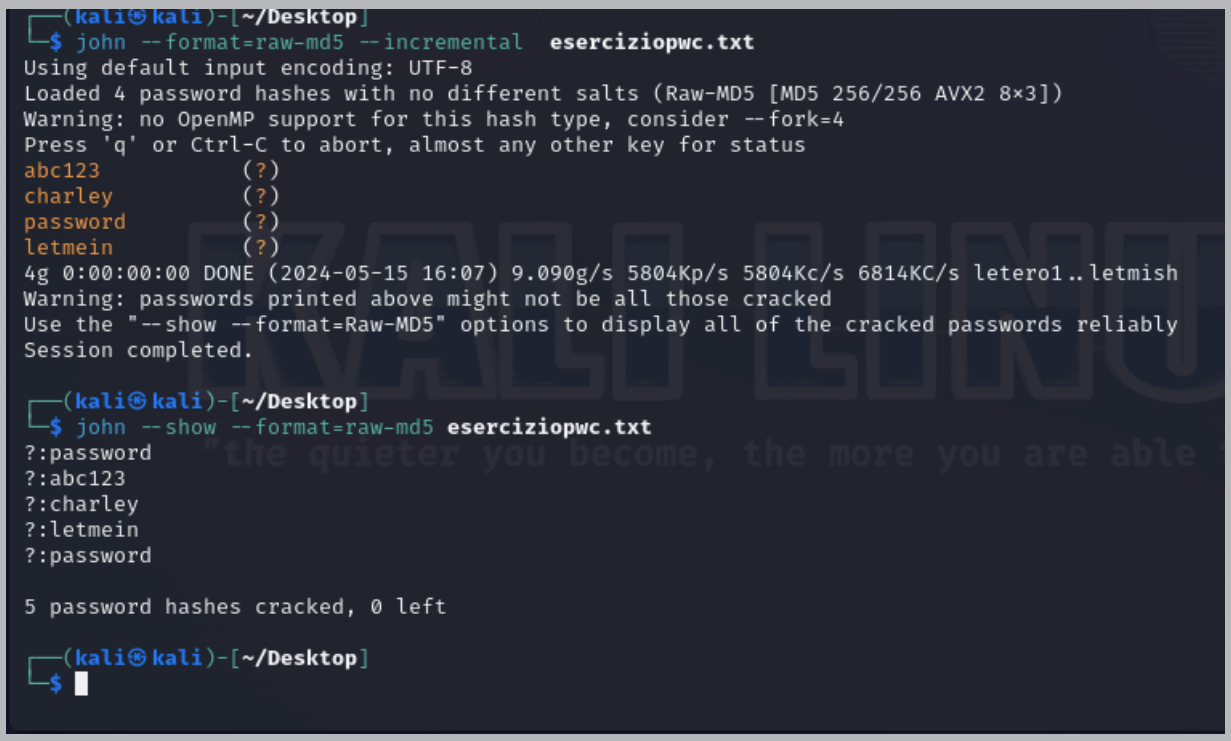
PASSWORD CRAKING

WITH JOHNTHERIPPER



in questo esercizio, utilizzeremo John the Ripper, un potente strumento di cracking delle password, per decifrare delle password hashate salvate in un file su Kali Linux. In particolare, ci concentreremo su hash di tipo MD5.

Creazione del File di Hash

Creiamo un file sul desktop di Kali Linux che contenga le password hashate in formato MD5. Gli hash MD5 sono una rappresentazione crittografica delle password, generata tramite l'algoritmo MD5 che produce una fingerprint di 128 bit rappresentata come 32 caratteri esadecimali.

Utilizzo di John the Ripper

-Una volta creato il file, utilizziamo John the Ripper per tentare di decifrare queste password. Il comando da eseguire è **john --format=raw-md5 --incremental nomefile.txt**. Questo comando specifica che gli hash nel file sono in formato MD5 e utilizza un attacco brute-force incrementale che tenta tutte le possibili combinazioni di caratteri.

Visualizzazione delle Password Decifrate

Dopo aver eseguito il comando, visualizziamo le password che John the Ripper è riuscito a decifrare con il comando **john --show --format=raw-md5 nomefile.txt.**

Decodifica degli Hash MD5

Gli hash MD5 sono sequenze crittografiche che rappresentano le password in un formato non leggibile. Quando John the Ripper decifra un hash, restituisce la password in chiaro. Questa password è la rappresentazione UTF-8 dei caratteri originali.

UTF-8 è uno standard di codifica che può rappresentare qualsiasi carattere del set Unicode utilizzando una sequenza variabile di 1-4 byte. È lo standard internazionale per la rappresentazione dei caratteri su internet e nei file di testo.

Quando John the Ripper decifra un hash, converte l'hash crittografato in una stringa di caratteri UTF-8. Questa conversione avviene perché John the Ripper, durante il processo di cracking, confronta gli hash calcolati dalle combinazioni di caratteri con gli hash presenti nel file. Una volta trovata una corrispondenza, la stringa di caratteri che ha generato quell'hash viene restituita come password in chiaro.

Conclusione

Seguendo questi passaggi, siamo riusciti a decifrare le password hashate salvate in un file utilizzando John the Ripper su Kali Linux. Il comando john --format=raw-md5 --incremental nomefile.txt ci ha permesso di decifrare gli hash MD5, restituendo le password in chiaro nel formato UTF-8. Questo processo dimostra come gli hash possono essere decifrati utilizzando tecniche di brute-force e l'importanza di utilizzare password complesse per migliorare la sicurezza.