**Relazione su Password Cracking con John the Ripper**

**Obiettivo:**

L’obiettivo di questa attività è quello di recuperare le password hashate presenti nel database della **DVWA (Damn Vulnerable Web Application)** e, successivamente, eseguire delle sessioni di cracking per ottenere la versione in chiaro delle password, utilizzando gli strumenti e le tecniche apprese durante la lezione teorica.

**Passaggi:**

1. **Impostazione della Sicurezza:**

Il primo passo è accedere alla DVWA e impostare la sicurezza al livello **basso**. Questo permette di avere un database vulnerabile che consente di testare tecniche di attacco come l’iniezione SQL.

2. **SQL Injection:**

Una volta che la sicurezza è impostata su basso, effettuiamo un attacco di **SQL Injection** per estrarre le informazioni di login. La query utilizzata è la seguente:

' UNION SELECT user, password FROM users #

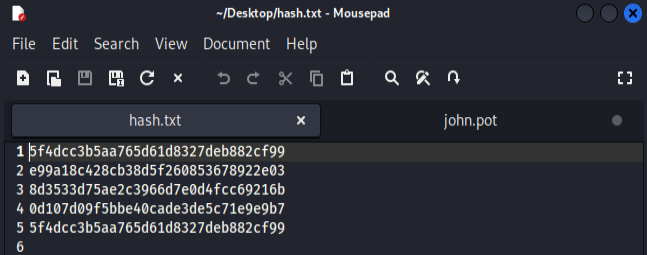
Questa query permette di selezionare gli utenti e le rispettive password dal database. Il carattere # è utilizzato per commentare il resto della query e impedire che vengano visualizzati altri risultati indesiderati.

3. **Visualizzazione degli Hash delle Password:**

Dopo l’iniezione SQL, visualizziamo le password, ma non in chiaro. Invece, vediamo i loro **hash**. Gli hash sono codifiche delle password che permettono di verificare la loro integrità senza esporre direttamente la password in chiaro.

4. **Salvataggio degli Hash:**

Una volta ottenuti gli hash delle password, li copiamo e li salviamo su un file di testo chiamato **hash.txt**, situato sul nostro desktop. Questo file conterrà tutti gli hash delle password da decifrare.



5. **Cracking con John the Ripper:**

Successivamente, apriamo il terminale e utilizziamo il tool **John the Ripper** per eseguire il cracking delle password. Il comando utilizzato è:

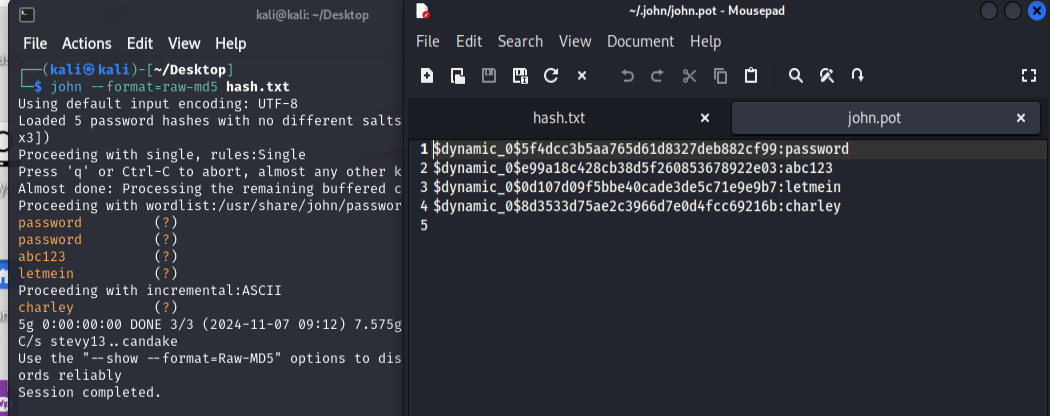
john --format=raw-md5 hash.txt

• --format=raw-md5: Questo specifica che gli hash da decifrare sono nel formato **raw MD5** (ossia in formato binario grezzo). MD5 è un algoritmo di hash crittografico utilizzato comunemente per “proteggere” le password.

• **hash.txt** è il file che contiene gli hash da decifrare.

6. **Decodifica delle Password:**

Dopo aver eseguito il comando, **John the Ripper** inizia a decifrare gli hash. Una volta completato il processo, vediamo le password recuperate, che sono salvate nel file nascosto **.john**. Accanto a ciascun codice hash, viene mostrata la password corrispondente in chiaro.



**Conclusione:**

In questa attività, abbiamo utilizzato **John the Ripper** per eseguire un attacco di cracking delle password, partendo da hash estratti tramite un attacco di **SQL Injection** in un’applicazione vulnerabile. Grazie alla tecnica del cracking delle password con il comando --format=raw-md5, siamo riusciti a recuperare le password originali.