

PENERAPAN *INTRUSION DETECTION SYSTEM* SEBAGAI *FIREWALL* DAN SARANA UNTUK MENANGKAL PENYUSUPAN *HACKER* PADA JARINGAN LOKAL ASURANSI JIWA INHEAL INDONESIA DI JAKARTA

¹Hendra Supendar dan ²Tunggul Yogi Hernowo

¹AMIK Bina Sarana Informatika

Jl. Kramat Raya No. 18 Jakarta Pusat, Indonesia

²Program Pascasarjana Magister Ilmu Komputer STMIK Nusa Mandiri

Jl. Salemba Raya No. 5 Jakarta Pusat (10250), Indonesia

hendrasupendar@gmail.com

Abstract

The attack on internet systems increasingly rampant, almost all of the information in the system vulnerable to attack and also generated a lot of financial losses due to these attacks, of course, as network administrators, is not an easy job to monitor the hundreds of IP in and out of clients. Install the honeypot to fool hackers also not the only way to better secure the internal regions and Demilitary Zone (DMZ). We need the help of a system that can monitor the data packet and record it and provide further information to be analyzed further. System Intrusion Detection System (IDS) can help users monitor and analyze problems in network security. In this case the IDS used a snort for windows software to monitor user activities on the system and out of the corporate network. The expected result is to know how much inconvenience caused to the system through a corporate network traffic. Data Base created using MySQL and what actions should be taken on these disorders will be the future. Testing of IDS performed on a local network of PT. Asuransi Jiwa Inhealth Indonesia for six days. Observations were made to the directory the user can monitor the daily activities in the network and the result will be a reference in determining how much disk capacity is needed for the system is not disturbed or damaged. Observations also held with the activities of suspected hacker activities, such as sending large data packets that can make the system unstable or monitor activity in and out of IP networks that are not known or suspected. The results of this analysis is that with as many as 45 (fourty five) user disk capacity to be provided for one year is 40 GB.

Keywords : hacker, Intrusion Detection System, snort for windows,

1. PENDAHULUAN

Serangan dan pencurian data yang dilakukan oleh seorang hacker untuk mengganggu sistem Komputer kita memang sudah sangat meresahkan. Banyak cara dilakukan untuk menanggulangi serangan dari *hacker* ini, mulai dari diskusi ilmiah, pembuatan peraturan tentang dunia maya dan pembelian *software* dan *hardware* yang berharga puluhan juta rupiah, namun hal tersebut sampai saat ini belum juga dapat menjaga system secara maksimal untuk terhindar dari serangan *hacker*.

Dari pengalaman Chris Brenton seorang Instruktur dan consultan Privat SANS Institute dimana pada bulan Desember tahun 2003 dia telah mengirimkan sebuah e-mail kepada *the North American Network Operators' Group (NANOG) mailing list*, dimana setelah mengirimkan e-mail tersebut sistem peringatan pada organisasinya menyala berkali kali, setelah diselidiki ternyata ada 16 kali upaya untuk me-relay email tersebut dari mail server-nya dari sumber IP yang sama. Andaikata pada saat itu

Christ Benton tidak menggunakan IDS, maka bisa kita duga bahwa usaha *hacker* tersebut akan berhasil (Northcutt, 2004).

Mengapa setiap organisasi atau perusahaan membutuhkan pengamanan yang maksimal ? Menurut (Sherif, 2002) dalam tulisannya mengenai *intrusion treath* dikatakan bahwa dalam *network* ada lima alasan mengapa pendeteksian terhadap ancaman penyusupan sangat perlu diperhatikan secara serius.

1. *The threat is real*: sejumlah informasi keamanan pada tahun 2000-an mencatat bahwa lebih dari 70% perusahaan melaporkan serangan keamanan.
2. *Everything is on the net*: Banyak perusahaan telah memindahkan kunci informasi dan sumber daya bisnisnya ke *internet*, dan ini telah membuka informasi sensitif perusahaan.
3. *Firewalls and VPNs are not enough*: Meskipun kebijakan *firewall* yang baik dapat meminimalkan pembukaan banyak jaringan, *hacker* mengembangkan serangan

mereka dan metode metode subversi jaringan. Teknik-teknik ini termasuk email berbasis Trojan horse, teknik *scanning* secara diam diam, dan serangan secara nyata yang mem-*bypass* kebijakan firewall dengan membuat terobosan akses diatas protocol yang diperbolehkan seperti ICMP atau DNS.

4. *The amount of new vulnerabilities is increasing*: Jumlah informasi pada jaringan yang rentan begitu meluas, banyak perusahaan sekarang menjual kepelangganan untuk mencari kerentanan

, secara otomatis disesuaikan ke pada profil perusahaan dari sistem operasi dan perangkat keras jaringan. Kerentanan juga muncul di peralatan keamanan, seperti *firewall* dan bahkan peralatan IDS.

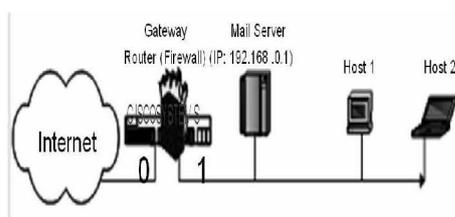
5. *Hackers are getting smarter*: *Hacker* dapat menggunakan *scanner port* untuk mencoba terhubung ke mesin *target* pada setiap *port* dan membangun daftar potensial aktif port. *Modern scanners port* termasuk identifikasi sistem operasi, dapat menargetkan seluruh rentang alamat IP dan bahkan mengirimkan umpan scan untuk membuatnya lebih sulit untuk target dalam mengidentifikasi sumber scanner yang sebenarnya.

2. PEMBAHASAN

Tinjauan Pustaka

A. FireWall

Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkungannya. Segmen tersebut dapat merupakan sebuah workstation, server, router, atau Local Area Network/LAN (Muammar, 2004)



Gambar 1. Ilustrasi FireWall (Liu, 2004)

Karakteristik sebuah firewall adalah : (Muamar, 2004)

1. Seluruh hubungan/kegiatan dari dalam ke luar, harus melewati firewall. Hal ini dapat dilakukan dengan cara memblokir/membatasi baik secara fisik semua akses terhadap jaringan Lokal, kecuali melewati firewall. Banyak sekali bentuk jaringan yang memungkinkan agar konfigurasi ini terwujud.
2. Hanya Kegiatan yang terdaftar/dikenal yang dapat melewati/melakukan hubungan, hal ini dapat dilakukan dengan mengatur policy pada konfigurasi keamanan lokal. Banyak sekali jenis firewall yang dapat dipilih sekaligus berbagai jenis *policy* yang ditawarkan.
3. Firewall itu sendiri haruslah kebal atau relatif kuat terhadap serangan/kelemahan. hal ini berarti penggunaan sistem yang dapat dipercaya dan dengan sistem yang relatif aman.

B. Hacker

1. Pengertian Hacker

Di Zaman dulu, *hacker* identik dengan pecandu komputer yang suka begadang sampai pagi, coba berbagai cara untuk mencari kelemahan keamanan sebuah sistem. Namun saat ini *hacker* adalah seseorang yang memiliki kemampuan pada komputer dan sistem jaringan, kemampuan standar yang dimiliki seorang *hacker* adalah *core programming* dan *network specialist*. *Hacker* merupakan pengguna komputer yang mampu masuk kedalam sistem komputer melalui jaringan, baik untuk keperluan *monitoring* (melihat sistem), *copying* (pengambilan/pencurian data), atau *crashing* (merusak sistem komputer) targetnya. (Chandra, 2009).

2. Klasifikasi Hacker

Hacker terdiri dari beberapa jenis sesuai dengan sifatnya. Baik orang itu seorang sistem administrator maupun user yang ingin membobol sistem komputer kita. Klasifikasi *hacker* antara lain sebagai berikut:

- a. **White Hats** : merupakan *hacker* yang bekerja sebagai *system analyst, system*

- administrator* maupun *security analyst*. *White hats* bekerja dalam sistem dan memiliki kemampuan yang tinggi untuk menjaga sistem agar tetap bekerja dengan baik dan tidak diacak-acak oleh orang lain. *White Hats hackers* rata-rata memiliki sertifikat kode etik *hacker*, misalnya CEH (*Certified Ethical Hacker*) (Wikipedia, 2009)
- b. **Gray Hats** : merupakan *hacker* yang bekerja *offensively* dan *defensively*. *Gray Hats* merupakan orang yang melakukan *attacking* terhadap sistem yang juga bekerja untuk membuat pertahanan terhadap sistem. Hacker tipe ini merupakan hacker yang membobol sistemnya untuk mendapatkan *bugs* dan lubang dari sistemnya yang kemudian mempelajari dan menutup lubang tersebut. (wikipedia, 2009)
 - c. **Black Hats** : merupakan *hacker* yang hanya bekerja sebagai *attacker* dan mengambil manfaat terhadap sistem yang diserangnya. *Black hats* merupakan *hacker* yang merusak sistem atau sering juga disebut sebagai *cracker*. Contoh aksi yang dilakukan oleh *hacker Black Hats* antara lain membobol situs perbankan, mengambil *account* (*Carding*), dsb.(wikipedia, 2008)
 - d. **Suicide Hacker** : *Hacker* yang bekerja persis seperti *Black Hats Hacker*, bersifat destruktif dan tidak peduli terhadap ancaman yang akan menimpanya. Rata rata *suicide hacker* merupakan orang yang tidak memiliki tujuan yang jelas, hanya membobol, mengambil keuntungan, ingin terkenal dan tidak takut terhadap hukum. (wikipedia, 2008)

Melihat macam macam *hacker* diatas maka kita mungkin akan merasa bahwa apapun yang kita lakukan pasti sistem kita tidak akan pernah aman, namun kita jangan pernah menyerah dan pasrah begitu saja, mempertahankan sistem yang telah kita bangun merupakan sebuah kewajiban yang harus kita tempuh dengan jalan apa saja.

Salah satu upaya untuk mengamankan sistem adalah dengan memasang sebuah hardware atau software penangkal hacker yang akan bekerja maksimal, Kemampuan mendeteksi penyusupan secara umum disebut IDS (*Intrusion Detection System*) dan kemampuan untuk mencegah akses dikenal dengan Firewall

C. Intrusion Detection System (IDS)

Intrusion Detection System digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. *Intrusion* adalah aktivitas tidak sah atau tidak diinginkan yang mengganggu konfidensialitas, integritas dan atau ketersediaan dari informasi yang terdapat di sebuah sistem. IDS akan memonitor lalu lintas data pada sebuah jaringan atau mengambil data dari berkas log. IDS akan menganalisa dan dengan algoritma tertentu akan memutuskan untuk memberi peringatan kepada seorang administrator jaringan atau tidak (laing, 2000).

IDS dapat melakukan inspeksi terhadap lalu lintas komunikasi data dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan penyusupan (termasuk kategori penyusupan atau tidak) dan terkadang memberikan penanganan terhadap susupan atau gangguan yang terjadi. Pendeteksian dilakukan IDS agar mem-blok gangguan jika segera dideteksi, bertindak sebagai *deterrent* (mencegah seseorang melakukan gangguan/*intrusion*), mengumpulkan informasi untuk meningkatkan keamanan.

Tipe dasar IDS menurut (Sherif, 2002)

1. *Rule-based systems* : berdasarkan atas database dari tanda penyusupan atau serangan yang telah dikenal. Jika IDS mencatat lalu lintas yang sesuai dengan database yang ada, maka langsung dikategorikan sebagai penyusupan.
2. *Adaptive systems*: mempergunakan metode yang lebih canggih. tidak hanya berdasarkan database yang ada, tetapi juga membuka kemungkinan untuk mendeteksi terhadap bentuk-bentuk penyusupan yang baru.

Bentuk yang sering digunakan untuk komputer secara umum adalah rule-based systems. pendekatan yang digunakan dalam rule-based systems ada 2, yaitu pendekatan pencegahan (*preemptory*) dan pendekatan reaksi (*reactionary*). Perbedaannya hanya masalah waktu saja. Pada pendekatan pencegahan, program pendeteksi penyusupan akan memperhatikan semua lalu lintas jaringan. Jika ditemukan paket yang mencurigakan maka program akan melakukan tindakan yang perlu. Pada pendekatan reaksi, program pendeteksi penyusupan, hanya mengamati file log. Jika ditemukan paket yang mencurigakan program juga akan melakukan tindakan yang perlu.

Ada dua jenis IDS, yakni: (sherif,2002)

1. Network-based Intrusion Detection System (NIDS):

Network intrusion detection systems adalah jenis IDS yang bertanggung jawab untuk mendeteksi serangan yang berkaitan dengan jaringan NIDS umumnya terletak di dalam segmen jaringan penting di mana server berada atau terdapat pada "pintu masuk" jaringan. (Bueno 2002) Kelemahan NIDS adalah bahwa NIDS agak rumit diimplementasikan dalam sebuah jaringan yang menggunakan switch Ethernet, meskipun beberapa vendor switch Ethernet sekarang telah menerapkan fungsi IDS di dalam switch buatannya untuk memonitor port atau koneksi.

2. Host-based Intrusion Detection System (HIDS):

Aktivitas sebuah host jaringan individual akan dipantau apakah terjadi sebuah percobaan serangan atau penyusupan ke dalamnya atau tidak. HIDS seringnya diletakkan pada server-server kritis di jaringan, seperti halnya firewall, web server, atau server yang terkoneksi ke Internet.

Dilihat dari cara kerja dalam menganalisa apakah paket data dianggap sebagai penyusupan atau bukan maka, IDS dibagi menjadi dua: (Arvidson, 2003)

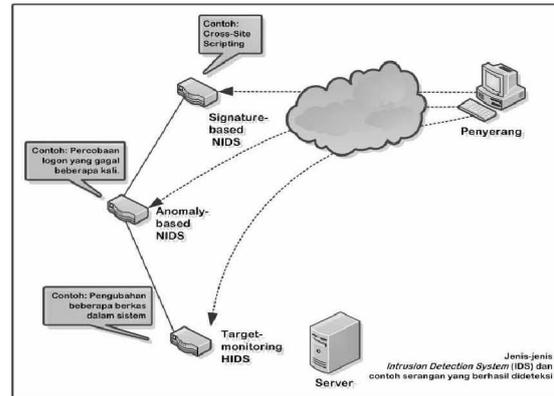
1. Knowledgebased atau misuse detection

Knowledge-based IDS dapat mengenali adanya penyusupan dengan cara menyadap paket data kemudian membandingkannya dengan database rule IDS (berisi *signature-signature* paket serangan). Jika paket data mempunyai pola yang sama dengan (setidaknya) salah satu pola di database rule IDS, maka paket tersebut dianggap sebagai serangan, dan demikian juga sebaliknya, jika paket data tersebut sama sekali tidak mempunyai pola yang sama dengan pola di database rule IDS, maka paket data tersebut dianggap bukan serangan.

2. Behavior based atau anomaly based.

Sedangkan *behavior based (anomaly)* dapat mendeteksi adanya penyusupan dengan mengamati adanya kejanggalan-kejanggalan pada sistem, atau adanya penyimpangan-penyimpangan dari kondisi normal, sebagai contoh ada penggunaan memori yang melonjak secara terus menerus atau ada koneksi parallel dari 1 buah IP dalam jumlah banyak dan dalam waktu yang bersamaan.

Kondisi-kondisi diatas dianggap kejanggalan yang kemudian oleh IDS jenis anomaly based dianggap sebagai serangan.



Gambar 2. Jenis-jenis *intrusion detection system* dan jenis serangan yang dapat di deteksi olehnya. (<http://id.wikipedia.org/wiki/Berkas:IDS.png>)

3. Local Area Network

Local Area Network biasa disingkat LAN adalah jaringan komputer yang jaringannya hanya mencakup wilayah kecil; seperti jaringan komputer kampus, gedung, kantor, dalam rumah, sekolah atau yang lebih kecil. Saat ini, kebanyakan LAN berbasis pada teknologi IEEE 802.3 Ethernet menggunakan perangkat switch, yang mempunyai kecepatan transfer data 10, 100, atau 1000 Mbit/s. Selain teknologi *Ethernet*, saat ini teknologi 802.11b (atau biasa disebut Wi-fi) juga sering digunakan untuk membentuk LAN. Tempat-tempat yang menyediakan koneksi LAN dengan teknologi Wi-fi biasa disebut hotspot.

Pada sebuah LAN, setiap node atau komputer mempunyai daya komputasi sendiri, berbeda dengan konsep dump terminal. Setiap komputer juga dapat mengakses sumber daya yang ada di LAN sesuai dengan hak akses yang telah diatur. Sumber daya tersebut dapat berupa data atau perangkat seperti printer. Pada LAN, seorang pengguna juga dapat berkomunikasi dengan pengguna yang lain dengan menggunakan aplikasi yang sesuai.

Berbeda dengan Jaringan Area Luas atau *Wide Area Network (WAN)*, maka LAN mempunyai karakteristik sebagai berikut :

- a. Mempunyai pesat data yang lebih tinggi
- b. Meliputi wilayah geografi yang lebih sempit
- c. Tidak membutuhkan jalur telekomunikasi yang disewa dari operator telekomunikasi
- d. Biasanya salah satu komputer di antara jaringan komputer itu akan digunakan

menjadi server yang mengatur semua sistem di dalam jaringan tersebut. (wikipedia, 2009)

4. Metode Pemasangan IDS

Menurut (Sherif, 2002), Penempatan IDS/NIDS dapat mengambil bentuk sebagai berikut :

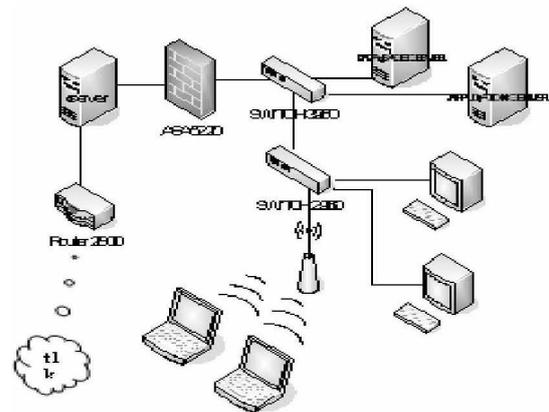
1. NIDS dapat ditempatkan pada host yang jika tidak terjaga, misalnya, windows 98, dan tidak mampu menciptakan log yang dapat diproses oleh sistem berbasis host.
2. IDS yang paling efektif pada perimeter jaringan, seperti di kedua sisi firewall, dekat dial-up server, dan di link ke jaringan *partner*.
3. NIDS dapat ditempatkan pada backbone WAN perusahaan di tempat yang dapat memonitor lalu lintas paket yang mencoba untuk memasuki jaringan.
4. Untuk server farms, Salah satu solusi mungkin untuk mengisolasi kekritisan server pada segmen jaringan mereka sendiri, dan mendedikasikan NIDS khusus untuk memantau segmen tersebut.

Dalam hal ini PT AJII memilih menempatkan NIDS pada jaringan *backbone* LAN/WAN perusahaan ditempat yang dapat memonitor lalu lintas paket yang berusaha memasuki jaringan.

Untuk mendeksi serangan yang terjadi maka sebuah sistem pengamanan IDS dengan menggunakan sebuah *software* Snort di install pada jaringan lokal Perusahaan sebagai sistem peringatan jika terdapat aktivitas – aktivitas ilegal yang terjadi dalam jaringan. IDS ini dipasang pada pada sistem Windows 2003 *Server* pada jaringan. Snort yang dapat diperoleh di <http://www.snort.org> biasanya di sebut sebagai *Network Intrusion Detection System* (NIDS). Snort sendiri adalah Open Source yang tersedia di berbagai variasi Unix (termasuk Linux) dan juga Microsoft Windows. Database yang digunakan adalah MySQL yang diinstall pada sistem berbasis *Windows* atau sistem operasi lain yang mendukung database MySQL. Alert IDS akan disimpan pada database mysql. Untuk administrasi dan *maintenance* sistem database dibuat suatu *interface* berbasis web yang dibuat dengan bahasa pemrograman PHP. Fungsi utama dari interface ini adalah untuk mengedit atau mengupdate entry database yang dijadikan input

bagi sistem yang lain. Dalam hal ini paket yang digunakan untuk file MYSQL dan PHP adalah XAMPP for *Windows*. Topologi yang digunakan adalah topologi *star* dengan kelas IP *local* adalah kelas B dan ISP menggunakan Telkom. Sebuah Router 2800 dipasang sebagai *gateway* dan kemudian sebuah server lalu setelah itu dipasang sebuah *hardware firewall* seri ASA-5220 untuk lebih menjaga keamanan data kedalam jaringan.

Gambar Jaringan

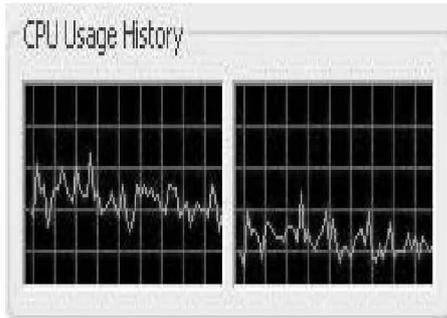


Gambar 3. Gambar Local Area Network pada Asuransi Jiwa Inhealth Jakarta

Dari gambar diatas IDS akan ditempatkan pada jaringan Perusahaan untuk megamati aktivitas para pengguna. *User* yang menggunakan akses jaringan pada PT. AJII ini kurang lebih adalah 45 *user*. Semua paket dari atau menuju klien akan melalui *Server*, sehingga untuk dapat mengamati lalu lintas paket tersebut sistem IDS ditempatkan dalam *Server* pada Router 2600. Semua paket yang masuk maupun keluar jaringan melalui *Server* akan dicerminkan ke IDS untuk kemudian dianalisis.

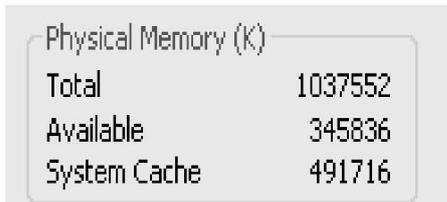
5. Hasil dan Pembahasan

Hasil pengamatan dari implementasi selama 6 hari, dapat dikatakan bahwa sistem IDS yang di bangun mampu memonitor secara terus menerus lalu lintas data pada jaringan PT AJII dan dapat mendeteksi paket paket serangan sesuai dengan aturan aturan yang sedang aktif, kemudian memberikan peringatan kepada pengatur jaringan melalui email. Secara teknis sistem IDS ini berjalan dengan persentase penggunaan *processor* antara 50% sampai dengan 70% dilihat dari grafik pemakaian CPU melalui *windows task manager*, seperti yang ditampilkan pada Gambar 4.



Gambar 4. CPU Usage History

Pemakaian RAM pada sistem ini masih menyisakan cukup banyak memori seperti yang ditunjukkan pada gambar 5.



Gambar 5. RAM Usage

Pengamatan dilakukan pula terhadap terhadap beberapa direktori yang berisikan berkas pencatatan total paket, jalur, kejadian dan system penyimpanan data MySQL untuk mengetahui rata rata pemakaian ruang pada harddisk tiap harinya agar pengatur jaringan dapat mengetahui seberapa besar harddisk yang diperlukan untuk menampung data selama beberapa waktu kedepan.

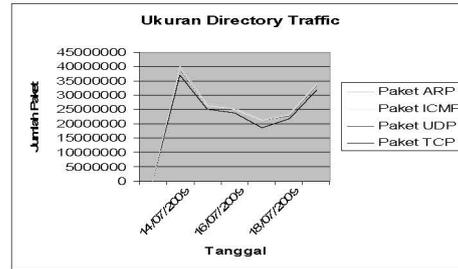
1. Directory Traffic dan Total Paket

Berikut pencatatan total paket perhari dan penambahan ukuran pada direktori Snort/traffic (sebagai direktori pencatatan berkas total paket) seperti yang ditampilkan pada Tabel-1.

Tabel 1. Ukuran Directory Traffic dan Total Paket

Tanggal	Paket				Total Paket	Ukuran Folder Traffic (bytes)	Pertambahan (bytes)
	TCP	UDP	ICMP	ARP			
13/07/2009	47.493.900	2.815.582	332.691	1.147.114	51.789.288	5.179	5.179
14/07/2009	32.116.683	1.767.883	170.200	803.244	34.858.210	8.885	3.486
15/07/2009	30.586.982	1.536.660	140.082	575.761	32.839.485	11.949	3.284
16/07/2009	24.033.743	3.204.595	90.681	587.218	27.916.237	14.740	2.792
17/07/2009	27.915.202	1.491.219	87.906	747.253	30.241.580	17.764	3.024
18/07/2009	40.865.984	2.119.413	155.983	806.185	43.967.565	22.161	4.397
					Rata rata		3.694

5. Grafik Ukuran Direktori Trafik



Dari tabel dan gambar tersebut maka dapat di simpulkan bahwa penambahan ukuran pada direktori trafik yang dicatat oleh IDS pada jaringan Lokal PT. AJII ini cukup konstan yakni antara 2792 – 5179 bytes (2-5KB) tiap harinya, dan perbandingan antara penambahan TCP, UDP, ICMP dan ARP hampir sama setiap harinya.

2. Directory Port

Pengamatan kemudian dilakukan kepada direktori port yang merupakan direktori pencatatan berkas jalur setiap paket, seperti yang ditampilkan pada tabel 2 berikut ini :

Tabel 2. Directory Port

Tanggal	Ukuran Folder (Bytes)		Ukuran Folder Port (TCP/UDP) (bytes)	Pertambahan (bytes)
	TCP	UDP		
13/07/2009	99.845.682	41.334.056	141.179.738	141.179.738
14/07/2009	167.364.503	67.287.401	234.651.903	93.472.165
15/07/2009	231.667.037	89.846.286	321.513.323	86.861.420
16/07/2009	282.192.798	136.891.241	419.084.038	97.570.715
17/07/2009	340.878.492	158.783.031	499.661.523	80.577.485
18/07/2009	426.832.457	189.896.997	616.729.454	117.067.931
			Rata rata	102.788.242

Melihat tabel tersebut maka dapat disimpulkan bahwa rata-rata pertambahan ukuran pada direktori port tiap harinya sekitar 102. 788. 242 bytes (± 103 MB).

3. Directory Log

Setelah melakukan pengamatan pada direktori port, maka pengamatan dilakukan pada direktori log sebagai direktori pencatatan berkas kejadian.

Tabel 3. Pertambahan ukuran Direktori Log

Tanggal	Total Event	Ukuran Folder Log (TCP/UDP) (bytes)	Pertambahan bahan (bytes)
13/07/2009	625	835.422	835.422
14/07/2009	2.010	3.522.181	2.686.758
15/07/2009	1.155	5.065.821	1.543.640
16/07/2009	1.774	7.438.006	2.372.185
17/07/2009	2.098	10.243.374	2.805.368
18/07/2009	697	11.175.058	931.684
		Rata rata	1.862.510

Dari tabel 3 dapat disimpulkan bahwa rata rata pertambahan ukuran pada direktori Log tiap harinya adalah sekitar 1. 862. 510 bytes (\pm 1, 9 MB)

4. Direktori XAMPP

Setelah mengamati ukuran direktori Log selanjutnya pengamatan tertuju pada besar direktori XAMPP yang merupakan direktori sistem penyimpanan data kejadian.

Tabel 4. Ukuran direktori XAMPP

Tanggal	Total Event	Total Ukuran Folder XAMPP (bytes)	Pertambahan bahan (bytes)
12/07/2009	0	360.592.710	0
13/07/2009	625	362.252.956	1.660.245
14/07/2009	2.010	367.592.503	5.339.547
15/07/2009	1.155	370.531.641	2.939.138
16/07/2009	1.774	375.374.361	4.842.720
17/07/2009	2.098	380.949.506	5.575.145
18/07/2009	697	382.801.055	1.851.549
		Rata rata	3.172.621

Dari tabel diatas dapat kita lihat bahwa rata rata pertambahan ukuran direktori XAMPP adalah 3. 172. 621 bytes atau setara dengan 3, 2 MB

Berdasarkan hasil pengamatan dan pencatatan semua tabel diatas maka didapat data keseluruhan sebagai berikut :

Tabel 5. Pertambahan nilai seluruh direktori

No	Direktori	Jumlah maksimal dalam Mega Byte
1	Traffic dan Total Paket	0,005 MB
2	Port	103 MB
3	Log	1,9 MB
4	XAMPP	3,2 MB
Total		108,105 MB

Berdasarkan pengamatan dan pencatatan semua tabel diatas, maka dapat diketahui bahwa rata rata ukuran hardisk yang akan terpakai setiap harinya sekitar 108,105 MB atau kita

anggap saja 109 MB. Dari rata rata ini, dapat ditarik kesimpulan bahwa dengan 109 MB perhari pemakaian kapasitas hardisk untuk mendeteksi pemakaian jaringan ini maka untuk satu tahun dibutuhkan kapasitas hardisk minimal 109 MB x 360 hari = 39240 MB atau 39,240 GB setahun hanya untuk mendeteksi rata rata pemakaian kapasitas hardisk terhadap aktifitas user yang menggunakan jaringan perusahaan secara normal.

Hasil pengamatan ini juga nantinya akan menjadi acuan *administrator* jaringan untuk terus menerus melakukan pemantauan agar tidak terjadi gangguan pada sistem akibat kekurangan ruang pada *hardisk*. Bila kehabisan ruang kosong pada *hardisk* ini terjadi maka akan mengakibatkan sistem menjadi *hang*.

Hasil ini juga akan menjadi acuan apabila suatu waktu nanti mungkin nilai nilai dari masing masing direktori meningkat secara signifikan yang berarti bahwa akan mengakibatkan ruang yang dibutuhkan untuk menyimpan data akan semakin besar, dan bila data tersebut terlalu besar dan melebihi kapasitas hardisk yang ada maka akan mengakibatkan sistem menjadi *down*.

Sistem IDS yang ditempatkan pada server dalam jaringan juga di fungsikan untuk memantau aktifitas para pengguna jaringan PT. AJII. Sistem ini akan melakukan penangkapan paket data dari para pengguna jaringan untuk kemudian dianalisa apakah paket tersebut memiliki kriteria berbahaya atau tidak. Bila terjadi serangan atau paket tersebut merupakan paket yang berbahaya maka sistem akan memberikan *alert* berupa log file sebagai berikut :

```
[**] [1:499:3] ICMP Large ICMP Packet [**]
[Classification:Potentially Bad Traffic] [Priority:
2] 05/09-20:15:14. 895348 10.1.4.113 ->
172.168.0.40 ICMP TTL:128 TOS:0x0 ID:6316
IpLen:20 DgmLen:65528 Type:8 Code:0 ID:512
Seq:3072 ECHO. Alert ini muncul ketika
seseorang mencoba mengirimkan sebuah paket
data yang besar dari luar sistem yang ber-IP
Address 10.1.4.113 ke dalam sistem yang ber-IP
Address 172.168.0.40 yang merupakan user dari
jaringan PT. AJII.
```

Dari hasil pengamatan ini juga dapat diketahui apakah sistem yang kita bangun telah disusupi oleh *hacker* atau tidak dengan cara membandingkan hasil pengamatan yang dilakukan secara normal selama enam hari dengan aktifitas hari hari selanjutnya, bila nanti terjadi kenaikan yang signifikan pada direktori

direktori yang diamati maka sudah dipastikan bahwa ada *hacker* yang mencoba menyusup kedalam sistem jaringan.

III. PENUTUP

3.1. Kesimpulan

Berdasarkan hasil evaluasi implementasi sistem IDS pada jaringan lokal PT. Asuransi Jiwa Inhealth Indonesia, maka dapat ditarik beberapa kesimpulan sebagai berikut :

1. Sistem IDS yang dibangun dapat mengamati lalu lintas paket data dengan memberikan informasi total paket tiap protokol pada jaringan lokal PT Asuransi Jiwa Inhealth Indonesia, dengan cepat dan akurat.
2. Sistem IDS yang dibangun mampu memberikan informasi total paket yang lewat melalui tiap jalur (TCP dan UDP), sehingga memudahkan pengatur jaringan untuk mengetahui jalur mana saja yang lalu lintas pakatnya terlalu tinggi dari keadaan normal dan yang berkemungkinan mengganggu kinerja keseluruhan sistem pada pada jaringan ataupun ancaman ancaman lain.
3. Sistem IDS yang dibangun dapat menangkap dan menampilkan informasi yang dianggap sebagai serangan atau berbahaya sesuai dengan aturan aturan yang sedang aktif
4. Sistem IDS yang dibangun dapat berjalan selama 24 jam penuh pada jaringan tanpa mengganggu kinerja sistem lain dan juga aktivitas para pengguna jaringan PT. Asuransi Jiwa Inhealth Indonesia karena sistem IDS ini hanya mengambil paket bayangan yang dikirim maupun diterima oleh para pengguna jaringan untuk kemudian dianalisis
5. Sistem IDS yang dibangun memberikan fasilitas laporan, *export*, dan *archive* yang dapat digunakan sebagai dokumentasi dari informasi kejadian yang terjadi pada jaringan dalam kurun waktu tertentu.
6. Sistem IDS yang dibangun memungkinkan pengatur jaringan untuk menentukan kriteria aturan baru yang ingin dibuat sesuai dengan kebutuhannya, serta dapat dengan mudah mengaktifkan, menonaktifkan serta menghapus aturan aturan dari sistem

penyimpanan data.

7. Dengan user sebanyak 45 user maka kapasitas yang dibutuhkan untuk menyimpan direktori direktori IDS sebesar 40 GB pertahun

3.2. Saran

1. IDS merupakan sistem pendeteksi gangguan pada jaringan. Untuk kedepan, sebaiknya sistem ini dikembangkan menjadi model **Intrusion Prevention System (IPS)** yang bukan hanya mendeteksi tetapi juga dapat melakukan pencegahan terhadap paket paket berbahaya yang mencoba masuk untuk merusak dan mengganggu kinerja sistem pada jaringan.
2. Sistem IDS dapat dikembangkan menjadi sistem yang tidak hanya mencatat total paket yang melewati jaringan dan mencatat pula total paket ditiap jalur namun dapat juga mencatat rincian setiap paket yang melalui jaringan untuk kemudian dianalisis lebih lanjut, dengan catatan memperhitungkan penggunaan memori pada *processor* maupun RAM serta kapasitas *harddisk* untuk sistem penyimpanan data secara otomatis.
3. Serangan dapat terdeteksi atau tidak tergantung pola serangan tersebut ada di dalam rule IDS atau tidak. Oleh karena itu, pengelola IDS harus secara rutin mengupdate rule terbaru.
4. Pemberitahuan *Alert* yang terjadi pada sistem disini hanya tampil pada monitor namun kedepan sistem *alert* dapat dikembangkan melalui pemberitahuan lewat *e-mail* maupun SMS.
5. Untuk pengembangannya, sistem IDS ini sebaiknya dilengkapi dengan metode deteksi lebih lanjut dimana sistem dapat mengenali pola serangan baru tanpa harus membandingkannya dengan pola aturan yang sudah tercatat.

DAFTAR PUSTAKA

- Ajawaila, Thomas Gregory. 2003. Tutorial Membangun Snort Sebagai Intrusion Detection System Integrasi terhadap BASE dan MySQL. [<http://ilmukomputer.org/2007/02/28/mem>]

- bangun-snort-sebagai-intrusion-detection-system*] (diakses tanggal 24 mei 2009).
- Ardiyanto, Yudhi. 2008. Membangun Sistem Intrusion Detection System Yang Open Source Pada Sistem Operasi Windows. Thesis, Universitas Muhammadiyah Yogyakarta.
- Ariyus, Dony. 2007. Intrusion Detection System Sistem Pendeteksi Penyusupan Pada Jaringan Komputer. Andi: Yogyakarta.
- Bueno, Pedro Paulo. 2002. Understanding IDS for Linux. [<http://www.linuxjournal.com/article/5616>] (diakses tanggal 20 Juli 2009)
- Chandra, Cristian A. 2009. Hackers and Their Threats: Incident Response and Protection Strategic for your company . dalam Seminar Security Attacks di Universitas Kristen Maranatha Bandung 17 Maret 2009, Diselenggarakan oleh Fakultas Teknologi Informasi, 5-10, Bandung, Fakultas Teknologi Informasi.
- Hartono, Puji. 2006. Sistem Pencegahan Penyusupan pada Jaringan berbasis Snort IDS dan IPTables Firewall. [http://www.cert.or.id/~budi/courses/security/2006/puji_report.pdf] (diakses tanggal 16 April 2009).
- Laing, Brian. 2000. Internet Security System. How To Guide Implementing a Network Based Intrusion Detection System. United Kingdom: Sovereign House 57/59 Vaster Road Reading RG18BT.
- Liu, Alex X., Mohamed G. Gouda. 2004. Diverse firewall design. In Proc. of the International Conference on Dependable Systems and Networks (DSN'04), pages : 595-604. [<http://www.cse.msu.edu/~alexliu/publications/Diver>] (diakses tanggal 26 mei 2009).
- Muammar, Ahmad. 2004. FireWall. Kuliah Umum Ilmu Komputer. [<http://ikc.depso.s.go.id/umum/ammam-firewall.php>] (diakses tanggal 01 Juni 2009).
- Northcutt, Stephen. 2004. E-mail Scums.dalam IT Ethic Hand Book, right and wrong for IT Professionals. ed. Stephen Northcutt. 125-143. Rokland : Syngress Publishing, Inc.
- Sherif, Joseph S., Tommy G. Dearmond. 2002. Intrusion Detection: Systems and Models. in proc. of the Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02), pages : 1-19. [<http://trs-new.jpl.nasa.gov/dspace/bitstream/2014/>] (diakses tanggal 01 Juni 2009).
- Wikipedia.org. 2009. White hat hacker. [http://id.wikipedia.org/wiki/White_hat_hacker] (diakses tanggal 23 Mei 2009).
- Wikipedia.org. 2007. Sistem Deteksi Intrusi. [http://id.wikipedia.org/wiki/Sistem_deteksi_intrusi] (diakses tanggal 07 Juli 2009).
- Wikipedia.org. 2008. Black hat hacker. [http://id.wikipedia.org/wiki/Black_hat_hacker] (diakses tanggal 23 mei 2009).
- Wikipedia.org. 2008. Local Area Network. [http://id.wikipedia.org/wiki/Local_Area_Network] (diakses tanggal 22 agustus 2009).