BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan komputer sebagai bagian dari sebuah sistem sangatlah penting untuk menjaga validitas dan integritas serta menjamin ketersediaan layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha usaha penyerangan oleh pihak yang tidak berwewenang. Adanya perangkat teknologi yang serba modern dan canggih akan tidak ada artinya tanpa diimbangi oleh pengaturan dan penggunaan secara tepat, efektif dan efesien. Perangkat yang sederhana namun dikelola secara tepat bisa menstabilkan bahkan akan sangat membantu terhadap serangan-serangan dari penyerang (*hacker*).

Jenis- jenis serangan yang umum terjadi pada jaringan meliputi *Port Scanning* dan DoS (*Denial of Service*). *Port Scanning* dilakukan dengan cara mengidentifikasi port-port apa saja yang terbuka dan mengenali sistem operasi target. Sedangkan serangan DoS (*Denial of Service*) dan DDoS (*Distributied Denial of Service*) lebih sering terjadi pada jaringan yang luas seperti WAN (*Wide Area Network*). DoS digunakan untuk menghabiskan *resource* yang dimiliki komputer tersebut sampai akhirnya tidak dapat menjalankan fungsinya dengan benar dan secara tidak langsung mencegah komputer lain untuk mendapatkan akses layanan dari komputer yang diserang. Dalam kasus jaringan LAN, serangan ini biasanya terjadi meliputi *spoofing, port scanning, sniffing,* dan *backdoor*, apabila serangan-serangan tersebut terjadi maka dibutuhkan sistem yang dapat

mendeteksi secara akurat dan dapat mengidentifikasi spesifikasi serangan pada jaringan kemudian menyampaikan peringantan kepada administrator jaringan.

Sebagai upaya untuk bisa memantau kondisi jaringan, salah satu teknologi yang dapat digunakan adalah dengan menggunkan notifikasi pada SMS Gateway dan E-Mail dengan tujuan memberikan informasi secara *realtime* kepada administrator. Kelebihan yang dimiliki SMS antara lain yaitu terletak pada kesederhanaannya, sehingga mudah untuk diaplikasikan. Saat ini pasti semua ponsel memiliki fitur SMS, tidak peduli apakah ponselnya dukung 2G, 3G, 4G, *touch screen*, *dual SIM card*, atau hanya ponsel *polyphonic*. SMS juga tetap dapat dikirim walaupun ponsel penerima sedang tidak aktif dalam jangka waktu tertentu, karena SMS mempunyai *validity period*. Penyampaian SMS juga biasanya lebih cepat jika dibandingkan dengan kita mengirimkan lewat *messenger*. Tidak juga bergantung pada sinyal GPRS serta biayanya yang saat ini juga relatif murah juga menjadi salah satu alasan kenapa SMS digunakan secara luas. Sedangakan kelebihan E-Mail sendiri yaitu pengiriman yang cepat diterima oleh orang yang dituju, biaya relatif lebih murah, praktis dapat mengirim ke beberapa alamat sekaligus, dapat mengirimkan gambar, foto, video ataupun dokumen, surat yang masuk mudah dibaca disimpan dan dicetak serta E-Mail sendiri bersifat pribadi privasi terjamin aman di lindungi oleh *password*.

1.2 Rumusan Masalah

Beradasarkan dari uraian latar belakang di atas maka dapat dirumusakan suatu peramasalahan sebagai berikut:

1. Bagaimana sistem mendekteksi dan memonitoring adanya serangan pada jaringan LAN?
2. Bagaimana mengirimkan pemberitahuan atau notifikasi kepada administrator apabila jaringan LAN sedang diserang?

1.3 Batasan Masalah

Dengan terbatasnya kemampuan dan waktu maka penulis menyadari bahwa perlu adanya batasan masalah antara lain:

1. Sistem hanya mampu mengirimkan notifikasi tentang kondisi jaringan bukan untuk memperbaiki jaringan ketika *down* atau tersusupi.
2. Sistem ini hanya dikonfigurasi pada sistem monitoring dan *alert* notifikasi bukan konfigurasi membangun sistem jaringan.
3. Sistem ini hanya diuji dengan beberapa macam aplikasi penyerangan dan belum diuji dengan jenis serangan yang lainnya
4. Sistem membutuhkan pulsa dan paket internet serta sinyal yang baik untuk mengirimkan notifikasi.

1.4 Tujuan Penelitian

Pemilihan Snort karena selain *open source* dan gratis juga bisa ditambahkan aturan-aturan yang bisa disesuaikan dengan kebutuhan. Sedangkan pemilihan SMS Gateway dan E-Mail untuk mengirimkan *alert* atau notifikasi yaitu SMS sendiri adalah bagian penting dari sebuah ponsel. Di era ini pasti setiap

orang memiliki ponsel bahkan lebih dari satu begitupula E-Mail setiap orang pasti memiliki E-Mail banyak perusahan yang menawarkan pembuatan E-Mail sebagai contoh Google dan Yahoo. Pemilihan Snort sebagai *tools* pendeteksi serangan serta SMS Gateway dan E-Mail karena mudah untuk di implementasikan kedalam sistem IDS (*Intrusion Detection System*) ini yang nantinya sistem akan mengirimkan *alert* berupa notifikasi kepada administrator ketika terjadi serangan atau penyusupan. Sehingga dengan peringatan tersebut administrator dapat mengambil tindakan selanjutnya. Ini akan sangat membantu administrator untuk memantau jaringan secara *realtime* tanpa harus *standby* didepan komputer.

1.5 Manfaat Penelitian

Berdasarkan penelitian yang penulis buat, maka ada manfaat bagi penulis, antara lain:

1. Dapat menerapkan ilmu yang diperoleh di Universitas AMIKOM Yogyakarta.
2. Dapat membandingkan antara teori dan praktek dalam pembuatan sebuah hasil karya.
3. Untuk memperluas wawasan dan memperdalam pengalaman mengenai sistem keamanan sekaligus mencegah terjadinya penyusupan terhadap sistem jaringan komputer.
4. Sebagai salah satu syarat kelulusan Srata Satu (S1) Jurusan Informatika Universitas AMIKOM Yogyakarta.
5. Dapat memberikan peringatan kepada administrator dan memberikan kemudahan administrator dalam memantau jaringan.

1.6 Metode Penelitian

Metode penelitian yang dilakukan penulis untuk mendukung kebenaran materi atau uraian teori pembahasan dalam penelitian ini adalah sebagai berikut :

1.6.1 Metode Pengumpulan Data

1. Studi Pustaka

   Pengumpulan data dilakukan dengan cara membaca sumber - sumber ilmiah dari jurnal dan skripsi di Universitas AMIKOM Yogyakarta maupun di Internet dan buku sebagai referensi untuk mendapatkan informasi yang sesuai dengan topik permasalahan yang dianalisa dan diteliti. Informasi-informasi tersebut untuk selanjutnya akan dijadikan sebagai landasan teori dalam pemecahan masalah maupun penyusunan laporan, agar dapat dipertanggung jawabkan secara ilmiah.

2. Studi Lapangan

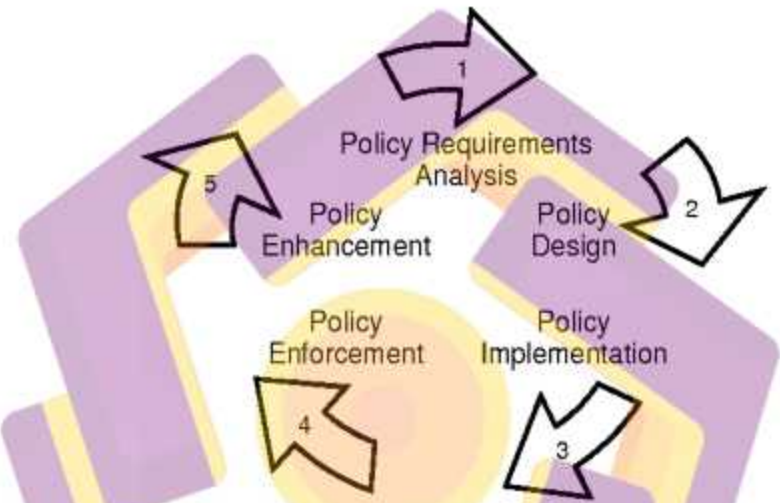
   Langkah ini dilakukan observasi berupa pengamatan langsung dan praktik dengan perangkat yang digunakan untuk memperoleh gambaran atau topologi dalam proses penerapan sistem IDS (*Intrusion Detection System)*.

3. Studi Literatur

   Studi literatur dilakukan dengan mempelajari dan membaca hasil laporan penelitian yang berhubungan dengan topik peneltian yang berkaitan dengan masalah IDS (*Intrusion Detection System)*.

1.6.2 Metode Pengembangan Sistem

Pada penelitian ini penulis menggunakan metode *Security Policy Development Life Cycle* (SPDLC), menurut Luay A. Wahsheh dan Jim Alves-Foss (2008).



Gambar 1.1 SPDLC (*Security Policy Development Life Cycle*)

(Sumber : https://www.semanticscholar.org/paper/Security-Policy-Development-%3A-Towards-a-Life-Cycle-Wahsheh-Alves-Foss/9fddb6cdf639847437 8c83c75971f141296d96cc)

1. Analisa (*Analysis*)

Tahapan pertama pada metode pengembangan sistem SPDLC (*Security Policy Development Life Cycle*) adalah analisis. Analisis adalah sebuah proses yang dilakukan untuk memecahkan suatu permasalahan kemudian memperikan solusi dari permasalah itu.

2. Desain (*Design*)

Selanjutnya adalah *Design*, tahap desain atau perancangan ini adalah membuat sebuah sistem yang akan dibangun, diharapkan dalam pembangunan sistem yang didesain akan membarikan gambaran seutuhnya dari kebutuhan yang sesuai. Pada fase ini, penulis merancang topologi sistem jaringan untuk simulasi dan sebagai reprensentasi sistem nyata untuk merancang sistem.

3. Implementasi (*Implementation*)

Tahap selanjutnya adalah implementasi atau penerapan, pada fase ini merupakan proses untuk mewujudkan sebuah sistem yang baru dalam sistem yang sebenarnya. Ini melingkupi instalasi dan konfigurasi komponen sistem.

4. Pengujian (*Enforcement*)

Setelah tahap implementasi adalah tahap *enforcement* atau pengujian dimana tahap ini penting. Proses pelaksanaan atau penyelenggaraan dilakukan melalui aktifitas pengoperasian dan pengamatan sistem yang sudah dibangun dan diterapkan apakah sistem sudah berjalan dengan baik dan benar.

5. Peningkatan (*Enhancement*)

Tahap terakhir pada metode SPDLC (*Security Policy Development Life Cycle*) adalah enhancement atau peningkatan. Pada fase ini akan dilakukan aktifitas peningkatan dan perbaikan terahadap sistem yang telah dibangun.

1.7 Sistematika Penelitian

Adapun sistematika penulisan agar dapat membantu dan mempermudah dalam melakukan penulisan laporan agar tidak menyimpang dari batasan masalah yang terdapat pada kerangka penulisan skripsi maka ditulis menjadi 5 bab sebagai berikut :

BAB I : PENDAHULUAN

Bab ini berisi tentang gambaran tentang latar belakang masalah, rumusan masalah, batasan masalah, manfaat dan tujuan penelitian, dan sistematika penulisan.

BAB II : LANDASAN TEORI

Bab ini membahas tentang dasar-dasar teori yang berkaitan dengan topik penelitian.

BAB III : METODE PENELITIAN

Bab ini membahas tentang analisis dan metode penelitian yang digunakan.

BAB IV : HASIL DAN PEMBAHASAN

Bab ini membahas tentang implementasi dan hasil pengujian dari sistem.

BAB V : PENUTUP

Bab ini merupakan bagian akhir dari penulisan penelitian yang berisi kesimpulan dan saran untuk sistem.

DAFTAR PUSTAKA