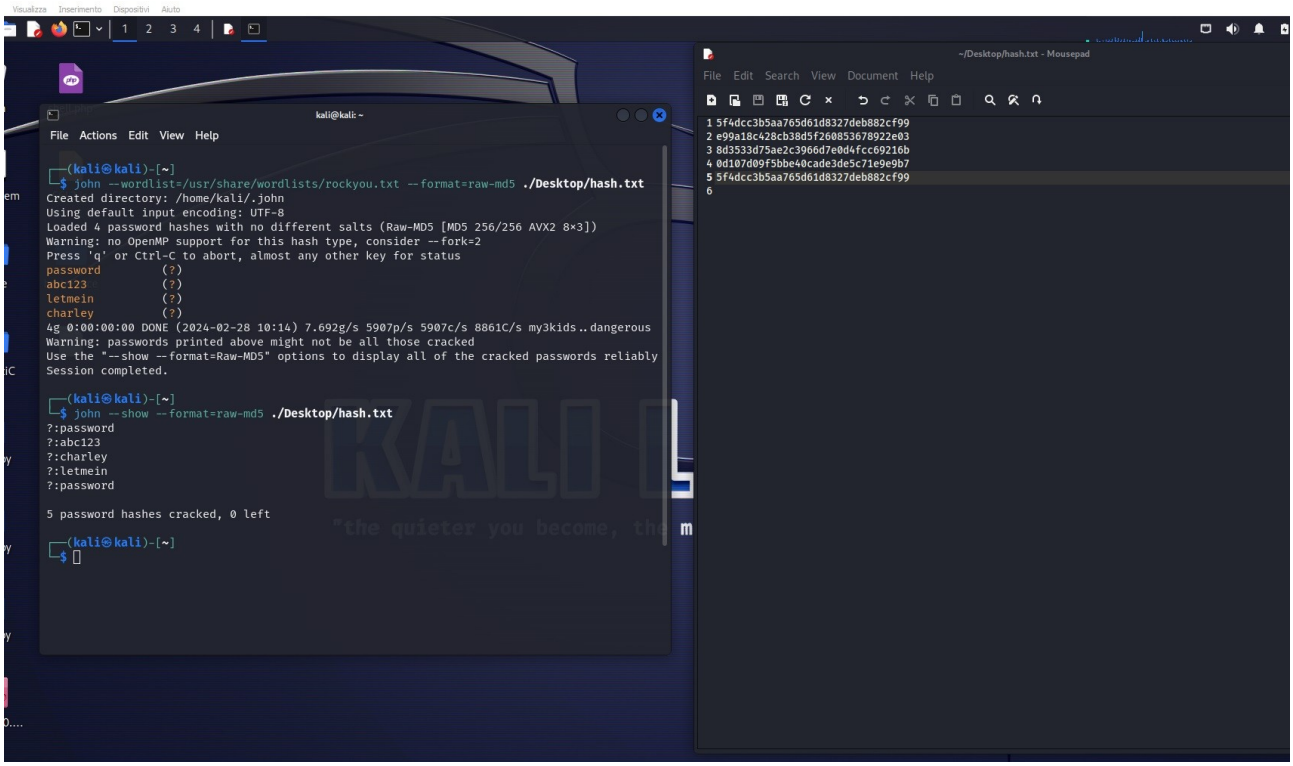

Come da immagine, ho estrapolato le password codificate in hash dalla UNION based SQLinjection fatta nell'esercizio precedente e le ho salvate in un file di testo. Dopodiche' ho aperto l'applicazione johntheripper da terminale e gli ho indicato dove andare a prendere la lista di parole che deve criptare in hash(rockyou.txt), gli hash salvati nel file di testo(hash.txt) con i quali deve trovare riscontro e il tipo di algoritmo per l'hash(DM5).
Johntheripper e' un tool per decifrare password da offline a differenza di Hydra che lo fa da online.
Durante la scansione john rende gia' disponibili delle risoluzioni ma non e' possibile farvi affidamento in quanto il risultato finale potrebbe essere diverso.
Per avere il risultato definitivo bisogna usare il comando show.
Un'altra opzione di scansione e' il brute force puro, senza usare dizionari ma semplicemente andando a tentativi partendo da una cifra e incrementando in continuazione fino ad arrivare alla password completa; ovviamente questo metodo richiede molto piu' tempo e sforzo computazionale .