EPICODE

S6 - L3

Svolto da:
Donato Tralli

Traccia

Password Cracking

Esercizio:
Sentitevi liberi di utilizzare qualsiasi tool o soluzione alternativa. L’obiettivo dell’esercizio di oggi è craccare tutte le password. Le password da craccare sono le seguenti:

- 5f4dcc3b5aa765d61d8327deb882cf99
- e99a18c428cb38d5f260853678922e03
- 8d3533d75ae2c3966d7e0d4fcc69216b
- 0d107d09f5bbe40cade3de5c71e9e9b7
- 5f4dcc3b5aa765d61d8327deb882cf99

Password Cracking

Questo esercizio verrà svolto mediante il programma John The Ripper che ci permetterà di craccare le password dal codice hash alla password in chiaro.
John the Ripper è un software per il cracking delle password, progettato per individuare e recuperare password deboli o sconosciute tramite attacchi di forza bruta o utilizzando dizionari.
È uno strumento ampiamente utilizzato nel campo della sicurezza informatica e del penetration testing.

Password 1

Password in hash: 5f4dcc3b5aa765d61d8327deb882cf99

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=raw-MD5 --incremental pass1

Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (?)
1g 0:00:00:00 DONE (2024-05-15 08:27) 1.851g/s 758755p/s 758755c/s 758755C/s
 password..patronet
Use the "--show --format=Raw-MD5" options to display all of the cracked pass
words reliably
Session completed.
```

Password 2

Password in hash: e99a18c428cb38d5f260853678922e03

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=raw-MD5 --incremental pass2
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123           (?)
1g 0:00:00:00 DONE (2024-05-15 08:28) 5.882g/s 76800p/s 76800c/s 76800C/s amina1.
.abby99
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords
 reliably
Session completed.
```

Password 3

Password in hash: 8d3533d75ae2c3966d7e0d4fcc69216b

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=raw-MD5 --incremental pass3
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
charley          (?)
1g 0:00:00:00 DONE (2024-05-15 08:28) 4.347g/s 93495p/s 93495c/s 93495C/s stevy13
..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords
 reliably
Session completed.
```

Password 4

Password in hash: 0d107d09f5bbe40cade3de5c71e9e9b7

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=raw-MD5 --incremental pass4
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
letmein          (?)
1g 0:00:00:00 DONE (2024-05-15 08:28) 1.123g/s 2869Kp/s 2869Kc/s 2869KC/s letero1
..letmish
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords
 reliably
Session completed.
```

Password 5

Password in hash: 5f4dcc3b5aa765d61d8327deb882cf99

Essendo che questo codice hash è uguale alla prima, sarà sempre “password”

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=raw-MD5 --incremental pass1

Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (?)
1g 0:00:00:00 DONE (2024-05-15 08:27) 1.851g/s 758755p/s 758755c/s 758755C/s
 password..patronet
Use the "--show --format=Raw-MD5" options to display all of the cracked pass
words reliably
Session completed.
```

Conclusione

Dopo aver eseguito il cracking delle password, John the Ripper è riuscito a recuperare diverse password dal codice hash, rendendole leggibili in chiaro. Queste password possono ora essere utilizzate per accedere ai sistemi o per valutare la sicurezza delle password utilizzate nell'ambiente target.

EXTRA: HASHCAT

Come secondo tool possiamo usare hashcat. Hashcat è un potente strumento di cracking delle password utilizzato per recuperare password perdute o dimenticate attraverso l'analisi degli hash.