Descripción

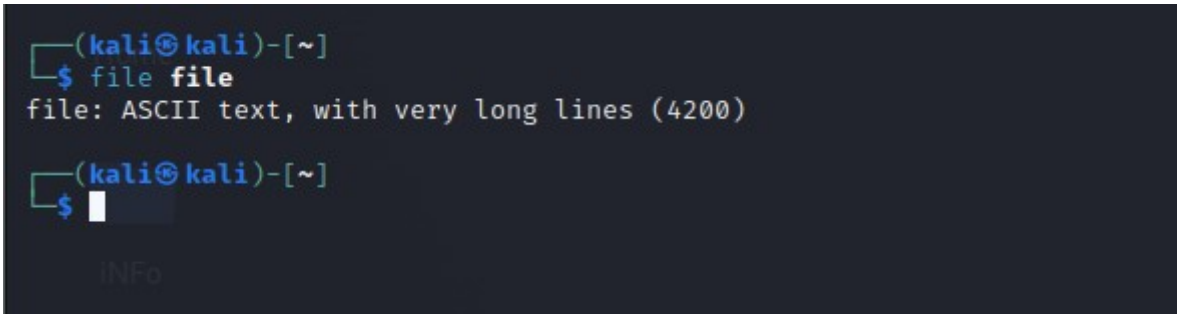
¿Puedes encontrar la bandera en el archivo? Esto sería realmente tedioso de revisar manualmente, algo me dice que hay una mejor manera.

// Este problema es de Ciberseguridad Forense, esta área de la ciberseguridad se centra en investigar y analizar incidentes cibernéticos, se involucra la recolección, preservación y análisis de pruebas.

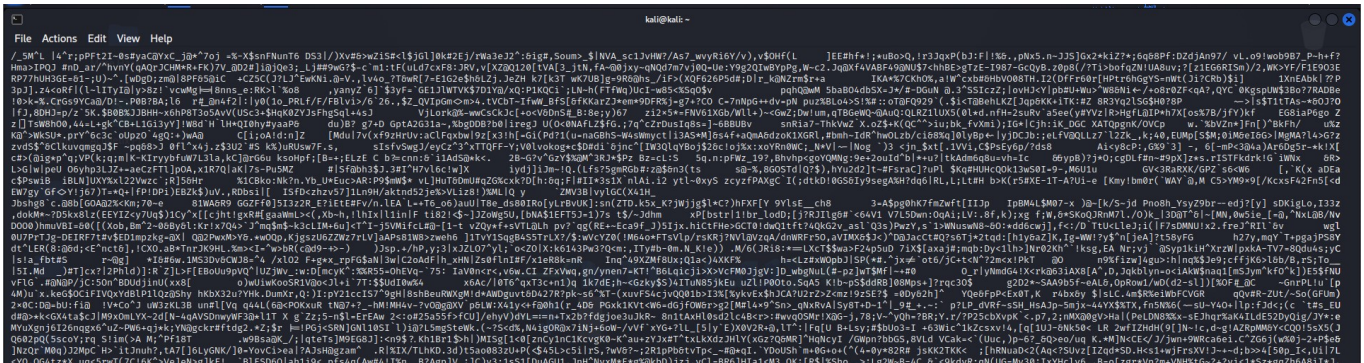
**¿Cómo resolverlo

Primero, necesitamos descargar el archivo que nos proporcionan en la descripción en nuestra shell, así que escribimos en la consola el comando "wget" (Este comando sirve para descargar archivos web en nuestra shell) seguido de la url del archivo (hacemos click derecho en el link indexado para copiarlo).

Ahora como vemos en la captura de pantalla se descargo nuestro archivo con el nombre de 'file', pero no sabemos que tipo de archivo es, el comando para saber esto es "file", así que usaremos el comando *file file* para saber que tipo de archivo es, (comprendiendo que el primer file hace referencia al comando y el segundo file al nombre del archivo que acabamos de descargar).

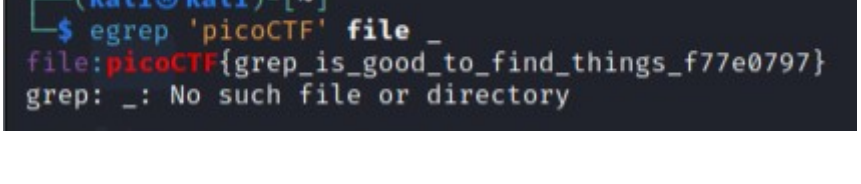


Encontramos que el archivo que acabamos de descargar es un archivo de código ASCCI y tiene una longitud de 4200 caracteres. Así que ahora tenemos que abrir el archivo, para hacer esto usaremos el comando 'cat' seguido del nombre, de esta manera "cat file".



Encontramos que efectivamente es un archivo en código ASCCI, este podría ser una practica de criptografía y tendríamos que descifrar todo el código, para tu suerte este no es el caso, ya que es una practica sencilla, entonces, ¿Qué buscamos?
Entre todo ese código se encuentra nuestra flag, pero, no vamos a buscar linea por linea, porque te aburrirías en 10 segundos, para nuestra fortuna existe un comando que nos facilita esta tarea, el comando 'egrep', este comando se utiliza para buscar o filtrar texto dentro de archivos, este texto puede ser combinado mayúsculas, minúsculas y otros caracteres, (te recomiendo investigar sobre el comando grep y sus derivados).

Así que utilizaremos el siguiente comando para buscar nuestra flag, **egrep 'picoCTF' file



¡Y listo! aquí tenemos nuestra flag, con esto abríamos terminado nuestra practica, solamente ingresando la flag 'picoCTF{grep_is_good_to_find_things_f77e0797}'