BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Dewasa ini perkembangan teknologi informasi telah berkembang dengan pesat, terutama dengan munculnya jaringan internet yang memberikan kemudahan dalam pertukaran informasi. Membuat semakin mudahnya mendapatkan informasi tersebut menimbulkan masalah baru yaitu pengaksesasan data atau informasi penting oleh pihak yang tidak bertanggung jawab untuk mendapatkan keuntungan pribadi maupun penyerangan jaringan oleh pihak dalam maupun dari luar. Dibutuhkannya suatu sistem keamanan jaringan menjadi salah satu aspek penting yang perlu diperhatikan.

Survei yang dilakukan *oleh infowatch analytical center* yang diunggah di situs www.securelist.com (diakses 21 Oktober 2013) memperlihatkan bahwa pada salah satu hasil survei menyatakan terjadi serangan jaringan yang kebanyakan merupakan serangan *denial of service*(dos) sebanyak 72,1% dan *exploit buffer-overflow* pada peringkat kedua sebanyak 16,4%. Survei yang juga menyebutkan bahwa ancaman yang terjadi dari pelanggaran *internal* maupun *external* menghasilkan (45%) terjadi di *external* dan (55%) terjadi di *internal.*

Berdasarkan survei yang dijelaskan sebelumnya dapat diambil kesimpulan bahwa pelanggaran terjadi sebanyak (55%) merupakan pelanggaran *internal* dan sebanyak (72,1%) adalah serangan *Denial of service*

Kejadian diatas dapat menjadi referensi bagi PT. Wahana Lintas Nusa Persada untuk menyadari bahwa semakin bertambahnya pelanggan, semakin meningkatnya node pada jaringan wahana yang harus selalu dimonitoring guna meningkatkan pelayanan. Dimana pelayanan kepada para pelanggan menjadi salah satu faktor yang berguna dalam memenangkan persaingan dan mencari peluang bisnis. Semakin bertambahnya pelanggan secara tidak langsung juga dapat memastikan kontinuitas bisnis dan mengoptimalkan *return on investmen* (ROI).

Pada saat ini para *technical support* PT Wahana Lintas Nusa Persada selalu *stanby* untuk melayani *troubleshooting* yang bisa terjadi sewaktu-waktu. Dalam manajemen setiap *node client* belum adanya sistem yang dapat memberikan *report* adanya serangan jaringan kepada *technical support* guna membantu dalam melakuakan analisis terhadap masalah yang terjadi ketika salah satu *client* mengalami *trouble* dalam jaringannya.

Beradasarkan latar belakang tersebut, penulis ingin mencoba menganalisis masalah yang dihadapi dan membuat solusi dari masalah tersebut. Dengan membuat *reactive intrusion detection system* menggunakan mikrotik berbasis *log* dan *mail report* agar para *technical support* yang sedang mobile dapat melakukan analisis terhadap *trouble* jaringan dan mengantisipasi bahaya keamanan dari faktor *internal* serta serangan terhadap jaringan pada *client* PT.Wahana Lintas Nusa Persada.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang dijelaskan sebelumnya, maka dapat diambil suatu rumusan masalah sebagai berikut.

1. Bagaimana membangun *reactive intrusion detection sistem* menggunakan mikrotik versi 5.20 yang dapat menampilkan *log* dan mengirim *email report* ke *technical support* PT. Wahana Lintas Nusa Persada ?

1.3 Batasan Masalah

Untuk menghidari pembahasan masalah yang terlalu luas, maka pada penulisan skripsi ini diberikan batasan yang jelas sehingga materi yang disampaikan tepat sasaran. Berikut batasan masalah tersebut.

1. Membangun rancangan *reactive intrusion detection sistem* menggunakan mikrotik versi 5.20 pada jaringan client PT. Wahana Lintas Nusa Persada yang telah dizinkan.
2. Pendekatan *reactive intrusion detection system* yang digunakan adalah *rule base detection*.
3. *Sistem reactive intrusion detection* yang akan dibangun menggunakan jenis *network-based IDS* (NIDS).
4. Uji coba dilakukan pada komputer client dengan sistem operasi XP SP2 dengan *reactive intrusion detection sistem* dengan mikrotik versi 5.20 pada PC *router*.
5. Uji coba serangan adalah dengan melakukan FTP Bruteforce, SSH Bruteforce, *ICMP flood (Ping of dead)*.

6. Pengujian serangan dilakukan secara serentak (*simultan*) dan berurutan (*sekuensial*).
7. Tidak membahas uji coba jenis-jenis serangan yang dilakukan ke jaringan secara lebih mendalam.

1.4 Maksud Dan Tujuan

1.4.1 Maksud

Sebagai salah satu syarat menyelesaikan pendidikan S1 pada program studi teknik informatika STMIK AMIKOM Yogyakarta.

1.4.2 Tujuan

Membangun *reactive intrusion detection system* menggunakan mikrotik versi 5.20 pada PT. Wahana Lintas Nusa Persada dengan kemampuan :

a. Dapat menampilkan *log*.
b. Dapat mengirim *email report*.

1.5 Manfaat Penelitian

Adapun manfaat yang ingin dicapai dalam penelitian ini adalah.

1.5.1 Bagi Penulis

- Memperoleh gelar sarjana komputer dari STMIK AMIKOM Yogyakarta.
- Memberikan gambaran tentang kondisi jaringan komputer di dunia nyata.
- Memberikan wawasan yang lebih luas dari penerapan ilmu-ilmu yang diperoleh selama perkuliahan.

1.5.2 Bagi Perusahaan

- Sebagai tolak ukur sejauhmana menerapkan *security policy*.
- Sebagai bahan pertimbangan bagi perusahaan untuk menerapkan *reactive intrusion detection system* menggunankan mikrotik versi 5.20 berbasisi *log* dan *mail report*.
- Membantu para *technical support* dalam menganalisis *trouble* jaringan pada *client* PT. Wahana Lintas Nusa Persada.

1.6 Metode Pengumpulan Data

Metode pengumpulan data yang dilakukan penulis adalah sebagai berikut:

1.6.1 Metode Observasi

Observasi dilakukan dengan berbagai tahapan adalah sebagai berikut:

1. Melakuakan survei langsung ke PT. Wahana Lintas Nusa Persada untuk mengetahui sistem dan model jaringan yang sedang berjalan untuk mengetahui masalah yang dihadapi.
2. Melakukan analisis terhadap temuan survei.
3. Melakukan identifikasi *hardware* dan *software*.

1.6.2 Metode Wawancara

Teknik pengumpulan data yang dilakuakan dengan mengadakan tanya jawab secara langsung maupun secara online kepada karyawan PT. Wahana Lintas Nusa Persada yang telah diberikan wewenang untuk melakukan tanya jawab guna memperoleh keterangan yang dibutuhkan untuk penelitian. Contoh pertanyaan saat melakukan wawancara adalah.

1. Tolopogi jaringan yang saat ini dipakai.
2. Peralatan jaringan serta media komunikasi yang dipakai saat ini.
3. Permasalahan yang sering terjadi pada jaringan client PT. Wahana Lintas Nusa Persada.
4. Sejauh mana penerapan *security policy* dan *reactive intrusion detection system* pada jaringan client PT. Wahana Lintas Nusa Persada.

1.6.3 Metode Pustaka

Untuk mendukung analisis dan perancangan *reactive intrusion detection system* ini, digunakan metode pustaka sebagai referensi. Pustaka yang digunakan berupa buku-buku referensi, dokumen yang relevan, artikel-artikel yang berkaitan dengan topik skripsi dan berbagai informasi mengenai *reactive intrusion detection sistem* dari internet.

1.7 Metodelogi Penelitian

Metodelogi penelitian yang dilakukan penulis adalah sebagai berikut:

1. Analisa Sistem

Metode analisis yang digunakan untuk mengidentifikasi masalah yang terjadi di lapangan dengan melakukan wawancara untuk mengidentifikasi masalah, selanjutnya adalah hipotesis solusi, juga analisis kebutuhan sistem.

2. Perancangan Sistem

Dalam perancangan sistem dilakukan konsep permodelan sistem seperti perancangan topologi, gambaran umum sistem, perancangan *firewall*, logika

scripting untuk dapat menampilkan *log* dan mengirim *email report* dan penjadwalan eksekusi *script* tersebut serta prosedur implementasi.

3. Konfigurasi Sistem

Proses konfigurasi sistem antara lain:

1. Konfigurasi *Network Time Protokol* (NTP).
2. Konfigurasi *firewall* pada mikrotik versi 5.20.
3. Konfigurasi *script* pada mikrotik versi 5.20.
4. Konfigurasi penjadwalan *script* tersebut dieksekusi.
5. Konfigurasi *system logging* dan *tool email* pada mikrotik versi 5.20.
6. Konfigurasi *Syslog Server The dude* dan *Mikrotik Syslog*.

4. Implementasi

Pada tahap ini dilakukan konfigurasi sub-sistem pada *PC Router* yang terinstall mikrotik versi 5.20 yang selanjutnya diintegrasikan untuk membangun *reactive intrusion detection system* dan konfigurasi *Syslog Server* untuk dapat menampilkan log secara terpusat, sesuai dengan rancangan sistem.

5. Pengujian Sistem

Sebelum sistem diimplemnetasikan maka perlu diadakan pengujian sistem dengan melakukan percobaan serangan secara *simultan* dan *sekuensial* terhadap sistem, apakah sistem dapat mengirimkan *email report* dan menampilkan *log* ketika percobaan penyerangan sistem dilakukan.

6. Evaluasi Sistem

Evaluasi sistem dilakukan untuk mengetahui apakah sistem telah berjalan sesuai dengan tujuan penelitian.

7. Pemeliharaan Sistem

Tahap pemeliharaan sistem dilakukan dengan pemantauan dan pemerikasaan rutin dengan melakukan *update firewall* agar sistem dapat beroperasi dengan baik.

1.8 Sistematika Penulisan

Penulisan skripsi ini yang berjudul "Analisa dan Perancangan *Reactive Intrusion Detection System* Menggunakan Mikrotik Berbasis *Log* dan *Mail Report*" mempunyai sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Bab ini merupakan pendahulaun yang menjelaskan tentang latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, metode pengumpulan data, pengembangan sistem dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini menjelaskan landasan-landasan teori yang digunakan sehubungan dengan percangan *reactive intrusion detection system* menggunakan mikrotik berbasis *log* dan *mail report*.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini berisi tentang analisis sistem yang akan dibangun, gambaran umum sistem dan perancangannya. Membahas tempat penelitian, identifikasi temuan masalah, hipotesis solusi, analisis kebutuhan sistem, perancangan topologi jaringan, perancangan *firewall* dan prosedur implementasi sistem.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini berisi pembahasan langkah-langkah dalam penerapan sistem, konfigurasi mikrotik versi 5.20 sebagai *reactive intrusion detection system*, percobaan serangan jaringan, serta pengujian terhadap hasil penelitian apakah telah sesuai dengan tujuan penelitian dan pembahasan terhadap hasil yang telah dicapai.

BAB V PENUTUP

Bab ini merupakan bagian akhir dari penulisan skripsi yang berisi kesimpulan dan saran yang diperoleh dari perancangan *reactive intrusion detection system* mengguanakan mikrotik versi 5.20 berbasis *log* dan *mail report*.

1.9 Pelaksamaan Kegiatan

Tabel. 1.1 Daftar Pelaksanaan Kegiatan

No	Nama Kegiatan	Tahun 2013																			
		September				Oktober				November				Desember				Januari			
		I	II	III	IV	I	II	III	IV	I	II	III	IV	I	II	III	IV	I	II	III	IV
1	Riset Lokasi																				
2	Penulisan Laporan Awal																				
3	Pengumpulan Data																				
4	Analisis dan Perancangan																				
5	Pembuatan Sistem																				
6	Testing dan Implemnetasi																				
7	Evaluasi																				
8	Penulisan Laporan Akhir																				