BAB II

TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Darapareddy dan Gummadi (2012) melakukan penelitian yang menggunakan *intrusion detection system* (IDS) sebagai dasar menjelaskan deteksi intrusi adalah proses *monitoring* komputer atau jaringan untuk aktivitas atau kegiatan yang tidak sah. IDS (*Intrusion Detection System*) juga dapat digunakan untuk memonitor lalu lintas jaringan sehingga dapat mendeteksi jika sistem sedang ditargetkan oleh serangan jaringan. Pada penelitian Faizal dkk (2009) dengan judul *Threshold Verification Technique for Network Intrusion Detection System* menerangkan bahwa terdapat dua tipe dasar deteksi intrusi : berbasis *host* (Host Intrusion Detection System) dan berbasis jaringan (Network Intrusion Detection System). Masing-masing memiliki pendekatan yang berbeda untuk memonitor dan mengamankan data. HIDS berbasis *host* memeriksa data yang diselenggarakan pada masing-masing komputer yang berfungsi sebagai tuan rumah, HIDS sangat efektif untuk mendeteksi pelanggaran *insider*. Contoh IDS berbasis *host* adalah keamanan Windows NT/2000 dengan penggunaan Log dan Syslog UNIX. Di sisi lain sistem deteksi intrusi berbasis jaringan (NIDS) menganalisis paket data yang melalui jaringan aktual. Paket diperiksa dan dibandingkan dengan data empiris untuk memverifikasi apakah mereka alam berbahaya atau jinak. Contoh dari NIDS adalah Snort, yang merupakan jaringan sistem deteksi intrusi *open source*

yang melakukan analisis lalu lintas *real-time.* Sistem Deteksi Intrusi (IDS) merupakan salah satu model sistem keamanan yang banyak diterapkam karena efektifitas dan efisiensi yang dimiliki (Rao and Nipur, 2012).

Terdapat banyak jenis teknik dan aplikasi yang bisa digunakan untuk menerapkan sistem deteksi intrusi, hal ini membuat deteksi intrusi lebih fleksibel untuk diterapkan sesuai kebutuhan (Vallinayagam and Sasikala, 2012). IDS bertugas melakukan pendeteksian anomali pada aliran data pada jaringan komputer, sebagai contoh anomali yang di deteksi IDS adalah akses ilegal, *flooding* data dan lain-lain. IDS memiliki kemampuan untuk menganalisis lalu lintas jaringan dan mengenali intrusi masuk dan keluar. Pada jaringan *real-time*, deteksi dini serangan dapat mencegah serangan lebih lanjut dan mengurangi akses tidak sah pada mesin yang ditargetkan (Koteswarao and Begum, 2012). Konfigurasi yang tepat, seleksi fitur dan ambang batas yang benar adalah keuntungan tambahan untuk IDS untuk mendeteksi anomali dalam jaringan. IDS menghasilkan sejumlah besar peringatan dan kebanyakan adalah *false positif* yang ditafsirkan sebagai perilaku untuk pola serangan parsial. Pemantauan dan mengidentifikasi ancaman beresiko merupakan perhatian utama untuk administrator keamanan (Victor, Rao and Venkaiah, 2010).

Informasi yang ditransmisikan pada jaringan adalah dalam bentuk “paket”, dengan kata lain informasi dibagi menjadi potongan-potongan kecil dari sumbernya, ditransmisikan dan kembali berkumpul pada penerima akhir (Raaj . and Kavitha M., 2013). *Firewall* memeriksa bagian yang relevan dari sebuah paket yang menjadikan paket data yang sesuai dengan konfigurasi yang akan

berhasil dikirim. Dalam kasus *firewall proxy*, lalu lintas tidak pernah mengalir langsung antara jaringan tetapi berdasarkan permintaan dan tanggapan *proxy repackages*. Tidak ada *host* internal dapat diakses secara langsung dari jaringan eksternal dan tidak ada host eksternal secara langsung dapat diakses oleh host internal. Pekerjaan utama dari *firewall* adalah *Packet Filtering*, yang mengontrol akses dengan memeriksa paket berdasarkan isi dari *header* paket (Lindqvist et al., 2010). Salah satu cara untuk menerapkan *firewall* adalah untuk memanfaatkan apa yang disebut *packet filtering. Packet filtering* telah terbukti menjadi alat yang berguna untuk menempatkan kontrol akses ke lalu lintas IP. *Packet filtering* yang dapat digunakan untuk memblokir paket data berdasarkan kriteria tertentu seperti protokol yang digunakan dan berbagai karakteristik protokol. Data sebagai sumber dan alamat tujuan, UDP dan TCP, port asal dan tujuan dapat digunakan dalam keputusan penyaringan. Metode ini juga banyak digunakan dalam sistem monitoring jaringan, dengan menerapkannya pengguna dapat memantau aktifitas pada jaringan setiap saat (Aluvala, 2011) (Al-Mukhtar, 2012).

Packet Capture merupakan metode yang digunakan untuk pengawasan lalu-lintas data pada jaringan komputer, *packet capture* sendiri adalah basis dari sistem penyaringan paket data ataupun klasifikasi paket data pada lalu-lintas data. Metode ini digunakan untuk melakukan monitoring trafik paket data yang juga banyak diterapkan pada berbagai macam sistem keamanan (Arai, 2012). Dalam pendekatan ini ketika paket ditransmisikan dari system umumnya menggunakan *tool* seperti Ethereal/Wireshark untuk mengendus paket dan menganalisis isinya agar dapat memeriksa akurasi data. Perangkat lunak open source (seperti

Ethereal/Wireshark) dikenal sebagai protokol analisa jaringan yang sangat berguna selama pengembangan proyek perangkat lunak pada dominan jaringan (Manchikanti, Prasanth and Murthy G., 2012), (Dhillon and Ansari, 2012), (Asrodia and Patel, 2012).

Paket data adalah entitas dasar dari semua sistem komunikasi, dengan demikian keamanan jaringan berarti keamanan dari paket data. Sebuah paket data adalah blok yang paling dasar komunikasi yang melibatkan aliran *streamline* terbatas untuk mengirimkan informasi dari satu perangkat ke perangkat lainnya. Sebuah paket data yang terkandung dalam segmen data yang menyimpan informasi lain seperti protokol yang digunakan, tujuan *hardware* alamat dan lain-lain. Singkatnya, identitas setiap paket yang datang dari sumber tidak bisa diandalkan dapat dideteksi dengan mempelajari isinya. Manajemen trafik data, pengukuran trafik jaringan komputer dan *sniffing* adalah beberapa produk dari *packet capture*, *packet capture* juga digunakan sebagai basis untuk berbagai macam sistem keamanan (Suri and Batra, 2012), (Aluvala, 2011).

Jaringan forensik pada dasarnya adalah sebuah pendekatan baru yang termasuk dalam keamanan informasi jaringan, hal ini dikarenan IDS dan *firewall* tidak dapat selalu menemukan dan menghentikan penyalahgunaan di seluruh jaringan. Metode ini yang disusulkan untuk menangkap dan menganalisa data yang dipertukarkan antara berbagai teknik *traceback* banyak IP, seperti menandai paket yang membantu penyelidik forensik untuk mengenali paket dari IP sumber *promicious*. Yang diusulkan pada forensik jaringan hanya fokus pada menangkap

lalu lintas jaringan, *spoofing* ARP, *spoofing* mac, *replay* serangan peringatan dan lalu lintas (Banerjee, Vashishtha and Saxena, 2010).

Firewall memberikan sejumlah keamanan tetapi dapat dikelabui setiap kali oleh serangan seperti *spoofing* IP, dengan begitu sistem cerdas yang dapat mendeteksi serangan dan intrusi diperlukan. GRANT (*Global Real-time Analisis of Network Traffic*) menjadi *Intrusion Detection System* berbasis Linux (LID), mengambil keuntungan dari keamanan Linux dan mengamankan node lain dalam perimeter jaringan. Hal ini mampu menanggapi serangan yang sukses, sehingga menyebabkan kerusakan minimal atau tidak ke seluruh jaringan. Untuk kinerja yang lebih baik Linux *Intrusion Detection System* harus menjadi bagian dari pertahanan dalam strategi mendalam seperti *Firewall* dan *Intrusion Prevention* (Anitha, 2011), (Jaisankar, Saravanan and Swamy, 2009).

Katankar and Thakare (2010) pada penelitiannya yang mengangkat tentang pemanfaatan SMS *Gateway* menjelaskan distribusi informasi yang baik menjadikan suatu sistem informasi menjadi lebih optimal dalam penerapannya. Terdapat berbagai macam kebutuhan distribusi informasi sesuai dengan keperluan yang variatif. Salah satu model distribusi informasi yang saat ini masih banyak digunakan adalah SMS Gateway, model ini memberikan efektifitas pada keperluan yang *real-time* dikarenakan pesan yang dapat didistribusikan kapan saja dan pengguna dapat menerima informasi secara langsung. SMS Gateway adalah sebuah perangkat atau layanan yang menawarkan SMS transit, mengubah pesan untuk lalulintas jaringan selular dari media lain atau sebaliknya, sehingga memungkinkan pengiriman atau penerimaan pesan SMS dengan atau tanpa

menggunakan ponsel. SMS Gateway adalah cara yang paling cepat dan handal untuk SMS *massal/bulk*. Sistem ini juga dikembangkan untuk meningkatkan keamanan pengguna.

Berikut adalah beberapa penelitian sejenis yang dituangkan dalam bentuk tabel perbandingan sebagai acuan dalam pengembangan penelitian. Tabel ini menjelaskan teknik atau metode, sensor, alarm dan sistem operasi yang digunakan dalam penelitian ini serta penelitian sebelumnya Data perbandingan penelitan dapat dilihat pada tabel 2.1.

Tabel 2.1 Perbandingan Penelitian Sejenis

	Lindqvist J., et all. (2010)	Anitha A., (2011)	Rao M., & Nipur, (2012)	Dhillon & Ansari U., (2012)	Gobel Mario A. A., (2014)
Metode/Teknik	Firewall	IDS	IDS	NTM	IDS
Sensor	Packet filter, Host identity protocol	GRANT Tool	Honeypot	Packet capture	Packet capture, Packet filter
Alarm	-	e-mail	-	-	SMS Gateway
Sistem Operasi	Firewall	Linux	Unix	Windows	Windows

2.2 Landasan Teori

2.2.1 Keamanan jaringan

Keamanan jaringan komputer didefinisikan sebagai tindakan untuk mencegah penyalahgunaan dan akses atau aktifitas illegal atas suatu informasi. Elemen dari keamanan jaringan itu sendiri terdiri dari 5 bagian yaitu kerahasiaan, integritas, autentikasi, ketersediaan (*avaliability*) dan tanpa penolakan (*non-repudiation*).

Ancaman dari keamanan jaringan itu dapat dibagi menjadi 4 jenis yaitu *interruption*, *interception*, *modification* dan *fabrication* (Stallings, 2006).

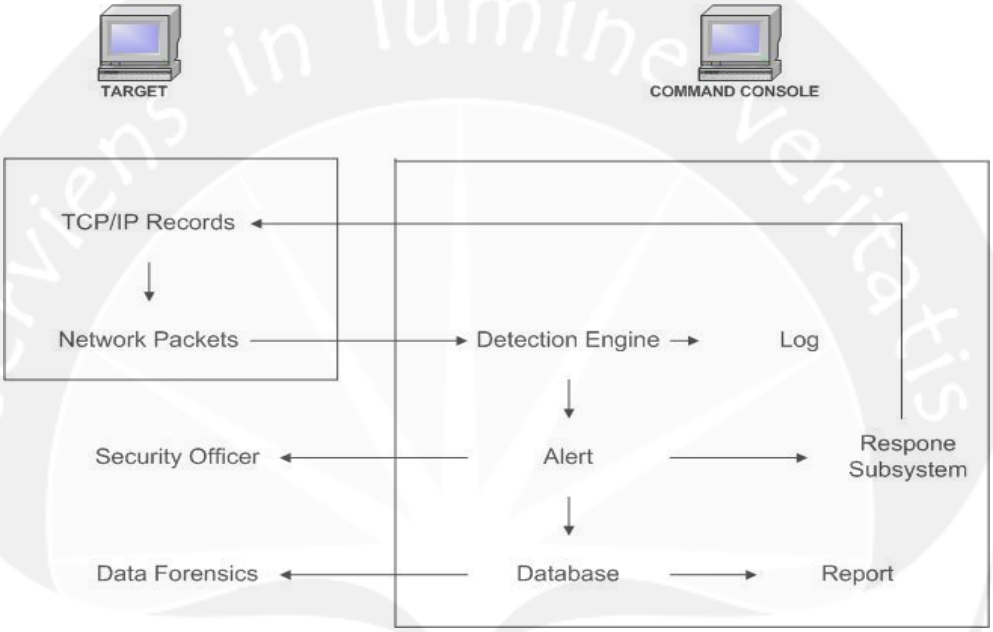
2.2.2 Sistem deteksi intrusi

Deteksi intrusi adalah teknik untuk mendeteksi akses tidak sah ke sistem komputer dan jaringan komputer. Sebuah intrusi ke dalam sistem adalah upaya oleh orang luar ke sistem untuk mendapatkan akses ilegal ke sistem. Pencegahan intrusi disisi lain adalah seni mencegah akses yang tidak sah sumber daya atau sistem. Dua proses yang terkait adalah deteksi intrusi pasif yaitu mendeteksi gangguan sistem dan pencegahan intrusi aktif yaitu menyaring lalu lintas jaringan untuk mencegah upaya penyusupan (Kizza, 2005).

Deteksi intrusi didasarkan pada asumsi bahwa perilaku penyusup berbeda dari pengguna yang sah dengan cara yang dapat diukur. Tentu saja, kita tidak bisa berharap bahwa akan ada perbedaan yang tepat antara serangan oleh penyusup dan pemakaian normal sumber daya oleh pengguna yang berwenang (Stallings, 2006).

Sistem deteksi intrusi (IDS) mengambil pendekatan berbasis jaringan dan juga *host* untuk mengenali atatupun membelokkan serangan. IDS yang mencari tanda serangan (pola tertentu) yang biasanya mengidentifikasi niat jahat atau mencurigakan. Ketika sebuah IDS memfilter pada pola-pola lalu lintas jaringan maka IDS berbasis jaringan (NIDS). Ketika sebuah IDS mencari tanda serangan dalam file log, maka itu adalah IDS berbasis host. Gambar 2.1 menunjukkan sensor berbasis arsitektur jaringan standar yang mendeteksi intrusi. Sebuah sensor digunakan untuk “mengendus” paket dari jaringan dimana mereka dimasukkan ke

mesin deteksi yang akan memicu alarm jika ada penyalahgunaan terdeteksi. Sensor ini diditribusikan ke berbagai *mission-critical* segmen jaringan. Sebuah pusat konsol digunakan untuk mengumpulkan alarm dari beberapa sensor (Anitha, 2011).



Gambar 2.1 Arsitektur jaringan IDS (Anitha, 2011).

1. Ketika komputer di jaringan berkomunikasi, paket jaringan dibuat.
2. Sistem deteksi intrusi digunakan untuk mendeteksi serangan dan intrusi, jika pola terdeteksi dan menghasilkan peringatan.
3. Peringatan keamanan diberitahu tentang penyalahgunaan.
4. Tanggapan terhadap intrusi yang dihasilkan berdasarkan pada respon yang telah ditentukan atau tanggapan dari petugas keamanan.
5. Peringatan tersebut disimpan untuk analisis kemudian.
6. Laporan yang dihasilkan terangkum.

7. Data forensik digunakan untuk mendeteksi tren jangka panjang.

2.2.3 Paket *capture* dan paket filter

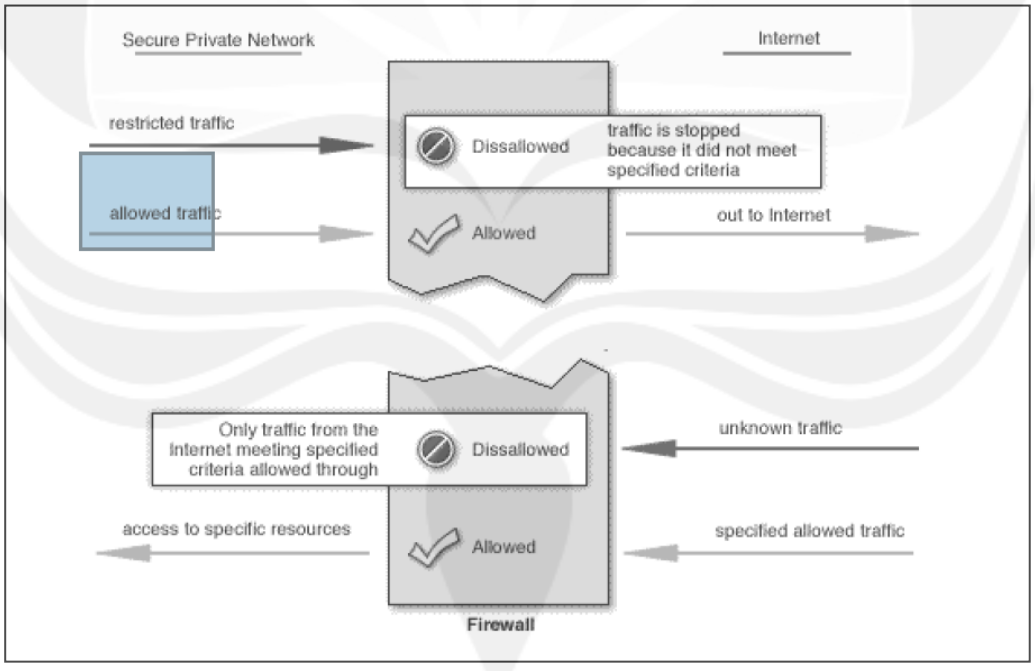
Di internet semua lalu lintas perjalanan dalam bentuk paket. Sebuah paket adalah data dalam ukuran terbatas. Seluruh *file* seperti *web retrievals* halaman, email, semua komunikasi internet selalu terjadi dalam bentuk paket. Paket adalah unit di format data dibawa oleh modus paket dalam jaringan komputer (Saravanakumar et al., 2011). Paket *capture* adalah tindakan menangkap paket data melalui sebuah jaringan komputer.

Paket *capture* digunakan oleh administrator jaringan dan insinyur keamanan untuk keperluan lalu lintas jaringan seperti monitor, menganaliasi pola lalu lintas, mengidentifikasi dan memecahkan masalah jaringan (Arai, 2012). Hasil *capture* paket di *filter* sesuai dengan kebijakan dari sistem keamanan yang telah ditetapkan.

Filter paket data dilakukan dengan melakukan pemeriksaan pada *header* paket yang kemudian diklasifikasikan sesuai dengan aturan yang telah ditetapkan untuk pendeteksian terhadap paket-paket data tertentu seperti pada gambar 2.2. Paket *filtering* akan menentukan apakah hendak menerima atau memblokir setiap paket berdasarkan informasi yang disimpan di dalam header sebuah paket (seperti halnya alamat sumber dan tujuan, port sumber dan tujuan, jenis protokol, serta informasi lainnya). Administrator jaringan dapat membuat peraturan tersebut sebagai daftar yang berurutan. Setiap paket yang datang kepada filter, akan dibandingkan dengan setiap peraturan yang diterapkan di dalam filter tersebut,

hingga sebuah kecocokan ditemukan. Jika tidak ada yang cocok, maka paket yang datang tersebut ditolak, dan berlaku sebaliknya (Raaj S & Kavitha, 2013).

Peraturan tersebut dapat digunakan untuk menerima paket atau menolaknya dengan menggunakan basis informasi yang diperoleh dari header protokol yang digunakan, dan jenis dari paket tersebut. Kebanyakan perangkat yang memiliki fitur packet filtering, menawarkan kepada administrator jaringan untuk membuat dua jenis peraturan, yakni inbound rule dan outbound rule. Inbound rule merujuk kepada inspeksi paket akan dilakukan terhadap paket yang datang dari luar, sementara outbound rule merujuk inspeksi paket akan dilakukan terhadap paket yang hendak keluar.



Gambar 2.2 Mekanisme Paket Filter Pada *Firewall* (Raaj S & Kavitha, 2013)

2.2.4 SMS gateway

SMS Gateway adalah sebuah perangkat atau layanan yang menawarkan SMS transit, membuat lalu lintas pesan atau SMS untuk komunikasi selular dari media lain ataupun sebaliknya, yang memungkinkan transmisi atau penerimaan pesan SMS dengan atau tanpa menggunakan ponsel. SMS Gateway adalah cara yang paling cepat dan dapat diandalkan untuk pengiriman SMS secara massal ataupun secara otomatis (Katankar and Thakare, 2010).

2.2.5 Port ekstensi alamat

Sebuah port adalah koneksi logis untuk komputer sebagai kebalikan dari koneksi fisik dan teridentifikasi dalam angka antara 1 sampai 65535 . Jumlah ini tidak memiliki korespondensi dengan jumlah koneksi fisik ke komputer yang mungkin ada hanya satu. Port diimplementasikan pada semua komputer yang terhubung pada jaringan. Setiap port dapat didedikasikan untuk server atau layanan tertentu. Nomor port dalam kisaran 1-1.023 disisihkan untuk penggunaan spesifik layanan standar yang sering disebut sebagai well-known port. Sebagai contoh, port 80 biasanya digunakan oleh Web server (Graba Jan, 2013).

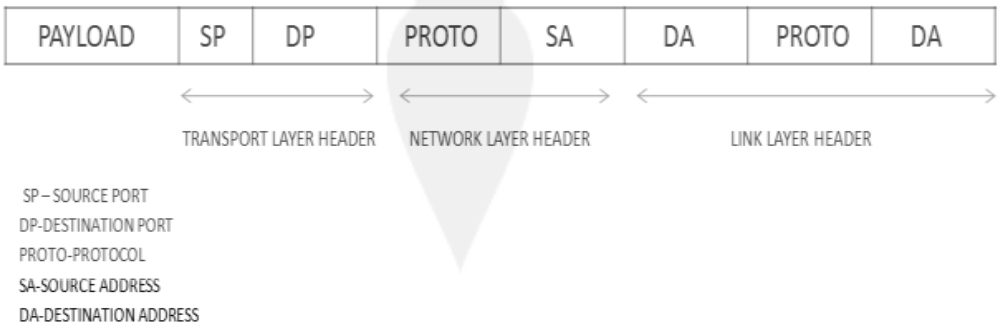
2.2.6 *Socket*

Socket adalah sebuah konsep abstrak dan bukan elemen *hardware* komputer. Hal ini digunakan untuk menunjukkan salah satu dari dua titik akhir dari hubungan komunikasi antara dua proses. Ketika klien ingin melakukan koneksi ke server hal itu akan menciptakan socket di ujung dari *link* komunikasi. Setelah menerima permintaan koneksi dari klien pada nomor port tertentu server akan membuat socket baru yang akan didedikasikan untuk komunikasi dengan klien

tertentu. Socket sendiri adalah aplikasi yang dibuat dan dikontrol aplikasi untuk dapat melakukan komunikasi dengan aplikasi lainnya (Graba Jan, 2013).

2.2.7 Paket data

Paket data adalah entitas dasar dari semua sistem komunikasi. Keamanan jaringan demikian berarti keamanan dari paket data. Sebuah paket data adalah blok yang paling dasar komunikasi yang melibatkan aliran streamline terbatas replika lainnya untuk mengirimkan informasi dari satu perangkat ke perangkat lainnya. Sebuah paket data yang terkandung dalam segmen data (*header data*) yang menimpan informasi lain seperti protokol yang digunakan, tujuan *hardware* alamat dan lain-lain seperti terlihat pada gambar 2.3. Singkatnya, identitas setiap paket yang datang dari sumber tidak bisa diandalkan dapat dideteksi dengan mempelajari isinya, contoh dari paket data yang dapat dideteksi dengan menggunakan firewall ataupun aplikasi monitoring lainnya. Manajemen trafik data, pengukuran trafik jaringan komputer dan *sniffing* adalah beberapa produk dari *packet capture, packet capture* juga digunakan sebagai basis untuk berbagai macam sistem keamanan (Suri and Batra, 2012), (Aluvala, 2011).



Gambar 2.3 *Header Packet Data* (Raaj et all, 2013)

2.2.8 Windows socket (WINSOCK)

Sistem operasi *Windows* memiliki *Application Programming Interface* (API) untuk berkomunikasi memlalui TCP/IP yang dikenal dengan nama *WinSock* API. Pemprograman API sendiri sudah sangat sulit karena pemprograman API sudah berurusan dengan aras rendah. Aras rendah tidak diizinkan secara langsung untuk diakses. Akan tetapi, *Windows* telah menyediakan API, yaitu berupa sekumpulan fungsi untuk mengakses aras rendah. Untuk membantu para programer dalam hal pembuatan *software* yang dapat berkomunikasi dengan komputer lain maka disediakan sebuah komponen *ActiveX control* yang bernama *WinSock Control*. *Winsock* secara khusus didefinisikan dengan bagaimana sebuah *software* jaringan *windows* harus mengakses layanan jaringan, terutama TCP/IP.

Winsock menyediakan layanan API tunggal dimana pengembang aplikasi dan *software* jaringan perlu untuk menyesuaikan diri. Untuk beberapa versi dari *windows*, *winsock* didefinisikan sebagai *binary interface* yang menjamin sebuah aplikasi cocok pada *winsock* API yang berjalan pada *software* jaringan dari berbagai pengembang. *Winsock* berbasiskan BSD (*Berkeley) socket*, tetapi memberikan fungsi tambahan yang mengizinkan API bekerja pada standar pemprograman *winsock*. Dengan *Winsock control* maka programer tidak perlu mengetahui detail TCP/IP dan pemanggilan fungsi API untuk membuat sebuah aplikasi jaringan karena programer hanya menggunkan metode, *properti*, atau *event* yang dimiliki oleh *winsock.*

2.2.9 Klasifikasi paket data

Klasifikasi paket data dimaksudkan untuk pengolahan data hasil penyaringan dari lalu-lintas paket data pada jaringan. Klasifikasi paket data dengan menggunakan parameter level bahaya dari suatu paket, level bahaya paket yang digunakan sebagai acuan adalah berdasarkan port layanan yang dapat dilihat pada tabel 2.2. *Traffic treshold* jumlah paket data yang terdeteksi dikalkulasi pada tiap sesi, apabila telah mencapai batas maksimal maka ditandai sebagai anomali. Hasil dari kalkulasi memiliki nilai batas yang rendah untuk paket data dengan port layanan di level *dangerous* begitu pula sebaliknya kemudian akan dimasukan pada data laporan untuk dikirim pada administrator melalui pesan singkat.

Tabel 2.2 Level Port Data Pada Keamanan Jaringan (Riadi I., 2013)

No	Level of Attacks	Port / Protocol	TCP Flags	Information
1	Dangerous	80 / TCP	16,32	HTTP
		8080 / TCP	16,32	HTTP alternate
		443 / TCP	16,32	HTTPS (Hypertext Transfer Protocol over SSL/TLS)
		20 / TCP	16,32	FTP data transfer
		21 / TCP	16,32	FTP control (command)
		22 / TCP	16,32	SSH
		23 / TCP	16,32	Telnet protocol
		53 / UDP	-	DNS
2	Rather Dangerous	161 / TCP	20 - 24	SNMP
		143 / TCP	20 - 24	IMAP
		162 / TCP	20 - 24	SNMPTRAP
		110 / TCP	20 - 24	POP3
		993 / TCP	20 - 24	IMAPS
		137 / UDP	-	NetBIOS
		161 / UDP	-	SNMP
3	Not Dangerous	In addition to the above mentioned	TCP (20-27) UDP (-)	In addition to the above mentioned