BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi dan akses *Internet* pada era ini memberikan keuntungan serta kemudahan bagi pengguna komputer dalam berbagi maupun mendapatkan informasi. Kini teknologi menjadi salah satu kebutuhan utama bagi manusia. Di sisi lain, semakin berkembangnya teknologi maka keamanan informasi menjadi salah satu problematika.

Keamanan merupakan salah satu masalah terbesar bagi pengguna *Internet* terutama penyedia sebuah *server* maupun sistem jaringan komputer. Masalah tersebut menimbulkan kecenderungan besar untuk memiliki *Intrussion Detection System* (IDS) pada setiap jaringan. IDS merupakan perangkat lunak atau perangkat keras sistem yang secara otomatis melakukan proses pemantauan (*monitoring*) insiden yang terjadi dalam sistem komputer atau jaringan serta menganalisis tanda-tanda adanya masalah terhadap keamanan sistem (Anitha, 2011). IDS melakukan penyaringan terhadap lalu lintas dan melakukan analisis terhadap informasi yang didapatkan guna mendapatkan bukti adanya percobaan penyusupan terhadap sistem.

Sistem yang tidak aman akan berdampak negatif bagi penyedia maupun pengguna sistem. Oleh karena itu, perlu adanya *monitoring* keamanan jaringan dengan tujuan untuk meminimalisir terjadinya penyusupan. Salah satu aplikasi yang digunakan sebagai IDS adalah Snort. Aplikasi *opensource* tersebut memiliki kemampuan untuk mendeteksi adanya penyusupan terhadap sistem sesuai dengan aturan yang telah ditetapkan. Hasil deteksi tersebut akan direkam dan disimpan pada *database*. Peringatan deteksi dapat memanfaatkan aplikasi *instant messaging* sebagai media untuk memberitahu kepada administrator jaringan mengenai indikasi penyusupan ke *server*.

Aplikasi *instant messaging* saat ini popular digunakan oleh berbagai kalangan. Salah satu aplikasi tersebut yang memiliki berbagai fitur yaitu Telegram. Aplikasi tersebut selain untuk *chatting*, terdapat fitur pertukaran

dokumen. Fitur tersebut dapat dimanfaatkan untuk memberikan laporan keamanan sistem dalam bentuk dokumen digital.

Dalam penelitian sejenis lainnya, terdapat beberapa aplikasi yang telah dikembangkan seperti *SMS Gateway*. Fitur yang ditampilkan pada penelitian tersebut hanya sebatas notifikasi pesan saja, belum termasuk tahap memberikan laporan dalam bentuk *file* dokumen.

Sistem peringatan (*alert*) ini akan dikirimkan ke administrator jaringan dalam beberapa kondisi, seperti (1) jika terindikasi adanya penyerangan, maka sistem akan mengirimkan notifikasi secara *real time*, (2) memberikan laporan dalam rentan waktu tertentu terhadap aktifitas *monitoring* jaringan dalam bentuk gambar grafik dan kuantitas lainnya.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan di atas, maka dapat dirumuskan masalah pada penelitian ini yaitu bagaimana membuat sistem pendeteksi adanya penyusup dan peringatan melalui notifikasi aplikasi *instant messaging* Telegram.

1.3 Batasan Masalah

Untuk menjaga fokus penelitian yang akan dilakukan, adapun batasan-batasan dalam pembuatan sistem, yaitu :

a. Pengujian menggunakan *Operating System* Kali Linux
b. Server yang dilindungi yaitu sebuah *server* dengan *Operating System* Ubuntu Server 14.04 yang memiliki layanan FTP, SSH, dan Web Server
c. Notifikasi melalui aplikasi *instant messaging* Telegram versi 3.10.1
d. Skenario pengujian adalah *Port Scanning* (SYN, FIN, XMAS), FTP *Bad login*, SSH *Brute force*, Ddos *Attack*

1.4 Tujuan Penelitian

Tujuan yang akan dicapai dari penelitian ini adalah membangun sistem deteksi dan pemberitahuan adanya penyusup pada sebuah sistem sebagai solusi untuk meminimalisir insiden terhadap keamanan sistem jaringan komputer.

1.5 Manfaat Penelitian

Manfaat yang dapat diperoleh dari terlaksananya penelitian tugas akhir ini adalah:

a. Terciptanya sistem yang mampu mendeteksi adanya penyusup terhadap komputer *server* pada jaringan komputer.
b. Administrator mendapatkan pemberitahuan secara *real time* maupun laporan detail terhadap adanya serangan pada komputer *server*.

1.6 Metodologi Penelitian

Metode penelitian yang akan digunakan pada Tugas Akhir (TA) ini terdiri dari beberapa tahapan berikut:

a. Studi Pustaka

   Studi pustaka bertujuan untuk memperkaya informasi dan menambah wawasan terkait dengan penelitian yang dilaksanakan.

b. Perancangan Desain

   Menyusun arsitektur jaringan yang akan digunakan untuk pengujian sistem serta menentukan alur kerja sistem.

c. Konfigurasi

   Melakukan instalasi *Operating System* yang dibutuhkan, pemasangan aplikasi IDS pada komputer *server* serta konfigurasi IDS. Konfigurasi juga dilakukan untuk menampilkan laporan insiden dan pemberitahuan notifikasi menggunakan aplikasi *instant messaging* Telegram.

d. Pengujian Sistem

   Melakukan pengujian sistem dengan metode penyerangan yang telah ditentukan serta pengujian terhadap notifikasi hingga pengiriman dokumen laporan dalam format PDF.

e. Analisa dan Evaluasi

   Menganalisa dan mengevaluasi kinerja sistem deteksi adanya penyusup pada sistem yang dibuat.

1.7 Sistematika Penulisan

Laporan penelitian Tugas Akhir ini disusun dengan strukur dan kerangka penulisan sebagai berikut :

BAB I PENDAHULUAN

Bab ini merupakan bab pendahuluan yang membahas tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan yang diangkat menjadi penulisan laporan Tugas Akhir.

BAB II LANDASAN TEORI

Bab ini membahas tentang dasar-dasar teori berdasarkan permasalahan yang digunakan sebagai landasan dalam penelitian mengenai *Intrusion Detection System* dan pembuatan sistem.

BAB III METODOLOGI

Bab ini memuat uraian tentang gambaran umum sistem, perancangan sistem, analisis kebutuhan sistem yang mencakup perangkat lunak yang digunakan dalam penelitian.

BAB IV HASIL DAN PEMBAHASAN

Pada bagian ini memuat dokumentasi hasil pengujian dan pembahasan mengenai kinerja sistem mulai dari tahap instalasi, konfigurasi dan hasil yang didapatkan terhadap sistem yang telah dibuat.

BAB V PENUTUP

Bab ini memuat uraian kesimpulan dari seluruh rangkaian perancangan hingga pengujian sistem terhadap penelitian yang dilaksanakan dan saran untuk pertimbangan maupun pengembangan sistem keamanan selanjutnya.