ATTACHI

BRUTE-FORCE

```
┌──(kali㉿kali)-[~/Desktop/S6 L3]
└─$ john --format=raw-md5 --incremental Hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Remaining 2 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=8
Press 'q' or Ctrl-C to abort, almost any other key for status
charley          (?)
letmein          (?)
2g 0:00:00:00 DONE (2024-05-15 09:51) 2.597g/s 3316Kp/s 3316Kc/s 3344KC/s letebru..letmish
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Ho usato John the Ripper per eseguire un attacco brute-force per trovare il testo corrispondete all'Hash all'interno del file "Hash.txt"

- john: È il comando principale per avviare John the Ripper;
- --format=raw-md5: Specifica il formato dell'hash da decifrare. In questo caso, "raw-md5" indica che l'hash è nel formato MD5;
- --incremental: Indica a John the Ripper di eseguire un attacco di forza bruta incrementale. Questo significa che proverà tutte le possibili combinazioni di caratteri in modo incrementale;
- Hash.txt: È il nome del file che contiene gli hash da decifrare.

In questo caso visualizziamo soltanto 2 password perché prima ho provato ad eseguire il comando solamente sui primi 2 codici, e John conoscendo già le password associate non andra a ricercarle.
Questo comando è utile quando non si ha alcuna informazione sulla password e si desidera provare tutte le possibili combinazioni di caratteri. Tuttavia, l'attacco brute-forcepuò richiedere molto tempo, specialmente per password complesse o lunghe.

Questa riga di comando esegue John the Ripper per mostrare le password trovate durante il cracking dell'hash contenuto nel file "Hash.txt":

- --show: Questa opzione indica a John the Ripper di mostrare le password trovate durante il processo di cracking;
- --format=raw-md5: Specifica il formato dell'hash;
- Hash.txt: John utilizzerà l'hash presente in questo file per visualizzare le password trovate.

Questo comando è utile dopo aver eseguito il cracking dell'hash, poiché ti consente di visualizzare le password trovate.
Qui verranno mostrate tutte le password trovate per quel file, anche se fatte in scansioni precedenti.