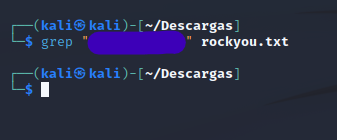
Romper contraseñas

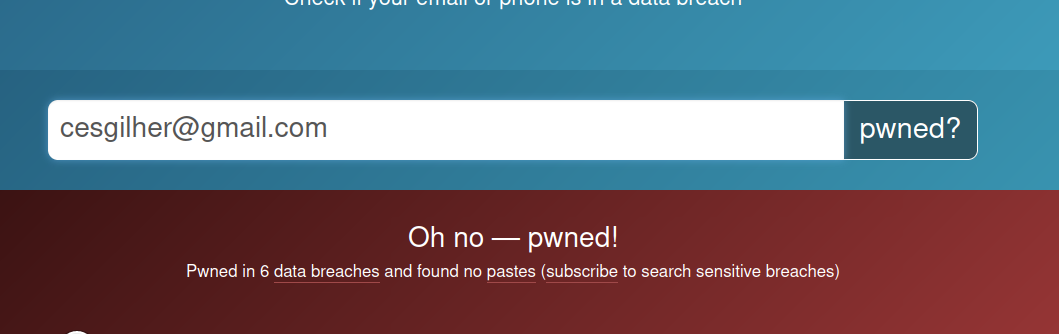
1º: busca si tu contraseña esta en rockyou

Podemos ver que efectivamente, mi contraseña no esta en el diccionario rockyou



2º:buscar si habeis sido pawneados

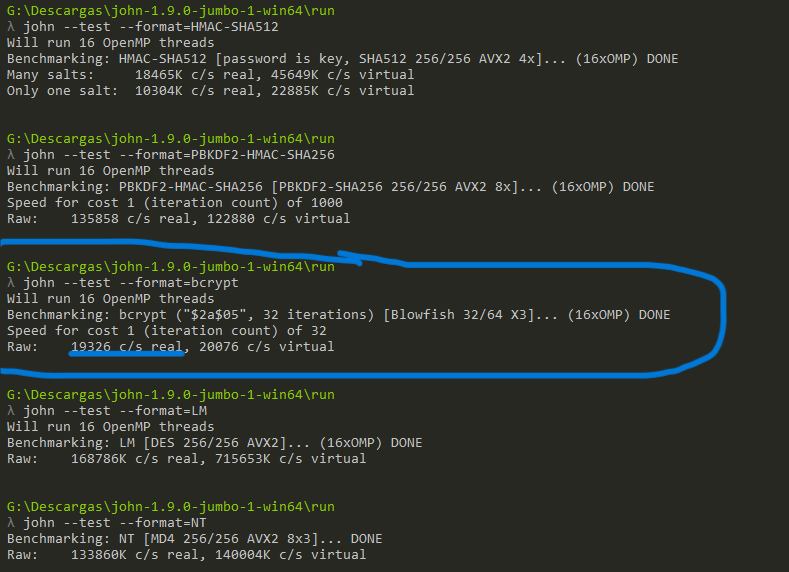
Accedemos a la web <https://haveibeenpwned.com> e introducimos nuestro correo electronico.



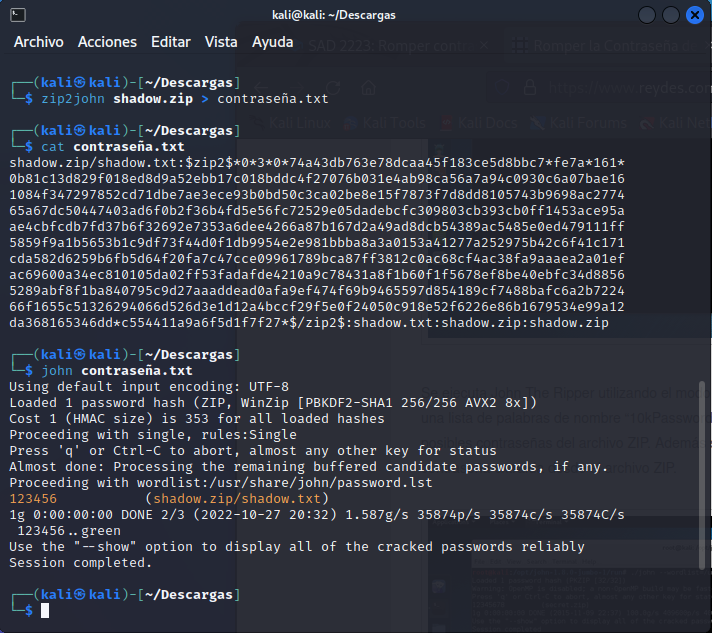
Lo adecuado aquí seria acceder a las paginas afectadas y cambiar la contraseña.

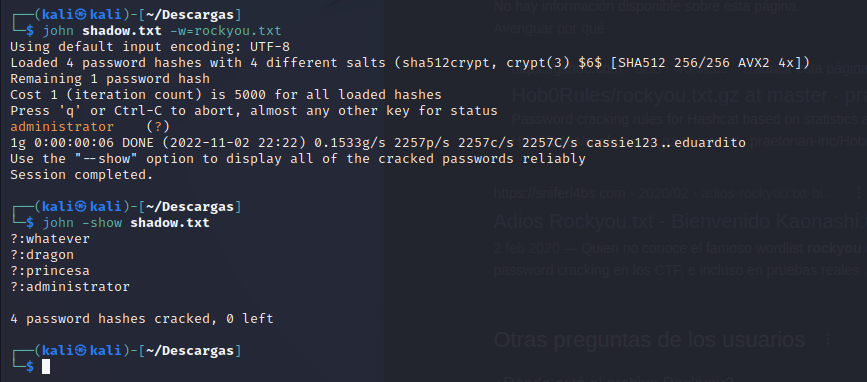
3º: buscar el algoritmo hash mas seguro de estos HMAC-SHA512,PBKDF2-HMAC-SHA256,bcrypt,LM,NT

Al final el algoritmo mas seguro es aquel que mas cuesta deshasear, y eso se puede averiguar con la cantidad de contraseñas que se analizan por segundo. Siguiendo esta logica el algoritmo mas seguro es el bcrypt.



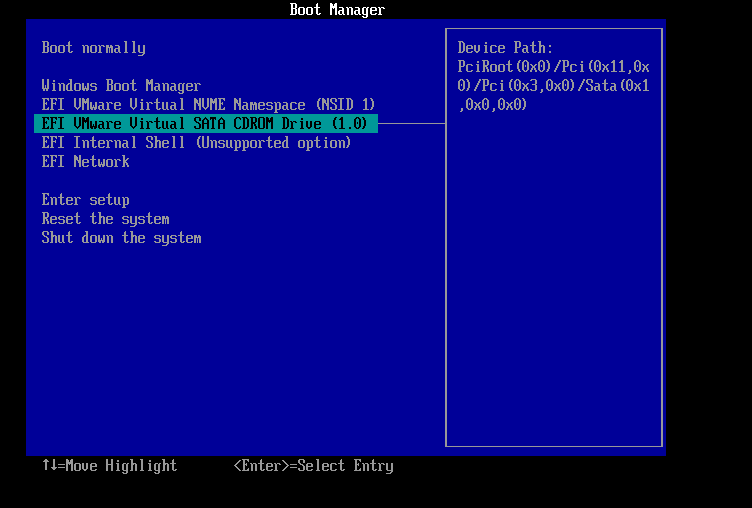
4º:rompe las contraseñas del zip, (we will rockyou)

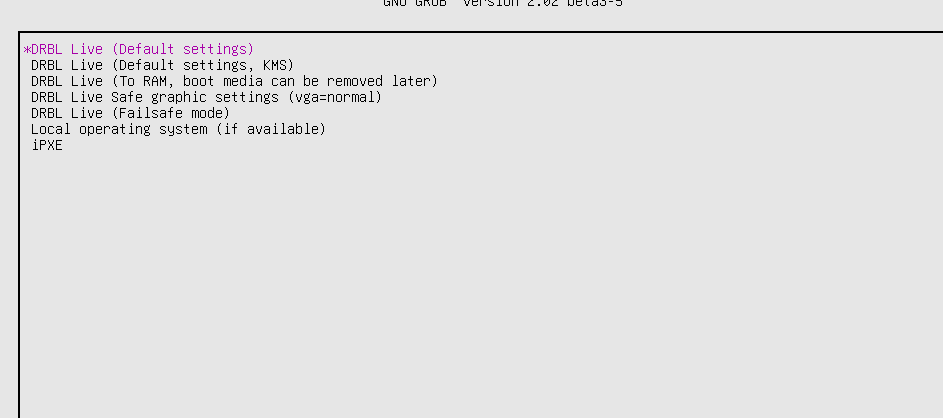
Lo primero es sacar la contraseña del zip para poder abrir los archivos que hay dentro. Pero antes vamos a convertir el zip a txt para que “juanito” puede leerlo.

Una vez que ya tenemos la primera contraseña, ya podemos usarla para descomprimir. Para sacar las siguientes cuatro contraseñas usaremos el diccionario rockyou. De forma que no tenga que hacerlo por fuerza bruta, ya que tradaria mucho más.

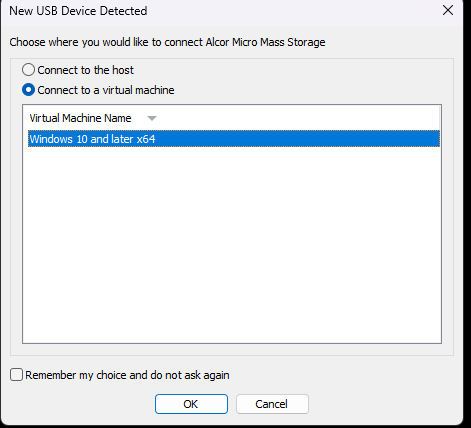
5º: de la maquina de windows sacar los usuarios y contraseñas

Para este ejercicio necesitamos acceder a los ficheros SAM y SYSTEM de la maquina que queremos atacar, para ello deberemos acceder al disco duro donde estas se almacenan.Bien podríamos añadir el disco duro en otra maquina y desde ahí copiar los ficheros. Pero me parecía poco realista, así que he preferido arrancar el ordenador con un live cd y desde ahí copiar a un usb los ficheros que necesitamos.



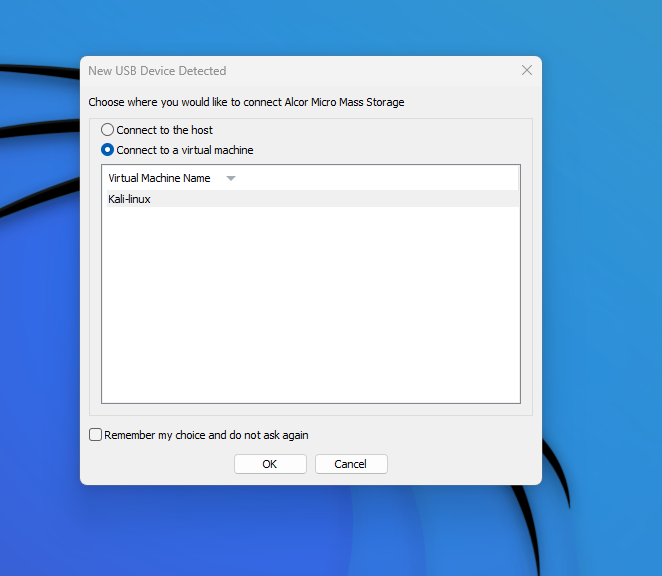


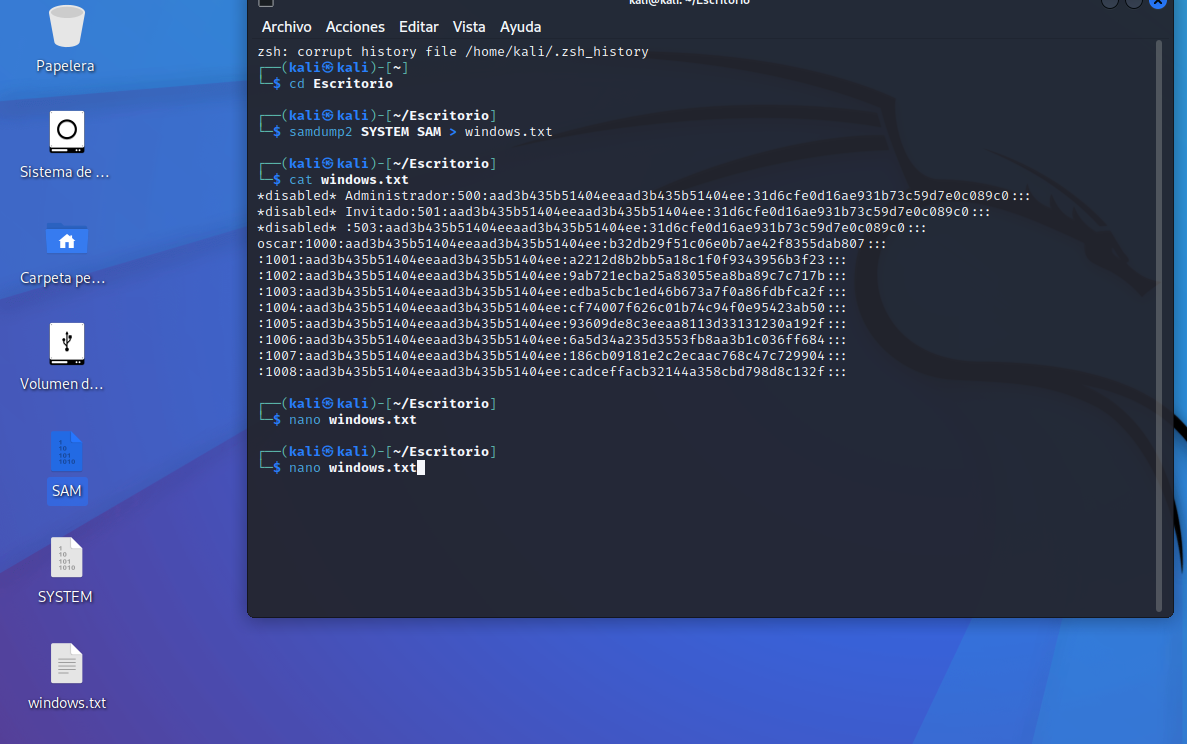
Conectamos el usb a la maquina virtual.



Y procedemos con los comandos necesarios para copiar los archivos.

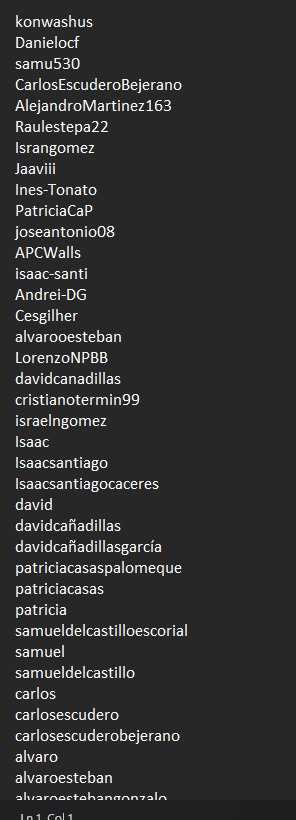
Ahora vamos a una maqui linux y convertimos los archivos SAM y SYSTEM a txt para que “juanito” una vez mas sea capaz de leerlos.



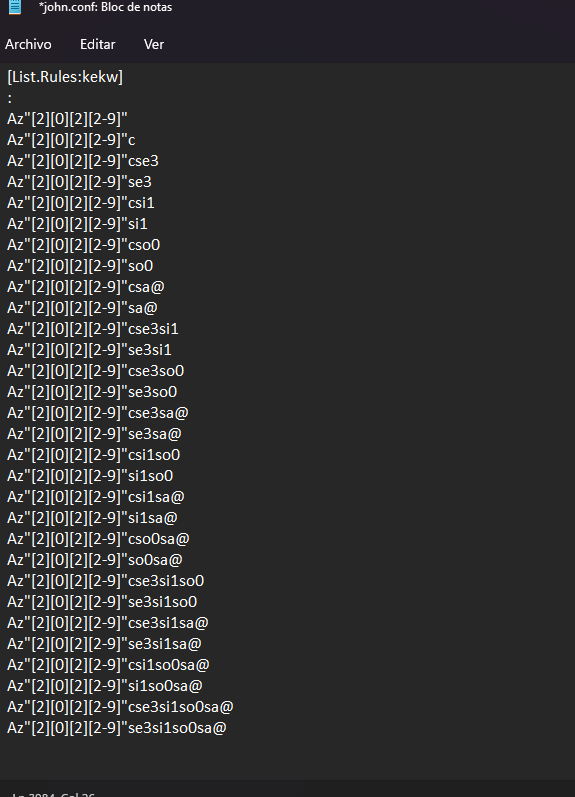


Ahora podriamos seguir el ejercicio en la maquina linux, pero he preferido hacerlo en mi windows ya que asi puedo usar todos los nucleos del procesador y agilizar el proceso. Para ello basta con conectar el usb, con los tres archivos, a windows.

Ahora vamos a crear el diccionario, no tiene mucha complejidad más alla de encontrar todos los nombres y los usuarios de github. El diccionario tiene este formato, una contraseña por linea.



Con el diccionario ya hecho solo falta crear un nuevo set de reglas en el archivo de configuracion de “juanito”.

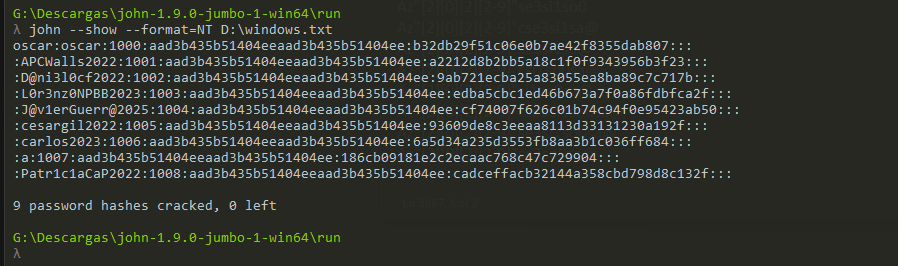


Ahora usando el diccionario en conjunción con la nueva lista de reglas, y especificando el formato NTLM, podemos proceder a desencriptar las contraseñas.

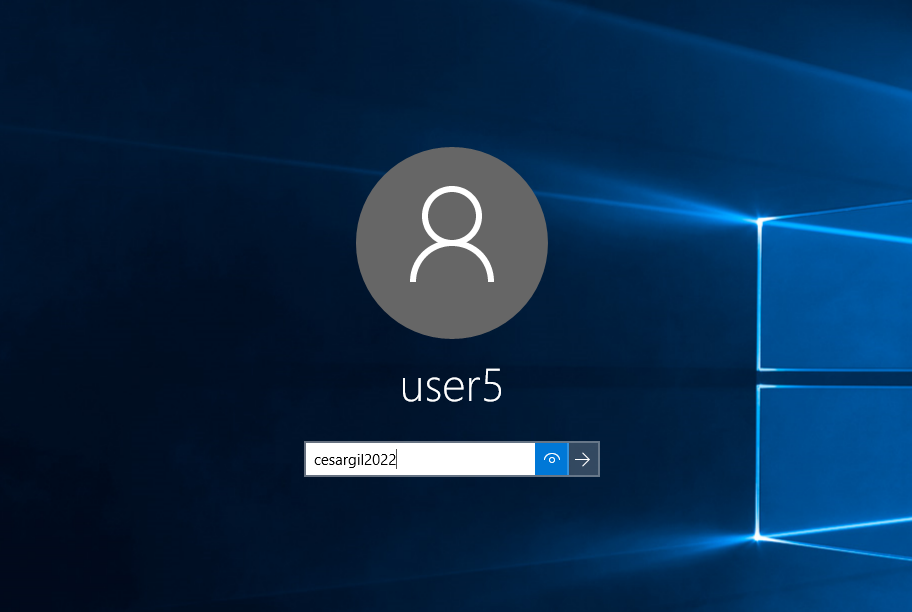
Dos de ellas salen por fuerza bruta asi que no necesitariamos ni el diccionario ni las reglas.

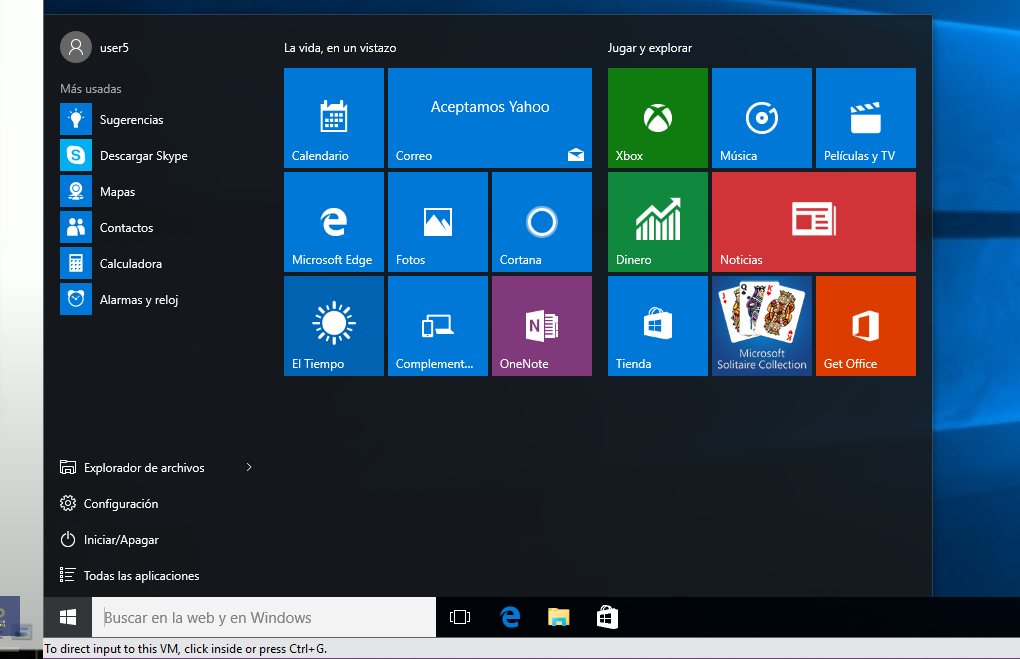


Si comprobamos las contraseñas, vemos que ahi estan.



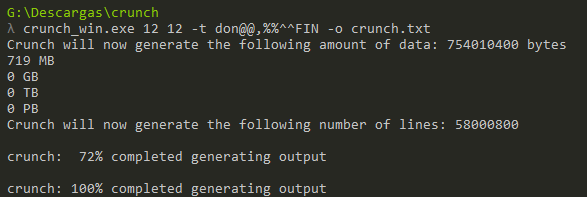
Ahora vamos a conectarnos a la maquina victima para ver que efectivamente tenemos las contraseñas.





6º:Deshasea las contraseñas del txt dado, don+dosletrasminusculas+unamayuscula+dosnumero+unsimbolo+FIN ej donniK12$FIN, HELP tomate un crunch

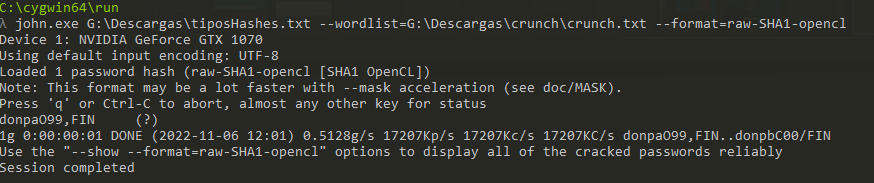
Lo primero es crear el diccionario con crunch, para ello el comando es el siguiente. En windows es algo diferente que en linux, porque para que te reconozca el caracter especial, hay que poner ^^ en vez de simplemente ^.



Ahora usamos John de ripper una vez mas pero empleando el nuevo diccionario.

Decir que solo he sido capaz de sacar una de las contraseñas a pesar de haber habilitado el uso de la gpu porque son demasiadas combinaciones y segun la propia maquina hasta el 10-11-2022 no acabaría de probarlas todas.

Formato SHA1



Formato bcrypt

