JTR ile Şifre Kırma

Kurulumu

> apt-get install john

Kullanımı

1.

Bir hash'i kırmak için aşağıdaki yapı kullanılır.

> john hashDosyasi // Önce jtr'nin sözlüğü denenir, sonra brute force denenir.

2.

JTR'nin “sadece” kendi içinde barındırdığı sözlük ile hash'i kırması için --single parametresi kullanılır.

> john --single hashDosyasi

3.

Var olan kırma işlemi yanlışlıkla abort edilirse işlemin kaldığı yerden devam edebilmesi için --restore parametresi kullanılır.

> john --restore

4.

Kendi oluşturduğumuz bir sözlük ile hash'in kırılması için --wordlist parametresi kullanılır.

> john --wordlist="benimsozluk.txt" hashDosyasi.txt

5.

Sadece brute force ile hash'in kırılması için --incremental parametresi kullanılır.

> john --incremental:ASCII /etc/shadow
> john --incremental:digits /etc/shadow
> ...

Yukarıda kullanılan ASCII ve digits gibi bir sürü charset vardır. Bunlar ve bunların brute force esnasında uygulanacak karakter limitleri (minLength ve maxLength'leri) /john-1.8.0/run/john.conf dosyasında mevcuttur. O dosyanın ilgili kesiti aşağıda verilmiştir.

/john-1.8.0/run/john.conf

…

[Incremental:ASCII]
File = $JOHN/ascii.chr
MinLen = 0
MaxLen = 13
CharCount = 95

[Incremental:LM_ASCII]
File = $JOHN/lm_ascii.chr
MinLen = 0
MaxLen = 7
CharCount = 69

[Incremental:Alnum]
File = $JOHN/alnum.chr
MinLen = 1
MaxLen = 13
CharCount = 62

[Incremental:Alpha]
File = $JOHN/alpha.chr
MinLen = 1
MaxLen = 13
CharCount = 52

[Incremental:LowerNum]
File = $JOHN/lowernum.chr
MinLen = 1
MaxLen = 13
CharCount = 36

[Incremental:UpperNum]
File = $JOHN/uppernum.chr
MinLen = 1
MaxLen = 13
CharCount = 36

[Incremental:LowerSpace]
File = $JOHN/lowerspace.chr
MinLen = 1
MaxLen = 13
CharCount = 27

[Incremental:Lower]
File = $JOHN/lower.chr
MinLen = 1
MaxLen = 13
CharCount = 26

[Incremental:Upper]
File = $JOHN/upper.chr
MinLen = 1
MaxLen = 13
CharCount = 26

[Incremental:Digits]
File = $JOHN/digits.chr
MinLen = 1
MaxLen = 20
CharCount = 10

...

Dilediğin charset'i --incremental parametesine koyabilir, seçtiğin charset için minLength ve maxLength ayarını conf dosyası üzerinden kendine göre ayarlayabilirsin.

NOT: Alnum charset'i çalışmıyor. JTR Alnum.chr dosyasının bulunamadığına dair hata mesajı veriyor. Charset'ler /john-1.8.0/run dizini içerisinde yer alıyor ve orada Alnum.chr maalesef yok.

(Sayfa 77 - Bilişimin Karanlık Yüzü)

http://www.openwall.com/john/
http://www.openwall.com/john/doc/CONFIG.shtml
https://countuponsecurity.files.wordpress.com/2015/06/jtr-cheat-sheet.pdf

Hatalar

i)

> john /etc/shadow

No password hashes left to crack (see FAQ)

Nedeni:

Kırma işlemi gerçekleşen hash'i bir daha kırmayı denersen “No password hashes left to crack (see FAQ)” uyarısı alırsın. Bu kırılmış hash'in bulunan değerini görmek için --show parametresi kullanılır:

> john --show /etc/shadow

Output:

hefese:**W.karabuk1992**:16677:0:99999:7:::
1 password hash cracked, 0 left

ii)

> john hash.txt

No password hashes *loaded (see FAQ)*

Nedeni:

Eğer JTR'nin desteklemediği bir hash kırılmaya çalışılırsa ya da JTR'nin tanımlayamadığı bir hash kırılmaya çalışılırsa bu durumda “No password hashes loaded (see FAQ)” hatası verir.

/etc/shadow Üzerine Notlar

1.

/etc/shadow dosyasındaki tüm parolaları kırmak için aşağıdaki yapı kullanılır.

> john /etc/shadow

NOT: Eğer “No password hashes left to crack (see FAQ)” hatası veriyorsa yukarıda bahsedilen uyarıyı oku.

2.

/etc/shadow dosyasında yer alan hesaplardan sadece belirli bir kullanıcının parolasını kırmak için --user parametresi kullanmak gerekir.

> john --user=hefese /etc/shadow

NOT: Eğer “No password hashes left to crack (see FAQ)” hatası veriyorsa yukarıda bahsedilen uyarıyı oku.

3.

JTR'nin kendi içinde barındırdığı sözlük ile /etc/shadow'un kırılması isteniyorsa bu durumda --single parametresi kullanılır.

> john --single /etc/shadow

NOT: Eğer "No password hashes left to crack (see FAQ)" diyorsa yukarıda bahsedilen uyarıyı oku.

4.

Kendi oluşturduğumuz bir sözlük ile /etc/shadow'u kırmak istiyorsak --wordlist parametresi kullanılır.

> john --wordlist="sozluk.txt" /etc/shadow

NOT: Eğer "No password hashes left to crack (see FAQ)" diyorsa yukarıda bahsedilen uyarıyı oku.

5.

Sadece brute force ile rakamları kullanarak hash.txt'teki hash'i kırmak istiyorsak --incremental parametresi kullanılmalıdır.

> john --incremental:digits /etc/shadow

Ekstra

1.

/etc/shadow'daki "bir" satır mesela şöyle bir şeydir:

hefese:6c5X47bMt$zRBy74tpLL.G.KA38LoaBEXmup7D.2FYrvSX.n7Jt45AFa3ya
dtL8Y7ufc/40NnFv4uUnSnIxIxImXr0WRyqC1:16677:0:99999:7:::

Bu veri, yani sadece bir satır hash.txt'ye kopyalanabilir ve böylece sadece seçtiğimiz satır için kırma işlemi uygulanabilir.

> john hash.txt

2.

Kendi hash'imizi openssl ile kendimiz oluşturabiliriz. Aşağıda örnek olarak salt değeri salata olan deneme parolasının hash'i oluşturulmaktadır:

> openssl passwd -1 -salt salata deneme

Output:

1salata$D2pdYRA7H6IjskEj4Qtue1

Bu şekilde hash oluşturup bunları JTR'ye kırdırabiliriz.

Örnekler

a.

includekarabuk'un yönetim paneli parolasının hash'ini JTR ile kıralım:

hash.txt

```
$2y$10$Y276DxFLh1.pG/Y.e3evNOteU1v0s5hDpTM0nKRwJXgtr0sDjJciu
```

sozluk.txt

```
hasan
fatih
simsek
hasan
fatih
simsek
hasan
fatih
simsek
hasan
fatih
simsek
hasan
fatih
simsek
hasan
fatih
simsek
hasan
fatih
simsek
tuzlucayir
```

Terminal:

```
john  --wordlist=sozluk.txt  hash.txt
```

Output:

```
?:tuzlucayir

1 password hash cracked, 0 left
```

b.

includekarabuk'un yönetim paneli parolasının hash'ini tekrar JTR'ye verelim:

Terminal
```
john hash.txt
```

Output:
```
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
No password hashes left to crack (see FAQ)
```

Terminal
```
john  --show hash.txt
```

Output:
```
?:tuzlucayir
```

c.

Kendi hazırladığımız wordlist ile /etc/shadow'u kırmaya çalışalım.

linuxWordlist.txt
```
hasan
fatih
simsek
hasan
fatih
simsek
hasan
simsek
hasan
fatih
simsek
hasan
fatih
simsek
hasan
fatih
simsek
hasan
fatih
simsek
W.karabuk1992
```

Terminal:
```
john --wordlist=linuxWordlist.txt  /etc/shadow
```

Output:
```
hefese:W.karabuk1992:16677:0:99999:7:::

1 password hash cracked, 0 left
```

d.

Eski Kali'deki Metasploit'ten netapi ile XP'ye sızdığımızı ve meterpreter payload'unun hashdump komutu ile XP'nin SAM dosyasını aşağıdaki gibi aldığımızı varsayalım.

SAM.txt

Administrator:500:aad3b435b51404eeaad3b435b51404ee:15feae27e637cb98ffacdf0a840eeb4b:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:aad3b435b51404eeaad3b435b51404ee:f638888c72f5c4e1a8f1e1270aaa6b85:::
IUSR_PENTEST-WINXP:1004:aad3b435b51404eeaad3b435b51404ee:f0a4854a729d96d5f8fddb3d144a9ee0:::
IWAM_PENTEST-WINXP:1005:aad3b435b51404eeaad3b435b51404ee:e4d4fc3f4174655f7884a06c27872477:::
pentest:1003:1e99d771a164613aaad3b435b51404ee:15feae27e637cb98ffacdf0a840eeb4b:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:4ad41e3eb3179b33e072f0c53e07d0db:::

Yukarıdaki hesaplardan sadece pentest kullanıcısının şifresi vardır. Şimdi bu şifreyi hash üzerinden JTR'ye buldurtalım:

Terminal:

```
cd /home/hefese/john-1.8.0/run
./john --format=LM  SAM.txt
```

Output:

```
Administrator::500:aad3b435b51404eea04ee:15feae27e637cb98ffacdf0a840eeb4b:::
Guest::501:aad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant::1000:aad3b435bb51404ee:f638888c7f1e1270aaa6b85:::
IUSR_PENTEST-WINXP::1004:aad3b435435b51404ee:f0a4854a729d96b3d144a9ee0:::
IWAM_PENTEST-WINXP::1005:aadd3b435b51404ee:e4d4fc3f417c27872477:::
pentest:PENTEST:1003:1e99d771a16461e:15feae27e637c40eeb4b:::
SUPPORT_388945a0::1002:aad3b51404ee:4ad41e3eb30c53e07d0db:::

7 password hashes cracked, 0 left
```

Görüldüğü üzere pentest kullanıcısının şifresinin PENTEST olduğu tespit edilmiştir. Diğerlerinin şifreleri olmadığından JTR direk yine onlara ait hash'leri ekrana basmıştır. O hash'ler NULL'ı temsil etmektedir.

```
NULL:
        aad3b435b51404eeaad3b435b51404ee
```

e.

Bu sefer sözlük ile değil de brute force ile şifre kırma işleminde bulunalım. Öncelikle JTR'ye vermek için elimizle (openssl ile) bir hash oluşturalım. Şifre test, salt da ab olsun (Çok kompleks bir şifre ve salt seçilmedi, çünkü şifre kırma işleminin uzamasını istemiyoruz).

> openssl passwd -1 -salt ab test

Output:
1ab$GR5WgfqnahyU5qOIirFwN0

Şimdi bu hash'i bir hash.txt dosyasına atalım ve jtr ile kırma işlemine başlayalım.

hash.txt
1ab$GR5WgfqnahyU5qOIirFwN0

Console
> john --incremental:ASCII hash.txt // Charset olarak ASCII seçilmiştir

Output
Loaded 1 password hash (md5crypt [MD5 32/64 X2])
Press 'q' or Ctrl-C to abort, almost any other key for status

test (?)
1g 0:00:02:29 0.006673g/s 12474p/s 12474c/s 12474C/s test..tesi

Use the "--show" option to display all of the cracked passwords reliably
Session completed

Bir müddet sonra şifre kırılacaktır ve şifrenin test olduğu yukarıda olduğu gibi bildirilecektir. Kırılan şifreyi tekrar görmek için --show parametresi kullanılabilir.

> john --show hash.txt

Output:
?:test
1 password hash cracked, 0 left