BAB IV
Mengamankan Sistem Informasi

Pendahuluan

- Pada umunya, pengamanan dapat dikategorikan menjadi dua jenis: pencegahan (*preventif*) dan pengobatan (*recovery*). Usaha pencegahan dilakukan agar sistem informasi tidak memiliki lubang keamanan, sementara usaha-usaha pengobatan dilakukan apabila lubang keamanan sudah dieksploitasi.

- Pengamanan sistem informasi dapat dilakukan melalui beberapa layer yang berbeda. Misalnya di layer "transport", dapat digunakan "*Secure Socket Layer*" (SSL). Metoda ini umum digunakan untuk server web. Secara fisik, sistem anda dapat juga diamankan dengan menggunakan "firewall" yang memisahkan sistem anda dengan Internet. Penggunaan teknik enkripsi dapat dilakukan di tingkat aplikasi sehingga data-data anda atau e-mail anda tidak dapat dibaca oleh orang yang tidak berhak.

Mengatur akses (Access Control)

- Salah satu cara yang umum digunakan untuk mengamankan informasi adalah dengan mengatur akses ke informasi melalui mekanisme "*authentication*" dan "*access control*". Implementasi dari mekanisme ini antara lain dengan menggunakan "*password*".

- Di sistem UNIX dan Windows NT, untuk menggunakan sebuah sistem atau komputer, pemakai diharuskan melalui proses ***authentication*** dengan menuliskan **"*userid*" dan "*password*"**. Informasi yang diberikan ini dibandingkan dengan userid dan password yang berada di sistem. Apabila keduanya **valid**, pemakai yang bersangkutan **diperbolehkan menggunakan sistem**. Apabila ada yang salah, pemakai tidak dapat menggunakan sistem.

Mengatur akses (Access Control)

- Informasi tentang kesalahan ini biasanya dicatat dalam **berkas *log***. Besarnya informasi yang dicatat bergantung kepada konfigurasi dari sistem setempat. Misalnya, ada yang menuliskan informasi apabila pemakai **memasukkan *userid* dan *password* yang salah sebanyak tiga kali**. Ada juga yang langsung menuliskan informasi ke dalam berkas *log* meskipun baru satu kali salah. Informasi tentang waktu kejadian juga dicatat. Selain itu asal hubungan (*connection*) juga dicatat sehingg administrator dapat memeriksa keabsahan hubungan.

- Setelah proses *authentication*, pemakai diberikan akses sesuai dengan level yang dimilikinya melalui sebuah *access control*. *Access control* ini biasanya dilakukan dengan mengelompokkan pemakai dalam "group". Ada group yang berstatus pemakai biasa, ada tamu, dan ada juga *administrator* atau *super user* yang memiliki kemampuan lebih dari group lainnya. Pengelompokan ini disesuaikan dengan kebutuhan dari penggunaan sistem anda. Di lingkungan kampus mungkin ada kelompok mahasiswa, staf, karyawan, dan administrator. Sementara itu di lingkungan bisnis mungkin ada kelompok *finance*, *engineer*, *marketing*, dan seterusnya.

Memilih password

- Dengan adanya kemungkinan password ditebak, misalnyadengan menggunakan program password cracker, maka memilih password memerlukan perhatian khusus. Berikut ini adalah daftar hal-hal yang sebaiknya tidak digunakan sebagai password.
  - Nama anda, nama istri / suami anda, nama anak, ataupun nama kawan.
  - Nama komputer yang anda gunakan.
  - Nomor telepon atau plat nomor kendaran anda.
  - Tanggal lahir.
  - Alamat rumah.
  - Nama tempat yang terkenal.
  - Kata-kata yang terdapat dalam kamus (bahasa Indonesia maupun bahasa
  - Inggris).
  - Password dengan karakter yang sama diulang-ulang.
  - Hal-hal di atas ditambah satu angka.

Menutup servis yang tidak digunakan

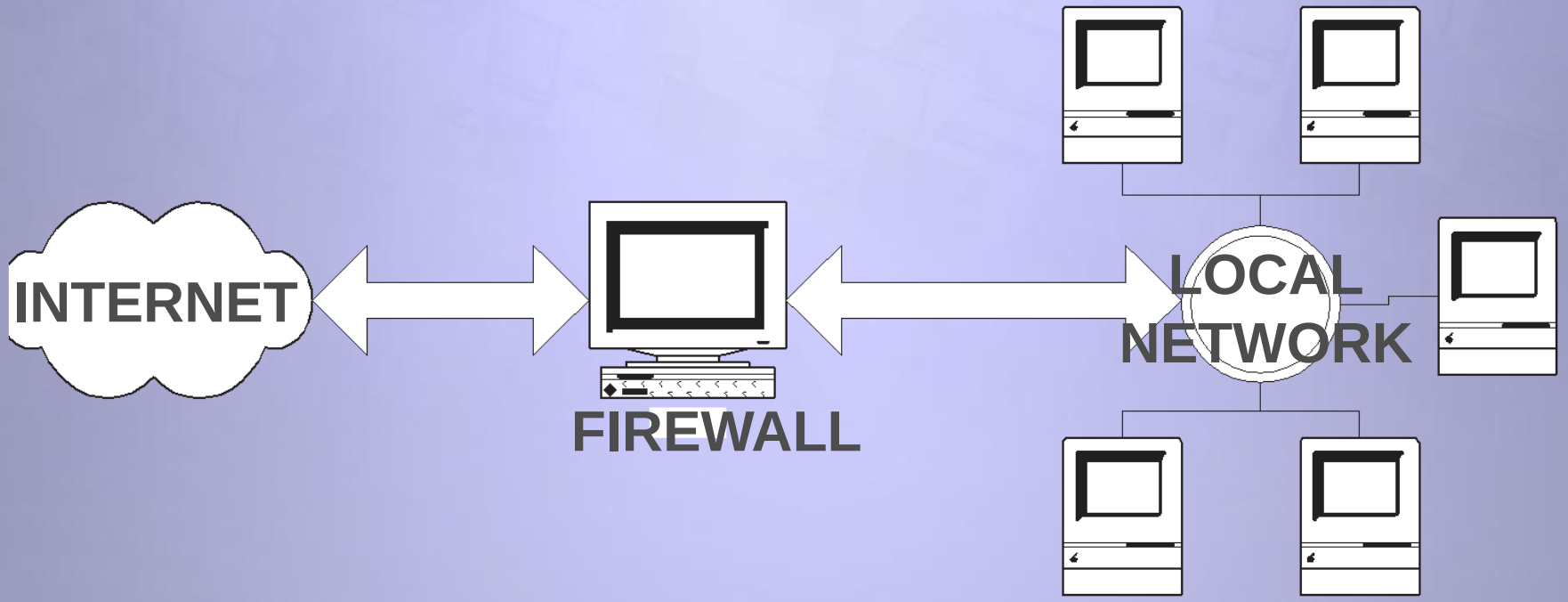
- Seringkali sistem (perangkat keras dan/atau perangkat lunak) diberikan dengan beberapa servis dijalankan sebagai *default*. Sebagai contoh, pada sistem UNIX servis-servis berikut sering dipasang dari vendornya: *finger*, *telnet*, *ftp*, *smtp*, *pop*, *echo*, dan seterusnya. Servis tersebut tidak semuanya dibutuhkan. Untuk mengamankan sistem, servis yang tidak diperlukan di server (komputer) tersebut sebaiknya dimatikan.
- Sudah banyak kasus yang menunjukkan *abuse* dari servis tersebut, atau ada lubang keamanan dalam servis tersebut akan tetapi sang administrator tidak menyadari bahwa servis tersebut dijalankan di komputernya.
- *Deamon* – service yang dijalankan saat sistem berjalan.

Memasang Proteksi

- Untuk lebih meningkatkan keamanan sistem informasi, proteksi dapat ditambahkan. Proteksi ini dapat berupa filter (secara umum) dan yang lebih spesifik adalah firewall. Filter dapat digunakan untuk memfilter e-mail, informasi, akses, atau bahkan dalam level packet. Sebagai contoh, di sistem UNIX ada paket program "*tcpwrapper*" yang dapat digunakan untuk membatasi akses kepada servis atau aplikasi tertentu. Misalnya, servis untuk "*telnet*" dapat dibatasi untuk untuk sistem yang memiliki nomor IP tertentu, atau memiliki domain tertentu. Sementara firewall dapat digunakan untuk melakukan filter secara umum.

FIREWALL

- Firewall merupakan sebuah perangkat yang diletakkan antara Internet dengan jaringan internal (Lihat Figure 4.1 on page 65). Informasi yang keluar atau masuk harus melalui firewall ini.



FIREWALL

- Tujuan utama dari firewall adalah untuk menjaga (*prevent*) agar akses (ke dalam maupun ke luar) dari orang yang tidak berwenang (*unauthorized access*) tidak dapat dilakukan. Konfigurasi dari firewall bergantung kepada kebijaksanaan (*policy*) dari organisasi yang bersangkutan, yang dapat dibagi menjadi dua jenis:
  - apa-apa yang tidak diperbolehkan secara eksplisit dianggap tidak diperbolehkan (*prohibitted*)
  - apa-apa yang tidak dilarang secara eksplisit dianggap diperbolehkan (*permitted*)
- Firewall bekerja dengan mengamati paket IP (Internet Protocol) yang melewatinya. Berdasarkan konfigurasi dari firewall maka akses dapat diatur berdasarkan IP address, port, dan arah informasi. Detail dari konfigurasi bergantung kepada masing-masing firewall.
- Firewall dapat berupa sebuah perangkat keras yang sudah dilengkapi dengan perangkat lunak tertentu, sehingga pemakai (administrator) tinggal melakukan konfigurasi dari firewall tersebut. Firewall juga dapat berupa perangkat lunak yang ditambahkan kepada sebuah server (baik UNIX maupun Windows NT), yang dikonfigurasi menjadi firewall. Dalam hal ini, sebetulnya perangkat komputer dengan prosesor Intel 80486 sudah cukup untuk menjadi firewall yang sederhana.

FIREWALL

- Firewall biasanya melakukan dua fungsi; fungsi (IP) filtering dan fungsi proxy. Keduanya dapat dilakukan pada sebuah perangkat komputer (device) atau dilakukan secara terpisah.

- Fungsi proxy dapat dilakukan oleh berbagai software tergantung kepada jenis proxy yang dibutuhkan, misalnya web proxy, rlogin proxy, ftp proxy dan seterusnya. Di sisi client sering kalai dibutuhkan software tertentu agar dapat menggunakan proxy server ini, seperti misalnya dengan menggunakan SOCKS. Beberapa perangkat lunak berbasis UNIX untuk proxy antara lain:
  - *Socks:* proxy server oleh NEC Network Systems Labs
  - *Squid*: web proxy server

- Satu hal yang perlu diingat bahwa adanya firewall bukan menjadi jaminan bahwa jaringan dapat diamankan seratus persen. Firewall tersebut sendiri dapat memiliki masalah. Sebagai contoh, Firewall Gauntlet yang dibuat oleh Network Associates Inc. (NAI) mengalami masalah1 sehingga dapat melewatkan koneksi dari luar yang seharusnya tidak boleh lewat. Padahal Gauntlet didengung-dengungkan oleh NAI sebagai "*The World's Most Secure Firewall*". Inti yang ingin kami sampaikan adalah bahwa meskipun sudah menggunakan firewall, keamanan harus tetap dipantau secara berkala.

FIREWALL

- Firewall biasanya melakukan dua fungsi; fungsi (IP) filtering dan fungsi proxy. Keduanya dapat dilakukan pada sebuah perangkat komputer (device) atau dilakukan secara terpisah.

- Fungsi proxy dapat dilakukan oleh berbagai software tergantung kepada jenis proxy yang dibutuhkan, misalnya web proxy, rlogin proxy, ftp proxy dan seterusnya. Di sisi client sering kalai dibutuhkan software tertentu agar dapat menggunakan proxy server ini, seperti misalnya dengan menggunakan SOCKS. Beberapa perangkat lunak berbasis UNIX untuk proxy antara lain:
  - *Socks:* proxy server oleh NEC Network Systems Labs
  - *Squid*: web proxy server

- Satu hal yang perlu diingat bahwa adanya firewall bukan menjadi jaminan bahwa jaringan dapat diamankan seratus persen. Firewall tersebut sendiri dapat memiliki masalah. Sebagai contoh, Firewall Gauntlet yang dibuat oleh Network Associates Inc. (NAI) mengalami masalah1 sehingga dapat melewatkan koneksi dari luar yang seharusnya tidak boleh lewat. Padahal Gauntlet didengung-dengungkan oleh NAI sebagai "*The World's Most Secure Firewall*". Inti yang ingin kami sampaikan adalah bahwa meskipun sudah menggunakan firewall, keamanan harus tetap dipantau secara berkala.

Pemantau adanya serangan

- Sistem pemantau (*monitoring system*) digunakan untuk mengetahui adanya tamu tak diundang (*intruder*) atau adanya serangan (*attack*). Nama lain dari sistem ini adalah "*intruder detection system*" (IDS). Sistem ini dapat memberitahu administrator melalui e-mail maupun melalui mekanisme lain seperti melalui sms.
- Ada berbagai cara untuk memantau adanya intruder. Ada yang sifatnya aktif dan pasif. IDS cara yang pasif misalnya dengan memonitor logfile. Contoh software IDS antara lain:
- *Autobuse*, mendeteksi probing dengan memonitor logfile.
  - *Courtney* dan *portsentry,* mendeteksi *probing* (*port scanning*) dengan memonitor packet yang lalu lalang. *Portsentry* bahkan dapat memasukkan IP penyerang dalam filter *tcpwrapper* (langsung dimasukkan kedalam berkas /etc/hosts.deny)
  - *Shadow* dari SANS
  - *Snort*, mendeteksi pola (*pattern*) pada paket yang lewat dan mengirimkan alert jika pola tersebut terdeteksi. Pola-pola atau *rules* disimpan dalam berkas yang disebut library yang dapat dikonfigurasi sesuai dengan kebutuhan.

Pemantau integritas sistem

- Pemantau integritas sistem dijalankan secara berkala untuk menguji integratitas sistem. Salah satu contoh program yang umum digunakan di sistem UNIX adalah program *Tripwire*. Program paket *Tripwire* dapat digunakan untuk memantau adanya perubahan pada berkas. Pada mulanya, tripwire dijalankan dan membuat database mengenai berkas-berkas atau direktori yang ingin kita amati beserta "*signature*" dari berkas tersebut.
- Signature berisi informasi mengenai besarnya berkas, kapan dibuatnya, pemiliknya, hasil *checksum* atau *hash* (misalnya dengan menggunakan program MD5), dan sebagainya. Apabila ada perubahan pada berkas tersebut, maka keluaran dari *hash function* akan berbeda dengan yang ada di database sehingga ketahuan adanya perubahan.

Audit: Mengamati Berkas Log

- Segala (sebagian besar) kegiatan penggunaan sistem dapat dicatat dalam berkas yang biasanya disebut "*logfile*" atau "*log*" saja. Berkas log ini sangat berguna untuk mengamati penyimpangan yang terjadi. Kegagalan untuk masuk ke sistem (login), misalnya, tersimpan di dalam berkas log. Untuk itu para administrator diwajibkan untuk rajin memelihara dan menganalisa berkas log yang dimilikinya.
- Letak dan isi dari berkas log bergantung kepada operating system yang digunakan. Di sistem berbasis UNIX, biasanya berkas ini berada di direktori /var/adm atau /var/log.
- Untuk itu adanya tools yang dapat membantu administrator untuk memproses dan menganalisa berkas log merupakan sesuatu yang sangat penting. Ada beberapa tools sederhana yang menganalia berkas log untuk mengamati kegagalan (*invalid password*, *login failure*, dan sebagainya) kemudian memberikan ringkasan. Tools ini dapat dijalankan setiap pagi dan mengirimkan hasilnya kepada administrator.
-

Backup secara rutin

- Seringkali tamu tak diundang (*intruder*) masuk ke dalam sistem dan merusak sistem dengan menghapus berkas-berkas yang dapat ditemui. Jika intruder ini berhasil menjebol sistem dan masuk sebagai super user (administrator), maka ada kemungkinan dia dapat menghapus seluruh berkas. Untuk itu, adanya backup yang dilakukan secara rutin merupakan sebuah hal yang esensial. Bayangkan apabila yang dihapus oleh tamu ini adalah berkas penelitian, tugas akhir, skripsi, yang telah dikerjakan bertahun-tahun.
- Untuk sistem yang sangat esensial, secara berkala perlu dibuat backup yang letaknya berjauhan secara fisik. Hal ini dilakukan untuk menghindari hilangnya data akibat bencana seperti kebakaran, banjir, dan lain sebagainya. Apabila data-data dibackup akan tetapi diletakkan pada lokasi yang sama, kemungkinan data akan hilang jika tempat yang bersangkutan mengalami bencana seperti kebakaran.
-

Penggunaan Enkripsi untuk meningkatkan keamanan

- Salah satau mekanisme untuk meningkatkan keamanan adalah dengan menggunakan teknologi enkripsi. Data-data yang anda kirimkan diubah sedemikian rupa sehingga tidak mudah disadap. Banyak servis di Internet yang masih menggunakan "*plain text*" untuk *authentication*, seperti penggunaan pasangan userid dan password. Informasi ini dapat dilihat dengan mudah oleh program penyadap atau pengendus (*sniffer*).
- Contoh servis yang menggunakan plain text antara lain:
  - akses jarak jauh dengan menggunakan telnet dan rlogin
  - transfer file dengan menggunakan FTP
  - akses email melalui POP3 dan IMAP4
  - pengiriman email melalui SMTP
  - akses web melalui HTTP
- Penggunaan enkripsi untuk remote akses (misalnya melalui ssh sebagai penggani telnet atau rlogin) akan dibahas di bagian tersendiri.

Telnet atau shell aman

- *Telnet* atau *remote login* digunakan untuk mengakses sebuah "*remote site*" atau komputer melalui sebuah jaringan komputer. Akses ini dilakukan dengan menggunakan hubungan TCP/IP dengan menggunakan userid dan password. Informasi tentang userid dan password ini dikirimkan melalui jaringan komputer secara terbuka. Akibatnya ada kemungkinan seorang yang nakal melakukan "sniffing" dan mengumpulkan informasi tentang pasangan userid dan password ini.
- Untuk menghindari hal ini, enkripsi dapat digunakan untuk melindungi adanya sniffing. Paket yang dikirimkan dienkripsi dengan algoritma DES atau Blowish (dengan menggunakan kunci session yang dipertukarkan via RSA atau Diffie-Hellman) sehingga tidak dapat dibaca oleh orang yang tidak berhak. Salah satu implementasi mekanisme ini adalah SSH (Secure Shell).

Telnet atau shell aman

- ssh untuk UNIX (dalam bentuk source code, gratis, mengimplementasikan protokol SSH versi 1 dan versi 2)
- SSH untuk Windows95 dari Data Fellows (komersial, ssh versi 1 dan versi 2)
- http://www.datafellows.com/
- TTSSH, yaitu skrip yang dibuat untuk *Tera Term Pro* (gratis, untuk
- Windows 95, ssh versi 1)
- http://www.paume.itb.ac.id/rahard/koleksi
- SecureCRT untuk Windows95 (shareware / komersial)
- putty (SSH untuk Windows yang gratis, ssh versi 1). Selain menyediakan ssh, paket putty juga dilengkapi dengan pscp yang mengimplementasikan secure copy sebagai pengganti FTP.

Merci bien
ありがとう
Matur Nuwun
Hatur Nuhun
Obrigado
Dank
Thanks
Matur se Kelangkong
Syukron
Kheili Mamnun
ευχαριστιες
Danke
Grazias
谢谢
Terima Kasih


Irawan_afrianto@yahoo.com

Irawan.afrianto

@Irawan_afrianto

+628170223513