Rainbow Tablosu Oluşturma ve Oluşturulan Tablo ile Parola Kırma

Rainbow tablosu oluşturmak için RainbowCrack tool'unun alt bileşeni olan rtgen'i, oluşturulan tablo ile bir hash'i kırmak için önce rtsort, sonra rcrack alt bileşenleri kullanılır. Tüm bunlar Kali'de yüklü olarak gelmektedir. Şimdi bir rainbow tablosu oluşturalım ve bu tabloyla aşağıdaki parolayı kıralım.

Kırılacak MD5 ile Şifrelenmiş Parola

fc3f318fba8b3c1502bece62a27712df // “hasan” string'inin MD5 hali

Aşama 1 (Generating) :

> rtgen md5 loweralpha 1 5 0 10000 9682 0 // Rainbow tablosu oluşturulur

Output:

rainbow table md5_loweralpha#1-5_0_10000x9682_0.rt parameters
hash algorithm: md5
hash length: 16
charset: abcdefghijklmnopqrstuvwxyz
charset length: 26
plaintext length range: 1 – 5

sequential starting point begin from 0 (0x00000000000000)
generating...
9682 of 9682 rainbow chains generated (0 minute 21.4 seconds)

Aşama 2 (Sorting) :

> rtsort md5_rainbowTable.rt // Rainbow tablosu sıralanır.

Aşama 3 (Cracking) :

> rcrack md5_loweralpha#1-5_0_10000x9682_0.rt -h fc3f318fba8b3c1502bece62a27712df

Output:

…
…
result
---
fc3f318fba8b3c1502bece62a27712df **hasan** hex:686173616e

Görüldüğü üzere rtgen ile oluşturduğumuz rainbow tablosunu rcrack'te kullanarak md5 ile şifrelenmiş parolayı kırdık ve parolanın hasan olduğunu gördük.

[DETAYLI ANLATIM]

RainbowCrack Tool'u

a. rtgen

Kali'de yüklü RainbowCrack'in bir alt bileşeni olan rtgen ile belirlenen kriterlere uygun rainbow tablosu oluşturulur. rtgen komutu ismini **r**ainbow **t**able **gen**erating'den almaktadır.

Usage:

> rtgen hashType [loweralpha | loweralpha-numeric | numeric | mixalpha-numeric| alpha-numeric] minLength maxLength tableIndex chainLen chainNum partIndex

NOT: Zincir ile kastedilen şey bir parolanın hash'i alındıktan sonra başından ve sonundan birkaç karakter alıp, gerisini atıp kalanların bir daha hash'ini almaya denir. Böylelikle bir hash zinciri oluşur.

Example:

> rtgen md5 loweralpha 1 5 0 10000 9682 0

Yukarıdaki kodda belirtilen parametrelere göre alfabedeki tüm küçük harflerle minimum 1 karakterli, maksimum 5 karakterli tüm kombinasyonların md5 hallerinin yer alacağı bir rainbow table oluşturulur.

NOT: Kullanılacak hash algoritması olarak md5 yerine lm de kullanılabilir (lm = LM)

b. rtsort

rtgen ile tablo oluşturma sonlandığında çıktıda tablonun ismi görünecektir. Mesela md5_loweralpha#1-5_0_10000x9682_0.rt şeklinde. Oluşturulan bu tablo rcrack ile kullanılmadan önce rtsort ile sıralanmaya tabi tutulmalıdır.

Usage:

> rtsort rtFiles [rtFiles …] // rtgen'in oluşturduğu rainbow tablo dosyaları

Example:

> rtsort md5_loweralpha#1-5_0_10000x9682_0.rt

c. rcrack

rcrack komutu kırılması gereken parolanın oluşturulan rainbow tablosu ile kırılmasını sağlar.

Usage:

> rcrack rainbowTable.rt -h hashValue

Example:

> rcrack md5_loweralpha#1-5_0_10000x9682_0.rt -h fc3f318fba8b3c1502bece62a27712df

Output:

…

…
result
---
fc3f318fba8b3c1502bece62a27712df **hasan** hex:686173616e

NOT: Eğer birden fazla hash bir defada kırılmak isteniyorsa bu durumda hepsi alt alta olacak şekilde bir dosyaya yerleştirilir (e.g. hash.txt) Ardından -l parametresi ile dosya rcrack komutuna dahil edilir.

Uyarı: Çoklu hash kırma yöntemi normalde var olan bi'şey, fakat pratikte çalışmadı. Dosya açılamadı hatası verdi.

hash.txt :

fc3f318fba8b3c1502bece62a27712df // hasan

87e9f0f7ed20bdf96ba715980e2aaa2b // nasah

b4b643cb1547b52057fdd15336581ca8 // fatih

Terminal:

> rcrack md5_loweralpha#1-5_0_10000x9682_0.rt -l hash.txt

Output:

hash

can't open hash

https://en.wikipedia.org/wiki/Hash_chain