1 ASIX

**MÒDUL 11: SEGURETAT I ALTA DISPONIBILITAT**

ACTIVITAT 1.5: Atacs de força bruta a Windows 10

línea horizontal



# 

**Alumne**: Daniel Mascarilla del Olmo

**Professor**: Sergi Andrés

**Curs**: 1 ASIX

**Centre**: Jaume Viladoms

**ÍNDEX**

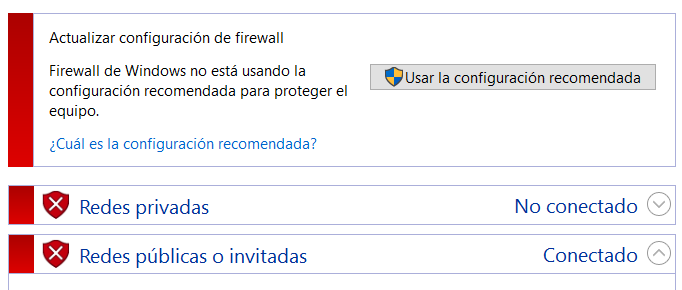
[**Exercici 1 – Dumping dels hashes dels usuaris amb Mimikatz**](#_58kxn12lb2b) **3**

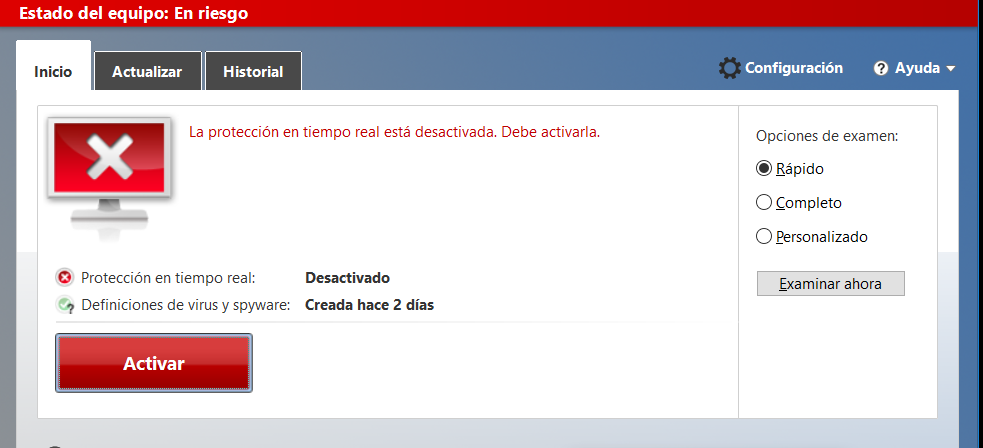
[**Exercici 2 – Força bruta contra el fitxer de hashes amb hashcat**](#_r2scqsocwww6) **9**

[**Exercici 3 – Força bruta contra el fitxer de hashes amb John The Ripper**](#_mz9gklgn9glp) **12**

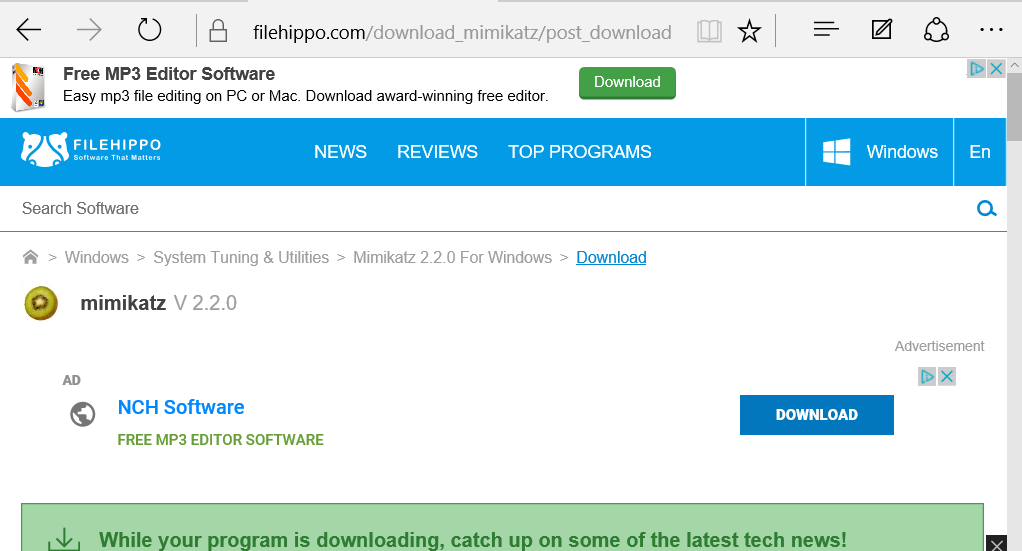
# Exercici 1 – Dumping dels hashes dels usuaris amb Mimikatz

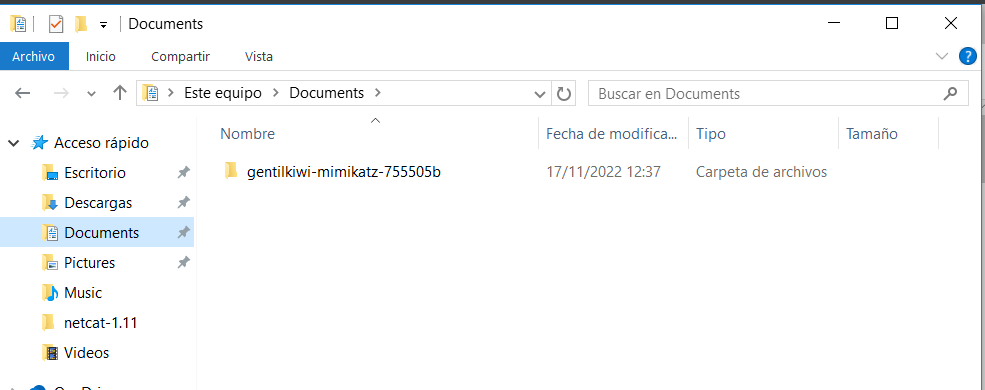
a. Desactiva Windows Defender i totes les opcions de protecció en temps real



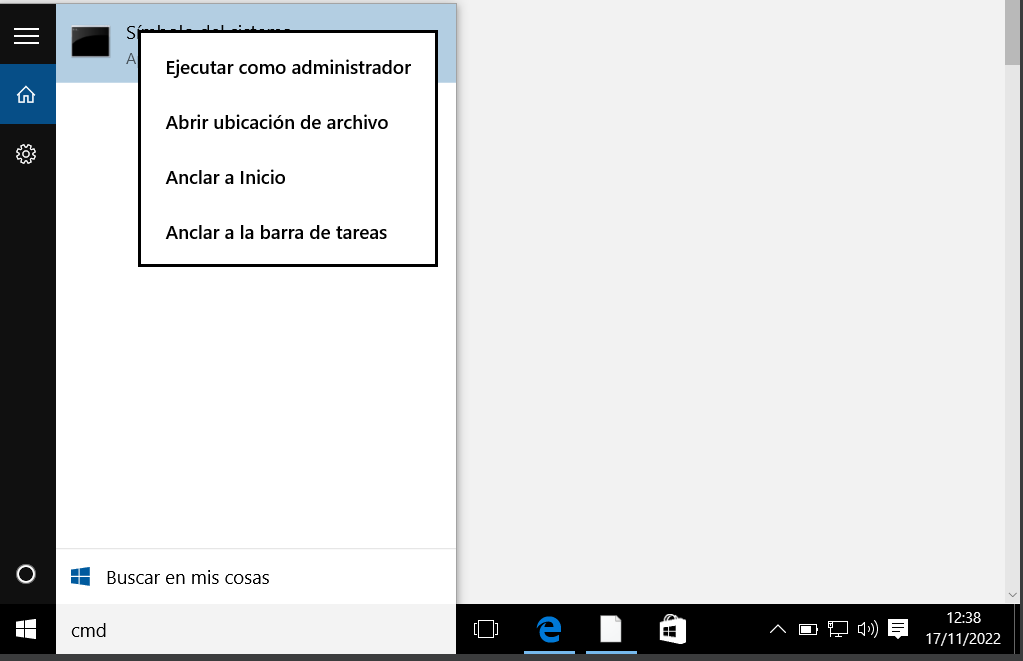


b. Descarrega’t Mimikatz en alguna carpeta del sistema víctima

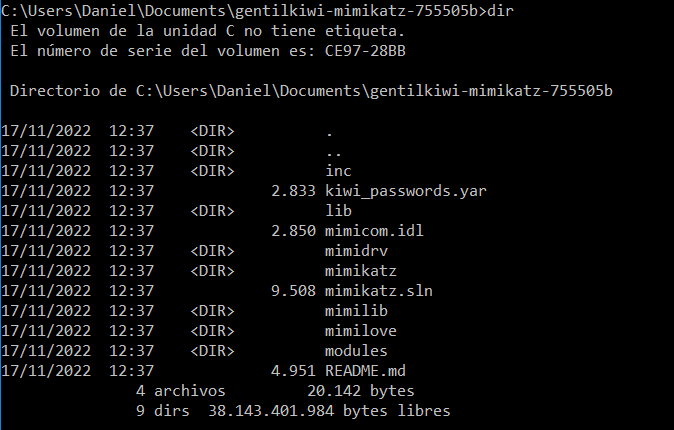


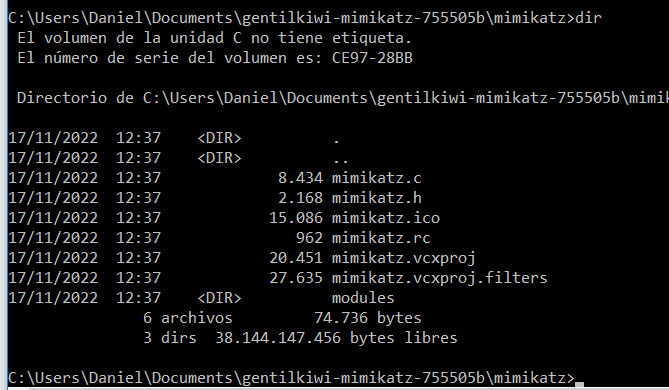


c. Obre un cmd com a usuari administrador



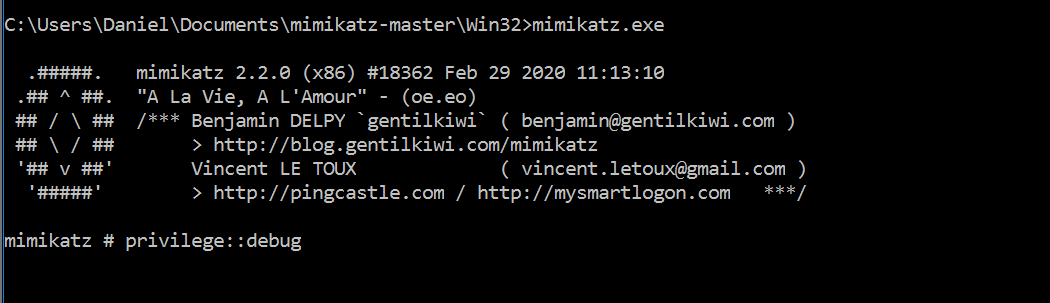
d. Des del terminal cmd, ves a la carpeta on has descomprimit Mimikatz i executa’l

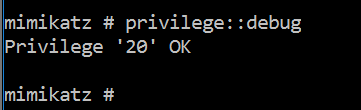




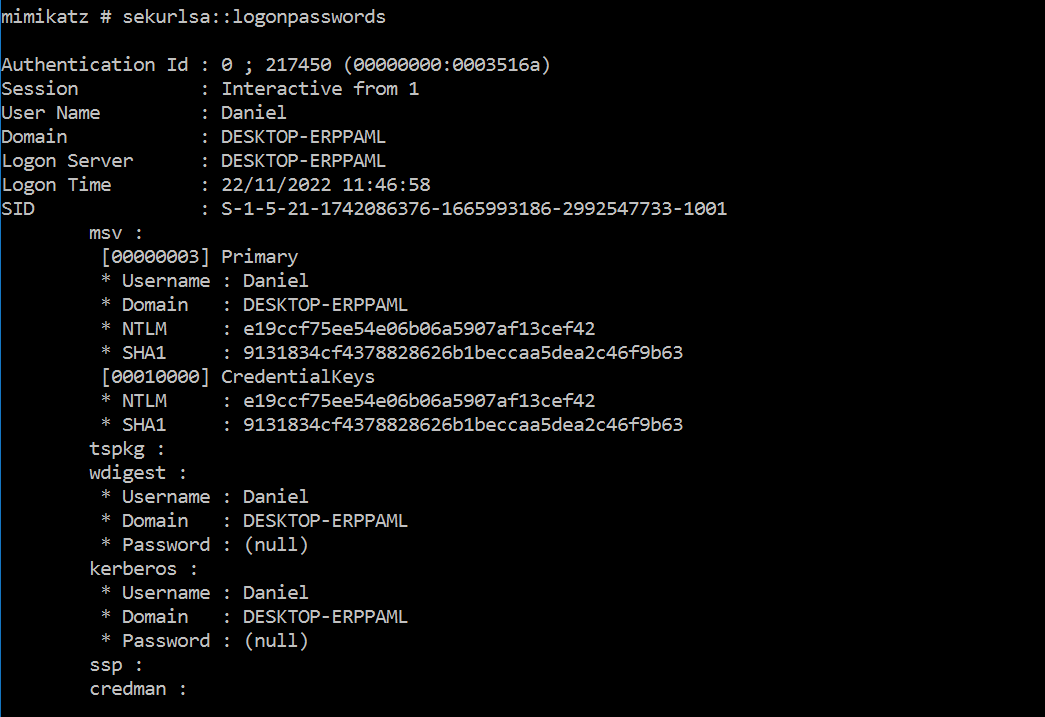
e. Dins de la pantalla de Mimikatz, executa → privilege::debug

→ hauria de donar missatge à privilege‘20’ OK

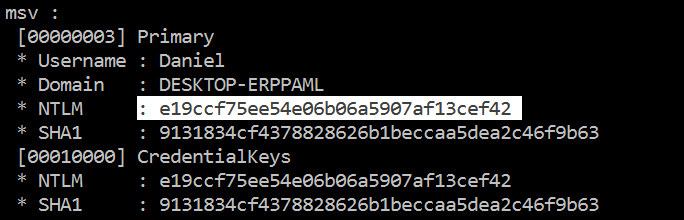


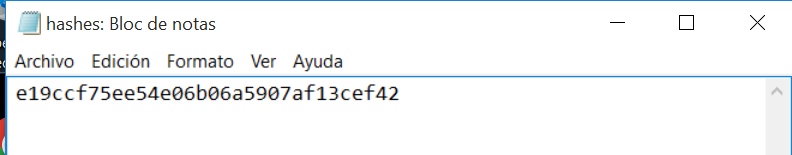


f. Seguidament des de M-imikatz, executa à sekurlsa::logonpasswords



g. Del llistat que apareix, busca els usuaris dels quals vulguis trobar el password i còpia els seus hashes -NTLM en un fitxer de text à hashes.txt





# 

# Exercici 2 – Força bruta contra el fitxer de hashes amb hashcat

a. Crea o descarrega’t algun diccionari de passwords à Recorda que Kali incorpora alguns diccionaris en la ruta à \usr\share\wordlists

→ El diccionari Rockyousi està comprimit, per descomprimir-lo

→ gzip -d rockyou.txt.gz

→ Pots trobar molts diccionaris de paraules a internet, per exemple: https://github.com/danielmiessler/SecLists/tree/master/Passwords/Common-Credentials

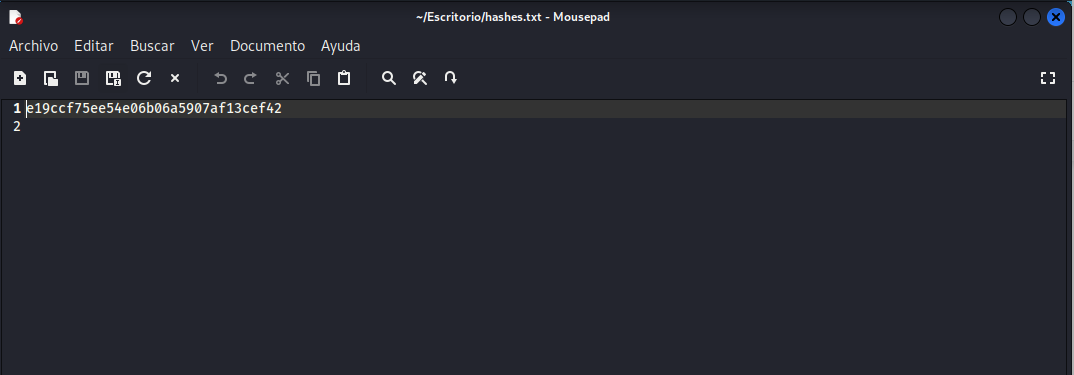
→ Recorda que també pots crear el teu diccionari amb l’eina à crunch





b. Instal·la’t hashcat en la màquina Windows 10, o pots treballar directament amb Kali Linux, però hauràs de passar el fitxer hashes.txt

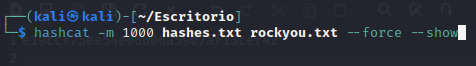
Treballaré amb kali linux, el que faré es escriure en hash en un document del kali:

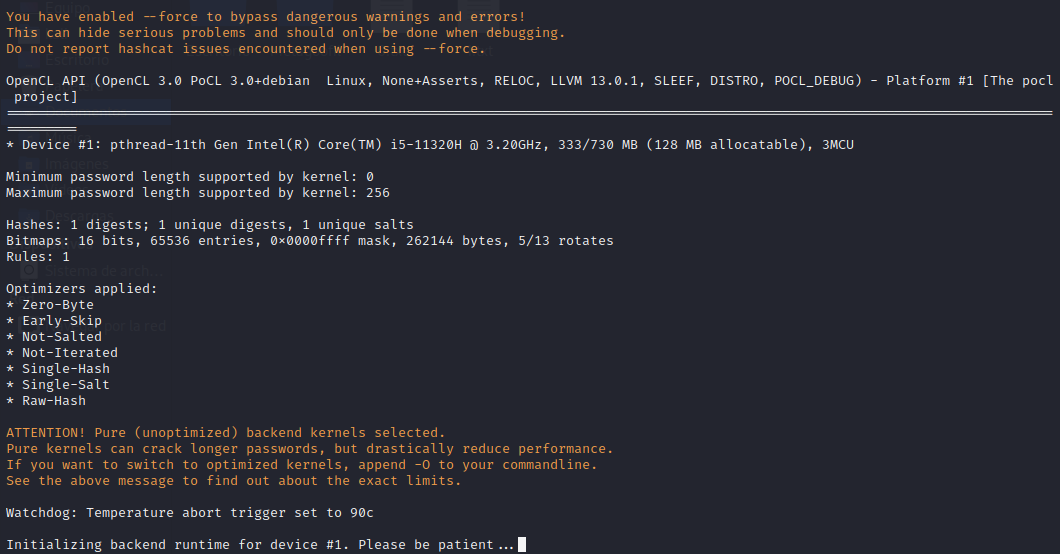


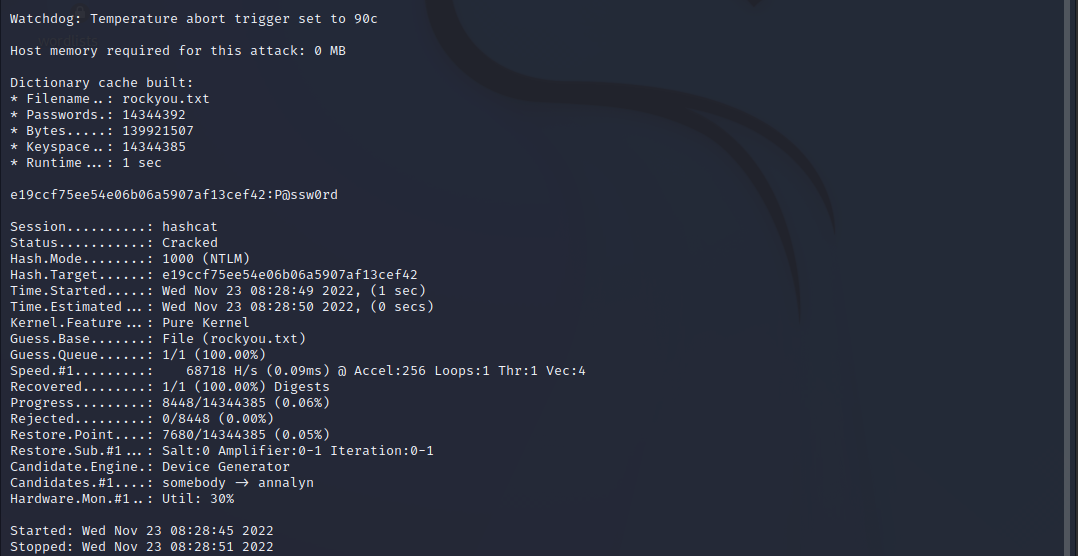
c. Per a fer l’atac, executa la següent sentència, des de la carpeta de hashcat

→ ./hashcat -m 1000 hashes.txt nom\_diccionari.txt --force --show

→ Observació: -m és per indicar que els hashes són en format NTLM





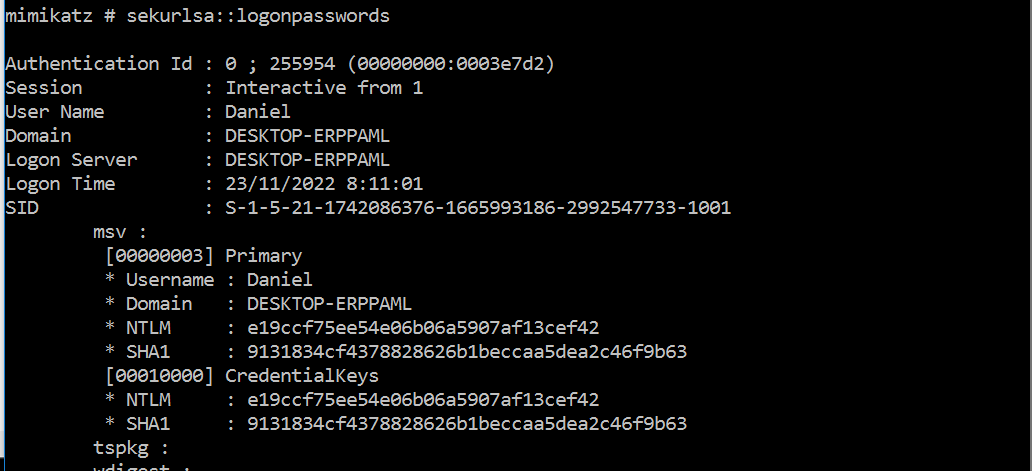


d. Comenta els resultats obtinguts

Podem observar que a sota del dictionary cache built, ens posa el hash de la contrasenya del usuari de windows 10, i a continuació la contrasenya del usuari.

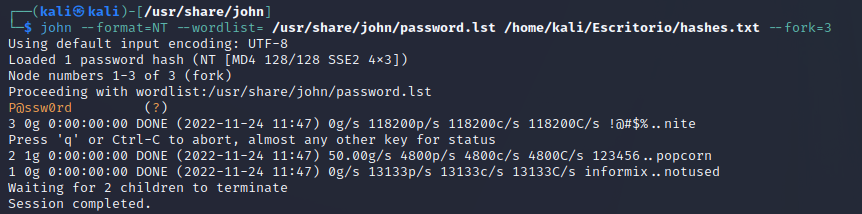
# Exercici 3 – Força bruta contra el fitxer de hashes amb John The Ripper

Torna a provar l’últim exercici però en comptes d’utilitzar hashcat, utilitza John The Ripper. Observació: - Tingues en compte que el format NTLM s’especifica → --format=NT



Extreurem el hash del password en NTLM (igual que al exercici anterior), i executarem la següent comanda al kali linux.

He utilitzat el document “password.lst” que inclou John The Ripper:



He hagut de modificar el arxiu de password.lst perquè no existía en aquell document el password “P@ssw0rd”:



