BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Salah satu aspek keamanan jaringan komputer yang paling penting adalah terhindar dari segala gangguan. Akan tetapi keamanan jaringan masih sering dipandang sebelah mata oleh banyak kalangan bisnis bahkan orang yang terjun di bidang teknologi informasi juga banyak yang tidak memperdulikan soal keamanan jaringan. Pada saat ini komputer dan teknologi jaringan sudah mencapai perkembangan yang amat pesat, akan tetapi seiring dengan kemajuan teknologi jaringan tersebut juga diikuti dengan semakin maraknya gangguan – gangguan maupun ancaman yang mengganggu teknologi keamanan jaringan tersebut. Adapun salah satu sistem yang bisa digunakan untuk mencegah gangguan tersebut adalah dengan menerapkan *firewall*. Secara umum firewall berfungsi sebagai lapisan pelindung untuk menahan serangan-serangan yang sifatnya mengancam keamanan jaringan. Firewall untuk mendeteksi gangguan dari segi-segi yang telah dipaparkan diatas memang telah banyak digunakan di berbagai macam lingkungan kerja, akan tetapi masih banyak firewall yang masih saja gagal dalam menangani gangguan tersebut dan masih memerlukan campur tangan seorang administrator dalam hal penanganan serangan dan penulisan rules firewall. *Intrusion detection system* (IDS) sebagai salah satu perangkat keamanan jaringan komputer yang berfungsi sebagai pendeteksi serangan merupakan salah satu bagian yang tidak bisa dipisahkan dari firewall, karena keduanya saling melengkapi. Ada beberapa macam perangkat keamanan buatan *vendor* ternama

STIKOM SURABAYA

yang telah menerapkan metode *artificial intelligence* seperti produk dari Juniper Networks dan GFI, akan tetapi sebagian besar perangkat keamanan tersebut harganya sangat mahal. Karena kondisi inilah diperlukannya suatu sistem keamanan dengan daya beli yang bernilai murah dan dilengkapi dengan suatu kecerdasan buatan, mampu melakukan analisa yang akurat serta mengambil tindakan sendiri atas kondisi yang ada. Adapun sistem yang akan diterapkan adalah firewall dengan menggunakan metode *fuzzy logic* dan *single layer neural network*, dimana dengan menggunakan penggabungan dua metode ini dapat membantu untuk mendapatkan hasil analisa yang lebih akurat dalam hal pendeteksian serangan, dengan menggunakan metode *fuzzy logic* diharapkan dapat menghasilkan analisa awal terhadap bentuk serangan sehingga nantinya keluaran dari *fuzzy logic* akan menjadi masukan untuk analisa lebih lanjut dengan metode *neural network,* yang kemudian akan mengelompokkan serangan tersebut menjadi beberapa macam kategori sehingga akan menghasilkan rules-rules baru ke dalam firewall untuk melakukan respon balik.

1.2. Perumusan Masalah

Berkaitan dengan latar belakang diatas maka permasalahan dalam Tugas Akhir ini dapat dirumuskan sebagai : " bagaimana menerapkan kecerdasan buatan ke dalam firewall dengan menggunakan metode fuzzy logic dan single layer neural network? ".

STIKOM SURABAYA

1.3. Pembatasan Masalah

Perlu diberikan beberapa pembatasan permasalahan dengan tujuan agar pembahasan tidak meluas dan menyimpang dari tujuan. Adapun batasan permasalahan dari sistem yang akan dibuat ini adalah hanya memfokuskan pada pemantauan paket dalam protokol TCP/IP.

1.4. Tujuan

Tujuan Tugas Akhir ini adalah membangun dan mengimplementasikan suatu firewall yang memiliki pola pikir seperti manusia yaitu mampu melakukan pendeteksian, analisis dan bertindak sendiri dalam menangani masalah yang timbul. Firewall tersebut diimplementasikan dengan menggunakan 2 metode yaitu fuzzy logic dan single layer neural network. Metode fuzzy logic digunakan untuk melakukan analisis paket untuk mengklasifikasikan kondisi awal dari suatu paket data. Sedangkan metode single layer neural network digunakan untuk melakukan analisa perhitungan hasil keluaran fuzzy, sehingga didapatkan suatu kesimpulan terakhir hasil keluaran dari neural network untuk menentukan klasifikasi serangan yang terjadi. Hasil klasifikasi atas jenis serangan yang terjadi akan memicu firewall secara otomatis untuk melakukan respon balik (*blocking ip-address*) dengan cara memasukkan *rules* baru ke dalam iptables.

1.5. Kontribusi

Sebagian besar sistem firewall yang digunakan saat ini, umumnya masih membutuhkan bantuan dari seorang administrator jaringan untuk melakukan *update rules* (pembaharuan kebijakan-kebijakan yang diterapkan di firewall) dan

STIKOM SURABAYA

respon balik untuk menangani sebuah serangan. Walaupun saat ini sudah ada beberapa vendor-vendor ternama yang menawarkan sebuah sistem keamanan jaringan yang berbasis artificial intelligence, akan tetapi harganya masih sangat mahal.

Sehingga dengan dibuatnya tugas akhir dengan judul "Penerapan Firewall Dengan Menggunakan Metode Fuzzy Logic Dan Single Layer Neural Network" , dengan menggunakan 2 macam metode yaitu fuzzy logic yang digunakan untuk melakukan klasifikasi atas kondisi awal dari suatu paket data dan metode single layer neural network untuk melakukan analisa perhitungan hasil keluaran fuzzy, sehingga didapatkan suatu kesimpulan terakhir hasil keluaran dari neural network untuk menentukan klasifikasi serangan yang terjadi. Hasil klasifikasi atas jenis serangan yang terjadi akan memicu firewall secara otomatis untuk melakukan respon balik (*blocking ip-address*) dengan cara memasukkan *rules* baru ke dalam iptables. Adapun hasil akhir yang ingin dicapai dalam pembuatan tugas akhir ini adalah dapat dibuatnya suatu sistem firewall dengan kecerdasan buatan yang berdaya beli murah serta memiliki kemampuan pendeteksian serangan yang lebih akurat dan kemampuan melakukan respon balik secara otomatis untuk penanganan serangan yang lebih efektif.

1.6. Sistematika Penulisan

Laporan penelitian tugas akhir ini tersusun atas beberapa bab dengan urutan sebagai berikut :

STIKOMP SURABAYA

BAB I : Pendahuluan

Pada bab ini diuraikan mengenai latar belakang dari topik tugas akhir yang diambil, kemudian dirumuskan menjadi suatu permasalahan yang akan diselesaikan dalam tugas akhir ini, batasan-batasan masalah yang akan diteliti, tujuan dari penelitian tugas akhir ini serta kontribusi yang dapat diberikan dari hasil penelitian ini terhadap perkembangan ilmu pengetahuan khususnya sistem keamanan jaringan komputer.

BAB II : Landasan Teori

Bagian landasan teori ini menguraikan tentang teori-teori yang terkait dengan variabel-variabel penelitian termasuk uraian tentang pemilihan suatu teori yang diterapkan dalam menyelesaikan masalah. Teori yang akan diuraikan adalah tentang Firewall, Intrusion Detection System, Fuzzy Logic, dan Neural Network.

BAB III : Metode Penelitian

Dalam bab ini diuraikan tentang metode penelitian yang digunakan dalam penelitian ini serta alasan penggunaan metode tersebut dalam penelitian. Pada metode penelitian ini dimuat perancangan perangkat lunak serta perealisasian sistem firewall sesuai dengan rancangan.

STIKOM SURABAYA

BAB IV : Pengujian dan Evaluasi Sistem

Dalam bagian pengujian dan evaluasi sistem ini diuraikan tentang prosedur dan hasil-hasil pengujian serta analisa hasil percobaan atau penelitian. Pada bagian ini dimuat tentang prosedur penelitian, hasil pengujian serta analisa hasil pengujian sistem firewall.

BAB V : Penutup

Bagian ini merupakan bagian akhir dari laporan penelitian tugas akhir ini yang menguraikan kesimpulan-kesimpulan yang diperoleh dari proses penelitian serta saran-saran untuk pengembangan penelitian selanjutnya.

STIKOMP SURABAYA