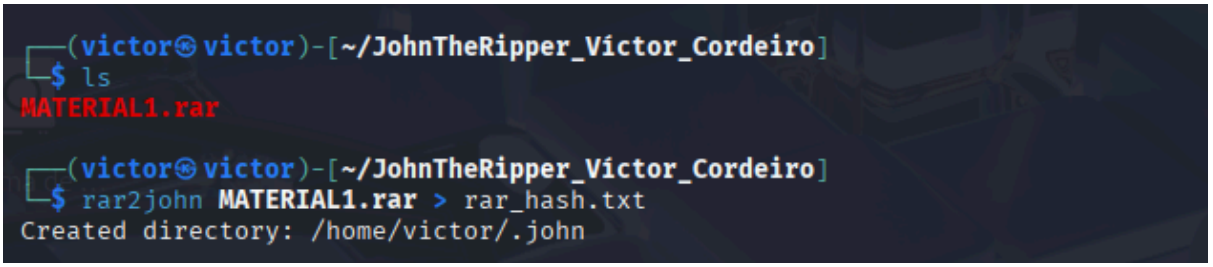
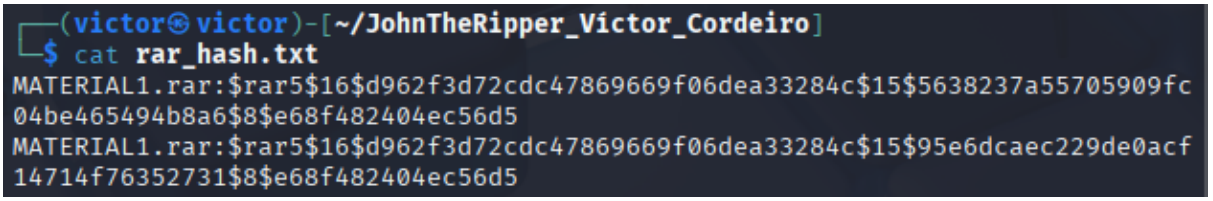
Descifrar archivo rar con John The Ripper.

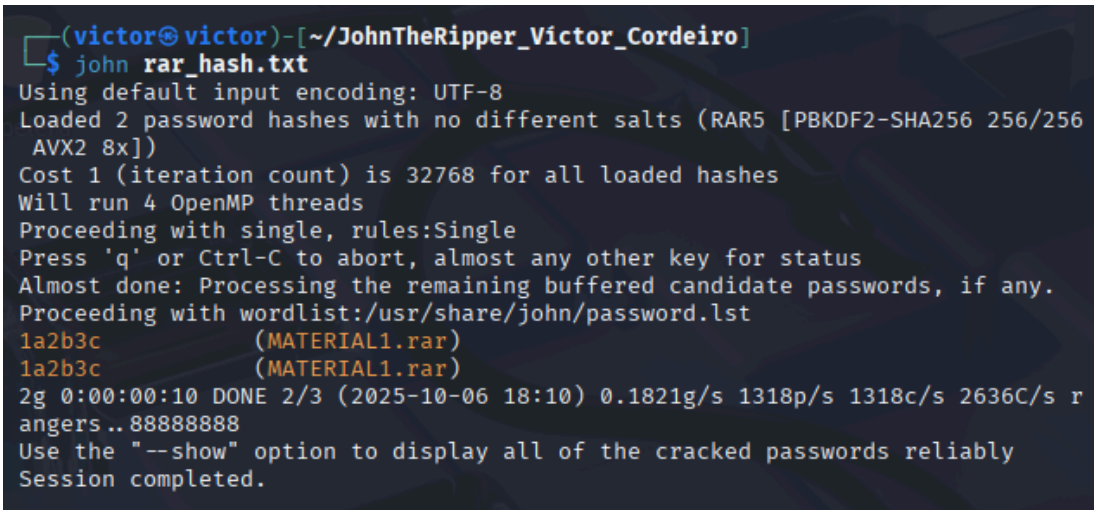
Tenemos un archivo .rar cifrado con clave, por lo que no podemos acceder a su contenido. Vamos a averiguar su contraseña para poder acceder a él.

1. Ejecutamos el comando 'rar2john' sobre el archivo .rar. Esta es una herramienta que incluye john the ripper, que permite obtener el hash de la clave de un archivo .rar cifrado. En la misma linea, redirigimos el hash obtenido a un archivo .txt para almacenarlo y acceder a él posteriormente. El comando se nos queda asi:
   `rar2john MATERIAL1.rar > rar_hash.txt`

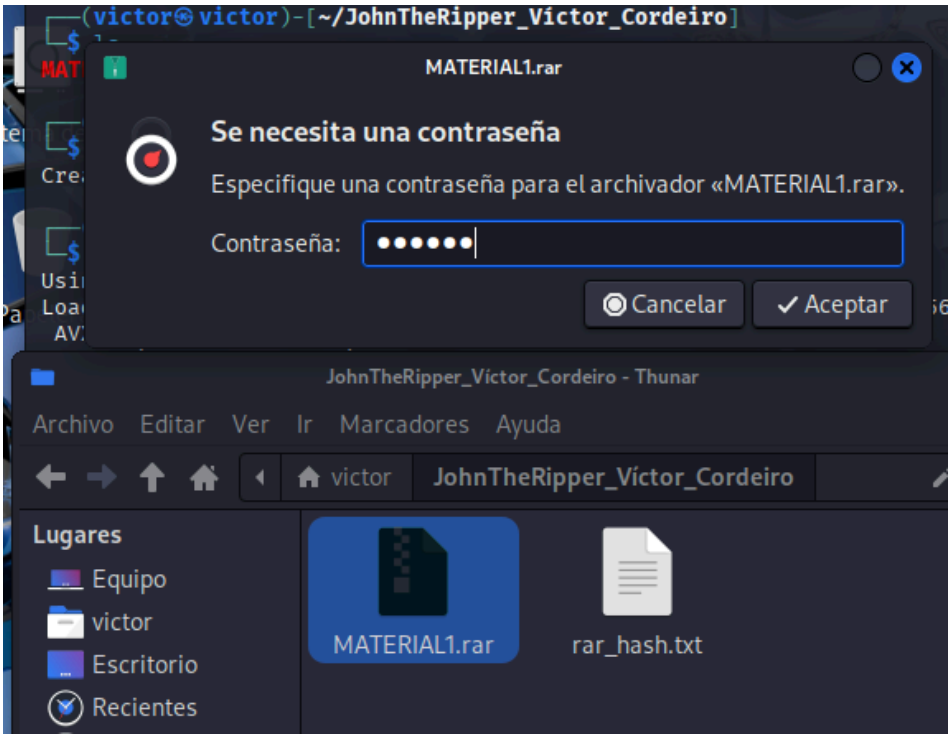


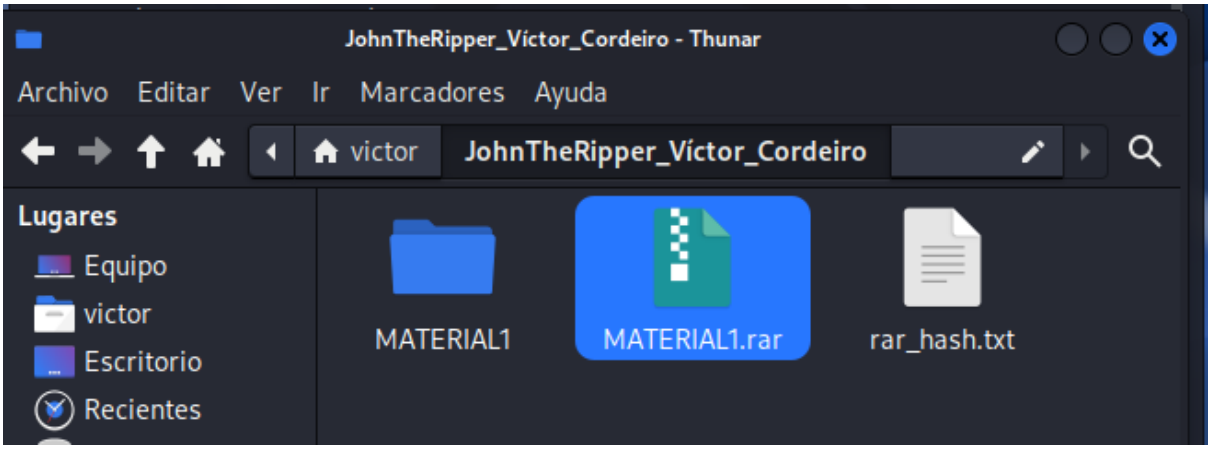


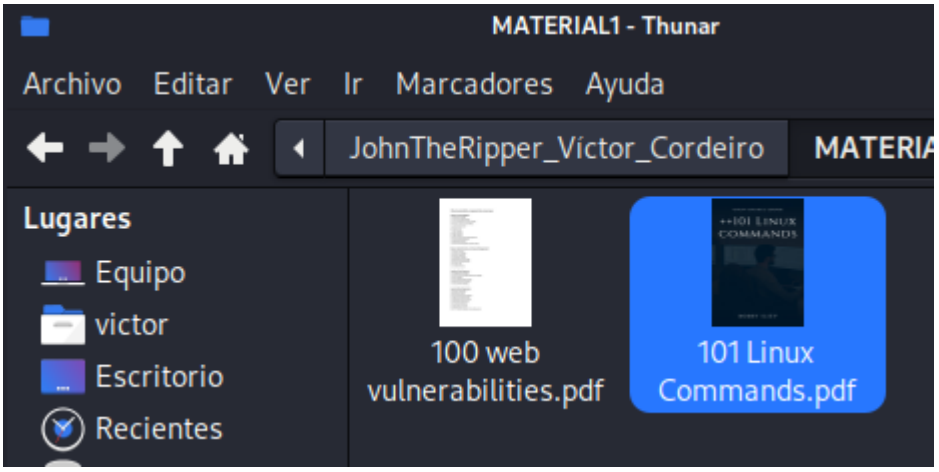
2. Ahora ejecutamos el comando john sobre el archivo que almacena nuestro hash. La herramienta descrifara la clave, y tardara en función de la complejidad de la clave y nuestro poder de procesamiento.



3. Ahora conocemos la contraseña que protege el archivo. rar, ‘1a2b3c’. Si la introducimos al intentar descomprimir el archivo nos da acceso, comprobando asi que es la correcta.



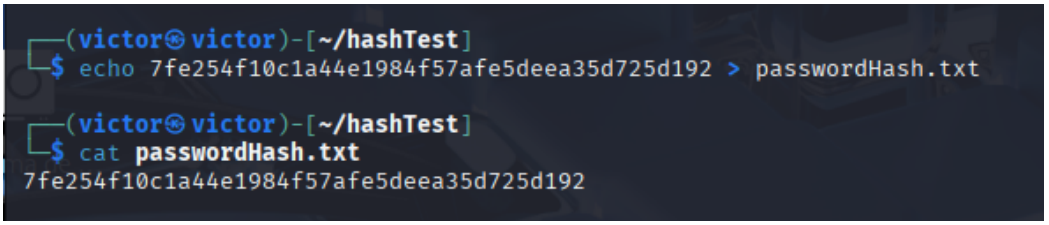




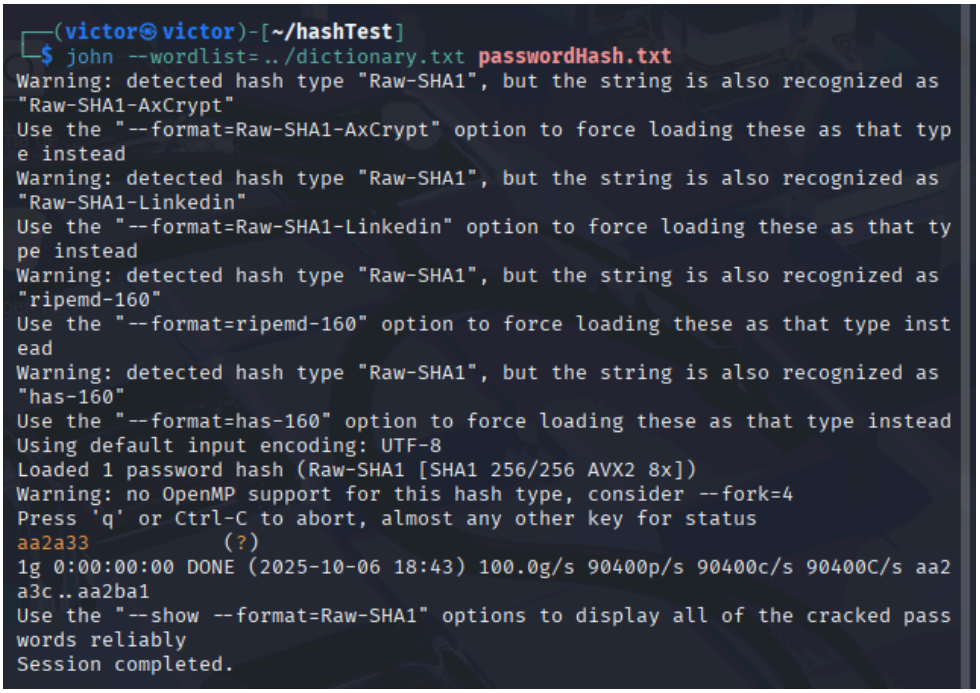
Descifrar el hash de una contraseña con John The Ripper.

En este caso conocemos el hash de una clave, y vamos a descifrarlo usando un diccionario de claves, en concreto el que creamos en otra actividad con crunch.

1. Primero creamos un archivo .txt que contenga el hash que queremos descifrar.



2. Una vez hecho esto, usamos el comando john con la opción - - wordlist, con la que le indicamos a la herramienta que trabaje con un diccionario. Indicamos la ruta del diccionario y seguido la ruta del archivo con el hash que queremos descifrar
`john --wordlist=../dictionary.txt passwordHash.txt`



Finalmente obtenemos la clave correspondiente a este hash:

aa2a23