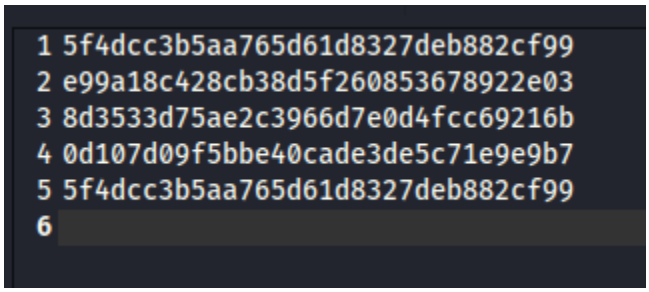
ESERCIZIO S6L3

Traccia: Password cracking. Sentitevi liberi di utilizzare qualsiasi tool o soluzione alternativa. L'obiettivo dell'esercizio di oggi è craccare tutte le password. Le password da craccare sono le seguenti:

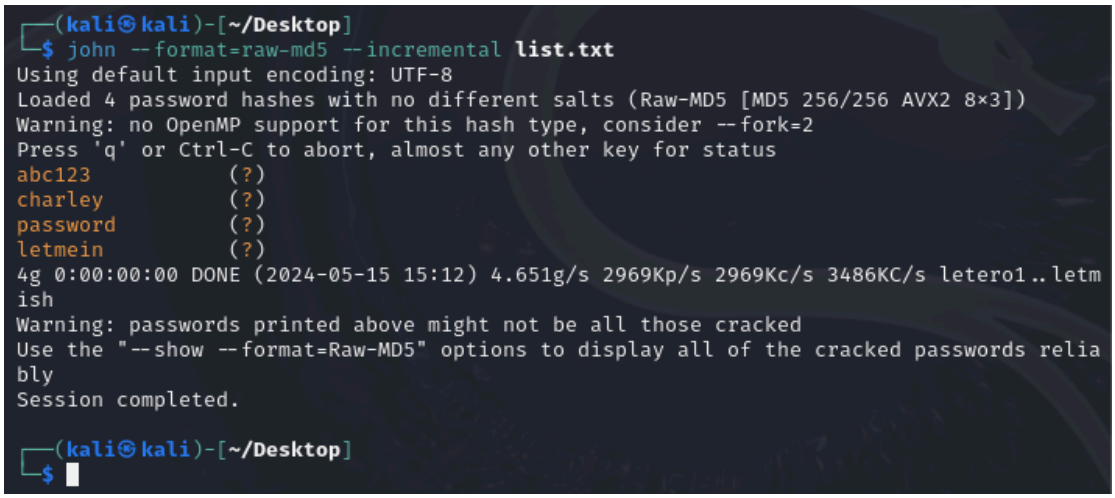
- 5f4dcc3b5aa765d61d8327deb882cf99
- e99a18c428cb38d5f260853678922e03
- 8d3533d75ae2c3966d7e0d4fcc69216b
- 0d107d09f5bbe40cade3de5c71e9e9b7
- 5f4dcc3b5aa765d61d8327deb882cf99

SVOLGIMENTO

Per poter craccare le password in hash scritte sopra si è usato il tool John The Ripper, un password cracking molto noto. Inizialmente si è creato un file che contenesse una lista di tutte le password scritte in hash, il file è stato chiamato **list.txt**.



Successivamente da terminale Kali, ci si è messi nella shell che contiene il file creato list.txt prima di lanciare John.



Con il primo comando codifichiamo il "**--format=raw-md5**", specifica il formato dell'hash che si sta cercando di craccare. Nel contesto di un hash MD5, questo indica che il programma dovrebbe interpretare l'hash come un hash MD5.
L'opzione "**--incremental**" in John the Ripper indica che l'attacco condotto sarà un attacco incrementale. Significa che John the Ripper proverà a generare e testare password in modo incrementale, cioè, generando e testando combinazioni di caratteri in modo sequenziale, partendo da una certa lunghezza e procedendo gradualmente fino a raggiungere una lunghezza massima specificata o fino a quando non viene trovata una corrispondenza.

Come si nota dall'immagine in alto, John The Ripper è riuscito a craccare le password scritte in hash e le ha stampate a schermo in colore arancione.
Di seguito scriviamo la password in hash e il corrispettivo in chiaro:

- 5f4dcc3b5aa765d61d8327deb882cf99 → abc123
- e99a18c428cb38d5f260853678922e03 → charley
- 8d3533d75ae2c3966d7e0d4fcc69216b → password
- 0d107d09f5bbe40cade3de5c71e9e9b7 → letmein
- 5f4dcc3b5aa765d61d8327deb882cf99 → abc123