Attacco alle password

La protezione delle password è uno degli aspetti che dovrebbe generare più preoccupazione, specialmente nel momento in cui le password sono potenzialmente accessibili a chiunque e con queste si può accedere a sistemi o informazioni sensibili.

Come vengono memorizzate le password oggi

- Noi inseriamo la password in chiaro su Amazon
- Il server Amazon produce il codice hash e lo conserva nel su database (durante la registrazione)
- Il server Amazon produce il codice hash e lo confronta con l'hash salvato nel database (durante il login)
- Se l'hash corrisponde, l'autenticazione andrà a buon fine.

Si memorizza il codice hash per due motivi:

- **Non è reversibile**: non si può risalire alla password partendo dal codice hash
- **Integrità**: tramite l'hash, siamo sicuri che la password inserita è sicuramente quella corretta ed è integra

L'unico modo per risalire alla password tramite il codice hash è quello di **provare tutte le passwor**d finché non si trova una password con lo stesso codice hash.

In realtà, su siti come Amazon, utilizzano una tecnica chiamata "sale e pepe".

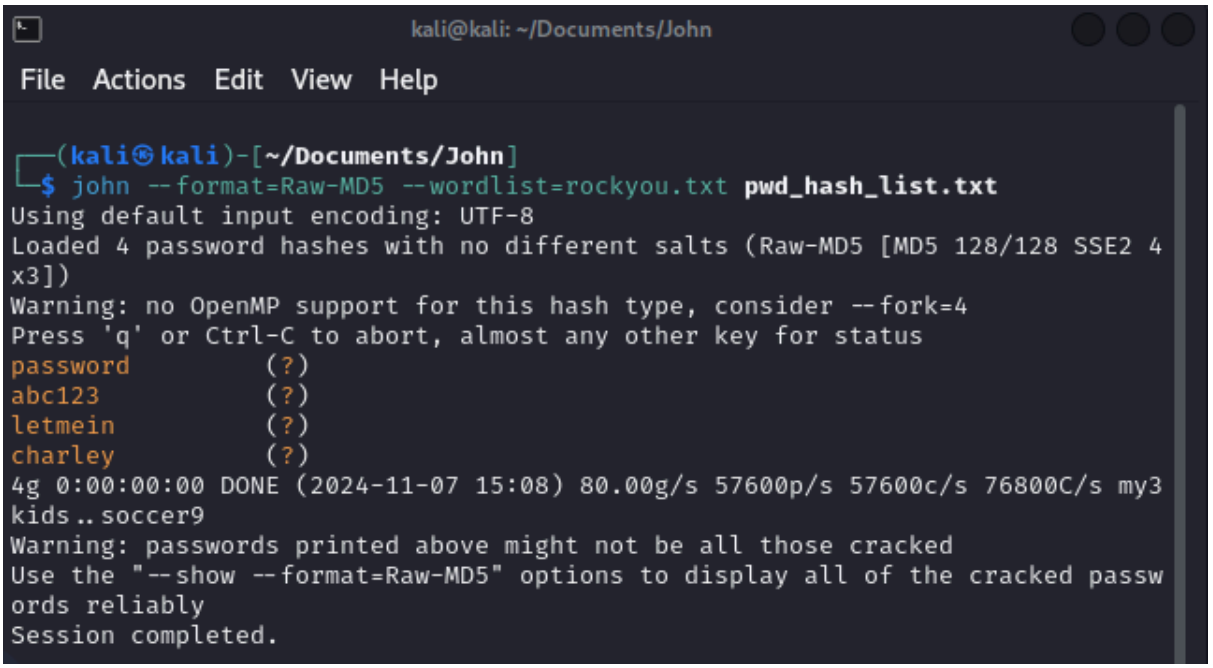
Anziché produrre il codice hash della nostra password, produce il codice hash della nostra password + **due caratteri aggiuntivi** (dipendono dal servizio).

Se la tua password è 123, allora amazon salverà l'hash di A123B.

Obiettivo dell’esercizio

Risalire alle password partendo dai codici hash. Gli hash sono stati rubati tramite una SQL Injection alla macchina DVWA.

Risultato dell’attacco



Tool: John the Ripper
Formato dei codici hash delle password: MD5
Dizionario: rockyou.txt (uno dei più famosi e diffusi)

In pochi istanti, john è in grado di risalire alle password partendo dai codici MD5 rubati dalla DVWA.

Ci riesce in pochi istanti in quanto le password sono molto semplici. Se le password fossero più complesse, potrebbero volerci ore, giorni, settimane o anni.

Una dimostrazione chiara del perché è necessario utilizzare password complesse 🙂