Password cracking

Introduzione

L'esercizio si è concentrato sulla pratica del **password cracking**, una tecnica utilizzata per recuperare le password originali da versioni hashate. Lo scopo principale era quello di acquisire familiarità con gli strumenti e le metodologie impiegate dagli hacker per violare la sicurezza dei sistemi informatici.

Obiettivi

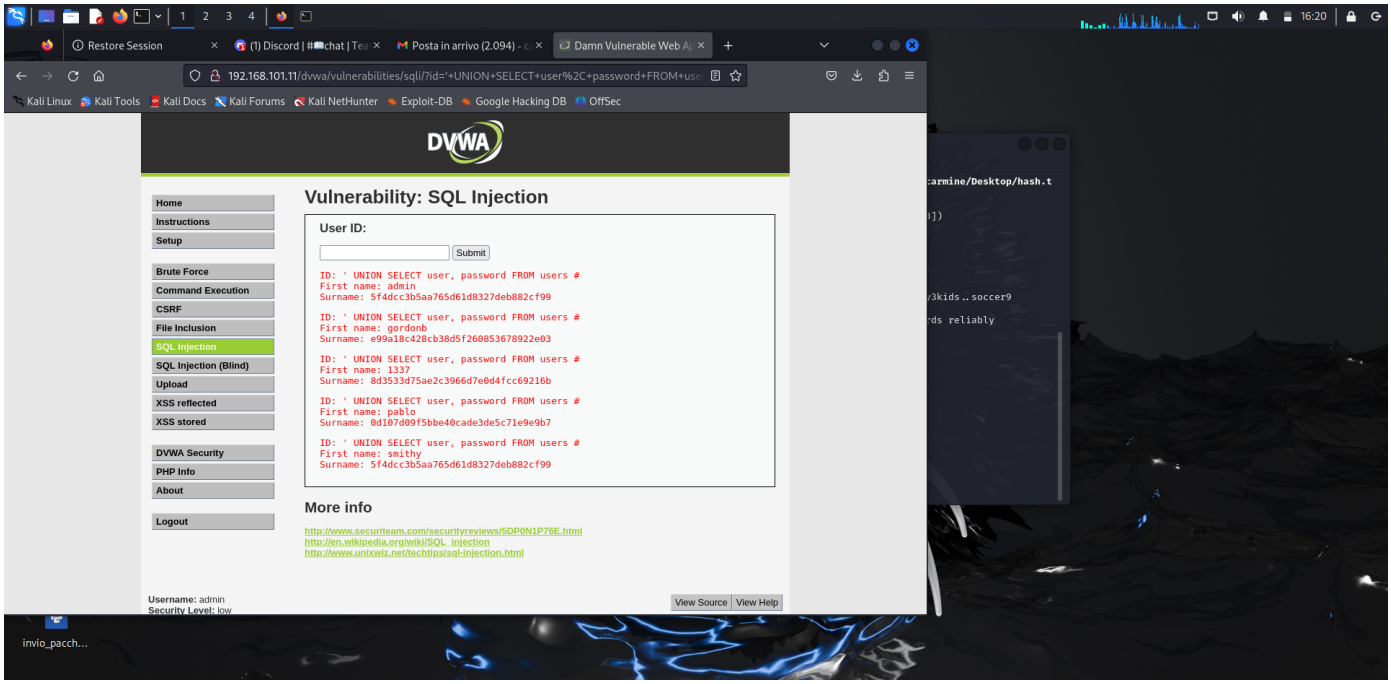
- **Recupero delle password hashate:** Estrarre le password criptate dal database della DVWA.
- **Identificazione del tipo di hash:** Determinare l'algoritmo di hashing utilizzato (nel nostro caso, MD5).
- **Cracking delle password:** Utilizzare strumenti specifici per tentare di recuperare le password originali a partire dagli hash.

Procedimento

1. Accesso al Database DVWA e Recupero delle Password:

- **Connessione:** È stato stabilito un collegamento al database della DVWA.
- **Query SQL:** È stata eseguita una query SQL per selezionare le colonne contenenti le password hashate usando il comando **‘' UNION SELECT user, password FROM users #**.
- **Estrazione:** I risultati della query sono stati esportati in un file di testo per le successive analisi.

Immagine con i codici hash recuperati su Dvwa.



Identificazione del Tipo di Hash:

- **Analisi visiva:** Le password estratte sono state inizialmente esaminate visivamente per individuare eventuali pattern caratteristici dell'algoritmo MD5.
- **Utilizzo di strumenti online:** Sono stati utilizzati strumenti online specializzati per l'analisi degli hash, confermando che l'algoritmo utilizzato era effettivamente MD5.

Esecuzione del Cracking delle Password:

- **Scelta degli strumenti:** Sono stati selezionati i seguenti strumenti per il cracking: John the Ripper
- **Configurazione:** Gli strumenti sono stati configurati specificando:
  - **Tipo di hash:** MD5
  - **File di input:** Il file contenente le password hashate estratte dal database
  - **Dizionario:** È stato utilizzato un dizionario contenente un ampio insieme di parole e combinazioni alfanumeriche: **rockyou.txt**
  - **Regole di cracking:** Sono state applicate diverse regole per generare nuove combinazioni di password a partire dal dizionario
- **Esecuzione:** Le sessioni di cracking sono state avviate, lasciando gli strumenti in esecuzione.

Risultati

- **Password recuperate:** abbiamo recuperato 5 password
- **Tempo di esecuzione:** Pochi secondi.

Immagine con le password recuperate.

Conclusioni

L'esercizio ha permesso di comprendere le vulnerabilità legate alla memorizzazione delle password in formato hash. Anche utilizzando algoritmi come MD5, che sono considerati obsoleti, è possibile recuperare le password originali, soprattutto se si dispone di un dizionario sufficientemente ampio e si applicano tecniche di cracking avanzate.