**PRATICA 07 NOVEMBRE 2024**

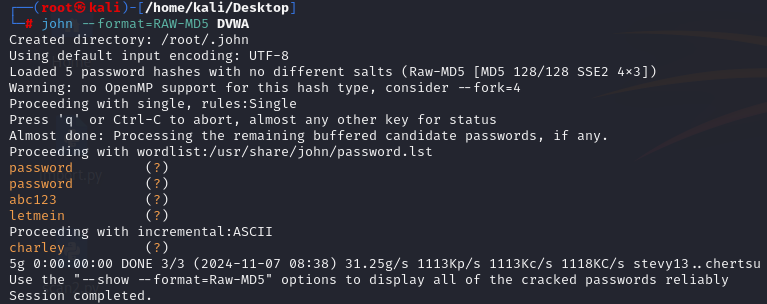
**Attacchi alle password**

L’obiettivo di oggi è recuperare le password in formato hash tipo MD5 utilizzando **John The Ripper**, un tool che serve al nostro scopo.

Dopo aver ottenuto le password dalla DVWA di **Metasploitable2** tramite l’SQL Injection effettuato pochi giorni fa dobbiamo, adesso, capirne il contenuto:



**JOHN THE RIPPER**

John the Ripper è uno degli strumenti di cracking delle password più conosciuti e utilizzati in ambito di sicurezza informatica, questo tool opera su file che contengono password cifrate in formato hash, un formato crittografato che garantisce la sicurezza dei dati sensibili.  
  
**Svolgimento**  
  
Recuperate le password in formato MD5, le andremo a scrivere su un file in formato .txt da dare in pasto a John tramite il seguente messaggio: john -format=RAW-MD5 **DVWA** (il nome del .txt in questo caso)  
  


Come possiamo vedere dall’immagine, le password sono state tradotte dal formato hash MD5 al formato in chiaro.

Per decriptare le password, andremo a dare il comando RAW-MD5 a John per fargli capire qual è il formato che deve andare a tradurre.