**Keamanan Sistem Komputer (KSK)**

 merupakan sebuah upaya yang dilakukan untuk mengamankan kinerja,fungsi atau proses

komputer. KSK juga berguna untuk menjaga komputer dari para hacker (penjahat dunia maya). Tetapi layaknya seperti gembok kunci dalam rumah yang menjaga rumah dari para maling untuk masuk.Sebaik apapun sistem keamanan rumah anda pasti ada cara untuk masuk kedalam rumah anda. sistem keamanan komputer dibutuhkannya karena meningkatnya perkembangan teknologi dalam jaringan.

Fungsi sistem keamanan komputer adalah untuk menjaga sumber daya sistem agar tidak

digunakan,dimodifikasi, dan diganggu oleh orang lain yang tidak bertanggungjawab.

**Alasan di butuhkan keamanan sistem komputer**

Keamanan Komputer dibutuhkan dikarenakan ada beberapa faktor, diantaranya :

1. “information-based society”, menyebabkan nilai informasi menjadi sangat penting dan menuntut kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi,.
2. Infrastruktur Jaringan komputer, seperti LAN dan Internet, memungkinkan untuk menyediakan informasi secara cepat, sekaligus membuka potensi adanya lubang keamanan (security hole)

**Letak PotensI lubang keamanan (Security HoLE)**



**Kejahatan Komputer semakin meningkat karena :**

1. Aplikasi bisnis berbasis TI dan jaringan komputer meningkat : online banking, ecommerce, Electronic data Interchange (EDI).
2. Desentralisasi server/server yang dibuat tersebar.
3. Transisi/perubahan dari single vendor ke multi vendor.
4. Meningkatnya kemampuan pemakai (user).
5. Kesulitan penegak hukum dan belum optimalnya perundang-undangan mengenai cyber crime.
6. Sistem yang terhubung dengan jaringan Internet.

**Penyebab keamanan sistem komputer diperlukan :**

1. Meningkatnya pengguna komputer dan internet
2. Banyaknya software yang pada awalnya digunakan untuk melakukan audit sebuah sistem dengan cara mencari kelemahan dan celah yang mungkin ada disalahgunakan untuk melakukan scanning sistem orang lain.
3. Banyaknya software-software untuk melakukan probe dan penyusupan yang tersedia di Internet dan bisa di download secara gratis.
4. Meningkatnya kemampuan pengguna komputer dan internet
5. Desentralisasi server sehingga lebih banyak sistem yang harus ditangani, sementara SDM terbatas.
6. Kurangnya hukum yang mengatur kejahatan komputer.
7. Semakin banyaknya perusahaan yang menghubungkan jaringan LAN mereka ke Internet.
8. Meningkatnya aplikasi bisnis yang menggunakan internet.
9. Banyaknya software yang mempunyai kelemahan (bugs).

**Pendekatan yang umum dilakukan untuk meningkatkan keamanan komputer**

1. membatasi akses fisik terhadap komputer
2. menerapkan mekanisme pada perangkat keras dan sistem operasi untuk keamanan komputer
3. membuat strategi pemrograman untuk menghasilkan program komputer yang dapat diandalkan

**Kebijakan dalam keamanan sistem komputer :**

**Pengamanan yang disarankan :**

1. Terapkan rencana pengamanan untuk mencegah pembobolan.
2. Buat rencana/planning penanganan jika pembobolan terjadi.
3. Buatlah backup.
4. Hanya ijinkan akses untuk pegawai tertentu.
5. Ubah password secara teratur.
6. Jagalah informasi yang tersimpan dengan aman.
7. Gunakan software antivirus.
8. Gunakan biometrik untuk mengakses sumberdaya komputasi.
9. Rekrut tenaga kerja / pegawai yang bisa dipercaya.
10. Enkripsi – proses penyandian pesan sebelum memasuki jaringan atau gelombang udara, kemudian membuka kembali pada ujung penerimaan(Dekripsi).

**Penyebab Meningkatnya Kejahatan Komputer**

1. Apliasi bisnis berbasis TI dan jaringan komputer meningkat : online banking, e-commerce, Electronic data Interchange (EDI).
2. Desentralisasi Server.
3. Transisi dari single vendor ke multi vendor.
4. Meningkatnya kemampuan pemakai (user)
5. Semakin kompeksnya sistem yang digunakan, semakin besarnya source code program yang digunakan. Berhubungan dengan jaringan / internet.

**Klasifikasi Kejahatan Komputer**

Menurut David Icove [Jhon D. Howard, “An Analysis Of Security Incidents On The Internet 1989-1995” PhD thesis, Engineering and Public policy, carnegia Mellon

University, 1997] berdasarkan lubang keamanan, kemanan dapat di klasifikasikan menjadi empat yaitu:

**Klasifikasi Kejahatan Komputer**

1. Keamanan yang bersifat fisik (Physical security), termasuk akses orang ke gedung, peralatan, dan media yang digunakan. Contoh:
2. Wiretapping atau hal-hal yang ber-hubungan dengan akses ke kabel atau komputer yang digunakan juga dapat dimasukan kedalam kelas ini.
3. Daniel of service, dilakukan misalnya dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan (yang dapat berisi apa saja karena yang diutamanakn adalah banyanya jumlah pesan)
4. Syn Flood Attack, dimana sistem (host) yang dituju dibanjiri oleh permintaan sehingga dia menjadi ter-lalu sibuk dan bahkan ndapat berakibat macetnya sistem (hang)
5. Keamanan yang berhubungan dengan orang (pesonal)
6. Indentifikasi user (username dan password)
7. Profil resiko dari orang yang mempunya akses (Pemakai dan
8. pengelola)
9. Keamanan dari data dan media serta teknik komunikasi
10. Keamanan dalam operasi:
11. Adanya prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga termasuk prosedur setetlah serangan (post attack recovery)

**Tipe Penyusup**

1. The Curios (Si ingin Tahu)

Tertarik menemuan jenis dan data yang anda miliki.

1. The Malicious (Si Perusak)

Berusaha merusak sistem, atau merubah web page, atau sebaliknya membuat waktu dan uang anda kembali pulih.

1. The High-Profile (Si Profil Tinggi)

 Berusaha menggunakan sistem, untuk memperoleh popularitas dan ketenaran. Dan juga mungkin menggunakan sistem profil tinggi anda untuk mengiklankan kemampuannya

1. The Competition (Si Pesaing)

Penyusup ini tertarik pada data yang anda miliki dalam sistem anda, ia mungkin seseorang yang beranggapan bahwa anda memiliki sesuatu yang dapat menguntungkan secara keuangan atau sebaliknya

**Istilah untuk penyusup**

1. Mundane: tahu mengenai hacking tapi tidak mengetahui metode dan prosesnya
2. Lamer (Script Kiddies): Mencoba script-script yang pernah dibuat oleh aktivis hacking, tapi tidak pernah paham bagaimana cara membuatnya.
3. Wannabe: Paham sedikit metode hacking, dan sudah mulai berhasil menerobos sehingga berfalsafah; HACK IS MY RELIGION.
4. Larva (newbie): Hacker pemula, teknik hacking mulai dikuasai dengan baik, sering bereksperimen.
5. Hacker: Aktivitas hacking sebagai profesi.
6. Wizar: Hacker yang membuat komunitas pembnelajaran diantara mereka.
7. Guru: master of the master hacker, lebih mengarah ke penciptaan tools-tools yang powerfull yang salah satunya dapat menunjang aktivitas hacing, namun lebih jadi tools pemrograman system yang umum.

**Aspek Kemanan Komputer**

1. Privacy / Confidentiality

Merupakan Menjaga informasi dari orang yang tidak berhak mengakses.

 Privacy : Lebih kearah data-data yang sifatnya prifat, Contoh: e-mail seorang pemakai (user) tidak boleh dibaca oleh administrator. SedangkanConfidentiality : berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut.

Contoh : Data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social scurity number, agama, status perkawinan, penyakityang pernah diderita, nomor kartu kredit dll) harus dapat diproteksi dalam penggunaan dan penyebarannya.

Bentuk Serangan : Usaha penyadapan (dengan program sniffer)

Usaha-usaha yang dapat dilakukan untuk meningkatkan privacy dan confidentiality adalah dengan menggunakan teknologi kriptografi.

1. Integrity

Informasi tidak boleh diubah tanpa seijin pemilik informasi.

Contoh : e-mail di Intercept ditengah jalan, diubah isinya,kemudian diteruskan ke alamat yang dituju. Bentuk serangan : adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa ijin, “man in the middle attack” dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.

1. Authentication

Metode untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul yang dimaksud.

Dukungan:

Adanya Tools membuktikan keaslian dokumen, dapat dilakukan dengan

teknologi watermarking (untuk menjaga “intellectual property” yaitu dengan

menandai dokumen atau hasil karya dengan “tanda tangan”

pembuat) dan digital signature.

Acces control, yaitu berkaitan dengan pembatasan orang yang dapat

mengakses informasi. User harus menggunakan password biometric (ciriciri

khas orang), dan sejenisnya.

1. Availability

Berhubungan dengan ketersediaan informasi ketika dibutuhkan.

Contoh hambatan :

“deniel of service attack” (Dos attack), dimana server dikirimi permintaan

(biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan

sehingga tidak dapat melayani permintaan lain atau bahkan sampai down,

hang, crash.

Mailbom, dimana seorang pemakai dikirim e-mail bertubi-tubi (katakan ribuan email) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya.

1. Acces Control.

Cara pengaturan akses kepada informasi. Berhubungan dengan masalah authentication dan juga privacy.

Metode : Menggunakan kombinasi userid/password atau dengan menggunakan mekanisme lain.

1. Non-repudation.

Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Dukungan bagi electronic commerce.

Model Serangan

1. Interruption : Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan (availability) dari sistem. Contoh serangan adalah “Denial of service attack”.
2. Interception : Pihak tidak berwenang berhasil mengakses asset atau informasi. Contoh dari serangan ini adalah penyadapan (wiretapping).
3. Modification : Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari website dengan pesan –pesan yang merugikan pemilik website.
4. Fabrication : Pihak yang tidak berwenang menyisip objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti e-mail palsu kedalam jaringan komputer.

**Prinsip Dasar Perancangan Sistem Yang aman**

1. Mencegah hilangnya Data

2. Mencegah masuknya penyusup

**Lapisan Keamanan**

1. Lapisan Fisik:

1. Membatasi akses fisik ke mesin:
2. Akses masuk ke ruangan komputer
3. Penguncian komputer secara hardware
4. Keamanan BIOS
5. Keamanan Bootloader
6. Backup Data :

Pemilihan piranti back-up

Penjadwalan Backup

1. Mendeteksi gangguan Fisik :
2. Log File : Log pendek atau tidak lengkap, log yang berisikan waktu yang aneh, log permisi atau kepemilikan yang tidak tepat, catatan pelayanan reboot atau restart, log yang hilang, masukan su atau logim dari tempat janggal.
3. Mengontrol akser sumber daya.

2. Keamanan Lokal :

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

3. Keamanan Root

1. Hanya menjadi root dalam melakukan tugas tunggal tertentu.
2. Batasi jalur perintah bagi pemakai root.
3. Jangan menggunakan perangkat utilitas rlogin/rshrexec.

4. Keamanan File dan system file

1. Directory home user tidak boleh mengakses perintah mengubah sistem, seperti partisi, perubahan device dan lain-lain.
2. Lakukan setting limit system
3. Atur akses dan permission file
4. Selalu cek program-program yang tidak dikenal.

5. Keamanan Password dan Enkripsi:

1. Hati-hati terhadap brute forec attack dengan menbuat password yang baik
2. Selalu mengenkripsi file yang diperlukan
3. Lakukan pengamanan pada level tampilan, seperti screen saver.

6. Kemanan Kernel :

1. Selalu Update kernel system operasi
2. Ikut review bugs dan kekurangan-kekurngan pada system operasi

7. Keamanan Jaringan :

1. Waspadai paket sniffer yang sering menyadap port ethernet
2. Lakukan prosedur untuk mengecek integritas data
3. Verifikasi informasi DNS
4. Lindungi Network File Sistem
5. Gunakan Firewall untuk barrier anatar jaringan privat dengan jaringan

eksternal.

Memahami Hacker Bekerja

Secara umum hacker bekerja melalui beberapa tahapan :

1. Tahap Mencari tahu system komputer sasaran.

2. Tahap Penyusapan.

3. Tahap Penjelajahan.

4. Tahap Keluar dan menghilangkan Jejak.