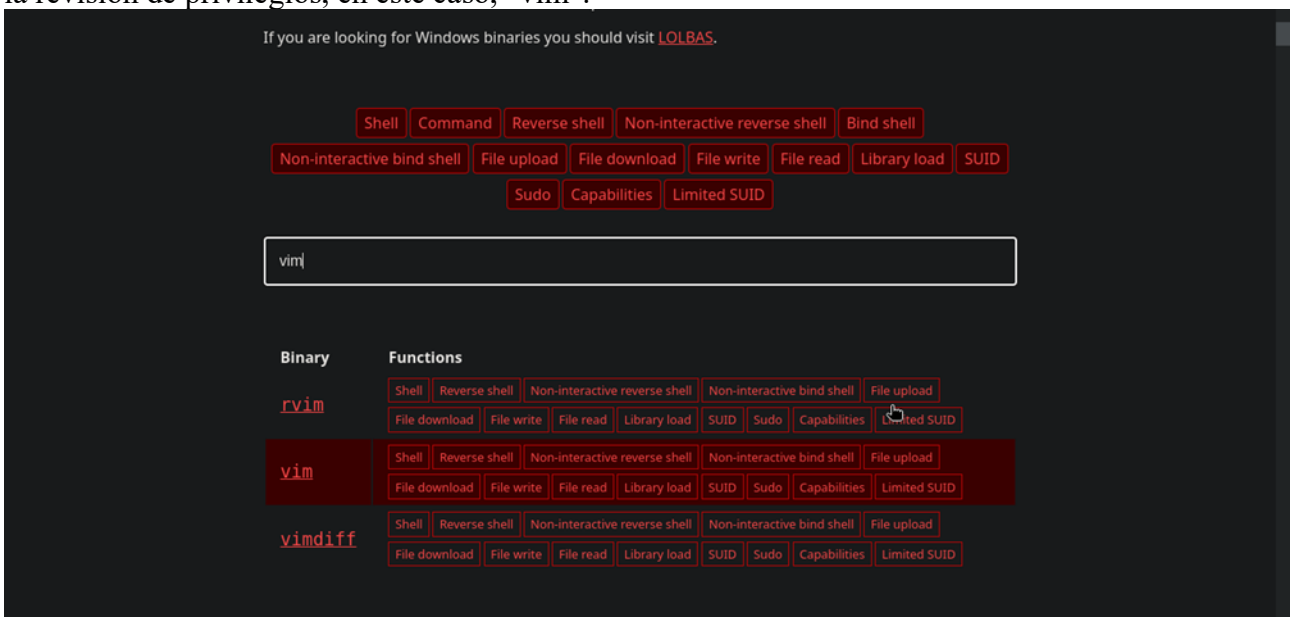
27. Al descubrir que existe la posibilidad de escalar privilegios mediante el uso de Vim, se puede responder a la pregunta planteada por la plataforma.



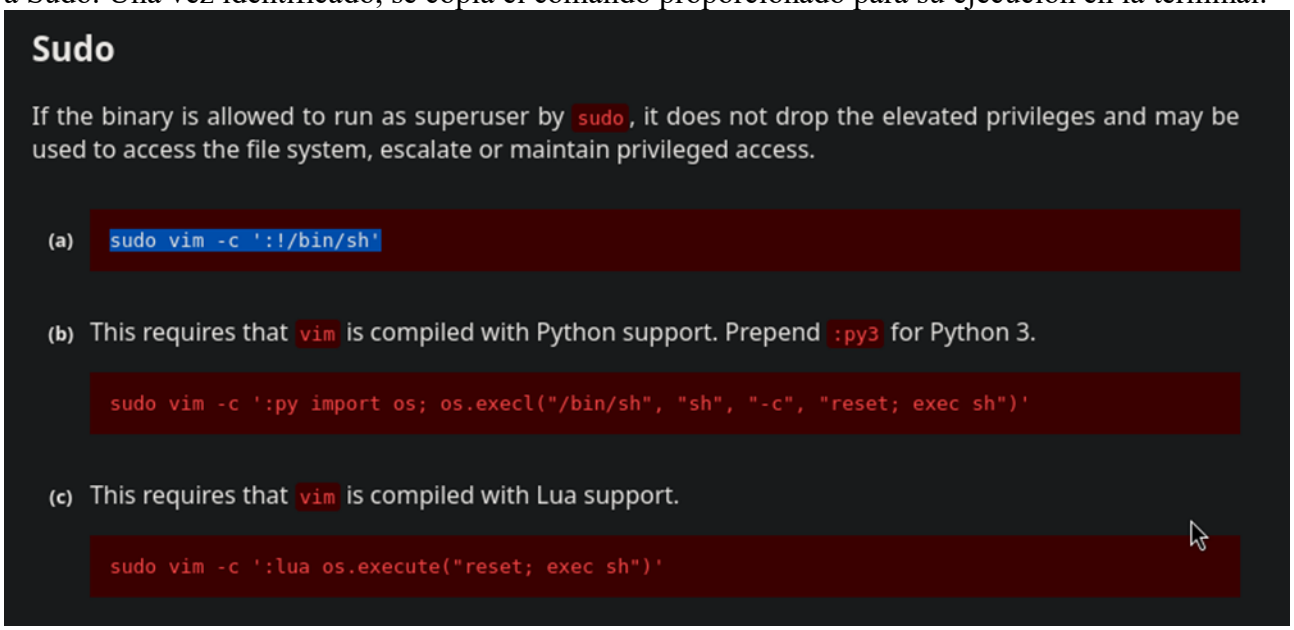
28. Con el objetivo de escalar los privilegios, se inicia la búsqueda de un binario que facilite la elevación de privilegios. Para llevar a cabo esta tarea, se realiza una consulta en la página web de GTFOBins, una fuente confiable que cataloga binarios y comandos susceptibles de ser utilizados para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



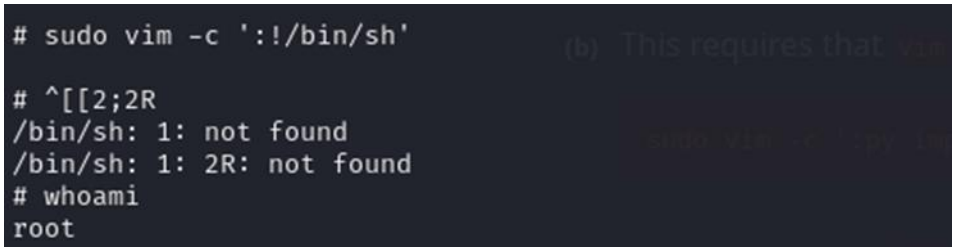
29. En la página de GTFOBins, se realiza una búsqueda específica del comando que surgió durante la revisión de privilegios, en este caso, "vim".



30. Dentro de la lista de binarios disponibles en GTFOBins, se procede a buscar el correspondiente a Sudo. Una vez identificado, se copia el comando proporcionado para su ejecución en la terminal.



31. Al ejecutar el comando en la terminal, es normal observar errores de "comando no encontrado". Este comportamiento es esperado y se debe a la ejecución de Vim en modo shell interactivo. Después de presionar Enter, se puede proceder a ejecutar el comando whoami para verificar que ahora se tiene el estatus de usuario root.



32. Después de escalar los privilegios y convertirse en el usuario root, se procede a moverse al directorio /root y listar su contenido. A continuación, se visualiza el contenido de la flag del usuario root utilizando el comando cat.
Flag: ***W3ll d0n3. You made it!***

```
# cd /root
# ls -la
total 28
drwx------  4 root root 4096 aug 17  2019 .
drwxr-xr-x 23 root root 4096 aug 19  2019 ..
-rw-r--r--  1 root root 3106 oct 22  2015 .bashrc
drwx------  2 root root 4096 aug 17  2019 .cache
drwxr-xr-x  2 root root 4096 aug 17  2019 .nano
-rw-r--r--  1 root root  148 aug 17  2015 .profile
-rw-r--r--  1 root root   24 aug 17  2019 root.txt
# cat root.txt
W3ll d0n3. You made it!
#
```

33. Con la exitosa obtención de la flag del usuario root, se está en posición de responder a la pregunta planteada por TryHackMe que solicitaba ingresar la flag específica del usuario root.

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