

## **BAB I**

### **PENDAHULUAN**

#### **1.1 Latar Belakang**

Rata-rata jumlah insiden keamanan jaringan komputer per hari mencapai 120.000 insiden dan aktivitas ini cenderung akan semakin meningkat. Menurut Lumanto (2012), Serangan terbesar ber-kategori SQL sekitar 82% diikuti oleh DNS, WEB Base, Windows Base, Botnet dan sebagainya. Sumber serangan 65% berasal dari Indonesia, dengan jumlah serangan sebesar 79.000 dalam sehari, baru kemudian diikuti oleh negara-negara lain di luar Indonesia, target serangan 49% adalah ke Indonesia dengan jumlah serangan sebesar 57.000 serangan perhari. Jumlah serangan mencapai 2.661.194 serangan, dimana serangan tertinggi terjadi pada tanggal 17 Oktober 2012 yaitu sebesar 121.238 serangan dan serangan terendah terjadi pada tanggal 2 Oktober 2012 sebesar 46.385 serangan. Pada bulan Oktober 2012 rata-rata serangan berjumlah 85.844 serangan per hari.

Menurut Salahuddien (2009), tren serangan terbesar diarahkan pada port 53 dengan total mencapai 300.000 serangan atau 12.000 serangan per hari. Serangan kedua terbesar diarahkan pada port 1434 dengan total serangan mencapai 278.000 serangan atau 8.000 serangan perhari, sedangkan serangan ketiga terbesar diarahkan pada port 1433 dengan total serangan 225.000 atau 7.000 serangan per hari. Puncak serangan terjadi pada tanggal 20 Oktober 2012 yang ditujukan pada port 53 dimana mencapai 21.000 serangan Penyebab insiden tertinggi lainnya

adalah diakibatkan oleh kesalahan prosedur pengamanan dan kelalaian pengelola sistem, kemudian akibat pengabaian dan ketiadaan prosedur serta pengelolaan sistem pengamanan yang memadai.

Menurut Salahuddien (2009), pada laporan tahunan Indonesia Security Incident Response Team Internet Infrastructure (ID-SIRTII) juga telah mengadakan survey random sampling tentang kesiapan sistem dan prosedur terhadap sejumlah perusahaan serta instansi pemerintah di berbagai sektor yang bisa dianggap strategis dan kritikal. Hasilnya meskipun sebagian besar telah memiliki instrument pengamanan namun banyak sekali kelemahan akibat sistem yang diterapkan secara parsial, pengabaian oleh manajemen, kelalaian dan masih rendahnya sikap perilaku pengamanan sendiri (*self protection*), semua ini mengakibatkan tingginya angka insiden yang tidak disadari oleh pemilik sistem.

Pada penelitian ini yang menjadi pokok pembahasan adalah permasalahan yang muncul dari penerapan keamanan jaringan komputer, karena permasalahan yang muncul bukan hanya datang dari luar seperti usaha-usaha pembobolan terhadap keamanan tersebut tetapi kendala yang terjadi akibat penerapan dari sekuritas itu sendiri. Keterbatasan *resource* dalam penerapan sistem keamanan, sistem yang diterapkan secara parsial, pengabaian oleh manajemen, kelalaian dan masih rendahnya sikap perilaku pengamanan sendiri (*self protection*) menjadi beberapa kendala utama. Analogi yang dapat dicontohkan misalkan pada kasus administrator keamanan yang harus setiap saat memantau kondisi sistem agar dapat berjalan normal tanpa ada gangguan dari dalam maupun dari luar, pada kondisi ini sistem keamanan akan bergantung penuh pada kesiagaan administrator

dalam menjaga keamanan, hal ini menjadikan sistem rentan mendapat gangguan dikarenakan kelengahan administrator keamanan dalam melakukan monitoring terhadap keamanan sistem atau pun dalam menutupi celah keamanan yang tidak terpantau selalu menjadi kasus yang sering muncul.

Dalam tulisan ini akan dibahas sistem peringatan keamanan untuk meningkatkan *self protection* melalui pendekatan deteksi intrusi sebagai alternatif solusi permasalahan yang terjadi, dengan kata lain memberikan peringatan secara *real-time* kepada administrator mengenai status keamanan sistem melalui SMS Gateway dengan memanfaatkan filter paket data.

Layanan SMS Gateway banyak dimanfaatkan untuk melakukan pendistribusian informasi secara cepat pada setiap penggunanya, pendistribusian informasi yang cepat dengan SMS Gateway memberikan sebuah ide pengamanan dengan pendekatan yang berbeda. SMS Gateway juga dipilih sebagai media peringatan karena membuat administrator secara *real-time* mendapat informasi tentang status keamanan tanpa harus bersentuhan dengan sistem. Pemanfaatan *packet capture* yang kemudian paket di *filter* berdasarkan kebijakan pada sistem keamanan yang diterapkan, dari sini sistem dapat mendeteksi gangguan atau pun ancaman yang mungkin saja masuk dan melaporkannya. *Packet capture* banyak digunakan pada sistem keamanan untuk melakukan monitoring terhadap lalu lintas data jaringan komputer (Kumar and S., 2012), (Al-Mukhtar, 2012), (Asrodia and Patel, 2012). Langkah prevensi menjadi fokus utama pada sistem ini, dengan melakukan langkah pencegahan *availability* dari sistem yang di *manage* akan lebih tinggi karena kemungkinan sistem *down* lebih rendah (Stiawan,

Abdullah and Idris, 2011). Sebagai contoh serangan *Distributed Denial of Service* (DDoS) dengan teknik *flooding request*, dengan memonitor paket data kita dapat mengetahui *request* palsu yang dikirimkan berulang sehingga dapat dilakukan langkah pencegahan sebelum terjadi kegagalan sistem (Agah and Das, 2007) (Guptas, Joshi and Mirsa, 2010) (Sharma, Sharma and Singh, 2012) (Chen et al., 2008).

## 1.2 Rumusan Masalah

Permasalahan keamanan jaringan yang menjadi inti pembahasan adalah :

1. Bagaimana membangun sebuah sistem keamanan jaringan komputer yang dapat melakukan peringatan.
2. Bagaimana melakukan *report* peringatan dengan memanfaatkan sistem SMS Gateway.
3. Bagaimana mengembangkan sistem keamanan jaringan komputer yang dapat melakukan monitoring terhadap aliran data dari luar yang masuk secara *real-time*.

## 1.3 Batasan Masalah

Pengembangan sistem keamanan mempunyai lingkup yang sangat luas dan memperhitungkan berbagai faktor dari segi keamanan itu sendiri, sehingga pada kasus ini pembahasan dibatasi pada :

1. Penerapan hanya untuk jaringan internal (*Local Area Network*).
2. Pengembangan terbatas hanya pada *platform Windows* dan berbasis *desktop*.

3. Pengembangan dengan menerapkan *SMS Gateway* sebagai pengiriman *report* informasi peringatan.
4. Pengiriman *report* peringatan dari *SMS Gateway* bersifat satu arah.
5. Sistem pendeteksi menggunakan *packet capture* dan *packet filter*.
6. Filter paket data berdasarkan *source* atau *destination* IP dan port.
7. Sistem mendeteksi berdasarkan kebijaksanaan keamanan yang diterapkan.
8. Sistem bertugas hanya mendeteksi dan melaporkan secara *real-time*.
9. Sistem tidak bertanggung jawab atas peringatan yang tidak di respon oleh administrator.

#### **1.4 Keaslian Penelitian**

Berdasarkan hasil studi terhadap beberapa jurnal ilmiah, buku dan penelitian yang pernah dilakukan belum ada penelitian yang fokus dalam membahas tentang Analisa dan Pengembangan Sistem Keamanan Jaringan Komputer Menggunakan *SMS Gateway* dan Paket Fiter.

#### **1.5 Tujuan dan Manfaat**

Adapun tujuan dari pengembangan sistem peringatan keamanan jaringan dengan menggunakan *SMS Gateway* bertujuan :

1. Membangun sistem keamanan jaringan komputer yang dapat melakukan peringatan.
2. Membangun sistem *SMS Gateway* yang dapat dimanfaatkan untuk melakukan *report* peringatan.

3. Membangun sistem keamanan yang dapat memonitoring aliran data yang masuk secara *real-time*.

Manfaat yang bisa didapat dari penelitian ini yaitu :

1. Untuk universitas sebagai bahan alternatif pembelajaran baru dengan pendekatan yang berbeda pada sistem keamanan.
2. Untuk pengguna sebagai alternatif pilihan dalam pengamanan jaringan komputer.
3. Untuk peneliti sebagai acuan untuk penelitian lain yang memiliki relevansi.
4. Dan yang terakhir untuk penulis sebagai pengalaman baru dalam penelitian dan pemenuhan syarat kelulusan dalam studi.

## **1.6 Sistematika Penulisan**

### **BAB I PENDAHULUAN**

Bab ini menjelaskan tentang latar belakang dari munculnya ide pembuatan penelitian ini yang juga termasuk didalamnya tujuan perumusan masalah, batasan masalah, tujuan dan manfaat serta beberapa hal terkait dengan penelitian ini.

### **BAB II TINJAUAN PUSTAKA**

Bab ini menjabarkan beberapa hasil studi terhadap penelitian-penelitian sebelumnya yang berkaitan dari beberapa literatur seperti jurnal ilmiah dan buku-buku.

### BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan tentang teknik-teknik dan langkah yang digunakan dalam melakukan penelitian ini secara sistematis. Lebih dalam lagi bab ini menjelaskan langkah penelitian secara rinci mulai dari pengumpulan data, teknik yang digunakan serta alat dan bahan dalam melakukan penelitian.

### BAB IV ANALISA DAN PERANCANGAN SISTEM

Bab ini menjabarkan hasil analisa dari penelitian yang dilakukan dan pembahasan dari pengembangan sistem yang teliti. Pembahasan bab ini menjelaskan hasil perancangan skema, algoritma deskriptif dan mekanisme kerja sistem yang dikembangkan pada penelitian ini.

### BAB V IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini menggambarkan teknik dan hasil dari implementasi dan pengujian perangkat lunak yang telah dibangun.

### BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan akhir dari penelitian yang dilakukan dan saran untuk pengembangan ataupun penelitian lanjutan dari penelitian ini.