Lama Waktu untuk Membongkar Password

Happy Chandraleka
hchandraleka@gmail.com
http://thecakrabirawa.wordpress.com

Ketika kita mencoba membongkar sebuah password menggunakan perangkat software, mungkin terbesit pertanyaan, berapa lama waktu yang dibutuhkan untuk membongkar atau mendapatkan password tersebut. Jawabnya lama pembongkaran password tergantung pada beberapa faktor, yaitu:

1. Panjang password yang akan dibongkar.
2. Ragam karakter dari password tersebut.
3. Kekuatan komputer yang digunakan untuk membongkar password.

Mari kita lihat lebih jauh. Sebuah password, makin panjang suatu password maka proses pembongkarannya makin lama, karena makin banyak variabel yang perlu dicoba. Sebuah password dengan tiga karakter saja (semisal password ‘qwe’) akan lebih mudah untuk dibongkar dan perlu waktu relatif lebih singkat ketimbang sebuah password yang memuat lima karakter (semisal password ‘abcde’). Dalam hal ini Anda perlu memahami cara kerja atau mekanisme proses pembongkaran password.

Gambar Lama pembongkaran password tergantung beberapa faktor

Proses pembongkaran password dilakukan dengan mencoba **semua** kemungkinan yang ada. Ini yang dikenal dengan nama **Brute Force Attack**. Semisal password ‘**qwe**’ di atas, berarti ada **tiga**

slot yang harus diinputkan karakter dengan banyak kemungkinan yang harus dicoba. **Berapa kemungkinan tersebut**? Hal ini dapat dihitung dengan mudah. Untuk satu slot, karakter yang harus dicoba diinputkan membentang dari 'a' sampai 'z', ada sebanyak 26 karakter alfabet lower case (huruf kecil). Demikian juga untuk slot kedua dan slot ketiga. Dengan demikian jumlah kemungkinan semua karakter password yang harus dicoba ada sebanyak:

$$26*26*26 = 17.576$$

Ada sebanyak 17.576 karakter password yang harus dicoba dan password 'qwe' masuk ke dalam salah satu kemungkinan karakter password di dalamnya.

Dengan demikian bila ada sebuah password yang terdiri dari lima karakter, dapat dihitung pula jumlah kemungkinan karakter password yang harus dicoba. Password dengan lima karakter (lower case) memuat lima slot yang perlu diisi. Kemungkinan password yang harus dicoba yaitu :

$$26*26*26*26*26 = 11.881.376$$

Berarti ada 11.881.376 kemungkinan password yang harus dicoba, dan password 'abcde' masuk ke dalam salah satu kemungkinan tersebut. Kesimpulannya makin panjang suatu password makin banyak kemungkinan password yang harus dicoba untuk proses pembongkarannya. Dengan demikian proses pembongkaran akan semakin sulit dan perlu waktu lebih lama.

Pada penjelasan diatas dianggap jumlah karakter password yang akan dibongkar telah diketahui, yaitu tiga atau lima. Bagaimana bila jumlah karakter password (yang akan mengisi slot-slot tersebut) belum diketahui? Tentunya kita harus melakukan tebak-tebakan untuk mengira jumlah karakter password yang akan dibongkar. Dan tentunya ini akan memperlama lagi proses pembongkaran password. Inilah penjelasan point yang pertama.

Kemudian, pada penjelasan di atas, ragam karakter yang digunakan dalam password hanya satu ragam, yaitu lower case (huruf kecil). Bila ragam karakter yang digunakan dalam password makin banyak tentunya akan menyebabkan semakin banyak kemungkinan password yang harus diuji coba. Berikut penjelasannya.

Semisal password di atas kita ubah menjadi 'qwE' (dengan huruf e kapital). Dengan demikian ragam karakter untuk password pun bertambah, ada alfabet dengan lower case (huruf kecil) dan ada alfabet dengan upper case (huruf besar). Imbasnya, kemungkinan password yang harus diujicoba untuk proses pembongkaran pun bertambah. Kita hitung saja. Bentangan karakter untuk alfabet lower case dari 'a' sampai 'z' ada 26, dan bentangan karakter untuk alfabet upper case dari 'A' sampai 'Z' ada 26. Dengan demikian, sebuah password dengan tiga karakter (tiga slot) yang mempunyai dua ragam karakter (alfabet lower case dan upper case) akan mempunyai kemungkinan password yang harus diujicoba sebanyak :

$$(26+26) * (26+26) * (26+26) = 140.608$$

Ada 140.608 kemungkinan password yang harus diuji coba. Ini untuk password dengan tiga karakter dengan dua ragam karakter (alfabet lower case dan upper case). Bandingkan dengan sebuah password dengan tiga karakter dengan satu ragam karakter saja, hanya mempunyai kemungkinan kombinasi password sebanyak 17.576. Lebih sedikit. Lalu bagaimana juga dengan password yang memuat ragam karakter alfabet lower case dan upper case, serta memuat angka digital,

simbol-simbol karakter khusus, atau bahkan semua karakter dalam kode ASCII? Kesimpulannya, makin banyak ragam karakter dalam suatu password, maka makin banyak kemungkinan password yang harus dicoba. Dengan demikian proses pembongkaran akan semakin sulit dan perlu waktu lebih lama.

Yang terakhir, lama proses pembongkaran password tergantung pada kekuatan komputer yang digunakan untuk membongkar password. Ambil misal sebuah komputer mampu melakukan komputasi untuk membongkar password dengan kecepatan 1000 password per detik. Kemudian kita bisa hitung berapa waktu yang dibutuhkan oleh komputer ini untuk membongkar password yang mempunyai satu ragam karakter baik sebuah password dengan tiga karakter maupun lima karakter. Perlu diingat dari hitung-hitungan sebelumnya, untuk password dengan tiga karakter (satu ragam karakter lower case) memuat 17.576 kemungkinan password yang harus dicoba. Sedangkan untuk password dengan lima karakter (satu ragam karakter lower case) memuat 11.881.376. Hasil perhitungannya dapat kita lihat pada tabel di bawah ini.

	Kekuatan komputasi	**Lama pembongkaran**
Password tiga karakter **17.576**	1000 per detik	Sekitar 17 detik
Password lima karakter **11.881.376**	1000 per detik	Sekitar 11.881 detik atau 3,3 jam

Dengan demikian, lama pembongkaran password tergantung pada faktor-faktor yaitu panjang password yang akan dibongkar, ragam karakter dari password tersebut, dan kekuatan komputer yang digunakan untuk membongkar password.

Biografi Penulis

Happy Chandraleka. Seorang penulis TI independen. Menyelesaikan S1 di Teknik Elektro Universitas Diponegoro. Saat ini mengelola Open Journal System Badan Penelitian dan Pengembangan Kesehatan, Kementerian Kesehatan Republik Indonesia. Informasi tentang penulis dapat dilihat di http://thecakrabirawa.wordpress.com dan dapat dihubungi via email hchandraleka@gmail.com.

(diedit ulang di Pare, Kediri, Jawa Timur, 26 November 2013, pukul 05.38 pagi)