BAB 2 Kemungkinan Ancaman dan Serangan Terhadap Keamanan Jaringan

Saat kita saling terhubung dalam suatu jaringan baik jaringan kecil maupun besar, pasti terdapat ancaman ataupun serangan yang bisa terjadi. Sehingga kita diharuskan untuk lebih berhati-hati saat berkomunikasi menggunakan jaringan. Diantara ancaman atau serangan yang bisa terjadi dari keamanan jaringan adalah :

Serangan fisik terhadap keamanan jaringan

Kebanyakan orang beranggapan bahwa serangan terhadap keamanan jaringan cenderung pada non-hardwarenya saja, tetapi sebenarnya serangan tersebut bisa terjadi pada hardware itu sendiri. Sebagai contoh saat jaringan kita dihack oleh orang lain, maka software baik data, file ataupun aplikasi akan rusak yang bisa juga menyebabkan hardware kita tidak bekerja secara normal, sehingga hardware kita akan mengalami kerusakan.

Serangan fisik apa yang bisa membahayakan jaringan?

o Pencurian perangkat keras komputer atau perangkat jaringan
o Kerusakan pada komputer dan perangkat komunikasi jaringan
o Wiretapping; atau penyadapan
o Bencana alam

Serangan logik terhadap keamanan jaringan

Serangan logic pada keamanan jaringan adalah hal yang paling rawan terjadi, sehingga kita harus lebih memperhatikan lagi security dalam jaringan kita. Diantara serangan yang bisa terjadi adalah :

1. SQL Injection adalah Hacking pada sistem komputer dengan mendapat akses Basis Data pada Sistem
2. DoS (Denial of Service) adalah Serangan pada Sistem dengan mengabiskan Resource pada Sistem.
3. Traffic Flooding adalah Serangan pada keamanan jaringan dengan membanjiri Traffic atau lalu lintas jaringan.
4. Request Flooding adalah Serangan dengan membanjiri banyak Request pada Sistem yang dilayani Host sehingga Request banyak dari pengguna tak terdaftar dilayani oleh layanan tersebut.
5. Deface adalah adalah Serangan pada perubahan tampilan
6. Social Engineering adalah Serangan pada sisi sosial dengan memanfaatkan kepercayaan pengguna. Hal ini seperti fake login hingga memanfaatkan kelemahan pengguna dalam socialmedia.
7. Malicious Code adalah Serangan dengan menggunakan kode berbahaya dengan menyisipkan virus, worm atau Trojan Horse.
    1. Virus: Program merusak yang mereplikasi dirinya pada boot sector atau dokumen.
    2. Worm: Virus yang mereplikasi diri tidak merubah fle tapi ada di memory aktif.
    3. Trojan Horse: Program yang sepertinya bermanfaat padahal tidak karena uploaded hidden program dan scipt perintah yang membuat sistem rentan gangguan.
8. Packet Sniffer adalah Serangan Menangkap paket yang lewat dalam sebuah Jaringan. Peralatan yang dapat memonitor proses yang sedang berlangsung
9. Spoofing; Penggunaan komputer untuk meniru (dengan cara menimpa identitas atau alamat IP).
10. Remote Attack; Segala bentuk serangan terhadap suatu mesin dimana penyerangnya tidak memiliki kendali terhadap mesin tersebut karena dilakukan dari jarak jauh di luar sistemjaringan atau media transmisi
11. Hole; Kondisi dari software atau hardware yang bisa diakses oleh pemakai yang tidak memiliki otoritas atau meningkatnya tingkat pengaksesan tanpa melalui proses otorisasi
12. Phreaking; Perilaku menjadikan sistem pengamanan telepon melemah

Peralatan pemantau kemungkinan ancaman dan serangan terhadap keamanan jaringan "intruder detection system" (IDS). Sistem ini dapat memberitahu administrator melalui e-mail maupunmelalui mekanisme lain. Ada berbagai cara untuk memantau adanya intruder. Ada yang sifatnya aktif dan pasif. IDS cara yang pasif misalnya denganmemonitor logfile. Contoh software IDS antara lain:

- Autobuse, mendeteksi probing dengan memonitor logfile.
- Courtney, mendeteksi probing dengan memonitor packet yang lalu lalang
- Shadow dari SANS