RANCANGAN WIRELESS INTRUSION DETECTION SYSTEM MENGGUNAKAN SNORT

Irwan Agus Sobari
Program Studi Teknik Informatika
Sekolah Tinggi Manajemen Informatika dan Komputer Nusa Mandiri
(STMIK Nusa Mandiri)
Jl. Kramat 18 Jakarta Pusat
http://www.nusamandiri.ac.id
irwan.igb@nusamandiri.ac.id

ABSTRAK

Implementation of wireless networks do not have a mature information security plan will open up a lot of vulnerabilities that will be exploited by intruders or people who are not responsible. The development of wireless networks is rapidly increasing making it vulnerable to a number of security threats. Some attack that occur are spoofing, denial of service, backdoor, man in the middle attack and the others. This is due to the wireless network can not be limited to a building and wireless network transmission of data packets is very easy to catch people who are not responsible. It is Therefore necessary to build a good system and not expensive but very useful for the company. Systems built the intrusion detection system using SNORT that has the function to monitor wireless network traffic, looking for a data packet or suspicious behavior patterns to be recorded into a log and warning to notify the network administrator. This research is expected to help network administrators to monitor and learn some new types of attacks that occur and protect computer network that exist today.
Keywords: Intrusion detection system, Wireless, SNORT

ABSTRAKSI

Implementasi jaringan *wireless* yang tidak memilki perencanaan keamanan informasi yang matang akan membuka banyak celah keamanan yang akan dimanfaatkan oleh penyusup atau orang yang tidak bertanggung jawab. Perkembangan jaringan *wireless* yang semakin pesat membuatnya rentan terhadap sejumlah ancaman keamanan. Beberapa serangan yang terjadi adalah *spoofing, denial of service, backdoor, man in the middle attack* dan lain-lain. Hal ini disebabkan jaringan *wireless* tidak dapat dibatasi sebuah gedung dan paket data transmisi jaringan *wireless* sangat mudah ditangkap orang yang tidak bertanggung jawab. Oleh karena itu diperlukan membangun sistem yang bagus dan tidak mahal tetapi sangat bermanfaat bagi perusahaan. Sistem yang dibangun yaitu *intrusion detection system* menggunakan *SNORT* yang mempunyai fungsi untuk memonitoring traffik jaringan *wireless*, mencari paket data atau tingkah pola yang mencurigakan untuk dicatat kedalam log dan memberitahukan peringatan kepada administrator jaringan. Penelitian ini diharapkan akan membantu administrator jaringan untuk memonitoring dan mempelajari beberapa jenis serangan baru yang terjadi serta melindungi jaringan komputer yang ada saat ini.
Kata kunci: *Intrusion detection system, Wireless, SNORT*

PENDAHULUAN

Implementasi jaringan nirkabel (*wirelless*) yang tidak memiliki perencanaan keamanan informasi yang matang akan membuka banyak celah keamanan yang dapat ditembus dan dimanfaatkan oleh penyusup atau orang yang tidak bertanggung jawab. Seorang penyusup yang berhasil masuk melalui jaringan nirkabel (*wireless*) dan melakukan kerusakan informasi atau sistem informasi sebuah organisasi atau perusahaan memiliki kemungkinan lolos yang cukup besar dari usaha identifikasi.

Wi-fi pada dasarnya adalah istilah yang diberikan untuk sistem *wireless local area network* (LAN) yang menggunakan standar IEEE 802.11 yang ada pada saat ini. *Wireless* LAN merupakan suatu jaringan area lokal tanpa kabel dimana media transmisinya melalui udara menggunakan gelombang radio. Prinsip dasar pada jaringan *wireless* LAN pada dasarnya sama dengan jaringan LAN yang menggunakan kabel, perbedaan utamanya hanya pada media transmisinya, yaitu *wireless* LAN dengan gelombang radio sedangan jaringan LAN dengan kabel.

Menurut Purbo (2007) spesifikasi wifi dibagi menjadi 4 yaitu a,b,g dan n, berikut tabelnya:

Tabel 1. Spesifikasi Wifi dan Kompatibilitas

Spesifikasi	Kecepatan	Frekuensi	kompatibilitas
802.11b	11 Mb/s	2,4 GHz	b
802.11a	54 Mb/s	5 GHz	a
802.11g	54 Mb/s	2,4 GHz	b, g
802.11n	100 Mb/s	2,4 GHz	b, g, a

Sumber: Purbo (2007)

Menurut Depkominfo (2008) *Intrusion Detection System* (IDS) adalah tahap awal dari sistem yang memiliki fungsi hanya sebagai pendeteksi apabila terjadi anomali pada lalu lintas paket data di jaringan. Apabila sistem *Intrusion Detection System* (IDS) mendeteksi anomali tersebut, langkah selanjutnya adalah mencatat data tersebut ke sebuah *log* lalu memberi peringatan kepada administrator jaringan. Sedangkan Menurut Brenton and Cameron (2005) *Intrusion Detection System* (IDS) adalah sistem pendeteksian penyusupan yang merupakan sebuah konsep canggih yang melibatkan beberapa teknologi yang berbeda. Boleh dikatakan *intrusion detection system* sudah menjadi sepenting *firewall* untuk security network.

Intrusion Detection System (IDS) mempunyai beberapa komponen yaitu:

1. *Sensor* untuk mengenali adanya *security events*.
2. *Console* untuk memonitor *event* dan *alert* dan mengontrol *sensor*.
3. *Central Engine* untuk menyimpan *event logged* yang dilakukan oleh *sensor* kedalam *database* dan menggunakan aturan-aturan keamanan yang berguna untuk menangani *event* yang terjadi.

Dilihat dari kemampuan mendeteksi serangan atau penyusupan di dalam jaringan, maka *Intrusion Detection System* (IDS) dapat dibagi menjadi 2 (dua) yaitu:

a. *Network-Based Intrusion Detection System (NIDS)*
   Merupakan sistem yang akan menganalisa semua lalu lintas yang melewati ke sebuah jaringan yang akan mencari adanya percobaan serangan atau penyusupan ke dalam

sistem jaringan. Network-Based IntrusionDetection System menggunakan adapter promiscuous mode sehingga dapat melihat dan menganalisa semua trafik paket yang melewati jaringan secara realtime. Modul untuk mengenai adanya serangan menggunakan empat macam teknik untuk mengetahui pola dari serangan, yaitu:

1. Pola, ekspresi atau pencocokan bytecode.

2. Frekuensi atau threshold paket yang lewat di dalam jaringan.

3. Hubungan antara setiap event.

4. Statistik pendeteksi anomaly paket

b. *Host-based Intrusion Detection System* (HIDS)

Merupakan sistem yang mampu mendeteksi hanya pada host tempat implementasi Intrusion Detection System. Aktivitas sebuah host jaringan individu akan dipantau apakah terjadi percobaan serangan atau penyusupan ke dalamnya atau tidak. Host-based Intrusion Detection System biasanya sering diletakkan pada server-server jaringan yang kritis, seperti halnya peletakkan firewall, web server, atau server yang terkoneksi ke internet.

Tabel 2. Perbandingan tipe IDS

***Network-Based* IDS**	***Host-Based* IDS**
Ruang lingkup yang luas (mengamati semua aktivitas jaringan)	Ruang lingkup yang terbatas (mengamati hanya aktivitas pada *client* tertentu)
Lebih mudah melakukan setup	Setup yang kompleks
Lebih baik untuk mendeteksi serangan yang berasal dari luar jaringan	Lebih baik mendeteksi serangan yang berasal dari dalam jaringan
Lebih murah untuk diimplementasikan	Lebih mahal untuk diimplementasikan
Pendeteksi berdasarkan pada apa yang direkam dari aktivitas jaringan	Pendeteksi berdasarkan pada single client yang mengamati semua aktifitas
Menguji paket *headers*	Paket *headers* tidak diperhatikan
Respon yang *realtime*	Selalu merespon setelah apa yang terjadi
Mendeteksi serangan terhadap jaringan serta *payload* untuk dianalisis	Mendeteksi serangan local sebelum mereka memasuki jaringan
Mendeteksi usaha dari serangan yang gagal	Menverifikasi suskes atau gagalnya suatu serangan

Sumber: depkomimfo (2008)

Menurut Rafiudin (2010:1) *snort* adalah sebuah aplikasi atau *tool security* untuk mendeteksi intrusi-intrusi jaringan (penyusupan, penyerangan pemindaian, dan berbagai bentuk ancaman lainnya), sekaligus juga melakukan pencegahan Istilah populernya, *snort* merupakan salah satu *tool Network Intrusion Prevention System* (NIPS) dan *Network Intrusion Detection System* (NIDS). Dalam prakteknya, *snort* sangat handal untuk membentuk *logging* paket-paket dan analisis trafik-trafik secara *real-time* dalam jaringan-jaringan berbasis TCP/IP. *Snort* merupakan bagian dari *Intrusion Detection System* yang terdiri dari beberapa komponen, yaitu:

1. *Packet Decoder*

   Packet Decoder mengambil paket dari beberapa jenis perangkat jaringan dan mempersiapkan paket data untuk

dapat masuk ke *preprocessed* atau dikirim ke mesin deteksi (*Detektion Engine*).

2. *Preprocessor*
   Yaitu komponen atau *plug-ins* yang dapat digunakan dengan *snort* untuk mengatur atau memodifikasi paket data sebelum *Detection Engine* melakukan beberapa operasi untuk mengetahui apakan paket sedang digunakan oleh penyusup.
3. *Detection Engine*
   Detection Engine merupakan bagian terpenting dari *snort*. Yang berfungsi untuk mendeteksi jika ada aktifitas intrusi dalam sebuah paket.
   Beban pada *detectin Engine* tergantung pada beberapa faktor, yaitu:
   a. Jumlah *rule*
   b. Kekuatan mesin yang menjalankan *snort*
   c. Kecepatan bus internal yang digunakan dalam mesin *snort*
   d. Beban pada jaringan
4. *Logging* dan *Alert System*
   Tergantung pada yang ditemukan didalam *Detection Engine* dalam sebuah paket, paket yang digunakan untuk mencatat aktivitas atau menghasilkan *alert*.
5. *Output Modules*
   Output modul atau *plug-in* dapat melakukan operasi yang berbeda-beda tergantung pada bagaimana ingin menyimpan output yang dihasilkan oleh *logging* dan sistem *alert* dari *snort.*

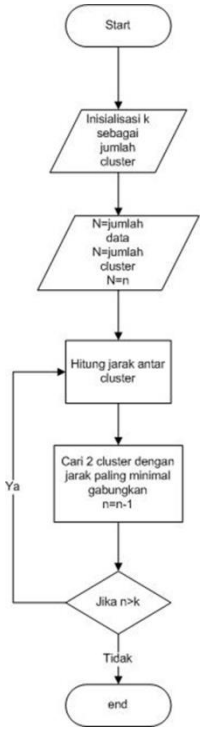
BAHAN DAN METODE

Jenis penelitian yang dilakukan oleh penulis adalah experimental yakni melakukan uji coba dengan batasan waktu dan tempat serta jumlah pengguna akses data yang diberikan. Beberapa hal yang dilakukan penulis untuk melakukan penelitian ini mengenai Perancangan *Wireless Intrusion Detectin System* dengan *Snort.* Desain penelitian yang dilakukan yakni studi literatur, observasi jaringan komputer, pengambilan data sebelum dan sesudah implementasi *Intrusion Detection System*.

Pada tahap ini dilakukan pengumpulan informasi mengenai beberapa hal yang berhubungan untuk implementasi yang dilakukan dengan mengambil referensi berasal dari buku-buku, *e-book*, dan jurnal-jurnal penelitian sesuai dengan pembahasan yang penulis buat yakni *Intrusion Detection System* untuk mendeteksi serangan dengan *snort.*

Algoritma yang digunakan untuk *Intrusion Detection System*, yaitu :

1. *algoritma Hierarchical 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. Contoh: *Single Linkage, Centroid Linkage, Complete Linkage, Average Linkage.*
2. *Flowchart Hierarchical Clustering*



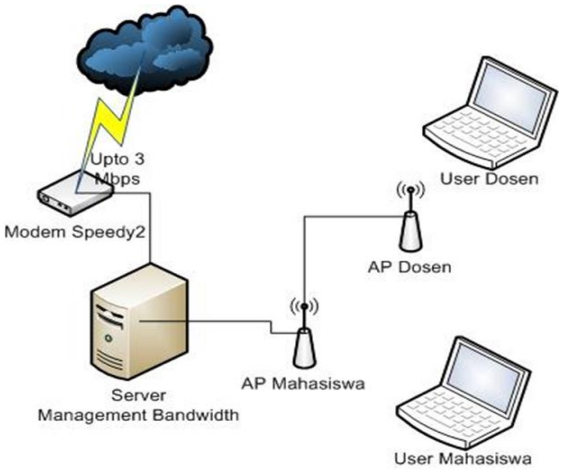
Sumber: hasil olahan sendiri

Gambar 1. Flowchart Hierarchical Clustering

HASIL DAN PEMBAHASAN

Infrastruktur jaringan komputer saat ini dengan media transmisi kabel dan media nirkabel (*wireless*). Koneksi jaringan Internet menggunakan ISP dari Telkom dengan kecepatan *bandwidth up to* 3 Mbps. Penggunaan *Provider* ini hanya untuk internet.

Dari deskripsi infrastruktur diatas penulis melakukan penelitian pada jalur koneksi Internet yang menggunakan menggunakan media *wireless* untuk para pengguna hotspot yang melalui *server management bandwidth*. Dibawah ini gambar infrastruktur yang akan penulis melakukan penelitian.

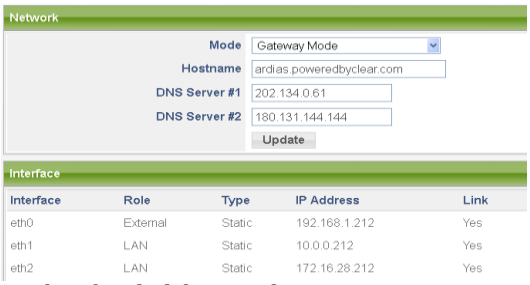


Sumber: hasil olahan sendiri

Gambar 2. Skema Jaringan Server IDS

Penulis melakukan penelitian pada infrastruktur ini dikarenakan jaringan nirkabel (*wireless*) sangat rentan terhadap penyusupan atau gangguan yang dilakukan oleh orang yang tidak bertanggung jawab. Dikarenakan jaringan komputer berbasis *wireless* masih memiliki banyak celah keamanan (vulnerabilities). Pada jaringan komputer yang penulis melakukan penelitian jalur koneksi Internet menggunakan *Provider* Telkom Speedy dengan kecepatan *bandwidth* Internet upto 3 Mbps yang tehubung melalui media jalur telepon dengan menggunakan modem ADSL kemudian diteruskan melalui media kabel UTP menuju server management bandwidth. Server ini menggunakan *snort* dimana terdapat tiga buah kartu jaringan internet yakni *eth0* untuk koneksi dari *modem*, *eth1* koneksi untuk *hotspot* dan *eth2* koneksi untuk jaringan komputer lokal. Untuk mengkonfigurasinya dapat di akses melalui *webconfig* dengan *browsing* ke alamat IP *server* tersebut yakni https://172.16.28.212:81, kemudian memilih fitur *Network* menu IP *Setting*. Gambar di bawah ini

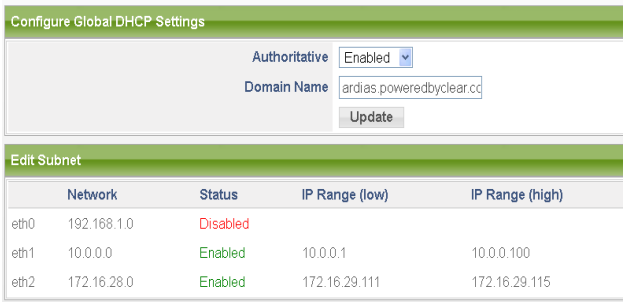
konfigurasi kartu jaringan dengan IP *address* yang terdapat pada server *management bandwidth*.



Sumber: hasil olahan sendiri

Gambar 3. Konfigurasi Ethernet Card

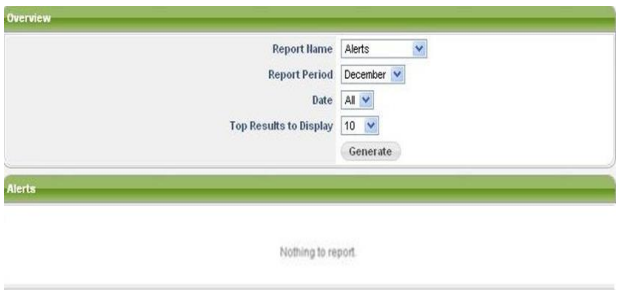
Untuk pengaturan distribusi IP *Address* diberikan kepada pengguna Internet baik melalui jaringan kabel lokal maupun melalui jalur *hotspot*. Pada *eth1* untuk para pengguna Internet melalui *hotspot* diberikan batasan IP *Address* sebanyak 100 (seratus) pengguna yang dimulai mulai dari IP *Address* 10.0.0.1 sampai dengan IP *Address* 10.0.0.100. pada *eth2* untuk para pengguna Internet melalui media kabel lokal diberikan batasan IP *Address* sebanyak 5 (lima) pengguna yang dimulai dari IP *Address* 172.16.29.111 sampai dengan IP *Address* 172.16.29.115. IP *Address* untuk pengguna Internet pada jaringan kabel lokal dibatasi hanya lima pengguna dikarenakan IP *Address* pada jaringan kabel lokal sudah dibuat tetap, distribusi ini hanya diperuntukkan uji coba dan alternatif dalam keadaan darurat. Untuk distribusi IP *Address* konfigurasinya pada fitur *Network* menu DHCP *server*, dapat dilihat pada gambar dibawah ini.



Sumber: hasil olahan sendiri

Gambar 4. Konfigurasi DHCP Server

Berdasarkan data yang diambil dari sistem *snort* pada fitur menu *Reports Intrusion Detection System* yang diambil berdasarkan satu bulan terakhir yaitu bulan Desember 2012, dapat dilihat pada gambar dibawah ini**.**



Sumber: hasil olahan sendiri

Gambar 5. Report Jenis Serangan IDS

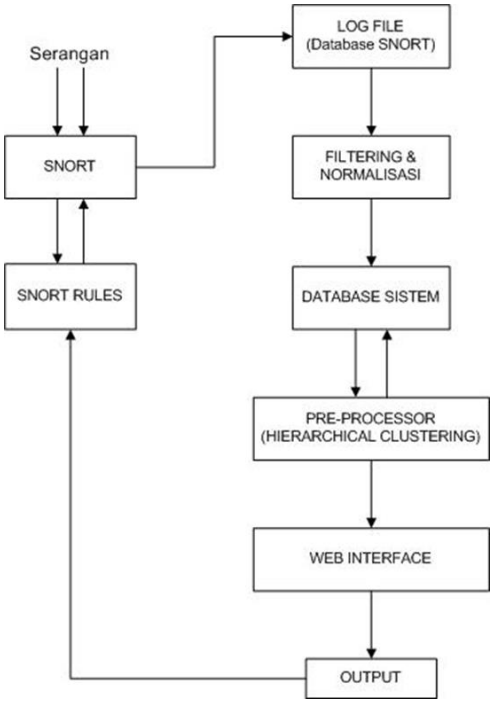
Dari gambar diatas terlihat jelas berdasarkan laporan periode bulan Desember 2012 tidak ada hasil (0%) yang dapat ditampilkan dari laporan *alert*, yakni jenis-jenis serangan yang didapat pada sistem *intrusion detection system*. Pada gambar dibawah ini juga terlihat jelas tidak adanya IP *address* penyerang yang ditangkap oleh sistem *intrusion detection system* berdasarkan laporan perbulan Desember 2012 tidak ada hasil (0%) yang dapat ditampilkan dari laporan perbulan pada server *intrusion detection system* yang belum diimplementasikan, dapat dilihat pada gambar dibawah ini.

Sumber: hasil olahan sendiri

Gambar 6. Report IP Addres Penyerang

Pada tahap ini akan dilakukan implementasi *intrusion detection* pada Infrastruktur jaringan Komputer di tempat penulis melakukan penelitian. Implementasi ini menggunakan infrastruktur yang ada seperti yang telah dibahas pada sub menu observasi jaringan komputer. Penggunaan perangkat keras juga masih menggunakan perangkat yang ada Untuk *server intrusion detection system* menggunakan *server management bandwidth* yang sedang berjalan. Disini penulis akan mendesain sistem *intrusion detection* yang diinginkan. Dibawah ini gambar skema jaringan implementasi *server intrusion detection system.*

Ada beberapa hal yang harus didesain sehingga *server intrusion detection system* dapat berjalan sesuai yang diharapkan.



Sumber: hasil olahan sendiri

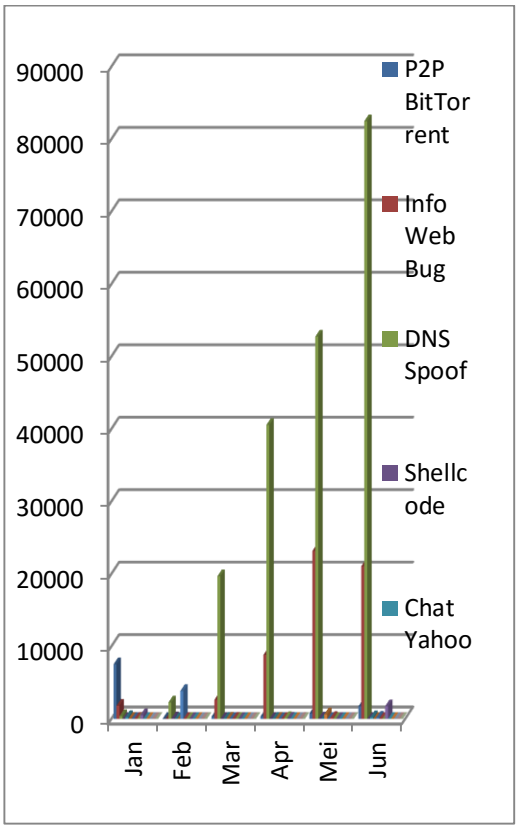
Gambar 7. Desain Intrusion Detection System

Pada gambar diatas menjelaskan bahwa serangan yang terjadi pada sistem akan *dicapture* oleh *snort* dan akan disimpan pada *log file snort*, selanjutnya di *filtering* parameter apa saja yang akan dipilih dan dimasukkan ke dalam *database* dan nantinya dianalisa dan di *clustering* pada *pre-processor* dengan *hierarchical clustering*, lalu hasil dari *clustering* ditampilkan pada *user interface* berbasis *web* secara *realtime*. *Output web interface* akan selalu mengupdate *rules snort* jika ada serangan baru atau yang belum dikenali oleh *snort*, sehingga *snort* akan melakukan *action* dengan memblokir IP *address* yang digunakan untuk melakukan serangan pada sistem jaringan tersebut.

Pada tahapan ini pengambilan data setelah implementasi dijalankan pada saat penelitian, waktu pengambilan data ini dimulai dari awal implementasi dijalankan yakni

mulai awal tahun 2013 dari bulan Januari 2013 sampai bulan Juni 2013 dimana penggunaan Internet pada jaringan nirkabel (*wireless*) yang melalui server *intrusion detection system* dapat terlihat hasil prosentase jenis serangannya, IP *address* yang digunakan oleh penyerang, dan IP *address* korban yang diserang yang tersimpan pada server *intrusion detection system***.**

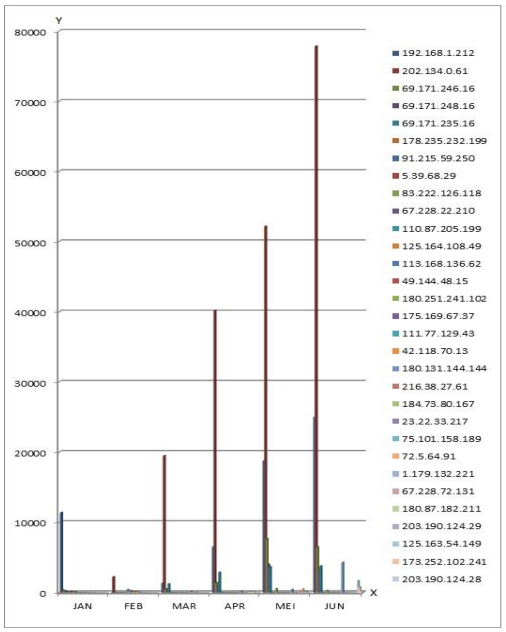
Laporan yang dapat diberikan dari data yang ada yakni berupa grafik jenis serangan dan IP *address* yang digunakan oleh penyerang. Gambar grafik dibawah ini merupakan paket data yang mencurigakan yang ditangkap oleh server *intrusion detection system* selama 6 (enam) bulan yaitu bulan Januari 2013 sampai Juni 2013.



Sumber: hasil olahan sendiri

Gambar 8. Serangan Bulan Januari-Juni 2013

Pada gambar grafik diatas dapat dilihat jenis serangan yang paling sedikit dan yang terbanyak yang terjadi pada jaringan *wireless* selama 6 (enam) bulan yakni bulan Januari 2013 sampai bulan Juni 2013. Dimana pada bulan Juni 2013 terdapat serangan DNS *Spoofing* terbesar dibandingkan bulan-bulan lainnya. Berdasarkan IP *address* yang digunakan oleh penyerang yang digunakan untuk menyerang jaringan *wireless* pada bulan Januari-Juni 2013, sebagai berikut:



Sumber: hasil olahan sendiri

Gambar 9. IP *Adrress* Penyerang Bulan Januari-Juni 2013

Pada gambar grafik diatas dapat dilihat IP *address* penyerang yang tertangkap yang paling sedikit dan yang terbanyak yang terjadi pada jaringan *wireless* selama 6 (enam) bulan yakni bulan Januari 2013 sampai bulan Juni 2013. Dimana pada bulan Juni 2013 terdapat IP *address* penyerang terbesar dibandingkan bulan-bulan

KESIMPULAN

Berdasarkan penelitian yang telah penulis lakukan maka dapat disimpukan sebagai berikut :

1. Perancangan *intrusion detection system* yang diterapkan pada jaringan nirkabel (*wireless*) telah berhasil mendeteksi jenis-jenis serangan yang menyerang sistem jaringan tersebut, hal ini dapat terlihat dari laporan dari data grafik *intrusion detection system*.
2. Hasil analisa yang didapat dari data yang telah dilakukan implementasi server *intrusion detection system* maka didapatkan grafik yang menunjukkan bahwa IP *address* yang digunakan untuk menyerang sistem jaringan *wireless* pada Bina Sarana Informatika tersimpan pada server *intrusion detection system* yang dilakukan selama 6 (enam) bulan yakni Januari 2013 sampai Juni 2013.
3. Hasil dari paket data yang mencurigakan yang ditangkap oleh server *intrusion detection system* dapat dilihat berdasarkan perbulan dari bulan Januari 2013 sampai Juni 2013 melalui aplikasi web secara *realtime*.
4. Hasil analisa yang didapat dari data setelah diimplementasikan server *intrusion detection system* yaitu metode *Hierarchical Clustering* dapat memdeteksi jenis serangan baru sehingga dapat mengupdate *rules snort* pada *server intrusion detection system.*

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Allah SWT atas segala nikmat yang berikan terutama nikmat sehat sehingga artikel ini bisa selesai, dan Istri saya Juliah Sari serta anak saya Adara Naila Maulida yang selalu memberikan semangat.

DAFTAR PUSTAKA

Purbo, Onno W. 2007. Jaringan Wireless Di Dunia Berkembang. Creative Commons Licence 3.0. Banjarbaru.

Departemen Komunikasi Dan Informatika. 2008. Panduan Topologi & Keamanan Sistem Informasi. Jakarta.

Departemen Komunikasi Dan Informatika. 2009. Tutorial Interaktif Instalasi Intrution Prevention System Berbasis Open Source. Jakarta.

Rafiudin, Rahmat. 2010. Mengganyang Hacker dengan SNORT. ANDI. Yogyakarta.

Hantoro, Gunadi Dwi. 2009. Wifi (Wireless LAN) Jaringan Komputer Tanpa Kabel. Informatika. Bandung

Micro, Andi. 2012. Buku Hijau ClearOS 5.2 Edisi Revisi. Creative Common License 3.0. Banjarbaru.