Password Cracking - Recupero delle Password in Chiaro

Obbiettivo :

Craccare tutte le password recuperate dal database.

Panoramica :

Il presente documento illustra le attività di analisi tecnica condotte sul database compromesso, con particolare focus sulla tabella *users*. L'obiettivo dell'attività è stato verificare la robustezza degli algoritmi di hashing utilizzati per lo stoccaggio delle password e dimostrare la fattibilità del recupero delle credenziali in chiaro tramite tecniche di crittoanalisi (password cracking).

Metodologia di Acquisizione:

Durante la fase precedente, è stata identificata e sfruttata una vulnerabilità di tipo **SQL Injection (SQLi)**. Questo vettore di attacco ha permesso l'accesso non autorizzato al database, consentendo l'esfiltrazione della tabella contenente le credenziali utente.

```
ID: ' UNION SELECT user, password FROM users -- -
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user, password FROM users -- -
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user, password FROM users -- -
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user, password FROM users -- -
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT user, password FROM users -- -
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

3. Analisi e Identificazione degli Hash

Prima di procedere all'attacco, è stata effettuata un'analisi preliminare per identificare l'algoritmo crittografico utilizzato.

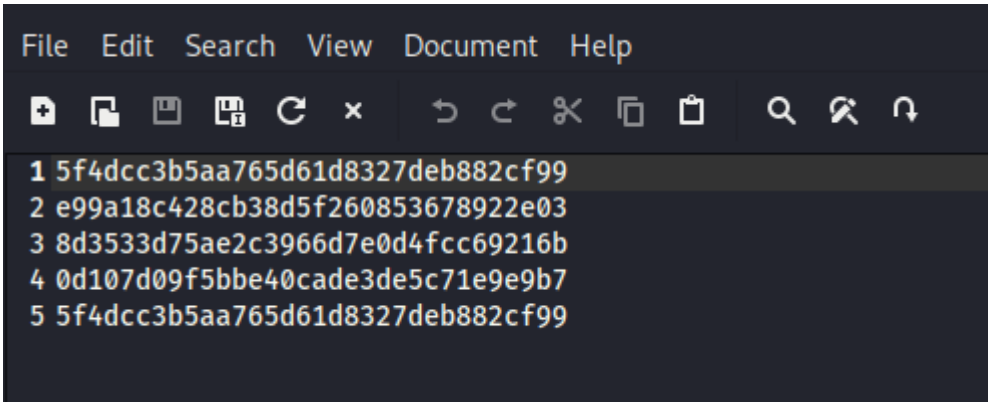
- **Lunghezza della stringa**
  - Le stringhe estratte presentano una lunghezza fissa di 32 caratteri. Poiché ogni carattere esadecimale rappresenta 4 bit, una stringa di 32 caratteri corrisponde a un digest di 128 bit. Questa caratteristica è la firma tipica dell'algoritmo MD5.
- **Analisi Strumentale**
  - Per confermare l'ipotesi, è stato utilizzato il tool *`hash-identifier`* su Kali Linux. Il software ha analizzato la struttura dell'hash e ha confermato con alta probabilità che l'algoritmo in uso è MD5.

4. Procedura di Cracking (Password Recovery)

Per il recupero delle password in chiaro è stato utilizzato il framework **John The Ripper**.

Configurazione dell'attacco:

Preparazione: Gli hash esfiltrati sono stati isolati in un file dedicato denominato *hash.txt.*



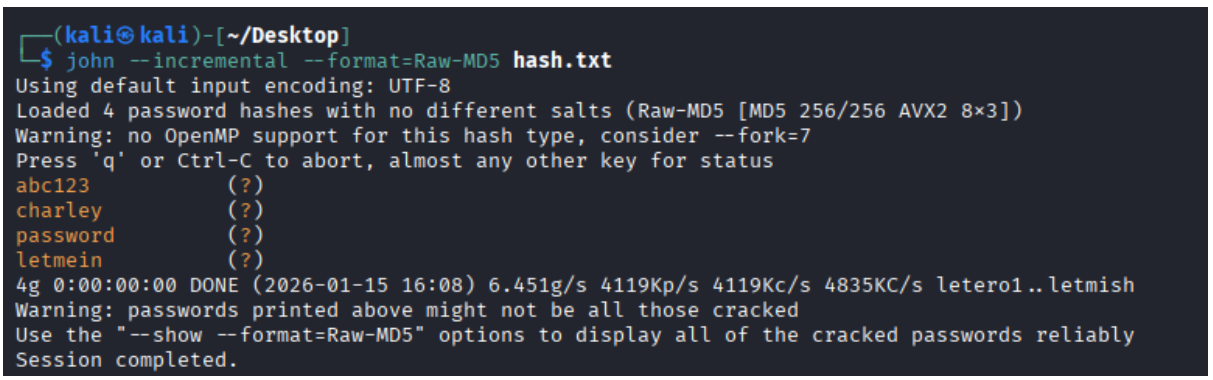
Modalità di Attacco: È stata selezionata la modalità **Incremental** (Brute-force intelligente) specificando il formato *Raw-MD5* per ottimizzare le prestazioni.

Per il cracking della password uso definitivamente questo comando :

> *" john --incremental --format=Raw-MD5 hash.txt "*

5. Risultati Ottenuti

L'attacco ha avuto successo immediato. Il processo ha evidenziato la debolezza intrinseca dell'algoritmo MD5, portando alla visualizzazione delle password in chiaro.



John The Ripper ha automaticamente salvato i risultati nel file di cache *(john.pot),* garantendo che in future analisi gli stessi hash vengano risolti istantaneamente senza richiedere nuova potenza di calcolo.

6. Conclusioni e Raccomandazioni

L'attività di cracking ha dimostrato in modo inequivocabile che l'attuale sistema di protezione delle password, basato sull'algoritmo MD5, non è più in grado di garantire la sicurezza dei dati aziendali. La facilità con cui è stato possibile recuperare le credenziali in chiaro evidenzia come questo standard, ormai obsoleto, non offra alcuna resistenza contro la potenza di calcolo dei computer moderni, rendendo l'intera infrastruttura vulnerabile anche ad attacchi condotti con risorse limitate.