ATTACCO PASS THE HASH

Traccia: Recuperare le password hashate nel database della DVWA e eseguire sessioni di cracking per recuperare la loro versione in chiaro utilizzando i tool studiati nella lezione teorica.
Istruzioni per l'Esercizio:

1. Recupero delle Password dal Database:
    - ○ Accedete al database della DVWA per estrarre le password hashate.
    - ○ Assicuratevi di avere accesso alle tabelle del database che contengono le password.
2. Identificazione delle Password Hashate:
    - ○ Verificate che le password recuperate siano hash di tipo MD5.
3. Esecuzione del Cracking delle Password:
    - ○ Utilizzate uno o più tool per craccare le password:
    - ○ Configurate i tool scelti e avviate le sessioni di cracking.
4. Obiettivo: Crackare tutte le password recuperate dal database.

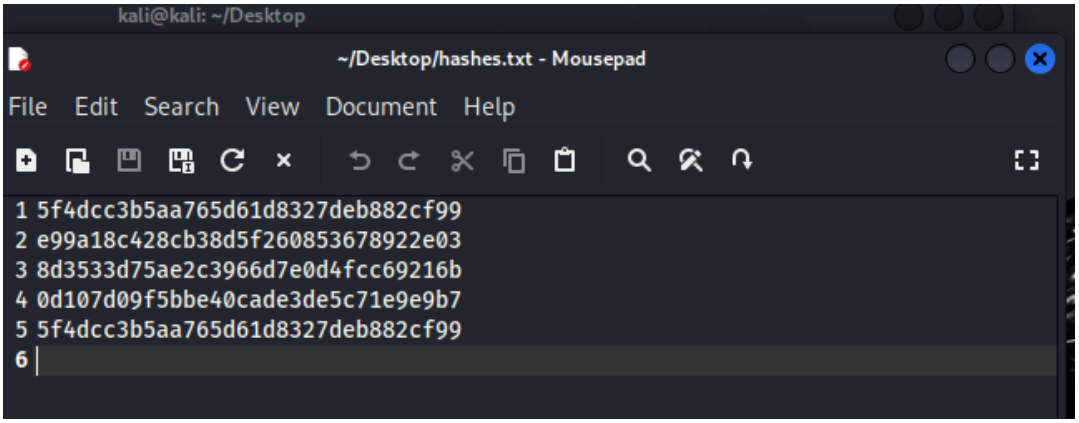
Svolgimento:
L'esercizio di oggi ci chiede di andare a recuperare le password criptate recuperate dall'esercizio già svolto di SQL injection.
Recupero del database
Per recuperare il database, ho eseguito nuovamente il comando SQL injection che ho utilizzato per ricavarlo la prima volta:

1' UNION SELECT user, password FROM users#

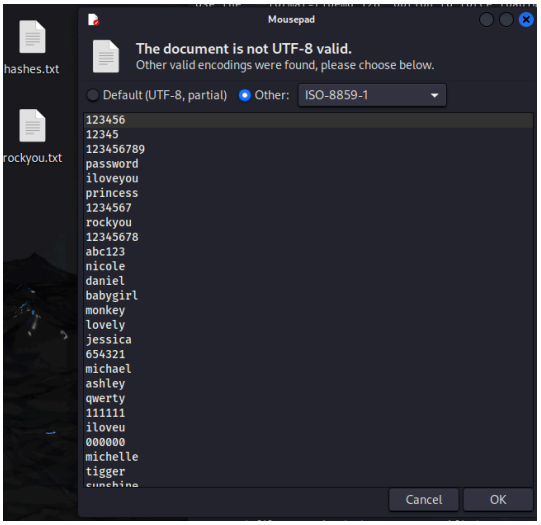
Il risultato sarà il seguente:

Da questo database riusciamo a recuperare le password criptate, per prima cosa bisogna capire in quale chiave di criptazione sono scritte.
Analizzandole con attenzione possiamo contare un totale di 32 caratteri, caratteristica della chiave di criptazione MD5.
Si tratta di una informazione importante che ci servirà in seguito per lanciare il comando sul programma John The Ripper.

File Hashes
Il passo successivo sarà quello di creare un file con tutte le password scritte in codice hash MD5, per creare la lista delle password da far decifrare al programma.



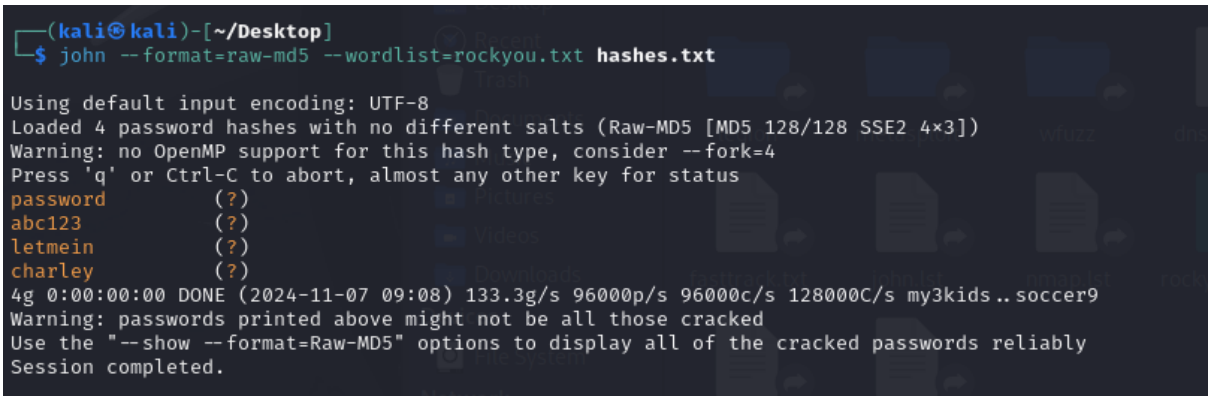
Wordlist
Per facilitare il programma, utilizzeremo il metodo a Dizionario, per fare ciò servirà attingere ad un Dizionario già esistente che servirà a confrontare le password criptate con quelle presenti sulla lista.
Facendo una rapida ricerca il dizionario presente in Kali Linux più appropriato risulta il calendario che si chiama rockyou.
Una volta capita la sua posizione nelle directory, sono andata ad estrarre il file, in maniera che sia accessibile al programma quando andrò a lanciare il comando sul programma di John The Ripper.



John The Ripper
Trattandosi di un file interno al dispositivo, il programma adatto a recuperare le password è John The Ripper.
Per andare a recuperare le password in lista andremo ad eseguire il seguente comando:

john --format=raw-md5 --wordlist=rockyou.txt hashes.txt

in cui con il comando format andremo a comunicare il formato di criptazione, con il comando wordlist andremo ad indicare il dizionario da cui andrà ad attingere per confrontare le password, ed infine è stato indicato il nome del file da cui il programma andrà a leggere le password criptate.
L'output che avremo una volta eseguito il programma sarà il seguente:



Le righe in arancione andranno ad indicare le password decifrate dal programma nell'ordine in cui sono state messe all'interno del file creato precedentemente, l'ultima password non la comunica in quanto esattamente uguale alla prima.

Conclusione
Il programma John The Ripper serve per l'individuazione di password, lo fa in diverse modalità:

- Forza bruta: andrà a provare tutte le combinazioni esistenti finchè non riesce a trovare quella corrispondente, metodo che richiede molto tempo a seconda di quanto è elaborata la password;
- Dizionario: proverà le password attingendo ad un dizionario contenente diverse combinazioni tra le più utilizzate, questo sistema velocizza di molto la procedura, ma ha il difetto che se le password non sono presenti nella lista non sarà in grado di trovarle.

Nell'esercizio di oggi abbiamo utilizzato il metodo a Dizionario che, confrontato con la wordlist rockyou, ha dato i risultati sperati.
L'esercizio aveva lo scopo di mostrare uno degli sistemi più utilizzati nell'ambito degli attacchi alle password.