KEAMANAN SISTEM

Subianto | AMIK JTC SEMARANG

Keamanan Sistem

- Masalah Keamanan Sistem Komputer Secara Umum
- Masalah Etika
- Dasar-dasar Gangguan Keamanan Komputer
- Prinsip Perancangan Sistem Yang Aman

Pendahuluan

- Masalah keamanan sistem merupakan aspek terpenting dari sebuah sistem informasi
- Kata AMAN dapat didefinisikan sebagai terhindar dari serangan atau kegagalan
- Tidak satu sistem komputerpun yang memiliki sistem keamanan yang sempurna
- Setidaknya kita harus mempunyai suatu mekanisme tertentu yang dapat mencegah terjadinya pelanggaran pada sistem komputer kita

Kenapa Pengamanan Itu Perlu ?

- Mengapa kita membutuhkan keamanan, seberapa aman, atau apa yang hendak kita lindungi, seberapa penting data kita sehingga kita perlu memusingkan diri dengan masalah keamanan ?

Minimalisasi Celah Keamanan.

- Hal yang dapat kita lakukan hanyalah mencoba meminimalisasi celah keamanan yang ada pada komputer kita.

- Hal yang perlu kita ingat adalah bahwa semakin aman sistem yang kita gunakan, sistem komputer kita akan menjadi semakin merepotkan.

- Kita harus menyeimbangkan antara kenyamanan pemakai sistem dan proteksi demi alasan keamanan.

Apa yang akan dilindungi ?

- apa yang anda lindungi ?
- Kenapa anda melindunginya ?
- Seberapa besar nilai data yang anda lindungi ?
- Siapa yang bertanggung jawab terhadap data dan aset lain dalam sistem anda ?
- Resiko adalah kemungkinan dimana seorang penyusup berhasil dalam usahanya untuk mengakses komputer anda.

Tipe Penyusup

- ***The Curious***

  Mencari tahu tipe sistem dan data yang anda miliki.
- ***The Malicious***

  Mengganggu sistem sehingga tidak dapat bekerja dengan optimal.
- ***The High-Profile Intruder***

  Mencoba menyusup untuk mendapatkan ketenaran dan pengakuan.
- ***The Competition***

  Tertarik pada data yang ada pada sistem.
- ***The Borrowers***

  Menggunakan sumber daya yang kita miliki untuk kepentingan mereka.
- ***The Leapfrogger***

  Menggunakan sistem yang kita miliki untuk masuk kesistem lain.

Keamanan Komputer

Keamanan sistem terbagi menjadi tiga :

1. **Keamanan eksternal**

   Fasilitas komputer dari penyusup dan bencana misal bencana alam

2. **Keamanan interface pemakai**

   Identifikasi pemakai sebelum diijinkan mengakses program dan data tersimpan di dalam sistem

3. **Keamanan internal**

   Pengamanan yang dibangun dalam perangkat keras dan sistem operasi untuk menjamin operasi yang handal dan untuk menjaga keutuhan program serta data

2 masalah yang penting

1. **Kehilangan data**
   - Bencana
   - Kesalahan perangkat keras dan perangkat lunak
   - Kesalahan manusia
2. **Penyusup *(interuder)***
   - Penyusup Pasif (membaca data yang tidak diotorisasi)
   - Penyusup Aktif (mengubah data yang tidak diororisasi)

4 kategori intruder

1. Keingintahuan seseorang akan hal-hal pribadi orang lain
2. Penyusupan oleh orang-orang dalam
3. Keinginan untuk mendapatkan uang
4. E-spionase komersial atau militer.

4 dasar pengamanan komputer

1. Pengamanan Fisik
2. Pengamanan Akses
3. Pengamanan Data
4. Pengamanan Jaringan

Ancaman Keamanan

- ***Interruption***

  Merupakan ancaman terhadap *avialibility* Informasi.

- ***Interception***

  Merupakan ancaman terhadap kerahasiaan *(secrecy)*.

- ***Modification***

  Merupakan ancaman terhadap integritas.

- ***Febrication***

  Merupakan ancaman terhadap integritas.

Aspek Keamanan Komputer

- ***Authentication* (Otentikasi)**

  Keaslian pesan tersebut datang dari orang yang dimintai informasi.
- ***Integrity* (Integritas)**

  Pesan yang dikirim tidak dimodifikasi oleh pehak ketiga.
- ***Nonrepudiation* (Nir Penyangkalan)**

  Sipengirim pesan tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut.
- ***Authority***

  Informasi yang berada pada sistem jaringan tidak dapat di modifikasi oleh pihak ketiga.
- ***Confidentiality* (Kerahasiaan)**

  Usaha untuk menjaga informasi dari orang yang tidak berhak mengaksis informasi.

Aspek Keamanan Komputer

- ***Privacy* (Pribadi)**

  Data-data yang bersifat pribadi.

- ***Avialibility* ()**

  Ketersediaan hubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang dapat menghambat atau meniadakan akses ke informasi

- ***Access Control***

  Berhubungan dengan cara mengatur akses kepada informasi.

Prinsip Pengaman Sistem

Otentikasi Pemakai

Password

- Salting
- One-time password
- Satu daftar pertanyaan dan jawaban yang panjang
- Tanggapan-tanggapan

Identifikasi Fisik

- Kartu berpita magnetik
- Sidik jari
- Analisis tanda tangan

Pembatasan

TUGAS 1 - KELOMPOK

- Serangan terhadap Komputer/Sistem Komputer
- Sejarah Perkembangan Virus
- Mencegah serangan terhadap Komputer/Sistem Komputer

Sistematika makalah

- Halaman Judul
- Daftar Isi
- Latar Belakang Masalah
- Pembahasan
- Kesimpulan
- Daftar Pustaka

SECURITY BREACH ACCIDENT

1996	U.S. Federal Computer Incident Response Capability (FedCIRC) melaporkan bahwa lebih dari 2500 "insiden" di system komputer atau jaringan komputer yang disebabkan oleh gagalnya sistem keamanan atau adanya usaha untuk membobol sistem keamanan
1996	FBI National Computer Crimes Squad, Washington D.C., memperkirakan kejahatan komputer yang terdeteksi kurang dari 15%, dan hanya 10% dari angka itu yang dilaporkan
1997	Penelitian Deloitte Touch Tohmatsu menunjukkan bahwa dari 300 perusahaan di Australia, 37% (dua diantara lima) pernah mengalami masalah keamanan sistem komputernya.
1996	Inggris, NCC Information Security Breaches Survey menunjukkan bahwa kejahatan komputer menaik 200% dari tahun 1995 ke 1996. Kerugian rata-rata US $30.000 / insiden.
1998	FBI melaporkan bahwa kasus persidangan yang berhubungan dengan kejahatan komputer meroket 950% dari tahun 1996 ke tahun 1997, dengan penangkapan dari 4 ke 42, dan terbukti (convicted) di pengadilan naik 88% dari 16 ke 30 kasus.

Akibat dari jebolnya sistem keamanan

1988	Keamanan sistem mail sendmail dieksploitasi oleh Robert Tapan Morris sehingga melumpuhkan sistem Internet. Kegiatan ini dapat diklasifikasikan sebagai "denial of service attack". Diperkirakan biaya yang digunakan untuk memperbaiki dan hal-hal lain yang hilang adalah sekitar $100 juta. Di tahun 1990 Morris dihukum (convicted) dan hanya didenda $10.000.
10 Maret 1997	Seorang hacker dari Massachusetts berhasil mematikan sistem telekomunikasi di sebuah airport local (Worcester, Massachusetts) sehingga mematikan komunikasi di control tower dan menghalau pesawat yang hendak mendarat. Dia juga mengacaukan sistem telepon di Rutland, Massachusetts. http://www.news.com/News/Item/Textonly/0,25,20278,00.html?pfv

Akibat dari jebolnya sistem keamanan

1990	Kevin Poulsen mengambil alih system komputer telekomunikasi di Los Angeles untuk memenangkan kuis di sebuah radio local.
1995	Kevin Mitnick, mencuri 20.000 nomor kartu kredit, menyalin system operasi DEC secara illegal dan mengambil alih hubungan telpon di New York dan California.
1995	Vladimir Levin membobol bank-bank di kawasan Wallstreet, mengambil uang sebesar $10 juta.
2000	Fabian Clone menjebol situs aetna.co.id dan Jakarta mail dan membuat directory atas namanya berisi peringatan terhadap administrator situs tersebut.
2000	Beberapa web site Indonesia sudah dijebol dan daftarnya (beserta contoh halaman yang sudah dijebol) dapat dilihat di koleksi <http://www.2600.com>
2000	Wenas, membuat server sebuah ISP di singapura down

MEMAHAMI HACKER BEKERJA

- Tahap mencari tahu system komputer sasaran.
- Tahap penyusupan
- Tahap penjelajahan
- Tahap keluar dan menghilangkan jejak.

PRINSIP DASAR PERANCANGAN SISTEM YANG AMAN

1. Mencegah hilangnya data
2. Mencegah masuknya penyusup

LAPISAN KEAMANAN

1. Lapisan Fisik :
   - membatasi akses fisik ke mesin :
     - Akses masuk ke ruangan komputer
     - penguncian komputer secara hardware
     - keamanan BIOS
     - keamanan Bootloader
   - back-up data :
     - pemilihan piranti back-up
     - penjadwalan back-up
   - mendeteksi gangguan fisik :
     - log file : Log pendek atau tidak lengkap, Log yang berisikan waktu yang aneh, Log dengan permisi atau kepemilikan yang tidak tepat, Catatan pelayanan reboot atau restart, Log yang hilang, masukan atau login dari tempat yang janggal
     - mengontrol akses sumber daya.

LAPISAN KEAMANAN

2. Keamanan lokal
   - Berkaitan dengan user dan hak-haknya :
     - Beri mereka fasilitas minimal yang diperlukan.
     - Hati-hati terhadap saat/dari mana mereka login, atau tempat seharusnya mereka login.
     - Pastikan dan hapus rekening mereka ketika mereka tidak lagi membutuhkan akses.

LAPISAN KEAMANAN

3. Keamanan Root

- Ketika melakukan perintah yang kompleks, cobalah dalam cara yang tidak merusak dulu dan pastikan anda ingin menghapus file-file yang anda pikirkan.
- Hanya menjadi root ketika melakukan tugas tunggal tertentu. Jika anda berusaha mengetahui bagaimana melakukan sesuatu, kembali ke shell pemakai normal hingga anda yakin apa yang perlu dilakukan oleh root.
- Jalur perintah untuk pemakai root sangat penting. Jalur perintah, atau variabel lingkungan PATH mendefinisikan lokal yang dicari shell untuk program. Cobalah dan batasi jalur perintah bagi pemakai root sedapat mungkin, dan jangan pernah menggunakan '.', yang berarti 'direktori saat ini', dalam pernyataan PATH anda. Sebagai tambahan, jangan pernah menaruh direktori yang dapat ditulis pada jalur pencarian anda, karena hal ini memungkinkan penyerang memodifikasi atau menaruh file biner dalam jalur pencarian anda, yang memungkinkan mereka menjadi root ketika anda menjalankan perintah tersebut.
- Jangan pernah menggunakan seperangkat utilitas rlogin/rsh/rexec (disebut utilitas r) sebagai root. Mereka menjadi sasaran banyak serangan, dan sangat berbahaya bila dijalankan sebagai root. Jangan membuat file .rhosts untuk root.
- File /etc/securetty berisikan daftar terminal-terminal tempat root dapat login. Secara baku (pada RedHat Linux) diset hanya pada konsol virtual lokal (vty). Berhati-hatilah saat menambahkan yang lain ke file ini. Anda seharusnya login dari jarak jauh sebagai pemakai biasa dan kemudian 'su' jika anda butuh (mudah-mudahan melalui ssh atau saluran terenkripsi lain), sehingga tidak perlu untuk login secara langsung sebagai root.
- Selalu perlahan dan berhati-hati ketika menjadi root. Tindakan anda dapat mempengaruhi banyak hal. Pikir sebelum anda mengetik!

LAPISAN KEAMANAN

4. Keamanan File dan system file
   - Directory home user tidak boleh mengakses perintah mengubah system seperti partisi, perubahan device dan lain-lain.
   - Lakukan setting limit system file.
   - Atur akses dan permission file : read, writa, execute bagi user maupun group.
   - Selalu cek program-program yang tidak dikenal

LAPISAN KEAMANAN

5. Keamanan Password dan Enkripsi
   - Hati-hati terhadap bruto force attack dengan membuat password yang baik.
   - Selalu mengenkripsi file yang dipertukarkan.
   - Lakukan pengamanan pada level tampilan, seperti screen saver.

6. Keamanan Kernel
   - selalu update kernel system operasi.
   - Ikuti review bugs dan kekurang-kekurangan pada system operasi.

7. Keamanan Jaringan
   - Waspadai paket sniffer yang sering menyadap port Ethernet.
   - Lakukan prosedur untuk mengecek integritas data
   - Verifikasi informasi DNS
   - Lindungi network file system
   - Gunakan firewall untuk barrier antara jaringan privat dengan jaringan eksternal