

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Pesatnya perkembangan teknologi jaringan juga disertai munculnya berbagai permasalahan keamanan. Contoh dari permasalahan keamanan ini adalah adanya berbagai metode serangan jaringan komputer diantaranya *Denial of Service Attack*, *User to Root Attacks*, *Remote to Locate Attacks*, *Scanning Port*. Untuk mengidentifikasi jenis serangan ini dapat menerapkan *Intrusion Detection System (IDS)* kedalam sebuah sistem jaringan.

IDS merupakan suatu tindakan untuk mendeteksi adanya trafik paket yang tidak diinginkan dalam sebuah jaringan atau *device* (Wu,2009). Dalam perkembangannya aplikasi IDS dapat dibangun dengan menggunakan beberapa metode yaitu *Enhanced Evolving Clustering Method*, *Adaptive Neuro-Fuzzy Inference System*, *PCA Neural Network* dan *Fuzzy Logic*. Setiap metode ini tentunya mempunyai beberapa kelebihan dan kelemahan.

Dari beberapa metode IDS diatas menurut Cox (1994) logika fuzzy merupakan metode yang mudah dimengerti karena logika fuzzy menggunakan dasar teori himpunan, sehingga konsep matematis yang mendasari penalaran fuzzy tersebut cukup mudah untuk dimengerti. Saat ini logika fuzzy telah diaplikasikan dalam berbagai bidang ilmu seperti pengendalian, jaringan dan industri. Dalam bidang jaringan logika fuzzy dapat diterapkan dalam membangun sistem IDS.

Untuk menerapkan metode fuzzy kedalam sistem IDS diperlukan data-data serangan guna menyusun variabel-variabel fuzzy. Untuk mengumpulkan data serangan tersebut dapat dilakukan melalui proses *sniffing*. Setelah data terkumpul selanjutnya dianalisa untuk membuat variabel-variabel fuzzy yang dibutuhkan beserta aturan-aturan fuzzy.

Karena memiliki konsep yang sederhana metode fuzzy dipilih sebagai pengambil keputusan sistem IDS. Dalam Tugas Akhir ini dapat dilihat seberapa akuratkah penerapan metode fuzzy, karena selain membahas tentang bagaimana membangun sistem IDS dengan metode fuzzy tugas akhir ini juga membahas hasil pendeteksian serangan sehingga dapat dilihat bagaimana hasil klasifikasi serangan melalui metode fuzzy.

1.2 Perumusan Masalah

Dari latar belakang masalah didapatkan rumusan masalah seperti yang ditulis dibawah ini.

1. Bagaimana mengidentifikasi dan mengklasifikasikan paket serangan dan paket normal
2. Bagaimana menerapkan logika fuzzy untuk mengidentifikasikan adanya serangan
3. Bagaimana membuat antarmuka yang mudah dimengerti oleh *user*.

1.3 Pembatasan Masalah

Adapun beberapa batasan masalah pada tugas akhir rancang bangun IDS dengan menggunakan metode fuzzy adalah sebagai berikut.

1. Sistem Operasi yang digunakan adalah Linux
2. Jenis serangan yang dideteksi adalah *Denial of Service Attack*
3. Hasil analisa paket ditampilkan dalam sistem log berbasis web
4. *Attack tools* yang digunakan adalah Longcat
5. Pengujian dilakukan oleh dua komputer dengan klasifikasi: komputer A (bisa disebut dengan komputer router) sebagai target serangan dan komputer B sebagai penyerang
6. Pengujian dilakukan dalam jaringan intranet.

1.4 Tujuan

Tujuan dalam membuat penelitian tugas akhir ini adalah sebagai berikut.

1. Dapat mengidentifikasi dan mengklasifikasikan paket serangan dan paket normal
2. Dapat menerapkan logika fuzzy untuk mengidentifikasi adanya serangan
3. Dapat membuat antarmuka yang mudah dimengerti oleh user

1.5. Sistematika Penulisan

Sistematika penulisan buku tugas akhir ini terdiri dari lima bab, dimana dalam tiap bab terdapat beberapa sub-bab. Ringkasan uraian dari tiap bab tersebut adalah sebagai berikut.

Bab I Pendahuluan

Pada bab ini menjelaskan tentang latar belakang, perumusan masalah, pembatasan masalah, tujuan, dan sistematika penulisan buku tugas akhir.

Bab II Landasan Teori

Bab ini menjelaskan tentang beberapa teori pendukung tugas akhir seperti mekanisme pengiriman data dalam jaringan atau lebih dikenal dengan nama *Open System Interconnection (OSI)*. Juga dijelaskan teori tentang *Intrusion Detection System*, konsep logika fuzzy mulai dari pengertian sampai tahap-tahap akhir pengambil keputusan serta teori *Denial of Service Attack (DoS)*.

Bab III Metode Penelitian

Bab ini menjelaskan tahap-tahap pembangunan sistem IDS dimulai dari konsep, algoritma pemrograman hingga penulisan kode-kode program.

Bab IV Pengujian Sistem

Bab ini menjelaskan pengujian yang dilakukan dengan cara melakukan serangan kedalam sebuah komputer yang telah dipasang aplikasi IDS yang telah dibuat oleh penulis. Dari hasil pengujian tersebut selanjutnya akan dijelaskan hasil analisis terhadap sistem IDS.

Bab V Penutup

Bab ini menjelaskan tentang kesimpulan dari tugas akhir yang telah dikerjakan dan saran-saran untuk pengembangan lebih lanjut.

