Report Attività: Cracking di Password Hashate in DVWA con John the Ripper

In questo esercizio ho simulato un attacco su un'applicazione vulnerabile (DVWA - Damn Vulnerable Web Application) con l'obiettivo di recuperare password hashate dal database e craccarle per ottenere le versioni in chiaro.

Per prima cosa, tramite un attacco SQL Injection eseguito dal pannello DVWA, sono riuscito a eseguire la query:
' UNION SELECT user, password FROM users --

che mi ha permesso di ottenere i nomi utente e le relative password hashate salvate nel database.

Ho poi copiato gli hash MD5 ottenuti e li ho incollati in un file chiamato hash.txt creato con nano. Gli hash erano i seguenti:

5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99

Notando che il primo e l'ultimo hash erano identici, mi aspettavo che corrispondessero alla stessa password in chiaro.

Per il cracking ho utilizzato John the Ripper, uno strumento potente per attacchi a dizionario. Il comando usato è stato:

john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/hash.txt

Il file rockyou.txt contiene un'ampia lista di password comuni ed è molto efficace per questo tipo di test.

Dopo il completamento del processo di cracking, ho eseguito il comando:

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

che ha mostrato le password corrispondenti agli hash, permettendomi di confermare l'efficacia dell'attacco.

In conclusione, questo esercizio mi ha permesso di comprendere il processo completo di estrazione, identificazione e cracking delle password hashate in un ambiente controllato e sicuro, utilizzando tecniche e strumenti fondamentali nel campo dell'ethical hacking e del penetration testing.

---

Scusi prof, il report l'ho generato con l'aiuto di GPT per questione di tempo.