APTIKOM
ASOSIASI PERGURUAN TINGGI INFORMATIKA DAN KOMPUTER

MODUL PJJ

## Mata Ajar

***MANAJEMEN KEAMANAN INFORMASI DAN INTERNET***

## Topik Bahasan

***MANAJEMEN PASSWORD***

## Versi

***2013/1.0***

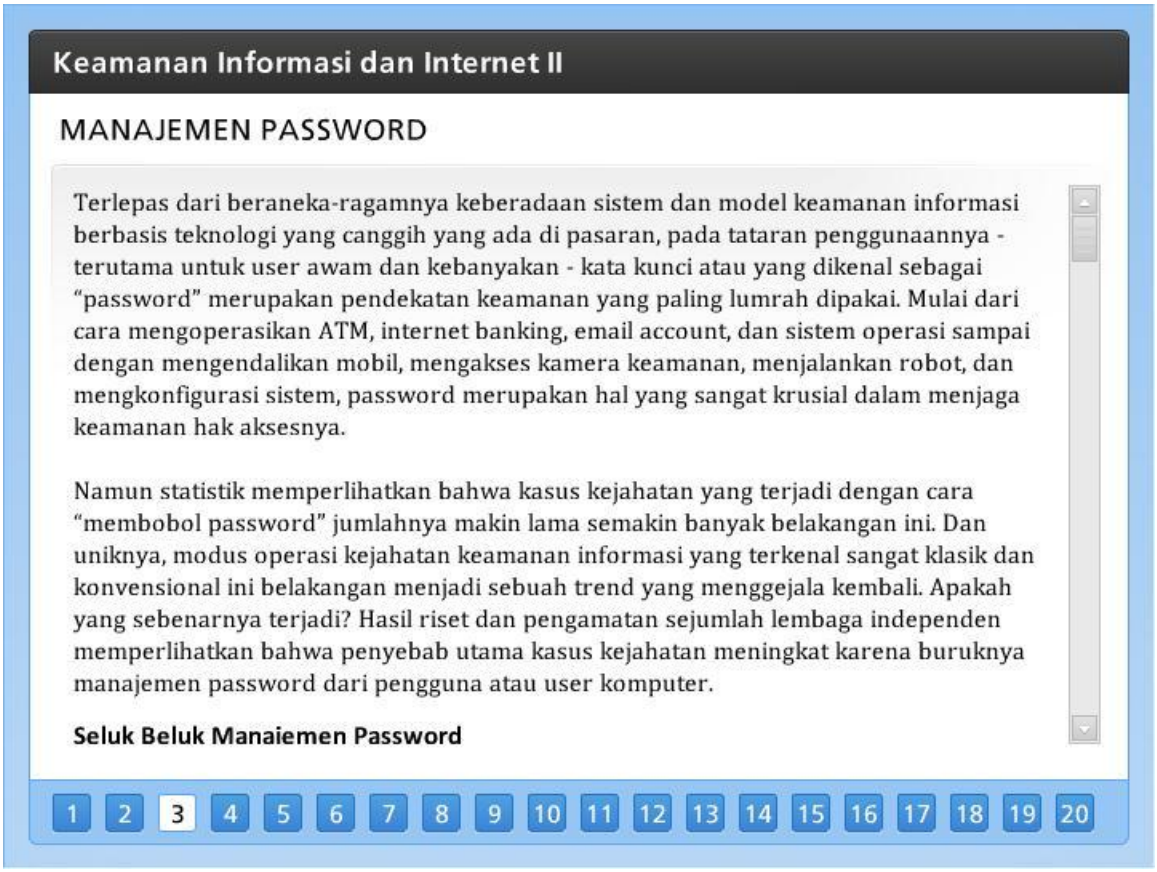
## Nama File

***MKIDI-6A-ManajemenPassword.pdf***

## Referensi Pembelajaran

***6-A***

# MANAJEMEN PASSWORD




Terlepas dari beraneka-ragamnya keberadaan sistem dan model keamanan informasi berbasis teknologi yang canggih yang ada di pasaran, pada tataran penggunaannya - terutama untuk user awam dan kebanyakan - kata kunci atau yang dikenal sebagai "password" merupakan pendekatan keamanan yang paling lumrah dipakai. Mulai dari cara mengoperasikan ATM, internet banking, email account, dan sistem operasi sampai dengan mengendalikan mobil, mengakses kamera keamanan, menjalankan robot, dan mengkonfigurasi sistem, password merupakan hal yang sangat krusial dalam menjaga keamanan hak aksesnya.

Namun statistik memperlihatkan bahwa kasus kejahatan yang terjadi dengan cara "membobol password" jumlahnya makin lama semakin banyak belakangan ini. Dan uniknya, modus operasi kejahatan keamanan informasi yang terkenal sangat klasik dan konvensional ini belakangan menjadi sebuah trend yang menggejala kembali. Apakah yang sebenarnya terjadi? Hasil riset dan pengamatan sejumlah lembaga independen memperlihatkan bahwa penyebab utama kasus kejahatan meningkat karena buruknya manajemen password dari pengguna atau user komputer.

## *Seluk Beluk Manajemen Password*

Manajemen password merupakan suatu tata cara mengelola kata kunci oleh pengguna agar fungsinya sebagai gerbang keamanan informasi dapat secara efektif berperan. Dalam mengelola password ini ada sejumlah hal yang perlu untuk diperhatikan sungguh-sungguh. Berikut adalah beberapa hal penting yang patut untuk dimengerti dan dipertimbangkan sungguh-sungguh oleh semua pengguna password.

### Memilih Password yang Baik

Kriteria password yang baik sebenarnya cukup sederhana, hanya dibatasi oleh dua syarat, yaitu: mudah diingat oleh pemiliknya, dan pada saat yang sama sulit ditebak oleh orang lain atau mereka yang tidak berhak mengetahuinya. Dalam prakteknya, persyaratan tersebut merupakan sesuatu yang susah-susah mudah untuk diterapkan. Kebanyakan password yang mudah diingat oleh pemiliknya cenderung mudah ditebak oleh orang lain. Sementara sebuah password yang dinilai aman karena sulit diterka oleh mereka yang tidak berhak, cenderung sulit diingat oleh yang memilikinya. Oleh karena itulah maka diperlukan suatu teknik khusus untuk memilih password agar di satu pihak aman karena terdiri dari susunan karakter yang sulit ditebak, namun di sisi lain mudah bagi sang pemilik untuk mengingatnya.

### Kriteria Password Ideal

Password yang baik disarankan memiliki sejumlah karakteristik sebagai berikut:

- Terdiri dari minimum 8 karakter - dimana pada prinsipnya adalah makin banyak karakternya semakin baik, direkomendasikan password yang relatif aman jika terdiri dari 15 karakter;
- Pergunakan campuran secara random dari berbagai jenis karakter, yaitu: huruf besar, huruf kecil, angka, dan simbol;
- Hindari password yang terdiri dari kata yang dapat ditemukan dalam kamus bahasa;
- Pilih password yang dengan cara tertentu dapat mudah mengingatnya; dan
- Jangan pergunakan password yang sama untuk sistem berbeda.

Dalam menentukan password tersebut, ada sejumlah hal yang sebaiknya dihindari karena karakteristik password berikut ini telah banyak “diketahui” variasinya oleh para kriminal, yaitu:

- Jangan menambahkan angka atau simbol setelah atau sebelum kata-kata yang biasa dikenal, seperti: pancasila45, nusantara21, 17agustus45, dan lain-lain;
- Jangan menggunakan pengulangan dari kata-kata, seperti: rahasiarahasia, racunracun, ayoayoayo, dan lain-lain;
- Jangan hanya membalikkan karakter dari sebuah kata yang lazim, seperti: gnudih, adamra, kumayn, dan lain-lain;
- Jangan merupakan sebuah kata yang dihilangkan huruf vokalnya, seperti: ndns (dari kata 'indonesia'), pncsl (dari kata 'pancasila'), pnsrn (dari kata 'penasaran'), dan lain-lain;
- Jangan menggunakan susunan karakter yang merupakan urutan penekanan pada tombol-tombok keyboard, seperti: qwerty, asdfghjk, mnbvcxz, dan lain-lain; dan
- Jangan hanya sekedar menggantikan karakter huruf dengan angka seperti halnya nomor cantik pelat mobil tanpa melakukan sejumlah improvisasi, seperti: s3l4m4t, g3dungt1ngg1, 5ul4we5i, dan lain-lain.

## *Teknik Membuat Password*

Berdasarkan prinsip-prinsip yang telah dipaprkan sebelumnya, berikut adalah sejumlah trik dalam mendesain atau menentukan password yang baik. Ada sejumlah pendekatan yang dipergunakan, yang pada intinya bertumpu pada bagaimana cara mengingat sebuah password yang aman.

Trik #1: Berbasis Kata

Katakanlah Donny seorang pemain basket ingin menentukan sebuah password yang aman dan sekaligus mudah diingat. Hal-hal yang dilakukannya mengikuti langkah-langkah sebagai berikut:

1. Memilih sebuah kata yang sangat kerap didengar olehnya dalam kapasistasnya sebagai pemain basket, misalnya adalah: **JORDAN**.
2. Merubah huruf "O" dengan angka "0" dan merubah huruf "A" dengan angka "4" sehingga menjadi: **J0RD4N**.
3. Merubah setiap huruf konsonan kedua, keempat, keenam, dan seterusnya menjadi huruf kecil, sehingga menjadi: **J0rD4n**.

4. Memberikan sebuah variabel simbol tambahan di antaranya; karena Donny terdiri dari 5 huruf, maka yang bersangkutan menyelipkan suatu variabel simbol pada urutan huruf yang kelima, menjadi: **J0rD%4n**.

Trik #2: Berbasis Kalimat

Ani adalah seorang karyawan perusahaan yang memiliki hobby bernyanyi, untuk itulah maka yang bersangkutan akan menggunakan kegemarannya tersebut sebagai dasar pembuatan password aman yang mudah diingat. Berikut adalah urutan pelaksanaannya:

1. Mencari kalimat pertama sebuah lagu yang disenangi, misalnya adalah: "Terpujilah Wahai Engkau Ibu Bapak Guru, Namamu Akan Selalu Hidup Dalam Sanubariku", dimana kumpulan huruf pertama setiap kata akan menjadi basis password menjadi: **TWEIBGNASHDS**.
2. Ubahlah setiap huruf kedua, keempat, keenam, dan seterusnya menjadi huruf kecil, sehingga menjadi: **TwEiBgNaShDs**.
3. Untuk sisa huruf konsonan, ubahlah menjadi angka, seperti: **Tw3i8gNa5hDs**.
4. Kemudian untuk huruf kecil, ubahlan dengan simbol yang mirip dengannya: **Tw3!8gN@5hDs**.

Kedua trik di atas hanyalah sejumlah contoh pendekatan yang dapat dipergunakan oleh siapa saja yang ingin menentukan atau menyusun password yang mudah diingat dan relatif aman seperti yang disyaratkan dalam paparan terdahulu.

## *Strategi Melindungi Keamanan Password*

Setelah memiliki password yang baik, hal selanjutnya yang perlu diperhatikan adalah bagaiaman menjaga dan melindunginya. Ada sejumlah hal yang perlu dilakukan, misalnya:

- Jangan sekali-kali menyimpan password di dalam piranti elektronik seperti komputer, telepon genggam, personal digital assistant, dsb. kecuali dalam keadaan ter-enkripsi (password yang telah disandikan sehingga menjadi sebuah karakter acak);
- Dilarang memberitahukan password anda kepada siapapun, termasuk "system administrator" dari sistem terkait;

- Hindari tawaran fitur "save password" dalam setiap aplikasi browser atau program lainnya yang memberikan tawaran kemudahan ini;
- Hindari memanfaatkan menu yang bisa membantu melihat password ketika sedang dimasukkan;
- Ketika sedang memasukkan password, pastikan tidak ada orang yang berada di sekitar, pastikan tidak terdapat pula kamera CCTV di belakang pundak; dan
- Jika karena suatu hal harus menuliskan password di kertas sebelum memasukkannya ke dalam sistem, pastikan bahwa setelah digunakan, kertas tersebut dihancurkan sehingga tidak mungkin direkonstruksi lagi.

Ada sebuah hal yang perlu diperhatikan, terutama ketika seseorang telah berhasil masuk ke dalam sistem dengan menggunakan password yang dimaksud:

- Lakukan "log out" setelah sistem selesai dipergunakan atau pada saat yang bersangkutan harus jeda sebentar melakukan sesuatu hal (misalnya: dipanggil bos, pergi ke toilet, menerima telepon, dan lain sebagainya);
- Jangan biarkan seseorang melakukan interupsi di tengah-tengah yang bersangkutan berinteraksi dengan sistem yang ada;
- Ada baiknya "protected automatic screen saver" diaktifkan jika dalam kurun waktu 15-30 detik tidak terdapat interaksi pada keyboard maupun mouse;
- Pastikan dalam arti kata lakukan cek-and-ricek terhadap kondisi komputer dan aplikasi agar benar-benar telah berada pada level aman sebelum meninggalkan perimeter; dan
- Biasakan memeriksa meja tempat mengoperasikan komputer untuk memastikan tidak ada bekas-bekas maupun torehan yang dapat mengarah atau menjadi petunjuk bagi aktivitas pembobolan password oleh mereka yang tidak berhak.

### *Kiat Memelihara Password*

Walaupun terlihat aman, adalah sangat bijaksana untuk mengganti password secara berkala, misalnya sebulan sekali atau seminggu sekali tergantung kebutuhan dan konteksnya. Password yang kerap diganti akan menyulitkan seorang kriminal untuk membobolnya. Dalam prakteknya, ada pula individu yang kerap mengganti passwordnya setiap kali kembali dari perjalanan dinas ke luar kota dan/atau ke luar negeri, hanya untuk memastikan bahwa tidak terdapat hal-hal mengandung resiko

yang dibawanya atau diperolehnya selama yang bersangkutan bepergian. Hal yang perlu diperhatikan pula adalah hindari menggunakan password yang sama untuk sistem yang berbeda, karena disamping akan meningkatkan resiko, juga akan mempermudah kriminal dalam menjalankan aksinya. Intinya adalah bahwa setiap kali seseorang merasa bahwa password yang dimilikinya sudah terlampau lama dipergunakan, dan/atau yang bersangkutan merasa sudah banyak orang di sekelilingnya yang terlibat dengannya dengan kemungkinan ada satu atau dua di antara mereka yang tertarik untuk mengetahui password terkait, tidak perlu ragu-ragu untuk segera mengganti password tersebut. Perhatian khusus perlu ditujukan bagi mereka yang aktif berwacana atau berinteraksi di media jejaring sosial seperti Facebook, Friendster, MySpace, dan Twitter - pastikan tidak ada kata atau kalimat yang secara langsung maupun tidak langsung dapat menjadi petunjuk bagi kriminal dalam melakukan kegiatannya. Ingat, cara klasik yang kerap dipergunakan oleh para pembobol password adalah:

- Menebak-nebak password dengan menggunakan analisa mengenai profil dan/atau karakteirstik pemiliknya;
- Menggunakan “brute force attack” alias mencoba segala bentuk kemungkinan kombinasi karakter yang bisa dipergunakan dalam password;
- Menggunakan referensi kata-kata pada kamus sebagai bahan dasar pembobolannya;
- Melakukan teknik “social engineering” kepada calon korban pemilik password;
- Melakukan pencurian terhadap aset-aset yang mengarah pada informasi penyimpanan password; dan lain sebagainya.

Perlu diperhatikan, bahwa teknik-teknik di atas saat ini dilakukan secara otomatis - alias menggunakan teknologi, tidak seperti dahulu yang bersifat manual, sehingga tidak diperlukan waktu lama untuk melaksanakannya (walaupun lama sekalipun tidak akan berpengaruh karena yang mengerjakannya adalah mesin komputer). Statistik memperlihatkan bahwa dari hari ke hari, waktu untuk mengeksploitasi keamanan komputer semakin bertambah singkat.