1. Menentukan Jenis-Jenis Serangan Keamanan Jaringan
2. Konsep Keamanan Berbasis Jaringan

Keamanan jaringan merupakan hal yang sangat penting, sistim keamanan akan berpengaruh pada kinerja system.

Aspek-aspek keamanan komputer meliputi hal-hal sebagai berikut :

1. Privacy/confidentiality, adalah aspek keamanan komputer yang berhubungan dengan usaha untuk menjaga informasi dari pihak yang tidak berhak mengakses.

Privacy biasanya mengarah ke data yang bersifat pribadi

Confidentiality mengarah pada data yang diberikan hanya untuk keperluan tertentu.

1. Integrity, merupakan aspek keamanan computer dengan menekankan informasi yang tidak boleh diubah tanpa seizing pemilik informasi.
2. Authentication, merupakan aspek keamanan yang berhubungan dengan metode untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud.
3. Availability, merupakan aspek keamanan yang berhubungan dengan ketersediaan informasi ketika dibutuhkan.
4. Access control, merupakan aspek keamanan yang berhubungan dengan cara pengaturan akses kepada informasi.
5. Non-repudiation, merupakan aspek keamanan yang menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi
6. Jenis-Jenis Keamanan Jaringan

Jenis kejahatan jaringan dapat digolongkan ke dalam beberapa jenis. Jenis-jenis keamanan dapat diklasifikasikan menjadi empat bagian, yaitu sebagai berikut :

1. Keamanan yang bersifat fisik *(physical securit*y): 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 dimasukkan ke dalam kelas ini.
3. *Denial of servic*e, dilakukan misalnya dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan (yang dapat berisi apa saja karena yang diutamakan adalah banyaknya jumlah pesan).
4. *Syn Flood Attac*k, dimana sistem *(hos*t) yang dituju dibanjiri oleh permintaan sehingga dia menjadi ter-lalu sibuk dan bahkan dapat berakibat macetnya sistem *(han*g).
5. Keamanan yang berhubungan dengan orang (personel), Contoh :
6. Identifikasi user (username dan password)
7. Profil resiko dari orang yang mempunyai akses (pemakai dan pengelola).
8. Keamanan dari data dan media serta teknik komunikasi *(communication*s).
9. Keamanan dalam operasi: Adanya prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga ter-masuk prosedur setelah serangan *(post attack recover*y).
10. Security Attack

Security Attack adalah serangan terhadap system informasi.Menurut William Stalling, serangan (attack) dapat dibagi menjadi berikut :

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 yang 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 web site dengan pesan-pesan yang merugikan pemilik web site.
4. Fabrication:
Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti e-mail palsu ke dalam jaringan komputer.
5. Tool untuk Keamanan Jaringan
6. Sniffer

Merupakan alat yang terhubung dengan jaringan computer dan mendengarkan seluruh lalu lintas jaringan.

1. Scanner

Merupakan alat keamanan yang memeriksa celah-celah keamanan.

1. Firewall

Merupakan sistem atau sekelompok sistem yang menetapkan kebijakan kendali akses antara dua jaringan.