

PENDAHULUAN KEAMANAN KOMPUTER DAN KEJAHATAN KOMPUTER

PERTEMUAN 1

MENGAPA KEAMANAN KOMPUTER DIBUTUHKAN?

Melindungi sistem dari kerentanan

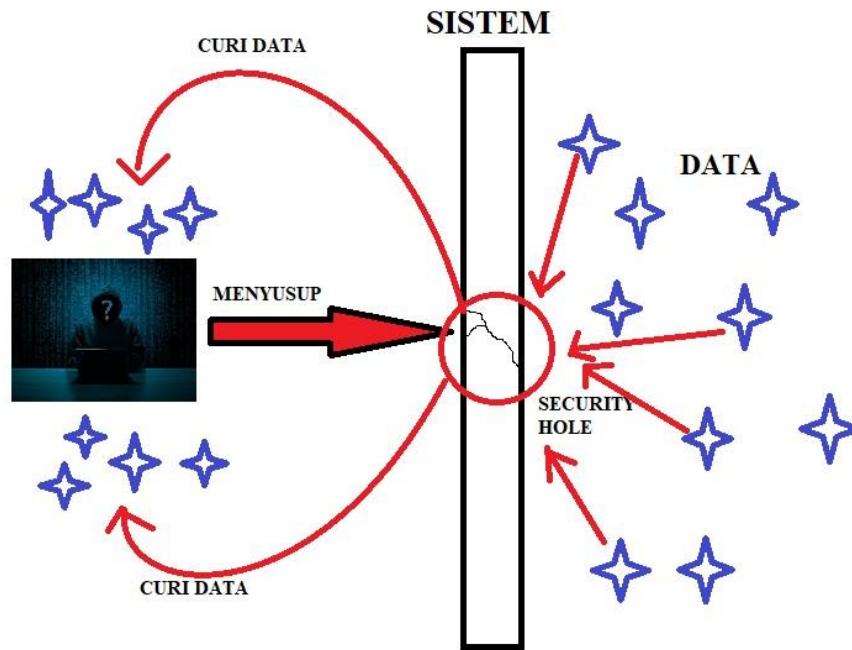


```
graph TD; A[Melindungi sistem dari kerentanan] --> B[Mengurangi resiko ancaman]; B --> C[Melindungi sistem dari gangguan alam (contoh petir dan lain-lainnya)]; C --> D[Menghindari resiko penyusupan];
```

Mengurangi resiko ancaman

Melindungi sistem dari gangguan alam
(contoh petir dan lain-lainnya)

Menghindari resiko penyusupan



ILUSTRASI
KERENTANAN
DAN ANCAMAN
SISTEM
KOMPUTER

PENYEBAB MENINGKATNYA KEJAHATAN KOMPUTER

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

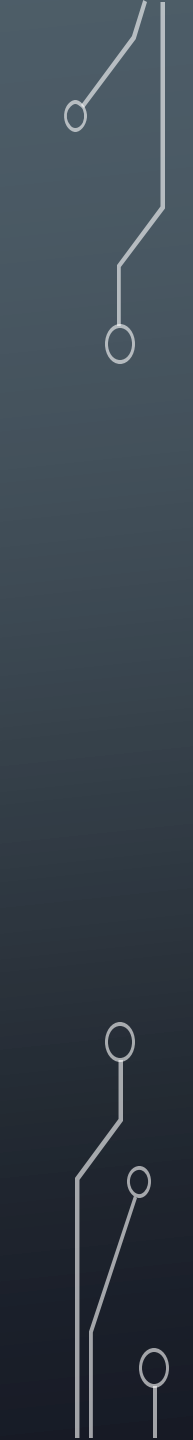




KLASIFIKASI KEAMANAN

- Keamanan yang bersifat fisik
- Keamanan yang berhubungan dengan personel
- Keamanan dari data dan media serta teknik komunikasi
- Keamanan dalam operasi


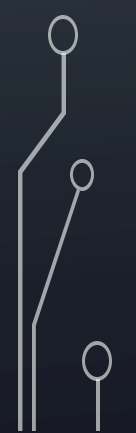


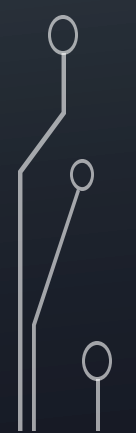


KEAMANAN YANG BERSIFAT FISIK

- Celah keamanan yang bisa diakses melalui peralatan, jaringan dan media yang digunakan
 - Contoh:
 - Wiretapping, penyadapan saluran komunikasi khususnya kabel (misalkan penyadapan telepon, listrik atau Internet)
 - Denial of Service, penghambat kerja sebuah layanan ataupun mematikannya, sehingga user yang berkepentingan tidak dapat menggunakan layanan tersebut, dengan cara membanjiri layanan dengan permintaan yang menyebabkan jaringan sibuk, sistem hang, bandwidth habis, ram terkuras
 - Pencurian, mengambil alih peralatan/media. Contohnya mencuri HDD, kabel USB, dll
- 



KEAMANAN YANG BERHUBUNGAN DENGAN PERSONEL

- Celah keamanan yang berkaitan dengan hak akses
 - Hak akses merupakan pemberian izin kepada user untuk dapat mengendalikan sistem/aplikasi; dapat berkaitan dengan izin akses untuk merubah, menyimpan, dan menghapus data.
 - Contoh: seorang user memanipulasi hak akses menjadi administrator
- 
- 



KEAMANAN DARI DATA DAN MEDIA SERTA TEKNIK KOMUNIKASI

- Celah keamanan yang terletak pada medianya itu sendiri
- Contoh kelemahan Software yang digunakan untuk mengelola data



KEAMANAN DALAM OPERASI

- Celah keamanan yang disebabkan kebijakan atau aturan untuk mengendalikan dan mengelola sistem

KARAKTERISTIK PENYUSUP

- The Curious (Si ingin Tahu) - tipe penyusup ini pada dasarnya tertarik menemukan jenis sistem korban dan data didalamnya
- The Malicious (Si perusak)- tipe penyusup ini berusaha untuk merusak atau merubah sistem dan web page korban
- The High-Profile Intruder (Si Profil tinggi) - tipe penyusup ini berusaha menggunakan sistem korban untuk memperoleh popularitas dan ketenaran. Penyusup mungkin menggunakan sistem profil tinggi korban untuk mengiklankan kemampuannya.
- The Competition (Si Pesaing) - tipe penyusup ini tertarik pada data yang dimiliki dalam sistem korban. Penyusup beranggapan bahwa data tersebut memiliki sesuatu yang dapat menguntungkannya secara keuangan atau sebaliknya.
- The Borrowers (Si Peminjam) – tipe penyusup ini tertarik untuk mendirikan toko di sistem korban dan menggunakan sumber dayanya untuk tujuan mereka sendiri. Dia biasanya akan menjalankan server obrolan atau irc, situs arsip porno, atau bahkan server DNS.
- The Leapfrogger - tipe penyusup ini hanya tertarik pada sistem korban dan menggunakannya untuk masuk ke sistem lain. Jika sistem korban terhubung dengan baik atau merupakan pintu gerbang ke sejumlah host internal, korban mungkin melihat jenis ini mencoba menyusupi sistemnya korban.

FASE SEORANG HACKER

- Mundane : tahu tentang hacking tetapi tidak tahu metode dan prosesnya
- Lamer : mendapatkan script yang pernah dibuat oleh aktivis hacking dan setelah itu mencoba script-script tersebut tetapi tidak paham cara meletakkan scrip-scriptnya
- Wannabe : orang yang tahu sedikit metode hacking, dan sudah mulai berhasil menerobos sehingga ber-falsafah; HACK IS MY RELIGION
- Newbie : hacker pemula, sering bereksperimen dan teknik hacking mulai dikuasainya dengan baik
- Hacker : aktivitas Hacking sebagai profesi
- Wizard : hacker yang membuat komunitas pembelajaran ke sesama mereka
- Guru : master of hacker

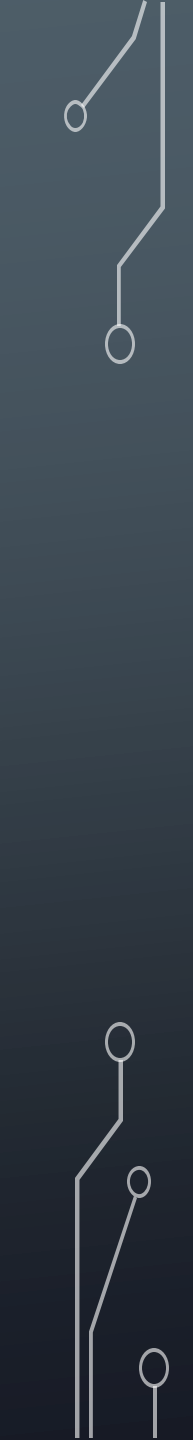


ASPEK KEAMANAN KOMPUTER

- Privacy / Confidentiality
- Integrity
- Authentication
- Availability
- Access Control
- Non-repudiation



PRIVACY / CONFIDENTIALITY

- Usaha untuk menjaga informasi dari orang yang tidak berhak mengakses
 - Contoh ancaman :
 - (Privacy) Email anggota tidak boleh dibaca oleh administrator server
 - (Confidentiality) Data pelanggan sebuah ISP dijaga kerahasiaannya
 - Solusi :
 - Kriptografi (enkripsi dan dekripsi)
- 

INTEGRITY

- Informasi tidak boleh diubah tanpa seizin pemilik informasi.
- Contoh ancaman :
 - Trojan, virus, man in the middle attack
 - Pengubahan isi email
- Solusi :
 - Enkripsi
 - Digital Signature

AUTHENTICATION

- Metode untuk menyatakan bahwa informasi betul-betul asli.
- Contoh ancaman :
 - Dokumen palsu, pengguna palsu
- Solusi :
 - Watermarking, digital signature
 - Access Control (What you have/know/are ?)
 - Digital certificate

AVAILABILITY

- Ketersediaan informasi ketika dibutuhkan.
- Contoh ancaman :
 - “Denial of Service attack” (DoS attack)
 - Mailbomb, dimana seorang pemakai dikirim e-mail bertubi-tubi (katakan ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya.
- Solusi :
 - Spam blocker
 - Connection limit

ACCESS CONTROL

- Cara pengaturan akses kepada informasi.
- Contoh ancaman :
 - Pengubahan data anggota oleh orang yang tidak berhak
- Solusi :
 - Membagi user dengan tingkatan (guest, operator, admin)

NON- REPUDIATION

- Menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi.
- Contoh ancaman :
 - Penyangkalan pesanan melalui email
- Solusi :
 - Digital signature, certificate dan kriptografi

CATATAN TAMBAHAN (1)

- Digital Signature:
 - Stempel autentikasi elektronik yang dienkripsikan pada informasi digital seperti pesan email, makro, atau dokumen elektronik
 - Tanda tangan mengonfirmasi bahwa informasi berasal dari penanda tangan dan belum diubah. Tanda tangan ini bukan tanda tangan yang discan dan disimpan dalam bentuk digital. Melainkan kode unik yang digenerate dengan teknologi kriptografi (Public Key Infrastructure)
 - Untuk membuat tanda tangan digital, memerlukan sertifikat tanda tangan yang membuktikan identitas. Saat mengirimkan makro atau dokumen yang ditandatangani secara digital, juga mengirimkan sertifikat dan kunci publik. Sertifikat dikeluarkan oleh otoritas sertifikat yang merupakan entitas yang serupa dengan notaris publik (menerbitkan sertifikat digital, menandatangani sertifikat untuk verifikasi validasi, dan melacak sertifikat yang telah dicabut atau kadaluarsa). Otoritas sertifikat ini fungsinya sama dengan surat izin mengemudi. Sertifikat biasanya berlaku hanya satu tahun, setelah itu, penanda tangan harus memperbaharui, atau mendapat sertifikat tanda tangan yang baru untuk menetapkan identitas.

CATATAN TAMBAHAN (2)

- Digital certificate:
 - Sebuah sertifikat untuk memastikan kepemilikan sebuah identitas digital, dalam hal ini public key.
 - Contoh ilustrasi dalam dunia nyata, untuk memastikan identitas seseorang digunakan KTP, misalnya mau membuat rekening BANK. Sehingga untuk memastikan identitas, harus menunjukkan KTP asli. KTP dikeluarkan oleh Dinas Kependudukan dan catatan sipil. Dinas ini juga melakukan verifikasi pada saat pembuatan KTP.