ANALISA MONITORING LALU LINTAS PAKET DATA PADA JARINGAN LOKAL

Yopi Handrianto [1] dan Hendra Supendar [2]

[1]AMIK BSI
Jl. Dewi Sartika No 77 Cawang Jakarta Timur
yopi.handrianto@yahoo.com
[2]AMIK BSI
Jl. Kramat Raya No 18 Jakarta Pusat
hendrasupendar@gmail.com

ABSTRACT

The attack on internet systems increasingly rampant, almost all of the information in the system, it is not an easy job to monitor the hundreds of IP in and out of clients. 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 can help users monitor and analyze problems in network security. The expected result is to know how much inconvenience caused to the system through a corporate network traffic. Testing of IDS performed on a local network of PT. Anta Citra Arges for three 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 17 use,r disk capacity to be provided for one year is 15,5GB.

1. PENDAHULUAN

Serangan dan pencurian data yang dilakukan oleh seorang hacker untuk mengganggu sistem komputer memang sudah sangat meresahkan. Banyak cara dilakukan untuk menanggulangi serangan dari *hacker* ini, mulai dari diskusi 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 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 (*Intrusion Detection System*), maka bisa diduga 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 perusahaaan 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

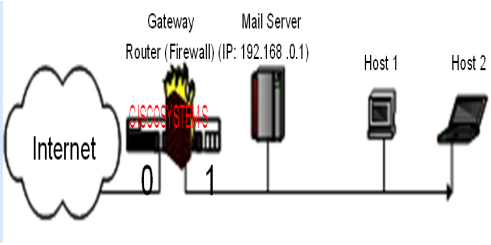
pada profil perusahaan dari sistem operasi dan perangkat keras jaringan. Kerentanan juga muncul di peralatan keamanan , seperti *firewall* dan bahkan peralatan IDS.

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 menarget kan seluruh rentang alamat IP dan bahkan mengirimkan umpan scan untuk membuatnya lebih sulit untuk target dalam mengidentifikasi sumber scanner yang sebenarnya.

2. TINJAUAN PUSTAKA

2.1 *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 atau kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. 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 memblok/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.

2.2. *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:

***White Hats* :** merupakan *hacker* yang bekerja sebagai *system analist*,*system administrator* maupun *security analist*. *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).

a. ***Gray Hats* :** merupakan *hacker* yang bekerja *offensivelly* dan *defensivelly*. *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).
b. ***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*), dan sebagainya (Wikipedia, 2008).

c. ***Suicide Hacker* :** *Hacker* yang bekerja persis seperti *Black Hats Hacker*, bersifat destruktif dan tidak peduli terhadap ancaman yang akan menimpa nya. 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* di atas 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 (*Instrusion Detection System*) dan kemampuan untuk mencegah akses dikenal dengan *Firewall.*

2.3 *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-*block* gangguan jika segera dideteksi, bertindak sebagai *deterrent* (mencegah seseorang melakukan gangguan/*intrusion*), mengumpulkan informasi untuk meningkatkan keamanan.

1.Tipe dasar IDS

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 lintaas 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.

3. Ada dua jenis IDS

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

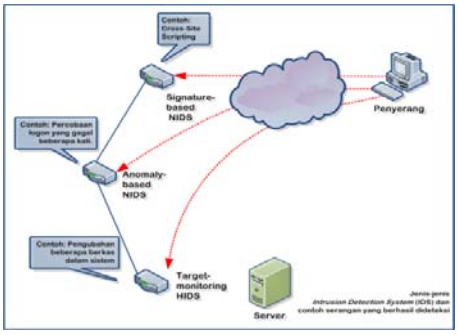
atau bukan maka, IDS dibagi menjadi dua (Arvidson, 2003) :

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.

3. *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 di atas 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
Sumber : (*http://id.Wikipedia.org/wiki/Berkas:IDS.png*)

2.4 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).

1. Paket-Paket Data *Local Area Network*

Internet protocol (IP), *User Datagram Protokol* (UDP), dan *Transmission Control Protocol* (TCP) merupakan dasar komunikasi berbasis jaringan (Sukarman, 2008).

1. TCP/IP

Protokol-protokol TCP/IP memberikan dukungan jaringan untuk menghubungkan seluruh tempat dan *host* serta mengikuti aturan standar tentang bagaimana komputer-komputer berkomunikasi dan bagaimana jaringan-jaringan diinterkoneksikan.

Protokol-protokol TCP/IP mengikuti model konsep empat *layer* yang dikenal sebagai model Department of Defense (DOD): *Application, Transport, Internet*, dan *Network Interface*.

TCP menyajikan komunikasi berorientasi koneksi yang dapat diandalkan untuk aplikasi-aplikasi yang secara khusus mentransfer sejumlah besar data pada suatu waktu. TCP juga dipakai untuk aplikasi-aplikasi yang memerlukan pengakuan bagi data yang diterima.

2. UDP

UDP menyediakan komunikasi tanpa koneksi dan tidak menjamin mampu mengirimkan paket.

Aplikasi-aplikasi yang memakai UDP secara khusus mentransfer sejumlah kecil data pada suatu waktu.

Pengiriman data yang dapat diandalkan merupakan tanggung jawab aplikasi. Layer Transport pada model DOD kira-kira sesuai dengan Layer Transport pada model OSI.

3. ICMP (*Internet Control Message Protocol*)

ICMP biasanya digunakan untuk melakukan pemeriksaan koneksi antar dua komputer dengan mengirim pesan ke komputer tersebut dan menunggu balasan dari komputer tersebut. Pesan yang dikirim disebut *echo* dan balasannya disebut *echo-reply*. Contoh dari penggunaan protokol ICMP ini adalah aplikasi *ping* (S'to, 2004).

4. ARP (*Address Resolution Protocol*)

ARP adalah sebuah protocol dalam TCP/IP *protocol suite* yang bertanggung jawab dalam melakukan resolusi alamat IP ke dalam alamat *Media Access Control* (*MAC Address*). Protokol ARP digunakan sebagai protokol untuk melakukan pencarian *host* tujuan, protokol ini juga merupakan jantung utama dari cara kerja IEEE 802.3.

Cara kerja dapat dijelasakan secara singkat:

1. Keadaan awal *host* pengirim belum memiliki informasi
2. *Host* pengirim mengirimkan pesan tersebar yang diterima keseluruhan *host* yang tersambung, menanyakan apakah ada yang merupakan tujuan
3. Jika ada, *host* tujuan akan menjawab dan memabalas pesan ke pengirim dengan memberikan informasi alamat
4. Tabel di sisi penerima dibentuk
5. Pesan diterima oleh pengirim, tabel informasi alamat dibentuk di sisi pengirim.
6. Pengiriman data dilakukan
7. Tabel tidak selamanya valid. Dalam suatu periodik, langkah 1sampai 6 akan berulang lagi.

Cara kerja protokol ARP menjadi lubang keamanan dari IPV4 dan sasaran eksploitasi yang mudah. Dari penjelasan kerja protokol ARP, dapat diidentifikasikan ada yang kurang dari protokol ini jika ditinjau dari ilmu kriptografi, yaitu authentifikasi, tidak ada sama sekali pendistribusian kunci privat publik, bahkan yang sederhana seperti mekanisme kunci seperti diffie-Helman.

Hal ini merupakan lubang keamanan terbesar dari protokol *Ethernet* yang tidak berevolusi, bahkan setelah jaringan menjadi daerah yang tidak aman. Protokol ini terlanjur menjadi urat nadi internet dan belum dapat digantikan secara menyeluruh (Bruschi, 2003).

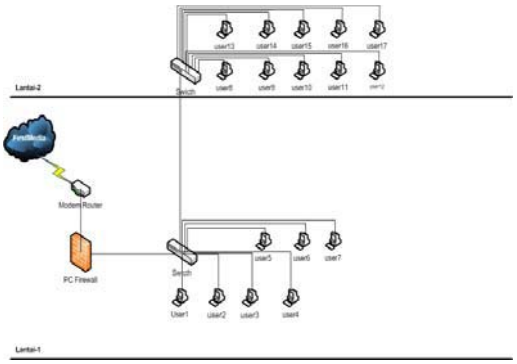
3. HASIL PENELITIAN

Metode penelitian yang digunakan di sini adalah dengan memanfaatkan ketujuh belas *user* pada perusahaan untuk melakukan trafik pada jaringan yang ada delapan jam per hari selama tiga hari berturut-turut dan diamati penggunaan CPU dan memori selama waktu tersebut. Lalu, pada hari ke-3 diperiksa ukuran direktori-direktori yang berpotensi terganggu akibat serangan. Direkori yang diamati dan dicatat adalah direktori trafik, direktori *port*, direktori *log*, direktori *xampp*, dan pertambahan nilai seluruh direktori. Kemudian, hasil ini akan dijadikan sebagai acuan administrator untuk mengetahui apakah ada serangan ke dalam sistem atau tidak dengan membandingkan keadaan normal sistem yang telah dicatat (t_0) dengan keadaan sistem setelah pencatatan (t_1). Bila hasil $t_0 \geq t_1$, maka dipastikan sistem aman. Namun, bila $t_0 < t_1$, maka sistem tersebut kemungkinan ada gangguan.

Penelitian yang dilakukan juga akan digunakan sebagai perkiraan berapa banyak kapasitas *hardisk* yang harus disediakan untuk menampung data direktori dalam satu tahun dan dapat diprediksi juga pemakaian kapasitas tersebut bila *user* bertambah.

Selain dari hal tersebut di atas, untuk membuktikan keandalan sistem dari serangan *bad traffic,* maka sistem juga diuji dengan melakukan pengiriman paket data yang besar dari luar sistem yang akan mengakibatkan sistem mengeluarkan sistem *alert*.

1. Analisa Jaringan PT Anta Citra Argess.



Gambar 3. Gambar Local Area Network pada PT Anta Citra Argess Jakarta.

Jaringan pada PT Anta Citra Argess Jakarta mengadopsi *design* jaringan bertopologi *star* dengan 17 *user* (klien) dan 1 PC *firewall*. IP *local* yang digunakan adalah kelas B dan ISP menggunakan First Media. Sebuah Modem Router dipasang sebagai *server gateaway* dan kemudian dipasang sebuah PC *server firewall*

untuk lebih menjaga keamanan data ke dalam jaringan. Pada Router juga di-*set* sebagai *access point* yang digunakan bagi user yang menggunakan laptop dengan metode *secure system*.

2. Metode Pemasangan IDS

Menurut Sherif (2002), penempatan IDS/NIDS (Network IDS) 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 Anta Citra Argess 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 disebut 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 di-*install* 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 meng-*update entry database* yang dijadikan input bagi sistem yang lain. Dalam hal ini, paket yang digunakan untuk file MySQL dan PHP adalah XAMPP for *Windows.*

Dari Gambar 3 di atas, IDS akan ditempatkan pada jaringan perusahaan untuk megamati aktivitas para pengguna. *User* yang menggunakan akses jaringan pada PT. Anta Citra Argess ini kurang lebih adalah 17 *user*. Semua paket dari atau menuju klien akan melalui PC Server *Firewall* , sehingga untuk dapat mengamati lalu lintas paket tersebut sistem IDS ditempatkan dalam PC *Server firewall*. Semua paket yang masuk maupun keluar jaringan melalui jaringan akan dicerminkan ke IDS untuk kemudian dianalisis.

3. Analisa dan Implementasi

Pengamatan dilakukan terhadap beberapa direktori yang berisikan berkas pencatatan total paket, jalur, kejadian dan sistem penyimpanan data MySQL untuk mengetahui rata-rata pemakaian ruang pada *hardisk* tiap harinya agar pengatur jaringan dapat mengetahui seberapa besar *hardisk* yang diperlukan untuk menampung data selama beberapa waktu ke depan.

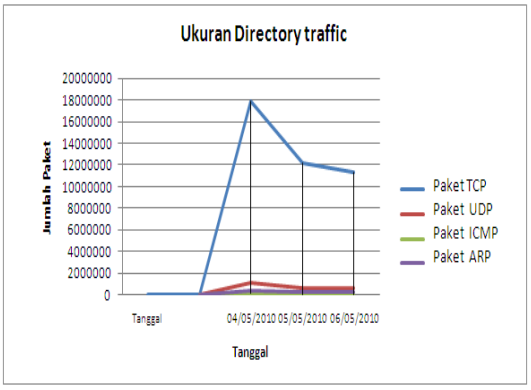
Direktori-direktori yang diamati tersebut adalah :

1. *Directory Traffic* dan Total Paket

Berikut pencatatan total paket per hari dan pertambahan 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

						Ukuran	
						Folder	Pertam
Tanggal	Paket				Total	Traffic	bahan
	TCP	UDP	ICMP	ARP	Paket	(bytes)	(bytes)
04/05/2010	17.942.140	1.063.665	125.683	433.354	19.564.842	1.957	1.957
05/05/2010	12.133.045	667.867	64.298	303.448	13.168.658	3.274	1.317
06/05/2010	11.377.489	580.516	52.920	217.510	12.228.435	4.497	1.223
					Rata rata		1.499



Gambar 4. Grafik Ukuran Direktori Trafik tanggal 04-06 Mei 2010

Dari tabel dan gambar tersebut, dapat disimpulkan bahwa pertambahan ukuran pada

direktori trafik yang dicatat oleh IDS pada jaringan Lokal PT Anta Citra Arges ini cukup konstan, yakni antara 1223–1957 *bytes* (1-2 KB) tiap harinya, dan perbandingan antara pertambahan 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. Ukuran Direktori *Port* (TCP/UDP)

Tanggal	Ukuran Folder (Bytes)		Ukuran Folder Port TCP/UDP	Pertambahan Bytes
	TCP	UDP	(Bytes)	
04/05/2010	37.719.480	15.615.088	53.334.568	53.334.568
05/05/2010	63.226.590	25.419.685	88.646.275	35.311.707
06/05/2010	87.518.658	33.941.930	121.460.588	32.814.313
			Rata-rata	40.486.863

Melihat tabel tersebut, maka dapat disimpulkan bahwa rata-rata pertambahan ukuran pada direktori *port* tiap harinya sekitar 40.486.863 *bytes* (± 41MB).

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 Even	Ukuran Folder Log (TCP/UDP) (Bytes)	Pertambahan (Bytes)
04/05/2010	236	315.604	315.604
05/05/2010	759	1.330.602	1.014.998
06/05/2010	436	1.913.755	583.153
		Rata-rata	637.918

Dari tabel 3, dapat disimpulkan bahwa rata-rata pertambahan ukuran pada direktori *Log* tiap harinya adalah sekitar 637.918 *bytes* (± 0, 6 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

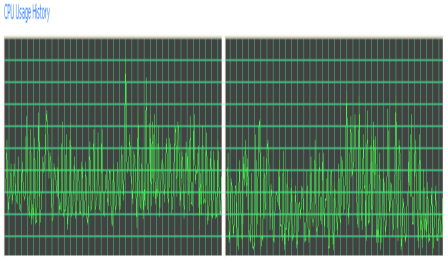
Tanggal	Total Even	Total Ukuran Folder XAMPP (Bytes)	Pertambahan (Bytes)
04/05/2010	0	360.592.710	0
05/05/2010	236	361.219.914	627.204
06/05/2010	759	363.237.076	2.017.162
		Rata-rata	881.455

Dari tabel diatas, dapat kita lihat bahwa rata-rata pertambahan ukuran direktori XAMPP adalah 881.455 *bytes* atau setara dengan 0,9 MB.

5. Hasil Analisa

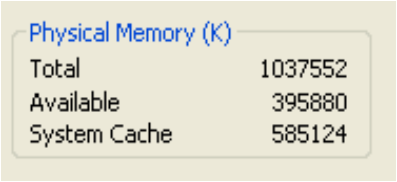
Hasil pengamatan dari implementasi selama 3 hari, dapat dikatakan bahwa sistem IDS yang dibangun mampu memonitor secara terus-menerus lalu lintas data pada jaringan PT Anta Citra Arges dan dapat mendeteksi paket-paket serangan sesuai dengan aturan-aturan yang sedang aktif, kemudian memberikan peringatan kepada pengatur jaringan melalui *e-mail*.

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 5.



Gambar 5. CPU *Usage History*, tanggal 06 Mei 2010

Pemakaian RAM pada sistem ini masih menyisakan cukup banyak memori seperti yang ditunjukkan pada Gambar 6.



Gambar 5. RAM *Usage,* tanggal 06 Mei 2010

Berdasarkan hasil pengamatan dan pencatatan semua tabel di atas, maka didapat data keseluruhan sebagai berikut :

Tabel 5. Pertambahan nilai seluruh direktori

No	Directory	Jumlah Maksimal Dalam Mega Byte
1	Traffic dan Total Paket	0,002
2	Port	41,000
3	Log	0,600
4	XAMPP	0,900
	Total	42,502

Berdasarkan pengamatan dan pencatatan semua tabel di atas, maka dapat diketahui bahwa rata-rata ukuran *hardisk* yang akan terpakai setiap harinya sekitar 42,5 MB atau kira-kira 43 MB. Dari rata-rata ini, dapat ditarik kesimpulan bahwa dengan 43 MB per hari pemakaian kapasitas *hardisk* untuk mendeteksi pemakaian jaringan ini, maka untuk satu tahun dibutuhkan kapasitas *hardisk* minimal 43 MB x 360 hari = 15.480 MB atau 15,5 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 difungsikan untuk memantau aktifitas para pengguna jaringan PT Anta Citra Arges. 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:0×0 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 Anta Citra Arges.

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 tiga 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 ke dalam sistem jaringan.

4.KESIMPULAN

Berdasarkan hasil evaluasi implementasi sistem IDS pada jaringan lokal PT Anta Citra Arges, 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 Anta Citra Arges 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-jalur mana saja yang lalu lintas paketnya 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 Anta Citra Arges 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 17 *user,* maka kapasitas yang dibutuhkan untuk menyimpan direktori direktori IDS sebesar 15,5 GB per tahun.

DAFTAR PUSTAKA

jawaila, Thomas Gregory. 2003. *Tutorial Membangun Snort Sebagai Intrusion Detection System Integrasi terhadap BASE dan MySQL*. [*http://ilmukomputer.org/2007/02/28/membangun-snort-sebagai-intrusion-detection-system*] (Accessed 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.

Bruschi, D, A. Ornaghi, E. Rosti. 2003. *S-ARP: A Secure Address Resolution Protocol.* [http://www.acsac.org/2003/papers/111.pdf] (Accessed 1 Juli 2010).

Bueno, Pedro Paulo. 2002. *Understanding IDS for Linux.* [http://www.linuxjournal.com/article/5616] (Accessed 20 Juli 2009).

Chandra, Cristian A. 2009. *Hackers and Their Threats: Insident 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] (Accessed 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] (Accessed 26 Mei 2009).

Muammar, Ahmad. 2004. *FireWall*. *Kuliah Umum Ilmu Komputer*. [http://ikc.depsos.go.id/umum/ammar-firewall.php] (Accessed 1 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/] (Accessed 1 Juni 2009).

S'to. 2004. *Seni Teknik Hacking I.* Jakarta: Jasakom Publisihing.

Sukarman.2008. *Akusisi Data Lewat Protocol Tcp/Ip Berbasis Labview*. Dalam Seminar Nasional IV SDM Teknologi Nuklir Yogyakarta, 25-26 Agustus 2008.