APLIKASI HIERARCHICAL CLUSTERING PADA INTRUSION DETECTION SYSTEM BERBASIS SNORT

Ellysabeth Januar Christine, Moch. Zen Samsono Hadi, Entin Martiana Kusumaningtyas
Jurusan Teknik Telekomunikasi, Politeknik Elektronika Negeri Surabaya
Institut Teknologi Sepuluh Nopember (ITS) Surabaya
Kampus PENS-ITS, Keputih, Sukolilo, Surabaya.
Telp : +62+031+5947280; Fax. +62+031+5946011
Email : ellysabeth@student.eepis-its.edu

Abstrak - Salah satu upaya melindungi jaringan dari ancaman-ancaman hacker, cracker dan security expert adalah dengan membangun Sistem Deteksi Intrusi atau Intrusion Detection System (IDS) pada jaringan tersebut. Masalah muncul ketika serangan-serangan baru muncul dalam waktu yang relatif cepat,sehingga seorang network administrator harus membuat signature sendiri dan tetap update terhadap jenis-jenis serangan baru yang muncul.

Inilah yang melatarbelakangi Penelitian Proyek Akhir ini. Pada Penelitian Proyek Akhir ini, akan dibuat suatu Intelligence Intrusion Detection System (IIDS) dimana Algoritma Hierarchical Clustering menjadi kecerdasan buatan yang digunakan sebagai Pattern Recognition dan diimplementasikan pada SNORT IDS. Hiearchical clustering diterapkan pada data training untuk menentukan banyaknya kluster yang diinginkan. Selanjutnya dilakukan pelabelan kluster, ada 3 label kluster, yaitu Normal, High Risk dan Critical. Metode Centroid Linkage digunakan untuk pengujian data serangan baru. Output system digunakan untuk meng-update database rule SNORT.

Tugas Akhir ini diharapkan akan membantu Administrator Jaringan untuk memonitor dan mempelajari beberapa jenis serangan baru dari serangan jenis Port Scanning, Vulnerability Scanning, Exploit, Buffer Over Flow, Exploit dan IP Spoofing yang belum ada pada rule sistem IDS yang digunakan, dalam hal ini IDS berbasis SNORT, yang selanjutnya dapat dilakukan antisipasi agar serangan-serangan tadi tidak menimbulkan hal-hal yang tidak diinginkan pada Network mereka.

Kata kunci : IDS, IIDS, SNORT, Hierarchical Clustering.

1. PENDAHULUAN

Tidak ada komputer yang aman seratus persen didunia ini kecuali anda menguburnya 100 meter dibawah tanah dan mematikannya. Oracle yang mengklaim “tidak bisa ditembus” hanya dalam beberapa waktu saja telah diacak-acak oleh hacker. KPU yang mengklaim bahwa sistem dengan biaya lebih dari 150 milyar mereka aman, pada akhirnya harus bertekuk lutut di depan hacker.

Salah satu upaya melindungi jaringan dari ancaman-ancaman hacker, cracker dan security expert adalah dengan 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 muculah 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).

Inilah yang melatarbelakangi Penelitian Proyek Akhir ini. Pada Penelitian Proyek Akhir ini, akan dibuat suatu Intelligence Intrusion Detection System (IIDS) dimana Algoritma Hierarchical Clustering menjadi kecerdasan buatan yang digunakan sebagai Pattern Recognition dan di implementasikan pada SNORT IDS.

2. DASAR TEORI

2.1. SNORT IDS

Snort merupakan salah satu contoh program NIDS yaitu program yang dapat mendeteksi penyusupan pada suatu jaringan komputer. Snort bersifat open source sehingga software ini bebas dipergunakan untuk mengamankan sistem server tanpa harus mempunyai lisence.

Tipe dasar IDS adalah:

- Rule-based system : brdasarkan atas database dari tanda penyusupan atau serangan yang telah dikenal. Jika IDS mencatat lalulintas yang sesuai dengan database yang ada, maka langsung dikategorikan sebagai penyusupan.
- Adaptive system : mempergunakan metode yang lebih canggih. Tidak hanya berdasarkan database yang ada. Tapi juga membuka kemungkinan untuk mendeteksi terhadap bentuk penyusupan yang baru.

Bentuk yang sering dipergunakan untuk komputer secara umum adalah rule-based system. Pendekatan yang dipergunakan dalam rule based system ada dua, yakni pendekatan pencegahan (preemtory) dan pendekatan reaksi (reactionary). Perbedaannya hanya masalah waktu saja. Pendekatan pemcegahan, program pendeteksi penyusupan akan memperhatikan semua lalu lintas jaringan. Jika ditemukan paket yang mencurigakan, maka program akan melakukan tindakan yang perlu. Pendekatan reaksi, program pendeteksi penyusupan hanya mengamati file log. Jika ditemukan paket yang mencurigakan, program juga akan melakukan tindakan yang perlu.

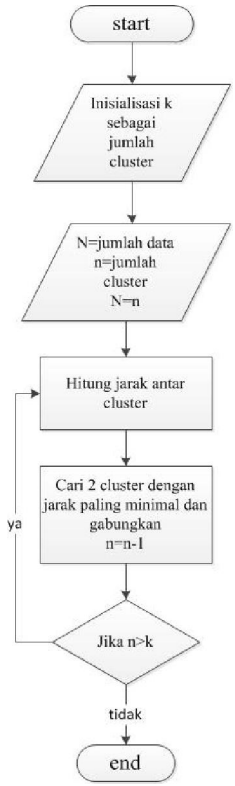
Snort dapat dioperasikan dalam 3 mode yaitu :

1. Sniffer mode, untuk melihat paket yang lewat di jaringan.
2. logger mode, untuk mencatat semua paket yang lewat di jaringan untuk di analisa di kemudian hari.
3. Intrusion Detection Mode, pada mode ini snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer. Untuk menggunakan mode IDS ini diperlukan setup dari berbagai file atau aturan yang akan membedakan sebuah paket normal dengan paket yang membawa serangan.

Snort mode logger pada umumnya menggunakan file untuk menulis log nya, namun snort juga menyediakan log ke dalam database mysql, freebsd maupun oracle. Dengan dukungan database maka akan memudahkan dalam proses pembacaan data log oleh program karena database sudah sangat dikenal dan dipahami. Untuk melakukan logging ke database maka dibutuhkan setting tambahan supaya snort akan otomatis logging ke dalam database.

2.2. Hierarchical Clustering

Hiearchical clustering merupakan metode analisa cluster yang bertujuan membangun hirarki cluster. Pada hierarchical clustering, setiap data harus termasuk cluster tertentu, dan suatu data pada suatu tahapan proses, tidak dapat berpindah ke cluster lain pada tahapan berikutnya. Algoritma Hierarchical clustering dapat dilakukan dengan langkah berikut :



Gambar 1. Flowchart Hierarchical Clustering

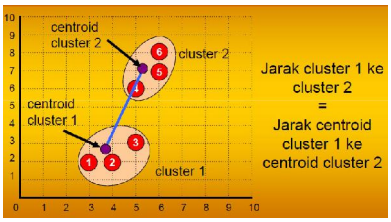
1. Tentukan k sebagai jumlah cluster yang ingin dibentuk.
2. Setiap data dianggap sebagai cluster. Jika N=jumlah data dan n=jumlah cluster, berarti ada n=N.
3. Hitung jarak antar cluster.
4. Cari 2 cluster yang mempunyai jarak antar cluster yang paling minimal dan gabungkan (berarti n=n-1).
5. Jika n>k, kembali ke langkah 3.

2.3. Metode penghitungan jarak menggunakan Centroid Linkage

Input algoritma centroid linkage berupa jarak antara cluster. Kelompok-kelompok dibentuk dari entities cluster dengan menggabungkan jarak titik tengah antar cluster. Untuk menghitung jarak antar cluster dengan menghitung titik tengah masing-masing cluster, yaitu berupa nilai rata-rata data masing-masing cluster. Jarak antar cluster dihitung dengan cara penghitungan jarak (Euclidian distance) antar titik tengah masing-masing cluster.

Metode centroid linkage ini digunakan dalam proyek akhir sebagai metode untuk pengujian data baru. Data training yang telah dibentuk dalam beberapa kluster yang telah ditentukan dicari titik centroid nya dengan mencari nilai rata-rata, dalam hal ini nilai rata-rata masing-masing parameter yang digunakan dalam proyek akhir. Data baru dihitung jaraknya dengan masing-masing titik centroid menggunakan Euclidian.

Metode centroid linkage digunakan karena paling baik dan mudah untuk kasus seperti pada proyek akhir ini.



Gambar 2. Centroid Linkage

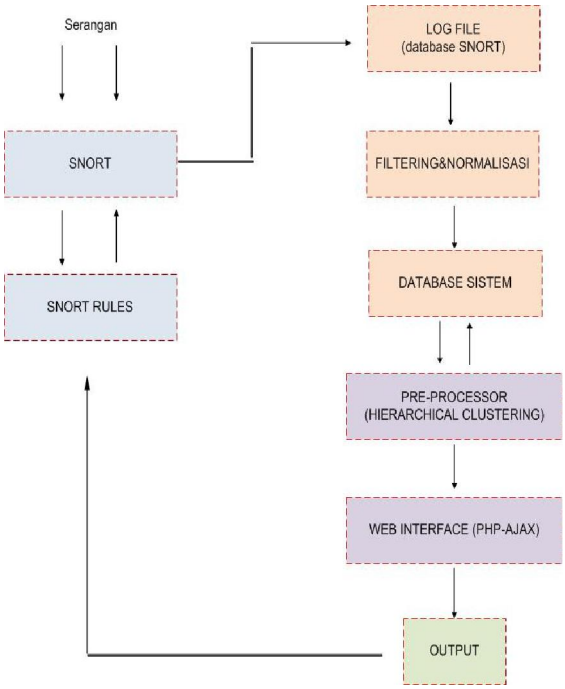
2.4. BASE (Base Analysis And Security Engine)

BASE dapat mencari dan memproses database yang berisi security events yang telah dicatat oleh berbagai macam alat monitor jaringan seperti firewall dan program IDS. BASE ditulis dalam bahasa pemrograman PHP dan menampilkan informasi dari database user interface. Ketika digunakan dengan Snort, BASE membaca kedua macam yaitu format log tcpdump dan format biner serta alert SNORT. Setelah data masuk dan diproses, BASE memiliki kemampuan untuk menampilkan grafis informasi paket. Query pencariaannya BASE dapat berdasarkan informasi alert seperti sensor, log alert, signature, klasifikasi, dan waktu deteksi, serta data paket seperti sumber / alamat tujuan, port, muatan paket, atau flag paket. Dukungan untuk login user, memungkinkan administrator untuk mengontrol apa yang dilihat melalui web interface, juga diharapkan dalam update BASE. BASE juga mendukung database lain dan dapat menampilkan informasi melalui semua web server yang mendukung PHP.

3. DESAIN SISTEM

Data yang berhasil di capture oleh SNORT akan disimpan pada log file SNORT, selanjutnya difiltering parameter apa saja yang akan dipilih dan dimasukkan ke dalam database dan nantinya di analisa dan di clustering pada pre-processor dengan hierarchical clustering, lalu hasil di tampilkan pada user interface yang menggunakan PHP

dan Ajax yang secara realtime berbasis web, output dari web interface akan selalu meng-update rules SNORT jika ada serangan baru dan nantinya akan dilakukan action dengan memblokir nomer IP yang digunakan untuk melakukan serangan.



Gambar 3. Desain Sistem

4. PENGUJIAN DAN ANALISA

Pada bab ini akan dibahas mengenai uji coba dan analisa Hierarchical Intrusion Detection Engine (HIDE) dari aktifitas Hacking yang digolongkan sebagai Active Attack dan Normal Attack sebagai berikut :

1. Port Scanning
2. Nessus Vulnerable Scanning
3. Exploit
4. Buffer Over Flow
5. Ping of Death (DoS)
6. Land Attack dan SYN Flooding (IP Spoofing)
7. Akses normal (HTTP, FTP, Telnet, SSH)

Hasil pengujian sistem HIDE dengan data training 257 dibandingkan dengan hasil dari penelitian sebelumnya FIRE (Fuzzy Intrusion Recognition Engine) yang menggunakan algoritma Fuzzy dengan 30 Fuzzy rule, alert SNORT dan metode lainnya yaitu K-Nearest Neighbor dan Fuzzy Neural Network dimasukkan ke dalam tabel berikut :

Tabel 4.1. HIDE vs FIRE

	Serangan	HIDE (%)			FIRE(%)		
		N	H	C	N	H	C
Scanning	TCP Connect Scan	25	0	75	0	25	75
	Windows Scan	33	0	67	0	33	67
	FIN Scan	100	0	0	87	13	0
	XMAS Scan	0	0	100	0	95	5
	NULL Scan	100	0	0	80	20	0
	Rata- rata	51,6	0	48,4	33,4	37,2	29,4
Serangan Lain	Nessus	22	0	78	24	1	75
	Exploit	86	0	14	86	0	14
	Buffer Over Flow	60	0	40	60	1	40
	Ping of Death	100	0	0	100	0	0
	Land Attack	99	1	0	99	0	1
	SYN Flooding	0	10	90	0	0	100
	Rata- rata	61,1	1,8	37	61,5	0,3	38,3
Akses Normal	HTTP	100	0	0	100	0	0
	FTP	100	0	0	100	0	0
	Telnet	100	0	0	100	0	0
	SSH	100	0	0	100	0	0
	Rata- rata	100	0	0	100	0	0

Dari tabel diatas, kedua algoritma memiliki hasil tidak jauh berbeda dalam mengenali jenis Network Package. Baik Hierarchical Clustering maupun Fuzzy Algorithm mampu mengenali jenis serangan dalam Network Package. Secara rata-rata perbedaan hasil kinerja kedua sistem sebesar 12 %.

Tabel berikut menjelaskan hasil kinerja sistem HIDE dan hasil dari alert SNORT dalam mengenali jenis serangan dalam Network Package.

Tabel 4.2. HIDE vs Alert SNORT

	Serangan	HIDE(%)			SNORT(%)	
		Normal	H	C	Normal	Serangan
			Serangan			
Scanning	TCP Connect Scan	25	0	75	91	1
	Windows Scan	33	0	67	70	30
	FIN Scan	100	0	0	20	80
	XMAS Scan	0	0	100	20	80
	NULL Scan	100	0	0	40	60
	Rata - rata	51,6	0	48,4	48,2	62,75
Serangan Lain	Nessus	22	0	78	24	76
	Exploit	86	0	14	6	94
	Buffer Over Flow	60	0	40	60	40
	Ping of Death	100	0	0	80	20
	Land Attack	99	1	0	50	50
	SYN Flooding	0	10	90	55	45
	Rata - rata	61,1	1,8	37	45,8	54,1
Akses Normal	HTTP	100	0	0	100	0
	FTP	100	0	0	100	0
	Telnet	100	0	0	100	0
	SSH	100	0	0	100	0
	Rata - rata	100	0	0	100	0

Dari hasil tabel diatas, dapat diketahui untuk beberapa jenis serangan hasil untuk Hierarchical Clustering dan alert SNORT berbeda karena dalam SNORT hanya memberikan informasi mengenai serangan dan bukan serangan, sistem HIDE mengklusterkan jenis serangan menjadi High Risk dan Critical.

Berikut adalah tabel hasil pengujian menggunakan beberapa jenis serangan yang sama dengan metode Hierarchical Clustering, K-Nearest Neighbor dan Fuzzy Neural Network sebagai perbandingan algoritma yang baik diintegrasikan dengan IDS SNORT dalam mengenali jenis Network Package.

Tabel 4.3. Perbandingan Metode (%)

	Serangan	H- Cluster(%)			K-Nearest Neighbor(%)			Fuzzy Neural Network(%)		
		N	H	C	N	H	C	N	H	C
Scanning	FIN Scan	98	2	0	0	19	81	74	26	0
	XMAS Scan	0	4	96	7	79	14	0	100	0
	NULL Scan	100	0	0	34	66	0	34	66	0
	Rata-rata	131,3	2	32	13,6	54,6	31,6	36	64	0
Serangan Lain	Ping of Death	99	1	0	13	87	0	14	86	0
	SYN Flooding	0	13	87	27	26	47	2	98	0
	Rata-rata	49,5	7	43,5	20	56,5	23,5	8	92	0
Akses Normal	HTTP	100	0	0	86	14	0	85	15	0
	Telnet	100	0	0	86	14	0	85	15	0
	Rata-rata	100	0	0	86	14	0	85	15	0

Dari tabel di atas dapat diketahui bahwa ketiga metode sudah mampu mengenali jenis Network Package. Namun dalam penggunaannya sebagi algoritma pendeteksi serangan, K-Nearest Neighbor memberikan hasil yang lebih baik dari ketiga metode karena hanya menghitung jarak terdekat dan menggunakan data training yang sudah berlabel.

5. KESIMPULAN

Dari pengujian sistem Hierarchical clustering (Hierarchical Intrusion Detection Engine) dalam pengenalan jenis Network Package, dapat dibuat kesimpulan sebagai berikut :

1. Sistem Hierarchical clustering sudah mampu membedakan jenis Attack Network Package ke dalam High Risk Network Package dan Critical Network Package.
2. Hasil sistem Hierarchical clustering sangat bergantung pada data training dan pengklusteran data training. Hal ini yang menyebabkan hasil Hierarchical clustering kurang stabil untuk mengenali beberapa jenis Network Package tertentu.
3. Untuk sistem pendeteksi jenis serangan, Hierarchical clustering kurang baik jika dibandingkan dengan algoritma Fuzzy yang digunakan dalam penelitian sebelumnya.
4. Hierarchical clustering cukup baik dalam pengenalan jenis Network Package untuk beberapa jenis serangan tertentu, seperti Exploit, Buffer Over Flow, DoS dan IP

Spoofing. Akurasi kinerja sistem HIDE untuk jenis serangan tersebut diatas adalah sebesar 90 %.

5. Waktu komputasi yang dibutuhkan sistem dalam pengklasteran dan pelabelan data training bergantung banyaknya jumlah data training yang digunakan. Begitu juga untuk pengujian data baru, bergantung dari jumlah data baru yang masuk. Rata – rata waktu komputasi yang dibutuhkan sistem adalah 2-3 detik.

6. DAFTAR PUSTAKA

[1] M. Zen Somsono Hadi, Network Security, Modul Ajar PENS-ITS, Surabaya, 2009.

[2] Ali Ridho Barakbah, "Clustering", Diktat Kuliah PENS-ITS, Surabaya, 2006.

[3] Bambang Wijanarko, "Algoritma Fuzzy Sebagai Metode Mendeteksi Pola Serangan pada Jaringan Berbasis SNORT IDS ", Tugas Akhir PENS-ITS, 2009.

[4] Charlie Scott, Paul Wolfe, Bert Hayes, SNORT for Dummies, Wiley Publishing, Inc, 2006.

[5] Toby Kohlenberg, SNORT IDS and IPS Toolkit, Syngress, September 2007.

[6] Hartono Puji, Sistem Pecegahan Penyusupan pada Jaringan berbasis IDS Snort IDS dan Iptables Firewall, juni 2006.