JOHN RIPPER

Nella lezione pratica di ieri, 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 ieri, 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.

Come prima cosa usiamo il comando SQL injection usato nell’esercizio precedente che interroga il data base e ci mostra le password in formato hash A screenshot of a computer

Description automatically generated

Come vediamo abbiamo preso di riferimento la prima password e caricata in una cartella chiamata Pass.txt dove inseriamo al suo interno la password in hash

A computer screen shot of a computer code

Description automatically generated

Adesso utilizzeremo il tool john the ripper che andrà a leggere il file e confronterà il codice hash in una lista predefinita di hash di password più comuni per ogni rispettivo algoritmo (es MD5,SHA1,SHA2 ecc)

A screenshot of a computer screen

Description automatically generated

A computer screen shot of a computer program

Description automatically generated