

John the ripper password cracker

Kullanım notları

23.07.2008 - Ali Okan YÜKSEL
okan[at]deu.edu.tr

<http://www.knyksl.com>

Program hakkında

John the ripper şifre kırma programıdır. Farklı algoritmalarla şifrelenmiş HASH 'leri programı kullanarak kırabilirsiniz.

DES/BSDI/MD5/BF/AFS/LM

Genellikle .htpasswd, linux kullanıcı şifreleri, MD5 parolalarını kırmak için kullanılır.

- Htpasswd – Okunan şifre dosyasında yer alan HASH'ler. DES veya MD5 tipinde olabilir.
- MD5 – SQL Injection yöntemi ile elde edilen parolaların kırılması.

Kurulum

Programın web sitesi <http://www.openwall.com/john/>

Unix/Linux/Windows ortamında sorunsuz çalışır.

Proceed to John the Ripper *Pro* homepage for your OS:

- [John the Ripper 1.7.3 Pro for Linux](#)
- [John the Ripper 1.7.2 Pro for Mac OS X](#) (also included is a beta version of 1.7.3.1 *Pro*)

Download one of the latest free "development" versions:

- [John the Ripper 1.7.3.1 \(Unix - sources, tar.gz, 796 KB\)](#) and its [signature](#)
- [John the Ripper 1.7.3.1 \(Unix - sources, tar.bz2, 642 KB\)](#) and its [signature](#)
- [John the Ripper 1.7.2 \(Unix - sources, tar.gz, 790 KB\)](#) and its [signature](#)
- [John the Ripper 1.7.2 \(Unix - sources, tar.bz2, 675 KB\)](#) and its [signature](#)

or the latest free "stable" release:

- [John the Ripper 1.7.0.2 \(Unix - sources, tar.gz, 784 KB\)](#) and its [signature](#)
- [John the Ripper 1.7.0.2 \(Unix - sources, tar.bz2, 675 KB\)](#) and its [signature](#)
- [John the Ripper 1.7.0.1 \(Windows - binaries, ZIP, 1360 KB\)](#) and its [signature](#)
- [John the Ripper 1.7.0.1 \(DOS - binaries, ZIP, 895 KB\)](#) and its [signature](#)

HASH nedir?

HASH karmaşık okunamaz halde şifrelenmiş veridir.

Örnek: 4QrcOUm6Wau+VuBX8g+IPg== gibi.

Üçüncü kişilerin eline geçme riskine karşı parolalar genellikle şifrelenerek HASH halinde saklanır.

Programcı tek yönlü fonksiyonları (bkz: one way functions) kullanarak üretmiş olduğu HASH'ı dosyada veya veritabanında saklar.

PHP programcıları bunun için md5, base64_encode, mdecrypt, crypt fonksiyonlardan yararlanabilir.

Apache'de .htaccess dosyasıyla yapılabilen giriş kontrolü, “htpasswd” uygulamasının üretmiş olduğu dosyada saklanan HASH ile karşılaştırma yaparak gerçekleşir.

John the ripper with MPI Patch

Şifre kırma işlemi daha güçlü bir işlemci ile daha kısa süre içerisinde sonuçlanacaktır. John the ripper MPI patch sürümü ile şifre kırma süresi kısaltılabilir. MPI sayesinde tek sistemle birden fazla işlemciyi kullanabilirsiniz veya cluster network üzerinde client'ları paralel olarak cracking işlemi için kullanabilirsiniz.

Aşağıdaki bağlantıyı inceleyebilirsiniz.

<http://usuarios.lycos.es/fedeaguirre2007/articulos/BackTrack%20John%20The%20Ripper%20MPI.pdf>

Örnek 1 – bruteforce attack

```
apptest# htpasswd -c sifredosyasi admin
```

```
New password:
Re-type new password:
Adding password for user admin
apptest# cat sifredosyasi
admin:Xp8LBR39bZsrs
apptest# echo "admin:6A8k81bErZEc6:admin" > sifrekir
apptest# john sifrekir
Loaded 1 password hash (Traditional DES [24/32 4K])
123456      (admin)
guesses: 1 time: 0:00:00:00 100% (2) c/s: 20198 trying: 12345 - boomer
apptest#
```

--format=Hash Type – hash tipini biliyorsanız --format=DES şeklinde belirtebilirsiniz.

--single – Tek bir hash kırmak istiyorsanız bu parametreyi kullanabilirsiniz.

Htpasswd ile oluşturduğumuz parola dosyası “sifredosyasi”, bu dosyadan okuduğumuz bilgileri “john”un algılayabileceği biçime sokup “sifrekir” dosyasına aktarıyoruz. Sonrasında “john sifrekir” komutu ile kısa süre içerisinde DES formatında saklanan parola geri dönüyor.

Örnek 2 – dictionary attack

```
apptest# john --wordlist=password.lst sifrekir.txt
```

John the ripper programı ile beraber gelen password.lst dosyasını inceleyebilirsiniz. Sözlük yöntemi ile sözlük dosyasındaki alternatif şifreler denenip, bizdeki HASH'le karşılaştırılır.