Strategi & Manajemen Password

Yudha Yudhanto, S.Kom
yyudhanto@gmail.com

Sepele namun puenting! Itulah yang kita rasakan jika membahas *password*. Password adalah kode sandi yang harus dimasukkan ke dalam suatu sistem berupa karakter tulisan, suara, atau ciri-ciri khusus yang harus diingat. Kalau sampai lupa, bisa berabe, ditambah ada hal penting dan harus segera dilakukan atau diketahui.

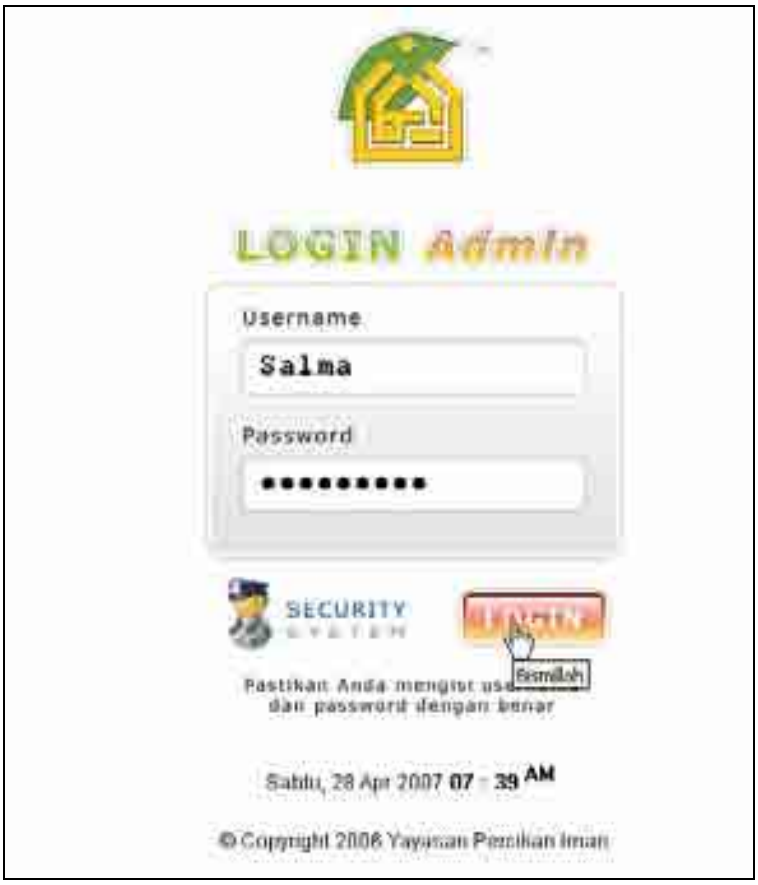
Di zaman tekno ini, setiap hari orang tidak terlepas dari proses password-mempassword. Misalnya, kode pin: ATM, kartu kredit, milist, e-mail, messeger/chatting, blog, bahkan ketika memakai komputer.

Kenapa kita membutuhkan password, bukankah tanpa password akan lebih enak. Kita tidak perlu susah mengingat dan proses akan lebih cepat, tanpa harus punten atau kulanuwun.

Ternyata, tujuan utama password tidak lain adalah sebagai sistem yang akan memastikan bahwa benar-benar hanya pemilik saja yang bisa masuk ke dalamnya. Kemudian, kita akan dapat melihat atau menggunakan data dan informasi yang kita miliki sesuai tujuan atau keperluan.

Proses password

Password adalah bagian dari proses authentikasi. Sebuah istilah yang merupakan ‘benteng’ terakhir dari sebuah sistem keamanan pada sebuah data atau informasi. Konkretnya, salah satu cara yang umum digunakan untuk mengamankan sebuah sistem adalah dengan mengatur akses pemakai (user) ke dalamnya melalui mekanisme pencocokan kebenaran (authentication) dan pemberian hak akses (access control). Implementasi dari mekanisme ini antara lain dengan menggunakan password. Contoh mudahnya adalah ketika akan menggunakan sebuah komputer, pemakai diharuskan melalui proses authentication dengan menuliskan user id dan password-nya. Informasi yang diberikan ini akan dicocokkan dengan data dalam sistem. Apabila keduanya cocok (valid), calon pemakai diperbolehkan ‘masuk’ tapi jika tidak, pesan kegagalan akan muncul.



Gbr. Contoh proses authentikasi

Setelah proses authentication, pemakai diberikan hak akses sesuai dengan tingkatan hak yang diberikan kepadanya. Access control ini biasanya dikelompokkan dalam kategori group. Ada group user biasa, ada tamu (guest), dan ada juga sebagai penguasa/pengatur atau admin yang memiliki hak istimewa. Pengelompokan ini disesuaikan dengan kebutuhan dan tugas masing-masing pengguna. Di lingkungan kampus, biasanya ada kelompok mahasiswa, staf, karyawan, dosen, rektor dan administrator. Sementara itu, di lingkungan bisnis ada kelompok finance, engineer, auditor, marketing, director, dan seterusnya.

Password Cracker

Adanya program-program pembobol password (password cracker) sangat berbahaya karena bisa dipakai untuk merusak, tetapi juga mendidik agar setiap orang selalu teliti dan perhatian terhadap hal yang dimilikinya. Prinsip program ini adalah melakukan coba dan mencoba. Program pembobol tersebut sangat mudah didapat/download dari internet, seperti tools: Hades, Claymore, Cain, PWLFind, LopthCrack, ScanNT, NTCrack, Password NT, Brutus, Crack, Crackerjack, Viper, John The Ripper, Hellfire, Guess, dan masih banyak lagi yang bergentayangan dan terus bertambah canggih. Setelah mendapatkan nama atau nomor user id, akan dicoba untuk mendapatkan ’pasangannya’ dengan beberapa metode, di antaranya:

Dictionary Attack

Mengambil perbendaharaan kata dari kamus (dictionary). Pemecahan password dilakukan melalui uji coba kata atau kalimat yang dikumpulkan dari berbagai sumber. Karenanya, akan sangat berisiko jika sobat memilih password dari kata-kata umum, termasuk juga istilah populer, nama, kota, atau lokasi. Seperti: bandung, jakarta, cihampelas, dsb. Mencocokkan kata sandi dengan isi kamus dari A-Z bukan hal yang sulit. Jika beruntung! Semakin cepat kemampuan komputer, akan semakin singkat menemukan kecocokan.

Hybrid Attack

Teknik ini mengandalkan beberapa algoritma heuristic, seperti menambahkan angka atau perkataan di belakang atau di depannya, membaca dari belakang (terbalik), dan cara-cara unik lainnya. Sang cracker mengumpulkan segala informasi tentang calon korbannya. Kemudian dijadikan bahan kombinasi, sering dijumpai penggunaan password, seperti nama user-nya kemudian hanya ditambah tahun lahir atau tahun sekarang, contoh: yunus78 atau agus2006

Brute Force Attack

Cara terakhir ini cukup jitu, hanya kelemahannya adalah terlalu banyak waktu yang dihabiskan. Apalagi, jika pin password yang ditebak cukup panjang dan merupakan perpaduan dari banyak karakter. Dengan memakai teknik ini, setiap karakter dalam keyboard, seperti: huruf dari a-z, A-Z, dan 0-9, serta ASCII character akan dikombinasikan satu per satu sampai mendapatkan jawabannya.
Ilustrasi praktis dalam mencari kombinasi password adalah dengan rumus berikut ini.

A = b ^ c

Keterangan :
a = Jumlah kombinasi password
b = Jumlah karakter yang dipersyaratkan
c = Jumlah karakter password yang harus ditebak
^ = Pangkat

Contoh:
Password yang ditebak terdiri atas angka, berarti karakternya hanya 10 (1,2,3,4,5,6,7,8,9,0)
Jumlah atau panjang karakter passwordnya = 6, misalnya (050679)
Maka dipastikan password tersebut bagian dari:

10 ^ 6 = 1.000.000 kombinasi

Bisa dibayangkan, berapa waktu yang dihabiskan jika karakter kombinasi password-nya terdiri atas alpha-numerik dan karakter spesial lainnya, ditambah lagi dengan panjang karakternya. Hal itu akan membutuhkan banyak sekali kemungkinan kombinasi. Dan pasti membutuhkan komputer untuk men-generate kombinasi serta mencocokkanya satu per satu dalam waktu berjam-jam, berhari-hari, bahkan berbulan-bulan.

Trik Memilih password

Selama masih menggunakan kode-kode dalam keyboard, sepertinya tidak ada password yang tidak dapat ditebak. Memilih atau merancang password memerlukan strategi khusus dan harus mau mengubah-ubah dalam kurun tertentu. Tidak memakai password sama sekali (blank password) sangat tidak dianjurkan, walaupun itu menjanjikan kemudahan.

Ingatlah! Kejahatan bukan hanya karena niat, bisa jadi karena tidak sengaja lewat, melihat, atau mendengar. Berikut ini adalah daftar hal-hal yang sebaiknya tidak digunakan sebagai password.

- Nama Anda, istri/suami, anak, ataupun famili, nama komputer, alamat rumah, nomor telepon, atau plat nomor kendaran.
- Tanggal lahir pribadi atau keluarga.
- Kata-kata populer yang terdapat dalam kamus (bahasa Indonesia/Inggris).
- Password dengan karakter sama yang diulang-ulang atau berurutan dalam penyebutan atau secara tata letak dalam keyboard. (contoh: 12345, asdfgh, qwerty)

Beruntunglah, ternyata ada banyak sistem komputer yang dilengkapi kemampuan menilai password yang kita buat. Contohnya, jika password yang kita usulkan tidak aman, komputer dapat mengatakan bahwa password Anda terlalu pendek, kombinasi password Anda buruk, password yang dibuat sama dengan username Anda, silakan ulangi lagi, dan seterusnya.

Menjamin 100% bahwa password kita tidak bisa ditembus adalah tidak mungkin.

Berikut tips membuat password.

- Gunakan kombinasi karakter dari huruf kecil, besar, dan karakter khusus, seperti @,#,$. Contohnya: $e@r(hEnG1N3, tr4nsmut4t10n, b@mb4ng, m45t3r, 3m1Lku, p3r(ik@n1m@n.
- Gunakan batas panjang karakter secara maksimal, kalau bisa tidak kurang dari 8.
- Jangan pernah memberitahukannya secara lisan (bisa jadi didengar orang lain) atau ditulis di kertas atau lewat sms. Menjadi repot atau dianggap kurang percaya dengan orang lain adalah lebih baik daripada mengizinkan orang yang meragukan untuk memasuki wilayah keamanan kita. Kecuali jika terpaksa. Jika memang perlu ditulis, simpan di tempat aman (misalnya: dompet). Tetapi kalau sudah benar-benar hafal, tulisan itu harus lekas dihancurkan/buang.
- Bagi yang mempunyai hobi banyak account. Misalnya dimilist, mail, atau messeger di Yahoo, MSN, ICQ, Gmail, Frendster, Plasa, Hotmail, blogger dsb. akan menyulitkan dan menghabiskan space otak jika harus mengingat banyak password. Apalagi harus menggantinya dalam kurun waktu tertentu, mungkin akan menambah pusing dulu sebelum bekerja, apalagi jika ternyata lupa.

Solusi single-password lebih disukai karena kita tinggal mengingat satu password untuk semua account. Kelemahannya, sekali tertebak berisiko dibobol. Solusi yang lain adalah password bertingkat. Misalnya, kita buat password untuk 3 kriteria: (1) penting; (2) sedang; dan (3) tidak penting. Contohnya, tabel di bawah ini:

(1) Penting	(2) Sedang	(3) Tidak Penting
Email dan milist untuk private, Login jaringan, dial-up ISP, Messeger	Email untuk milist pengetahuan, dsb	Email untuk milist hiburan, dsb

Jika suatu saat kita lupa password-nya kita hanya perlu mencoba mengulang password dua atau tiga kali saja langsung tembus.

Semoga bermanfaat.

Biografi Penulis

Yudha Yudhanto. Alumni STMN 1 Surakarta (1997) dan UNIKOM(2005). Pernah bergelut dengan hardware komp, network, coding dan akhirnya terdampar di dunia desain. Sangat menyukai hal-hal yang berbau 'design' baik untuk cetak atau non-cetak. Sambilan untuk cari klethikan adalah webmaster, webdesain, nulis artikel dan ngopreg hp. *Maturnuwun*