

STUDI TINGKAT KEAMANAN PASSWORD PADA DATA, EMAIL, DAN APLIKASI

Disusun sebagai:

Tugas Akhir Mata Kuliah Sistem Keamanan Informasi (EC5010)

Oleh:

Kurniawan

13203003



PROGRAM STUDI TEKNIK ELEKTRO
SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA
INSTITUT TEKNOLOGI BANDUNG

2007

ABSTRAKSI

Saat ini, istilah *password* sudah sangat meluas dan mendunia. Di jaman yang serba digital ini, *password* sangatlah penting karena *password* masih merupakan kunci utama untuk kebanyakan sistem atau aplikasi yang berhubungan dengan komputer. Selain itu, *password* dibutuhkan karena ada sesuatu yang sifatnya *confidential*.

Password digunakan sebagai salah satu otentikasi yang diketahui oleh pemakai. Untuk itu, biasanya sebelum kita masuk atau ingin membuka sesuatu yang bersifat pribadi, alangkah baiknya jika ada otentikasi dahulu. Hal-hal yang biasanya menggunakan *password* adalah email, *messenger*, *operating system*, *database*, dokumen, USB, dan hal-hal lain yang memiliki informasi bernilai tinggi.

Oleh karena itu, untuk mendapatkan informasi yang bernilai tersebut banyak orang melakukan berbagai macam cara untuk menembus *password*, hal ini sering dinamakan *hacking*. Semakin kuat sistem keamanan informasi yang digunakan, semakin canggih pula teknik *hacking* yang digunakan. Salah satunya adalah dengan cara *Brute Force Attack*. Dengan cara ini, dapat diestimasi berapa lama waktu yang dibutuhkan untuk mendapatkan *password* yang diinginkan. Semakin panjang dan bervariasi *password* yang digunakan, semakin lama waktu yang dibutuhkan untuk memperolehnya.

Untuk menghindari hal tersebut terjadi, para pengguna *password* seharusnya mengerti kebijakan *password* (*policy*) dan mengetahui *password* seperti apa yang dapat dikatakan baik dan kuat; karena *password* digunakan untuk mengamankan suatu informasi.

Dari penelitian ini nantinya akan dapat dilihat data-data mengenai seberapa jauh masyarakat mengetahui bagaimana memilih *password* yang baik, seberapa kompleks *password* yang digunakan, dan seberapa *secure* mereka melakukan pengamanan terhadap informasi-informasi tersebut.

DAFTAR ISI

ABSTRAKSI	ii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Tujuan	2
1.3 Batasan Masalah	2
BAB II PEMBAHASAN	3
2.1 Masalah Keamanan Informasi	3
2.2 Prinsip Pengamanan Sistem Informasi	6
2.3 Password / Kata Sandi	7
2.3.1 Pengertian Password	7
2.3.2 Perkembangan Password	7
2.3.3 Proteksi Password	10
2.4 Password Policy / Kebijakan Pengamanan	10
2.4.1 Panjang Pengamanan	11
2.4.2 Formasi Pengamanan	11
2.4.3 Durasi Pengamanan	12
2.4.4 Pengamanan yang ‘Sehat’	12
2.4.5 Sanksi	12
2.4.6 Pertimbangan Pengamanan	13
2.5 Kesalahan Utama Para Pengguna Password	13
2.6 Penggunaan Password yang Baik	15
2.7 Aplikasi Lain Ber-Password	16
BAB III PENELITIAN	17
3.1 Hasil Kuisisioner	17
3.2 Analisis	22
BAB IV KESIMPULAN	26
4.1 Kesimpulan	26
4.2 Saran	26
DAFTAR PUSTAKA	27

BAB I

PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi informasi yang begitu cepat telah mempengaruhi segala aspek kehidupan manusia, dengan suatu kebutuhan informasi yang tidak bisa lepas dari kehidupan manusia. Ada pihak yang memberi informasi dan ada pula pihak yang menerima informasi. Biasanya proses pengiriman atau pertukaran informasi tersebut saat ini sudah dalam bentuk digital. Oleh karena itu, internet dan aplikasi-aplikasi perangkat lunak sering berperan penting sebagai media penyampaian dan penyimpanan informasi tersebut.

Namun, dengan berkembangnya kecanggihan pengelolaan informasi melalui internet dan aplikasi-aplikasi perangkat lunak, semakin berkembang pula kejahatan sistem informasi. Dengan berbagai macam metode banyak yang mencoba untuk mengakses informasi yang bukan haknya (*hacking*). Semakin bernilai informasi tersebut, semakin banyak pula oknum-oknum yang mencoba untuk mendapatkannya. Oleh karena itu, hal-hal seperti ini harus ditanggulangi dengan meningkatkan pengamanan sistem informasi.

Salah satu metode pengamanan sistem informasi yang umum diketahui oleh banyak orang adalah **password**. Tanpa disadari *password* mempunyai peranan penting dalam mengamankan informasi-informasi yang sifatnya pribadi (*confidential*). Pada beberapa aplikasi yang berhubungan dengan piranti lunak, seperti HP, kartu ATM, dll., ada juga sistem pengamanannya yang fungsinya mirip dengan *password*; biasa dikenal sebagai Kode PIN. Walaupun hanya terdiri dari angka, namun kegunaannya sama seperti *password*, yaitu untuk mengamankan informasi. Informasi yang disimpan tersebut biasanya sudah berbentuk digital.

Tetapi banyak dari para pengguna *password* yang membuat *password* secara sembarangan tanpa mengetahui kebijakan pengamanan (*password policy*) dan bagaimana membuat *password* yang kuat (*strong password*). Mereka tidak sadar dengan bahayanya para ‘penyerang’ (*attacker*) yang dapat mencuri atau mengacak-acak informasi tersebut.

Jadi, dapat dikatakan bahwa *password* sudah menjadi bagian dalam kehidupan kita. Diharapkan untuk ke depannya, pengamanan informasi yang sifatnya pribadi tersebut dapat lebih terjaga dan memiliki otentikasi yang kuat dan tahan terhadap gangguan. Masyarakat pun dapat lebih peduli terhadap perkembangan sistem pengamanan informasi dan akan terus memperbaikinya.

1.2. Tujuan

Tujuan dari pembuatan makalah ini adalah untuk mengetahui sampai mana tingkat kesulitan *password* yang digunakan, seberapa jauh orang mengerti penggunaan *password* yang baik, seberapa penting informasi yang ingin diamankan, dan hal-hal apa saja yang diproteksi dengan menggunakan *password*.

1.3. Batasan Masalah

Batasan-batasan masalah yang saya pakai ketika melakukan penelitian ini adalah:

1. Password yang diteliti hanya sebatas data, email, dan aplikasi-aplikasi yang piranti lunaknya mempunyai fitur proteksi.
2. Pembahasan akan dilakukan secara umum, dimulai dari permasalahan dasar keamanan sampai dengan bagaimana *password* yang baik untuk melakukan perlindungan terhadap informasi.
3. Informasi yang dimaksud dalam makalah ini adalah sesuatu yang sifatnya pribadi atau rahasia.
4. Penyebaran angket hanya dilakukan di kota Bandung, yang terdiri dari berbagai macam profesi (keterangan lebih lengkap pada bagian penelitian).

BAB II

PEMBAHASAN

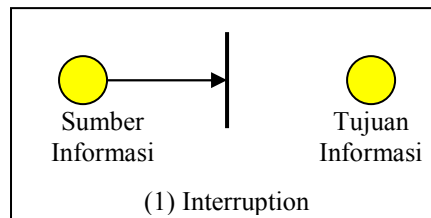
2.1. Masalah Keamanan Informasi

Target pengamanan adalah menghindari, mencegah, dan mengatasi ancaman-ancaman terhadap sistem. Kebutuhan akan pengamanan komputer dapat dikategorikan dalam tiga aspek, yaitu:

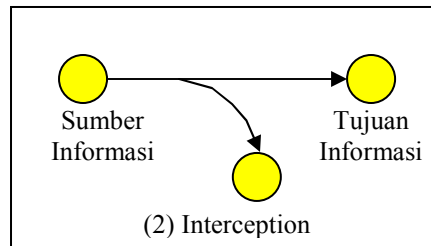
- 1) Kerahasiaan (*Confidentiality*), dimana informasi pada sistem komputer itu terjamin kerahasiaannya, hanya dapat diakses oleh pihak-pihak yang diotorisasi, keutuhan serta konsistensi data pada sistem tersebut tetap terjaga.
- 2) Integritas (*Integrity*), dimana sumber daya sistem terjamin hanya dapat dimodifikasi oleh pihak-pihak yang diotorisasi.
- 3) Ketersediaan (*Availability*), adalah sumber daya sistem komputer terjamin akan tersedia bagi pihak-pihak yang diotorisasi pada saat diperlukan.

Banyak cara yang dapat menimbulkan masalah terhadap suatu sistem informasi. Fungsi sistem komputer dapat digunakan sebagai dasar untuk menentukan model tipe ancaman dari suatu sistem komputer sebagai penyedia informasi, ancaman terhadap sistem komputer dikategorikan menjadi empat, yaitu:

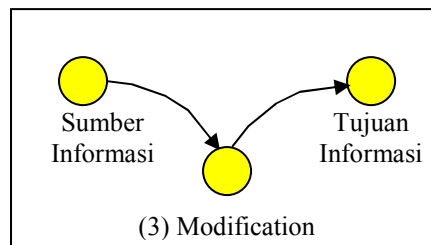
- 1) *Interruption*, merupakan suatu ancaman terhadap *availability*, informasi atau data yang ada dalam sistem komputer dirusak, dihapus, sehingga jika dibutuhkan maka sudah tidak ada lagi.



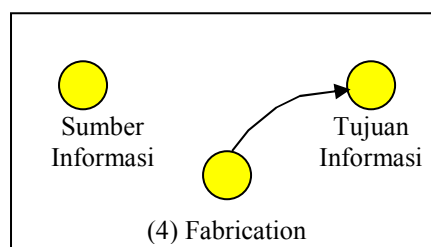
- 2) *Interception*, merupakan ancaman terhadap kerahasiaan (*secrecy*). Informasi yang ada di dalam sistem disadap oleh orang yang tidak berhak.



- 3) *Modification*, merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalu-lintas informasi yang sedang dikirim lalu mengubahnya sesuai keinginan orang tersebut.



- 4) *Fabrication*, merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil meniru atau memalsukan suatu informasi sehingga orang yang menerima informasi tersebut menyangka informasi tersebut berasal dari orang yang dikehendaki oleh si penerima informasi tersebut.



Banyaknya metode atau cara untuk mendapatkan suatu informasi menimbulkan adanya klasifikasi dalam dunia informasi. Para penjahat informasi ini dapat digolongkan menjadi yang sangat berbahaya sampai ke yang hanya mengesalkan (*annoying*). Menurut *David Icove*, berdasarkan lubang keamanan, keamanan dapat diklasifikasikan menjadi empat, yaitu:

- 1) Keamanan yang bersifat fisik (*physical security*); termasuk akses orang ke gedung, peralatan, dan media yang digunakan. Beberapa bekas penjahat komputer (*crackers*) mengatakan bahwa mereka sering pergi ke tempat sampah untuk mencari berkas-berkas yang mungkin memiliki informasi tentang keamanan. Misalnya pernah ditemukan coretan password atau manual yang dibuang, tanpa dihancurkan. *Wiretapping* atau hal-hal yang berhubungan dengan akses ke kabel atau komputer yang digunakan juga dapat dimasukkan ke dalam kelas ini.

Denial of service, dimana servis tidak dapat diterima oleh pemakai. *Denial of service* dapat dilakukan misalnya dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan yang dapat berisi apa saja karena yang diutamakan adalah banyaknya pesan.

Beberapa waktu yang lalu ada lubang keamanan dari implementasi protokol TCP/IP yang dikenal dengan istilah *Syn Flood Attack*, dimana sistem yang dituju kemudian dibanjiri oleh permintaan sehingga dia menjadi terlalu sibuk, yang kemudian bahkan berakibat terhentinya sistem.

- 2) Keamanan yang berhubungan dengan orang, termasuk identifikasi dan profil resiko dari orang yang mempunyai akses. Seringkali kelemahan keamanan sistem informasi bergantung kepada manusia (pemakai atau *user*). Ada sebuah teknik yang dikenal dengan istilah *social engineering* yang sering digunakan oleh para kriminal untuk berpura-pura menjadi orang yang berhak mengakses informasi. Kriminal ini berpura-pura sebagai pemakai yang lupa akan password-nya dan minta agar diganti dengan kata lain.
- 3) Keamanan dari data dan media serta teknik komunikasi. Yang termasuk di dalam kelas ini adalah kelemahan dalam software yang digunakan untuk mengelola data. Seorang kriminal dapat memasang *virus* atau *trojan horse* sehingga dapat mengumpulkan informasi (seperti password) yang seharusnya tidak berhak diakses.
- 4) Keamanan dalam operasi, termasuk prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga prosedur setelah serangan (*post attack recovery*).

2.2. Prinsip Pengamanan Sistem Informasi

Dibawah ini akan dijelaskan beberapa prinsip pengamanan yang biasanya sering digunakan untuk mengamankan hal-hal yang bersifat *confidential*, diantaranya:

3) Otentikasi Pemakai

Identifikasi pemakai saat login merupakan dasar asumsi sistem proteksi sehingga metode otentikasi didasarkan pada tiga cara, yaitu: sesuatu yang diketahui pemakai, yang dimiliki pemakai, dan mengenai pemakai.

4) Password

Password atau yang biasa sering disebut sebagai kata sandi merupakan salah satu otentikasi yang diketahui pemakai, dimana pemakai memilih suatu kata-kode, mengingatnya, dan mengetikkannya saat akan mengakses sistem komputer. Teknik pengamanan dengan password mempunyai beberapa kelemahan, terutama karena pemakai sering memilih password yang mudah diingatnya.

5) Identifikasi Fisik

Pendekatan identifikasi fisik ini dilakukan dengan memeriksa apa yang dimiliki pemakai.

a) Kartu Berpita Magnetik

Kartu pengenalan dengan selarik pita magnetik umumnya dikombinasikan dengan password. User akan dapat login ke komputer bila memenuhi syarat, yaitu mempunyai kartu dan mengetahui password khusus untuk kartu tersebut.

b) Sidik Fisik

Identifikasi fisik sidik jari atau sidik suara, analisis panjang jari, dsb.

c) Analisis Tanda Tangan

Dengan menggunakan pena khusus, pemakai diharuskan untuk membuat tanda tangan. Dalam hal ini yang dibandingkan adalah arah gerakan dan tekanan pena saat *user* membuat tanda tangan.

6) Pembatasan

Pembatasan dapat dilakukan untuk memperkecil peluang penembusan oleh pemakai yang tidak diotorisasi. Untuk pembatasan login, misalnya dengan login pada terminal dan waktu tertentu, *call back*, login dapat dilakukan oleh siapapun tetapi setelah sukses maka sistem akan segera memutuskan koneksi dan memanggil nomor telepon yang telah disepakati.

Cara lain yang dapat dilakukan adalah dengan membatasi jumlah usaha login sampai dengan tiga kali berturut-turut selama kurang dari 1 jam; kemudian jika masih salah akan segera terkunci. Hal-hal seperti ini biasanya disebut dikenal dengan *Technical Control*.

2.3. Password / Kata Sandi

2.3.1. Pengertian Password

Adalah suatu bentuk dari data otentikasi rahasia yang digunakan untuk mengontrol akses ke dalam suatu sumber informasi. Password akan dirahasiakan dari mereka yang tidak diijinkan untuk mengakses, dan mereka yang ingin mengetahui akses tersebut akan diuji apakah layak atau tidak untuk memperolehnya. [10]

Walaupun demikian, *password* bukan berarti suatu bentuk kata-kata; tentu saja *password* yang bukan suatu kata yang mempunyai arti akan lebih sulit untuk ditebak. Sebagai tambahan, *password* sering digunakan untuk menggambarkan sesuatu yang lebih tepat disebut *pass phrase*. *Password* kadang-kadang digunakan juga dalam suatu bentuk yang hanya berisi angka (*numeric*); salah satu contohnya adalah *Personal Identification Number* (PIN). *Password* umumnya cukup pendek sehingga mudah untuk diingat.

2.3.2. Perkembangan Password

Perkembangan otentikasi *password* ini dapat dilihat dengan contoh-contoh dari kelemahan, sistem yang mudah dibahayakan, yang kebanyakan masih

digunakan sampai saat ini. Dibawah ini akan diperlihatkan beberapa kategori utama dari sistem otentikasi *password*, bersamaan dengan beberapa contoh implementasi yang mengilustrasikan kekurangan masing-masing:

1) Otentikasi Lemah (Weak Authentication)

Secara umum, sistem dengan otentikasi yang lemah dicirikan dengan protokol yang memiliki kebocoran *password* langsung diatas jaringan atau membocorkan informasi yang cukup untuk diketahui ‘penyerang’ sehingga *password* dapat dianalisis dan ditebak.

- **Cleartext Passwords**

Metode otentikasi yang paling tidak aman adalah menyimpan *password* pada database di suatu tempat di server. Selama otentikasi, *user* mengirim *password* langsung ke server dan server akan membandingkan dengan *password* yang ada di server. Masalah keamanan disini sangat jelas terlihat.

- **Hashed Passwords**

Password pengguna dapat dijalankan melalui suatu fungsi *one-way hash*, dimana dapat mengubahnya ke dalam urutan byte secara acak. Sebagai fungsi ini akan lebih susah dikembalikan: lebih mudah mengubah *password* menjadi *hash* daripada *hash* menjadi *password*. Otentikasi terdiri dari menjalankan fungsi *hash* ketika *password* diketik dan membandingkannya dengan *password* yang telah disimpan. Sistem seperti ini masih digunakan sampai sekarang pada sistem utama UNIX.

- **Challenge-Response**

Untuk menghindari kemunculan *password* secara langsung pada jaringan yang tidak terpercaya, dibuatlah sistem *challenge-response*. Server akan mengirim beberapa *challenge*, yang mencirikan beberapa string pendek secara acak. Sayangnya, sistem *challenge-response* sudah tidak mampu lagi mengimbangi aplikasi jaringan modern.

2) Otentikasi Kuat (Strong Authentication)

Walaupun enkripsi yang baik sudah ada sejak beberapa dekade yang lalu, pengembangan dari otentikasi protokol langsung yang kuat baru dimulai tahun 1990 dengan publikasi dari “EKE family of algorithms”.

- **EKE**

Merupakan keluarga protokol yang terdiri dari simetrik dan *public-key cryptosystems* untuk melakukan otentikasi *password*. Untuk pertama kalinya, protokol dapat menghindari *dictionary attacks* dan memungkinkan pemberitahuan secara rahasia tanpa melibatkan pihak ketiga atau *key-management*.

- **DH-EKE, SPEKE**

EKE yang paling terkenal dan aman, sama dengan protokol pengganti kunci *Diffie-Hellman*. Sebagai contoh: DH-EKE, adalah EKE yang di-implementasikan menggunakan *Diffie-Hellman*. Perbedaan yang paling signifikan yaitu pada pertukaran pesan pada DH yang sekarang dienkripsi dengan *shared password*.

Demikian juga dengan SPEKE, yang juga berbasis *Diffie-Hellman*. Tetapi *password* sekarang digunakan untuk mempengaruhi pemilihan dari parameter generator di dalam fungsi *session-key generation*.

- **A-EKE**

Merupakan modifikasi dari EKE, biasa disebut *Augmented-EKE*; di-mana server dapat menyimpan beberapa yang tidak *plaintext-equivalent* ke *password* pengguna. Protokol ini adalah satu-satunya protokol yang sampai saat ini tahan terhadap *dictionary attacks* dan tidak mempunyai database *password* yang *plaintext-equivalent*. Sayangnya, A-EKE mengorbankan kerahasiaan dalam usahanya untuk menghindari *plaintext-equivalence*.

3) Gangguan Otentikasi (Inconvenient Authentication)

Ketidakhadiran otentikasi yang kuat, teknologi otentikasi *password* yang mudah, membuat para pendesain sistem tahun 1980an mencoba

teknik lain untuk menjamin keamanan *password*. Kebanyakan dari sistem yang ada, tidak sepenuhnya *password-based* dan sering membutuhkan sesuatu yang lebih pada bagian pengguna, administrator, atau keduanya untuk meng-operasikan secara halus. Ada tiga metode yang dapat dilakukan, yaitu *one-time passwords*, *Kerberos*, dan *SSH*.

2.3.3. Proteksi Password

Upaya untuk mengamankan proteksi password tersebut antara lain:

a) *Salting*

String password yang diberikan pemakai ditambah suatu string pendek sehingga mencapai panjang password tertentu.

b) *One-time Passwords*

Password yang dimiliki oleh pemakai diganti secara teratur, dimana seorang pemakai memiliki daftar password sendiri sehingga untuk login ia selalu menggunakan password berikutnya. Dengan cara ini pemakai akan menjadi lebih direpotkan karena harus menjaga daftar password tersebut tidak sampai tercuri atau hilang.

c) Satu pertanyaan dan jawaban yang panjang

Yang mengharuskan pemakai memberikan satu pertanyaan yang panjang beserta jawabannya, yang mana pertanyaan dan jawabannya dapat dipilih oleh pemakai, yang mudah untuk diingat sehingga ia tidak perlu menuliskannya pada kertas.

d) Tanggapan-tanggapan

Pemakai diberikan kebebasan untuk menggunakan satu atau beberapa algoritma sekaligus.

2.4. Password Policy / Kebijakan Pengamanan

Kebijakan pengamanan atau yang biasa dikenal dengan **password policy** adalah sekelompok peraturan yang dibuat untuk meningkatkan keamanan informasi dengan mendorong pengguna untuk memakai *password* yang kuat dan

menggunakannya dengan tepat. Kebijakan pengamanan sering menjadi bagian dari regulasi resmi suatu organisasi. Kebijakan pengamanan dapat dilaporkan atau ditugaskan dengan melakukan berbagai jenis pengujian ke dalam *operating system*.

Kebijaksanaan pengamanan biasanya sederhana dan umum digunakan, dimana setiap pengguna dalam sistem dapat mengerti dan mengikutinya. Isinya berupa tingkatan keamanan yang dapat melindungi data-data penting yang disimpan oleh setiap *user*.

Beberapa hal yang dipertimbangkan dalam kebijaksanaan pengamanan adalah siapa sajakah yang memiliki akses ke sistem, siapa sajakah yang diizinkan untuk menginstall program ke dalam sistem, siapa memiliki data apa, perbaikan terhadap kerusakan yang mungkin terjadi, dan penggunaan yang wajar dari sistem.

2.4.1 Panjang Pengamanan

Banyak kebijakan yang membutuhkan batas minimal panjang password (*password length*), umumnya 6-8 karakter. Beberapa sistem bahkan telah menentukan panjang maksimum yang dapat digunakan.

2.4.2 Formasi Pengamanan

Beberapa kebijakan menyarankan atau menentukan persyaratan dalam menentukan *password* apa yang dapat digunakan, seperti:

- 1) Penggunaan karakter *uppercase* dan *lowercase* (*case sensitivity*)
- 2) Penyisipan satu atau beberapa digit angka
- 3) Penyisipan karakter-karakter spesial, seperti %, \$, ?, &, dll
- 4) Larangan untuk penggunaan kata-kata yang ada pada kamus
- 5) Larangan untuk penggunaan tanggal-tanggal yang memiliki makna

Sebagai contoh **password formation**, pada bulan Oktober 2005, para pegawai negeri di Inggris disarankan untuk menggunakan *password* dengan

susunan: konsonan, vokal, konsonan, konsonan, vokal, konsonan, angka, angka (contoh: pinray45). Bentuk seperti ini dinamakan “Environ Password” dan *case-insensitive*. [12]

2.4.3 Durasi Pengamanan

Beberapa kebijakan membutuhkan pengguna untuk mengganti *password* secara berkala, misalnya 90 atau 180 hari. Hal ini dikenal dengan istilah **password duration**. Sistem yang mengimplementasikan kebijakan seperti itu terkadang mencegah pengguna dari penggunaan *password* sebelumnya.

Kebijakan seperti ini sering membuat *password* mudah ditebak. Sulitnya untuk memilih *password* yang ‘kuat’ dan mudah untuk diingat karena mereka harus menggantinya secara berkala, membuat mereka sering menggunakan *password* yang ‘lemah’.

Hal ini membuat lebih baik untuk menggunakan *password* yang ‘kuat’ dan dapat digunakan dalam kurun waktu yang lama daripada harus mengubah *password* yang mungkin akan sering menggunakan *password*-nya mudah untuk ditebak.

2.4.4 Pengamanan yang ‘Sehat’

Biasa dikenal dengan istilah **password hygiene**. Kebijakan pengamanan sering termasuk nasehat yang tepat untuk manajemen *password*, seperti:

- Tidak menggunakan *account computer* bersama orang lain
- Tidak menggunakan *password* yang sama untuk otentikasi yang berbeda
- Tidak memberitahukan *password* kepada orang lain
- Tidak menulis *password* disuatu tempat
- Tidak menginformasikan *password* lewat telepon, email, dll
- Jangan lupa untuk melakukan *logout* sebelum meninggalkan komputer

2.4.5 Sanksi

Kebijakan pengamanan dapat termasuk sanksi-sanksi awal dengan peringatan dan kemungkinan untuk kehilangan hak istimewa terhadap akses

yang dipunyai atau penghentian kerja. Dimana kerahasiaan tersebut dibawah perlindungan hukum, kekerasan terhadap kebijakan pengamanan (*hack*) dapat dianggap sebagai penyerangan kriminal. Beberapa memilih untuk mengetahui dengan meminta penjelasan dari pelaku sehingga sistem keamanan dapat diperkuat daripada memberikan sanksi.

2.4.6 Pertimbangan Pengamanan

Tingkat kekuatan *password* yang dibutuhkan tergantung dari berapa banyak kemungkinan ‘penyerangan’ yang terjadi. Biasanya, sistem yang baik dilengkapi dengan pembatasan (3-5 kali coba). Sehingga jika sudah melebihi batas, *login* dapat dinonaktifkan (*frozen*) atau ada jeda waktu (*delay*) untuk pengaktifannya.

Ada juga sistem yang menggunakan versi *specially hashed*, yang berarti siapa saja dapat melakukan validasi. Jika metode ini yang digunakan memungkinkan ‘penyerang’ untuk mencoba berbagai kombinasi *password* dengan cepat. Dengan kata lain, dibutuhkan *password* yang sangat ‘kuat’.

Untuk validasi yang mempunyai tingkatan yang tinggi, seperti *root* atau *system administrator account*, dibutuhkan penggunaan pengamanan (*password*) yang lebih ketat dan tepat. Namun, teori kebijakan pengamanan ini sulit untuk diterapkan ke dalam praktek pemilihan *password* yang sering kita lakukan.

2.5. Kesalahan Utama Para Pengguna Password

Ada lima kesalahan yang biasanya dilakukan orang sehingga mengakibatkan data mereka dapat dicuri orang lain, *login* dapat di-hack, dan sebagainya. Umumnya orang mengunci pintu rumahnya terlebih dahulu sebelum pergi meninggalkan rumah. Namun dalam penggunaan komputer, orang cenderung bertindak ceroboh. Tidak hanya pengguna saja, tetapi termasuk juga administratornya. [8]

Dari kelima kesalahan tersebut, hanya empat yang berkaitan erat dengan penggunaan *password*. Berikut ini adalah empat kesalahan utama yang berhubungan dengan pengamanan *password*:

- 1) Menuliskan password di kertas. Pengguna biasanya menuliskan password di secarik kertas dan kemudian menempelkannya di PC atau di samping monitor. Mereka terlalu malas mengingat password itu sehingga mencatatnya di kertas dan meletakkannya begitu saja sehingga semua orang dapat membacanya. Hal ini didasarkan atas penelitian yang dilakukan oleh lembaga security di US yang menyatakan sekitar 15-20% penggunan disuatu perusahaan melakukan hal ini.
- 2) Pemilihan password yang buruk. Di dalam memilih password, orang cenderung menggunakan nama orang dekat, seperti nama suami atau istri, nama pacar, nama orang-tua, nama binatang kesayangan, atau tulisan disekitar mereka yang gampang ditebak oleh orang lain. Atau bahkan menggunakan tanggal lahir mereka sendiri. Password yang buruk akan dengan gampang di-*crack*, apalagi kalau password itu sama dengan *username*. Jika anda menggunakan password dengan kombinasi abjad, nomor, dan huruf besar-kecil (*case sensitive*), maka akan dibutuhkan waktu yang cukup lama untuk meng-*crack*. Hal itu juga tergantung seberapa panjang password yang digunakan. Saat ini beberapa situs tertentu menggunakan kalimat sebagai password, misalnya situs “hushmail”.
- 3) Meninggalkan komputer yang masih hidup begitu saja. Banyak orang meninggalkan komputer mereka tanpa proteksi apa-apa. Dengan demikian orang lain tinggal datang dan duduk untuk mengakses data. Berbagai sistem operasi sudah memberikan fasilitas seperti *screen saver* yang bisa diaktifkan passwordnya setelah lima menit (tergantung *setting* dari pengguna) atau bisa di-lock begitu kita mau meninggalkan komputer kita.
- 4) Tidak adanya kebijakan keamanan komputer di perusahaan. Bukan hal yang aneh jika banyak perusahaan di Indonesia tidak memilikinya karena mereka masih belum peduli dengan keamanan, terkecuali untuk perusahaan multinasional. Hal itupun karena adanya keharusan dari *headquarter* yang

mengharuskan mereka menerapkan kebijakan itu di perusahaan mereka yang berada di Indonesia. *Security policy* ini mengatur segala hal yang berkaitan dengan keamanan komputer, seperti penerapan password untuk setiap orang (misalnya: panjang *password* minimal 9 karakter dengan kombinasi numerik dan karakter), yang juga disertai dengan sanksi yang akan diberikan jika mereka melanggarnya.

2.6. Penggunaan Password yang Baik

Ada beberapa cara untuk menjaga keamanan komputer, terutama dalam hal pemakaian password. Password merupakan hal vital dalam proses otentikasi. Penggunaan password yang baik dan efektif seharusnya:

- 1) Minimal mempunyai panjang 6-8 karakter, yang dikombinasikan dengan karakter angka, simbol atau menggunakan *sensitive case*.
- 2) Tidak memiliki maksud atau makna. Password yang memiliki makna relatif mudah untuk ditebak. Jadi penggunaan nama anggota keluarga, alamat, tanggal lahir, dan sejenisnya harus dihindari.
- 3) Tidak terdiri dari urutan abjad atau angka, misalnya '67890' atau 'hijklmn'.
- 4) Sebaiknya diberi periode berlaku. Ini berarti harus sering mengganti password.
- 5) Jangan gunakan nama login (*username*) sebagai password dalam bentuk apapun, baik dengan mengganti huruf kapital, dibalik, diulang, dan sebagainya.
- 6) Jangan menggunakan kata-kata yang umum dan terdapat dalam kamus.
- 7) Jangan pernah menuliskan password yang Anda pakai di tempat-tempat yang dapat diakses umum.
- 8) Jangan membuat password yang membuat Anda kesulitan untuk menghafalnya. Buatlah password yang mudah diingat, namun sulit untuk ditebak.
- 9) Jangan pernah memberitahu password Anda kepada orang lain.
- 10) Apabila diperlukan, ada baiknya jika menggunakan software atau utilitas tambahan untuk menambah keamanan komputer Anda.

2.7. Aplikasi Lain Ber-Password

Beberapa contoh aplikasi lain yang juga menggunakan proteksi *password*:

1. USB (Kingston U3)



2. Messenger (Yahoo)



3. Database (Microsoft Access)



BAB III

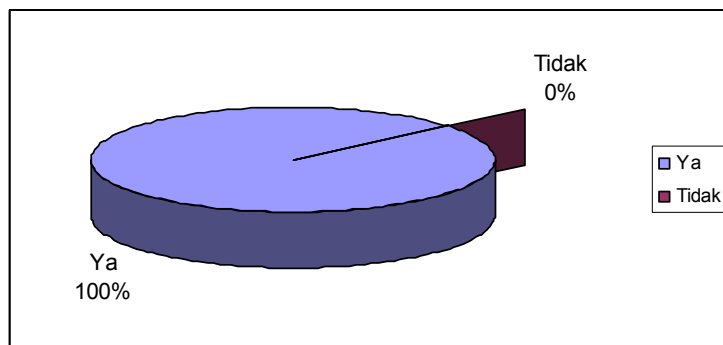
PENELITIAN

3.1. Hasil Kuisioner

Penelitian ini mengambil survei terhadap 150 orang yang terdiri dari 126 Pria dan 24 Wanita. Profesi-profesi mereka yang menjadi sampel dalam penelitian ini adalah Pelajar, Mahasiswa/Mahasiswi, Peneliti, Wirausahawan, Auditor, Programmer, Dosen, dan Karyawan/Karyawati. Dibawah ini akan diperlihatkan prosentase yang diperoleh dari masing-masing pertanyaan yang diajukan:

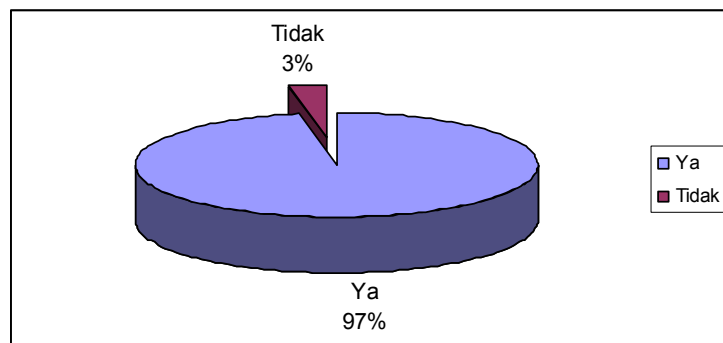
1. Pertanyaan: Apakah Anda tau apa itu *Password*?

Hasil prosentase yang diperoleh:



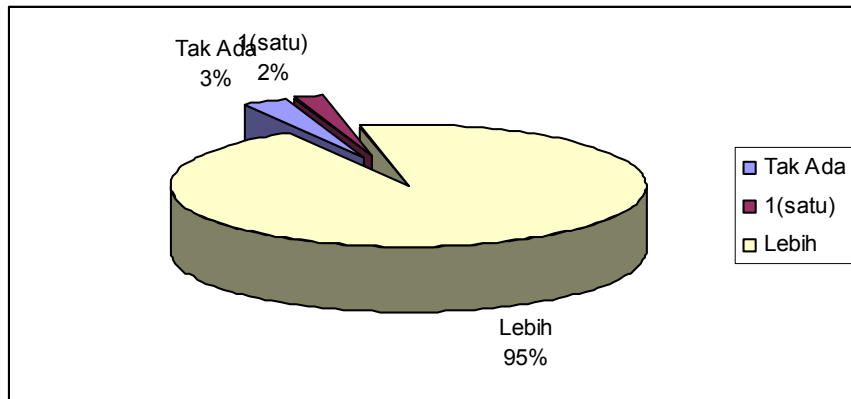
2. Pertanyaan: Apakah Anda pernah menggunakan *Password*?

Hasil prosentase yang diperoleh:



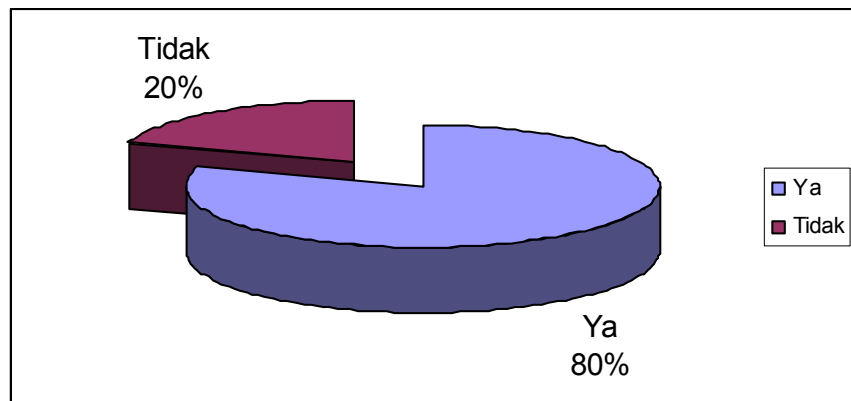
3. Pertanyaan: Berapa banyak *Password* yang Anda punya?

Hasil prosentase yang diperoleh:



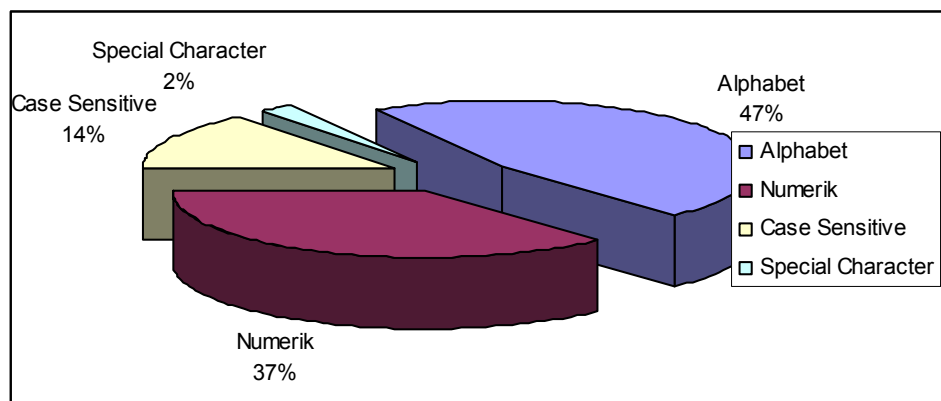
4. Pertanyaan: Apakah Anda mencatat *Password* Anda di suatu tempat?

Hasil prosentase yang diperoleh:



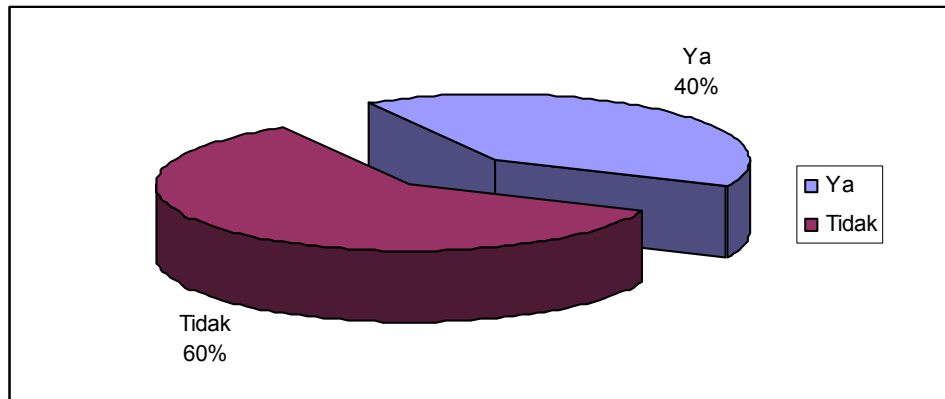
5. Pertanyaan: Karakter apa saja yang digunakan pada *Password* Anda? (*)

Hasil prosentase yang diperoleh:



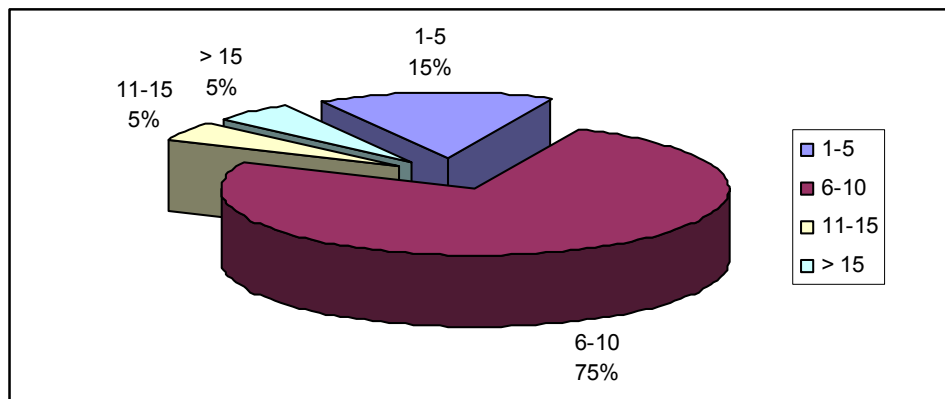
6. Pertanyaan: Apa *Password* yang Anda gunakan merupakan suatu kata bermakna atau merupakan kata dalam kamus?

Hasil prosentase yang diperoleh:



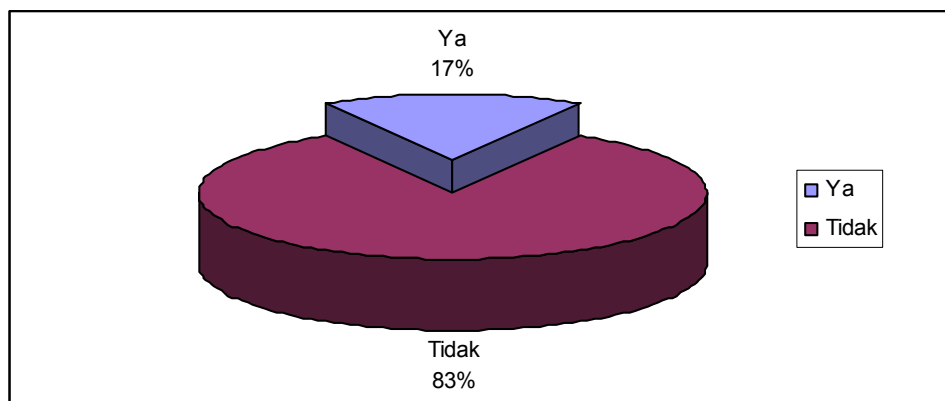
7. Pertanyaan: Berapa panjang *Password* yang digunakan?

Hasil prosentase yang diperoleh:



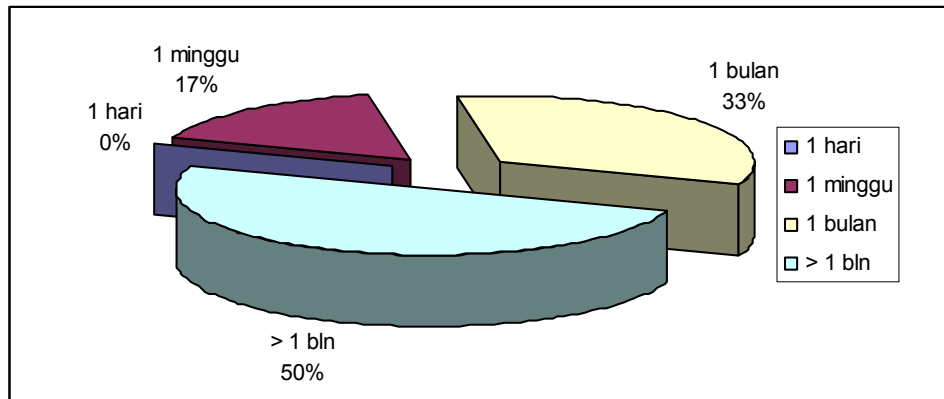
8. Pertanyaan: Seringkah Anda mengganti *Password*?

Hasil prosentase yang diperoleh:



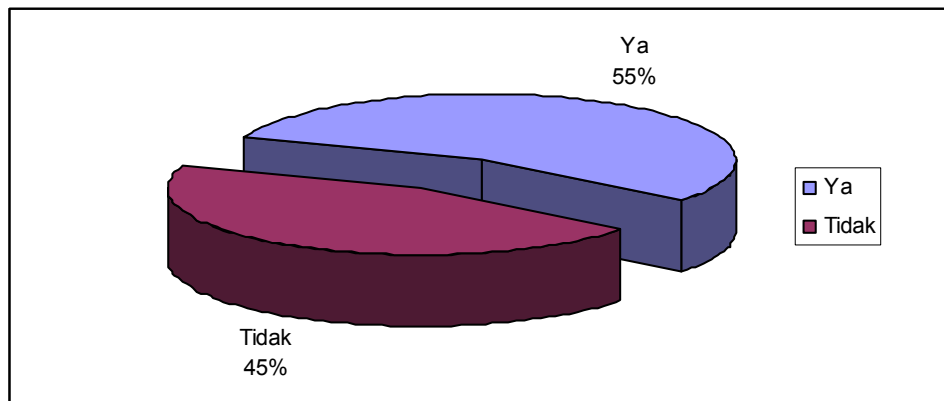
9. Pertanyaan: Jika no.8 Anda menjawab “Ya”, berapa lama kira-kira?

Hasil prosentase yang diperoleh (21 orang):



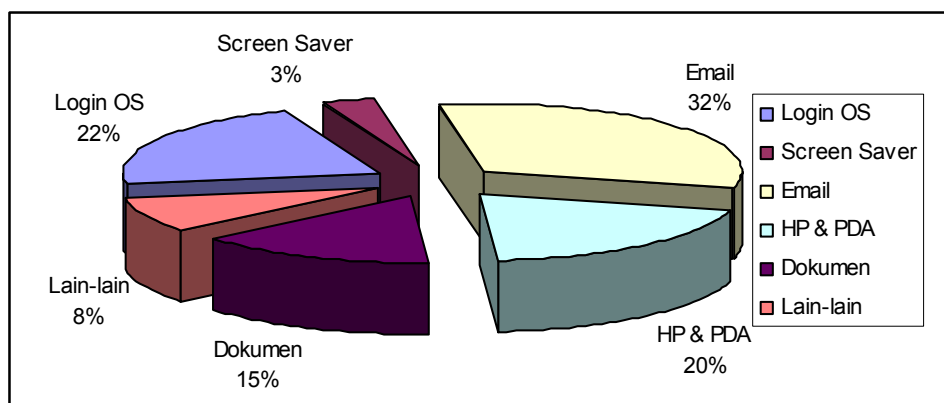
10. Pertanyaan: *Password* yang Anda gunakan apa berhubungan dengan Anda, seperti tanggal lahir, nama orang tua, nama sekolah, dll?

Hasil prosentase yang diperoleh:



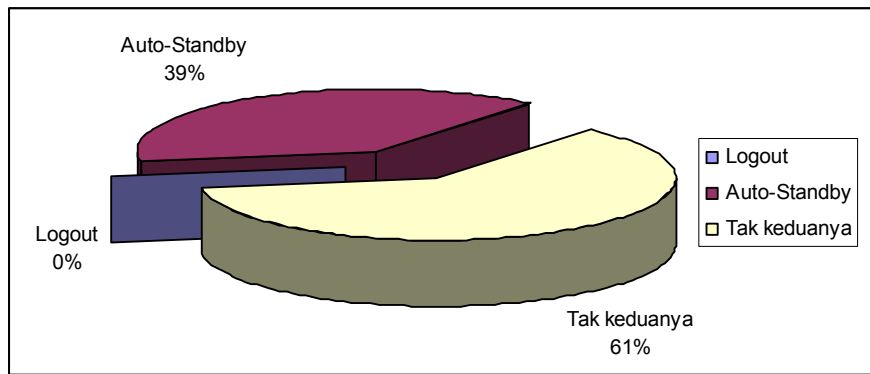
11. Pertanyaan: Apa saja yang Anda *Password*? (*)

Hasil prosentase yang diperoleh:



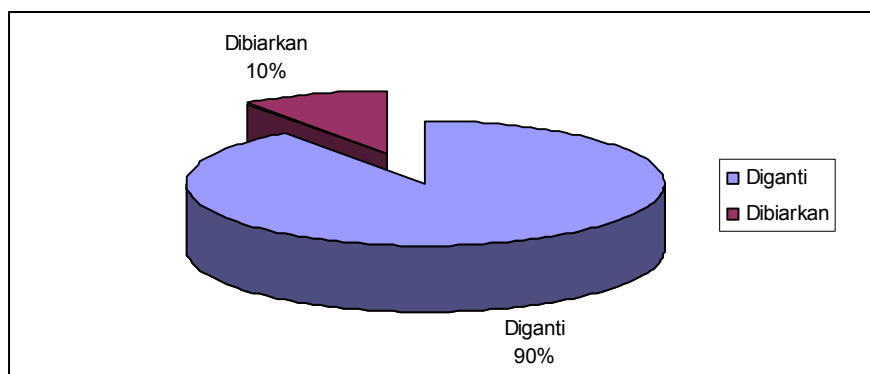
12. Pertanyaan: Jika komputer Anda tinggal menyala, apa yang Anda lakukan?

Hasil prosentase yang diperoleh:



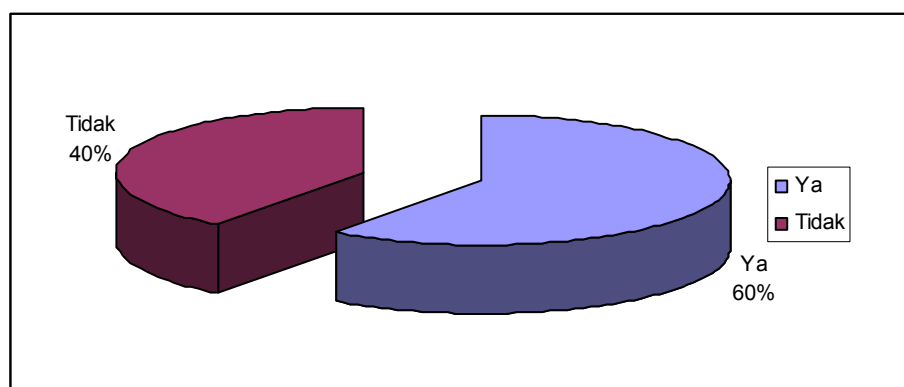
13. Pertanyaan: Jika ada yang mengetahui *Password* Anda, apa yang Anda lakukan?

Hasil prosentase yang diperoleh:



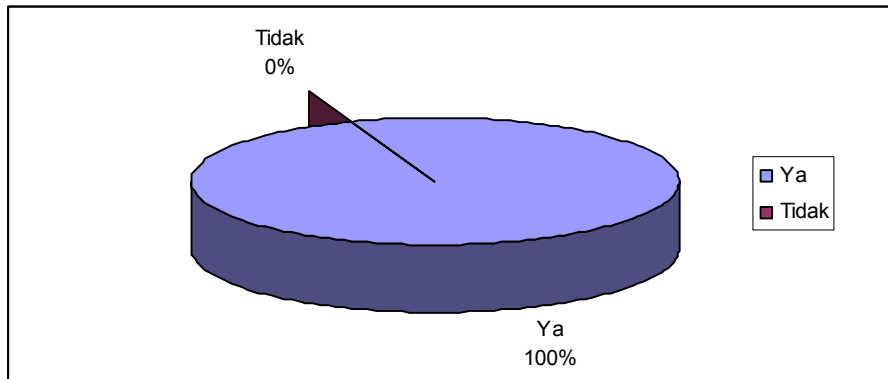
14. Pertanyaan: Pada komputer pribadi, apa Anda melakukan *logout* setiap kali Anda selesai mengakses sesuatu yang memerlukan otentikasi?

Hasil prosentase yang diperoleh:



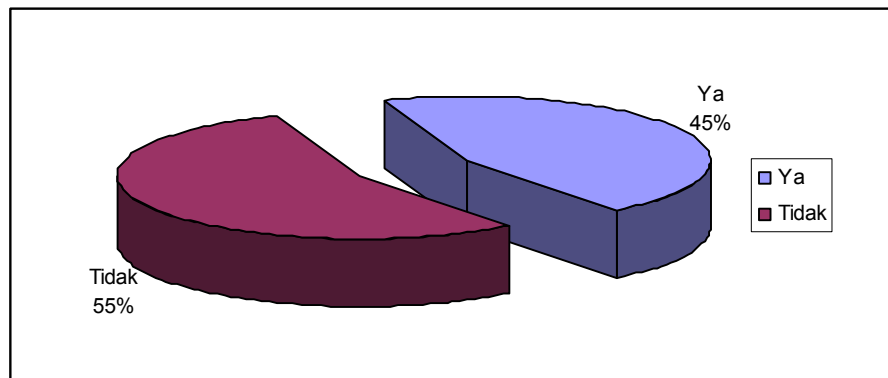
15. Pertanyaan: Jika kondisi pada no.14, diganti menjadi pada komputer teman/umum?

Hasil prosentase yang diperoleh:



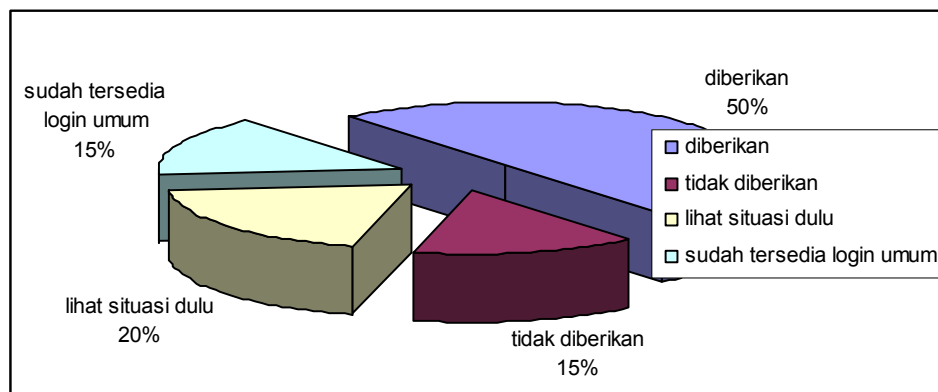
16. Pertanyaan: Apa Anda pernah melakukan *Password Hacking*?

Hasil prosentase yang diperoleh:



17. Pertanyaan: Studi Kasus (lihat lampiran)

Hasil prosentase yang diperoleh:



3.2. Analisis

Dilihat dari hasil penelitian yang diperoleh, dapat dilihat bahwa rata-rata semua orang mengetahui dan menggunakan *password*. Tentunya, dilihat dari cakupan

umur mereka yang dijadikan sampel kira-kira berumur 16 tahun keatas. Intinya, orang sudah tidak asing lagi dengan istilah *password* dan mereka menggunakannya untuk memproteksi suatu informasi yang sifatnya pribadi dan rahasia. Hal ini jelas terlihat dengan banyaknya jumlah sampel yang mengatakan bahwa mereka mempunyai lebih dari satu *password* (95%). Dari hasil tersebut dapat diasumsikan bahwa mereka menggunakan *password* untuk memproteksi berbagai keperluan, seperti email (32%), login OS (22%), HP (20%), Dokumen (15%), Screen Saver (3%), dan lain-lain (8%). Untuk menghindari terjadinya akses ke semua hal jika ada salah satu *password*-nya yang diketahui pihak lain maka kebanyakan dari mereka menggunakan *password* yang berbeda pada validasi (*login*) yang berbeda.

Namun, hal ini mempunyai kelemahan. Karena banyaknya informasi yang ingin mereka amankan sehingga membuat banyak *password* yang harus mereka ingat. Sebanyak 80% sampel memutuskan untuk menulis *password*-nya disuatu tempat. Hal ini dilakukan supaya jika lupa, ada catatan *password* sebagai *backup*-nya. Di dalam pembahasan makalah ini, sudah dikatakan bahwa hal seperti ini sangat rentan untuk mengalami ‘kebocoran’. Oleh karena itu, lebih dari setengah sampel memilih menggunakan *password* yang memiliki hubungan dengan hidup pribadi mereka agar lebih mudah untuk diingat (55%) sehingga tidak perlu dicatat.

Mengenai pemahaman terhadap *password policy* dan *good password*, rata-rata *password* tiap sampel sudah memenuhi kriterianya. Untuk penggunaan karakter dalam *password*, hampir semua sample minimal menggunakan dua jenis karakter (alphabet-numeric, alphabet-sensitive case, dll). Selain itu, lebih dari 50% sampel yang tidak menggunakan kata-kata yang ada dalam kamus dan panjang *password* yang mereka gunakan sebagian besar berkisar antara 6-10 karakter (75%). Tetapi untuk sampai pada tahap penggantian *password* secara berkala hanya sedikit sampel yang melakukannya (17%). Hal ini terjadi karena sudah terbiasa dengan *password* yang digunakan dan untuk menghindari salah ingat untuk masing-masing validasi yang berbeda. Menurut teori pada bab II, jika sering dilakukan ganti *password*, lama-kelamaan *password* yang digunakan akan ada yang lemah.

Dari hasil penelitian juga terlihat betapa pentingnya dan bersifat pribadi informasi yang mereka *password*. Hal ini terlihat dari cukup banyak sampel yang melakukan *lock* atau *auto-standby password* pada komputer ketika mereka meninggalkan komputer dalam keadaan menyala. Diperkuat lagi dengan hasil yang menunjukkan bahwa 90% sampel akan mengganti *password*-nya jika sudah diketahui pihak lain. Bahkan setelah melakukan *login* pada suatu hal yang berisi suatu informasi di komputer pribadi, kebanyakan dari mereka tetap melakukan *logout* (60%). Jika mereka melakukannya bukan di komputer pribadi, sudah dapat dipastikan mereka akan melakukan *logout* (100%). Dari analisis ini dapat dilihat bahwa betapa bergunanya *password* bagi kita untuk mengamankan informasi dari akses pihak lain.

Pada penelitian ini, saya juga ingin mengetahui berapa sampel yang pernah melakukan *password hacking*. Ternyata, cukup besar juga dari mereka yang mengetahui cara melakukannya, yaitu sebesar 45%. Berbagai alasan diungkapkan; dari yang hanya ingin coba-coba sampai ke yang mempunyai tujuan ‘khusus’. Untuk jawaban pada studi kasus sebenarnya banyak faktor yang mempengaruhinya, seperti siapa yang meminta *password*, punya jabatan apa mereka di kantor, siapa saja yang boleh memakai komputer tersebut, seberapa pentingnya sampai komputer tersebut yang harus digunakan, dan sebagainya. Maka dari itu, jawabannya pun bervariasi. Namun, sebanyak 50% sampel mengatakan akan memberikannya karena jika itu merupakan komputer kantor berarti bukan komputer pribadi dan biasanya tidak ada hal-hal yang privasi; paling hanya kerahasiaan perusahaan.

Sebagai tambahan, saya ingin membahas secara singkat mengenai berapa lama waktu yang dibutuhkan untuk melakukan *bruteforce attack* pada panjang *password* dengan prosentase sampel terbanyak, yaitu 6-10 karakter. Percobaan dilakukan dengan memakai *bruteforce calculator* dari **Mandylion Research Labs**. [3] Pada kalkulator tersebut tiap jenis karakter mempunyai nilai entropi yang didapatkan dari banyaknya kemungkinan pada jenis karakter tersebut dipangkatkan dengan jumlah karakter yang dipakai (contoh: 2005; jenis karakter *numeric* yang berjumlah 10 (0-9) dipangkat dengan banyak digit yang ada (4) sehingga

diperoleh nilai entropinya = 10.000). Untuk mendapatkan nilai entropi total, nilai entropi dari tiap jenis karakter akan dikalikan. Dari nilai tersebut akan terlihat berapa banyak kombinasi yang mungkin dari karakter yang digunakan. Kemudian untuk mengurangi *keyspace search*, hasilnya dibagi 2 menurut hukum rata-rata (misal:x). Dengan memperkirakan satu komputer ‘super’ dapat mencoba secara efisien sebanyak $2 \cdot (2^{33})$ kode dalam 1 jam (misal:y) maka dapat diestimasi secara kasar waktu yang dibutuhkan untuk meng-*crack*, yaitu x dibagi y.

Pertama, dilakukan beberapa percobaan dengan menggunakan dua jenis karakter yang banyak karakter untuk tiap jenis karakternya dipilih secara *random*.

Jenis Karakter				Total Karakter	Banyak Kombinasi	Waktu yang dibutuhkan (jam)
Lower Case	Upper Case	Numeric	Spesial Karakter			
4	-	2	-	6	45 juta	< 0,01
2	-	-	4	6	708 juta	0,02
-	-	4	3	7	327 juta	0,01
	4	-	3	7	14 milyar	0,44
5	-	3	-	8	11 milyar	0,35
-	-	3	5	8	33 milyar	0,98
6	-	4	-	10	3 triliun	89,91

Kedua, dilakukan beberapa percobaan dengan menggunakan tiga atau empat jenis karakter yang banyak karakter untuk tiap jenis karakternya dipilih secara *random*.

Jenis Karakter				Total Karakter	Banyak Kombinasi	Waktu yang dibutuhkan (jam)
Lower Case	Upper Case	Numeric	Spesial Karakter			
4	-	1	1	6	146 juta	< 0,01
2	1	-	3	6	575 juta	0,02
2	-	2	4	8	46 milyar	1,36
2	-	4	2	8	70 milyar	2,06
5	1	4	-	10	3 triliun	89,91
3	3	2	2	10	31 triliun	920,64

Dari hasil diatas dapat dilihat bahwa semakin panjang *password*, semakin lama waktu yang dibutuhkan. Penggunaan spesial karakter pada *password* dalam jumlah yang banyak juga akan lebih memperbesar waktu yang dibutuhkan daripada memperbanyak jenis karakter yang lain.

BAB IV

KESIMPULAN

4.1. Kesimpulan

Password sudah menjadi istilah umum yang dimengerti oleh banyak orang. *Password* digunakan untuk memproteksi hal-hal yang sifatnya *confidential*. Beberapa orang sudah membuat *password* dengan menggabungkan beberapa jenis karakter sehingga sulit untuk ditebak. Ini membuktikan bahwa mereka tidak ingin informasi yang tersimpan didalamnya di-*hack* oleh pihak lain.

Password yang mereka punya juga tidak ditulis disembarang tempat atau diberikan kepada sembarang orang. Bentuk apa pun yang membutuhkan validasi (*login*) untuk mengaksesnya, tidak akan dibiarkan terbuka jika ingin ditinggalkan. Hanya pembatasan saja yang masih jarang ditemukan. Namun, tanpa mengerti *policy password*, orang sudah mengerti bagaimana cara membuat *password* yang baik sehingga otentikasinya kuat.

Informasi yang diamankan tentunya yang bersifat pribadi. Untuk yang bersifat rahasia (contoh: data perusahaan), masih memungkinkan untuk diakses oleh pihak lain yang masih mempunyai kepentingan yang sama (intern). *Password* banyak digunakan pada email, data (dokumen), dan aplikasi sistem (HP, PDA, USB, dll).

4.2. Saran

Untuk yang mempunyai *password* dalam jumlah yang banyak, lebih baik memakai *password management* daripada ditulis disuatu tempat. Pemilihan *password* sebaiknya yang mudah diingat tetapi mempunyai suatu algoritma tertentu (misal: 82469173; membentuk tanda [*] dengan menghilangkan semua angka 5).

DAFTAR PUSTAKA

- [1] Anderson, Ross. 2001. *Social Engineering: A Guide to Building Dependable Distributed System*. USA: Wiley Publishing, Inc.
- [2] Beaver, Kevin. 2004. *Hacking for Dummies*. USA: Wiley Publishing, Inc.
- [3] BruteForce Attack Time Estimator – Mandyllion Research Labs
— Available at <http://www.mandyllionlabs.com/index15.htm>
- [4] Choosing a Good Password
— Available at <http://www.cs.umd.edu/faq/Passwords.shtml>
- [5] History of Password
— Available at <http://www.ussrback.com/crypto/srp/history.html>
- [6] Password Hacking Techniques
— Available at <http://www-128.ibm.com/developerworks/library/s-crack/>
- [7] Password Recovery Methods: Brute Force Attack
— Available at http://lastbit.com/rm_bruteforce.asp
- [8] Security: 5 Kesalahan Utama Dalam Security
— Available at <http://students.ukdw.ac.id/~22033120/5security.html>
- [9] The Simplest Security A Guide To Better Password Practices
— Available at <http://www.securityfocus.com/infocus/1537>
- [10] Wikipedia - The Free Encyclopedia. *Password*
— Available at <http://en.wikipedia.org/wiki/Password.htm>
- [11] Wikipedia - The Free Encyclopedia. *Password Cracking*
— Available at http://en.wikipedia.org/wiki/Password_cracking.htm
- [12] Wikipedia - The Free Encyclopedia. *Password Policy*
— Available at http://en.wikipedia.org/wiki/Password_policy.htm
- [13] Wikipedia - The Free Encyclopedia. *Password Strength*
— Available at http://en.wikipedia.org/wiki/Password_strength.htm
- [14] Wikipedia - The Free Encyclopedia. *Social Engineering*
— Available at http://en.wikipedia.org/wiki/Social_engineering.htm

LAMPIRAN

Angket yang digunakan pada penelitian ini:



Tugas Kuliah Sistem Keamanan Informasi (EC5010)
STEI - Institut Teknologi Bandung
Dosen: Dr. Ir. Budi Rahardjo

Dimohon kesediaannya untuk mengisi angket ini dengan benar. **Lingkari** jawaban anda! Jawaban dengan tanda (*) boleh dilingkari lebih dari satu. Hasil dari angket tersebut akan digunakan untuk menjadi bahan penelitian mengenai "Penggunaan Password Untuk Keamanan Informasi".

Pekerjaan:

Jenis Kelamin: L / P

1. Apakah anda mengetahui apa itu *password*? Ya / Tidak
2. Apakah anda pernah menggunakan *password*? Ya / Tidak
3. Ada berapa banyak *password* yang anda punyai? 1 / Lebih
4. Apakah anda mencatat *password* tersebut di suatu tempat? Ya / Tidak
5. Karakter apa yang biasa anda gunakan pada *password*? Alphabet / Numerik / Case Sensitive / Simbol (?,",%, dll) *
6. Apakah *password* yang anda gunakan merupakan suatu kata yang memiliki arti dan ada di kamus bahasa? Ya / Tidak
7. Berapa panjang karakter yang biasa anda gunakan sebagai *password*? 1-5 / 6-10 / 11-15 / Lebih
8. Apa anda sering mengganti *password* anda? Ya / Tidak
9. Jika pada no.8 anda menjawab "Ya", berapa kira-kira periode waktunya? 1 hari / 1 minggu / 1 bulan /
10. Password yang anda biasa gunakan apakah ada hubungannya dengan anda (mis.tgl lahir, nama binatang piaraan, nama orang tua, nomor keberuntungan, dll)? Ya / Tidak
11. Apa saja yang anda *password*? *login OS (windows)* / *screen saver* / email / HP / dokumen (word, excel, zip, dll) / *
12. Jika komputer ditinggal dalam keadaan menyala, apa yang anda lakukan? *logout* / *auto-standby password* / tdk keduanya
13. Apa yang anda lakukan jika seseorang mengetahui *password* anda? langsung diganti / dibiarkan saja /
14. Apakah pada komputer pribadi, anda melakukan *logout* setiap kali anda selesai mengakses sesuatu yang memiliki *password*, seperti: email, friendster, windows, dll? Ya / Tidak
15. Jika no.14 diganti menjadi komputer teman/umum? Ya / Tdk
16. Apakah anda pernah melakukan *password hacking*? Ya / Tdk
17. Contoh kasus: Jika anda seorang karyawan yang berhalangan datang ke kantor. Kemudian, ada teman atau atasan anda yang perlu memakai komputer anda. Jika anda ditanya *password* komputer tersebut, apa yang anda lakukan?

Terima kasih atas waktu dan kesediaannya untuk mengisi angket diatas. Semoga data yang saudara/i berikan dapat berguna bagi penelitian ini. (W41)

--- ^⊙^⊙^⊙^ ---