Nell’esercizio odierno abbiamo una serie di password, che tuttavia non ci vengono restituite in chiaro, ma come hash. Attraverso questa tecnica i siti web possono camuffare le password che hanno nel loro database e renderle incomprensibili ad eventuali Black Hat Hacker.

Esistono, tuttavia dei tool molto potenti (già installati su Kali Linux) che si occupano proprio di decifrare gli hash. Uno di questi è “John the Ripper”. Vediamo di seguito come fare per decifrare gli hash dell’esercizio:

- 5f4dcc3b5aa765d61d8327deb882cf99
- e99a18c428cb38d5f260853678922e03
- 8d3533d75ae2c3966d7e0d4fcc69216b
- 0d107d09f5bbe40cade3de5c71e9e9b7
- 5f4dcc3b5aa765d61d8327deb882cf99

Poiché sappiamo già che l’algoritmo di hashing è md5, il comando che utilizziamo su John the Ripper è il seguente: “john --format=raw-md5 --incremental (file da decifrare)". Vediamo il programma in funzione:

Otteniamo, così le seguenti password: “charley”, “letmein”, “abc123”, “password”.