APLIKASI WEB UNTUK METODE FUZZY NEUARAL NETWORK PADA INTRUSION DETECTION SYSTEM BERBASIS SNORT

Feriana Istining Tiyas[1], Moch Zen Samsono Hadi[2], Entin Martiana K.[3]
Jurusan Telekomunikasi, Piliteknik Elektronika Negeri Surabaya
Institut Teknologi Sepuluh Nopember (ITS) Surabaya
Kampus PENS-ITS, Keputih, Sukolilo, Surabaya.
feri@student.eepis-its.edu

Abstrak

Mencocokan pola atau signature adalah metode yang paling umum untuk mendeteksi serangan dan ini berarti IDS harus mampu mengenali setiap teknik serangan. IDS memiliki database yang besar dengan ribuan signature yang memungkinkan IDS mencocokan signature atau pola serangan. Respon otomatis yang biasanya dilakukan adalah memberikan alert, logging, atau mengirim email. Kelemahan respon otomatis yang umum adalah terjadinya respon terhadap false negative dan false positive. Adalah penting untuk memahami mengapa signature memicu dan mengidentifikasi true dari false positive.

Pengunaan algoritma fuzzy neural network dilandasi oleh pemikiran perlu adanya solusi terhadap nilai anggota bilangan atau membership value (MV) yang tidak hanya berorientasi pada benar atau salah, terpenuhi (MV=1), atau tidak terpenuhi (MV=0). Algoritma fuzzy neural network ini nantinya akan diletakkan pada metode pembacaan signature atau pola tertentu dari suatu paket serangan yang umum. Sehingga Algoritma Fuzzy Neural Network menjadi kecerdasan buatan yang digunakan sebagai Pattern Recognition pada SNORT IDS.Hasil dari pengujian data real-time di jaringan dan data serangan akan didefinisikan melalui aplikasi web.

Hasil dari pembuatan tugas akhir ini dengan mengggunakan algoritma Fuzzy Neural Network dapat mendeteksi setiap jenis serangan scanning, DoS, dan IP Spoofing. Dengan algoritma Fuzzy Neural Network telah mampu mengklasifikasikan setiap serangan, dengan menggunakan serangan land_attack diperoleh 100% alert dapat di clasifikasikan. Dan dengan metode Fuzzy Neural Network dapat mengklasifikasikan alert pada serangan DoS yang tidak dapat di klasifikasi pada metode Fuzzy.

Kata kunci: IDS, Fuzzy Neural Network, SNORT

1. PENDAHULUAN

Ketergantungan suatu sistem terhadap sekuritas tidak perlu diperdebatkan lagi. Perkembangan komputer yang pesat semakin hari menuntut kompleksitas yang semakin tinggi, namun dengan penggunaan yang mudah oleh pengguna. Para developer sistem berlomba-lomba membuat produk yang mudah untuk digunakan namun keamanan sering dianak tirikan. Atas nama waktu dan target, developer sering kali hanya melakukan pengetesan terhadap fungsi suatu sistem atau program dan masalah keamanan kurang mendapat perhatian.

Keadaan diatas adalah salah satu pemicu ancaman terhadap keamanan komputer yang semakin hari semakin berbahaya dan jumlah serangan yang dilakukan hacker semakin meningkat dari waktu ke waktu. Salah satu upaya melindungi jaringan dari ancaman-ancaman diatas adalah membangun Sistem Deteksi Intrusi atau Intrusion Detection System (IDS) pada jaringan tersebut. Secara berkala vendor IDS akan merilis signature untuk serangan-serangan baru dan menjadi tugas Network Administrator untuk men-deploy signature tadi kedalam IDS yang ada pada jaringan nya. Masalah muncul ketika serangan-serangan baru muncul dalam interval waktu yang relatif cepat, network administrator tidak bisa sepenuhnya berharap kepada vendor IDS untuk membuat signature yang baru dalam kurun waktu yang singkat,

sehingga seorang network administrator harus membuat signature sendiri dan tetap update terhadap jenis-jenis serangan baru yang muncul. Mengingat beban pekerjaan network administrator yang besar dan luas, sangat tidak mungkin seorang network administrator untuk selalu update tiap waktu terhadap serangan-serangan baru dan dengan singkat membuat signature untuk serangan baru tersebut.

Maka mucullah ide bagaimana membuat suatu sistem deteksi intrusi baru yang dapat mengenali pola serangan baru dari serangan-serangan lama yang sudah ada dan secara otomatis membuat signature untuk serangan tersebut dan menambahkannya kedalam rule yang ada pada IDS tersebut. Sistem ini kemudian dikenal dengan nama Intelligence Intrusion Detection System (IIDS) dimana secara sengaja memasang suatu kecerdasan buatan (Artificial Intelligence) kedalam Intrusion Detection System (IDS). Dengan tujuan adalah membuat Sistem Deteksi Intrusi Baru yang menggabungkan SNORT IDS dengan Algoritma Fuzzy Neural Network yang nantinya dapat mempelajari pola-pola serangan yang sudah ada dan mengidentifikasi jenis-jenis serangan baru.

2. DASAR TEORI

Beberapa materi pustaka yang mendukung perancangan dan pembuatan Aplikasi Mobile Untuk Metode Fuzzy Neural Network Pada Intrusion Detection Sistem Berbasis Snort. Materi – materi tersebut meliputi : Intrusion Detection System dan Fuzzy Neural Network.

2.1 IDS (Intrusion Detection Sistem)

IDS adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas inbound dan outbound dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan).

2.2 Jenis-jenis IDS

Ada dua jenis IDS, yakni:

a. Network-based Intrusion Detection System (NIDS)
b. Host-based Intrusion Detection System (HIDS)

   Kebanyakan produk IDS merupakan sistem yang bersifat pasif, mengingat tugasnya hanyalah mendeteksi intrusi yang terjadi dan memberikan peringatan kepada administrator jaringan bahwa mungkin ada serangan atau gangguan terhadap jaringan. Akhir-akhir ini, beberapa vendor juga mengembangkan IDS yang bersifat aktif yang dapat melakukan beberapa tugas untuk melindungi host atau jaringan dari serangan ketika terdeteksi, seperti halnya menutup beberapa port atau memblokir beberapa alamat IP. Produk seperti ini umumnya disebut sebagai Intrusion Prevention System (IPS). Beberapa produk IDS juga menggabungkan kemampuan yang dimiliki oleh HIDS dan NIDS, yang kemudian disebut sebagai sistem hibrid (hybrid intrusion detection system).

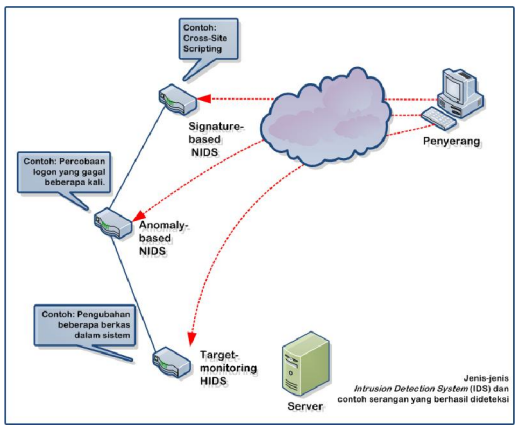
2.3 Implementasi dan Cara Kerja

Ada beberapa cara bagaimana IDS bekerja. Cara yang paling populer adalah dengan menggunakan pendeteksian berbasis signature (seperti halnya yang dilakukan oleh beberapa antivirus), yang melibatkan pencocokan lalu lintas jaringan dengan basis data yang berisi cara-cara serangan dan penyusupan yang sering dilakukan oleh penyerang. Sama seperti halnya antivirus, jenis ini membutuhkan pembaruan terhadap basis data signature IDS yang bersangkutan.

Metode selanjutnya adalah dengan mendeteksi adanya anomali, yang disebut sebagai Anomaly-based IDS. Jenis ini melibatkan pola lalu lintas yang mungkin merupakan sebuah serangan yang sedang dilakukan oleh penyerang. Umumnya, dilakukan dengan menggunakan teknik statistik untuk membandingkan lalu lintas

yang sedang dipantau dengan lalu lintas normal yang biasa terjadi. Metode ini menawarkan kelebihan dibandingkan signature-based IDS, yakni ia dapat mendeteksi bentuk serangan yang baru dan belum terdapat di dalam basis data signature IDS. Kelemahannya, adalah jenis ini sering mengeluarkan pesan false positive. Sehingga tugas administrator menjadi lebih rumit, dengan harus memilah-milah mana yang merupakan serangan yang sebenarnya dari banyaknya laporan false positive yang muncul.

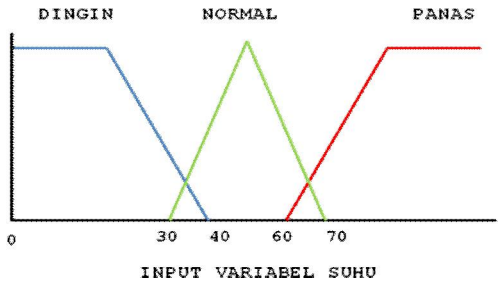
Teknik lainnya yang digunakan adalah dengan memantau berkas-berkas sistem operasi, yakni dengan cara melihat apakah ada percobaan untuk mengubah beberapa berkas sistem operasi, utamanya berkas log. Teknik ini seringnya diimplementasikan di dalam HIDS, selain tentunya melakukan pemindaian terhadap log sistem untuk memantau apakah terjadi kejadian yang tidak biasa.



Gambar 1 Jenis-jenis IDS dan contoh serangan yang berhasil dideteksi

2.4 Logika Fuzzy

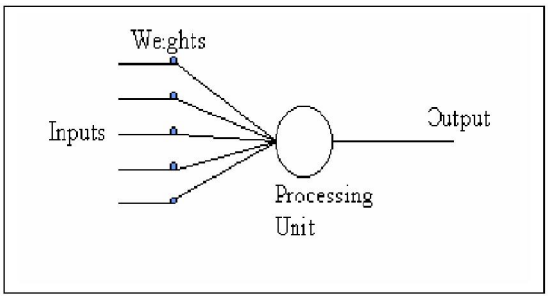
Logika Fuzzy adalah teknik penalaran ketidakpastian. Dalam ilmu komputer Logika Fuzzy digunakan untuk menangani masalah ketidakpastian. Didalam teori fuzzy, kebenaran tidak lagi bersifat absolute 0 atau 1. Namun kebenaran dinyatakan dalam bentuk himpunan nilai dari fungsi keanggotaan (membership function) dengan nilai berada pada interval 0 dan 1, tingkat keabuan dan juga hitam dan putih, dan dalam bentuk linguistik, konsep tidak pasti seperti "sedikit", "lumayan", dan "sangat". Logika Fuzzy berhubungan dengan set fuzzy dan teori kemungkinan. Logika Fuzzy diperkenalkan oleh Dr. Lotfi Zadeh dari Universitas California, Berkeley pada 1965.



Gambar 2 Perbedaan temperatur dalam logika Fuzzy

2.5 Neural Network (Jaringan Syaraf Tiruan)

Jaringan syaraf adalah merupakan salah satu representasi buatan dari otak manusia yang selalu mencoba untuk menstimulasikan proses pembelajaran pada otak manusia tersebut. Istilah buatan disini digunakan karena jaringan syaraf ini diimplementasikan dengan menggunakan program computer yang mampu menyelesaikan sejumlah proses pehitungan selama proses pembelajaran. Contoh syaraf secara biologis ditunjukkan pada gambar 2 dibawah ini :



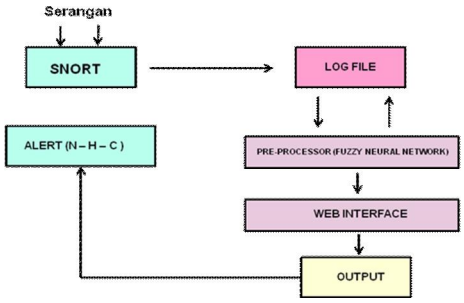
Gambar 3 Bentuk dasar neuron

3. RANCANGAN SISTEM

Dalam sistem yang dibuat ini diperlkan komputer/PC sebagai media dalam pembuatan jaringan lokal yang telah

terinstalasi dan konfigurasi Web Server, database Server dan SNORT IDS pada Debian/GNU Linux 5.0 (lenny).

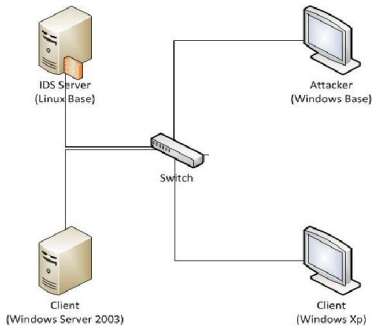
Diagram Sistem untuk penelitian yang dibuat ini dapat dilihat pada gambar 3:



Gambar 4 Diagram alur dari Fuzzy Neural Network Intrusion Recognition Engine

Fuzzy Neural Network Intrusion Recognition Engine memiliki 3 bagian utama yaitu Real Time Engine, Fuzzy Neural Network Engine dan Main Control dimana ketiga bagian ini akan terintegrasi secara langsung dan real time dengan SNORT IDS.

Topologi Jaringan yang digunakan ditunjukkan seperti gambar 4 :



Gambar 5 Desain Topologi Jaringan

Desain topologi jaringan yang dibangun terdiri dari sebuah server IDS yang akan terhubung dengan external network, sebuah server sebagai engine dan client. Koneksi yang digunakan adalah dengan menggunakan LAN yang terhubung dengan router.

4. PEMBUATAN SISTEM DAN ANALISA

4.1 Instalasi dan Konfigurasi Server

a. Instalasi Web Server
b. Instalsi Database Server

4.2 Instalasi SORT IDS

a. Instalasi Library pcap dan pcre
b. Instalasi dan Konfigurasi Snort IDS
c. Konvigurasi SNORT Database
d. Menambahkan SNORT Database Schema

4.3 Instalasi Base

a. Install acidbase 1.2 7
b. Copy library acidbase ke Web Root
c. Konfigurasi /var/www/acidbase/base_conf.php
d. Konfigurasi etc/acidbase/database.php

4.4 Hasil Yang Dikerjakan

Dari hasil percobaan tersebut diperoleh data perbedaan antara sistem fuzzy dan fuzzy neural network pada tiap serangan. Pada serangan –sT dan –sS kedua sistem sama-sama belum dapat mendeteksi adanya allert, karena pada serangan tersebut paket yang dikirim dengan protokol RAW IP. Pada sistem FNN lebih banyak mendeteksi alert dengan memberikan label Normal dan High Rish.

Pada percobaan dengan scanning diperoleh data beda yang sangat tinggi mencapai 66,67% dikarenakan data yang di hasilkan dalam scanning hanya 3 data. Pada sisstem Fuzzy terdeteksi 1 data high risk dan 2 data critical. Sedangkan pada sistem Fuzzy Neural Network terdeteksi sebagai 3 data adalah high risk.

a. Hasil Perbandingan FNN dan Snort

Perbandingan antara sistem dengan metode Fuzzy Neural Network dan Snort dapat dilihat pada tabel 1.

Tabel 1 Perbandingan FNN dan Snort

SERANGAN	FNN (%)			SNORT (%)		jumlah data
	normal	serangan	tidak terdeteksi	normal	serangan	
SCANNING						
-sF (FIN scan)	77,31	22,53	0,15	0,00	100,00	648
-sX(Xmas scan)	1,71	98,00	0,29	1,71	98,29	350
-sN(Null scan)	0,00	75,00	25,00	0,00	100,00	4
-sU(UDP scan)	27,42	25,81	46,77	72,58	27,42	62
-O (OS scan)	28,57	14,29	57,14	21,43	78,57	14
Jumlah	27	47,126	25,87	19,14	80,856	1078
DoS						
POD	12,96	87,04	0,00	12,96	87,04	54
normal						
telnet	100	0,00	0,00	100,00	0,00	6
http	85,71	14,29	0,00	85,71	14,29	14
IP SPOOFING						
syn_flad	2,19	94,33	3,47	2,19	97,81	547
land_attack	0,00	100,00	0,00	0,58	99,42	2060

Pada tabel 1 menjelaskan bahwa, dengan menggunakan scanning alert yang dapat dideteksi oleh FNN sebanyak 47,126% berupa serangan dan 27% bukan serangan. Pada serangan POD, normal, dan IP Spoofing FNN dan Snort mendeteksi serangan dengan jumlah data yang sama, begitu pula dengan menggunakan land_attack packet yang terdeteksi sebagai serangan sebanyak 100%.

b. Hasil Perbandingan FNN dan Fuzzy

Pada uji coba ini, akan dibedakan antara sistem fuzzy dan fuzzy neural network.

Tabel 2 Perbandingan FNN dan Fuzzy

SERANGAN	FNN (%)			FUZZY (%)			
	N	H	C	N	H	C	unclass
SCANNING							
-sF (FIN scan)	78,36	21,6	0	79,91	20,09	0	0
-sX(Xmas scan)	15,18	84,81	0	1,72	91,12	7,16	0
-sN(Null scan)	33,33	66,66	0	33,33	66,67	0	0
-sU(UDP scan)	51,51	48,48	0	100	0	0	0
-O (OS scan)	66,66	33,33	0	50	50	0	0
jumlah	49,02	50,98	0	52,99	45,58	1,42	0
DoS							
POD	12,9	87,03	0	14,81	0	0	89,19
normal							
telnet	100	0	0	100	0	0	0
http	85,71	14,29	0	85,71	0	14,29	0
IP SPOOFING							
syn_flad	2,27	97,73	0	2,27	49,62	48,11	0
land_attack	0,58	99,42	0	0,58	99,42	0	0

Keterangan :
N = normal
H = high
C = critical

Dari hasil percobaan tersebut diperoleh data perbedaan antara sistem fuzzy dan fuzzy neural network pada tiap serangan. Pada serangan –sT dan –sS kedua sistem sama-sama belum dapat mendeteksi adanya allert, karena pada serangan tersebut paket yang dikirim dengan protokol RAW IP. Pada sistem FNN lebih banyak mendeteksi alert dengan memberikan label Normal dan High Rish.

5. KESIMPULAN

Engine yang dibuat sudah bisa mendeteksi serangan berupa berbagai tipe scanning dengan parameter pada paket yaitu protokol, destination port, flag dan size.

Pada sistem ini baik untuk mendeteksi dengan menggunakan serangan land_attack diperoleh 100% alert dapat di klasifikasikan, dan dengan menggunakan serangan syn_flad sebanyak 96,53% serangan dapat diklasifikasikan seperti yang terlihat pada tabel 2.

6. DAFTAR PUSTAKA

[1] Wijanarko Bambang, “Algoritma Fuzzy Sebagai Metode Pendeteksi Pola Serangan Pada Jaringan Berbasis Snort IDS”, Proyek Akhir, PENS-ITS, 2009.

[2] Moch Zen Samsono Hadi, S.T., M.Sc., Intrusion Detection System [SNORT], Modul Praktikum 7, _ , _ .

[3] Sri Kusumadewi dan Sri Hartati, “Neuro-Fuzzy Integrasi Sistem Fuzzy dan Jaringan Syaraf”, Edisi Pertama, Graha Ilmu, Yogyakarta, 2006.

[4] Entin Martiana Kusumaningtyas, S.Kom., M.Kom., Kecerdasan Buatan Pertemuan 11, Modul Ajar, PENS-ITS,2010.

[5] Endah Sri Utami, “Pembacaan Plat Nomor Kendaraan Menggunakan Metode Jaringan Saraf Tiruan (JTS) Backpropagation Berbasis Image Processing”, Proyek Akhir, PENS-ITS, 2009.

[6] Ardyono Pribadi, Ahmad Muslich, dan Mauridhi Hery Purnomo, “Pengendalian Osilasi Inter-Area Sistem Tenaga Listrik Menggunakan Logika Fuzzy”, Jurnal EEPIS Volume 7 – Number 1, July 2002.