CONSEGNA 28 FEBBRAIO S6L3

L'obbiettivo di oggi è quello ci craccare delle password , mappate in una stringa arbitraria tramite la funzione hash. In Fig.1 vediamo le password criptate che andremo a "tradurre" tramite un tool di Kali, John the Ripper.

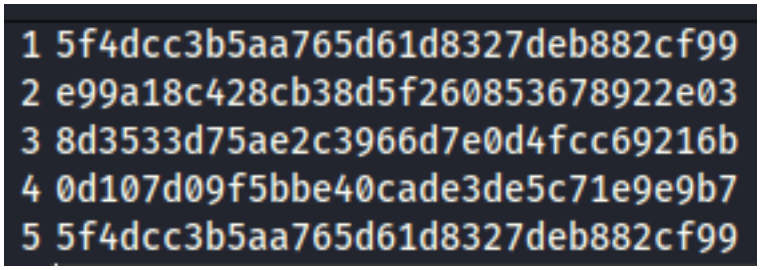

Fig.1

In Fig.2 possiamo vedere il programma in azione: ho usato la funzione wordlist , che andrà ad attingere password usuali da una lista in rockyou.txt, cripterà la password con la funzione crittografica MD5 e la confronterà con la lista di Fig.1 che ho inserito nel file hash.txt.

Fig.2

In breve tempo il tool mi ha restituito il risultato (Fig.3), sottolineo che le tempistiche sono state brevi perché le password era semplici, totalmente diverso è se andiamo ad inserire password non convenzionali perché le tempistiche si dilatano : possono volerci giorni.

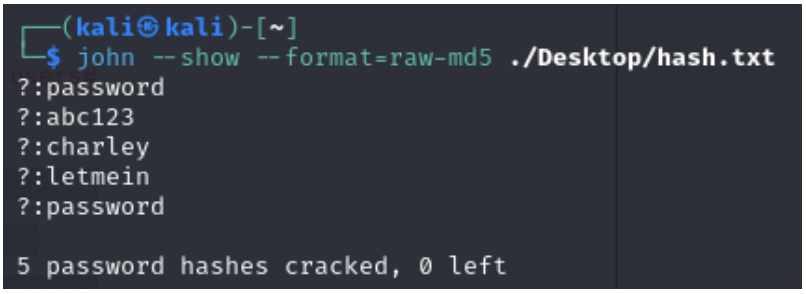

Fig.3

Ho anche provato ad usare l'incrementale (Fig.4), che funziona diversamente dalla wordlist: tenta di "scovare" la password provando carattere per carattere, ed incrementando lo stesso nella caso di esito negativo della prima prova,. Ho provato ad inserire una password casuale, per vedere se era all'interno di una delle lista offerte da seclists., ma date le tempistiche molto lunghe ho dovuto interrompere il processo.

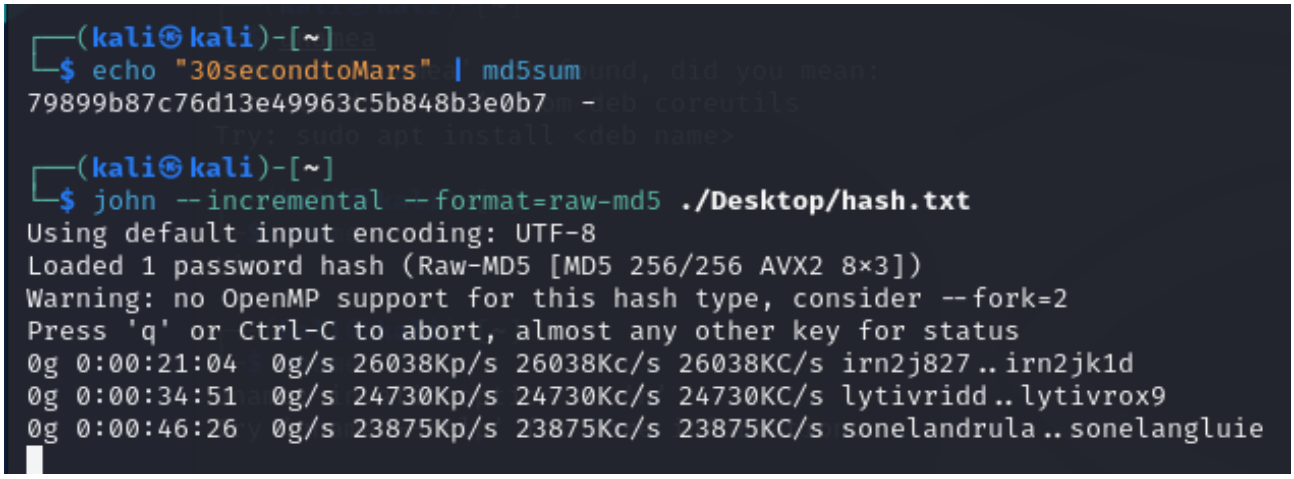

Fig.4