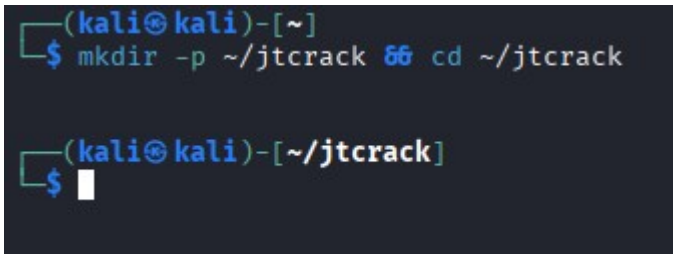
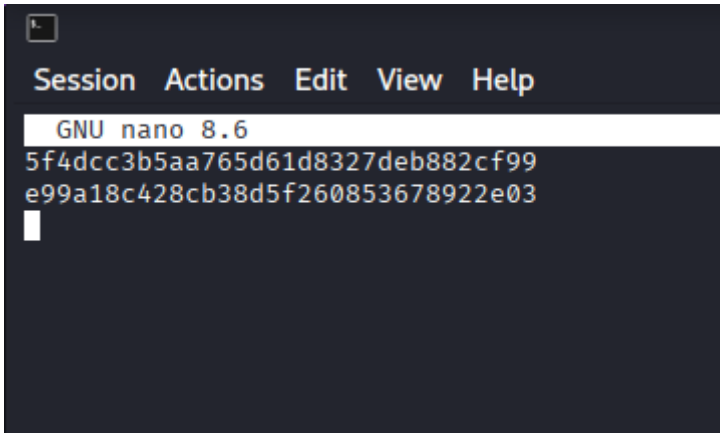
W14D1 – FRANCESCO MONTALTO

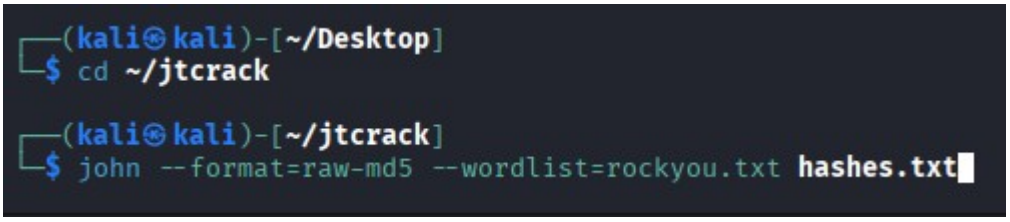
1.Innanzitutto ho creato una cartella ~/jtcrack su Kali (in quanto utilizzerò John The Ripper) e mi sono posizionato al suo interno per contenere tutti i file relativi all'operazione di cracking (hash, wordlist, output).



2. Ho poi creato il file hashes.txt e per incollare gli hash estratti dalla SQLi., tramite il classico nano (nano hashes.txt).
Ci ho incollato dentro ogni hash, su una riga separata.

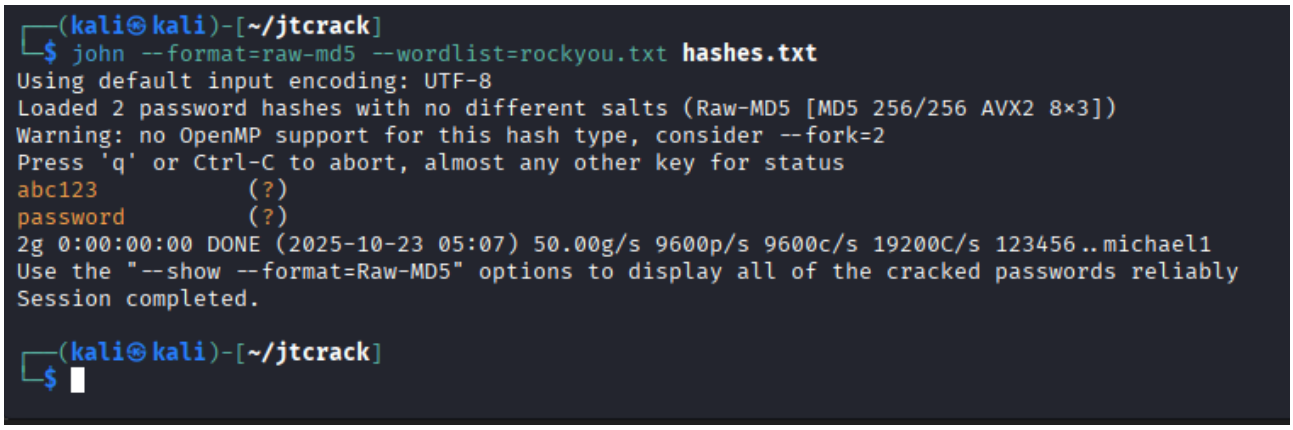


3. A questo punto ho ritenuto opportuno tentare subito con un attacco dizionario usando rockyou. Chiaramente ho copiato rockyou.txt in ~/jtcrack per tenerla insieme agli hash e ai log dell'attività.



“rockyou.txt” è una wordlist che ho scoperto essere molto utilizzata nei test di cracking password. Deriva da una raccolta di password reali (ottenute da data breach pubblici) e contiene milioni di password in chiaro, in ordine di popolarità d’uso.

4. Interpretazione dell’output.



john --format=raw-md5 --wordlist=rockyou.txt hashes.txt
Comando eseguito: avvia John the Ripper specificando che gli hash sono MD5 puri (raw-md5) e che deve provare le parole contenute nella wordlist rockyou.txt sul file hashes.txt.

Loaded 2 password hashes with no different salts (Raw-MD5 ...)
John ha caricato 2 hash MD5 e conferma che non sono stati usati salt diversi: significa che sono hash MD5 “nudi”, quindi confrontabili direttamente con MD5(parola) delle wordlist.

Warning: no OpenMP support for this hash type, consider –fork=2
John segnala che non sta usando parallelismo OpenMP per accelerare; si può accelerare il cracking con --fork=N su macchine multicore.

Press 'q' or Ctrl-C to abort, almost any other key for status
Indicazione interattiva: premi un tasto per vedere lo stato, q o Ctrl-C per fermare (ma John salva lo stato per poter riprendere).

Le due righe in output tipo abc123 e password (sotto le parentesi (?))
Durante l’esecuzione John ha provato parole e ha trovato due corrispondenze. Quelle righe sono anteprime delle password trovate (John mostra la parola candidata accanto).

2g 0:00:00:00 DONE (2025-10-23 05:07) 50.00g/s 9600p/s ...
Statistiche di fine sessione:

2g = 2 password trovate (2 guesses di successo),

50.00g/s ecc. = velocità (hash al secondo) e altre metriche
mostra anche esempi di password provate (123456..michael1) come anteprima del lavoro svolto.

5. Ho proceduto a craccare le password rimanenti, con lo stesso metodo.