BAB II

TINJAUAN PUSTAKA

Pada bab ini akan membahas tentang tinjauan pustaka yang melandasi penelitian yang diangkat dalam penyusunan tesis ini. Tinjauan pustaka yang digunakan meliputi jaringan komputer, jenis – jenis jaringan komputer, protokol jaringan komputer, model OSI, Protokol TCP/IP, keamanan jaringan komputer, serangan pada jaringan komputer, konsep dari *Intrusion Detetction System* (IDS).

2.1 Jaringan Komputer

Jaringan komputer (*computer network)* adalah suatu interkoneksi antara kelompok – kelompok komputer dengan kelompok komputer yang lainnya. Dengan menggunakan jaringan komputer, komputer – komputer akan saling mengakses dan bertukar data tanpa harus berpindah sebuah media penyimpanan (usb/disket) dari satu komputer ke komputer yang lain [7].

Model komputer tunggal yang melayani seluruh tugas – tugas komputasi telah diganti dengan sekumpulan komputer berjumlah banyak yang terpisah tetapi saling berhubungan dalam melaksanakan tugasnya, sistem tersebut yang disebut jaringan komputer [7].

Jaringan komputer merupakan sistem yang terdiri dari gabungan atau sekumpulan perangkat (sering disebut *nodes*) yang saling terhubung satu sama lain melalui sebuah jalur komunikasi. Sebuah node dapat berupa komputer, printer, atau

perangkat lain yang mampu mengirim dan atau menerima data yang dikirimkan oleh node lain pada jaringan [8].

2.1.1 Jenis Jaringan Komputer

Menurut jangkauannya, jenis jaringan komputer dibagi menjadi tiga jenis yaitu :

1. *Local Area Network* (LAN) merupakan jaringan komputer yang saling terhubung ke suatu komputer server dengan menggunakan teknologi tertentu, biasanya digunakan dalam kawasan satu gedung atau kawasan yang jaraknya tidak lebih dari 1 Km [9].
2. *Metropolitan Area Network* (MAN) merupakan jaringan komputer yang saling terkoneksi dalam satu kawasan kota yang jaraknya bisa lebih dari 1 Km. Pilihan untuk membangun jaringan komputer antar kantor dalam suatu kota [9].
3. *Wide Area Network* (WAN) merupakan jaringan komputer yang menghubungkan banyak LAN ke dalam suatu jaringan terpadu, antara satu jaringan dengan jaringan lain dapat berjarak ribuan kilometer atau terpisahkan letak geografi dengan menggunakan metode komunikasi tertentu [9].

2.1.2 Protokol Jaringan Komputer

Protokol dalam dunia komputer adalah aturan, atau ketentuan agar satu atau lebih perangkat dapat saling berkomunikasi. Sedangkan protokol jaringan komputer adalah aturan agar perangkat satu dengan perangkat lain dapat saling berkomunikasi sesuai sistem jaringan komputer yang ada. Macam – macam protokol jaringan yang sering kita jumpai adalah IPV4 dan DHCP, serta dalam

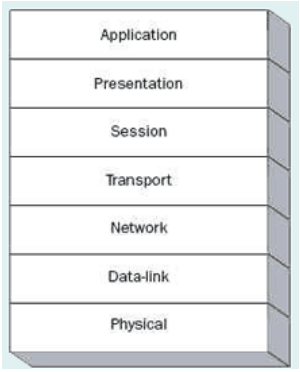
komunikasi internet kita bertemu dengan bermacam – macam protocol, misal HTTP dan POP3.

1. *Post Office Protokol Version 3* (POP3) adalah protocol yang digunakan untuk mengambil surat elektronik (*email*) dari server *mail*. Protokol ini erat hubungannya dengan protocol SMTP.
2. *Hypertext Transfer Protocol* (HTTP) adalah sebuah protokol jaringan lapisan aplikasi yang digunakan untuk sistem informasi terdistributif, kolaboratif, dan menggunakan hypermedia. Penggunaannya banyak pada pengambilan sumber daya yang saling terhubung dengan tautan, yang disebut dengan dokumen hiperteks yang kemudian membentuk *world wide web*.
3. *File Transfer Protocol* (FTP) adalah sebuah protokol internet yang berjalan dalam lapisan aplikasi yang merupakan standar untuk pengiriman berkas (file) komputer antar mesin – mesin dalam sebuah jaringan.
4. *Simple Mail Transfer Protocol* (SMTP) adalah standar internet untuk surat elektronik *(email*) transmisi di internet jaringan protokol.
5. *Secure Sh*ell (SSH) adalah protokol jaringan yang memungkinkan pertukaran data melalui saluran aman antara dua perangkat jaringan.
6. *Telecomunication Network* (Telnet) adalah sebuah protokol jaringan yang digunakan pada internet atau *local network* untuk menyediakan fasilitas komunikasi berbasis teks interaksi dua arah yang menggunakan koneksi virtual terminal.

7. User Datagram Protocol (UDP) adalah salah satu protokol lapisan transport TCP/IP yang mendukung komunikasi yang tidak andal (*unreliable*), tanpa koneksi antara *host – host* dalam jaringan yang menggunakan TCP/IP.

2.1.3 Model OSI

The International Organization for Standarization (ISO) mengembangkan model referensi *Open System Interconnection* (OSI) sebagai pemandu untuk mendefinisikan sekumpulan protokol terbuka. Walaupun minat pada protokol OSI telah berkurang, model referensi OSI tetap merupakan standar yang paling umum untuk menggambarkan dan membandingkan rangkaian protokol. Model OSI memiliki tujuh lapisan.



Gambar II-1 OSI Layer

1. *Physical Layer* (*Lapisan Fisik)*

Berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya *ethernet* atau *token ring*), topologi jaringan dan pengkabelan. Selain itu, level ini mendefinisikan

bagaimana *Network Interface Card* (NIC) dapat berinteraksi dengan media kabel atau radio.

2. *Data Link Layer* (Lapisan Data Link)

Berfungsi untuk menentukan bagaimana bit – bit dapat dikelompokan menjadi format yang disebut sebagai *frame*. Selain itu, pada level ini terjadi koreksi kesalahan, *flow control*, pengalamatan perangkat keras (seperti halnya *Media Access Control Address* (MAC Address) dan menentukan bagaimana perangkat – perangkat jaringan seperti hub, bridge, repeater, dan switch layer 2 beroperasi. Spesifikasi IEEE 802, membagi level ini menjadi dua level yaitu lapisan *Logical Link Control* (LLC) dan lapisan *Media Access Control* (MAC).

3. *Network Layer* (Lapisan Jaringan)

Berfungsi untuk pengendalian operasi *subnet* dengan meneruskan paket – paket dari suatu node ke node lain dalam jaringan. Masalah desain yang penting adalah bagaiman caranya menentukan *route* pengiriman paket dari sumber ke tujuannya.

4. *Transport Layer* (Lapisan Transport)

Fungsi dasar *transport layer* adalah menerima data dari *session layer*, memecah data menjadi bagian – bagian yang lebih kecil bila perlu, meneruskan data ke *network layer*, dan menjamin bahwa semua potongan data tersebut bisa tiba di sisi lainnya dengan benar. Selain itu, semua hal tersebut harus dilaksanakan secara efisien, dan bertujuan dapat melindungi layer-layer bagian atas dari perubahan teknologi perangkat keras yang tidak dapat dihindari. Dalam keadaan normal,

transport layer membuat koneksi jaringan yang berbeda bagi setiap koneksi *transport* yang diperlukan oleh *session layer*. Bila koneksi *transport* memerlukan *throughput* yang tinggi, maka *transport layer* dapat membuat koneksi jaringan yang banyak. *Transport layer* membagi-bagi pengiriman data ke sejumlah jaringan untuk meningkatkan *throughput*.

5. *Session Layer* (Lapisan Sesi)

Session layer mengijinkan para pengguna untuk menetapkan *session* dengan pengguna lainnya. Layer ini membuka, mengatur dan menutup suatu *session* antara aplikasi-aplikasi. Sebuah *session* selain memungkinkan *transport* data biasa, seperti yang dilakukan oleh *transport layer*, juga menyediakan layanan yang istimewa untuk aplikasi-aplikasi tertentu. Sebuah *session* digunakan untuk memungkinkan seseorang pengguna *log* ke *remote time sharing* sistem atau untuk memindahkan file dari satu mesin ke mesin lainnya. Sebuah layanan *session* layer yang lain adalah untuk melaksanakan pengendalian dialog. *Session* dapat memungkinkan lalu lintas bergerak dalam bentuk dua arah pada suatu saat, atau hanya satu arah saja. Jika pada suatu saat lalu lintas hanya satu arah (analog dengan rel kereta api tunggal), *session* layer membantu untuk menentukan giliran yang berhak menggunakan saluran. Layanan *session* di atas disebut manajemen token. Untuk sebagian protokol, adalah penting untuk memastikan bahwa kedua pihak yang bersangkutan tidak melakukan operasi pada saat yang sama. Untuk mengatur aktivitas ini, *session layer* menyediakan token-token yang dapat digilirkan. Hanya pihak yang memegang token yang diijinkan melakukan operasi kritis.

6. *Presentation Layer* (Layer Presentasi)

Presentation layer melakukan fungsi-fungsi tertentu yang diminta untuk menjamin penemuan sebuah penyelesaian umum bagi masalah tertentu. Selain memberikan sarana-sarana pelayanan untuk konversi, format dan enkripsi data, *presentation layer* juga bekerja dengan file berformat ASCII, EBCDIC, JPEG, MPEG, TIFF, PICT, MIDI, dan Quick Time. *Presentation layer* tidak mengijinkan pengguna untuk menyelesaikan sendiri suatu masalah. Tidak seperti layer-layer di bawahnya yang hanya melakukan pemindahan bit dari satu tempat ke tempat lainnya, *presentation layer* memperhatikan sintaks dan semantik informasi yang dikirimkan.

7. *Application Layer* (Layer Aplikasi)

Lapisan ini bertugas memberikan sarana pelayanan langsung ke pengguna, yang berupa aplikasi-aplikasi dan mengadakan komunikasi dari program ke program. Jika kita mencari suatu file dari file server untuk digunakan sebagai aplikasi pengolah kata, maka proses ini bekerja melalui layer ini. Demikian pula jika kita mengirimkan e-mail, browse ke internet, chatting, membuka telnet session, atau menjalankan FTP, maka semua proses tersebut dilaksanakan di layer ini.

2.2 Keamanan Jaringan Komputer

Suatu komputer yang terhubung dengan sebuah jaringan komputer mempunyai ancaman keamanan yang lebih besar dibandingkan dengan komputer yang tidak terhubung dengan jaringan komputer. Keamanan jaringan komputer biasanya berbanding terbalik dengan akses jaringan dimana akses jaringan semakin

mudah maka keamanan jaringan komputer semakin rentan tetapi apabila jaringan komputer semakin aman maka akses jaringan akan semakin tidak nyaman [8].

Langkah awal dalam mengembangkan rencana *network security* yang efektif adalah dengan mengenali ancaman yang mungkin dating. Dalam RFC 1244, *Site security Handbook*, dibedakan tiga tipe ancaman yaitu :

1. Akses tidak sah oleh orang yang tidak memiliki wewenang.
2. Kesalahan informasi, segala masalah yang dapat menyebabkan diberikannya informasi yang penting atau sensitif kepada orang yang salah, yang seharusnya tidak boleh mendapatkan informasi tersebut.
3. Penolakan terhadap service, segala masalah mengenai security yang menyebabkan sistem mengganggu pekerjaan-pekerjaan yang produktif.

2.3 Tipe Serangan Keamanan Komputer

Fungsi sistem komputer dapat digunakan sebagai dasar untuk menentukan model tipe ancaman dari suatu sistem komputer. Berdasarkan fungsi sistem komputer sebagai penyedia informasi, ancaman terhadap sistem komputer dikategorikan menjadi empat, yaitu :

1. *Interruption*, merupakan suatu ancaman terhadap availability, informasi atau data yang ada dalam sistem komputer dirusak, dihapus, sehingga jika dibutuhkan maka sudah tidak ada lagi.
2. *Interception*, merupakan ancaman terhadap kerahasiaan (*secrecy*). Informasi yang ada di dalam sistem disadap oleh orang yang tidak berhak.

3. *Modification*, merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalu-lintas informasi yang sedang dikirim lalu mengubahnya sesuai keinginan orang itu.
4. *Fabrication*, merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil meniru atau memalsukan suatu informasi sehingga orang yang menerima informasi tersebut menyangka informasi tersebut berasal dari orang yang dikehendaki oleh si penerima informasi tersebut.

2.4 Risiko Jaringan Komputer

Pendekatan yang umum dilakukan untuk meningkatkan keamanan komputer antara lain adalah dengan membatasi akses fisik terhadap komputer, menerapkan mekanisme pada perangkat keras dan sistem operasi untuk keamanan komputer serta membuat strategi pemrograman untuk menghasilkan program komputer yang dapat diandalkan.

Segala bentuk ancaman fisik maupun logik yang langsung atau tidak langsung mengganggu kegiatan yang sedang berlangsung dalam jaringan. Faktor – faktor penyebab risiko atau gangguan dalam jaringan komputer :

1. Kelemahan manusia (*human error*).
2. Kelemahan perangkat keras komputer.
3. Kelemahan sistem operasi jaringan.
4. Kelemahan sistem jaringan komunikasi.

2.5 Jenis – Jenis Serangan Jaringan Komputer

Gangguan dan ancaman kemanan jaringan komputer adalah pengacauan, penyusupan atau serangan lainnya pada infrastruktur jaringan untuk menganalisa jaringan dan memperoleh informasi secepatnya, lalu membuat jaringan hancur dan rusak. Ancaman dapat berupa manusia, objek, atau kejadian yang jika tercapai dapat berpotensi menyebabkan kerusakan pada jaringan.

Serangan yang dilakukan secara sengaja adalah serangan yang berbahaya dilakukan oleh karyawan yang tidak puas untuk menyebabkan kerusakan organisasi dan tidak disengaja serangan penyebab kerusakan keuangan organisasi dengan menghapus file data penting. Ada sejumlah serangan yang terjadi yaitu *denial of service (dos), spoofing attack, port scanning,* dan *application based attack,* serta *malware.*

2.5.1 Denial of Service (DoS)

Merupakan sebuah jenis serangan terhadap sebuah computer atau server di dalam jaringan. DOS ini bekerja dengan cara menghabiskan *resource* yang dimiliki oleh computer tersebut sampai akhirnya computer tersebut tidak dapat menjalankan fungsinya dengan benar yang secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari computer yang diserang tersebut. DOS ini akan menyerang dengan cara mencegah seorang pengguna untuk melakukan akses terhadap system atau jaringan yang dituju [1].

Berikut jenis – jenis serangan atau gangguan Denial of Service (DoS) :

1. Ping of Death

   Merupakan serangan klasik yang dulu sering digunakan. Serangan ini dilancarkan dengan menggunakan *utility ping* pada sebuah system operasi [5] [1].

2. UDP Flood

   Pada dasarnya mengkaitkan dua system tanpa disadari dengan cara spoofing. UDP flood attack akan menempel pada service UDP di salah satu mesin yang untuk keperluan percobaan akan mengirimkan sekelompok karakter ke mesin lain.

3. ICMP Flood

   Melakukan eksploitasi system agar dapat membuat suatu target client menjadi crash, karena diakibatkan oleh pengiriman sejumlah paket yang besar ke arah target client.

4. Smurf Attack

   Merupakan serangan secara paksa pada fitur spesifikasi IP. Smurf hacker biasanya membanjiri jaringan dengan paket permintaan echo ICMP.

2.5.2 Port Scanning

Port scanning adalah suatu kegiatan atau aktifitas atau proses untuk mencari dan melihat serta meneliti port pada suatu komputer atau peralatan lainnya. Tujuannya adalah meneliti kemungkinan kelemahan dari suatu sistem yang terpasang pada komputer melalui port yang terbuka.

2.5.3 IP Spoofing

IP *Spoofing* juga dikenal sebagai *Source Address Spoofing*, yaitu pemalsuan alamat IP penyerang sehingga sasaran menganggap alamat IP penyerang tersebut adalah alamat IP dari *host* didalam jaringan bukan diluar jaringan.

2.5.4 Malware (Virus)

Sebuah software atau kode yang diciptakan oleh seseorang dengan tujuan untuk merugikan orang lain.

2.6 Intrusion Detection System

Deteksi intrusi adalah pendekatan baru untuk memberikan rasa aman dalam jaringan komputer dan data yang ada. Tujuan dari deteksi intrusi adalah untuk mengidentifikasi, sebaiknya *real time*, penggunaan yang tidak sah, penyalahgunaan sistem komputer dengan sistem *insider* baik dari dalam maupun dari luar jaringan [9].

Intrusion Detection System (IDS) merupakan sebuah perangkat lunak yang dapat mendeteksi aktifitas yang mencurigakan dalam sebuah sistem maupun jaringan. Dengan kata lain, IDS merupakan sistem untuk mendeteksi intrusi yang dilakukan *intruder*. Dalam mendeteksi suatu intrusi, IDS menggunakan dua teknik, yaitu dengan teknik *signature based detection* dan *anomaly based detection* [3].

2.6.1 Jenis – Jenis IDS

IDS adalah sebuah aplikasi perangkat lunak atau perangkat keras yang bekerja secara otomatis untuk memonitor kejadian pada jaringan komputer dan menganalisis masalah keamanan jaringan. Sasaran IDS adalah memonitoring asset

jaringan untuk mendeteksi perilaku yang tidak lazim, kegiatan yang tidak sesuai, serangan atau menghentikan serangan dan bahkan menyediakan informasi untuk menelusuri penyerang [10]. IDS mengelompokan kedalam dua kategori utama bentuk dasar, yaitu :

1. Host – Based Intrusion Detection System (HIDS) hanya melakukan pemantauan pada perangkat komputer tertentu dalam jaringan. HIDS biasanya akan memantau kejadian seperti kesalahan login berkali – kali dan melakukan pengecekan pada file [5] [11] [12].
2. Network – Based Intrusion Detection System (NIDS) menempati secara langsung pada jaringan dan melihat semua aliran yang melewati jaringan. NIDS merupakan strategi yang efektif untuk melihat trafik masuk atau keluar maupun trafik diantara host ataupun diantara segmen jaringan local. NIDS biasanya dikembangkan didepan dan di belakang firewall dan VPN gateway untuk mengukur keefektifan pranti – peranti keamanan tersebut dan berinteraksi dengan mereka untuk memperkuat keamanan jaringan [5] [11] [12].

2.6.2 Fungsi IDS

Intrusion Detection System (IDS) terdiri dari empat fungsi utama yaitu koleksi data (*data collection*), pemilihan fitur (*feature selection*), analisis (*analysis*), dan tindakan (*action*) [1].

2.6.2.1 Koleksi Data (Data Collection)

Modul ini melewati data sebagai masukan IDS. Data yang dicatat ke dalam sebuah file dan kemudian dianalisis. Jaringan berbasis IDS mengumpulkan dan mengubah paket data dalam IDS berbasis host mengumpulkan rincian seperti penggunaan disk dan proses system [1].

2.6.2.2 Pemilihan Fitur (Feature Selection)

Untuk memilih fitur tertentu yang besar data tersedia dalam jaringan dan biasanya dievaluasi oleh intrusion. Sebagai contoh, *internet protocol* (IP) sumber dan target, jenis protocol, panjang header dan ukuran dapat dijadikan sebagai kunci intrusi [1] [13].

2.6.2.3 Analisis (Analysis)

Data dianalisis untuk menemukan kebenaran. Aturan berdasarkan IDS menganalisis lalu lintas data yang masuk diperiksa berdasarkan *signature* atau pola. Metode lain adalah IDS berdasarkan anomaly dimana system mempelajari perilaku jaringan normal [1].

2.6.2.4 Tindakan (Action)

Mendefinisikan tentang serangan dari reaksi system. Dapat memberi tahu administrator system dengan semua data yang dibutuhkan melalui alarm atau dapat memainkan peran aktif system dengan memblok paket agar tidak memasuki system [1].

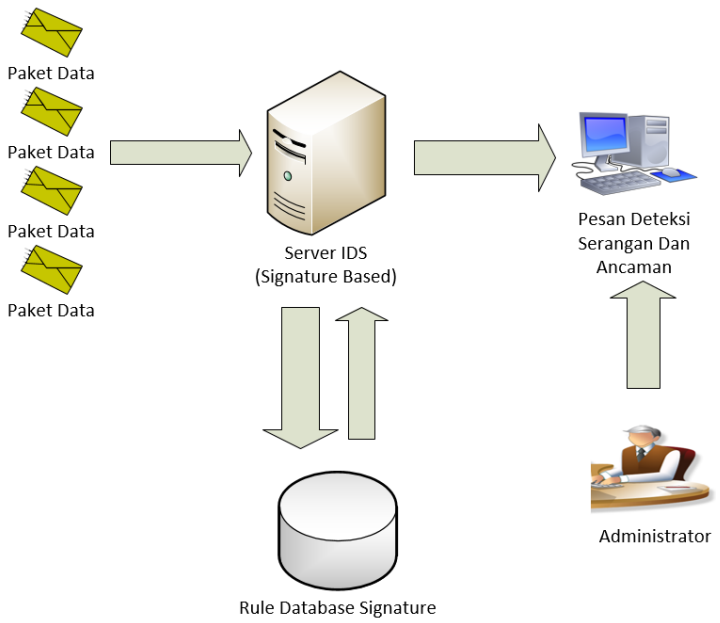
2.6.3 Metode IDS

2.6.3.1 Signature Based Detection

IDS berbasis *signature* bekerja dengan cara menyadap paket data kemudian membandingkannya dengan basis data *rules* IDS yang berisi pola – pola serangan. Jika paket data mempunyai pola yang sama dengan salah satu pola di basis data *rules* IDS, maka paket tersebut dianggap sebagai sebuah serangan. Jika paket data tersebut sama sekali tidak mempunyai pola yang sama dengan pola di basis data *rules* IDS, maka paket tersebut dianggap bukan serangan [11].

IDS yang berbasis pada *signature* akan melakukan pengawasan terhadap paket – paket dalam jaringan dan melakukan perbandingan terhadap paket – paket tersebut dengan basis data *signature* yang dimiliki sistem IDS ini atau atribut yang dimiliki oleh percobaan serangan yang pernah diketahui. Cara ini hampir sama dengan cara kerja aplikasi anti virus dalam melakukan deteksi terhadap malware. Intinya adalah akan terjadi keterlambatan antara terdeteksinya sebuah serangan dengan *signature* yang digunakan untuk melakukan deteksi yang diimplementasikan dalam basis data IDS yang digunakan.

Paket data merupakan paket data yang di *capture* yang melewati *Ethernet card* untuk selanjutnya digunakan oleh metode *signature* untuk dilakukan pengecekan. IDS yang berbasis *signature based* akan membandingkan paket data dengan *rule* dalam database IDS yang digunakan. Jika terdapat kecocokan pada database maka akan memberikan pesan deteksi terjadi gangguan seperti ditunjukan pada gambar II-2.



Gambar II-2 Cara Kerja Signature Based Detection

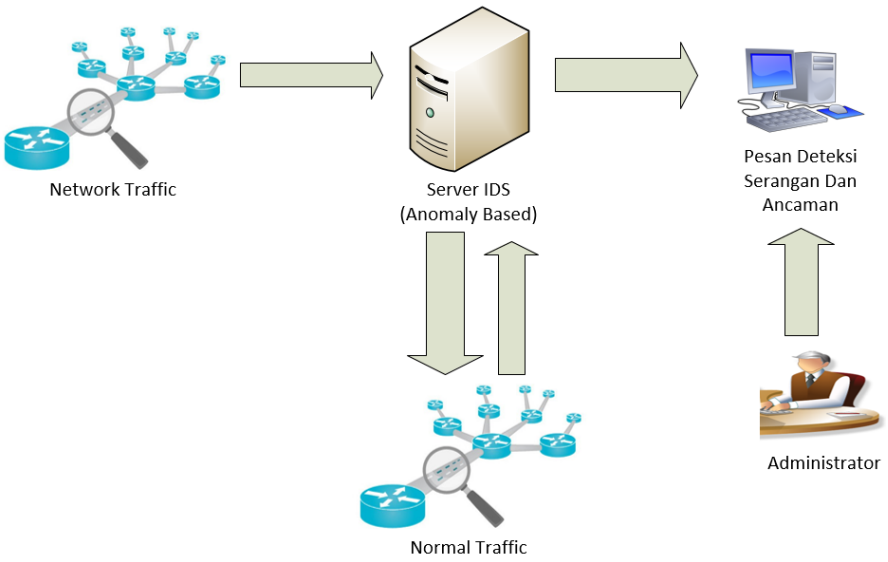
Metode *signature based* cocok digunakan untuk pola ancaman atau gangguan yang sudah diketahui pola sebelumnya. *Signature based* juga cocok untuk digunakan mendeteksi semua jenis serangan seperti *port scanning, exploit, dan* DoS [3].

2.6.3.2 Anomaly Based Detection

IDS jenis ini akan mengawasi trafik dalam jaringan dan melakukan perbandingan trafik yang terjadi dengan trafik yang ada. Sistem akan melakukan identifikasi apa yang dimaksud dengan jaringan normal dalam jaringan tersebut. Jaringan normal tersebut dapat dilihat pada penggunaan bandwidth yang biasa digunakan dalam jaringan, protocol apa yang digunakan, port dan perangkat apa saja yang terhubung dalam jaringan tersebut [17].

Anomaly based dapat mendeteksi adanya penyusupan dengan mengamatai adanya keanehan pada sistem. Keanehan tersebut akan dibandingkan dengan situasi normal yang ada pada sistem [11].

Cara kerja IDS dengan teknik *anomaly based* dapat dilihat pada gambar II-3 berikut :



Gambar II-3 Cara Kerja Anomaly Based Detection

Metode *anomaly based* cocok digunakan untuk mendeteksi gangguan atau ancaman dengan kategori *Denial of Service* (DOS) [3].

Metode anomali ini bersifat dalam perbandingan jaringan normal terhadap jaringan yang tidak normal, jika jaringan normal tersebut tidak didefinisikan terlebih dahulu maka gangguan tersebut akan menjadi ancaman bagi jaringan tersebut.

2.7 Snort

Snort merupakan bagian dari IDS berupa perangkat lunak *open source*. Snort mampu melakukan analisa *realtime traffic* dan *packet logger* pada jaringan IP dan dapat menganalisa protokol dan melakukan pendeteksian variasi gangguan. Snort juga memiliki kemampuan *realtime alert*, dimana mekanisme pemasukan *alert* dapat berupa *user syslog, file, unix socket* ataupun melalui *database*.

Dalam mengoperasikan snort mempunyai tiga buah mode yaitu :

1. *Sniffer Mode*

   Sniffer Mode ini berfungsi untuk melihat paket yang lewat di jaringan.

2. *Packet Logger Mode*

   Packet Logger Mode berfungsi untuk mencatat semua paket yang lewat dijaringan kemudian akan dianalisa. Bahkan dapat menyimpan paket ke dalam disk.

3. *Intrusion Detection Mode*

   Mode snort ini akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan computer.

2.8 Penelitian Sebelumnya

Pada penelitian sebelumnya telah banyak yang meneliti dalam bidang keamanan jaringan yang berkaitan dengan penggunaan intrusion detection system (IDS). Penelitian sebelumnya berkaitan dengan penggunaan metode signature based dan anomaly based diantaranya :

1. Pada tahun 2012 I Gusti Ngurah Arya Sucipta, I Made Widhi Wirawan, dan Agus Muliantara melakukan penelitian dengan judul Analisis Kinerja Anomaly Based Intrusion Detection System (IDS) Dalam Mendeteksi Serangan DOS (Denial Of Service) Pada Jaringan Komputer. Penelitian yang dilakukan dengan melakukan pengujian serangan DoS dengan merubah baseline secara terus menerus. Pengujian dilakukan sebanyak tiga kali pengujian dan menghasilkan deteksi bahwa dengan metode anomaly dapat mendeteksi serangan DoS dan jenis pola serangan baru, tetapi memiliki kesalahan yang cukup besar [3].
2. Pada tahun 2011 Noviana Sagita, Niken Dwi Cahyani, dan Fazmah Arif Yulianto melakukan penelitian dengan judul Perbandingan Performansi Antara Signature Based Dan Anomaly Based Dalam Pendeteksian Intrusi. Penelitian yang dilakukan dengan menguji serangan dengan port scanning, exploit, dan Dos menggunakan metode signature dan anomaly based secara bergantian dalam mendeteksi serangan. Menghasilkan penelitian bahwa signature based dapat mendeteksi jenis serangan port scanning, exploit. Sedangkan anomaly based hanya bias mendeteksi serangan DoS [4].
3. Pada tahun 2015 Lutfi Nur Hakim melakukan penelitian dengan judul Analisis Perbandingan Intrusion Detection System Snort dan Suricata. Penelitian yang dilakukan dengan melakukan serangan dengan *port scanning*, *Bruto Force*, dan DoS terhadap penggunaan tools Suricata dan Snort. Selain itu, dilakukan pengukuran sumber daya terhadap aplikasi yang digunakan. Hasil penelitian menunjukan bahwa dalam akurasi deteksi Suricata mempunyai deteksi yang

lebih unggul dibandingkan snort, sedangkan IDS snort mengkonsumsi memori dan processor yang lebih sedikit dibandingkan dengan Suricata [18].

4. Pada tahun 2016 Safwan Mawlood Hussein melakukan penelitian dengan judul "*Performance Evaluation of Intrusion Detection System Using Anomaly And Signature Based Algorithms to Reduction False Alarm Rate and Detect Unknown Attacks*" penelitian dilakukan dengan mengkombinasikan IDS signature dan anomaly dengan menggunakan algoritma K-Means dan Naïve Bayes serta menggunakan data set dalam menguji metode yang digunakan. Hasilnya didapatkan bahwa yang dilihat perbandingan adalah penggunaan algoritma K-Means dan Naïve Bayes dalam membangun klasifikasi deteksi [14].