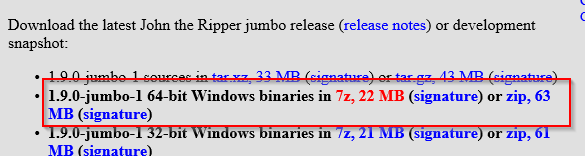
# Objetivos

* En una MV con W7 o W10, crea 3 usuarios (con sus contraseñas correspondientes) e intenta descifrar dichas contraseñas con el equipo "en caliente" en los siguientes casos:
  + - Dos contraseñas tengan como máximo 6 caracteres alfanuméricas y una contraseña de máximo 6 caracteres con al menos un símbolo.
    - Dos contraseñas que sean de 8 caracteres y una que tenga un símbolo.
    - Todas las contraseñas de más de 8 caracteres.

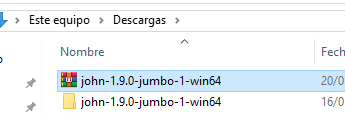
**Ejecución**

## Descarga de herramientas

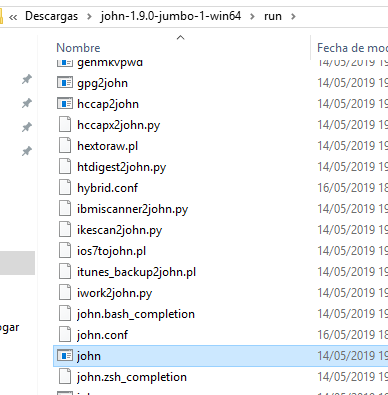
Primero hay que descargar la herramienta para crackear los hashes ([John Te Zipper](https://www.openwall.com/john/)):



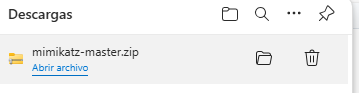
Luego lo extraemos:



Ya podríamos usar la herramienta. Que en realidad es este ejecutable:



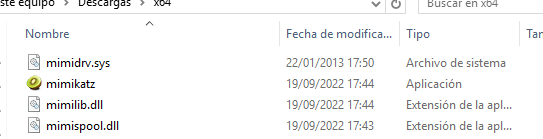
Lo siguiente será descargar “[Mimikatz](https://github.com/gentilkiwi/mimikatz?tab=readme-ov-file)”:



Luego extraemos el archivo “.zip”:



Ya tendríamos el ejecutable:

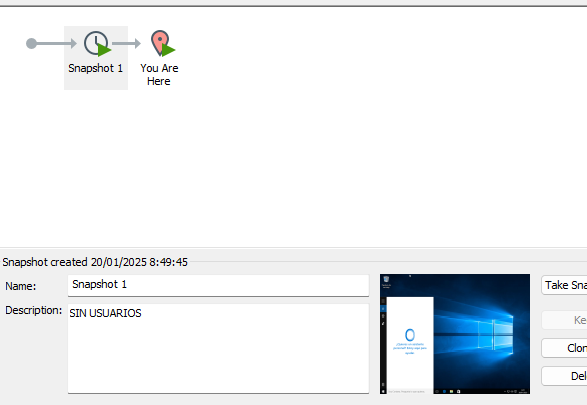


Una vez abierto, pondremos el comando “privilege::debug” para tener permisos de NT AUTHORITY/SYSTEM:

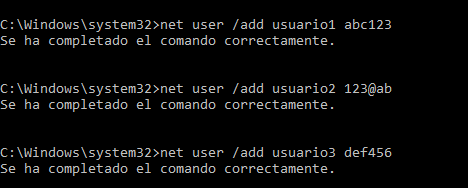


### Caso 1

Creamos una snapshoot antes de crear ningún usuario:



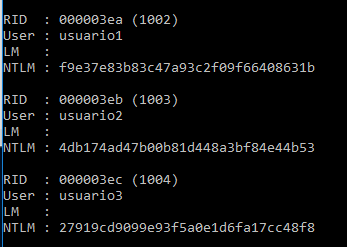
Abrimos el CMD y creamos 3 usuarios con las contraseñas del primer caso:



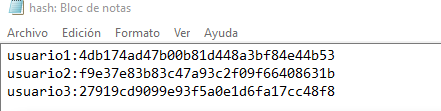
Luego ponemos el comando “lsadump::lsa /patch” para que nos muestre los hashes de las contraseñas de los usuarios que han iniciado sesión alguna vez en el sistema:



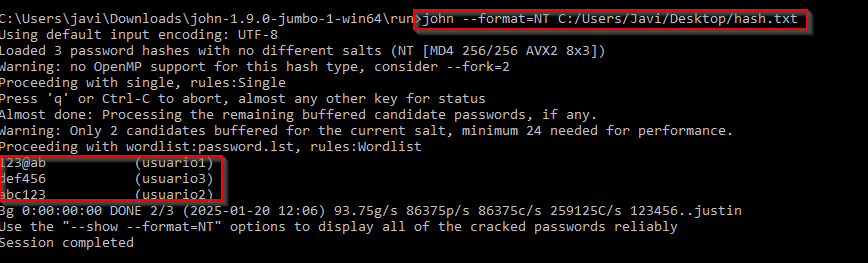
Luego buscamos a cada usuario y su hash:



Después vamos a un bloc de notas, y configuramos el usuario y el hash como si fuse de tipo “NT”:

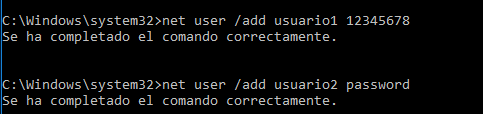


Luego abrimos un cmd y crackeamos estos hashes:



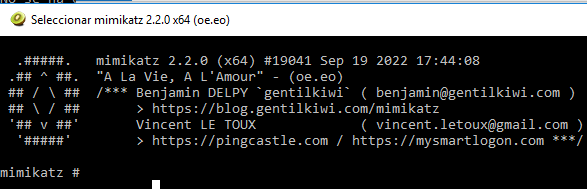
### Caso 2

Volvemos con el snapshoot y de nuevo, volvemos a crear los usuarios en el terminal:





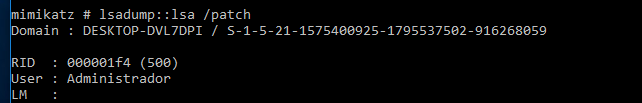
Ahora volvemos de nuevo a abrir “Mimikatz”:



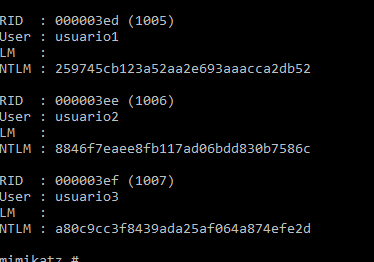
Ponemos el comando “privilege::debug” para tener permisos de NT AUTHORITY/SYSTEM:



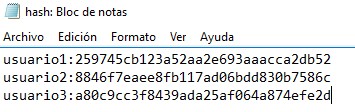
Luego sacamos la BD SAM con el comando “lsadump::lsa /patch”:

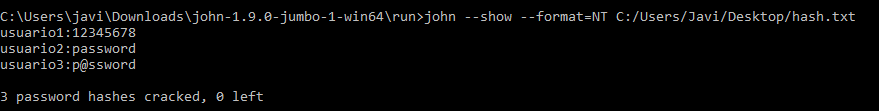


Buscamos los usuarios para coger sus hashes:



Los volvemos a dejar en un bloc de notas en tipo NT:

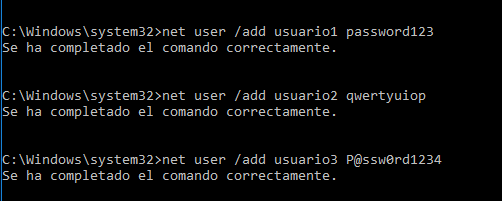


Usaremos John de nuevo para descifrar las contraseñas de estos hashes:  


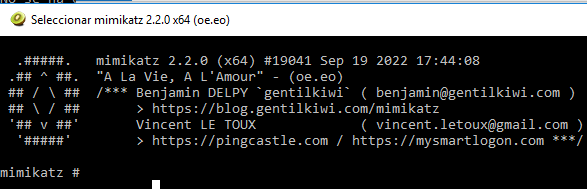
***Esta vez el tiempo para crackearlas ha sido mucho mayor, sobre todo la que incluía el símbolo***

### Caso 3

Volvemos con el snapshoot y de nuevo, volvemos a crear los usuarios en el terminal:



Ahora volvemos de nuevo a abrir “Mimikatz”:



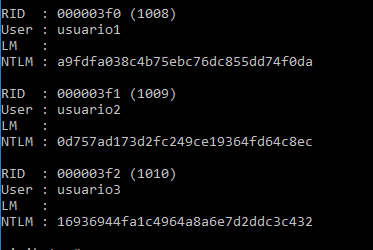
Ponemos el comando “privilege::debug” para tener permisos de NT AUTHORITY/SYSTEM:

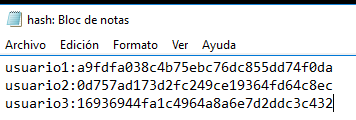


Luego sacamos la BD SAM con el comando “lsadump::lsa /patch”:

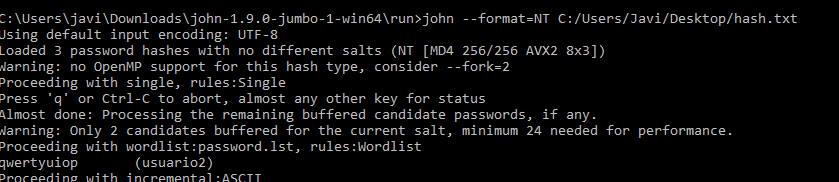


Buscamos los usuarios y sus hashes y lo pegamos en un fichero como tipo NT:

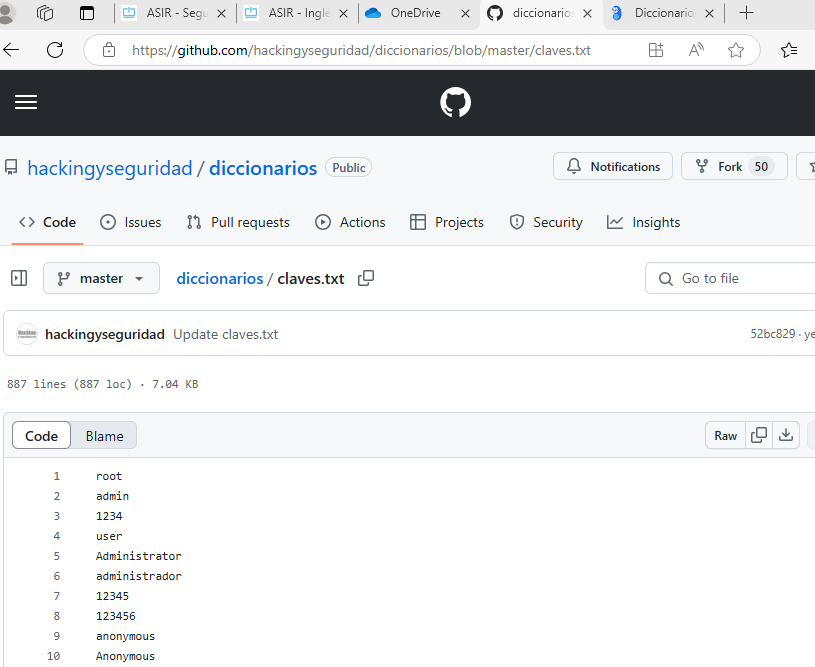




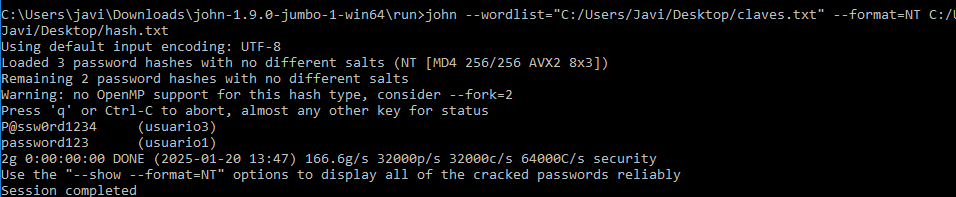
Ahora usaremos John para descifrarlo:

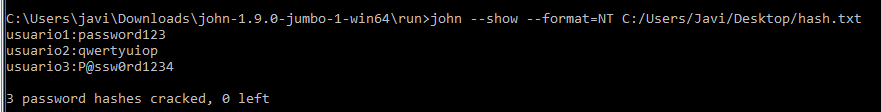


Como vemos, solo ha podido encontrar una contraseña. Las otras dos, al ser más compleja necesita otra wordlists con palabras más complejas. Yo me voy a descargar una grande con mucha variedad de palabras comunes:



Ahora usaremos John con esta wordlist para sacar las otras dos contraseñas:



Por ultimo pondremos “John –show –format=NT hash.txt” para ver todas las claves:  


***Vemos que, con estas claves, no solo ha aumentado el tiempo, sino que también hemos tenido que usar una wordlist más compleja.***