Ghassan Haouem

Ghassan Haouem

Uso di John the Ripper per il Cracking di Password MD5

1. Introduzione

Il *cracking* delle password è una tecnica utilizzata per decifrare le password codificate (o "hashate") e riportarle alla loro forma leggibile, detta "in chiaro". **John the Ripper** è uno dei software più famosi e versatili per questo scopo. Viene utilizzato per tentare di indovinare le password corrispondenti agli hash, ovvero alle versioni codificate delle password, che possono essere protette tramite algoritmi di hashing come MD5, SHA, MD4 ecc.

2. Scopo

L'obiettivo di questa procedura era utilizzare John the Ripper per identificare le password in chiaro contenute in un file (`CrackMe`) che contiene hash di password MD5. Questo tipo di procedura viene comunemente impiegato durante test di sicurezza per verificare la robustezza delle password aziendali o durante la verifica di vulnerabilità informatiche.

3. Procedura Svolta

Una volta estrapolate con una **SQL injection** copiamo tutte le password hash in un file di testo una in capo all'altra.

3.1 Preparazione

1. **Navigazione alla Cartella di Lavoro**: Abbiamo aperto il terminale e ci siamo spostati nella cartella `Desktop`, dove si trova il file `CrackMe` contenente gli hash delle password.
2. **Controllo del File**: Verificato che il file `CrackMe` fosse presente. Inizialmente abbiamo avuto un errore di mancato file, ma successivamente è stato corretto.

3.2 Comando Principale di Cracking

Per avviare il processo di cracking delle password, abbiamo usato il comando:

```
john --format=RAW-MD5 CrackMe
```

Questo comando dice a John the Ripper di:

- Usare il **formato MD5** per decodificare gli hash. L'algoritmo di hashing MD5 è uno dei metodi di codifica più comuni, anche se oggi non è più considerato sicuro per la protezione delle password.
- Prendere gli hash dal file `CrackMe` e provare a trovare le password originali che producono quegli hash.

3.3 Spiegazione del Comando:

- `john`: Avvia il programma John the Ripper.
- `--format=RAW-MD5`: Specifica che gli hash presenti nel file sono codificati con MD5 senza l'uso di "salt" (ovvero senza chiavi di sicurezza aggiuntive).
- `CrackMe`: Indica il file che contiene gli hash.

3. **Avvio della Decodifica delle Password**:
    - **Caricamento degli Hash**: John the Ripper ha caricato gli hash presenti in `CrackMe`.
    - **Tentativi di Cracking**: John ha cominciato a fare tentativi per scoprire le password in chiaro. Ha utilizzato inizialmente un *wordlist* (lista di parole comuni) e, successivamente, è passato a tentare combinazioni incrementali di caratteri.
    - **Risultato**: Dopo alcuni secondi , John the Ripper ha trovato le password corrispondenti a ciascun hash presente nel file.

4. Verifica dei Risultati

Dopo aver completato il cracking, abbiamo eseguito un comando di verifica per vedere il riepilogo delle password trovate

```
john --show --format=raw-md5 CrackMe
```

Questo comando ha prodotto l'elenco delle password in chiaro decifrate da John. Di seguito il risultato mostrato:

- `password`
- `abc123`
- `letmein`
- `charley`
- `password`

Queste sono le password originali che John ha decifrato dagli hash presenti nel file `CrackMe`. Il software ha inoltre indicato che **5 hash sono stati craccati e 0 rimasti**.

5. Conclusione

John the Ripper si è dimostrato efficace nel trovare le password corrispondenti agli hash MD5 contenuti in `CrackMe`. Questo strumento funziona utilizzando vari metodi di cracking:

- **Wordlist**: Prova una serie di parole comuni, password conosciute e combinazioni semplici.
- **Incrementale**: Se il dizionario non basta, John prova tutte le possibili combinazioni di caratteri, partendo da sequenze semplici.

L'utilizzo di un software di cracking per testare la sicurezza delle password è molto utile per capire quanto sia sicuro l'algoritmo di hashing e per verificare se le password sono vulnerabili. In questo caso, molte delle password erano semplici (come "password" e "abc123") e sono state facilmente decifrate, evidenziando l'importanza di utilizzare password complesse e uniche.

Procedura :