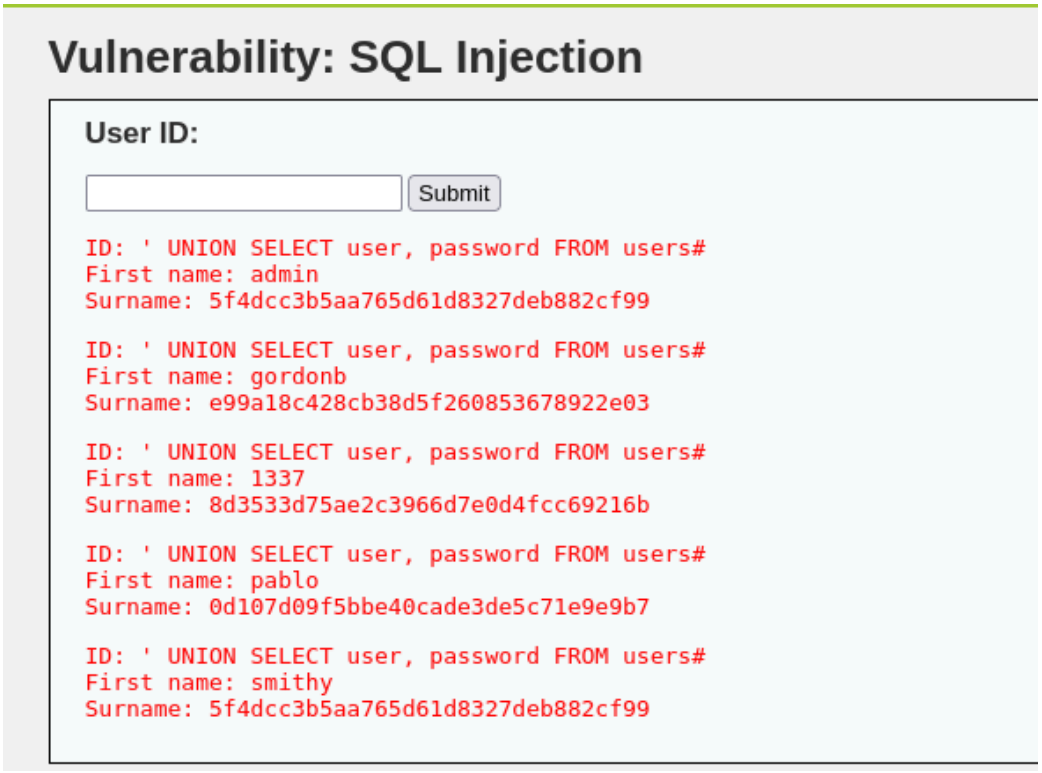
Nella lezione di ieri abbiamo trovato unendo le tabelle gli users e le password (in formato Hash)



Le hash di password MD5 rappresentano una tecnologia crittografica ampiamente utilizzata per garantire la sicurezza delle password all'interno dei sistemi informatici. L'MD5, acronimo di "Message Digest Algorithm 5", è un algoritmo di hash che converte in modo univoco un input di lunghezza variabile in una sequenza alfanumerica fissa di 32 caratteri. Questa sequenza, nota come hash, è tipicamente utilizzata per rappresentare la password in maniera sicura, senza memorizzare il testo della password in chiaro.

L'utilità principale delle hash MD5 risiede nella protezione delle informazioni sensibili, come le password degli utenti. Quando un utente crea o modifica la propria password, il sistema applica l'algoritmo MD5 per generare l'hash corrispondente. L'hash viene quindi memorizzato nel database al posto della password in chiaro. Questo approccio aumenta la sicurezza poiché le password non sono direttamente accessibili e non possono essere lette o recuperate in caso di accesso non autorizzato al database.

Tuttavia, è importante notare che l'MD5 ha dimostrato alcune vulnerabilità nel corso degli anni, rendendo possibile attacchi di tipo "rainbow table" e altre tecniche di decriptazione. A causa di tali preoccupazioni per la sicurezza, l'industria ha spostato l'attenzione verso algoritmi di hash più sicuri, come SHA-256 e SHA-3.

In questa lezione, esploreremo il funzionamento delle hash di password MD5, le loro limitazioni in termini di sicurezza, e l'importanza di implementare pratiche aggiuntive, come l'utilizzo di salt, per rafforzare la protezione delle password all'interno dei sistemi informatici.

L'algoritmo MD5 è stato progettato per produrre un hash di dimensioni fisse, indipendentemente dalla lunghezza dell'input. Questo rende l'MD5 particolarmente utile per la memorizzazione di password, poiché consente di rappresentare in modo coerente anche password di lunghezza diversa con una stringa fissa di 32 caratteri esadecimali. La velocità di calcolo e l'efficienza dell'MD5 hanno contribuito alla sua diffusa adozione in sistemi operativi, applicazioni web e database.

Vulnerabilità di MD5

Nonostante la sua popolarità, l'MD5 ha dimostrato alcune vulnerabilità nel corso degli anni. La più significativa è la sua suscettibilità agli attacchi di "collisione", in cui due input diversi possono produrre lo stesso hash. Questo ha reso l'MD5 inadatto per applicazioni in cui la sicurezza è cruciale, poiché un attaccante potrebbe creare intenzionalmente una password diversa che produce lo stesso hash, ottenendo così un accesso non autorizzato.

Evoluzione della Sicurezza delle Password

A causa delle vulnerabilità scoperte, la comunità della sicurezza informatica ha spostato l'attenzione su algoritmi di hash più sicuri, come SHA-256 e SHA-3, che offrono una maggiore resistenza contro gli attacchi di collisione e forza bruta. Tuttavia, è importante notare che la sicurezza di un sistema password non si basa solo sull'algoritmo di hash utilizzato, ma anche su pratiche aggiuntive come l'uso di salt.

Ruolo dei Salt nella Sicurezza delle Password

L'introduzione di salt, ovvero stringhe casuali uniche associate a ciascuna password prima di essere hashate, aumenta notevolmente la sicurezza complessiva. I salt rendono più difficile l'utilizzo di tecniche come le tabelle arcobaleno (rainbow tables) e rafforzano la protezione contro attacchi di forza bruta. Pertanto, anche se l'MD5 ha le sue limitazioni, l'implementazione di buone pratiche può ancora garantire una sicurezza accettabile nelle applicazioni in cui è utilizzato.

Per completare l’esercizio andiamo a utilizzare

John the Ripper è uno degli strumenti più potenti e ampiamente utilizzati per il cracking delle password. Integrato spesso nei sistemi operativi basati su Unix, John the Ripper è particolarmente noto per la sua efficacia nella violazione di hash di password mediante attacchi di tipo dictionary o brute-force.

Caratteristiche Principali di John the Ripper:

Password Cracking: John the Ripper è specializzato nel cracking delle password attraverso attacchi di forza bruta o utilizzando dizionari di parole. Questo strumento è in grado di testare migliaia di password al secondo, cercando di trovare una corrispondenza con l'hash di una password memorizzato nel sistema.

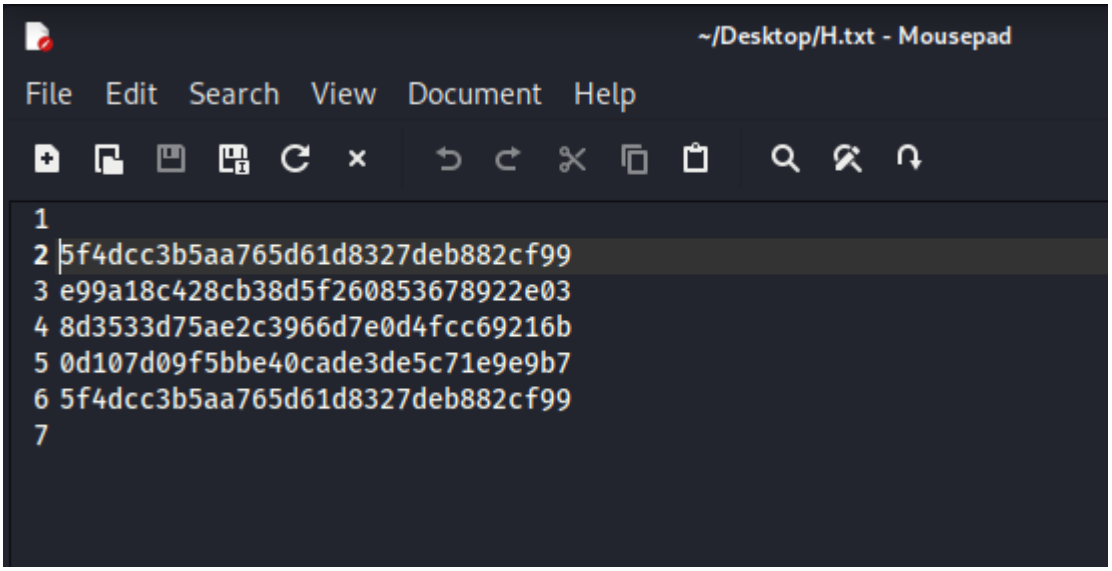
Supporto per Diversi Algoritmi di Hash: John the Ripper supporta vari algoritmi di hash, inclusi MD5, SHA-1, SHA-256, e molti altri. Questa flessibilità lo rende adatto per una vasta gamma di scenari di cracking.

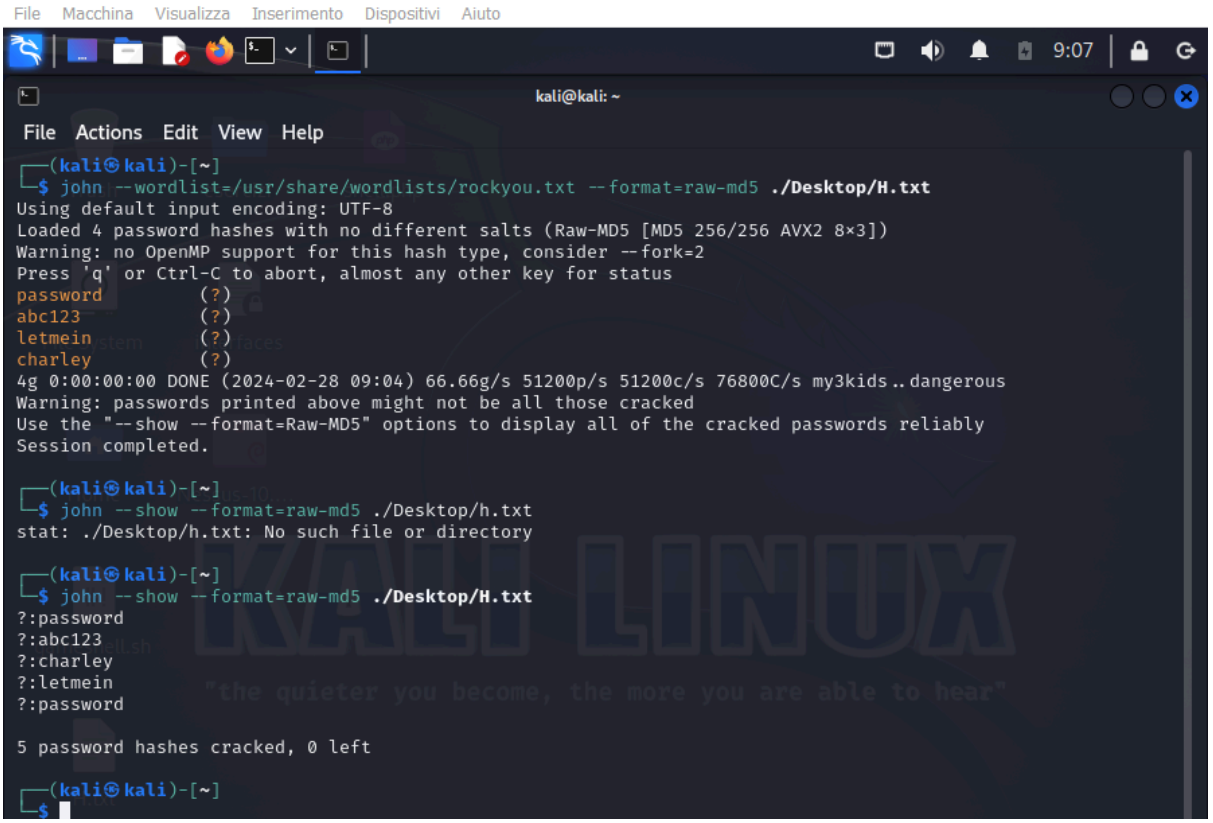
Modalità di Utilizzo Flessibili: John the Ripper può essere utilizzato in diverse modalità, come "single crack" per violare una singola password o "incremental" per eseguire attacchi di forza bruta su una gamma di possibili password.

Supporto per GPU: Questo strumento può sfruttare la potenza di elaborazione delle GPU per aumentare significativamente le prestazioni durante gli attacchi di cracking delle password.

Per utilizzare John the Ripper su Kali Linux, è possibile eseguire comandi dalla shell con opzioni specifiche per avviare attacchi di cracking su file di hash di password o su account specifici.

Alla luce di ciò detto sopra John troverà le nostre password una volta creato il file H.txt e selezionato il file già presente in Kali rockyou.txt





una volta finita l’elaborazione chiederemo al programma di mostrare i risultati ottenuti.

Grazie per l’attenzione