Sistem Monitoring Pendeteksian Penyusup Menggunakan Snort pada Jaringan Komputer Fakultas Ekonomi Universitas Methodist Indonesia

[1]Arpenta L.T. Ginting, [2]Junika Napitupulu, [3]Jamaluddin Jamaluddin

[1]Mahasiswa Program Studi D-III Manajemen Informatika
[2,3]Dosen Program Studi D-III Manajemen Informatika
Universitas Methodist Indonesia
[1]arpenta_l@yahoo.com, [2]junica.nptu@gmail.com, [3]jac.satuno@gmail.com

Abstrak

Berkembangnya teknologi informasi khususnya jaringan komputer dan layanannya disatu sisi mempermudah pekerjaan manusia sehari-hari, akan tetapi di sisi lain timbul masalah yang sangat serius, yakni faktor keamanannya. Sistem informasi pada jaringan komputer yang rentan mengakibatkan mudahnya penyusup (intruder) untuk masuk dan mengambil informasi rahasia pada sistem tersebut. Oleh karena itu diperlukan adanya sistem pendeteksian untuk mengetahui adanya aktivitas-aktivitas yang mencurigakan. Snort merupakan tools yang mampu mendeteksi dan memberikan alert apabila terjadi serangan di dalam jaringan.

1. Pendahuluan

Berkembangnya teknologi informasi khususnya jaringan komputer dan layanannya disatu sisi mempermudah pekerjaan manusia sehari-hari, akan tetapi di sisi lain timbul masalah yang sangat serius, yakni faktor keamanannya. Di satu sisi manusia sudah sangat tergantung dengan sistem informasi, akan tetapi di sisi lain keamanan dan kerahasiaan informasi pada jaringan komputer tidak terjamin[3][6]. Hal ini secara umum terjadi karena kepedulian terhadap keamanan sistem informasi yang sangat kurang.

Sistem informasi pada jaringan komputer yang rentan mengakibatkan mudahnya penyusup (*intruder*) untuk masuk dan mengambil informasi rahasia pada sistem tersebut. Oleh karena itu diperlukan adanya sistem pendeteksian untuk mengetahui adanya aktivitas-aktivitas yang mencurigakan. Sistem pelaporan pertahanan tehadap aktivitas-aktivitas mencurigakan yang ada saat ini umumnya dilakukan secara manual oleh *administrator*. Hal ini mengakibatkan integritas sistem bergantung pada ketersediaan dan kecepatan *administrator*. Selain itu *administrator* harus selalu *standby* untuk melihat kondisi jaringannya jika terjadi penyusupan.

2. Landasan Teori

2.1 Jaringan Komputer

Jaringan komputer adalah dua atau lebih komputer yang saling berhubungan melalui kabel (atau dalam beberapa kasus, dengan kondisi nirkabel) sehingga mereka dapat saling bertukar informasi[10].

Keamanan jaringan adalah proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Langkah-langkah pencegahan membantu menghentikan pengguna yang tidak sah untuk mengakses setiap bagian dari sistem jaringan komputer. Keamanan jaringan komputer sendiri bertujuan untuk mengantisipasi resiko pada jaringan komputer berupa bentuk ancaman fisik maupun logika baik langsung ataupun tidak langsung menggangu aktivitas yang sedang berlangsung dalam jaringan komputer. Secara umum, terdapat 3 hal dalam konsep keamanan jaringan, yakni:

a. Resiko atau tingkat bahaya (*risk*)
b. Ancaman (*threat*)
c. Kerapuhan sistem (*vulnerability*)[10]

Keamanan sendiri menyangkut 3 elemen dasar yakni:

a. Keamanan jaringan (*network security*)
b. Keamanan aplikasi(*application security*)
c. Keamanan komputer (*computer security*)[4]

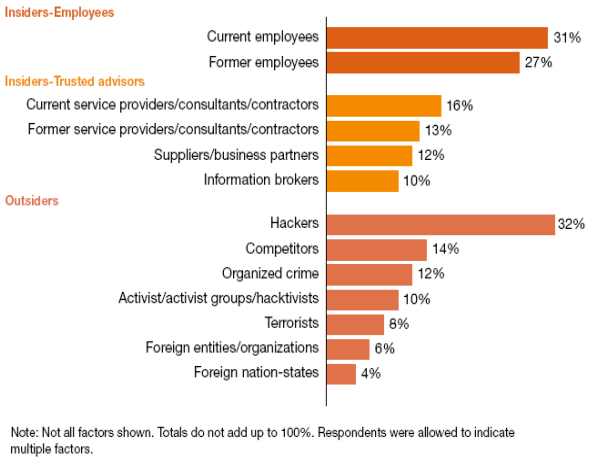
Keamanan jaringan sering dipandang sebagai hasil dari beberapa factor. Faktor ini bervariasi tergantung pada bahan dasar, tetapi secara normal setidaknya ada beberapa hal dalam konsep keamanan jaringan diantaranya adalah kerahasiaan, integritas dan ketersediaan[4].

2.2 Penyusup

Penyusup (*intruder*) merupakan orang yang melakukan tindakan yang menyimpang (*anomaly*), tidak tepat (*incorrect*), dan tidak pantas (*inappropriate*) terhadap suatu jaringan komputer.

Dari hasil yang dilakukan *Key findings from The Global State of Information Security Survey 2014*, menunjukkan grafik orang-orang yang melakukan penyusupan kedalam sistem ataupun membobol sistem

keamanan komputer. Sebagaimana dicatat, sebagian besar responden atribut insiden keamanan yang melakukan ancaman dan penyusupan sehari-hari pada instalasi tersebut kebanyakan seperti karyawan dan mantan karyawan.



Gambar 1: Grafik tabulasi penyusupan tahun 2014

2.3 IDS (Intrution Detection System)

IDS (Intrution Detection System) adalah sebuah sistem yang melakukan pengawasan terhadap traffic jaringan dan pengawasan terhadap kegiatan-kegiatan mencurigakan berhubungan dengan traffic jaringan maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan. Dalam banyak kasus IDS juga merespon terhadap traffic yang tidak normal/anomali melalui aksi pemblokiran seorang user atau alamat IP (Internet Protocol) sumber dari usaha pengaksesan jaringan.

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.

2.4 Snort

Snort adalah NIDS yang bekerja dengan menggunakan *signature detection*, berfungsi juga sebagai *sniffer* dan *packet logger*[2].Snort pertama kali di buat dan dikembangkan oleh Marti Roesh, lalu menjadi sebuah opensource project. Versi komersial dari snort dibuat oleh Sourcefire (www.sourcefire.com). Snort memiliki karakteristik, sebagai berikut:

1. Berukuran kecil – *Source code* dan *rules* untuk rilis 2.1.1 hanya 2256k.
2. *Portable* untuk banyak OS – Telah diporting ke Linux, Windows, OSX, Solaris, BSD,dll.
3. Cepat – Snort mampu mendeteksi serangan pada network 100Mbps.
4. Mudah dikonfigurasi – Snort sangat mudah dikonfigurasi sesuai dengan kebutuhan network kita. Bahkan kita juga dapat membuat *rule* sendiri untuk mendeteksi adanya serangan baru.
5. Free – Kita tidak perlu membayar sepeser pun untuk menggunakan snort. Snort bersifat open source dan menggunakan lisensi GPL.

Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu dapat menganalisis lalu lintas *real-time*, hal ini dapat mendeteksi berbagai jenis serangan. Snort bukanlah sebatas protocol analisis atau sistem pendeteksi penyusupan (*Intrusion Detection System*) IDS, melainkan sedikit gabungan diantara keduanya, dan bias sangat berguna dalam merespons insiden-insiden peyerangan terhadap host-host jaringan. Fitur Snort dapat menjadi penolong administrator sistem dan jaringan, dimana mampu memperingatkan kita atas penyusup yang berpeluang berbahaya[5][8].

Fitur-fitur inilah yang menjadikan Snort sebuah sistem pendeteksi gangguan dan serangan jaringan yang sangat berguna bagi tim penanggulangan insiden. Snort sekarang dapat dioperasikan dengan empat (4) buah mode[2]:

1. *Paket sniffer:* Praktis membaca paket-paket dari jaringan dan memperlihatkan pada kita dalam bentuk aliran tak terputus pada layar.
2. *Packet logger:* untuk mencatat semua paket yang lewat di dalam disk.
3. NIDS (*Network Intrusion Detection System*): deteksi penyusup pada network: pada mode ini Snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer.
4. *Inline Mode*, mengambil paket dari *iptable* dan menginstruksikan *iptable* untuk meneruskan paket tersebut berdasarkan jenis *rule* dari Snort yang digunakan.

3. Analisis dan Perancangan

3.1 Analisis

Pada bab ini, penulis akan membahas tentang analisis masalah yang diperlukan dalam menganalisis pendeteksian serangan yang terjadi pada sebuah jaringan komputer dan kebutuhan sistem monotoring penyusup jaringan komputer.

Adapun analisis yang akan dilakukan penulis ada 3 hal, yaitu:

1. Mendeteksi komputer yang hidup dalam jaringan.
2. Mendeteksi port yang terbuka.
3. Mendeteksi IP Address komputer yang aktif di dalam jaringan.

Adapun analisis kebutuhan sistem monotoring penyusup jaringan komputer meliputi perangkat keras (Hardware) dan perangkat lunak (software).

3.2 Perancangan

Perancangan adalah strategi untuk memecahkan masalah dan mengembangkan solusi terbaik bagi permasalahan itu. (*Nugroho, A. 2002*).

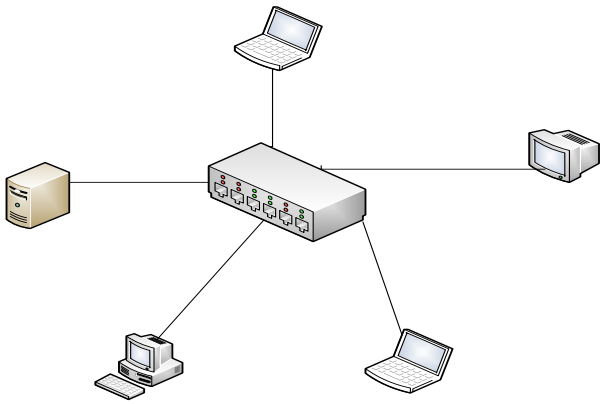
Dalam perancangan ini penulis akan membahas tentang perancangan yang digunakan dalam melakukan penelitian yaitu sebagai berikut:

1. Perancangan Jaringan
2. Perancangan Sistem

3.2.1 Perancangan Jaringan

Perancangan jaringan yang dilakukan penulis adalah jaringan dengan topologi star. Topologi star yang digunakan oleh penulis dalam melakukan penelitian ini untuk menghubungkan unit-unit komputer yang dilindungi oleh aplikasi snort.

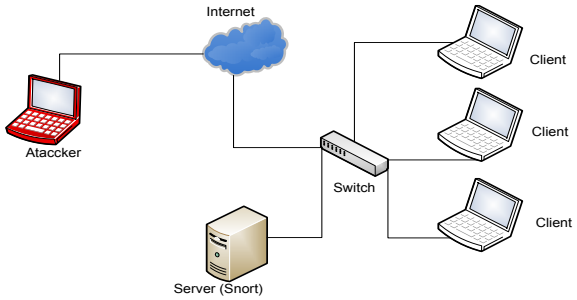
Topologi star ini membentuk seperti bintang karena semua komputer di hubungkan ke sebuah hub atau switch dengan kabel UTP, sehingga hub/switch lah pusat dari jaringan dan bertugas untuk mengontrol lalu lintas data, jadi jika komputer 1 ingin mengirim data ke komputer 2, data akan dikirim ke switch dan langsung di kirimkan ke komputer tujuan tanpa melewati komputer lain[1].



Gambar 2. Topologi Star

3.2.2 Perancangan Sistem

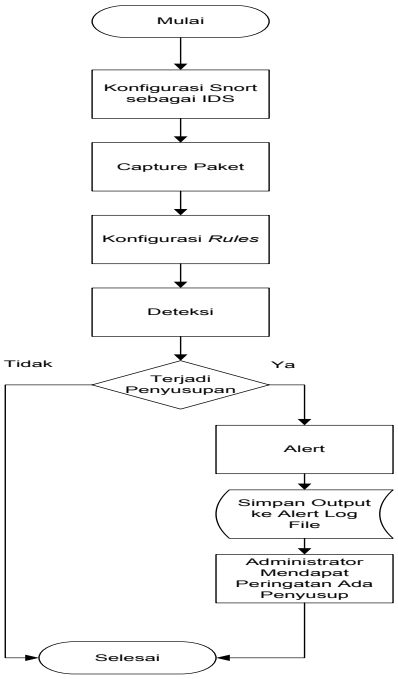
Dalam perancangan sistem penulis akan membahas tentang cara membuat perancangan sistem monotoring pendeteksi penyusup di dalam sistem operasi Ubuntu. Secara sederhana skema jaringan pendeteksian menggunakan Snort dapat dilihat pada gambar 3.



Gambar 3. Skema Jaringan untuk Pendeteksian SNORT

3.3 Flowchart Prosedural

Setelah selesai dalam merancang skema pendeteksian, maka penulis akan membahas prosedur tentang prosedur dari cara kerja Snort. Secara sederhana penulis juga membuat gambar dari cara kerja server yang menggunakan snort dapat dilihat pada gambar berikut:

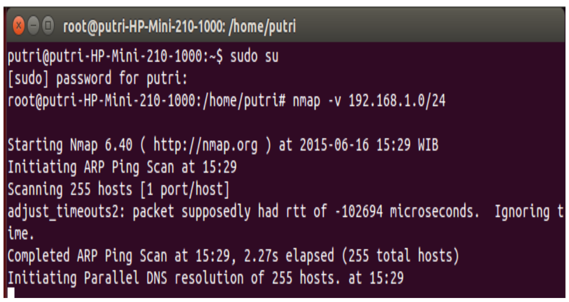


Gambar 4. Flowchart Sistem Monitoring Penyusup

Dari gambar 4 dapat dilihat cara kerja dari Snort saat melakukan pendeteksian. Mulai dari menjalankan Snort dan melakukan pendeteksian sampai dengan Snort selesai dijalankan ataupun dihentikan melakukan monitoring/pendeteksian.

4 Hasil dan Pembahasan

Pengujian dilakukan dengan menghubungkan dua atau lebih komputer, komputer-komputer tersebut terdiri dari 1 unit sebagai komputer server yang di install aplikasi snort, beserta beberapa komputer lainnnya sebagai client dan ataccker yang dihubungkan dengan switch menggunakan topologi star. Aplikasi snort akan diaktifkan dan memantau setiap aliran data yang masuk dan keluar pada sistem jaringan yang diamankannya. Pada penelitian ini jumlah komputer yang dipantau berjumlah maksimal 256 unit dengan skema jaringan 192.168.1.0/24. Pada penelitian ini penulis mencoba untuk melakukan penyusupan dengan menggunakan komputer yang berada diluar sistem jaringan yang dilindungi komputer server.



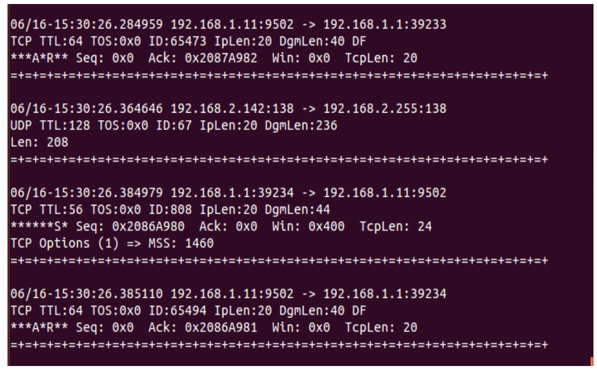
Gambar 5. Port Scanning (melakukan pencarian IP Address)

Sebelum melakukan serangan ataupun penyusupan, laptop attacker akan mencari IP Address yang terbuka ataupun yang ada di dalam jaringan. Pengujian dilakukan dengan tujuan membuktikan bahwa administrator dapat melihat alamat IP Address yang mencoba melakukan serangan.

Gambar 6 Snort dijalankan

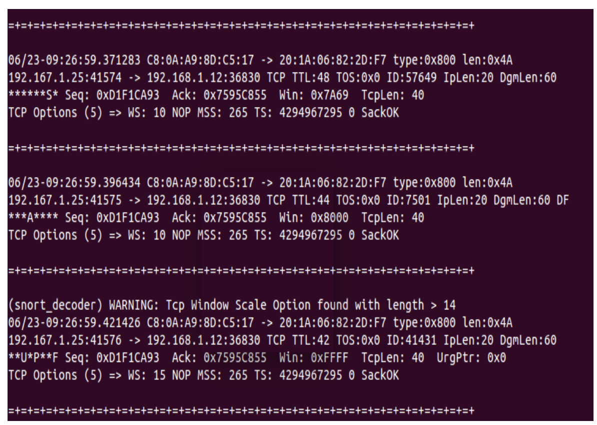
Dari gambar di atas dapat dilihat bahwa snort sedang dijalankan dan melakukan scanning ataupun mendeteksi dari semua alamat IP Address yang banyaknya berjumlah 256. Saat Snort dijalankan maka paket data akan langsung muncul. Paket data yang muncul adalah sebagai berikut:

06/16-15:14:21.250738 192.168.1.209:137 -> 192.168.1.255:137
UDP TTL : 128 TOS : 0X0 ID : 24505 IpLen : 20 DgmLen : 78
=+
06/16-15:14:21.999540 192.168.1.209:137 -> 192.168.1.255:137
UDP TTL : 128 TOS : 0X0 ID : 24602 IpLen : 20 DgmLen : 78
=+



Gambar 7. Alamat IP Address yang mencoba masuk

Dari gambar 7 dapat dilihat bahwa Alert tersebut menunjukkan bahwa seseorang dari IP 192.168.1.11 melakukan port scanning untuk komputer dengan IP 192.168.1.1 dan mencoba masuk ke dalam jaringan ataupun menyusup masuk ke dalam komputer dengan IP Address 192.168.1.11.



Gambar 8. Snort mendeteksi ada serangan

Dari gambar 8 dapat dilihat bahwa alamat IP Address 192.168.1.1 masuk dan melakukan serangan/penyusupan ke dalam komputer client dengan alamat IP Address 192.168.1.11 yang berhasil masuk ke dalam jaringan.

Dari gambar tersebut menunjukkan bahwa alamat IP Address 192.168.1.11 bukan hanya melakukan penyusupan tetapi juga melakukan serangan lebih dari 1 (satu) serangan dan bahkan sudah berhasil melakukan pengambilan maupun mengubah database ataupun data-data lain yang ada dari komputer client dengan alamat IP Address 192.168.1.1. Dapat dilihat banyaknya serangan ataupun penyusupan yang terjadi pada banyaknya

paket data yang dapat dan berhasil di monitoring ataupun terdeteksi oleh server (Snort).

Saat ataccker melakukan pencarian alamat IP Address yang terbuka maka server (Snort) bekerja dan mencari alamat IP Address yang melakukan scanning port di jalur lalu lintas data (dapat dilihat pada gambar 7). Setelah ataccker berhasil menemukan alamat IP Address yang terbuka maka ataccker melakukan penyusupan ke dalam komputer client yang alamat IP Address yang diketahui (dapat dilihat pada gambar 7).

Saat atacker masuk ke dalam jaringan komputer client dan melakukan penyusupan maka server (Snort) akan berjalan dan menunjukkan alert ke layar monitor yaitu alamat IP Address. Tentunya hasil dari serangan dapat dilihat pada gambar 8 saat melihat paket TCP yang terlihat.

Sama seperti sebelumnya maka line pertama di atas adalah milik Internet Protocol (IP), dapat dilihat bahwa terjadi penyusupan antara IP 192.168.1.1 port sumber 39234 dengan IP 192.168.1.11 port tujuan 9502. Di bawah kalimat milik protocol IP, ada satu kalimat yang berisi informasi umum dari paket yang dikirim merupakan gabungan informasi milik protokol IP & TCP. Beberapa informasi seperti di bawah ini:
TCP TTL: 64 TOS:0x0 ID:808 IpLen:20 DgmLen:44
TCP TTL : 56 ada 56 router yang masih bisa di lewati.
TOS:0x0 : Type of Service dari protocol IP, 0x0 adalah servis normal.
IpLen:20 : Panjang protocol IP 20 byte.
DgmLen:52 : Panjang seluruh paket 44 byte.

Selanjutnya ada dua (2) kalimat yang semuanya milik Transmission Control Protocol (TCP).
******S* Seq: 0x2086A980 Ack: 0x0 Win: 0x400 TcpLen: 24
TCP Options (1) => MSS: 1460

Pada gambar 8 dapat dilihat state/kondisi sambungan, terlihat dari jenis paket yang dikirim, seperti:

******S* = paket sinkronisasi hubungan

***A**R* = paket acknowledge sinkronisasi hubungan

Sisanya adalah nomor urut paket data yang dikirim Sequence number (Seq), dan Acknowledge number (Ack) yang menunjukan sejauh ini nomor paket mana yang sudah berhasil masuk ataupun menyusup ke dalam komputer client tersebut.

5. Kesimpulan

Berdasarkan analisis dan pengujian yang telah dilakukan dapat diambil kesimpulan bahwa:

1. Sistem deteksi penyusup yang digunakan adalah Snort dan dapat mendeteksi pola serangan baik dari dalam (*local*) atau luar (internet) sesuai dengan rules yang telah dibuat sebelumnya.
2. Secara umum Snort bekerja hanya sebagai sistem deteksi dan tidak mampu menahan serangan, sehingga memerlukan kombinasi menggunakan Iptables *firewall* sebagai tindak pencegahan serangan.
3. Data keluar masuk yang dideteksi oleh Snort sebagai sistem *monitoring*
4. Informasi penyusup diketahui oleh admin saat melihat alamat IP Address yang masuk yang ditampilkan oleh Snort.

Daftar Pustaka

[1] Apriawan, Dwi N.H. 2015. *Protokol Jaringan Komputer*. http://ilmukomputer.com/hendra protokol jaringan.pdf diakses tanggal 27 April 2015.

[2] Ariyus, Dony. 2007. *Intrusion Detection System*. Yogyakarta: Andi Offset.

[3] Diansyah, Tengku M., 2014. *Analisa Mekanisme Snort dalam Menangani Serangan Flooding*. pada Prosiding Snastikom 2014 hal. 9 Networking & Data Communication. Medan: STT Harapan.

[4] IBISA, 2011, *Keamanan Sistem Informasi,* Yogyakarta: Andi Offset.

[5] Jamaluddin, 2012. *Modul Praktikum Keamanan Web dan Virus Komputer*. Medan: Lab.Komputer FE-UMI.

[6] Manimaran, G. 2004. *Internet Infrastructure Security in High Performance Interconnects*, pada Proceedings of 12th Annual IEEE Symposium on 2004, p.109.

[7] Pressman, Roger S. 2005. *Software Engineering,* USA: Mc.Graw Hill Inc.

[8] Rafiudin, Rahmat. 2010. *Mengganyang Hacker dengan Snort*, Yogyakarta: Andi Offset.

[9] Sofana, Iwan. 2008. *Membangun Jaringan Komputer*, Bandung: Informatika.

[10] Tanenbaun, Andrew S., 1989. *Computer Network*. Englewood: Prentice-Hall International, Inc.