



Networking
Academy



Antonius P.G Manginsela

antonpgm@gmail.com, antonpgm@polimdo.ac.id

Administrasi & Keamanan Jaringan Komputer

Ancaman & Insiden Keamanan Jaringan Komputer

Modul No.2



Topik Bahasan

- Macam – macam ancaman terhadap keamanan jaringan dan cara penanggulangannya.
- Macam – macam accident dan cara penanggulangannya



Serangan pada Sistem Komputer

Serangan pada suatu sistem jaringan komputer sendiri pada dasarnya memiliki tiga gelombang tren utama yaitu (Schneier, 2000):

1. Gelombang pertama adalah ***serangan fisik***. Serangan ini ditujukan kepada fasilitas jaringan, perangkat elektronik, dan komputer.

Sebagai pertahanan terhadap serangan jenis ini biasanya digunakan sistem backup ataupun sistem komputer yang terdistribusi, sehingga mencegah kesalahan di satu titik mengakibatkan seluruh sistem menjadi tak bekerja.



Serangan pada Sistem Komputer

2. Gelombang kedua adalah ***serangan sintaktik***. Serangan ini ditujukan terhadap kerentanan (vulnerability) pada software, celah yang ada pada algoritma kriptografi atau protokol. Serangan Denial of Services (DoS) juga tergolong pada serangan jenis ini.

Serangan jenis inilah yang saat ini paling populer. Tetapi cara penanganannya telah diketahui dan biasanya pihak administrator atau pengguna yang lalai menerapkannya.



Serangan pada Sistem Komputer

3. Gelombang ketiga adalah **serangan semantik**.

Serangan jenis ini memanfaatkan arti dari isi pesan yang dikirim. Dengan kata lain adalah menyebarkan disinformasi melalui jaringan, atau menyebarkan informasi tertentu yang mengakibatkan timbulnya suatu kejadian. Pada dasarnya banyak pengguna cenderung percaya apa yang mereka baca. Sering kali keluguan mempercayai berita ini disalahgunakan pihak tertentu untuk menyebarkan isu-isu yang menyesatkan.



Ancaman Keamanan Sistem Komputer

- Terjadi karena terjadinya serangan dari dalam atau lokal komputer (local attack), karena melakukan akses ke Internet,
- Adanya serangan hacker (Hacker attack). Serangan lokal (Local attack) atau console hacking adalah usaha rekan kita sendiri untuk mengakses data secara tidak baik.



Ancaman Keamanan Sistem Komputer

- Bahaya jaringan yang terhubung ke jaringan publik dibagi atas dua bagian besar:
 - Remote Controlled PC ,
 - Infeksi Digital: virus dan Trojan.



Definisi Keamanan Sistem

- Untuk menjamin sumber daya tidak digunakan atau dimodifikasi orang yang tidak berhak.
- Tindakan pengamanan termasuk masalah teknis, manajerial, legalitas dan politis
- Keamanan sistem terdiri atas :
 - Keamanan External, berkaitan dengan pengamanan fasilitas komputer dari penyusup dan bencana seperti kebakaran, banjir dlsb.
 - Keamanan Interface Pemakai, berkaitan dengan identifikasi pemakai sebelum pemakai diijinkan mengakses program dan data yang disimpan
 - Keamanan Internal, adalah pengamanan beragam kendali yang dibangun pada perangkat keras dan SO yang menjamin yang handal dan tidak cacat untuk menjamin integritas program dan data.



Masalah-masalah keamanan

1. Kehilangan data (Data Losses):

- a. Bencana : Kebakaran, Banjir, Gempa Bumi, Perang, Kerusuhan, Gangguan Binatang.
- b. Kesalahan perangkat (Lunak&Keras) : Bugs, Saluran Komunikasi, Pemrosesan Tidak Berfungsi, Media penyimpanan yang rusak
- c. Kelalaian Manusia : Input Data, Pemasangan Media Penyimpanan yang salah, Eksekusi Program Salah, Kehilangan media penyimpanan

Tindakan Pencegahan : Menyediakan beberapa cadangan penyimpanan data (back-up) yang terpisah dengan data on-line.)



Masalah-masalah keamanan

2. Penyusupan (Intruder):

- a. Penyusup pasif, membaca data yang tak diotorisasi
- b. Penyusup aktif, mengubah data yang tak diotorisasi

Kategori Penyusupan :

1. Non-Teknis – (Mengintip/Lirikan Mata) pada saat input data/ password
2. Penyadapan oleh orang dalam
3. Hacker untuk berbagai macam tujuan
4. Intelejen (Spionase militer / bisnis)



Ancaman-ancaman keamanan

Tujuan adalah agar aspek-aspek berikut ini tercapai :

1. Kerahasiaan (Secrecy)

Adalah keterjaminan bahwa informasi di sistem komputer hanya dapat diakses oleh pihak-pihak yang diotorisasi dan modifikasi tetap menjaga konsistensi dan keutuhan data di sistem.

2. Integritas (Integrity)

Adalah jaminan bahwa sumber daya sistem komputer hanya dapat dimodifikasi oleh pihak-pihak yang berhak.

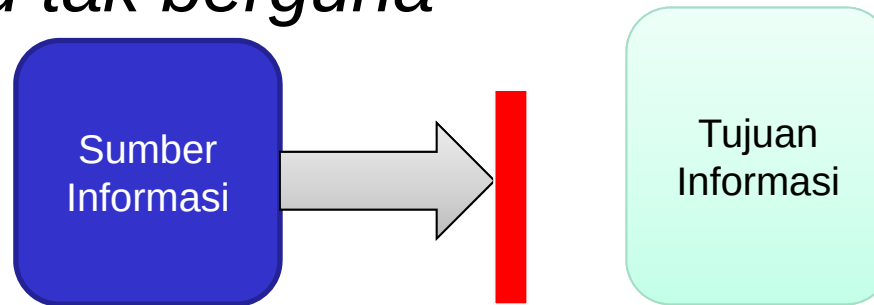
3. Ketersediaan (Availability)



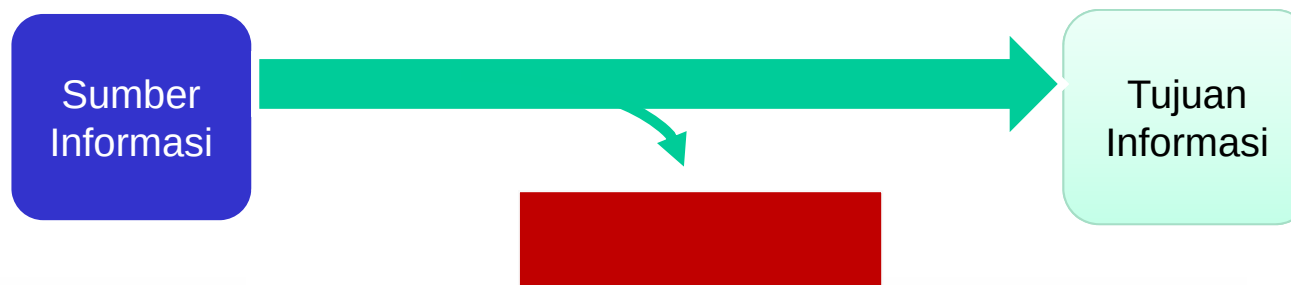
Ancaman-ancaman keamanan

Berdasarkan fungsi :

1. **Interupsi**, *sistem komputer dihancurkan atau menjadi tidak tersedia atau tak berguna*



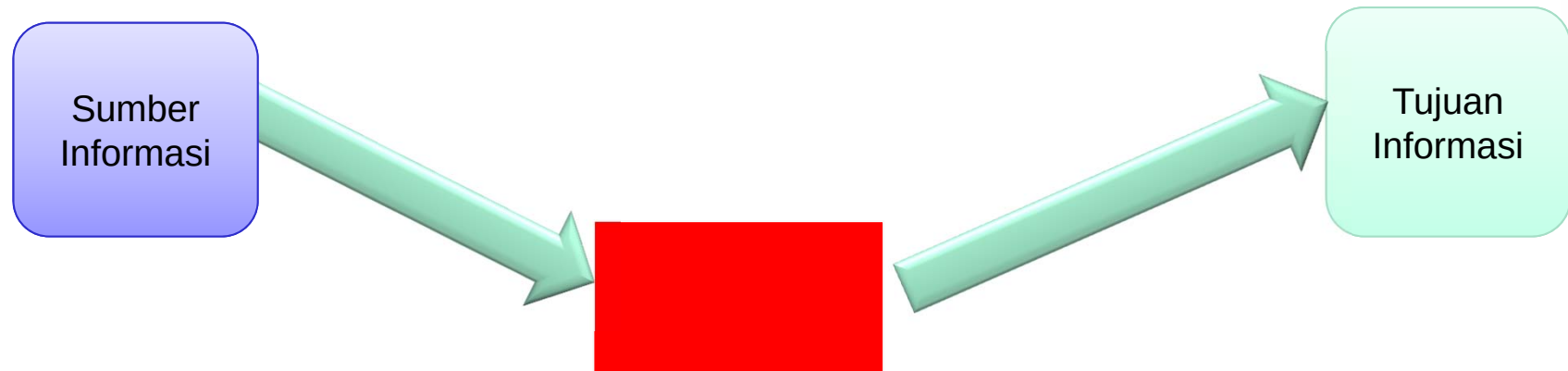
2. **Intersepsi**, *pihak yg tidak berwenang dapat mengakses sistem, mengancam kerahasiaan. Dapat berupa orang atau program komputer.*



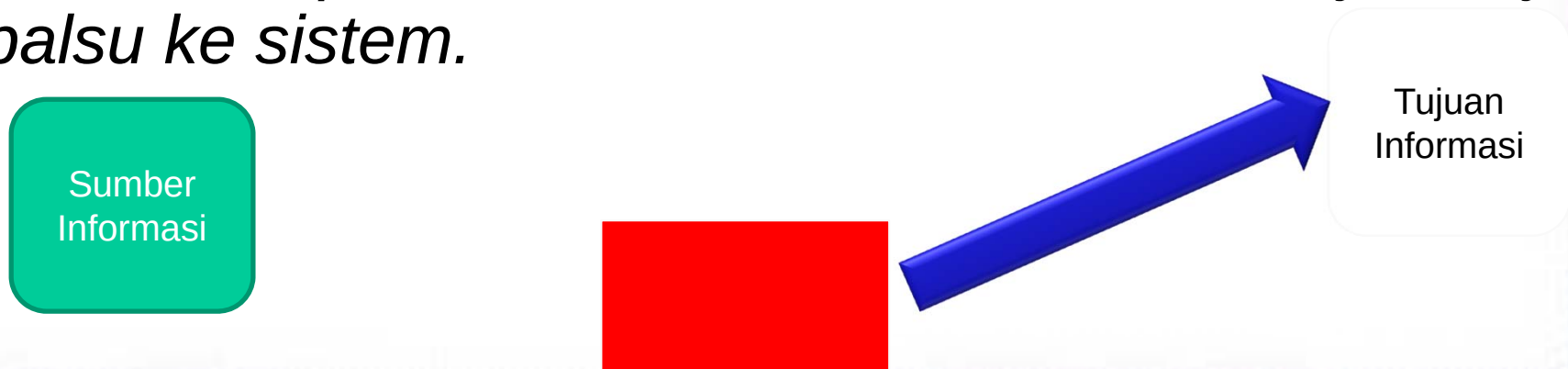


Ancaman-ancaman keamanan

1. **Modifikasi**, *pihak tak berhak bukan saja mengakses sistem tetapi juga merusak sistem / sumber daya.*



2. **Fabrikasi**, *pihak tak berhak memasukkan objek-objek palsu ke sistem.*





Bentuk Ancaman

- **Sniffer**

Peralatan yang dapat memonitor proses yang sedang berlangsung

- **Spoofing**

Penggunaan komputer untuk meniru (dengan cara menimpa identitas atau alamat IP).

- **Remote Attack**

Segala bentuk serangan terhadap suatu sistem/komputer dimana penyerangnya memiliki kendali terhadap mesin tersebut karena dilakukan dari jarak jauh diluar sistem jaringan atau media transmisi

- **Hole**

Kondisi dari software atau hardware yang bisa diakses oleh pemakai yang tidak memiliki hak / otoritas atau meningkatnya tingkat pengaksesan tanpa melalui proses otorisasi



Bentuk Ancaman

- **Phreaking**

Perilaku menjadikan sistem pengamanan telepon lemah

- **Hacker**

Orang yang secara diam-diam mempelajari sistem yang biasanya sukar dimengerti untuk kemudian mengelolanya dan men-share hasil ujicoba yang dilakukannya.

Hacker tidak merusak sistem

- **Craker**

Orang yang secara diam-diam mempelajari sistem dengan maksud jahat

Muncul karena sifat dasar manusia yang selalu ingin membangun(salahsatunya merusak)



Bentuk Ancaman

- **Cracker**

- Ciri-ciri cracker :

- Bisa membuat program C, C++ atau perl
 - Memiliki pengetahuan TCP/IP
 - Terhubung ke internet untuk menjalankan aksinya
 - Melakukan aksinya pada malam hari, dengan alasan waktu yang memungkinkan, jalur komunikasi tidak padat, tidak mudah diketahui orang lain



Bentuk Ancaman

- **Cracker**

Penyebab cracker melakukan penyerangan:

- *Spite*, kecewa, balas dendam
- *Sport*, petualangan
- *Profit*, mencari keuntungan dari imbalan oranglain
- *Stupidity*, mencari perhatian
- *Cruriosity*, rasa ingin tahu
- *Politics*, alasan politis



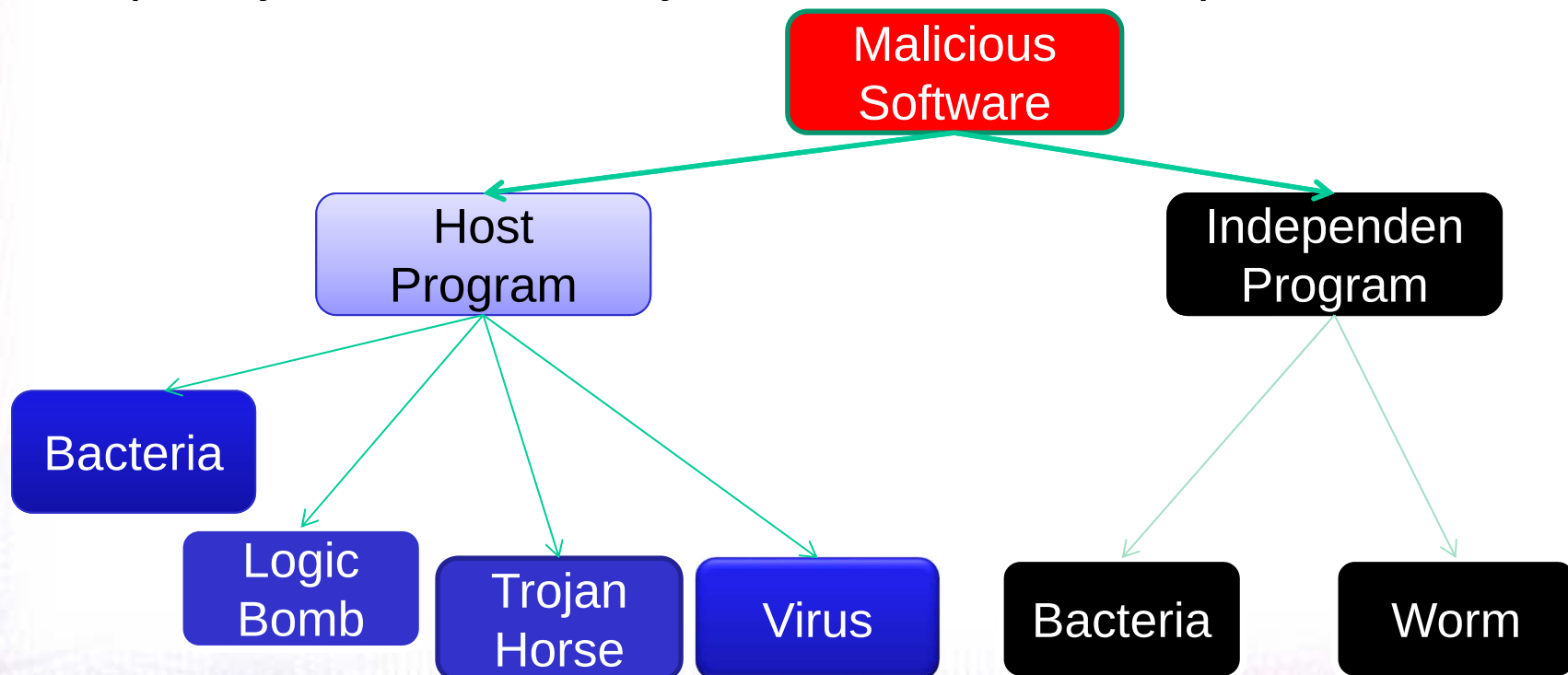
Ancaman Keamanan Sistem Komputer

- *Cracker* adalah seseorang yang masuk ke sistem orang lain, biasanya di jaringan komputer, mem-bypass kata Sandi atau lisensi program komputer, atau secara sengaja melawan keamanan komputer.
- Cracker dapat mengerjakan hal tertentu untuk keuntungan, maksud jahat, atau karena sebab lainnya karena ada tantangan.
- Beberapa proses pembobolan dilakukan untuk menunjukkan kelemahan keamanan sistem



Ancaman Perangkat Lunak (Malicious Program)

1. Program yang memerlukan host (Inang), dimana program ini tidak dapat mandiri secara independen dari suatu program aplikasi, utilitas atau program sistem
2. Program yang tidak memerlukan host (Inang), yaitu program yang dapat dijadwalkan dan dijalankan oleh sistem operasi.





VIRUS

Definisi :

Sebuah program yang dirancang untuk menyebarkan diri ke program atau menginfeksi file lain, sistem, harddisk, floppy disk, flash disk, dengan melakukan perubahan atau penghancuran file atau menyebabkan sistem menjadi crash.

- Sebuah komputer terinfeksi virus apabila terjadi pemanggilan/pembukaan program/file bervirus oleh sistem. Saat program/file bervirus dipanggil/dibuka, maka virus akan mengambil satu atau lebih *segmen* di dalam memori untuk melakukan penyebaran.

-



VIRUS

Empat langkah kerja virus yaitu:

1. Development, Tahap penetrasi.

Tahap dimana komputer yang menjalankan/membuka program/file bervirus hingga menetap di memori. Jangka waktu yang digunakan pada tahap ini bergantung dari tipe atau jenis virus, karena ada beberapa virus yang dirancang melakukan penetrasi secara cepat, tetapi ada pula yang dirancang dengan memperhitungkan perubahan waktu



VIRUS

2. Tahap *propagation*.

Tahapan dimana virus akan berusaha menginfeksi program lain.

Target infeksi juga bisa mengarah ke sistem operasi dan *boot block/Master Boot Record (MBR)*.

Tahap ini akan cepat terjadi pada komputer yang tidak memiliki sistem keamanan.



VIRUS

3. Tahap *triggering*.

Tahap mulai aktifnya virus dalam usaha penyebaran diri.

Tahap ini bisa digambarkan seperti proses pembelahan sel.

Untuk tipe virus yang memerhitungkan waktu jam dan tanggal, maka proses *triggering* terjadi pada jam atau tanggal yang ditentukan oleh perancangannya.



VIRUS

4. Tahap *Damage*.

Pada tahap ini virus menunjukkan betapa berbahayanya virus itu.

Hal ini tidak bisa diprediksi seberapa banyak kerusakan yang ditimbulkan oleh virus.

Tetapi hal ini bergantung dari kekuatan dari virus itu sendiri. Mulai dari kerusakan ringan seperti pesan-pesan adanya virus, hingga kerusakan berat seperti rusaknya atau terhapusnya file-file sistem.

Bisa menyebabkan hancurnya struktur *boot block* (*MBR*).



Trojan Horse

Trojan horse datang dengan kejutan tersembunyi yang diharapkan oleh programmernya tetapi secara total tidak diduga oleh pengguna komputer.

Dirancang untuk membuat kerusakan atau keanehan pada sistem komputer tetapi disamarkan, seolah-olah semuanya bekerja normal.

Berbeda dengan virus, *trojan horse* tidak melakukan penyebaran diri, *tetapi trojan horse* dapat menyebabkan kerusakan yang serius pada sebuah komputer.



Worm

Tidak menyebarkan diri dari satu file ke file lainnya, tetapi *worm* menyebarkan diri untuk menginfeksi dari satu komputer ke komputer yang lain.

Dirancang untuk melakukan infeksi melalui medium jaringan seperti *TCP/IP*, *E-Mail*, dan lain-lain.

Worm lebih tertarik menginfeksi komputer dalam jaringan sebanyak-banyaknya dari pada menginfeksi file-file pada sebuah komputer.

Sekali *worm* menginfeksi sebuah sistem, *worm* akan melakukan penyebaran diri untuk menginfeksi sistem lain yang ada dalam sebuah jaringan.



Worm

- *Worm* memanfaatkan *ActiveX* atau teknologi java yang bekerja pada sistem operasi. Kebanyak aplikasi-aplikasi pada sistem operasi **Microsoft Windows** dan **MacOS** melibatkan *ActiveX* atau teknologi java seperti *mail-client*, *web browser*, dan lain-lain.
- Walaupun hanya melakukan *browsing* saja, sangat memungkinkan terbawanya *worm* atau *trojan horse* ke dalam sistem komputer apabila sistem keamanan tidak diperhatikan.



Hoax

- Sebuah email yang berisi provokasi untuk meyakinkan bahwa tidak ada ancaman virus, atau menakut-nakuti agar email tersebut di-*forward* ke orang lain.
- Proses *forward* ini akan menyebabkan jaringan mengalami *traffic* yang tinggi, sehingga sistem jaringan bisa terganggu.
- Hal ini akan sangat terasa apabila semakin banyak orang melakukan *forwarding email*, apalagi dalam lingkungan jaringan yang besar.



Spyware

- Komponen aplikasi yang tersembunyi yang umumnya terdapat pada program-program *freeware (demo)* atau *shareware*.
- Sekali *spyware* terinstal pada komputer, maka *spyware* akan melakukan monitor aktifitas pengguna komputer secara *underground* (tanpa diketahui pengguna).
- *Spyware* bekerja mulai dari sekedar menampilkan pesan-pesan promosi melalui internet hingga pengumpulan informasi-informasi yang ada dalam sistem.



Malware

- *Hardware* atau software yang disisipkan melalui celah sistem keamanan untuk tujuan yang berbahaya.
- *Malware* kependekan dari *Malicious Software* adalah sebuah istilah yang mencakup beberapa program yang dirancang untuk menyerang, menurunkan, dan menghambat kinerja sistem atau jaringan.
- *Malware* bisa berupa *virus*, *trojan*, *worm*, *malicious active content*, atau *denial of service attacks (DOS)*.
- Kasus invasi pribadi untuk kepentingan penipuan atau pencurian identitas melalui software yang disisipkan pada sebuah sistem juga termasuk *malware*.



Adware

- Mirip dengan *spyware*. Adware memberikan pesan iklan yang memungkinkan lebih sesuai dengan yang diharapkan.
- *Adware* juga merupakan komponen aplikasi yang tersembunyi dari program *freeware (demo)* atau *shareware*.
- *Adware* yang sudah terinstal dalam sistem biasanya akan bekerja saat program utamanya dijalankan



Pencegahan

1. Serangan virus, biasanya diinstal software antivirus dalam sistem operasi
2. Melakukan update antivirus
3. Hati-hati dalam melakukan transformasi file baik melalui *floppy disk*, *harddisk*, *flash disk*, jaringan atau yang lain.
4. Individual *firewall* sebagai salah satu pelindung bagi komputer terhubung dengan jaringan
5. Berhati-hati dalam penggunaan e-mail client
6. Penggunaan software *web browser* yang dilengkapi sistem keamanan seperti *popup blocker* sangat dianjurkan.
7. Meng-*update* sistem keamanan sistem operasi dapat memperkecil resiko penyebaran virus.



Mengetahui Gangguan Keamanan & Virus

Indikasi adanya virus dalam sistem dapat dirasakan, antara lain:

- Kinerja sistem kadang lambat kadang normal
- Sering terjadi *not responding* atau aplikasi beku.
- Sering hard dan *restart* dalam beberapa menit.
- Sering *restart* sendiri dan tidak bisa *booting* normal.
- Aplikasi tidak bekerja normal.
- *Disk* atau *disk-drive* sibuk seperti selalu ada yang mengaksesnya.
- Proses pencetakan tidak bekerja normal.
- Sering muncul pesan *error*.
- Sistem seolah-olah sibuk.



Recovery / Perbaikan

1. Perbaikan Akibat Serangan Virus

- a. Lakukan *backup* data.
- b. *Scan harddisk* yang terinfeksi dengan komputer lain yang bebas virus.
- c. Setelah *scanning* terjadi kerusakan sistem, sehingga sistem tidak bisa bekerja, lakukan instalasi ulang.
- d. Scan data yang di-*backup* dengan komputer yang bebas virus.
- e. Instal antivirus terbaru atau *update* program terbaru.
- f. Update database program antivirus.
- g. Update sistem keamanan sistem operasi.



Serangan Sistem Jaringan Komputer

1. Port Scanning

- ❑ Dilakukan sebagai tahap awal sebuah serangan. Untuk dapat melakukan penyerangan, seorang *cracker* perlu *mengetahui aplikasi apa saja yang berjalan dan siap menerima koneksi dari lokasinya berada.*

2. DOS/DDOS (*Denial of Services dan Distributed Denial of Services*)

- ❑ *Serangan yang bertujuan untuk menghabiskan sumber daya sebuah peralatan jaringan komputer sehingga layanan jaringan komputer menjadi terganggu*



Serangan Sistem Jaringan Komputer

3. Packet Sniffing

- ❑ Serangan dengan cara mendengarkan seluruh paket yang lewat pada sebuah media komunikasi, baik itu media kabel maupun radio. Setelah paket didapat, kemudian disusun ulang sehingga data yang dikirimkan oleh sebuah pihak dapat dicuri oleh pihak yang tidak berwenang.

4. IP Spoofing dan DNS Forgery

- ❑ Serangan yang bertujuan untuk menipu seseorang. Dilakukan dengan cara mengubah alamat asal sebuah paket, sehingga dapat melewati perlindungan *firewall* dan *menipu host penerima data*



Tugas Individu

1. Uraikan / membuat ringkasan penjelasan dari masing-masing jenis serangan terhadap sistem jaringan komputer.
2. Uraikan / membuat ringkasan langkah-langkah perlindungan menghadapi serangan terhadap sistem jaringan komputer.

Hasil / Tugas dan materi modul 2 ini adalah bahan tes sumatif individual pertemuan berikut.



Aspek pengamanan sistem

1. Rancangan sistem, tidak harus bergantung pada kerahasiaan rancangan mekanisme pengamanan.
2. Dapat diterima oleh banyak pemakai tanpa mengganggu kerja pemakai dan memenuhi kebutuhan otorisasi pengaksesan.
3. Pemeriksaan otoritas 1 kali pada waktu akses
4. Kewenangan serendah mungkin sesuai tugas dan tanggung jawab pemakai.
5. Mekanisme yang ekonomis, sederhana dan seragam hingga memudahkan verifikasi.



Langkah-Langkah Pengamanan

Berdasarkan lapisan TCP/IP:

1. Layer 2 (Link)

- Menjaga titik akses : Fisik (Gedung, Switch, Access Point) & Logika (Protokol 802.1x, Mac-Address, *WEP (Wired Equivalent Privacy)* dan *WPA (Wi-Fi Protected Access)*)

2. Layer 3 (Internetwork)

- Semua peralatan komputer aktif harus memiliki sebuah nomor IP unik yang akan menjadi identitasnya di jaringan komputer, dan *Port Number* sebagai saluran protokol yang digunakan.



Langkah-Langkah Pengamanan

3. Layer 4 & 5

Mengamankan saluran data yang dikirimkan :

- **VPN** (Virtual Private Network)

4. Layer Application (5, 6 & 7)

- **SSL (*Secure Socket Layer*)** adalah sebuah protokol yang bekerja tepat di bawah sebuah aplikasi jaringan komputer.
- ***Application Firewall*** (Paket Filtering) sebuah sistem yang akan memeriksa seluruh data yang akan diterima oleh sebuah aplikasi jaringan komputer. Paket-paket data yang diterima dari pihak lain akan disatukan untuk kemudian diperiksa apakah data yang dikirimkan berbahaya atau tidak.

Langkah-langkah Pengamanan



Untuk mempermudah pengamanan, pemeliharaan serta meningkatkan kompatibilitas antar berbagai peralatan , maka langkah-langkah dibagi sesuai dengan lapisan TCP/IP :

1. **Link** (Lapisan OSI 1 dan 2), Ethernet, Wi-Fi. Implementasi untuk lapisan ini biasanya terletak pada device driver ataupun chipset firmware.
2. **Internetwork** (Lapisan OSI 3), lapisan yang berfungsi untuk mengirimkan sebuah paket ke tujuan melalui sebuah kelompok jaringan komputer. Jugamengatur bagaimana sebuah paket akan sampai tujuan melalui beberapa kelompok jaringan komputer apabila dibutuhkan.
3. **Transport** (Lapisan OSI 4 dan 5), TCP, UDP dan RTP
4. **Applications** (Lapisan OSI 5 sampai dengan 7): HTTP, FTP dan DNS.



Mekanisme pertahanan

1. **Intrusion Detection System (IDS) & Intrusion Prevention System (IPS)** adalah sistem yang banyak digunakan untuk mendeteksi dan melindungi sebuah sistem keamanan dari serangan oleh pihak luar maupun dalam.
2. **Network Topology**, Pembagian kelompok komputer sesuai dengan tugas & fungsinya. Lihat contoh [Topologi Jaringan Intranet Kampus](#).
3. **Port Scanning**, Aplikasi yang memeriksa port yang terbuka yang menunjukkan adanya aplikasi jaringan komputer yang siap menerima koneksi. Aplikasi ini dapat menjadi pintu masuk penyerang ke dalam sistem jaringan komputer.
4. **Packet Finger Printing**, sebuah peralatan *fingerprinting* akan melihat bagaimana peralatan jaringan komputer atau sistem operasi yang bersangkutan memberikan nilai-nilai awal pada beberapa bagian di *header IP*.
5. **Security Information Management**, berfungsi untuk menyediakan seluruh informasi yang terkait dengan pengamanan jaringan komputer secara terpusat.



Studi Kasus & Tugas Kelompok

Pilih salah satu perencanaan jaringan dan pengelolaan keamanan jaringan komputer dari 6 pilihan berikut ini:

1. Hotel Bintang 3 dengan layanan Hotspot Internet untuk tamu hotel (50 Kamar), Web server, Email Server dan LAN perusahaan.
2. Perusahaan Pengalengan Ikan dengan layanan Internet dan Intranet untuk 5 departemen.
3. Sekolah dengan layanan Internet dan LAN untuk jaringan lokal di kantor sekolah dan Lab.Komputer.
4. Perusahaan Penjualan Tiket Pesawat & Kapal Laut dengan layanan internet dan booking tiket lewat internet.
5. Restoran dengan layanan web site, hotspot dan internet café.
6. Jaringan RT/RW net untuk 50 rumah dengan menggunakan Speedy dari Telkomnet dan Access Point dan kabel ke rumah-rumah klien.



Studi Kasus & Tugas Kelompok

Bentuk Laporan:

1. Denah lokasi dan organisasi.
2. Topologi Jaringan Fisik
3. Topologi Jaringan Logika
4. Perencanaan Keamanan Jaringan Komputer:
 - Sesuai dengan Lapisan TCP/IP
 - Secara Fisik dan Logika
 - Prosedur Organisasi.



Penutup

Semakin aman sistem yang anda miliki, maka sistem komputer akan menjadi semakin merepotkan

Terima Kasih