Esercitazione W14D1 - Pratica 1

Password cracking

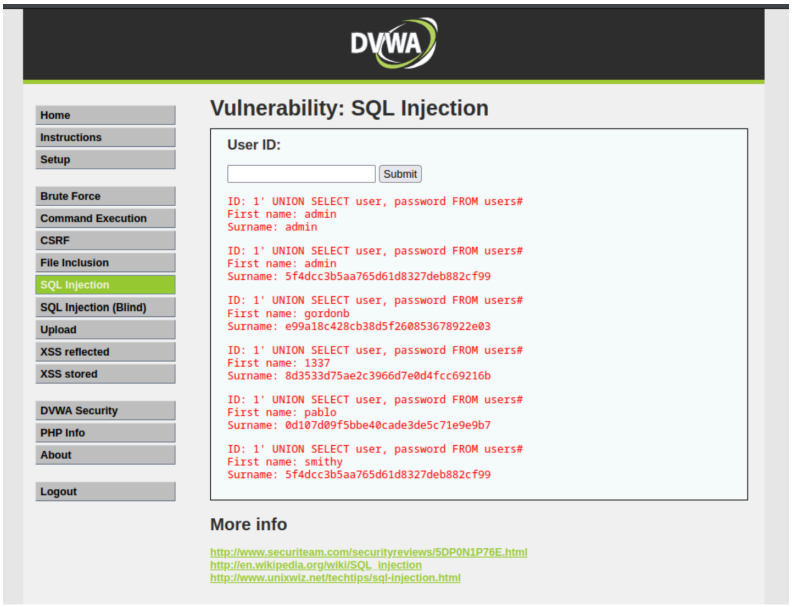
Fabio Benevento - 07/02/2024

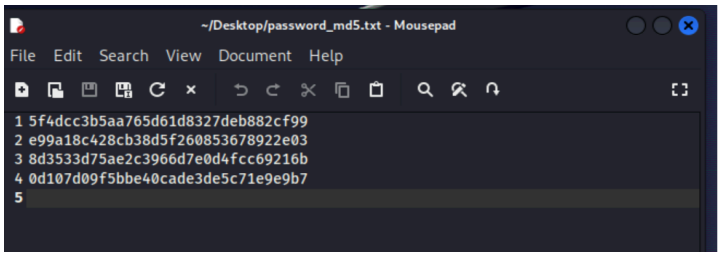
Traccia

Obiettivo della lezione è craccare tutte le password degli utenti del database SQL trovate nella precedente lezione mediante i tool visti nella lezione teorica.

Implementazione

Tra i software utili per effettuare il craking delle password, è disponile in Kali Linux l'applicazione John the Ripper. Essa permette di effettuare 2 tipi di attacco: l'attacco a forza bruta e l'attacco a dizionario. Nel primo caso, John the ripper prova tutte le possibili combinazioni di caratteri e ciò richiede un tempo molto lungo. Nel secondo caso invece, Jonh the Ripper effettua il confronto con una lista di password fornite come input all'applicazione.
Per l'esercitazione è stata utilizzata questa seconda modalità. Nello specifico ho preso le differenti hash individuate nell'esercitazione precedente e le ho riportate in un file (`password_md5.txt`)

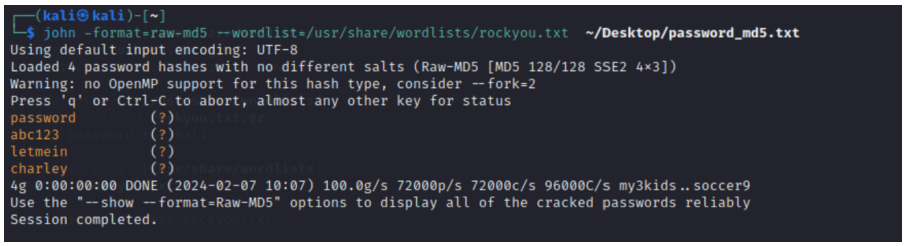




Ho quindi dato in pasto il file con le hash da decifrare a John the Ripper con il comando

```
johh –format-raw=md5 –wordlist=/usr/shar/wordlist/rockyou.txt
```

in cui ho specificato il formato delle passowrd che in questo caso era conosciuto (md5).
Cone dizionario ho utilizzato una delle wordlist fornite da Kali Linux, nello specifico la wordlist rockyou.txt che risulta essere una delle più complete.
Di seguito è mostrato il risultato dell'esecuzione di John the Ripper con in arancione le password decifrate dal tool



In effetti, utilizzando le credenziali username: gordonb e password: abc123, trovata da John The Ripper è possibile loggarsi sulla piattaforma DVWA come mostrato in figura.