KERENTANAN YANG DAPAT TERJADI DI JARINGAN KOMPUTER PADA UMUMNYA

Andre M. R. Wajong

Department of Industrial Engineering, Faculty of Engineering, Universitas Bina Nusantara
Jln. K. H. Syahdan No. 9 Palmerah Jakarta Barat 11480
awajong@yahoo.com

ABSTRACT

The rapid development of computer technology allows ease of access, yet lurking threats. Security in computer networks are categorized into two, namely the physical and non physical security. Physical security is a security that is more likely to focus to all things physical. This type of security can be avoided by more careful guarding of the thieves' threats by putting in locked places and so on. As with the non-physical security, the more important issue involved is such as data security where its physical value may be less important. Therefore, this article discussed the safety factor especially on a computer network, vulnerable points on the computer network, techniques often used on attacks and some things you can do to ward off them.

***Keywords**: computer network, vurnerability, physical security, non physical security*

ABSTRAK

Pesatnya perkembangan teknologi komputer tidak serta-merta membuat para pengguna merasa tertolong. Di samping kemudahan akses, terdapat juga ancaman yang mengintai. Keamanan dalam jaringan komputer dikategorikan menjadi dua, yaitu keamanan fisik dan non fisik. Keamanan fisik merupakan keamanan yang lebih cenderung berfokus ke segala sesuatu yang bersifat fisik. Jenis keamanan ini bisa dihindari dengan lebih teliti menjaganya dari ancaman pencuri dengan meletakkan di tempat yang terkunci dan sebagainya. Lain halnya dengan keamanan non fisik, di mana keamanan yang lebih penting dibandingkan dengan fisiknya karena menyangkut masalah keamanan data yang nilainya boleh jadi lebih besar dibandingkan dengan nilai fisik. Untuk itu, dalam artikel ini dibahas faktor keamanan khususnya pada jaringan komputer, titik-titik rentan pada jaringan komputer, teknik yang sering digunakan dalam melakukan serangan dan beberapa hal yang dapat dilakukan untuk menangkal serangan tersebut.

***Kata kunci**: kerentanan jaringan computer, keamanan fisik, keamanan non fisik*

PENDAHULUAN

Jaringan komputer adalah sebuah kumpulan komputer, printer dan peralatan lainnya yang terhubung dalam satu kesatuan. Informasi dan data bergerak melalui kabel-kabel atau tanpa kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data, mencetak pada *printer* yang sama dan bersama-sama menggunakan *hardware/software* yang terhubung dengan jaringan. Setiap komputer, printer atau periferal yang terhubung dengan jaringan disebut node. Sebuah jaringan komputer dapat memiliki dua, puluhan, ribuan atau bahkan jutaan node.

Secara umum jaringan komputer dibagi atas lima jenis, yaitu; (1) Local Area Network (LAN), merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer. LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan workstation dalam kantor suatu perusahaan atau pabrik-pabrik untuk memakai bersama sumberdaya (misalnya printer) dan saling bertukar informasi; (2) Metropolitan Area Network (MAN), pada dasarnya merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN. MAN dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum. MAN mampu menunjang data dan suara, bahkan dapat berhubungan dengan jaringan televisi kabel; (3) Wide Area Network (WAN), jangkauannya mencakup daerah geografis yang luas, seringkali mencakup sebuah negara bahkan benua. WAN terdiri dari kumpulan mesin-mesin yang bertujuan untuk menjalankan program-program (aplikasi) pemakai; (4) internet – sebenarnya terdapat banyak jaringan di dunia ini, seringkali menggunakan perangkat keras dan perangkat lunak yang berbeda-beda. Orang yang terhubung ke jaringan sering berharap untuk bisa berkomunikasi dengan orang lain yang terhubung ke jaringan lainnya. Keinginan seperti ini memerlukan hubungan antar jaringan yang seringkali tidak kampatibel dan berbeda. Biasanya untuk melakukan hal ini diperlukan sebuah mesin yang disebut gateway guna melakukan hubungan dan melaksanakan terjemahan yang diperlukan, baik perangkat keras maupun perangkat lunaknya. Kumpulan jaringan yang terinterkoneksi inilah yang disebut dengan internet; (5) jaringan tanpa kabel – merupakan suatu solusi terhadap komunikasi yang tidak bisa dilakukan dengan jaringan yang menggunakan kabel. Misalnya orang yang ingin mendapat informasi atau melakukan komunikasi walaupun sedang berada diatas mobil atau pesawat terbang, maka mutlak jaringan tanpa kabel diperlukan karena koneksi kabel tidaklah mungkin dibuat di dalam mobil atau pesawat. Saat ini jaringan tanpa kabel sudah marak digunakan dengan memanfaatkan jasa satelit dan mampu memberikan kecepatan akses yang lebih cepat dibandingkan dengan jaringan yang menggunakan kabel (Van Basten, 2009, pp.5 – 6).

Keamanan jaringan saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus menyangkut keamanan sistem saat ini menjadi suatu garapan yang membutuhkan biaya penanganan dan proteksi yang sedemikian besar. Sistem-sistem vital seperti sistem pertahanan, sistem perbankan dan sistem-sistem setingkat itu, membutuhkan tingkat keamanan yang sedemikian tinggi. Hal ini lebih disebabkan karena kemajuan bidang jaringan komputer dengan konsep open sistemnya sehingga siapapun, di manapun dan kapanpun, mempunyai kesempatan untuk mengakses kawasan-kawasan vital tersebut.

Keamanan jaringan didefinisikan sebagai sebuah perlindungan dari sumber daya daya terhadap upaya penyingkapan, modifikasi, utilisasi, pelarangan dan perusakan oleh person yang tidak diijinkan. Beberapa ahli jaringan mengatakan bahwa hanya ada satu cara mudah dan ampuh untuk mewujudkan sistem jaringan komputer yang aman yaitu dengan menggunakan pemisah antara komputer dengan jaringan selebar satu inci, dengan kata lain, hanya komputer yang tidak terhubung ke jaringanlah yang mempunyai keamanan yang sempurna. Meskipun ini adalah solusi yang buruk, tetapi ini menjadi trade-off antara pertimbangan fungsionalitas dan memasukan kekebalan terhadap gangguan.

Keamanan jaringan komputer sendiri sering dipandang sebagai hasil dari beberapa faktor yang bervariasi tergantung pada bahan dasar, tetapi secara normal setidaknya beberapa hal di bawah ini diikutsertakan: (1) *confidentiality* (kerahasiaan) – ada beberapa jenis informasi yang tersedia di dalam sebuah jaringan komputer. Setiap data yang berbeda pasti mempunyai grup pengguna yang berbeda pula dan data dapat dikelompokkan sehingga beberapa pembatasan kepada penggunaan data harus ditentukan. Pada umumnya data yang terdapat di dalam suatu perusahaan bersifat rahasia dan tidak boleh diketahui oleh pihak ketiga yang bertujuan untuk menjaga rahasia perusahaan dan strategi perusahaan. *Backdoor*, sebagai contoh, melanggar kebijakan perusahaan dikarenakan menyediakan akses yang tidak diinginkan ke dalam jaringan komputer perusahaan; (2) *integrity* (integritas) – jaringan komputer yang dapat diandalkan juga berdasar pada fakta bahwa data yang tersedia apa yang sudah seharusnya. Jaringan komputer mau tidak mau harus terlindungi dari serangan yang dapat merubah data selama dalam proses transmisi. *Man-in-the-Middle* merupakan jenis serangan yang dapat merubah integritas dari sebuah data yang mana penyerang (*attacker*) dapat membajak *session* atau memanipulasi data yang terkirim; (3) *availability* (ketersediaan) – ketersediaan data atau layanan dapat dengan mudah dipantau oleh pengguna dari sebuah layanan. Ketidaktersediaan dari sebuah layanan dapat menjadi sebuah halangan untuk maju bagi sebuah perusahaan dan bahkan dapat berdampak lebih buruk lagi, yaitu penghentian proses produksi. Sehingga untuk semua aktifitas jaringan, ketersediaan data sangat penting untuk sebuah sistem agar dapat terus berjalan dengan benar (Kelompok 123P, 2005).

METODE

Mengamankan jaringan komputer membutuhkan tiga tingkatan proses, yaitu: *prevention* (pencegahan), *observation* (observasi), dan *response* (respon).

Prevention (Pencegahan)

Kebanyakan dari ancaman akan dapat ditepis dengan mudah, walaupun keadaan yang benar-benar100% aman belum tentu dapat dicapai. Akses yang tidak diinginkan ke dalam jaringan komputer dapat dicegah dengan memilih dan melakukan konfigurasi layanan (*services*) yang berjalan dengan hati-hati.

Observation (Observasi)

Ketika sebuah jaringan komputer sedang berjalan, dan sebuah akses yang tidak diinginkan dicegah, proses perawatan dilakukan. Perawatan jaringan komputer harus termasuk melihat isi *log* yang tidak normal yang dapat merujuk ke masalah keamanan yang tidak terpantau.

Response (Respon)

Bila sesuatu yang tidak diinginkan terjadi dan keamanan suatu sistem telah berhasil disusupi, personil perawatan harus segera mengambil tindakan. Bila sebuah proses sangat vital pengaruhnya kepada fungsi sistem dan apabila di-*shutdown* akan menyebabkan lebih banyak kerugian daripada membiarkan sistem yang telah berhasil disusupi tetap berjalan. Maka dari itu, harus dipertimbangkan rencana perawatan pada saat yang tepat. Ini merupakan masalah yang sulit dikarenakan tidak seorangpun akan segera tahu apa yang menjadi celah begitu sistem telah berhasil disusupi dari luar.

Victims/Statistic (Korban/Statistik)

Keamanan jaringan komputer meliputi beberapa hal yang berbeda yang mempengaruhi keamanan secara keseluruhan. Serangan keamanan jaringan komputer dan penggunaan yang salah dan sebagai contoh adalah virus, serangan dari dalam jaringan komputer itu sendiri, pencurian perangkat keras (*hardware*), penetrasi ke dalam sistem, serangan Denial of Service (DoS), sabotase, serangan *wireless* terhadap jaringan komputer, penggantian halaman depan situs (*website defacement*), dan penggunaan yang salah terhadap aplikasi web. Beberapa titik rentan yang sering terjadi pada jaringan komputer adalah sebagai berikut:

Weak Protocols

Komunikasi jaringan komputer menggunakan protokol antara *client* dan *server*. Kebanyakan dari protokol yang digunakan saat ini merupakan protocol yang telah digunakan beberapa dasawarsa belakangan. Protokol lama ini, seperti *File* Transmission Protocol (FTP), TFTP ataupun telnet, tidak didesain untuk menjadi benar-benar aman. Malahan faktanya kebanyakan dari protocol ini sudah seharusnya digantikan dengan protokol yang jauh lebih aman, dikarenakan banyak titik rawan yang dapat menyebabkan pengguna yang tidak bertanggung jawab dapat melakukan eksploitasi. Sebagai contoh, seseorang dengan mudah dapat mengawasi *traffic* dari *telnet* dan dapat mencari tahu nama *user* dan *password*.

Software Issue

Menjadi sesuatu yang mudah untuk melakukan eksploitasi celah pada perangkat lunak. Celah ini biasanya tidak secara sengaja dibuat tapi kebanyakan semua orang mengalami kerugian dari kelemahan seperti ini. Celah ini biasanya dibakukan bahwa apapun yang dijalankan oleh *root* pasti mempunyai akses *root*, yaitu kemampuan untuk melakukan segalanya di dalam sistem tersebut. Eksploitasi yang sebenarnya mengambil keuntungan dari lemahnya penanganan data yang tidak diduga oleh pengguna, sebagai contoh, *buffer overflow* dari celah keamanan *format string* merupakan hal yang biasa saat ini. Eksploitasi terhadap celah tersebut akan menuju kepada situasi di mana hak akses pengguna akan dapat dinaikkan ke tingkat akses yang lebih tinggi. Ini disebut juga dengan *rooting* sebuah *host* dikarenakan penyerang biasanya membidik untuk mendapatkan hak akses *root*.

Buffer Overflow

"Buffer overflow" mempunyai arti sama dengan istilahnya. *Programmer* telah mengalokasikan sekian besar *memory* untuk beberapa variabel spesifik. Bagaimanapun juga, dengan celah keamanan ini, variabel ini dapat dipaksa menuliskan ke dalam *stack* tanpa harus melakukan pengecekan kembali bila panjang variabel tersebut diizinkan. Jika data yang berada di dalam *buffer* ternyata lebih panjang daripada yang diharapkan, kemungkinan akan melakukan penulisan kembali *stack frame* dari *return address* sehingga alamat dari proses eksekusi program dapat dirubah.

Penulis *malicious code* biasanya akan akan melakukan eksploitasi terhadap penulisan kembali *return address* dengan merubah *return address* kepada *shell code* pilihan mereka sendiri untuk melakukan pembatalan akses *shell* dengan menggunakan hak akses dari *user-id* dari program yang tereksploitasi tersebut. *Shell code* ini tidak harus disertakan dalam program yang tereksploitasi, tetapi biasanya dituliskan ke dalam bagian celah dari *buffer*. Ini merupakan trik yang biasa digunakan pada variabel *environment* seperti ini.

Buffer overflow adalah masalah fundamental berdasarkan dari arsitektur komputasi modern. Ruang untuk variabel dan kode itu sendiri tidak dapat dipisahkan ke dalam blok yang berbeda di dalam *memory*. Sebuah perubahan di dalam arsitektur dapat dengan mudah menyelesaikan masalah

ini, tapi perubahan bukan sesuatu yang mudah untuk dilakukan dikarenakan arsitektur yang digunakan saat ini sudah sangat banyak digunakan.

Format String

Celah *format string* tercipta karena kemalasan (*laziness*), ketidakpedulian (*ignorance*), atau *programmer* yang mempunyai *skill* pas-pasan. Celah *format string* biasanya disebabkan oleh kurangnya *format string* seperti *%s* di beberapa bagian dari program yang menciptakan *output*, sebagai contoh fungsi printf() di C/C++. Bila *input* diberikan dengan melewatkan *format string* seperti *%d* dan *%s* kepada program, dengan mudah melihat *stack dump* atau penggunaan teknik seperti pada *buffer overflow*.

Celah ini berdasarkan pada *truncated format string* dari *input*. Ini merujuk kepada situasi di mana secara external, data yang disuplai yang diinterpretasikan sebagai bagian dari *format string argument*, secara khusus membuat suatu *input* dapat menyebabkan program yang bermasalah menunjukkan isi *memory* dan juga kontrol kepada eksekusi program dengan menuliskan apa saja kepada lokasi pilihan sama seperti pada eksploitasi *overflow*.

Hardware Issue

Biasanya perangkat keras tidak mempunyai masalah pada penyerangan yang terjadi. Perangkat lunak yang dijalankan oleh perangkat keras dan kemungkinan kurangnya dokumentasi spesifikasi teknis merupakan suatu titik lemah.

Misconfiguration

Kesalahan konfigurasi pada *server* dan perangkat keras (*hardware*) sangat sering membuat para penyusup dapat masuk ke dalam suatu sistem dengan mudah. Sebagai contoh, penggantian halaman depan suatu situs karena kesalahan konfigurasi pada perangkat lunak www-*server* atapun modulnya. Konfigurasi yang tidak hati-hati dapat menyebabkan usaha penyusupan menjadi jauh lebih mudah terlebih jika ada pilihan lain yang dapat diambil oleh para penyusup. Sebagai contoh, sebuah *server* yang menjalankan beberapa layanan SSH dapat dengan mudah disusupi apabila mengijinkan penggunaan protokol versi 1 atau *remote root login* (RLOGIN). Kesalahan konfigurasi yang jelas ini menyebabkan terbukanya celah keamanan dengan penggunaan protokol versi 1, seperti *buffer overflow* yang dapat menyebabkan penyusup dapat mengambil hak akses *root* atau dengan menggunakan metode *brute-force password* untuk dapat menebak *password root*.

DoS, DDoS

Serangan *Denial of Service* (DoS) adalah serangan yang mengakibatkan setiap korbannya akan berhenti merespon atau berlaku tidak lazim. Contoh serangan klasik DoS adalah *Ping of Death* dan *Syn Flood* yang untungnya sudah hampir tidak dapat dijumpai pada saat sekarang. Biasanya serangan DoS menyerang celah yang terdapat pada layanan sistem atau pada protokol jaringan kerja untuk menyebabkan layanan tidak dapat digunakan. Teknik yang lainnya adalah menyebabkan sistem korban tersedak dikarenakan banyaknya paket yang diterima yang harus diproses melebihi kemampuan dari sistem itu sendiri atau menyebabkan terjadinya *bottleneck* pada *bandwidth* yang dipakai oleh sistem. Serangan *Distributed Denial of Service* (DDoS) merupakan tipe serangan yang lebih terorganisasi. Jenis serangan ini biasanya membutuhkan persiapan dan juga taktik untuk dapat menjatuhkan korbannya dengan cepat dan sebelumnya biasanya para penyerang akan mencari sistem kecil yang dapat dikuasai. Setelah mendapat banyak sistem kecil, penyerang akan menyerang sistem yang besar dengan menjalankan ribuan bahkan puluhan ribu sistem kecil secara bersamaan untuk menjatuhkan sebuah sistem besar.

Viruses

Salah satu definisi dari program virus adalah menyisipkan dirinya kepada objek lain seperti *file executable* dan beberapa jenis dokumen yang banyak dipakai orang. Selain kemampuan untuk mereplikasi dirinya sendiri, virus dapat menyimpan dan menjalankan sebuah tugas spesifik. Tugas tersebut bisa bersifat menghancurkan atau sekedar menampilkan sesuatu ke layar monitor korban dan bisa saja bertugas untuk mencari suatu jenis *file* untuk dikirimkan secara acak ke internet bahkan dapat melakukan format pada *hard disk* korban.

Virus yang tersebar di internet dan belum dikenali tidak akan dapat ditangkap oleh program antivirus ataupun semacamnya, sehingga apabila korban telah terjangkit, tetap tidak mengetahuinya. Perangkat lunak antivirus biasanya mengenali virus atau calon virus melalui tanda yang spesifik yang terdapat pada bagian inti virus itu sendiri. Beberapa virus menggunakan teknik *polymorphic* agar luput terdeteksi oleh antivirus. Kebiasaan virus polymorphic adalah merubah dirinya pada setiap infeksi yang terjadi yang menyebabkan pendeteksian menjadi jauh lebih sulit. Praktisnya setiap *platform* komputer mempunyai virus masing-masing dan ada beberapa virus yang mempunyai kemampuan menjangkiti beberapa *platform* yang berbeda (multi-*platform*). Virus multi-*platform* biasanya menyerang *executable* ataupun dokumen pada Windows dikarenakan kepopuleran oleh sistem operasi Microsoft Windows dan Microsoft Office sehingga banyak ditemukan virus yang bertujuan untuk menghancurkan kerajaan Microsoft Corp.

Worms

Sebuah *worm* komputer merupakan program yang menyebar sendiri dengan cara mengirimkan dirinya sendiri ke sistem yang lainnya. *Worm* tidak akan menyisipkan dirinya kepada objek lain. Pada saat sekarang banyak terjadi penyebaran *Worm* dikarenakan para pengguna komputer tidak melakukan *update* pada perangkat lunak yang mereka gunakan, sebagai contoh, Outlook Express mempunyai fungsi yang dapat mengizinkan eksekusi pada *file* sisipan (*attachment*) email tanpa campur tangan dari pengguna komputer itu sendiri.

Trojan Horse

Trojan Horse adalah program yang berpura-pura tidak berbahaya tetapi sebenarnya mereka sesuatu yang lain. Salah fungsi yang biasa terdapat pada *Trojan Horse* melakukan instalasi *backdoor* sehingga si pembuat program dapat menyusup ke dalam komputer atau sistem korban.

Time Bomb

Time Bomb adalah program yang mempunyai tugas tetapi dengan waktu tertentu baru akan menjalankan tugasnya. Beberapa jenis virus dan *worm* juga mempunyai kesamaan fungsi dengan aplikasi ini. *Time Bomb* berbeda dengan *virus* ataupun *worm* karena ia tidak melakukan replikasi terhadap dirinya tetapi melakukan instalasi sendiri ke dalam sistem.

Jenis-jenis Serangan yang Sering Terjadi Melalui Jaringan Komputer

Berikut ini dipaparkan beberapa jenis serangan yang sering terjadi via jaringan komputer (Malekzadeh et al., 2010).

Scanning

Scanning adalah metode bagaimana caranya mendapatkan informasi sebanyak-banyaknya dari IP/Network korban. Biasanya *scanning* dijalankan secara otomatis mengingat *scanning* pada multiple-

host sangat menyita waktu. *Hackers* biasanya mengumpulkan informasi dari hasil **scanning** ini. Dengan mengumpulkan informasi yang dibutuhkan maka hackers dapat menyiapkan serangan yang akan dilancarkannya. Nmap adalah sebuah *network scanner* yang banyak digunakan oleh para professional di bidang *network security*, walaupun ada *tool* khusus dibuat untuk tujuan *hacking*, tetap belum dapat mengalahkan kepopuleran Nmap. Nessus juga merupakan *network scanner* tapi dapat melaporkan apabila terdapat celah keamanan pada target yang diperiksanya. *Hacker* biasanya menggunakan Nessus untuk pengumpulan informasi sebelum benar-benar meluncurkan serangan. Untungnya beberapa *scanner* meninggalkan jejak unik yang memungkinkan para *System Administrator* untuk mengetahui bahwa sistem mereka telah di-*scanning* sehingga mereka bisa segera membaca artikel terbaru yang berhubungan dengan informasi *log*.

Password Cracking

Brute-force adalah sebuah teknik di mana akan dicobakan semua kemungkinan kata kunci (*password*) untuk bisa ditebak untuk akses ke dalam sebuah sistem. Membongkar kata kunci dengan teknik ini sangat lambat tapi efisien, semua kata kunci dapat ditebak asalkan waktu tersedia. Membalikkan *hash* pada kata kunci merupakan hal yang mustahil, tapi ada beberapa cara untuk membongkar kata kunci tersebut walaupun tingkat keberhasilannya tergantung dari kuat-lemahnya pemilihan kata kunci oleh pengguna. Bila seseorang dapat mengambil data *hash* yang menyimpan kata kunci, cara yang lumayan efisien adalah menggunakan metode *dictionary attack* yang dapat dilakukan oleh *utility* John The Ripper.

Rootkit

Rootkit adalah alat untuk menghilangkan jejak apabila telah dilakukan penyusupan. *Rootkit* biasanya mengikutkan beberapa *tool* yang dipakai oleh sistem dengan sudah dimodifikasi sehingga dapat menutupi jejak. Sebagai contoh, memodifikasi PS di Linux atau Unix sehingga tidak dapat melihat *background process* yang berjalan.

Pengamanan Jaringan Komputer

Komputer dan jaringan kerja yang terhubung dengan internet perlu dilindungi dari serangan. Beberapa hal yang dapat dilakukan dalam rangka menangkal serangan-serangan yang datang melalui jaringan adalah sebagai berikut (Supriyanto, 2006).

Firewall

Firewall adalah cara yang lumayan efeltif untuk melakukannya. Secara umum *Firewall* akan memisahkan *public network* dan *private network*. Tipe *Firewall* dapat dibagi menjadi beberapa kategori, contohnya: Packet Filtering Firewall, Proxy Firewall.

Logs

Seorang *System Administrator* wajib untuk melihat *log* sistem dari waktu ke waktu. Dengan melihat *log, system Administrator* dapat melihat aktifitas yang terjadi dan kemungkinan besar dapat melakukan antisipasi apabila terlihat beberapa aktifitas mencurigakan.

IDS (*Intrusion Detection System*)

Satu cara umum melakukan otomatisasi pada pengawasan penyusupan adalah dengan menggunakan IDS. IDS akan mendeteksi jenis serangan dari *signature* atau *pattern* pada aktifitas jaringan. Bahkan dapat melakukan blokade terhadap *traffic* yang mencurigakan.

Honeypot

Honeypot adalah *server* umpan yang merupakan pengalih perhatian. Tujuan dari *honeypot* adalah agar mereka tidak menjalankan layanan sebagaimana umumnya *server* tetapi berpura-pura menjalankannya sehingga membiarkan para penyusup untuk berpikir bahwa mereka benar-benar *server* sesungguhnya. *Honeypot* juga bermanfaat untuk melihat teknik yang digunakan oleh para penyusup untuk dapat masuk ke dalam sistem juga sebagai alat untuk mengumpulkan bukti sehingga para penyusup dapat diproses secara hukum.

Configuration

Seperti yang telah dibahas sebelumnya, konfigurasi yang hati-hati akan membantu anda untuk bertahan terhadap kemungkinan serangan yang terjadi. Kebanyakan kasus penggantian halaman muka situs (*web defacement*) terjadi dikarenakan kesalahan konfigurasi sehingga menyebabkan pihak ketiga dapat mengambil keuntungan dari kesalahan ini.

PENUTUP

Banyak manfaat yang dapat diambil dari teknologi jaringan komputer, baik dalam kegunaan sebagai akses untuk dunia informasi (internet) maupun sebagai infrastruktur dalam perusahaan. Namun demikian, terkoneksinya komputer ke sistem luar akan membuka ancaman bagi keamanan data yang dimiliki. Ancaman-ancaman tersebut diantaranya adalah: *Weak Protocols, Software issue, Buffer overflow, Format string, Hardware Issue, Misconfiguration, DoS, DDoS, Viruses, Worms, Trojan horse* dan *Time bomb*. Serangan-serangan pada jaringan komputer sering terjadi melalui: *Scanning, Password Cracking*, dan juga melalui teknik *Rootkit.* Untuk dapat bertahan dari serangan-serangan yang ada pada jaringan komputer, ada beberapa hal yang bisa dilakukan, di antaranya adalah: membuat Firewall, melakukan pemeriksaan terhadap *log* komputer untuk memastikan tidak ada aktifitas yang mencurigakan, melakukan otomatisasi pada pengawasan penyusupan dengan menggunakan IDS (Intrusion Detection System) dan dapat juga menggunakan Honeypot sebagai umpan untuk mengalihkan perhatian.

DAFTAR PUSTAKA

Kelompok 123P IKI-83408T MTI UI. 2005. *Keamanan Jaringan Komputer*.

Malekzadeh, M., Abdul Ghani, A. A., & Subramaniam, S. (2010). Design of cyberwar laboratory exercises to implement common security attacks against IEEE 802.11 Wireless Networks. *Journal of Computer Systems, Networks, and Communications, 2010*.

Supriyanto, Aji. (2006), Analisis kelemahan keamanan pada jaringan *wireless*. *Jurnal Teknologi Informasi DINAMIK 9* (1), 38-46.

Van Basten, Marco. (2009). Optimalisasi Firewall pada jaringan skala luas. *Jurnal Jaringan Komputer*. Fakultas Ilmu Komputer, Universitas Sriwijaya, Palembang.