**S6 L4**

**AMATO SARA**

**PASSWORD CRACKING**

Recupero delle Password in Chiaro

L'obiettivo di questo esercizio è recuperare le password hashate nel database della DVWA (Damn Vulnerable Web Application) e eseguire il cracking di queste password per ottenere le loro versioni in chiaro, utilizzando gli strumenti di cracking appresi durante la lezione teorica.

Recupero delle Password dal Database

In questa fase, l'accesso al database della DVWA è stato effettuato utilizzando una SQL injection. Ho usato una query SQL per estrarre gli hash delle password dalla tabella degli utenti. La query SQL eseguita è stata: 'UNION SELECT user, password FROM users#

Identificazione delle Password Hashate

Le password recuperate dal database erano tutte in formato MD5. MD5 è un algoritmo di hash comunemente usato per proteggere le password, ma noto per essere vulnerabile a tecniche di cracking come il Dictionary Attack e Brute Force Attack.

Esecuzione del Cracking delle Password

Per eseguire il cracking delle password hashate, ho utilizzato lo strumento John the Ripper su Kali Linux. John the Ripper è un potente strumento di cracking che supporta vari algoritmi di hash, tra cui MD5.

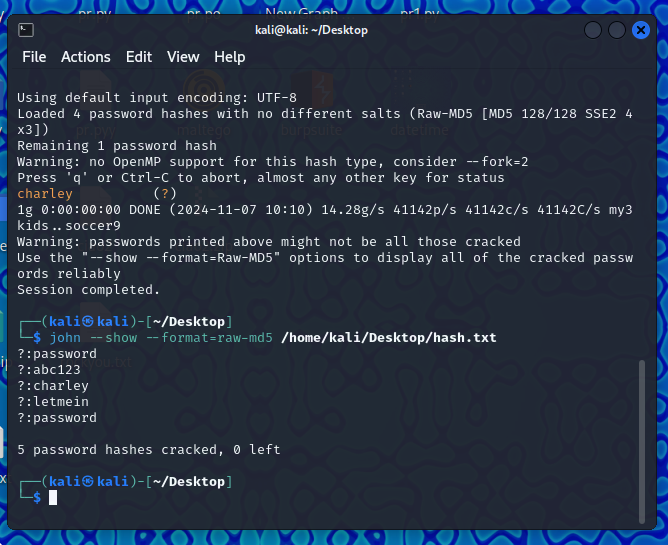
Il comando utilizzato è stato il seguente:

john --format=raw-md5 --wordlist=/home/kali/Desktop/rockyou.txt /home/kali/Desktop/hash.txt

Successivamente, ho eseguito il comando per visualizzare le password trovate:

john --show --format=raw-md5 /home/kali/Desktop/hash.txt

Dopo aver eseguito il cracking, John the Ripper ha recuperato con successo una delle password in chiaro, il risultato è stato il seguente:



L'esercizio ha dimostrato con successo come recuperare e craccare le password hashate in formato MD5 da un database vulnerabile. Utilizzando strumenti come John the Ripper e un dizionario di parole come rockyou.txt, è stato possibile recuperare le password in chiaro. Tuttavia, è importante notare che l'uso di un algoritmo di hash come MD5 per memorizzare password è altamente insicuro.