**Report sull'Esercizio di Password Cracking**

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

**Obiettivo dell'Esercizio**

L'obiettivo dell'esercizio era craccare tutte le seguenti password hash utilizzando qualsiasi tool o soluzione alternativa:

- 5f4dcc3b5aa765d61d8327deb882cf99

- e99a18c428cb38d5f260853678922e03

- 8d3533d75ae2c3966d7e0d4fcc69216b

- 0d107d09f5bbe40cade3de5c71e9e9b7

- 5f4dcc3b5aa765d61d8327deb882cf99

**Strumento Utilizzato**

Ho utilizzato **John the Ripper**, un popolare software di cracking delle password.

**Passaggi Svolti**

1. Preparazione del File degli Hash:

Ho salvato gli hash in un file di testo chiamato “**hashes.txt**”.

2. Esecuzione di John the Ripper:

Ho eseguito John the Ripper utilizzando il comando:

“

**john --format=Raw-MD5 --incremental hashes.txt**

“

Questo comando specifica:

- “--format=Raw-MD5”: Indica a John il formato degli hash da craccare.

- “--incremental”: Utilizza un attacco brute force incrementale, provando tutte le combinazioni di caratteri possibili.

3. Visualizzazione delle Password Craccate:

Dopo che John the Ripper ha terminato l'attacco, ho utilizzato il comando seguente per mostrare tutte le password craccate:

“

**john --show --format=Raw-MD5 hashes.txt**

“

Questo comando visualizza gli hash e le corrispondenti password in chiaro trovate da John the Ripper.

**Risultati Ottenuti**

John the Ripper ha craccato con successo tutte le password associate agli hash forniti. Ecco il risultato:

- 5f4dcc3b5aa765d61d8327deb882cf99: password

- e99a18c428cb38d5f260853678922e03: abc123

- 8d3533d75ae2c3966d7e0d4fcc69216b: charley

- 0d107d09f5bbe40cade3de5c71e9e9b7: letmein

- 5f4dcc3b5aa765d61d8327deb882cf99: password (ripetuto, quindi già craccato)

**Conclusione**

L'uso di John the Ripper con un attacco incrementale si è rivelato efficace per craccare tutti gli hash MD5 forniti nell'esercizio. Questo dimostra l'efficacia degli attacchi a forza bruta su hash deboli come MD5, sottolineando l'importanza di utilizzare algoritmi di hashing più sicuri per proteggere le password.