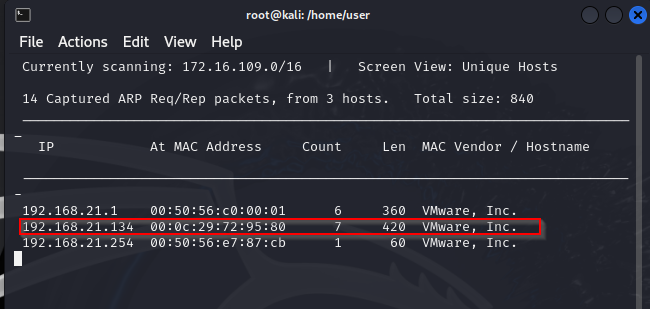
Sherlock Vulnhub Walkthrough

Primero descubriremos cual es la Ip Objetivo con netdiscover y nmap: 192.168.21.134

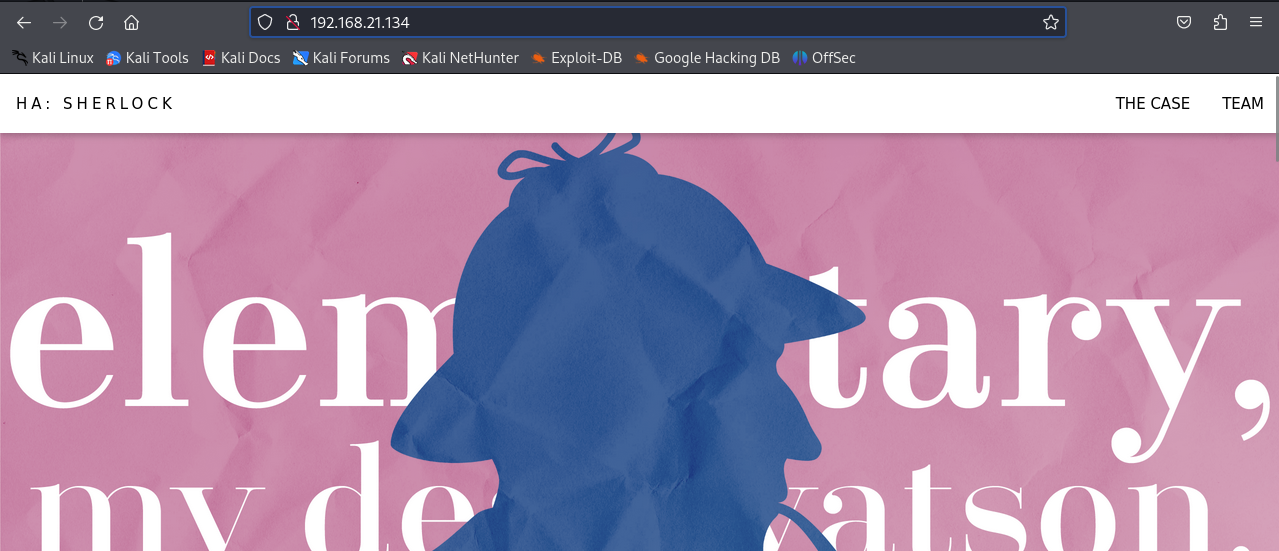


Como ya hemos obtenido la dirección IP, nuestro siguiente paso será escanear la red utilizando Nmap. Usando nmap podremos descubrir todos los puertos abiertos y servicios presentes en la máquina para poder explotarlos posteriormente. Para ello, podemos utilizar el comando: nmap –sV

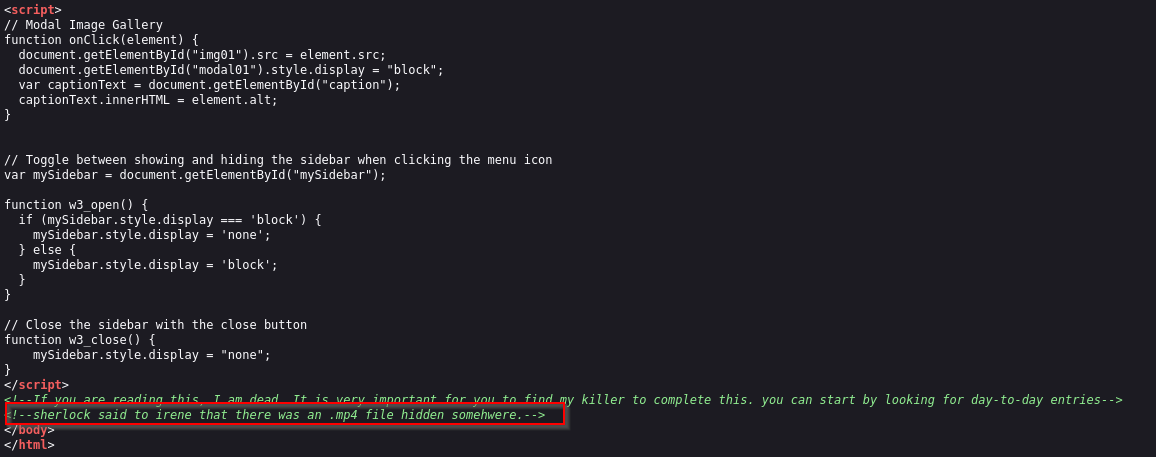


Aquí puede ver que hay múltiples servicios abiertos como ftp, ssh, SMTP, http, pop3, IMAP, SSL/IMAP, SSL/pop3, etc. y se muestran sus respectivas versiones.

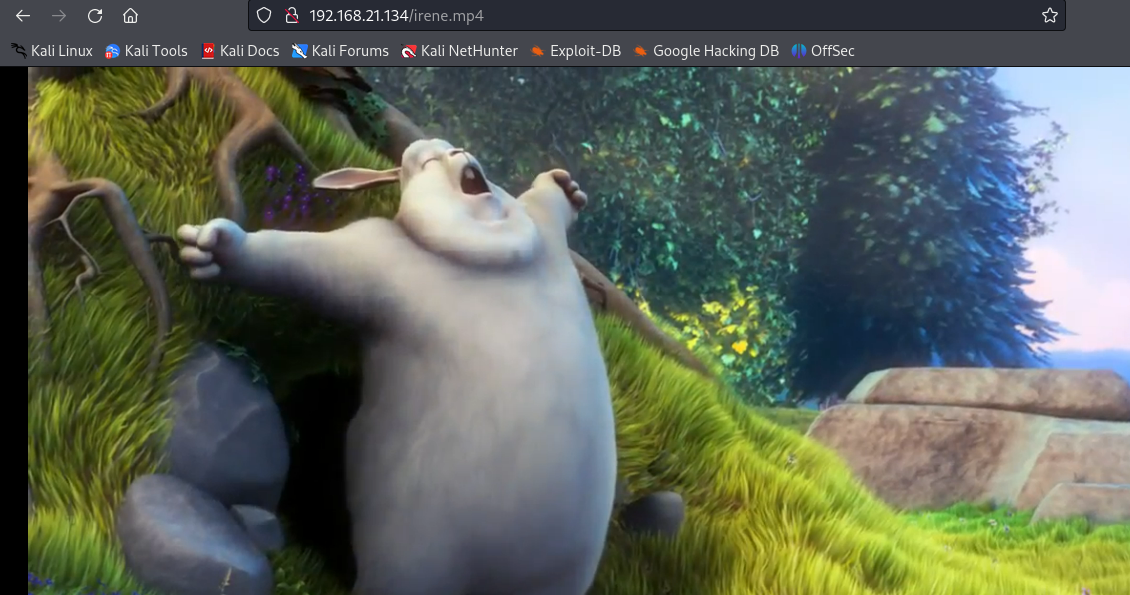
Ya que vemos los servicios HTTP en ejecución, vamos a cazar nuestra primera FLAG buscando la página web en el navegador.



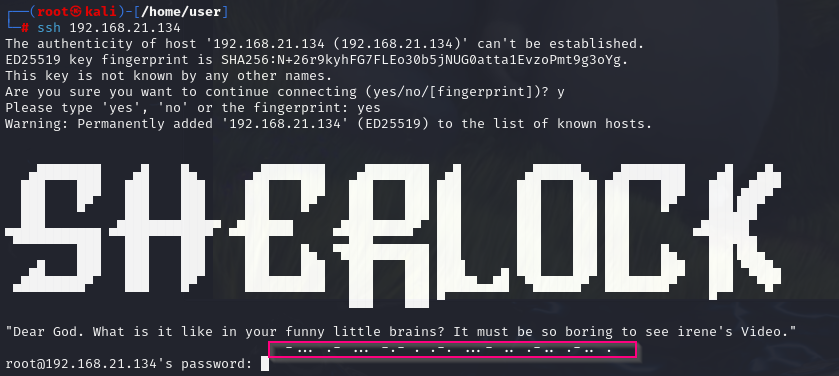
Vayamos a "Ver fuente de la página" de la página HTML y miremos si podemos encontrar algo relacionado con la flag. Y aquí encontramos nuestra primera pista que indica la presencia de un archivo .mp4 en la máquina. Así que busquemos el archivo .mp4.



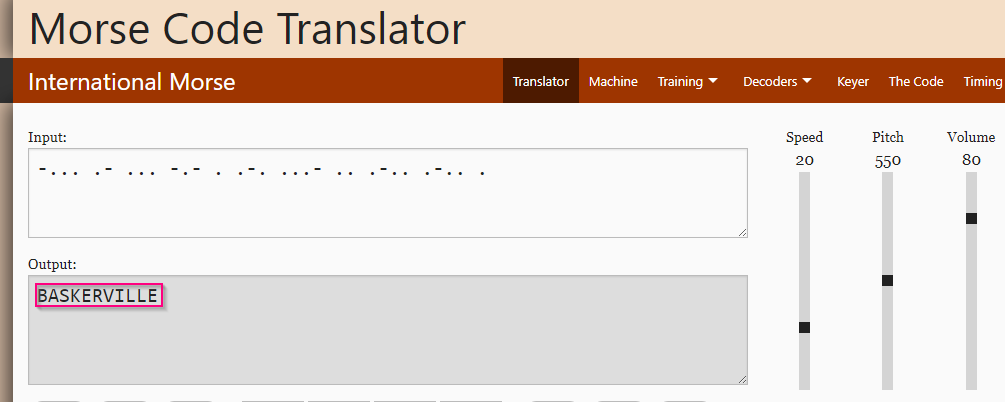
Por tanto, tratamos de recoger las palabras clave del comentario de la fuente de la página HTML y vemos dos nombres destacados, Irene y Sherlock. Entonces, intentamos usar los dos nombres como un archivo .mp4 en el navegador web. Y aquí, en irene.mp4, encontramos un vídeo reproduciéndose, que podría estar protegido por contraseña. Descarguemos el vídeo y veamos.



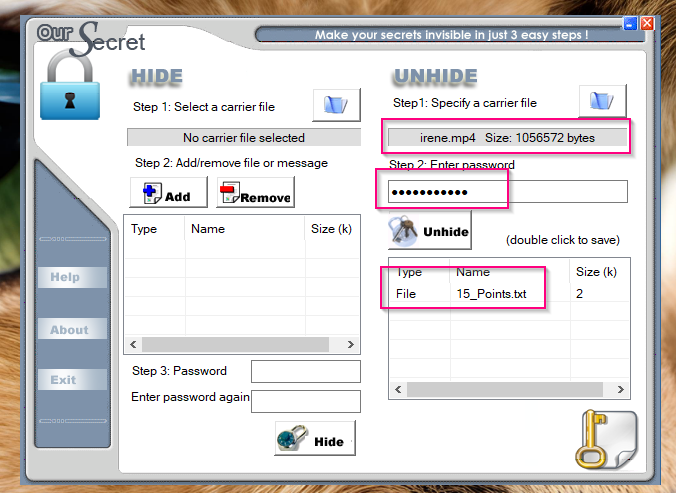
Después de ver el vídeo, nos damos cuenta de que no hay nada presente en el vídeo, así que pasamos al servicio ssh. Al hacerlo vemos un banner llamado sherlock y vemos que hay una pista en forma de "código morse".



Copiemos el código morse y utilicemos un traductor de códigos morse en línea. Aquí hemos encontrado la contraseña como BASKERVILLE.



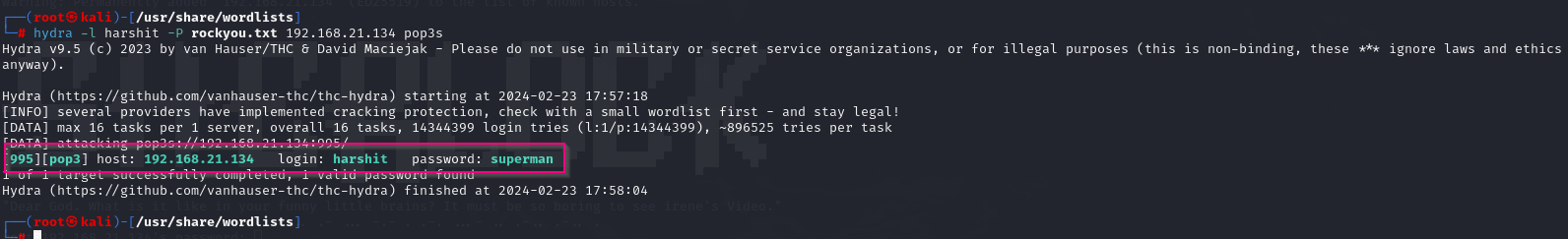
A continuación, podemos utilizar la contraseña "BASKERVILLE' para descifrar el archivo.mp4 y ver que hay un archivo con el nombre 15\_points.txt. Puedes hacer uso de la herramienta de esteganografía OurSecret para desocultar el contenido detrás del archivo de vídeo.

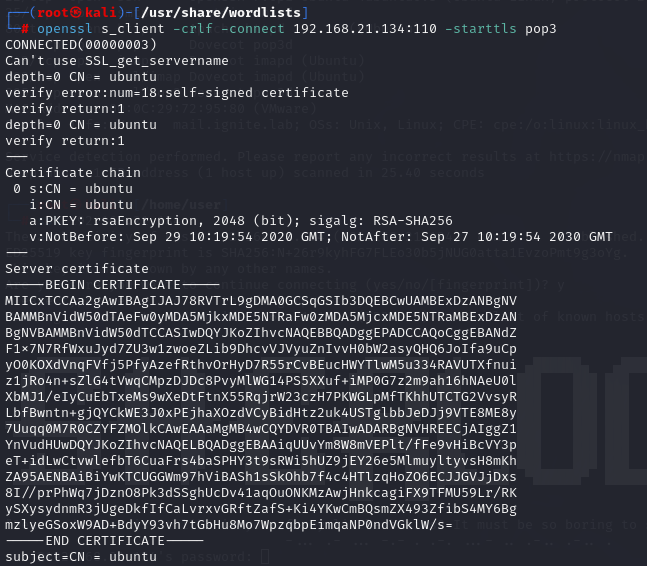


Encontrada la primera flag.



Ahora intentemos usar el nombre de Harshit como nombre de usuario para encontrar más pistas y hagamos 'fuerza bruta' en los POP3 usando la herramienta Hydra. Usamos el diccionario rockyou.txt.

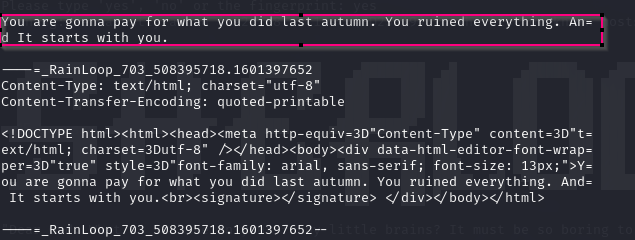
Aquí se ve que la contraseña del nombre de usuario Harshit ha sido descifrada y es superman. Ahora nos conectamos con el puerto pop3.



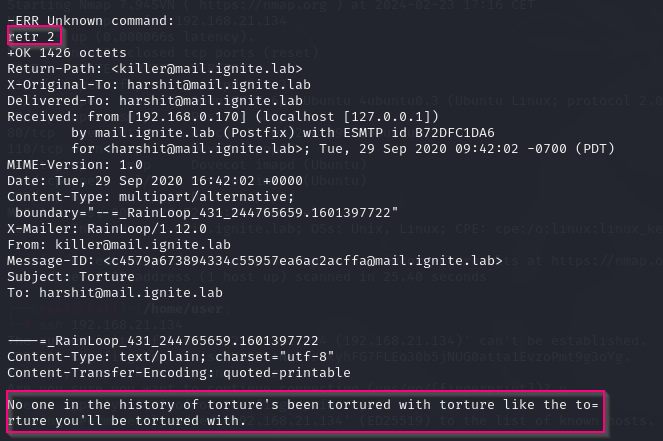
Puedes utilizar el nombre de usuario y la contraseña anteriores para iniciar sesión y encontrar más pistas relacionadas con el asesinato de Harshit.



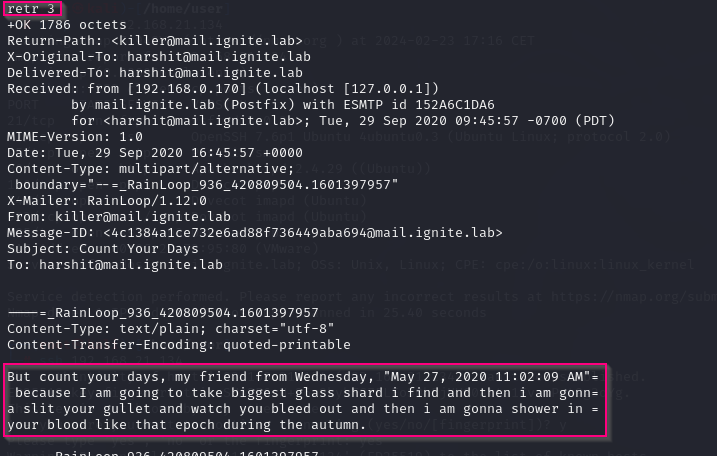
Y un mensaje:



En el segundo correo electrónico, se intercambian algunos mensajes y el asesino vuelve a amenazar a Harshit con torturarle. De ahí que se sucedan una serie de mensajes.

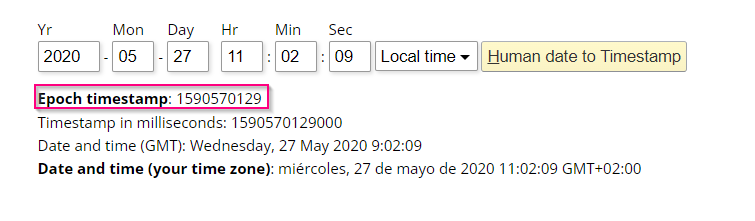


En el tercer hilo de correo electrónico, vemos que Harshit ha recibido un correo electrónico el "27 de mayo de 2020 11.02.09 AM" donde fue amenazado por el asesino y hay una palabra inusual época que se menciona en el mensaje. Así que juntemos todas las piezas y busquemos epoch en google.

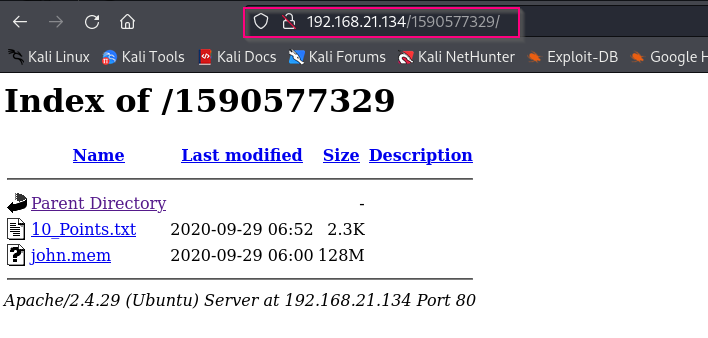


Abra su navegador web y busque un conversor de épocas que convierta las marcas de tiempo en un valor numérico diferente.

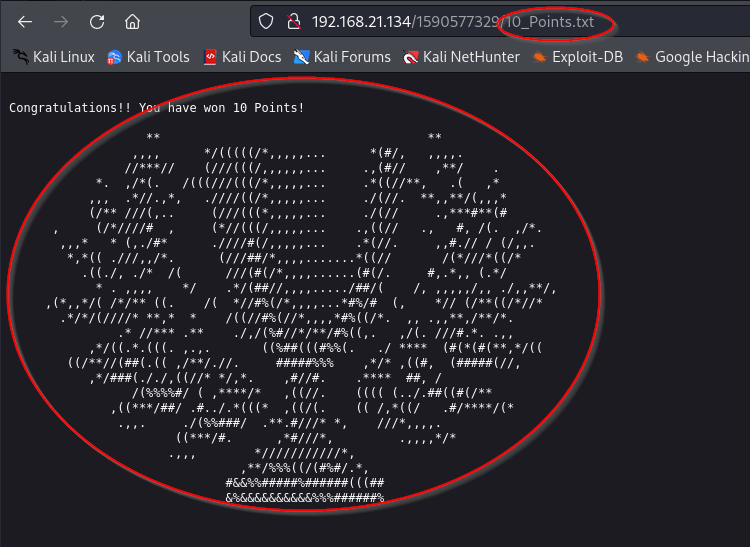
Introducimos el valor en el conversor de fecha humana a marca de tiempo del conversor de época y se generará una marca de tiempo de época.



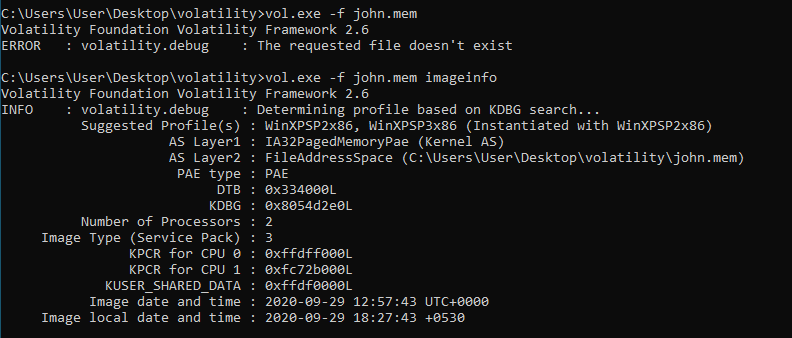
Lo buscamos en la url del navegador el numero epoch:



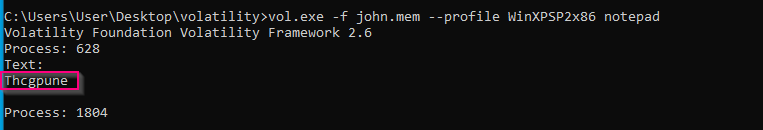
Y nos metemos en el archivo .txt:



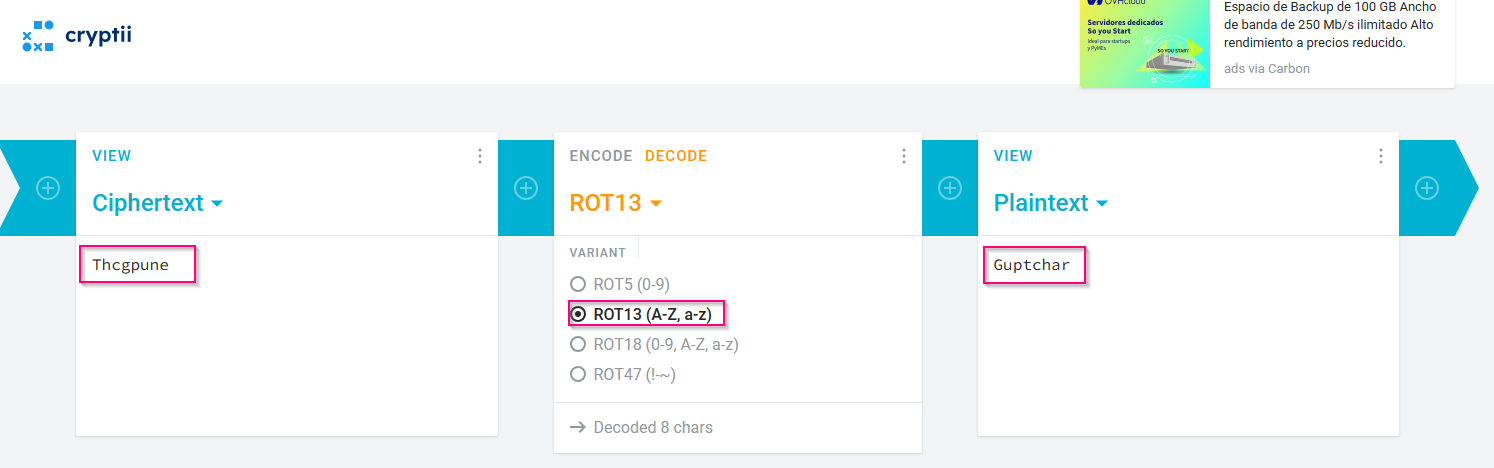
El archivo mem : A partir de la extensión del archivo, podemos entender que se trata de un archivo de volcado de memoria y podemos analizarlo utilizando el marco de volatilidad. Podemos buscar los archivos clave que se pueden encontrar en el volcado de memoria. Podemos utilizar el siguiente comando para obtener detalles sobre la ram.



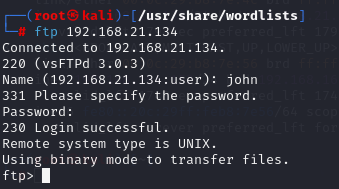
Podemos probar los diferentes plugs y ahora vamos a buscar un plugin de archivo de bloc de notas y aquí podemos encontrar algunas letras en el archivo.



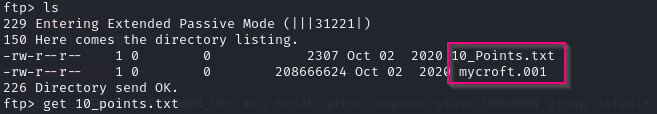
Copiamos el texto que hemos encontrado en el bloc de notas y vamos a intentar convertirlo usando rot13 y ahí encontramos un texto que dice Guptchar. Guptchar es una palabra hindi para el detective.



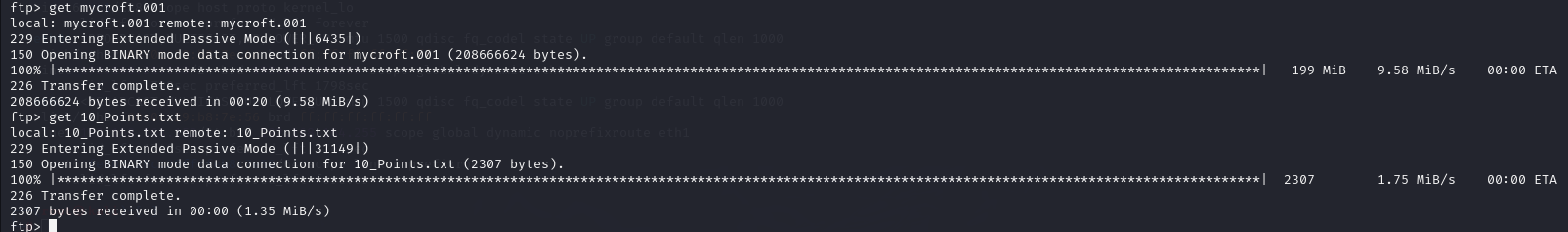
Hacer que el nombre de usuario como John y puede utilizar Guptchar como contraseña. Si volvemos atrás y recordamos, habíamos visto que el puerto FTP estaba abierto y nos permitía conectarnos al FTP.



Vemos que hay 2 archivos presentes, descargarlos para leer el contenido en el archivo .txt.

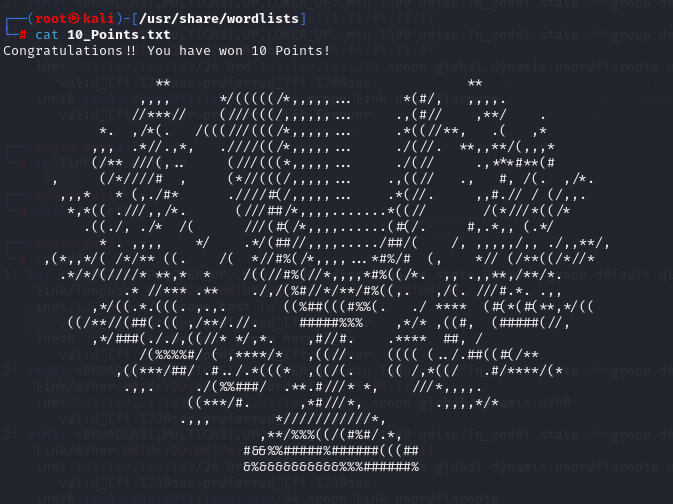


Y los descargamos:

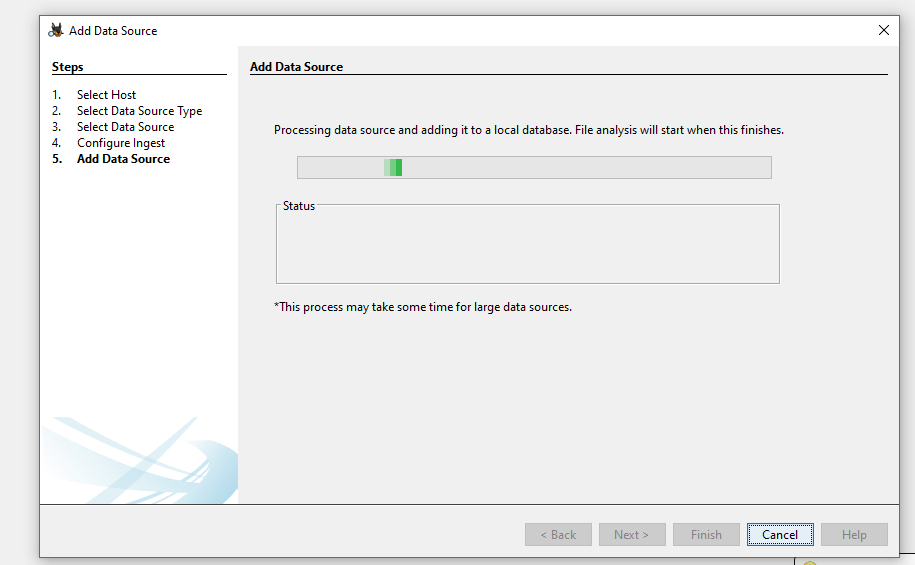


Ahora echemos un vistazo al otro archivo con nombre mycroft.001, la extensión del archivo implica que es un archivo de imagen en bruto que necesita ser analizado utilizando la herramienta Autopsy en kali Linux.

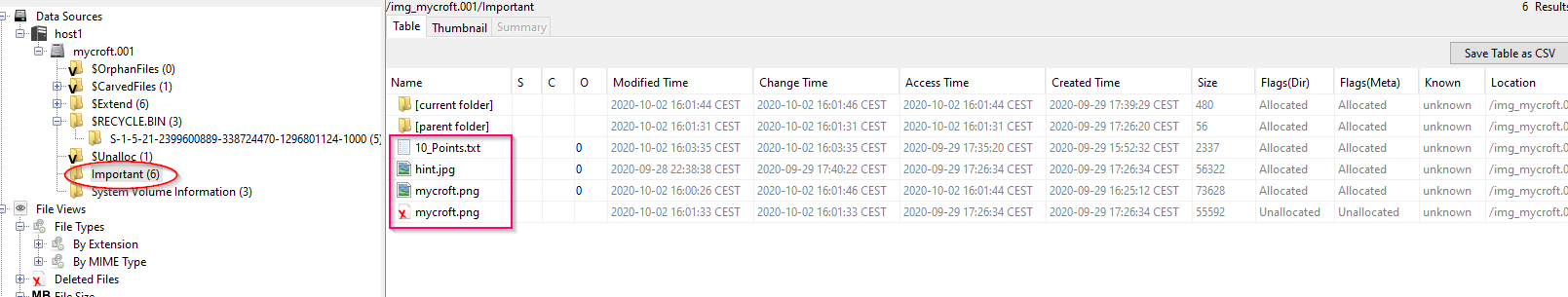
Abrimos el archivo de .txt



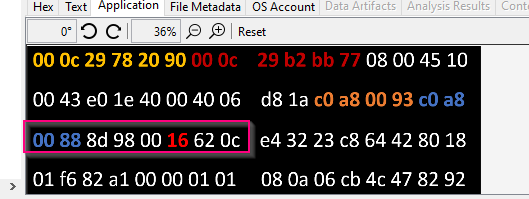
Archivo .001: usamos el autopsy de Windows, le llamamos Sherlock, le ponemos Host1 y que tenga toda la configuración puesta.



Archivos importantes dentro de una carpeta llamada Important: donde podemos ver el archivo de 10\_Points.txt y tres imagenes.

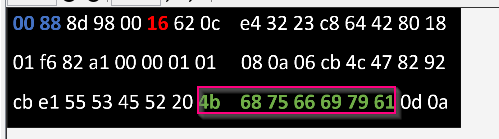


Una de las imágenes que nos interesa es: mycroft.png



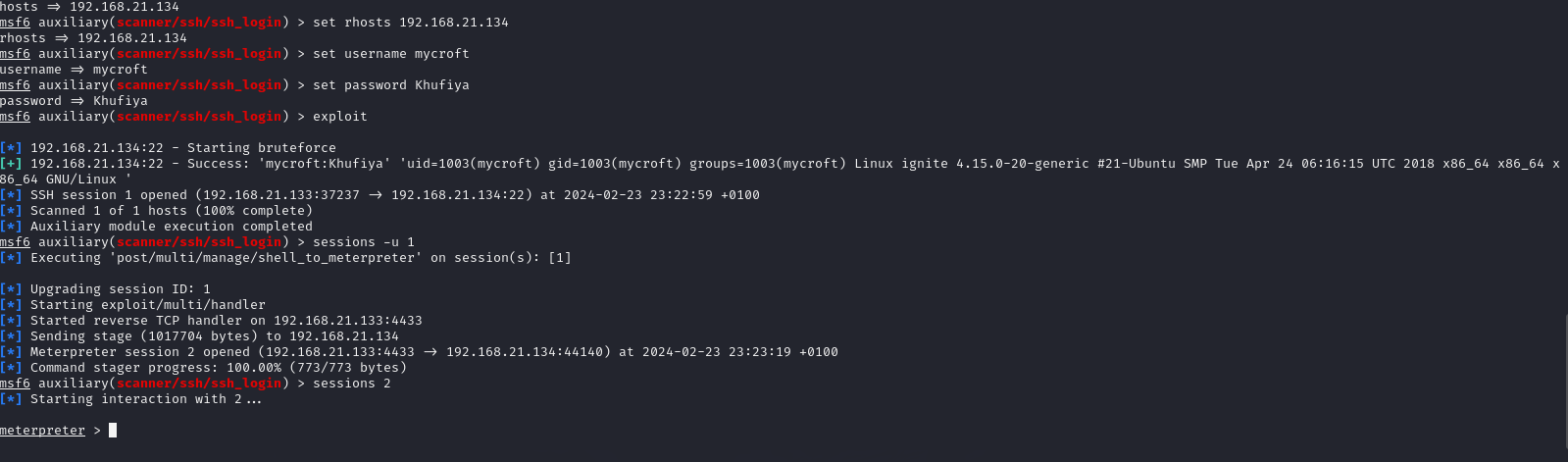
Y el número que vemos interesante es el 16 que es hexadecimal es 22 y podemos pensar que dicho número pertenece a un puerto.

El valor hexadecimal resaltado en verde claro se selecciona y se convierte en texto y hemos encontrado el texto que dice khufiya. Khufiya en hindi significa confidencial. Así que ahora vamos a ver cómo podemos hacer uso de esta palabra.

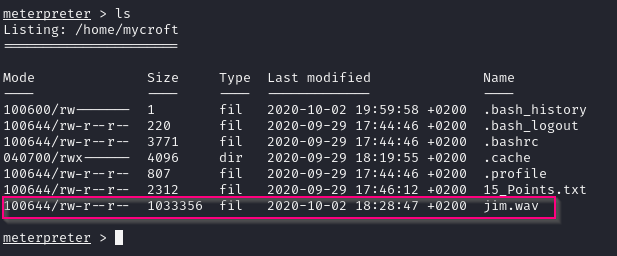




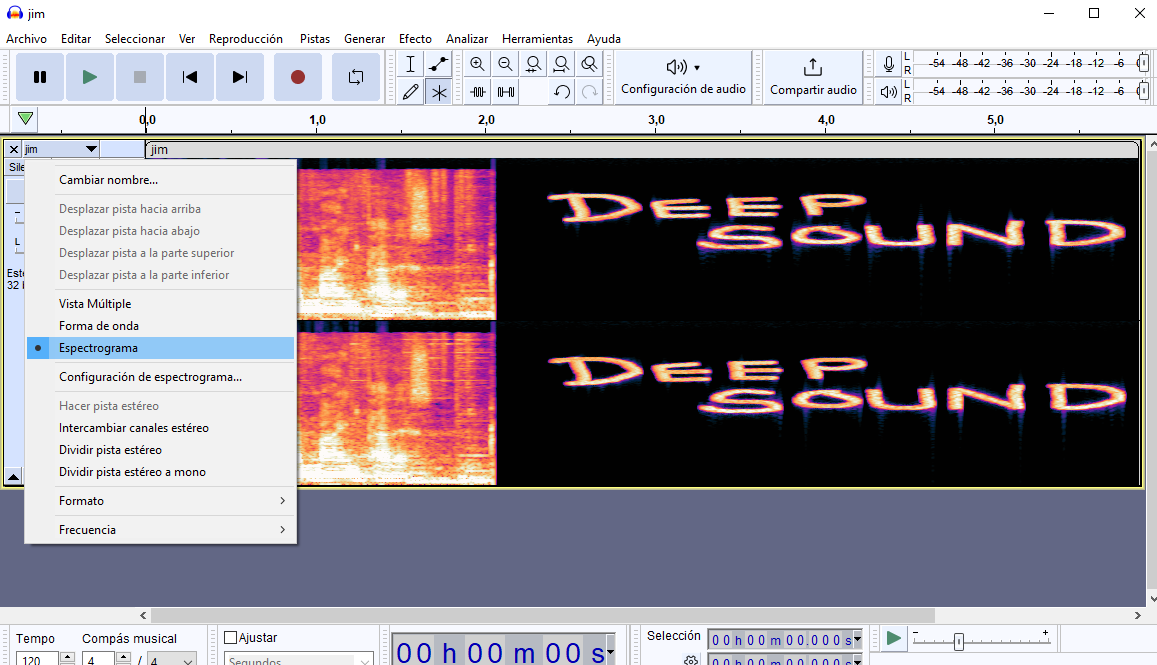
Anteriormente habíamos encontrado un archivo llamado mycroft.png y encontramos la pista del puerto 22, así que vamos a explotar ssh login usando Metasploit.

Tenemos 2 sesiones.

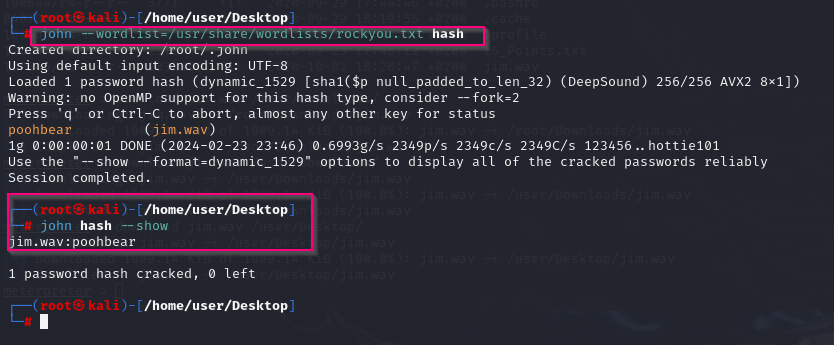
En la segunda hacemos un ls y encontramos un archivo interesante llamado jim.wav:



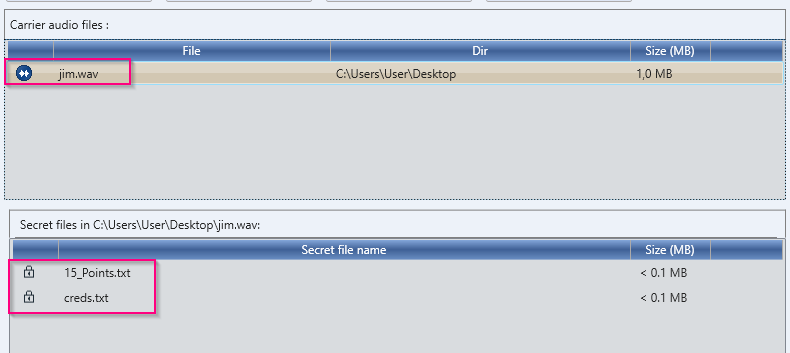
Ahora cogemos ese archivo lo metemos en la herramienta de Audacity, en la misma pista seleccionamos Espectograma:



Entonces, usemos deepsound2john.py, para convertir un archivo .wav a un archivo hash. Y el archivo es de fuerza bruta utilizando John



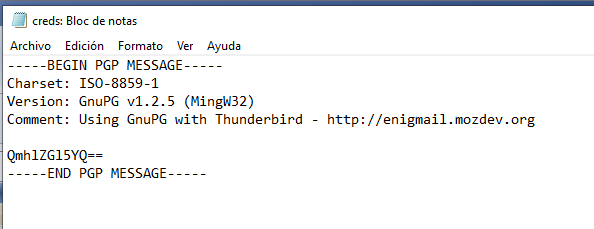
Ahora podemos abrir el Deep sound e introducir la contraseña (poohbear) en él. Y ahora se puede ver que hay dos archivos presentes en el .wav. Vamos a descargar los dos archivos y luego verlos uno por uno.



Archivo 15\_Ponits.txt:



Archivo creds.txt:



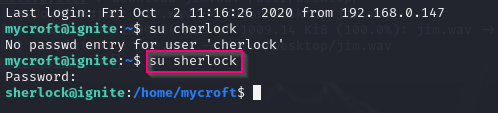
Tenemos un código en Base64: lo desencriptamos y vemos que significa Bhediya



Ahora entramos por ssh con el usuario mycroft:



Y ahora cambiamos al root que es el usuario sherlock con la contrasena Bhediya:



Nos vamos a la carpeta de root: y vemos la última flag

