PENYELEKSIAN NOTIFIKASI SERANGAN PADA JARINGAN KOMPUTER BERBASIS IDS SNORT MENGGUNAKAN METODE K-MEANS

Sultanuddin Prakoso Zuhri[1], Erfan Rohadi[2]

Program Studi Teknik Informatika, Jurusan Teknologi Informasi, Politeknik Negeri Malang
[1]sultanuddinpz@gmail.com, [2]erfanr@gmail.com

Abstrak

Berkembangnya teknologi saat ini diikuti juga dengan berkembangnya serangan untuk merusak teknologi tersebut khususnya didalam jaringan komputer seperti *DOS attack, port scanning, sniffer* dll. Oleh karena itu dibutuhkan sebuah sistem yang bisa mendeteksi serangan secara *realtime*.

Penyeleksian notifikasi serangan pada jaringan komputer berbasis IDS snort menggunakan metode *k-means* adalah sistem yang mendeteksi serangan jaringan berdasarkan data *log* pada snort dengan cara mengelompokkan data *log* tersebut menjadi 2 jenis serangan, bahaya dan tidak bahaya. Kemudian sistem ini akan mengirimkan notifikasi berupa SMS lewat aplikasi SMS *gateway* untuk serangan yang berjenis bahaya ke ponsel *administrator* jaringan. Sistem ini mendeteksi jenis serangan dengan proses pengelompokkan dari 100 data training yang diambil secara acak dari *rules* yang ada di snort.

Proses pengelompokkan jenis serangan ini menggunakan metode *k-means* karena metode ini dapat mengelompokkan data dengan ukuran besar dengan cepat. Tentunya metode ini sangat ditentukan oleh pembangkitan *centroid* awal yang di ambil secara acak.

Kata kunci : *K-Means*, *cluster*, Snort, IDS, SMS Gateway

1. Pendahuluan

Perkembangan teknologi di bidang pendidikan atau pun bisnis dewasa ini mengalami pertumbuhan yang sangat signifikan. Adanya perangkat teknologi yang serba *modern* atau canggih akan tidak ada artinya tanpa diimbangi oleh pengaturan dan penggunaan secara tepat efektif dan efisien. Semakin berkembangnya teknologi pasti juga diikuti dengan berkembangnya serangan untuk merusak teknologi tersebut. Oleh karena itu dibutuhkan strategi dan pengaturan yang tepat untuk mendapatkan kehandalan jaringan dan bisa menjadi apa yang diinginkan oleh perusahaan. Seorang *administrator* jaringan bertanggung jawab penuh atas segala sesuatu ketersediaan dan kerahasiaan informasi. Seorang *administrator* jaringan juga tidak mungkin akan berada di depan layar komputer 24 jam selama seminggu. Maka dari itu dibutuhkannya notifikasi langsung tentang pendeteksi serangan pada jaringan yang sering dikenal *Intrusion Detection System* (IDS) melalui *Short Message Service* (SMS). Serangan pada jaringan sendiri bermacam-macam, ada serangan yang berbahaya dan serangan yang tidak berbahaya. Maka dari itu penulis mencoba membuat sistem pendeteksi serangan (IDS) yang bisa memberi notifikasi hanya untuk serangan yang berbahaya melalui SMS.

2. Tinjauan Pustaka

2.1 Intrusion Detection System (IDS)

Intrusion Detection System (IDS) adalah sebuah sistem yang melakukan pengawasan terhadap *traffic* jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan. Jika ditemukan kegiatan-kegiatan yang mencurigakan berhubungan dengan *traffic* jaringan maka IDS akan memberikan peringatan kepada sistem atau *administrator* jaringan.

2.2 Snort

Salah satu aplikasi Linux yang dapat dipakai untuk meningkatkan keamanan komputer adalah Snort. Secara garis besar, Snort adalah sebuah program yang memiliki tiga fungsi atau tiga modus operasi. Snort dapat dipakai dalam ***packet sniffer mode*** *sehingga bekerja sebagai sniffer sama seperti Wireshark. Sama seperti Wireshark, Snort juga dapat menyimpan setiap packet yang di-capture ke dalam media penyimpan di modus* ***packet logger mode****. Akan tetapi berbeda dengan Wireshark, Snort dapat dipakai sebagai komponen NIDS dengan menjalankannya pada* ***Network Intrusion Detection System (NIDS) mode****. Pada modus yang terakhir ini, Snort akan menganalisa packet berdasarkan rule*

yang ada untuk mengenali adanya upaya serangan hacker.

2.3 *K-Means*

K-means merupakan salah satu metode *clustering* non hirarki yang berusaha mempartisi data yang ada ke dalam bentuk satu atau lebih *cluster*. Metode ini mempartisi data ke dalam *cluster* sehingga data yang memiliki karakteristik yang sama dikelompokkan ke dalam satu *cluster* yang sama dan data yang mempunyai karakteristik yang berbeda dikelompokkan ke dalam *cluster* yang lain. Secara umum algoritma dasar dari K-means *clustering* adalah sebagai berikut:

1. Tentukan jumlah *cluster*.
2. Alokasikan data ke dalam *cluster* secara *random*.
3. Hitung *centroid* / rata-rata dari data yang ada di masing-masing *cluster*.
4. Alokasikan masing-masing data ke *centroid* / rata-rata terdekat.
5. Kembali ke tahap 3, apabila masih ada data yang berpindah *cluster* atau bila ada perubahan nilai *centroid*, jika tidak ada data yang berpindah *cluster* atau ada perubahan nilai *centroid* maka proses *clustering* sudah selesai.

Distance space digunakan untuk menghitung jarak antara data dan *centroid*. Adapun persamaan yang dapat digunakan salah satunya yaitu *Euclidean Distance Space*. *Euclidean distance space* sering digunakan dalam perhitungan jarak, hal ini dikarenakan hasil yang diperoleh merupakan jarak terpendek antara dua titik yang diperhitungkan. Adapun persamaan adalah sebagai berikut:

$$d(x_j, c_j) = \sqrt{\sum_{j=1}^{n} (x_j - c_j)^2}$$

d = jarak
j = banyaknya data
c = centroid
x = data
n = dimensi data

3. Design dan Implementasi

2.1 Analisis

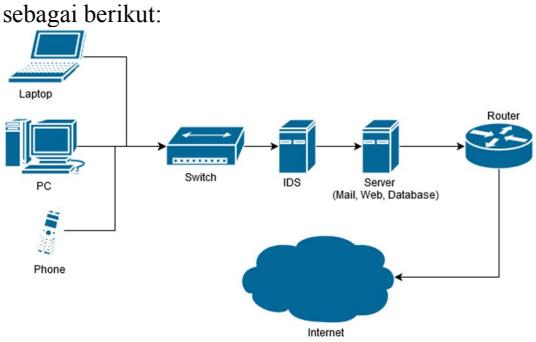
Pada bagian ini akan ditunjukan design model dan struktur implementasi dari solusi yang ditawarkan.

3.1.1 Deskripsi Umum

Sistem ini adalah sistem pendeteksi serangan pada jaringan dengan menggunakan aplikasi snort yang akan mengirimkan serangan melalui notifikasi SMS. Tidak semua notifikasi yang akan dikirimkan, hanya notifikasi yang berjenis bahaya saja yang akan di kirimkan ke ponsel *administrator* jaringan. Penyeleksian jenis serangan ini menggunakan Metode K-Means yang mana akan membagi jenis serangan menjadi 2 macam, bahaya dan tidak bahaya.

3.1.2 Desain Arsitektur Jaringan

Desain arsitektur jaringan dalam sistem ini sebagai berikut:



4. Uji Coba dan Evaluasi.

2.1 Spesifikasi Hardware

Processor Dual Core, Hardisk 500 GB, Memory 2GB, Linux Ubuntu 14.04.

2.2 Spesifikasi Software

Snort, Barnyard2, PHP, Apache2, MySQL, Gammu dan ACID.

2.3 Perancangan Proses

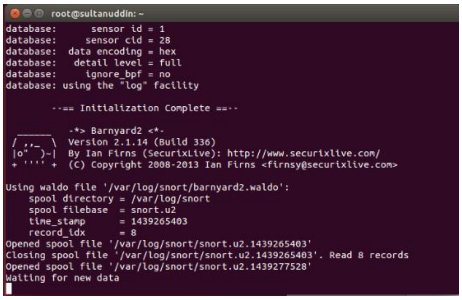
Pada bagian ini adalah proses utama yang ada pada sistem yang dibangun. Pada sistem ini terdapat proses penyeleksian jenis serangan menggunakan algoritma K-means.

4.3.1 *Running* Snort

Perintah untuk menjalankan Snort adalah
/usr/local/snort/bin/snort -i wlan0 –c /usr/local/snort/etc/snort.conf -l /var/log/snort -g snort -u snort Berikut adalah hasil *running* Snort.

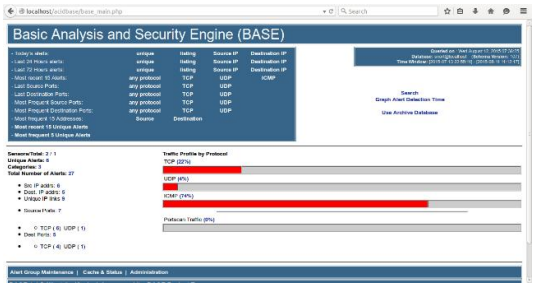
4.3.2 *Running* Barnyard2

Perintah untuk menjalankan Barnyard2 adalah
barnyard2 -c /usr/local/snort/etc/barnyard2.conf -d /var/log/snort -f snort.u2 -w /var/log/snort/barnyard2.waldo -g snort -u snort
Berikut adalah hasil *running* Barnyard2.



4.3.3 ACIDBASE

ACIDBASE adalah *report* dari *log* Snort berbentuk *website.* ACIDBASE memudahkan *administrator* jaringan untuk melihat serangan yang terdeteksi.



4.3.4 Normalisasi Data

Pada proses *clustering* ini hanya menggunakan 2 parameter untuk menentukan jenis serangan yaitu data *protocol* dan *destination port*. Untuk menghitung *cluster* dari data tersebut maka data itu perlu untuk dinormalisasikan terlebih dahulu. Aturan normalisasi sebagai berikut:

Data *protocol*: TCP = 1, UDP = 2, ICMP = 3

Data *destination port*:

0 *range* 65535 = data *real*(Y)

0 *range* 100 = data normalisasi(R)

d = (X – Ymin) * (Rmax – Rmin) / (Ymax – Ymin) + Rmin

dimana: d = data hasil normalisasi

X = data yang akan dinormalisasi

Ymin = nilai minimal data real

Ymax = nilai maksimal data real

Rmin = nilai minimal data normalisasi

Rmax = nilai maksimal data normalisasi

4.3.5 *Clustering* Data

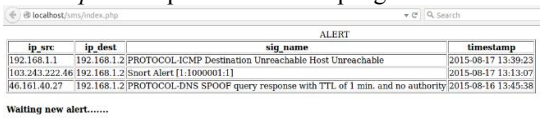
Setelah proses normalisasi maka data akan di*cluster* menggunakan metode K-Means. Dari proses *cluster* tersebut akan menghasilkan label bahaya dan tidak bahaya. Hasil dari *cluster* adalah sebagai berikut:

K-Means

No	Protocol	Port	Jarak Cluster 1	Jarak CLuster 2	Label
1	1	11.59227893	11.914833679482	11.262424537612	tidak bahaya
2	1	0.22278172	23.28056574535	0.17617476293526	tidak bahaya
3	1	0.03204395	23.471271455647	0.32953362697595	tidak bahaya
4	1	1.01625086	22.487235810408	0.69953349855425	tidak bahaya
5	2	5.10414282	18.404132790943	4.8504142632231	tidak bahaya
6	2	5.10261692	18.405657955316	4.8489125901295	tidak bahaya
7	1	0.12054627	23.382783946313	0.25210886923885	tidak bahaya
8	1	0.03509575	23.468220164499	0.32677018712515	tidak bahaya
9	1	0.03509575	23.468220164499	0.32677018712515	tidak bahaya
10	1	0.03509575	23.468220164499	0.32677018712515	tidak bahaya
11	1	0.03509575	23.468220164499	0.32677018712515	tidak bahaya
12	1	0.03509575	23.468220164499	0.32677018712515	tidak bahaya
13	1	0.03509575	23.468220164499	0.32677018712515	tidak bahaya
14	1	0.03509575	23.468220164499	0.32677018712515	tidak bahaya
15	1	0.03509575	23.468220164499	0.32677018712515	tidak bahaya
16	1	0.03509575	23.468220164499	0.32677018712515	tidak bahaya
17	1	0.03509575	23.468220164499	0.32677018712515	tidak bahaya
18	1	0.03509575	23.468220164499	0.32677018712515	tidak bahaya
19	1	0.03509575	23.468220164499	0.32677018712515	tidak bahaya
20	2	47.81414511	24.32145649618	47.491231050755	bahaya
21	2	47.81414511	24.32145649618	47.491231050755	bahaya
22	1	42.21408408	18.719588289431	41.883600370652	bahaya
23	1	42.21408408	18.719588289431	41.883600370652	bahaya
24	1	42.21408408	18.719588289431	41.883600370652	bahaya
25	2	41.87685069	18.386339192295	41.555060247908	bahaya

4.3.6 Pengiriman SMS melalui SMS Gateway

Setelah data di*cluster* akan diteruskan untuk mengirim data serangan yang berbahaya saja. Proses pengiriman SMS di sistem ini menggunakan PHP. Berikut adalah *website* PHP yang mana tabelnya akan selalu *update* tiap 10 detik untuk pengiriman SMS.



ALERT

ip_src	ip_dest	sig_name	timestamp
192.168.1.1	192.168.1.2	PROTOCOL-ICMP Destination Unreachable Host Unreachable	2015-08-17 13:39:23
103.243.222.46	192.168.1.2	Snort Alert [1:1000001:1]	2015-08-17 13:13:07
46.161.40.27	192.168.1.2	PROTOCOL-DNS SPOOF query response with TTL of 1 min. and no authority	2015-08-16 13:45:38

Waiting new alert.....

4.3.7 Notifikasi SMS

Setelah pengiriman SMS melalui SMS Gateway maka *administrator* jaringan akan menerima notifikasi SMS sesuai format yang sudah ditentukan di web PHP. Berikut adalah contoh notifikasi SMS yang diterima:

5. Kesimpulan dan Saran.

5.1 Kesimpulan

Dari sistem ini dapat diperoleh beberapa kesimpulan sebagai berikut :

a. Hasil pengujian menunjukkan bahwa sistem keamanan jaringan bisa mendeteksi serangan.
b. Serangan dapat terdeteksi atau tidak tergantung dari pola data serangan tersebut ada di dalam *rule* snort atau tidak.
c. Hasil pengujian menunjukkan bahwa sistem bisa mengelompokkan jenis serangan menjadi dua kelompok, bahaya dan tidak bahaya.
d. Notifikasi SMS berhasil dikirim secara *realtime* dengan menggunakan PHP.
e. Hasil pengujian menunjukkan bahwa SMS gateway berhasil mengirimkan data serangan yang berlabel "bahaya" saja.

5.2 Saran

Pada penelitian ini sistem menghitung normalisasi data, menentukan *centroid*, menghitung jarak, menghitung *centroid* baru dan mengirim SMS dengan Bahasa PHP,agar perhitungan menjadi lebih efisien dapat dilakukan penelitian lanjutan dengan menggunakan *platform* Java dalam penentuan *centroid*, normalisasi data, menghitung jarak dan mengirimi SMS.

Daftar Pustaka:

Rehman, Rafeeq Ur. 2003. Intrusion Detection System with Snort: Advanced IDS Techniques Using Snort, Apache, MySQL, PHP and ACID. New Jersey: Prentice Hall PTR

Scoot, C., P. Wolfe, and B. Hayes. 2004. *Snort For Dummies*. Indiana: Willey Publishing, Inc.

Ramadhika A, *SMS Gateway Menggunakan Gammu Dan MySQL*, http://www.ubaya.ac.id/ubaya/articles_detail/33/SMS-Gateway-menggunakan-Gammu-dan-MySQL.html, edisi 29 Februari 2012, [25 Januari 2015]

Kendall, J.E. & Kendall, K.E. 2010. *Analisis dan Perancangan Sistem*. Jakarta: Indeks

Baker A. et al. 2004. *Snort 2.1 Intrusion Detection Second Edition.* Massachusetts: Syngress Publishing, Inc