

Crack Kata Sandi File ZIP

Menggunakan John The Ripper

Dengan Teknik Dictionary Attack



Ditulis oleh: Rofi (Fixploit03)
<https://github.com/fixploit03/E-Books>

Disclaimer

Materi ini saya buat hanya untuk tujuan edukasi semata, tanpa ada niat untuk mendorong kegiatan ilegal atau yang melanggar hukum. Gunakanlah ilmu ini dengan bijak! Gunakanlah atau terapkanlah materi ini hanya jika Anda lupa kata sandi pada file ZIP milik Anda sendiri, dan hindarilah mencoba untuk meng-crack file ZIP milik orang lain tanpa izin.

Penulis materi ini tidak bertanggung jawab atas segala risiko yang timbul, baik di dunia maupun di akhirat. Semua risiko sepenuhnya menjadi tanggung sendiri.

Ditulis oleh: Rofi (Fixploit03)

Tanggal: Selasa, 15 April 2025

Pendahuluan

Apa itu John The Ripper?

John The Ripper (sering disingkat JTR) adalah salah satu tool password cracker (alat pemecah kata sandi) paling populer di dunia, terutama digunakan untuk pengujian keamanan kata sandi. Tool ini digunakan oleh ethical hacker, penetration tester, dan sysadmin untuk menemukan kata sandi yang lemah atau mudah ditebak dalam sistem.

Apa itu Dictionary Attack?

Dictionary attack adalah sebuah teknik dalam proses cracking kata sandi yang dilakukan dengan mencoba berbagai kemungkinan kata sandi berdasarkan daftar kata yang telah disiapkan sebelumnya, yang disebut sebagai wordlist atau kamus. Teknik ini bekerja dengan cara mencocokkan setiap kata dalam wordlist dengan kata sandi target, baik secara langsung (jika kata sandi masih dalam bentuk plaintext), maupun dengan cara mengenkripsi kata tersebut terlebih dahulu untuk dicocokkan dengan Hash yang ada.

Nah, sekarang sudah paham kan apa itu John The Ripper dan teknik Dictionary Attack?

Persyaratan:

Untuk meng-crack kata sandi file ZIP, ada beberapa persyaratan yang harus dipenuhi, di antaranya sebagai berikut:

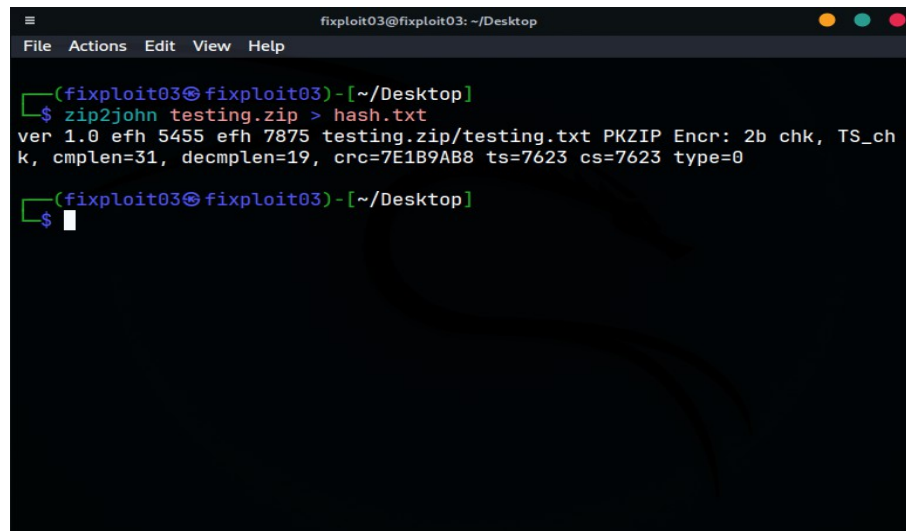
1. Laptop/PC (Personal Computer)
2. Sistem operasi Kali Linux (disarankan versi terakhir)
3. john
4. zip2john
5. File ZIP yang dilindungi kata sandi
6. Wordlist (file yang berisi kandidat kata sandi)
7. Kopi Kapal Api (biar makin mantap)

Langsung aja kita masuk ke tahap proses cracking-nya.

Tahap 1 (Ekstrak hash file ZIP)

Untuk meng-crack kata sandi file ZIP kita memerlukan hash file ZIP. Untuk mendapatkan hash-nya ketikkan perintah berikut ini:

```
$ zip2john [FILE ZIP] > [FILE HASH]
```

A screenshot of a terminal window with a dark background. The window title is 'fixploit03@fixploit03: ~/Desktop'. The menu bar shows 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows a prompt '(fixploit03@fixploit03)-[~/Desktop]' followed by the command '\$ zip2john testing.zip > hash.txt'. The output of the command is displayed on the next line: 'ver 1.0 efh 5455 efh 7875 testing.zip/testing.txt PKZIP Encr: 2b chk, TS_chk, cmplen=31, decmplen=19, crc=7E1B9AB8 ts=7623 cs=7623 type=0'. Below the output, the prompt '(fixploit03@fixploit03)-[~/Desktop]' is shown again, followed by a new prompt '\$' with a cursor.

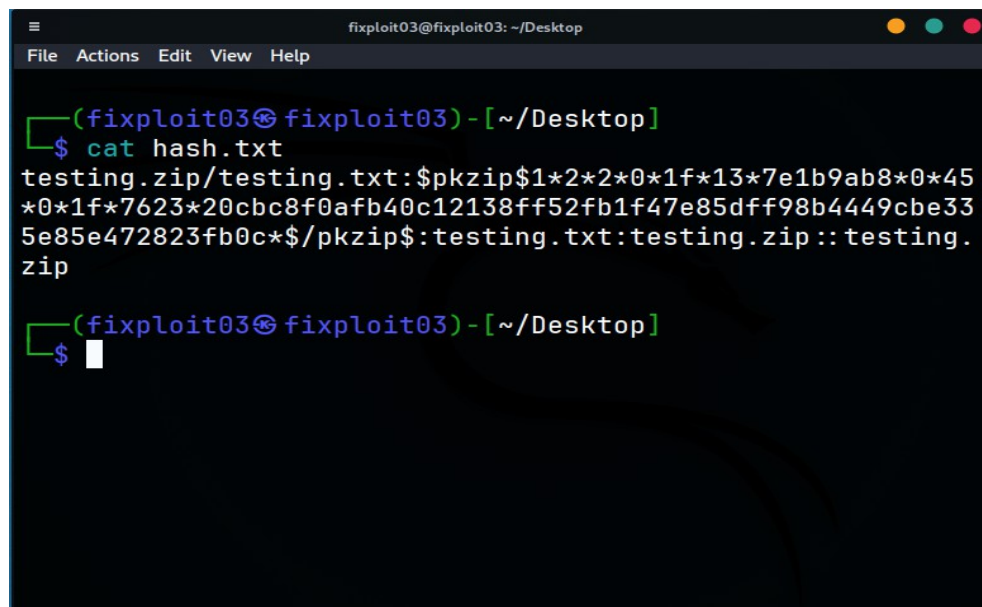
Gambar 1: Ekstrak hash file ZIP menggunakan zip2john

Keterangan perintah:

- zip2john : Alat yang digunakan untuk mengekstrak hash dari file ZIP.
- [FILE ZIP] : Nama file ZIP yang ingin diekstrak hash-nya.
- > : operator pengalihan output.
- [FILE HASH] : Nama file di mana hasil hash akan disimpan.

Untuk mengecek apakah kita sudah berhasil mengekstrak hash file ZIP-nya ketikkan perintah berikut ini:

```
$ cat hash.txt
```



```
fixploit03@fixploit03: ~/Desktop
File Actions Edit View Help

(fixploit03@fixploit03)-[~/Desktop]
$ cat hash.txt
testing.zip/testing.txt:$pkzip$1*2*2*0*1f*13*7e1b9ab8*0*45
*0*1f*7623*20cbc8f0afb40c12138ff52fb1f47e85dff98b4449cbe33
5e85e472823fb0c*$/pkzip$:testing.txt:testing.zip::testing.
zip

(fixploit03@fixploit03)-[~/Desktop]
$
```

Gambar 2: Melihat hasil ekstrak hash file ZIP menggunakan cat

Keterangan perintah:

- cat : Perintah untuk menampilkan isi dari sebuah file.
- hash.txt : File Hash hasil ekstraksi dari file ZIP.

Pada gambar di atas, kita sudah mendapatkan hash dari file ZIP-nya. Hash yang kita dapatkan adalah hash file ZIP dengan format PKZIP yang ditandai dengan “\$pkzip\$”.

Format Hash file ZIP

Sebelum masuk ke tahap selanjutnya (Cracking Hash File ZIP), ada sedikit materi mengenai format hash pada file ZIP. Secara umum, hash file ZIP memiliki dua format utama, yaitu:

1. Format Tradisional (PKZIP Klasik)
2. Format Modern (AES Encryption)

1. Format Tradisional (PKZIP Klasik)

Format ini digunakan pada file ZIP yang memakai enkripsi klasik atau enkripsi lama (ZipCrypto). Hash dari format ini biasanya diawali dengan \$pkzip\$ dan terdiri dari berbagai bagian penting, seperti versi PKZIP, metode kompresi, panjang data sebelum dan sesudah kompresi, CRC32, serta blok data terenkripsi yang akan digunakan dalam proses cracking. Proses cracking hash dari format ini umumnya lebih cepat dan ringan secara komputasi.

Contoh hash-nya:

```
$pkzip$1*2*2*0*1f*13*7e1b9ab8*0*45*0*1f*7623*5f1db5f3198bab299bf  
6eb7a085e3fab68a87aa4fa1fa4ef8b44d8ff77f286*$/pkzip$
```

Untuk meng-crack hash format Tradisional (PKZIP klasik), kamu dapat menggunakan opsi - - format=PKZIP pada tool John The Ripper-nya.

2. Format Modern (AES Encryption)

Format ini digunakan pada file ZIP yang telah dienkripsi dengan algoritma AES, baik AES-128, AES-192 maupun AES-256. Hash dari jenis ini umumnya lebih kompleks dan lebih panjang dibandingkan format klasik, serta bisa diawali dengan \$zip2\$. Karena tingkat enkripsi yang jauh lebih kuat, proses cracking untuk hash AES membutuhkan sumber daya yang besar dan waktu yang lebih lama.

Contoh hash-nya:

```
$zip2$*0*3*0*a1392883bf3f3117e2f9e9faca5a3b6f*b211*13*3b0a5eda06  
e2919e9fd3593b3ac8255215c6db*1cd75b26acd0568207e4*$/$zip2$
```

Untuk meng-crack hash format Modern (AES Encryption) kamu dapat menggunakan opsi - - format=ZIP pada tool John The Ripper-nya.

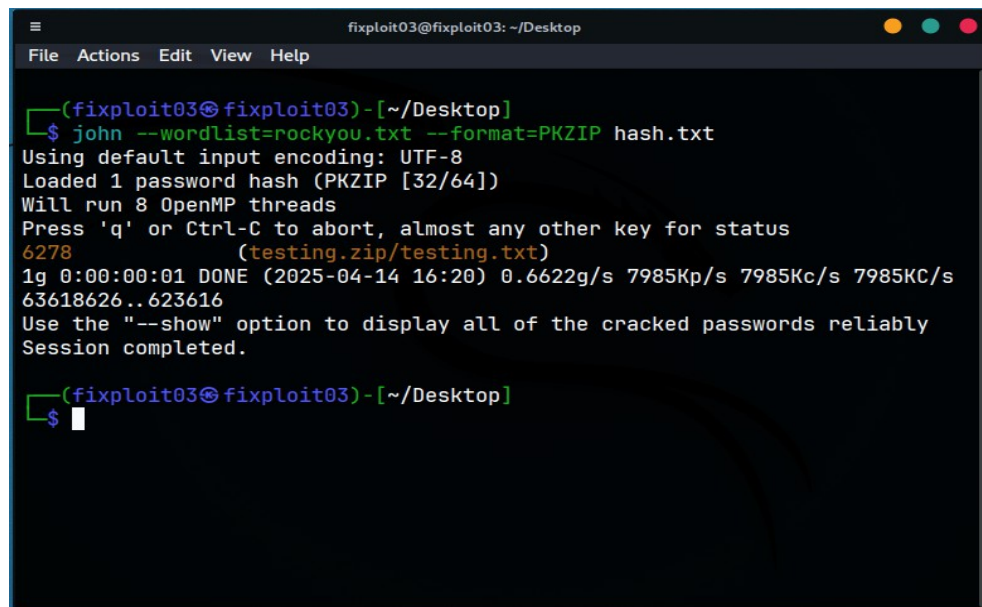
Itu dia sedikit penjelasan mengenai format hash pada file ZIP. Sekarang, langsung saja kita masuk ke tahap selanjutnya.

Tahap 2 (Crack Hash file ZIP)

Untuk meng-crack hash file ZIP, kita menggunakan tool John the Ripper.

Langsung saja ketikkan perintah berikut ini:

```
$ john --wordlist=[wordlist] --format=[format] hash.txt
```

A screenshot of a terminal window titled 'fixploit03@fixploit03: ~/Desktop'. The terminal shows the command '\$ john --wordlist=rockyou.txt --format=PKZIP hash.txt' being executed. The output indicates that the default input encoding is UTF-8, 1 password hash (PKZIP [32/64]) was loaded, and 8 OpenMP threads will be used. The session is completed, showing a progress bar and the message '1g 0:00:00:01 DONE (2025-04-14 16:20) 0.6622g/s 7985Kp/s 7985Kc/s 7985KC/s 63618626..623616'. The terminal prompt returns to '\$ '.

Gambar 3: Crack hash file ZIP menggunakan john

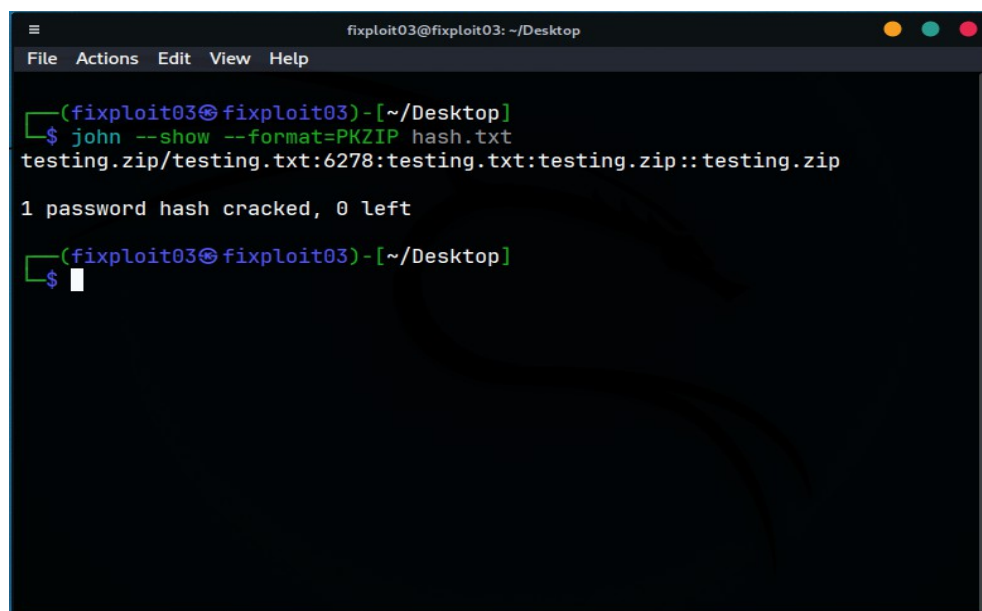
Keterangan:

- john : Alat yang digunakan untuk meng-crack hash.
- wordlist : Mengaktifkan mode Dictionary Attack.
- [wordlist] : Nama file wordlist yang ingin digunakan.
- format : Menentukan format Hash yang digunakan.
- [format] : Format Hash file ZIP (PKZIP atau ZIP).
- hash.txt : File Hash hasil ekstraksi dari file ZIP.

Pada gambar di atas, kita berhasil mendapatkan kata sandi dari hash file ZIP. Kata sandinya adalah “6278”.

Untuk memastikan apakah hash-nya sudah benar-benar berhasil di-crack atau tidak, ketikkan perintah berikut ini:

```
$ john --show --format=[format] hash.txt
```



```
fixploit03@fixploit03: ~/Desktop
File Actions Edit View Help

(fixploit03@fixploit03)-[~/Desktop]
$ john --show --format=PKZIP hash.txt
testing.zip/testing.txt:6278:testing.txt:testing.zip::testing.zip

1 password hash cracked, 0 left

(fixploit03@fixploit03)-[~/Desktop]
$
```

Gambar 4: Lihat status hasil crack hash file ZIP menggunakan john

Keterangan:

john	: Alat yang digunakan untuk meng-crack hash.
--show	: Menampilkan status hash.
--format	: Menentukan format Hash yang digunakan.
[format]	: Format Hash file ZIP (PKZIP atau ZIP).
hash.txt	: File Hash hasil ekstraksi dari file ZIP.

Berdasarkan gambar di atas, kita sudah berhasil meng-crack satu hash. Untuk melihat kata sandinya, kamu bisa melihatnya di antara tanda titik dua (:), yaitu "6278".

Pada tahap ini, kamu sudah berhasil meng-crack kata sandi file ZIP menggunakan tool John The Ripper dengan teknik Dictionary Attack. Selamat, kamu berhasil mendapatkan akses ke file ZIP tersebut!

Kesimpulan:

Dalam materi ini, kita telah mempelajari cara meng-crack kata sandi file ZIP menggunakan teknik Dictionary Attack dengan tool John The Ripper. Dengan cara ini, kita berhasil mengekstrak hash file ZIP, memverifikasinya, dan akhirnya mendapatkan kata sandi file ZIP tersebut.

Namun, perlu diingat bahwa teknik ini hanya efektif jika kata sandi yang digunakan mudah ditebak atau termasuk dalam daftar wordlist. Untuk file ZIP yang menggunakan enkripsi kuat seperti AES, proses cracking menjadi jauh lebih sulit dan memerlukan waktu yang sangat lama, kecuali jika kata sandinya sangat lemah.

Tips Tambahan/Saran:

1. Gunakan Jenis Enkripsi yang Kuat

Pastikan file ZIP yang Anda buat menggunakan enkripsi yang kuat seperti AES. Jika memungkinkan, gunakan enkripsi AES-256, karena enkripsi ini memiliki tingkat keamanan yang lebih tinggi dibandingkan AES-128.

2. Hindari Menggunakan kata sandi Umum

Jangan gunakan kata sandi yang mudah ditebak, seperti kombinasi angka berurutan atau kata yang sering digunakan (misalnya, "12345678" atau "rofiganteng123"). Sebaiknya, gunakan kombinasi karakter yang kompleks, termasuk huruf kecil, huruf besar, angka, dan simbol, serta pastikan panjangnya cukup (disarankan lebih dari 8 karakter).

Troubleshooting

Jika tool zip2john dan john belum terinstal di sistem, kamu bisa menginstalnya dengan menjalankan perintah berikut ini:

```
$ sudo apt-get update  
$ sudo apt-get install john john-data
```

Jika kamu mendapatkan pesan berikut saat mencoba men-crack hash file ZIP:

```
Using default input encoding: UTF-8  
No password hashes loaded (see FAQ)
```

Pesan tersebut menandakan bahwa hash file ZIP yang dimasukkan tidak valid.

Jika ada hal lain atau pertanyaan yang ingin ditanyakan, silakan tanyakan di sini:

<https://github.com/fixploit03/E-Books/issues>

Penutup

Semoga materi ini bisa menjadi panduan yang bermanfaat bagi siapa saja yang ingin memahami proses cracking file ZIP dengan teknik Dictionary Attack menggunakan tool John The Ripper . **Ingatlah bahwa pengetahuan adalah pedang bermata dua gunakanlah dengan bijak dan bertanggung jawab.**

Jangan pernah menyalahgunakan ilmu ini untuk hal-hal yang melanggar hukum atau merugikan orang lain. Jadilah pembelajar yang etis dan profesional.

Teruslah belajar, bereksperimen, dan berkembang di dunia keamanan siber.

Sampai jumpa di materi selanjutnya!

– Rofi (Fixploit03) -

Harap jangan menggunakan materi ini untuk melakukan hal-hal bodoh.

Penulis tidak bertanggung jawab atas kerusakan yang disebabkan oleh materi ini.

GUNAKAN DENGAN RISIKO ANDA SENDIRI.