Keamanan Jaringan

TKB7351 - Keamanan Informasi & Jaringan
TKB7358 - Keamanan Sistem Informasi

Chalifa Chazar
http://script.id
chalifa.chazar@gmail.com

Keamanan Jaringan

- Secara umum, keamanan jaringan harus dirumuskan/disusun terutama pada ujung-ujung terminal (penerima/pengirim)
- Secara teknik, keamanan bertanggung jawab atas integritas data, kerahasiaan data dan dapat dipercaya penerimanya

Ancaman

- Suatu jaringan terdiri dari banyak titik terminal (*nodes*) yang dihubungkan satu sama lain sehingga membentuk komunikasi
- Fungsi tertentu dilakukan pada terminal-terminal
- Resiko pada masing-masing terminal lebih tinggi dibandingkan jaringannya
  - → Kegagalan jaringan atau putusnya hubungan
  - → Mengakses jaringan oleh user yang tidak memiliki wewenang
  - → Mengganggu atau mengacaukan pengiriman data (mencegat dan memanipulasi data)

Ancaman (2)

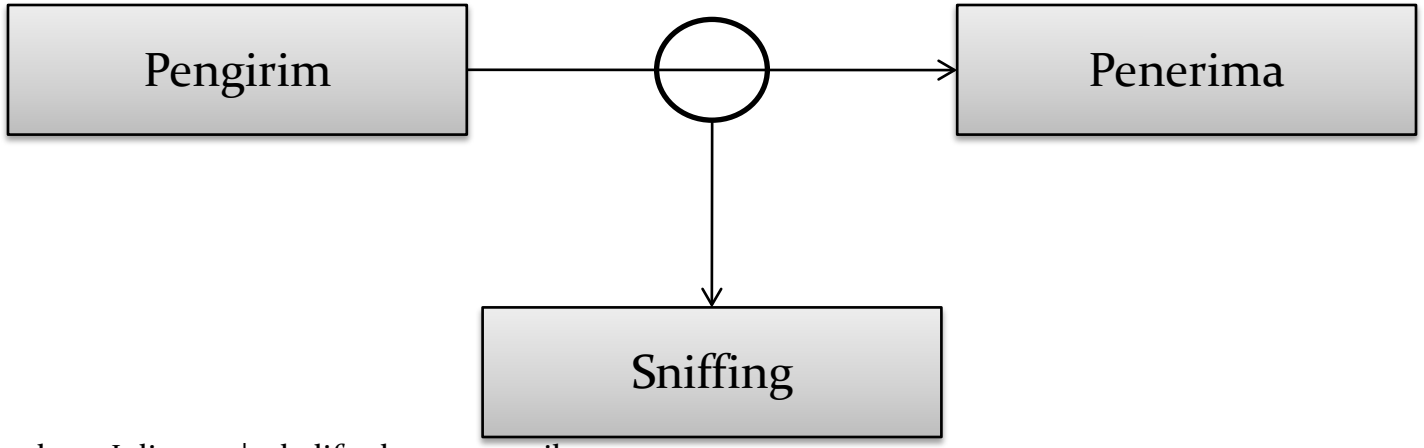
- *Logic* Bom
- Bom Waktu
- Virus
- *Worm*
- *Trojan Horses*
- Spyware
- *Denial of Service*
- *Malicious Java*/Active X
- *Tunneling*
- *Interception* komunikasi

Interception Komunikasi

- Pasif *interception*
- Aktif *interception*

Pasif Interception

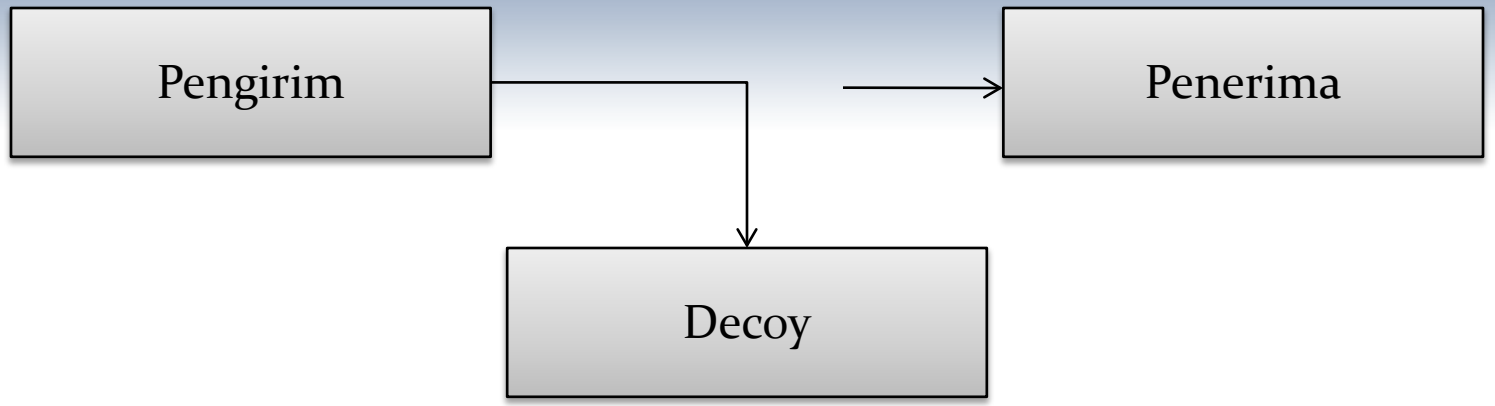
- Biasa disebut **Sniffing**
  - → Memasang program untuk menangkap informasi paket data di jaringan unyuk mengetahui isi data
  - → Kebocoran pada frekuensi radio
  - → Terrestrial microwave interception
  - → Satellite broadcast interception



Aktif Interception

- Biasa disebut **Spoofing**
  - → **Decoy** = hubungan ke penerima diputus dan pengiriman data diterima oleh pihak yang tidak berwenang. Pengirim beranggapan pengiriman data berjalan normal
  - → **Relay** = data yang dikirim diterima oleh pihak yang tidak berwenang dan setelah dimanipulasi, data kembali diteruskan ke pihak berwenang

Decoy =



Relay =

Langkah Pengamanan Jaringan

- Manajemen jaringan
- Enkripsi
- Jaringan cadangan
- Call back
- Firewall

Matriks Ancaman & Tindakan

Tindakan yang perlu dilakukan untuk mengamankan jaringan terhadap Ancaman	1	2	3	4
a. Manajemen jaringan	X			X
b. Enkripsi	X		X	
c. Jaringan cadangan				X
d. Call back	X	X		
e. Firewall	X	X		

Ancaman:

1 = Integritas jaringan kurang (*lack of network integrity*)
2 = penggunaan dengan tidak memiliki otoritas (*unauthorized use*)
3 = pelanggaran kepercayaan (*breach of reliability*)
4 = mengganggu kelancaran operasional (*disruption of continuity*)

Keamanan Jaringan Internet

- Persetujuan dari manajemen/steering committee jika in-house ingin mengakses jaringan eksternal
- Jaringan in-house dan mesin utama untuk produksi tidak boleh diakses langsung oleh jaringan eksternal
- Lingkungan tertentu harus dapat dibuat memiliki pemberian service kepada jaringan eksternal
- Pertanggung jawaban bagi supervisi dan monitoring hubungan dengan jaringan luar

Ancaman Jaringan LAN

- Pengaksesan data produksi, departemen dan pemakai oleh individu yang tidak memiliki wewenang
- Pasif (membaca&melihat data) dan aktif (memanipulasi data) menangkap koneksi
- Menyambung workstation yang tidak otentik ke dalam LAN perusahaan
- Menginstal program yang ilegal
- Pencurian PC atau komponen PC
- Terkontaminasi oleh virus

Matriks Ancaman & Tindakan

Ancaman / Langkah yang diambil	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Akses data/fungsi secara tidak sah	X	X		X	X	X	X	X		X			X		
Pasif dan aktif tapping koneksi													X	X	
Workstation yang tidak sah pada LAN perusahaan							X	X	X				X		
Software yang tidak dikenal/tidak sah	X	X										X			
Pencurian PC /komponen	X							X		X					
Tertular virus	X	X	X								X	X			
Distribusi software	X		X									X			X

Tindakan Pengamanan

A. Physical security
B. Access control
C. Pencegahan virus
D. Enkripsi file
E. “Hard” user authentication (data yang kritis)
F. Enkripsi disk
G. Proteksi boot
H. “Hard” user authentication (laptop, netbook)
I. PC authentication
J. Server diletakkan di ruang terkunci
K. Penguncian ports
L. Fungsi gateway
M. Enkripsi session
N. Enkripsi line
O. Keamanan proses

Keamanan Jaringan LAN

- LAN data harus disimpan di dalam server untuk memudahkan proses backup
- Tindakan keamanan sebanyak mungkin diimplementasikan di tingkat server
- Hanya PC dan software milik perusahaan yang boleh terhubung dengan jaringan LAN
- Notebook dan media penyimpanan eksternal harus disimpan ditermpat terkunci
- PC dan software dapat didistribusikan melalui pihak berwenang
- Informasi bersifat rahasia disimpan di hard disk atau flash disk dalam bentuk ter-enkripsi
- Modem tidak diperbolehkan tersambung di PC yang terkoneksi jaringan LAN perusahaan

</THANKS>

Chalifa Chazar
http://script.id
Email: chalifa.chazar@gmail.com