KEAMANAN JARINGAN PADA MEDIA KOMUNIKASI DATA ELEKTRONIK

Sakiwan

Peneliti Bidang Informasi
Pusat Analisis dan Informasi Kedirgantaraan

RINGKASAN

Keamanan jaringan merupakan hal yang penting seiring dengan berkembangnya teknologi informasi (TI), internet merupakan suatu sistem jaringan komputer yang telah menyebar keseluruh dunia dengan menyajikan berbagai informasi, selain itu internet juga merupakan sarana bagi kebutuhan dalam dunia penelitian, usaha bahkan sampai pada dunia pendidikan untuk mengakses informasi. Ancaman dan keamanan di internet dapat dipandang dari dua sisi, yang pertama adalah integritas data dan yang kedua adalah keamanan dalam jaringan komputer itu sendiri.

Makalah ini membahas masalah keamanan jaringan pada media komunikasi data elektronik dalam upaya mengatasi ancaman terhadap keamanan data dan informasi dengan menggunakan software maupun hardware sebagai pengaman.

I. PENDAHULUAN

Di era globalisasi saat ini informasi berperan penting dalam kehidupan sehari-hari, salah satu media komunikasi untuk mencari sumber informasi yang digunakan adalah internet. Internet merupakan suatu sistem jaringan komputer yang telah menyebar keseluruh dunia, jaringan ini telah memberikan keuntungan dan kerugian, keuntungannya yaitu dapat saling tukar menukar informasi dengan cepat sedangkan kerugiannya jika terjadi pencurian atau pengrusakan data oleh para tangan jahil. Hal tersebut menunjukkan bahwa kita harus waspada terhadap orang-orang jahat karena dapat menjadi ancaman serius bagi keamanan data di internet.

LAPAN sebagai instansi yang salah satu tugasnya adalah membantu pemerintah melakukan pengembangan informasi kedirgantaraan, pengadaan data, pengumpulan data, penyusunan data, serta pengolahan data informasi kedirgantaraan, dalam upaya meningkatkan kualitas pelayanannya kepada masyarakat, LAPAN membangun sistem jaringan informasi kedirgantaraan yang terpadu dengan sistem jaringan informasi nasional yang terhubung melalui internet. Dengan dibangunnya jaringan LAPAN ke internet, maka jaringan tersebut akan menghadapi ancaman-ancaman baik penyusupan, pengrusakan maupun pencurian data. Masalah keamanan jaringan internet di LAPAN hingga saat ini belum mengalami permasalahan yang serius, akan tetapi sesuai dengan kemajuan teknologi yang canggih, kondisi keamanan jaringan internet di LAPAN dapat terancam. Makalah ini membahas tentang keamanan jaringan pada komunikasi data elektronik, dengan tujuan memberikan masukan kepada LAPAN khususnya Pusisfogan dalam menentukan kebijakan pengembangan informasi khususnya di bidang keamanan jaringan yang ada di LAPAN.

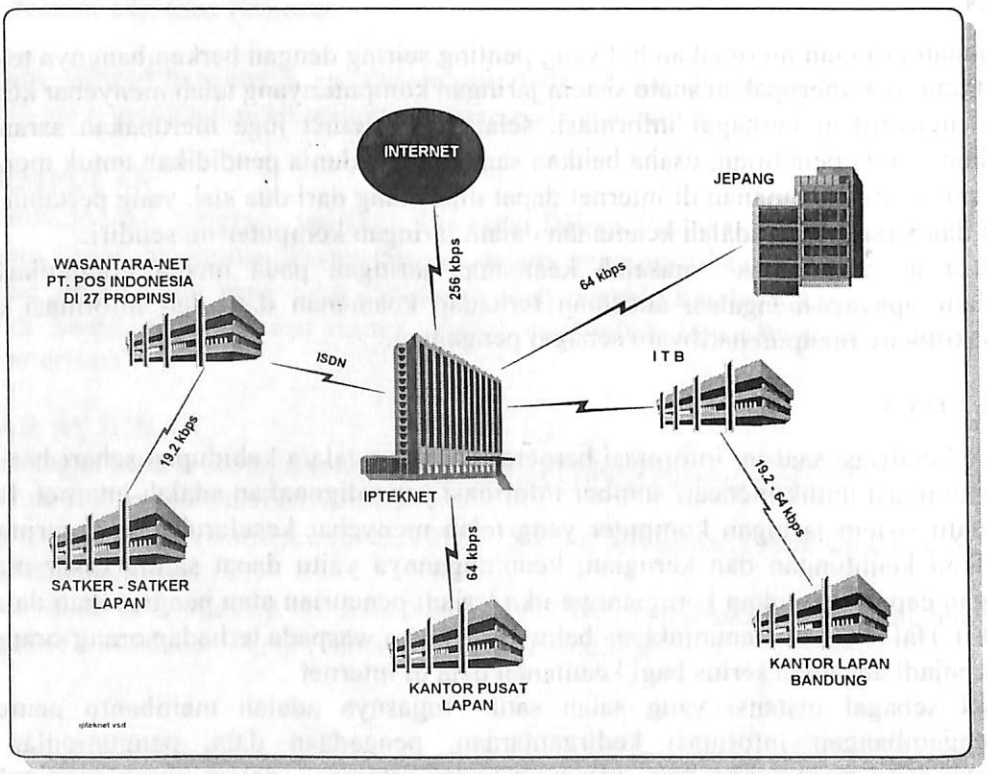
2. KONDISI SAAT INI

Jaringan komputer LAPAN Pusat dibangun sejak tahun 1988 yaitu dimulai dari jaringan Lokal Area Network (LAN), dan terus dikembangkan menjadi jaringan Wide Area Network (WAN). LAPAN pusat memiliki sebuah PC server, router, modem leased line, passive dan active hub serta beberapa PC sebagai terminal kerja yang terkoneksi dengan jaringan kabel UTP. Sistem operasi (SO) yang digunakan pada jaringan LAPAN untuk LAN menggunakan SO netware 3.11

dan windows NT 4.0 sedangkan untuk internet menggunakan SO Unix, Jaringan Internet di LAPAN terlihat pada gambar 2-1.

LAPAN sebagai lembaga penelitian, fasilitas internet merupakan kebutuhan primer, karena internet merupakan penghubung dengan dunia luar dalam pertukaran informasi, namun komunikasi data internet yang ada pada saat ini keamanannya masih diragukan, karena media pertahanan jaringan LAPAN masih sangat sederhana yaitu hanya menggunakan password. Hal ini, memungkinkan jaringan di LAPAN akan berhadapan dengan ancaman, penyusupan dan pengrusakan data dari para pengrusak (*hacker*).

GAMBAR 3.1 JARINGAN INTERNET LAPAN



2.1 MASALAH YANG DIHADAPI

Secara garis besar, ancaman keamanan di internet dapat di pisahkan dalam dua jenis bentuk penyerangan; (a) serangan pasif, Serangan ini berusaha untuk mencuri dengar komunikasi yang sedang terjadi antara dua pemakai atau dua komputer yang saling terhubung, gangguan jenis ini sulit dideteksi dan penyerangan jenis ini hanya dapat diatasi dengan menggunakan pengamanan transaksi; (b) Serangan aktif, Serangan ini berusaha untuk membobol atau menembus masuk ke suatu jaringan komputer privat untuk mengambil informasi atau mengambil alih sistem yang ada. Gangguan jenis ini dapat di deteksi serta dapat ditanggulangi dengan memperkuat pengamanan jaringan.

Ancaman keamanan di internet dapat datang dari beberapa pihak antara lain : (a) *hacker* yang sekedar iseng dan mencari tantangan;(b) penjahat yang mencari keuntungan *finansiil*; (c) mata-mata industri yang berusaha mencuri rahasia-rahasia perusahaan.

Untuk keamanan jaringan Internet di LAPAN melindungi data hingga saat ini masih dapat dibilang umum, karena hanya menggunakan program password yang Password merupakan perlindungan dasar dari suatu sistem komputer.

3. ANALISIS DAN PEMECAHAN

Pada era informasi digital, jaringan Internet LAPAN pada saat ini mempunyai kecepatan transfer data hingga 64 Kbps dengan menggunakan jalur leased line, jalur ini memungkinkan pengaksesan berupa data maupun berupa grafik. LAPAN sebagai Pusat Sistem Informasi Kedirgantaraan Nasional (SIDNAL), diharapkan mampu menyediakan, melayani, dan mendayagunakan, serta menyebarkan luaskan informasi kedirgantaraan melalui jaringan komputer. Dengan terkoneksinya Pussisfogan LAPAN dan satuan-satuan kerja di lingkungan LAPAN ke internet, maka semua informasi di bidang kedirgantaraan baik berupa database dan informasi lain dapat diakses secara on line melalui homepage LAPAN oleh pengguna.

Berkaitan dengan hal tersebut maka untuk memperkecil resiko ancaman keamanan jaringan pada komunikasi data komputer sehingga potensi internet dapat dimanfaatkan sepenuhnya oleh peneliti LAPAN dan masyarakat pengguna, tentunya homepage LAPAN perlu dilindungi. Hal ini disebabkan karena sifat dari jaringan internet yang terbuka, sehingga dimungkinkan terjadinya gangguan oleh para hacker dengan mudah.

Beberapa metode yang digunakan penyusup untuk memperoleh akses ke sistem pada suatu jaringan adalah dengan menggunakan sebuah packet sniffer. Sniffer digunakan untuk mendengarkan port Ethernet yang akan konek kesebuah jaringan untuk melihat '*Password*, *Login* dan *SU* yang terdapat pada aliran paket, dan kemudian mencatat lalu lintas, dengan cara ini penyerang dapat memperoleh password pada suatu jaringan yang terkena sniffer. Password teks biasanya sangat rentan terhadap serangan. Contoh; host A telah dimasuki penyerang, kemudian penyerang menginstal sebuah sniffer. Sniffer mencatat login admin ke host B dari host C, kemudian diperoleh password personal admin ketika login ke B. dan admin melakukan SU untuk mengatasi suatu masalah. Mereka sekarang memiliki password root untuk Host B. Kemudian admin membolehkan seseorang telnet dari rekeningnya ke host Z di site lain. Sekarang penyerang memiliki password/login di host Z.

Metode lain yang digunakan penyusup dalam penyerangan sistem jaringan antara lain; penyusup menscan sistem yang rapuh dengan menggunakan *daemon dialer*, yaitu suatu program yang digunakan menredial sebuah nomor berulang-ulang secara otomatis sampai koneksi tercipta, sehingga penyusup dapat mencuri file passwd dari jarak jauh pada jaringan tertentu, dan kemudian file passwd sebagai file penyimpan kata sandi (password) dapat dibaca dengan cara menjalankan program Crack dan John the Ripper, dan masih banyak lagi cara para penyusup untuk mencari mangsanya.

Sebagai strategi keamanan jaringan, LAPAN telah menggunakan password sebagai antisipasi serangan para hacker. Namun demikian, dengan berkembanganya ilmu komputer yang semakin canggih maka password yang digunakan sebagai penangkal kejahatan pada jaringan yang ada di LAPAN masih sangat mudah dibobol pertahanannya oleh para hacker.

Oleh karena itu sebagai antisipasi keamanan jaringan LAPAN perlu melakukan peningkatan penanggulangan ancaman dan keamanan data dengan cara :

Menambah *Firewall*

Firewall merupakan suatu cara untuk membatasi dibolehkannya masuk dan keluar suatu informasi pada jaringan. Umumnya host firewall terhubung ke Internet dan LAN serta akses LAN ke Internet hanya dilakukan melalui firewall. Dengan demikian firewall dapat mengendalikan apa yang diterima dan dikirim dari Internet dan LAN.

Dalam implementasinya firewall mempunyai fungsi sebagai screening filter dan *proxy gateway*. Screening filter dipasang pada router yang menghubungkan jaringan privat dengan internet, yang bertugas untuk membaca setiap paket internet protocol yang lewat, sehingga komunikasi dapat dibatasi oleh pihak-pihak yang telah diketahui dan diidentifikasi keabsahannya. Sebagai *proxy gateway* tingkat keamanannya lebih tinggi, karena mesin ini bekerja pada lapisan protocol OSI (yaitu pada lapisan transport). Dengan menggunakan proxy

gateway resiko ancaman keamanan dapat diperkecil, karena keberadaan jaringan privat dibelakang firewall tidak terlihat dari jaringan publik, jadi dengan menggunakan firewall, resiko ancaman keamanan jaringan lebih terjamin sehingga data dan informasi yang ada tidak mudah untuk ditesusupi. Fungsi dari *firewall* adalah; *(a)Screening filter,* Pada prinsipnya screening filter bertugas untuk membaca setiap paket internet protocol yang lewat. Filter dapat diprogram untuk meneruskan atau menolak dan membuang paket internet protocol yang bersangkutan. Dengan cara ini, screening filter dapat digunakan untuk membatasi komunikasi hanya diantara pihak-pihak yang diketahui dan diidentifikasi keabsahannya. Screening filter mampu memberikan perlindungan dasar kepada jaringan privat terhadap percobaan akses dari luar. (b) *Proxy gateway, Proxy gateway* suatu program yang memberikan perlindungan penuh terhadap jaringan privat, karena hubungan antara jaringan lokal dan jaringan publik diputuskan dimesin firewall. Sehingga keberadaan jaringan lokal dibelakang firewall tidak terlihat dari jaringan publik. Mengingat firewall merupakan mesin yang berhubungan langsung dengan internet, kemudian firewall juga akan menjadi sasaran utama dalam suatu penyerangan. Firewall tidak akan ada gunanya melindungi jaringan privat apabila firewall itu sendiri ternyata dapat ditembus.

Memverifikasi Informasi DNS, yaitu memelihara informasi DNS tentang seluruh host pada jaringan agar tetap baru. Jika ada host yang tidak dijinkan terhubung ke jaringan, DNS dapat mengenalinya.

Menambah *software Security Administrators Tool for Analyzing Networks* (SATAN) dan *Internet Security Scanner* (ISS), dimana SATAN merupaka.n sebuah program yang bekerja untuk menelusur port dengan antara muka web. SATAN dapat dikonfigurasi untuk melakukan pemeriksaan ringan, menengah, maupum berat pada jaringan mesin, serta dapat langsung memperbaiki masalah-masalah yang ditemukan. Pastikan suatu jaringan untuk memperoleh SATAN dari sun-site atau FTP atau web site yang bereputasi. Sedangkan ISS merupakan program penelusur berdasarkan port yang lain. ISS lebih cepat daripada SATAN, dan mungkin lebih baik untuk jaringan yang besar, namun demikian, SATAN memberikan banyak informasi.

KESIMPULAN

Dari Pembahasan di atas dapat disimpulkan bahwa seiring dengan berkembangnya teknologi informasi Pusisfogan LAPAN, perlu segera melakukan peningkatan keamanan jaringan internet. Beberapa langkah yang perlu segera dilakukan yaitu: melakukan a)evaluasi jaringan b)menambah software keamanan seperti memverifikasi Informasi DNS, Identd, SATAN, ISS dan password, serta menambah hardware firewall yang berfungsi sebagai filter dan *proxy gateway.*

Dengan demikian, resiko ancaman keamanan jaringan akan terjamin, sehingga data dan informasi yang ada pada jaringan akan terlindungi keselamatannya.

DAFTAR RUJUKAN

1. Gunawan, Hendy, 1997. *Analisis potensi informasi kedirgantaraan LAPAN dalam internet.* Prosiding seminar sehari dalam rangka HUT LAPAN, LAPAN Jakarta
2. Prihanto, Igif dan Hendy Gunawan, 1997. *Internet dan pemanfaatanya di LAPAN* Prosiding Pusdokinfo LAPAN. Jakarta LAPAN
3. Susanti, Dini dkk. 1999. *Keamanan Jaringan Internet,* Publikasi Ilmiah LAPAN, LAPAN Jakarta
4. http://idp.linux.or.id/HOWTO/other-formats/html/ID-Security-HOWTO-8.html
5. http://www.infokomputer.com/inilah/inilah.asp?id=1294