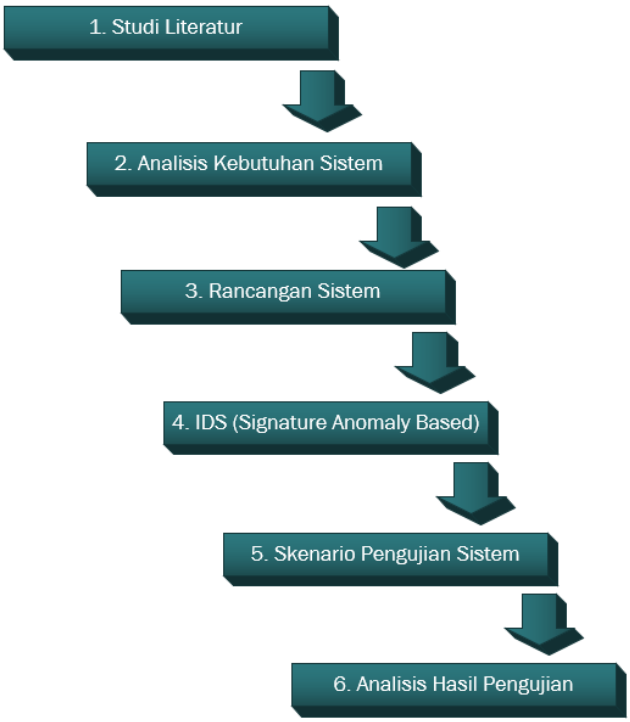
BAB III

METODE PENELITIAN

3.1 Tahapan Penelitian

Dalam pembuatan model sistem jaringan IDS menggunakan penggabungan metode signature based dan anomaly based dilakukan beberapa tahapan penelitian yang diperlihatkan pada gambar III-1 :



Gambar III-1 Diagram Alir Penelitian

Adapun penjelasan dari metodologi penelitian yang digunakan pada penelitian ini adalah :

a. Studi Literatur

Metode studi literatur digunakan untuk mengumpulkan data dan informasi yang dijadikan referensi dalam membangun sistem IDS yang digunakan. Referensi tersebut berasal dari buku – buku pegangan maupun publikasi hasil penelitian, artikel, situs internet serta sumber lain yang berkaitan dengan penelitian ini.

b. Analisis Kebutuhan Sistem

Pada tahapan analisis sistem ini digunakan analisis kebutuhan untuk sistem yang akan dibangun. Kebutuhan tersebut meliputi kebutuhan sistem baik perangkat keras maupun perangkat lunak yang akan digunakan pada sistem IDS.

c. Rancangan Sistem

Rancangan sistem meliputi arsitektur dan topologi jaringan yang akan digunakan dalam membangun sistem IDS yang akan digunakan.

d. Penggabungan Metode IDS (Signature dan Anomali)

Pada tahapan ini merupakan tahapan untuk menggabungkan metode IDS baik *signature* dan *anomaly* yang digunakan untuk system IDS. Selain itu juga digunakan penentuan baseline penggunaan jaringan normal yang digunakan.

e. Skenario Pengujian Sistem

Skenario pengujian digunakan untuk menentukan pengujian sistem IDS yang telah dibangun dengan membuat simulasi gangguan yang diberikan kepada sistem yang telah dibangun.

f. Analisis Hasil Pengujian

Pada tahap ini dilakukan analisis terhadap hasil pengujian sistem IDS yang digunakan.

3.2 Analisis Kebutuhan Sistem

Analisa kebutuhan sistem merupakan proses identifikasi dan evaluasi kebutuhan sistem IDS yang akan dirancang untuk mendapatkan sistem IDS sesuai yang dibutuhkan. Analisa kebutuhan sistem ini meliputi pada kebutuhan baik perangkat keras maupun perangkat lunak.

3.2.1 Analisis Kebutuhan Perangkat Keras

Dalam membangun sistem IDS maka diperlukan spesifikasi perangkat keras yang dapat mendukung jalannya sistem IDS tersebut. Kebutuhan perangkat keras tersebut bergantung terhadap sistem yang akan dibuat. Semakin banyak pengguna dalam jaringan tersebut maka dibutuhkan spesifikasi perangkat keras yang memadai. Berikut spesifikasi perangkat keras yang akan digunakan pada sistem IDS yang akan dibangun :

Spesifikasi perangkat keras untuk server IDS ditunjukan pada tabel III-1 :

Tabel III-1 Spesifikasi Server IDS

Processor	Intel Dual Core
RAM	2 GB
Harddisk	80 GB
VGA	Intel Grafik

Spesifikasi perangkat keras untuk pengguna jaringan ditunjukan pada tabel III-2 :

Tabel III-2 Spesifikasi Perangkat Keras Pengguna

Processor	Intel Dual Core
RAM	512 MB
Harddisk	40 GB
VGA	Intel Grafik

3.2.2 Analisis Kebutuhan Perangkat Lunak

Dalam membangun sistem IDS maka diperlukan spesifikasi perangkat lunak yang dapat mendukung jalannya sistem IDS tersebut. Kebutuhan perangkat lunak tersebut bergantung terhadap sistem yang akan dibuat. Semakin banyak pengguna dalam jaringan tersebut maka dibutuhkan spesifikasi perangkat lunak yang memadai. Berikut spesifikasi perangkat lunak yang akan digunakan pada sistem IDS merujuk pada tabel III-3.

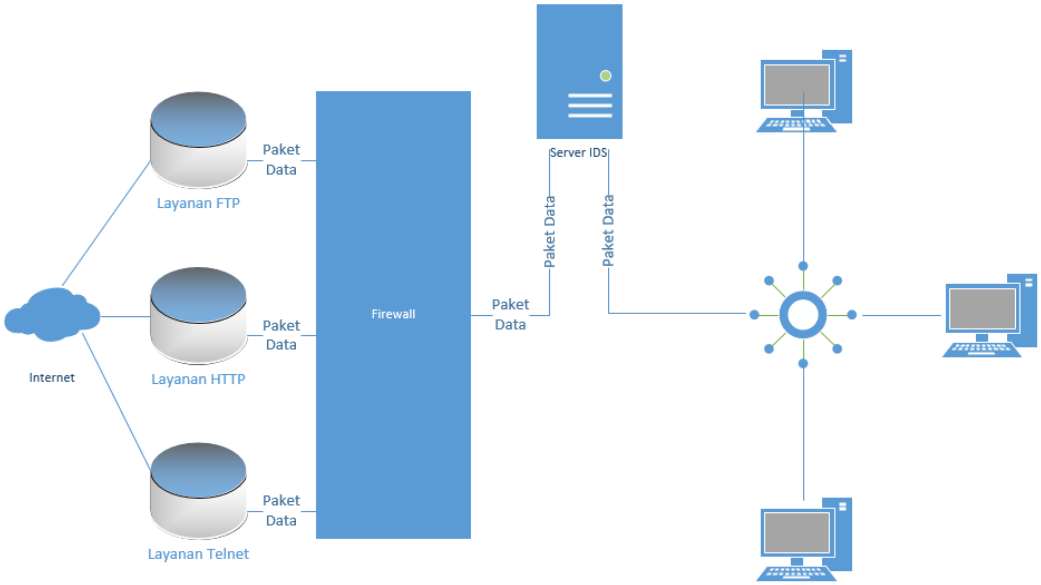
Spesifikasi perangkat lunak server IDS :

Tabel III-3 Spesifikasi Perangkat Lunak Server IDS

Sistem Operasi	Ubuntu Server 16
Sistem IDS	Snort IDS

3.3 Rancangan Sistem

Pada tahapan rancangan sistem, dibuat rancangan sistem yang akan digunakan untuk deteksi intrusi dengan metode Signature Anomaly Based (SAB) IDS. Berikut rancangan topologi yang digunakan :



Gambar III-2 Topologi Sistem IDS

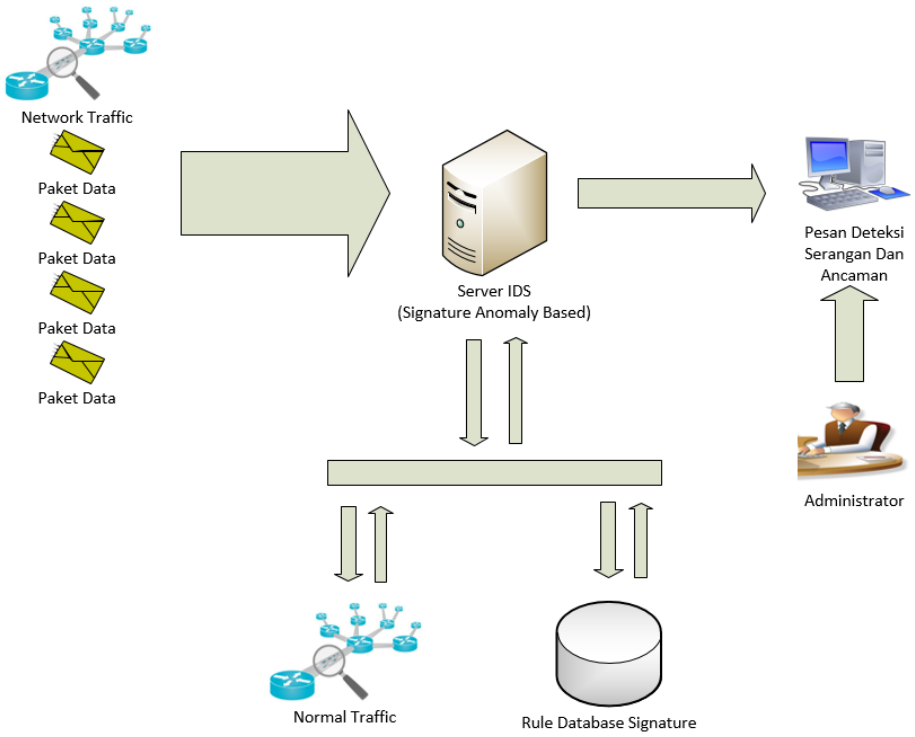
Keterangan Gambar III-2 pada sistem IDS:

1. *Client* merupakan pengguna dalam jaringan komputer yang dapat dijadikan sebagai pengguna yang dapat melakukan ancaman atau serangan.
2. Web Server IDS merupakan web server yang digunakan sebagai pendeteksi dan memonitor paket serta trafik yang melalui jaringan yang dimonitor. Dalam server IDS ini digunakan metode dengan *Signature Anomaly Based*. Selain itu dijadikan sebagai tujuan serangan.

Rancangan sistem yang digunakan pada sistem IDS yang digunakan yaitu IDS yang berbasis jaringan. Penempatan sensor IDS ini merupakan hal yang sangat penting, penempatan sensor berhubungan dengan trafik jaringan yang akan dimonitor. Dalam hal ini penempatan IDS digunakan untuk memonitor dan mengawasi trafik jaringan yang berada di lingkungan internal jaringan.

3.4 Signature Anomali Based (SAB)

Signature Anomali Based (SAB) merupakan penggabungan metode *signature based* dan *anomaly based* dalam mendeteksi serangan dalam jaringan. Metode *signature based* mempunyai kelebihan dalam mendeteksi serangan yang sudah mempunyai pola, sedangkan metode *anomaly based* mempunyai kelebihan dalam mendeteksi serangan yang belum diketahui polanya. Dengan menggabungkan kedua metode tersebut sebagai deteksi dalam serangan yang berbasis IDS dalam jaringan, maka dapat mendeteksi semua serangan baik yang mempunyai pola maupun yang belum mempunyai pola serangan. Berikut cara kerja metode *Signature Anomali Based* (SAB) :



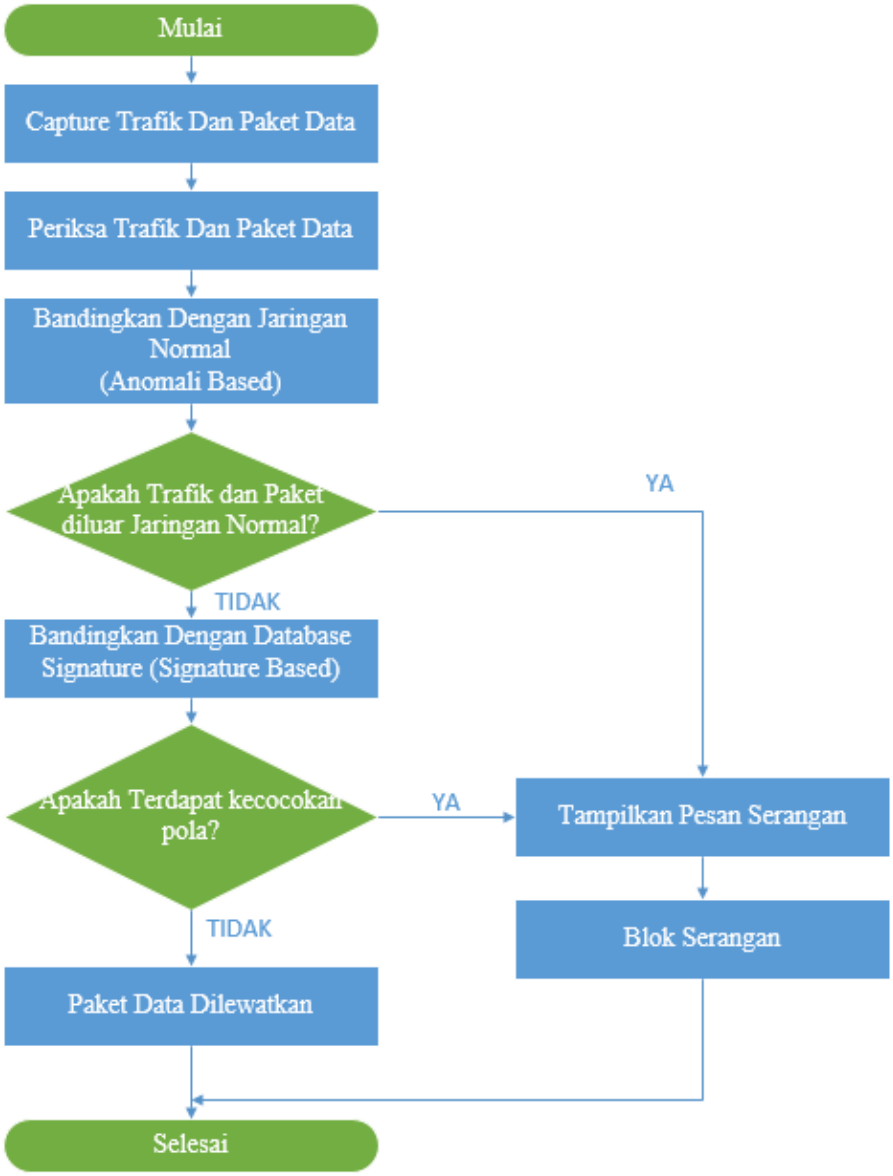
Gambar III-3 Cara Kerja SAB IDS

Berdasarkan gambar III-3, pendeteksian dan penanganan pada serangan dalam jaringan dengan menggunakan *Signature Anomali Based* dijelaskan sebagai berikut :

1. Paket data dan trafik data yang berada dalam jaringan tersebut akan dimonitor dan diperiksa dalam server IDS.
2. Server IDS akan memeriksa apakah trafik dan paket data dalam jaringan tersebut, jika terdapat kecocokan pola serangan atau trafik yang melebihi batas normal jaringan akan dideteksi sebagai sebuah serangan.
3. Jika terdapat serangan, maka IDS akan memunculkan pesan hal tersebut sebagai serangan yang dapat membahayakan. Pesan yang ditampilkan merupakan alamat, dan port sumber serangan.

Pada tahapan penggabungan metode *signature* dan *anomaly based* digunakan sebuah perangkat lunak yang digunakan yaitu Snort. Aplikasi ini dapat menerapkan kedua metode secara bersamaan digunakan dalam server IDS. Berikut diagram alir *Signature Anomaly Based* dalam gambar III-4.

Penempatan server IDS ini bersifat *network based*, dimana server IDS berfungsi untuk merekam dan mendeteksi setiap paket data dalam jaringan yang melewati *Ethernet* baik paket data yang menuju keluar maupun paket data yang akan menuju kedalam jaringan internal. Setiap paket data akan dilakukan *capture* data untuk melihat paket data yang akan dikirim atau yang akan diterima dari dalam maupun dari luar jaringan.



Gambar III-4 Diagram Alir Signature Anomali Based

Setelah paket data dilakukan *capture*, maka hasil proses *capture* data tersebut diperiksa isi header dan konten paket tersebut dengan menggunakan IDS yang berbasis *Signature Anomali Based* (SAB). Untuk tahapan yang berbasis *signature* paket tersebut akan dilakukan pencocokan baik header dan konten paket data tersebut dengan setiap rule yang ada dalam basis data IDS, jika ditemukan

kecocokan dalam pola paket data tersebut maka sistem akan memberikan pesan deteksi terjadi gangguan. Sedangkan untuk tahapan yang berbasis anomaly jaringan, paket tersebut akan dibandingkan dengan kondisi normal pada jaringan tersebut yang sudah didefinisikan sebelumnya dalam rule anomali. Jika terdapat kecocokan atau perbedaan antara kondisi paket data dengan jaringan normal maka sistem akan memberikan pesan deteksi gangguan.

3.4.1 Penentuan Baseline Jaringan Normal

Pada tahapan ini untuk melakukan implementasi penggunaan IDS dengan menggunakan metode Signature Anomali Based (SAB) diperlukan adanya pembangunan *baseline* jaringan normal. Pembangunan *baseline* ini digunakan untuk menentukan jaringan normal yang digunakan ketika IDS tidak mendeteksi adanya serangan. *Baseline* ini dijadikan sebagai acuan dalam membangun metode anomali yang akan digunakan. Penentuan *baseline* dilakukan dengan memperhatikan jaringan saat kondisi normal, dimana jaringan tidak ada ancaman dan serangan. Pengamatan data trafik jaringan digunakan sebagai dasar dalam menentukan metode anomali yang diterapkan, data trafik diambil sebagai acuan yang diperoleh dalam bulan - bulan tertentu ketika trafik tersebut mengalami kepadatan yaitu saat jaringan terpakai. Data dikelompokan berdasarkan rentang jam tertentu yaitu :

1. Jam tidak ada aktifitas kerja (00.00 – 07.00)
2. Jam aktifitas kerja (07.00 – 17.00)
3. Jam aktifitas rendah (17.00 – 00.00)

Berikut data trafik berdasarkan rentang jam ditunjukan tabel III-4 :

Tabel III-4 Data Trafik Jaringan

Waktu	Ukuran (GigaByte)
00.00 – 07.00	293.5
07.00 – 17.00	198.35
17.00 – 00.00	37.94

3.4.2 Penggunaan Rule Database Signature Serangan

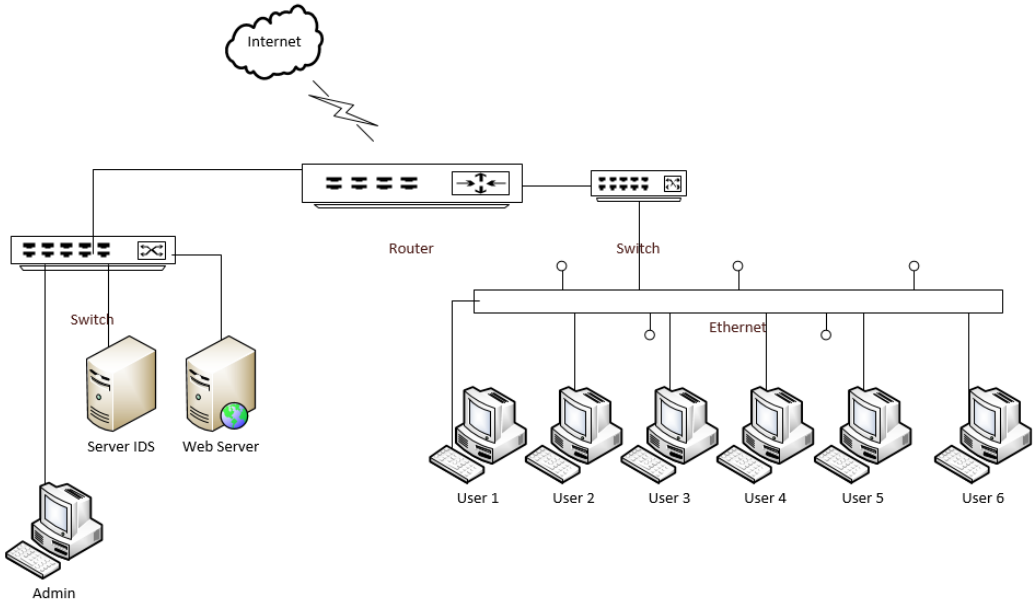
Dalam implementasi penerapan metode *Signature Anomaly Based* (SAB), maka diperlukan *rule database* yang berisi berbagai macam serangan yang sudah diketahui polanya sebagai data acuan untuk pencocokan setiap data yang akan dibandingkan. Untuk *rule* yang digunakan adalah dengan menggunakan database rule yang ada pada snort. *Rule* serangan yang digunakan menggunakan database rule snort dengan tipe snapshot 2.9.9.0. Tipe rule yang digunakan sesuai dengan tipe aplikasi snort yang akan diaplikasikan dalam memonitor jaringan.

3.5 Skenario Pengujian

Pada skenario pengujian IDS ini akan dilakukan simulasi percobaan serangan dengan melakukan beberapa aktifitas serangan dan gangguan diantaranya *icmp flood, udp flood, smurf attack, malware (trojan), syn attack,* dan *fin attack.* Serangan ini pada dasarnya merupakan suatu aktifitas dengan tujuan untuk menghentikan atau meniadakan layanan sistem jaringan sehingga pengguna tidak dapat mendapatkan layanan yang diinginkan.

Pada pengujian ini akan dilakukan percobaan untuk mendeteksi serangan dengan beberapa metode diantaranya *signature based, anomaly based,* dan *signature anomaly based*.

Dalam tahap skenario pengujian ini dengan menerapkan metode IDS seperti pada gambar III-5 :



Gambar III-5 Skenario Pengujian Signature Anomaly Based

Pada skenario pengujian ini, akan dilakukan aktifitas serangan dari pengguna menuju ke web server. Serangan ini dilakukan dengan menerapkan berbagai macam serangan yang sudah ditentukan sebelumnya. Pada sisi server telah dipasang berupa *intruder* yang menggunakan aplikasi snort untuk memonitor jaringan dengan menerapkan beberapa metode yaitu *anomaly based*, *signature based,* dan gabungan *signature anomaly based*. Admin dapat memonitor kejadian yang terjadi dan menerima peringatan jika terdapat serangan.

3.6 Pengukuran Kinerja IDS

3.6.1 Parameter Gangguan

Parameter gangguan yaitu meliputi pengujian sistem IDS terhadap gangguan yang diberikan. Melihat apakah IDS dapat mendeteksi setiap gangguan yang terjadi baik yang bersifat anomali jaringan maupun yang bukan anomali jaringan. Parameter gangguan yang diberikan yaitu :

- *UDP Flood*
- *ICMP Flood*
- *Smurf Attack*
- *Syn Attack*
- *Fin Attack*
- *Malware (Trojan)*

Serangan yang dilakukan dengan jumlah serangan pertama sebesar 2000 serangan. Kemudian, serangan ditambahkan secara terus menerus sampai mencapai 20000 serangan dengan interval kenaikan serangan sebesar 2000 serangan. Simulasi serangan tersebut, dilakukan selama kurang lebih 15 menit waktu penyerangan.

3.6.2 Parameter Responsi IDS

Parameter responsi IDS dilakukan untuk mengukur waktu yang dibutuhkan oleh IDS dalam mendeteksi gangguan yang terjadi baik gangguan yang mempunyai pola ataupun gangguan baru yang belum mempunyai pola. Respon waktu ini digunakan untuk melihat waktu yang dibutuhkan oleh setiap metode dalam merespon adanya ancaman yang dapat mengganggu jaringan.

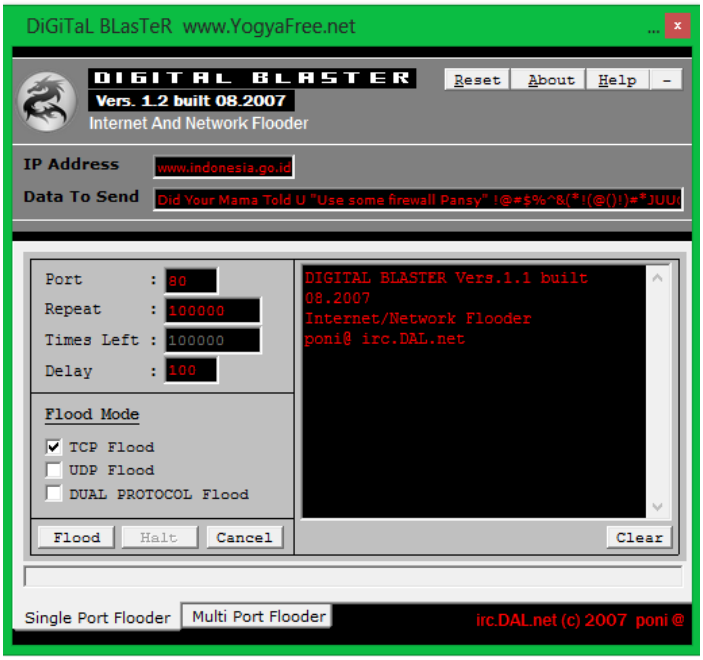
3.6.3 Parameter Komputasi

Pengukuran parameter komputasi ini dilakukan untuk mengetahui penggunaan sumber daya yaitu baik penggunaan processor maupun memori terhadap metode yang digunakan. Pengukuran ini dilakukan untuk melihat apakah metode IDS yang diterapkan mengkonsumsi jumlah sumber daya processor dan memori yang berlebih atau tidak.

3.6.4 Pengujian Serangan Dengan Digital Blaster

Digital blaster merupakan sebuah perangkat lunak yang dapat digunakan untuk memberikan gangguan dengan membanjiri sistem secara terus menerus. Pada digital blaster terdapat beberapa komponen yang dapat dijadikan pilihan untuk menentukan gangguan, diantaranya alamat IP tujuan, port yang akan digunakan, serta jumlah gangguan yang akan diberikan.

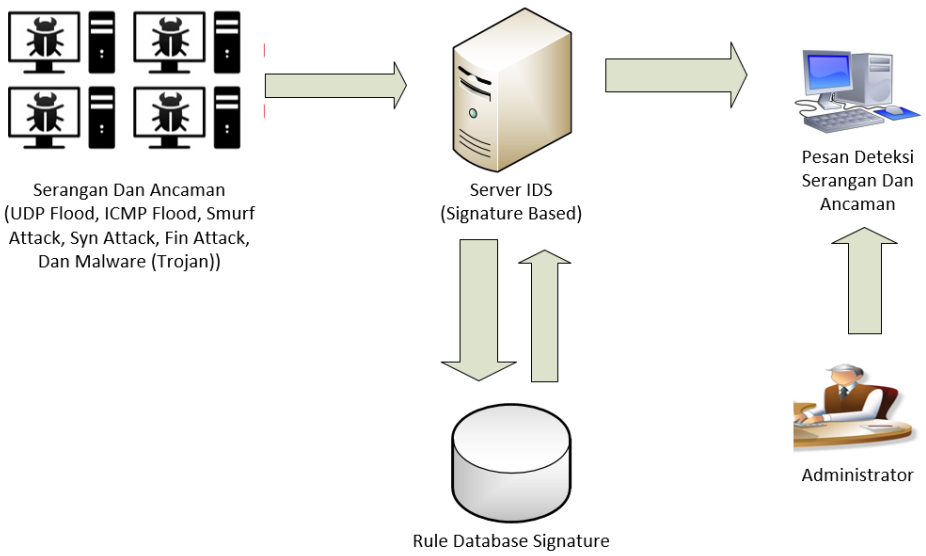
Pada pengujian ini akan digunakan Digital Blaster seperti pada gambar III-6 sebagai perangkat yang akan memberikan serangan dengan memberikan parameter alamat IP yang akan diberikan serangan, port tujuan, serta jumlah gangguan yang dapat diatur jumlah nya. Dalam pengujiannya, yang menjadi masukan pada Digital Blaster berupa alamat IP pada komputer target, data yang akan dikirimkan, port yang digunakan, jumlah serangan yang diberikan, dan jenis protokol yang digunakan.



Gambar III-6 Digital Blaster Untuk Gangguan

3.6.5 Pengujian Metode Signature Based

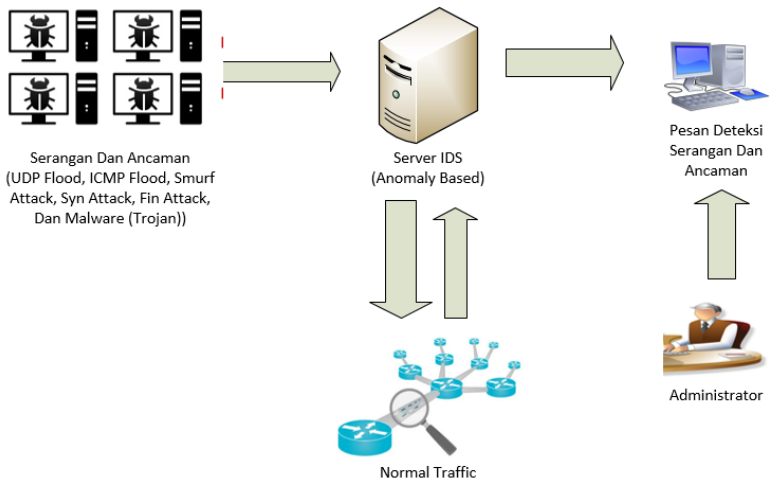
Pada pengujian dengan menggunakan metode *signature* based, akan dilakukan percobaan serangan atau gangguan berupa *udp flood*, *icmp flood*, *smurf attack*, *syn attack*, *fin attack*, dan *malware (trojan)*. Dari gangguan yang sudah diberikan terhadap metode tersebut akan dilakukan pengukuran deteksi gangguan, waktu deteksi yang dibutuhkan serta pemakaian sumber daya komputasi yang digunakan oleh metode *signature based*. Berikut penjelasan diagram skenario pengujian seperti ditunjukan pada gambar III-7:



Gambar III-7 Blok Skenario Pengujian Signature Based

3.6.6 Pengujian Metode Anomali Based

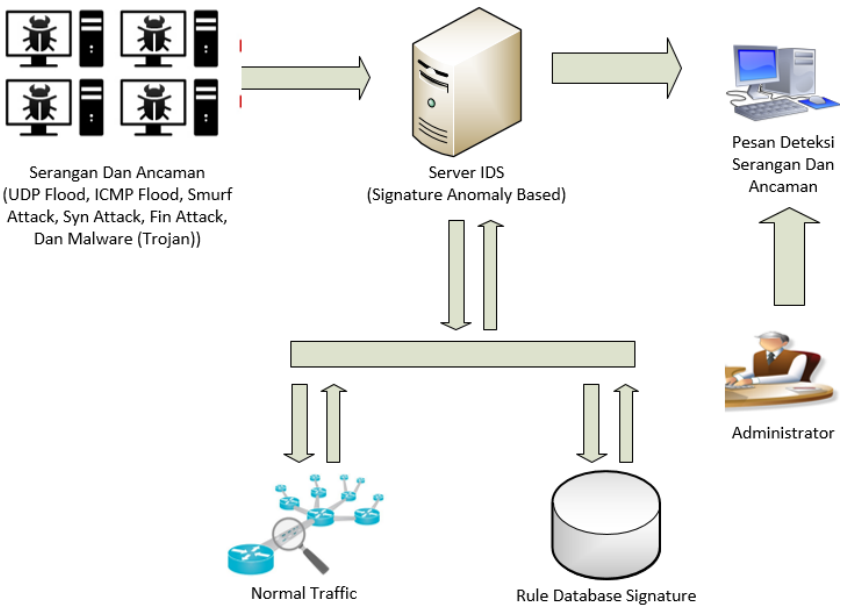
Pada pengujian dengan menggunakan metode *anomali* based, akan dilakukan percobaan serangan atau gangguan berupa *udp flood*, *icmp flood*, *smurf attack*, *syn attack*, *fin attack*, dan *malware (trojan)*. Dari gangguan tersebut, dilihat apakah metode *anomaly based* dapat mendeteksi serangan yang ada, berapa lama waktu yang dibutuhkan untuk mendeteksi dan seberapa besar sumber daya yang dibutuhkan untuk mendeteksi serangan tersebut. Berikut diagram skenario pengujian metode *anomaly based* pada server IDS :



Gambar III-8 Blok Skenario Pengujian Anomaly Based

3.6.7 Pengujian Metode Signature Anomali Based (SAB) IDS

Pada pengujian dengan menggunakan metode *signature anomaly based* akan dilakukan percobaan serangan atau gangguan dengan gangguan berupa *udp flood, icmp flood, syn attack, fin attack* dan *malware (trojan)*. Bagaimana metode SAB tersebut dapat mendeteksi gangguan yang diberikan serta membutuhkan waktu berapa lama metode tersebut mendeteksi adanya gangguan tersebut. Selain mengukur waktu deteksi juga akan dilakukan pengukuran penggunaan sumber daya komputasi yang dipakai oleh metode SAB. Berikut blok skenario pengujian SAB IDS :



Gambar III-9 Blok Skenario Pengujian SAB IDS

3.7 Teknik Analisis Data

Dalam penelitian ini, akan diberikan sejumlah serangan yang sudah ditentukan dari pengguna menuju web server. Selanjutnya server IDS akan mencatat setiap aktifitas serangan yang terjadi, selain mencatat aktifitas serangan server juga akan dilihat penggunaan terhadap sumber daya komputasi yang digunakan pada saat mendeteksi adanya serangan. Data aktifitas serangan serta penggunaan sumber daya komputasi yang deiperoleh akan disajikan dalam bentuk tabular dan grafik dengan penyajian berupa :

1. Jumlah serangan dengan persentase serangan yang terdeteksi.
2. Jumlah serangan dengan persentase penggunaan memori.
3. Jumlah serangan dengan persentase penggunaan processor.