Traccia: password cracking

Abbiamo visto come sfruttare un attacco SQL injection per recuperare le password degli utenti di un determinato sistema.
Se guardiamo meglio alle password trovate, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5.

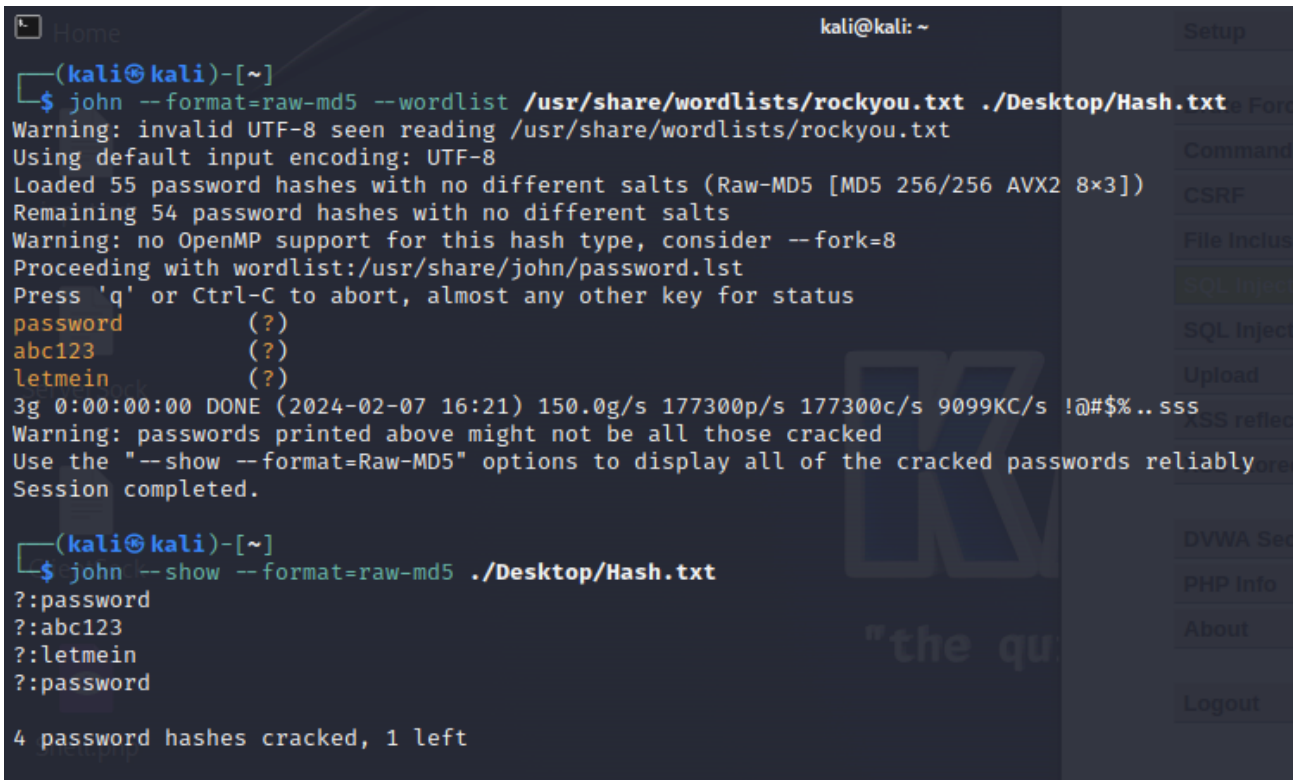
Recuperate le password dal DB come visto, e provate ad eseguire delle sessioni di cracking sulla password per recuperare la loro versione in chiaro.

Sentitevi liberi di utilizzare qualsiasi dei tool visti nella lezione teorica.

L'obiettivo dell'esercizio di oggi è craccare tutte le password trovate precedentemente.

Consegna:

1. Screenshot dell'SQL injection già effettuata
2. Due righe di spiegazione di cos'è questo cracking (quale tipologia / quale meccanismo sfrutta)
3. Screenshot dell'esecuzione del cracking e del risultato



Utilizzando il tool John the Ripper con il flag –wordlist abbiamo dato in pasto allo stesso un file che contiene una wordlist con una serie di password ed i rispettivi hash insieme al file degli hash catturati.
Come si vede dallo screnshot il tool ha fatto dei confronti e trovato dei match positivi tra gli hash, grazie ai quali riusciamo a risalire alle password.