Traccia: password cracking

Se guardiamo meglio le password, della lezione precedente, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5.

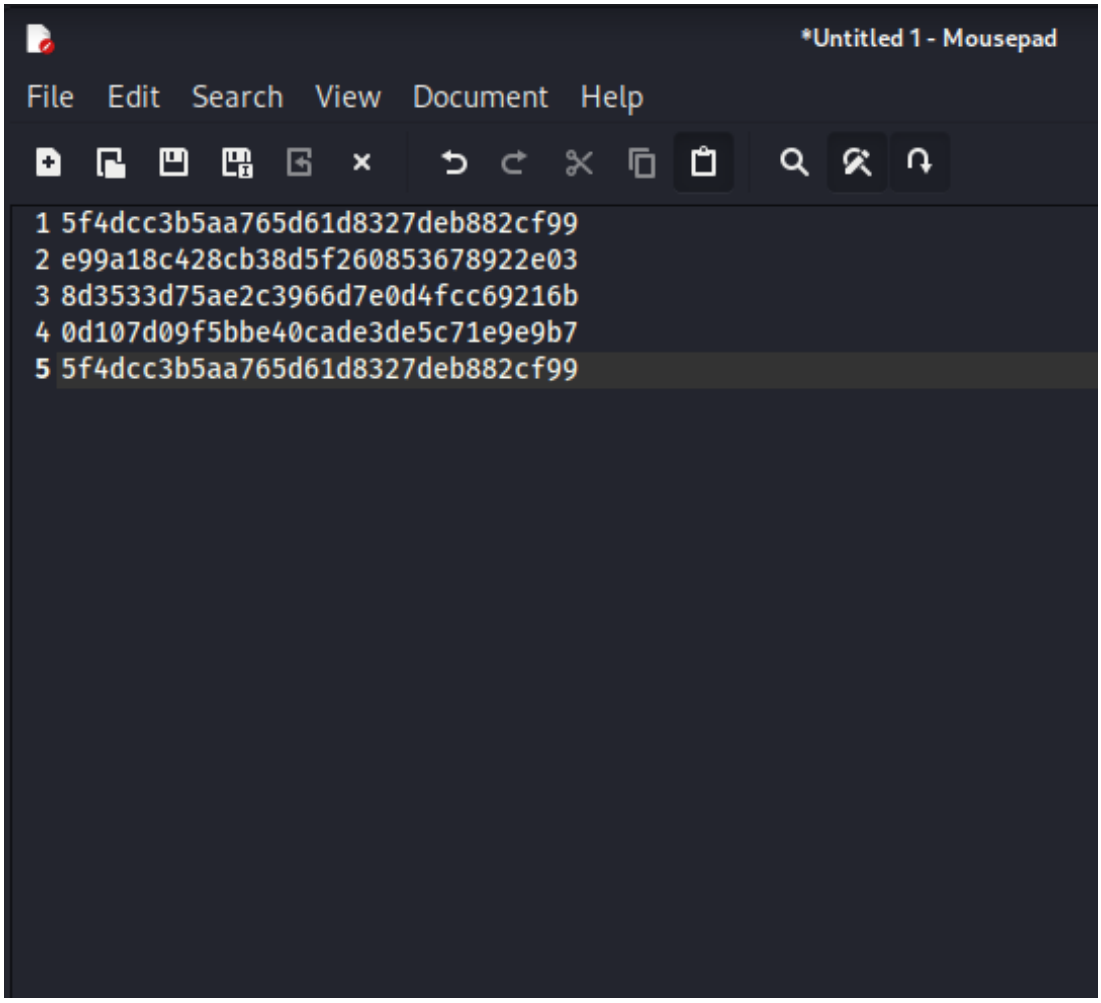
Recuperate le password dal DB e provate ad eseguire delle sessioni di cracking sulla password per recuperare la loro versione in chiaro.

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

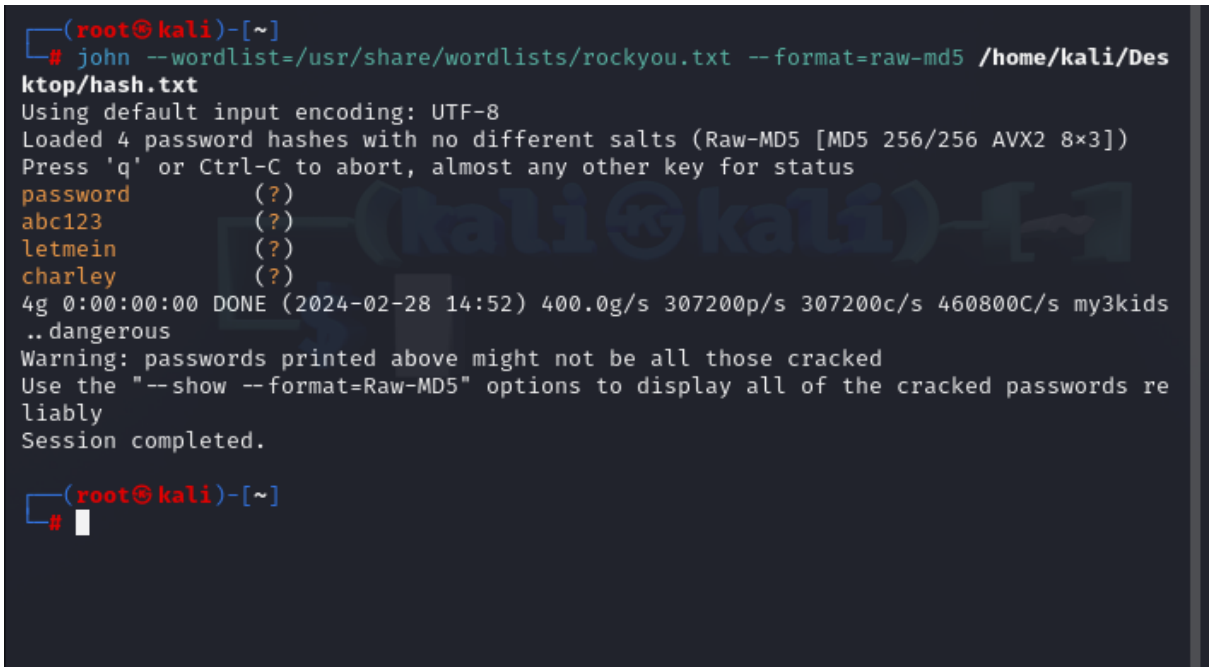
L'obiettivo dell'esercizio di oggi è craccare tutte le password.

Abbiamo iniziato con l'attacco al server per avere l'hash della password.

Ci creiamo il nostro file con mousepad.



E mandiamo il comando con John the Ripper.



Printiamo le password.

John the Ripper - una caratteristica notevole di questo tool è che può rilevare automaticamente la crittografia per i formati comuni. Questo ci farà risparmiare tempo nella ricerca dei formati hash e trovare lo strumento corretto per decifrarli.
Come funziona di default:

- Riconosce il tipo di hash dell'hash corrente
- Generare hash per tutte le password nel dizionario
- Si ferma quando un hash generato corrisponde all'hash corrente.