



COMPUTER SECURITY

Pertemuan I

Rianto, S.Kom., M.Eng.

Fakultas Sains dan Teknologi

Universitas Teknologi Yogyakarta

Email : me@rianto.com Website : <http://www.rianto.com>

Mobile : 0815 787 02873

Daftar Isi

- Keamanan dan Manajemen Perusahaan
- Dasar-dasar Gangguan Keamanan Komputer
- Prinsip Dasar Perancangan Sistem Yang Aman

Pendahuluan

❑ Mengapa perlu aman?

- Resiko kerugian finansial
- Resiko kerugian kerahasiaan
- Resiko kerugian harga diri
- Dan lain-lain

❑ Motif-motif serangan pada sistem komputer

- Politis
- Finansial
- Dendam (sakit hati)
- Iseng
- Sebagai pekerjaan (cracker bayaran)
- Dan lain-lain

Keamanan dan Manajemen Perusahaan

Pengelolaan terhadap keamanan dapat dilihat dari sisi pengelolaan resiko (risk management).

Lawrie Brown dalam “**Lecture Notes for Use with Cryptography and Network Security by William Stallings**”

menyarankan menggunakan “*Risk Management Model*” untuk menghadapi ancaman (*managing threats*).

Ada tiga komponen yang memberikan kontribusi kepada Risk, yaitu *Asset*, *Vulnerabilities*, dan *Threats*.

Keamanan dan Manajemen Perusahaan

No	Komponen	Keterangan
1	<i>Assets</i>	hardware, software, dokumentasi, data, komunikasi, lingkungan, manusia
2	<i>Threats</i>	pemakai (<i>users</i>), teroris, kecelakaan (<i>accidents</i>), crackers, penjahat kriminal, nasib (<i>acts of God</i>), intel luar negeri (<i>foreign intelligence</i>)
3	<i>Vulnerabilities</i>	software bugs, hardware bugs, radiasi (dari layar, transmisi), tapping, crosstalk, <i>unauthorized users</i> cetakan, <i>hardcopy</i> atau print out, keteledoran (<i>oversight</i>), cracker via telepon, storage media

Aspek Keamanan Komputer

- **Confidentiality**
Informasi (data) hanya bisa diakses oleh pihak yang memiliki wewenang.
- **Integrity**
Informasi hanya dapat diubah oleh pihak yang memiliki wewenang.
- **Availability**
Informasi tersedia untuk pihak yang memiliki wewenang ketika dibutuhkan.
- **Authentication**
Pihak yang terlibat dengan pertukaran informasi dapat diidentifikasi dengan benar dan ada jaminan bahwa identitas yang didapat tidak palsu.
- **Nonrepudiation**
Pengirim maupun penerima informasi tidak dapat menyangkal pengiriman dan penerimaan pesan.

Aspek Serangan

- **Interruption**

Suatu aset dari suatu sistem diserang sehingga menjadi tidak tersedia atau tidak dapat dipakai oleh yang berwenang. Contohnya adalah perusakan/modifikasi terhadap piranti keras atau saluran jaringan.

- **Interception**

Suatu pihak yang tidak berwenang mendapatkan akses pada suatu aset. Pihak yang dimaksud bisa berupa orang, program, atau sistem yang lain. Contohnya adalah penyadapan terhadap data dalam suatu jaringan.

- **Modification**

Suatu pihak yang tidak berwenang dapat melakukan perubahan terhadap suatu aset. Contohnya adalah perubahan nilai pada file data, modifikasi program sehingga berjalan dengan tidak semestinya, dan modifikasi pesan yang sedang ditransmisikan dalam jaringan.

- **Fabrication**

Suatu pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contohnya adalah pengiriman pesan palsu kepada orang lain.

Aspek Serangan

❑ Hukum alam keamanan komputer

- Tidak ada sistem yang 100% aman
- Keamanan berbanding terbalik dengan kenyamanan

❑ Contoh insiden serangan pada sistem komputer

- Tahun 2004, situs KPU (<http://tnp.kpu.go.id>) dicracked sehingga content situs tersebut berubah
- Tahun 2001, Nasabah klickbca.com disadap identitas accountnya oleh seseorang yang membuat situs mirip (url dan tampilannya) dengan klickbca yang asli
- 10 Maret 1997. Seorang hacker dari Massachusetts berhasil mematikan sistem telekomunikasi di sebuah airport lokal (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>

<http://www.news.com/News/Item/0,4,20226,00.html>

Ancaman Keamanan

❑ Ancaman keamanan pada sistem Komputer antara lain:

- Social engineering
- Keamanan fisik
- Security hole pada sistem operasi dan servis
- Serangan pada jaringan
- DOS attack
- Serangan via aplikasi berbasis web
- Trojan, backdoor, rootkit, keylogger
- Virus, worm

❑ Anatomy of a hack

Langkah-langkah yang umum digunakan oleh hacker

Social Engineering

❑ Ancaman

- Mengaku sebagai penanggung jawab sistem untuk mendapatkan account user
- Mengaku sebagai user yang sah kepada pengelola sistem untuk mendapatkan account
- Mengamati user yang sedang memasukkan password
- Menggunakan password yang mudah ditebak
- Dan lain-lain

❑ Solusi

Mendidik seluruh pengguna sistem dari level manajer sampai operator akan pentingnya keamanan

Keamanan Fisik

❑ Ancaman

- Pembobolan ruangan sistem komputer
- Penyalahgunaan account yang sedang aktif yang ditinggal pergi oleh user
- Sabotase infrastruktur sistem komputer (kabel, router, hub dan lain-lain)
- Dan lain-lain

❑ Solusi

- Konstruksi bangunan yang kokoh dengan pintu-pintu yang terkunci
- Pemasangan screen saver
- Pengamanan secara fisik infrastruktur sistem komputer
 - CPU ditempatkan di tempat yang aman
 - Kabel → direl
 - Router, hub → ditempatkan yang aman dari jangkauan
- Dan lain-lain

Security Hole pad OS dan Service

❑ Ancaman

- Buffer over flow yang menyebabkan local/remote exploit
- Salah konfigurasi
- Instalasi default yang mudah dieexploit
- Dan lain-lain

❑ Pencegahan

■ Sisi Programmer:

Coding dengan teliti dan sabar sehingga kemungkinan kekeliruan coding yang menyebabkan buffer over flow dapat dihindari

■ Sisi User

- Selalu mengikuti informasi bug-bug melalui milis dan situs-situs keamanan (Securityfocus.com dan lain-lain)
- Update..update...dan update!

Kesalahan Konfigurasi

❑ Ancaman

- Sistem dapat diakses dari host yang tidak berhak
- *Privilege* yang dapat dieksploitasi
- Dan lain-lain

❑ Pencegahan

- Pengaturan hak akses host yang ketat
- Pengaturan *privilege* yang ketat
- Dan lain-lain

Default Installation

❑ Ancaman

- Servis yang tidak diperlukan memakan *resource*
- Semakin banyak servis semakin banyak ancaman karena bug-bug yang ditemukan
- Servis-servis jaringan membuka port komunikasi
- Password default diketahui oleh khalayak
- Sample program dapat dieksploitasi
- Dan lain-lain

❑ Pencegahan

- Nyalakan servis yang diperlukan saja
- Konfigurasikan seaman mungkin
- Buang semua yang tidak diperlukan setelah instalasi
- Dan lain-lain

Serangan Pada Jaringan

❑ Ancaman

■ Sniffing (penyadapan)

Sniffer mengubah mode ethernet untuk mendengarkan seluruh paket data pada jaringan yang menggunakan hub sebagai Konsentrator

■ Pencegahan :

Enkripsi (SSL, SSH, PGP, dan lain-lain)

Penggunaan switch sebagai pengganti hub

■ Spoofing (pemalsuan)

IP, MAC Address, DNS, Routing

Pencegahan :

■ Implementasi firewall dengan benar

■ Patch yang mencegah prediksi *sequence number*

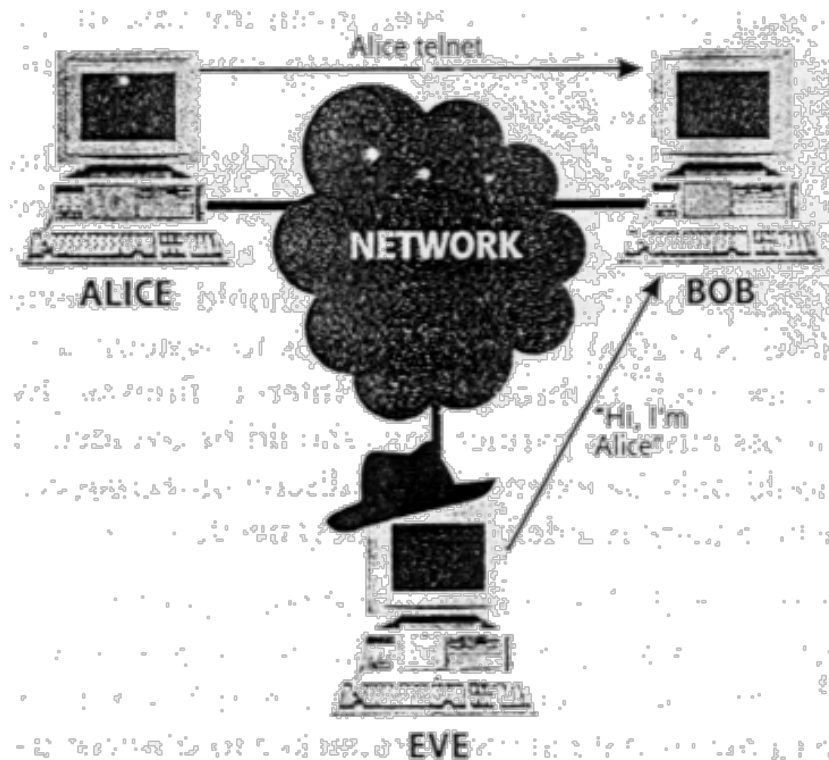
■ Mengeset router agar tidak bisa dilewatkan kecuali melalui rute yang telah ditentukan

■ Dan lain-lain

Serangan Pada Jaringan

❑ Ancaman

- Session hijacking (pembajakan)



Serangan Pada Jaringan

❑ DOS (Denial of Service)

Servis tidak mampu melayani sebagaimana mestinya

❑ Jenis-jenis DOS Attack

- Mematikan servis secara local/remote
- Menguras resource: hardisk, memory, processor, bandwidth

❑ Ancaman mematikan servis secara local

- Membunuh proses pada servis
- Mengubah konfigurasi servis
- Meng*crash*kan servis
- Dan lain-lain

❑ Pencegahan

- Patch terbaru
- Pengaturan *privilege* user dengan tepat
- Deteksi perubahan dengan program *integrity-checking*

Serangan Pada Jaringan

❑ DOS (Denial of Service)

Servis tidak mampu melayani sebagaimana mestinya

❑ Jenis-jenis DOS Attack

- Mematikan servis secara local/remote
- Menguras resource: hardisk, memory, prosessor, bandwidth

❑ Ancaman mematikan servis secara local

- Membunuh proses pada servis
- Mengubah konfigurasi servis
- Meng*crash*kan servis
- Dan lain-lain

❑ Pencegahan

- Patch terbaru
- Pengaturan *privilege* user dengan tepat
- Deteksi perubahan dengan program *integrity-checking*

Serangan Pada Aplikasi Web

❑ Ancaman

- Serangan untuk mendapatkan account

Analisa manajemen account untuk mendapatkan account

Brute force attack

- SQL injection

Query pada aplikasi database

```
select * from user where id=$id;
```

Penyerang memasukan nilai variabel "id" dengan query yang "diinginkan"

```
$id=212; select * from admin
```

Query akhir menghasilkan 2 buah query

```
select * from users where id=212;
```

```
select * from admin;
```

❑ Pencegahan

- Sanitasi nilai input dengan baik di sisi server