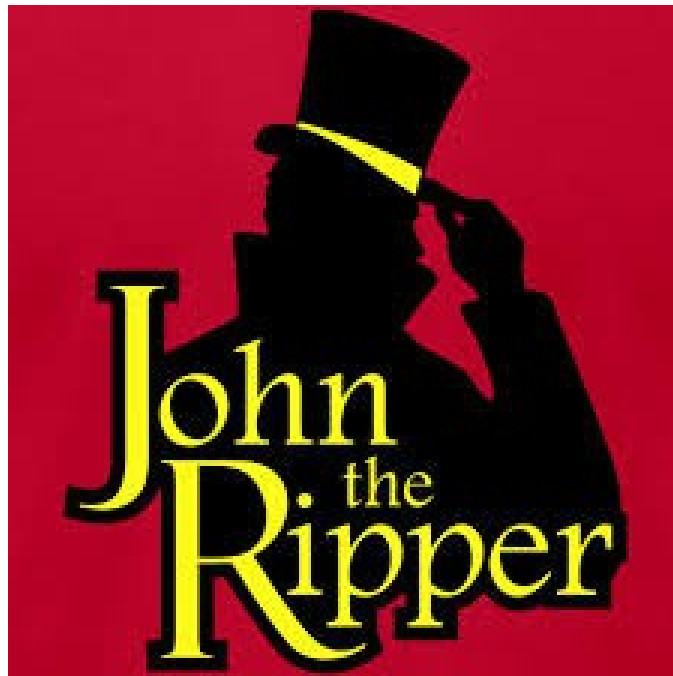


Crack Kata Sandi File ZIP dengan JTR Teknik Dictionary Attack



Ditulis oleh: Rofi (Fixploit03)

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.

- Rofi (Fixploit03) -

Pendahuluan

Apa itu John The Ripper

John The Ripper (sering disingkat **JTR**) adalah salah satu alat pemecah kata sandi (password cracker tool) paling populer di dunia, terutama digunakan untuk pengujian keamanan kata sandi. Alat 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. Wordlist ini biasanya berisi kata-kata umum yang sering digunakan sebagai password, seperti nama, angka, tanggal lahir, atau kombinasi populer seperti **"123456"** atau **"rofiganteng123"**. Teknik ini bekerja dengan cara mencocokkan setiap kata dalam wordlist dengan password target, baik secara langsung (jika password masih dalam bentuk plaintext), maupun dengan cara mengenkripsi kata tersebut terlebih dahulu untuk dicocokkan dengan Hash yang ada. Karena mengandalkan kata-kata yang sudah dikenal atau umum, dictionary attack jauh lebih cepat dibanding brute-force attack, namun efektivitasnya bergantung pada kualitas dan kelengkapan wordlist yang digunakan. Teknik ini sering digunakan oleh ethical hacker dan pentester untuk menguji kekuatan kata sandi dalam sistem keamanan.

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

Langsung aja kita masuk ke tahap proses cracking-nya.

Persyaratan:

Untuk melakukan cracking kata sandi file ZIP, ada beberapa persyaratan yang perlu dipenuhi, di antaranya sebagai berikut:

1. Laptop/PC (Personal Computer)
2. Sistem operasi Kali Linux
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)

Tahap 1 (Mengekstrak Hash file ZIP)

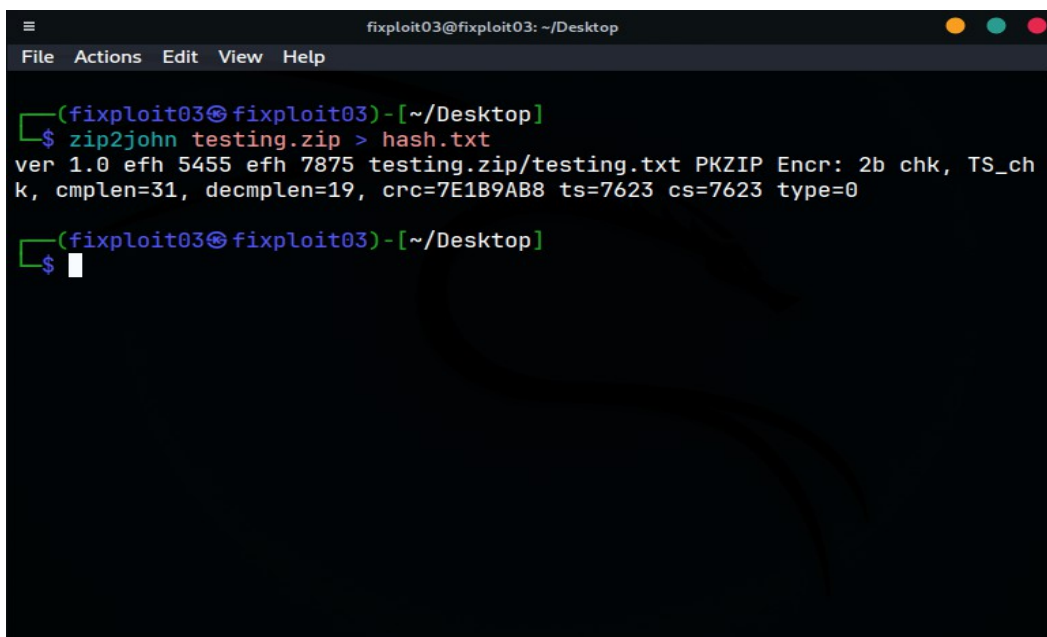
Untuk meng-crack kata sandi file ZIP kita memerlukan Hash file ZIP. Untuk mendapatkan Hash file ZIP kita menggunakan alat **zip2john** yang sudah tersedia secara default di sistem operasi Kali Linux.

Langsung saja, kita ekstrak Hash file ZIP dengan cara membuka terminal, kemudian ketikkan perintah berikut:

```
$ zip2john [file zip] > [file hash]
```

Keterangan:

[file zip] : Nama file ZIP yang akan di-crack.
> : Mengalihkan output standar (stdout) ke file.
[file hash] : Nama file untuk menampung Hash dari file ZIP.

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

Hasilnya akan terlihat seperti gambar di atas. Kalo mau membuktikan atau memverifikasi apakah Hash file ZIP sudah benar-benar diekstrak ketikkan "**cat hash.txt**" untuk melihat isi file **hash.txt**.

Format Hash file ZIP

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

1. PKZIP
2. ZIP

1. Format PKZIP

Format **PKZIP** adalah format yang digunakan oleh file ZIP lama yang menggunakan enkripsi **ZipCrypto**. Format ini memiliki tingkat keamanan yang sangat lemah dan rentan untuk di-crack atau dibobol, sehingga sangat disarankan untuk tidak menggunakannya untuk melindungi data sensitif.

Contoh Hash:

```
$pkzip$1*2*2*0*1f*13*7e1b9ab8*0*45*0*1f*7623*5f1db5f3198bab299bf6eb7a085e3fab68a87aa4fa1fa4ef8b44d8ff77f286*$/pkzip$
```

2. Format ZIP

Format **ZIP** adalah format yang digunakan oleh file ZIP baru dengan enkripsi **AES (128, 192, dan 256)**. File ZIP dengan enkripsi AES sangat sulit bahkan hampir mustahil untuk di-crack, kecuali jika kata sandinya memang mudah ditebak, seperti kata sandi umum yang sering digunakan banyak orang, misalnya **"12345678"**.

Contoh Hash:

```
$zip2$*0*3*0*a1392883bf3f3117e2f9e9faca5a3b6f*b211*13*3b0a5eda06e2919e9fd3593b3ac8255215c6db*1cd75b26acd0568207e4*$/zip2$
```

Itu dia sedikit materi mengenai format Hash file ZIP. Langsung saja ke tahap selanjutnya.

Tahap 2 (Crack Hash file ZIP)

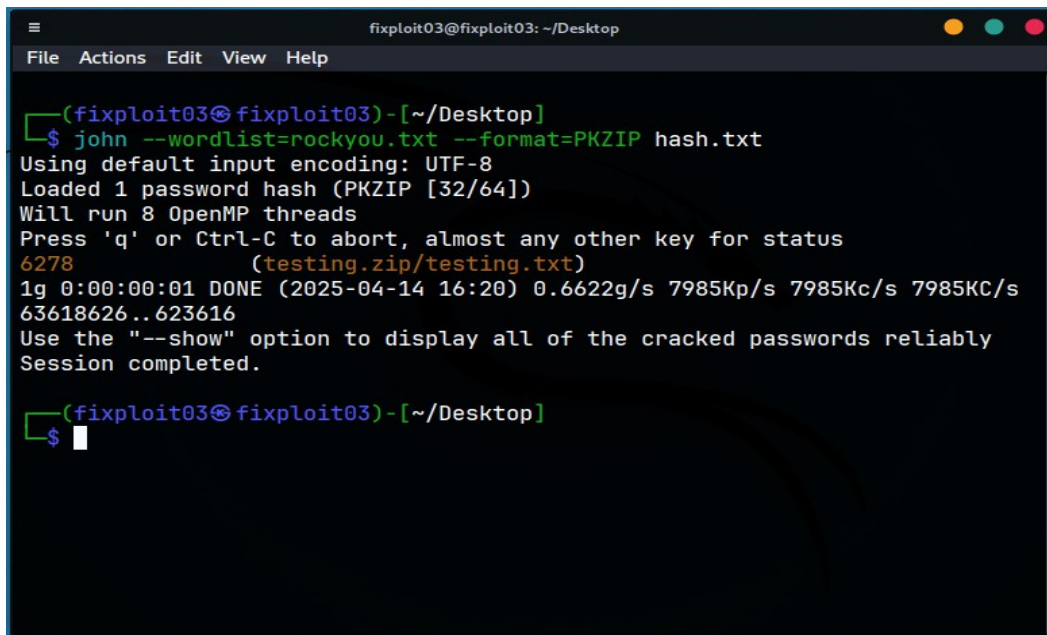
Untuk meng-crack Hash file ZIP kita menggunakan alat **john** yang sudah tersedia secara default di sistem operasi Kali Linux.

Langsung saja, kita buka terminal yang tadi, kemudian ketikkan perintah berikut:

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

Keterangan:

<code>--wordlist</code>	: Mengaktifkan mode Dictionary Attack.
<code>[wordlist]</code>	: Nama file wordlist yang ingin digunakan.
<code>--format</code>	: Menentukan format Hash yang digunakan.
<code>[format]</code>	: Format Hash file ZIP (PKZIP atau ZIP).
<code>hash.txt</code>	: File Hash hasil ekstraksi dari file ZIP.



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

(fixploit03@fixploit03)-[~/Desktop]
$ john --wordlist=rockyou.txt --format=PKZIP hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
6278 (testing.zip/testing.txt)
1g 0:00:00:01 DONE (2025-04-14 16:20) 0.6622g/s 7985Kp/s 7985Kc/s 7985KC/s
63618626..623616
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

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

Gambar 2: Crack Hash file ZIP menggunakan john

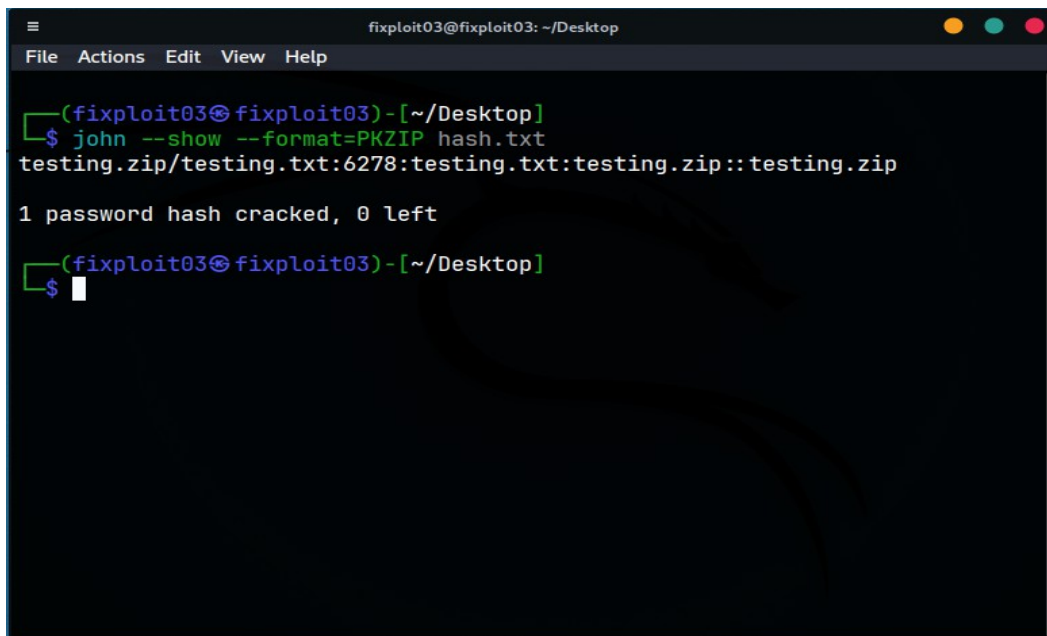
Pada gambar di atas, kita berhasil mendapatkan kata sandi dari file ZIP. Kata sandinya adalah **“6278”**, yang disorot dengan warna kuning. Di sebelah kanan, kita dapat melihat metadata dari Hash tersebut, yang mencakup informasi seperti **“nama file ZIP”** dan **“isi dari file ZIP”** tersebut.

Untuk memastikan bahwa Hash sudah benar-benar berhasil di-crack, ketikkan perintah berikut:

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

Keterangan:

<code>--show</code>	: Menampilkan kata sandi yang telah berhasil di-crack.
<code>--format</code>	: Menentukan format Hash yang digunakan.
<code>[format]</code>	: Format Hash file ZIP (PKZIP atau ZIP).
<code>hash.txt</code>	: File Hash hasil ekstraksi dari file ZIP.



```
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 3: Melihat Status Hash file ZIP menggunakan john

Berdasarkan hasil di atas, kita sudah berhasil meng-crack 1 Hash. Untuk melihat kata sandinya, kamu bisa melihatnya di antara tanda titik dua (:), yaitu “6278”.

Pada tahap ini, Anda telah berhasil meng-crack kata sandi file ZIP menggunakan **John The Ripper (JTR)** dengan teknik **Dictionary Attack**. Selamat, Anda 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 bantuan **John The Ripper (JTR)**. 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 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**).

Penutup

Semoga materi ini bisa menjadi panduan yang bermanfaat bagi siapa saja yang ingin memahami proses cracking file ZIP dengan teknik **Dictionary Attack** menggunakan **John The Ripper (JTR)**. 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.