BAB III
ANALISIS DAN PERANCANGAN SISTEM

3.1. Analisis Sistem

Analisis sistem adalah proses meneliti dan mencari informasi untuk mendapatkan sebuah data mengenai peningkatan keamanan jaringan yang ada di Universitas Sahid Surakarta. Analisis sistem ini adalah langkah awal untuk peningkatan keamanan jaringan yang ada di Universitas Sahid Surakarta sebagai penggambaran struktur jaringan komputer yang ada di Universitas Sahid Surakarta.

Analisis ini ditekankan pada struktur jaringan komputer serta keamanannya yang akan menjadi topik utama dalam penelitian ini. Dalam hal analisis tersebut akan mencangkup *hardware*, *software*, struktur dan cara kerja dari jaringan serta keamanannya. Dalam hal peningkatan keamanan jaringan sehingga dibutuhkan sebuah langkah awal untuk menggali informasi yang berhubungan langsung terhadap jaringan beserta keamanannya sehingga hal tersebut dapat mengetahui cara kerja jaringan dan keamanan jaringan yang ada di Universitas Sahid Surakarta.

Analisis sistem yang ada di Universitas Sahid Surakarta dilakukan dengan berapa metode untuk mengetahui informasi yang berhubungan dengan keamanan jaringan yang diterapkan di Universitas Sahid Surakarta apakah pengamanan perlu dilakukan ataupun sudah baik, sehingga dibutuhkan suatu penelitian yang jeli untuk mendapatkan informasi yang tepat dan dapat dilakukan suatu tindakan pengamanan jaringan yang baik dan sesuai untuk diterapkan di Universitas Sahid Surakarta. Metode yang digunakan yaitu metode observasi, wawancara, dan pengambilan contoh (*sample*) melalui pengguna jaringan yang ada di Universitas Sahid Surakarta. Dari beberapa metode tersebut sehingga mendapatkan sebuah gambaran dan kesimpulan dari sistem jaringan komputer dan keamanan jaringan yang ada di Universitas Sahid Surakarta.

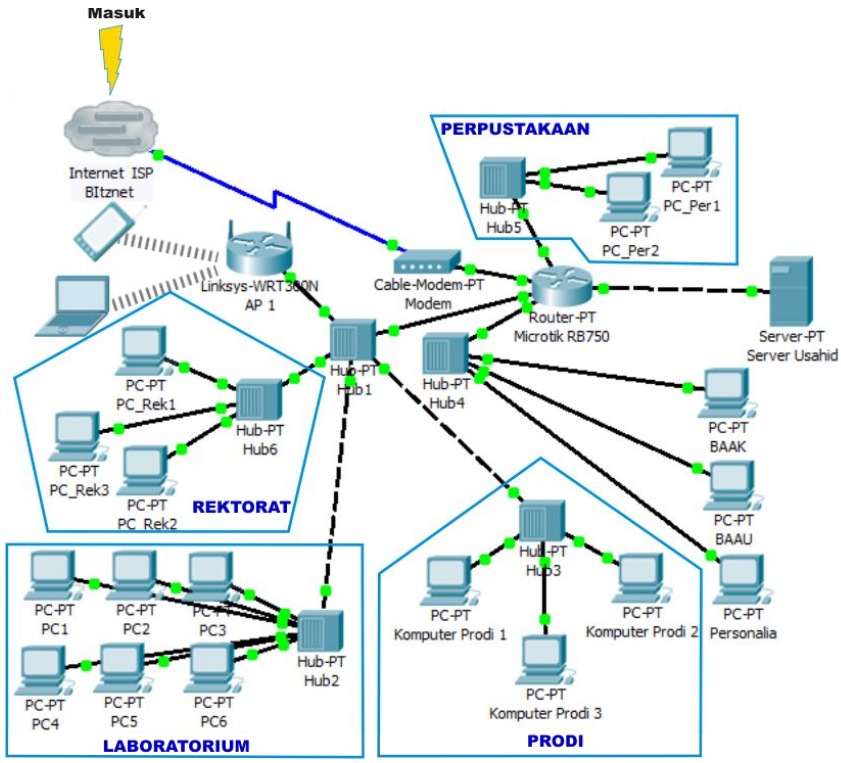
3.1.1. Analisis Sistem Yang Berjalan Saat Ini

3.1.1.1. Analisis Relasi *Hardware* dan Struktur Jaringan Komputer

Saat ini Universitas Sahid Surakarta menerapkan sistem jaringan terpusat dengan satu *server* yaitu pada *router* Mikrotik RB750. *Router* Mikrotik RB750 memiliki lima *port* LAN *suport* konektor RJ 45. Dimana pada *port* pertama sebagai jalur masuk akses internet, satu *port* ke *server* dan 3 *port* lainnya untuk keluar (*output)* ke jaringan lokal di Universitas Sahid Surakarta seperti pada Gambar 3.1.

Tiga *port* keluar (*output)* di *router* Mikrotik RB750 tersambung ke HUB sehingga jaringan komputer tersebut dapat memiliki jumlah pengguna yang banyak. Selain itu dari output dari *router* Mikrotik RB750 tersebut tersalurkan ke *acces point* sehingga pengguna tidak hanya jaringan LAN tetapi pengguna dapat memanfaatkannya melalui jaringan *wireless* (WIFI) .

Setiap HUB tersebut berperan menyalurkan jaringan ke setiap bagian pengguna jaringan LAN , yang diantaranya bagian rektorat, akademik, keuangan, prodi dan *laboratorium* komputer yang ada di Universitas Sahid Surakarta.



Gambar 3.1 Struktur Perangkat Keras dan Jaringan di Usahid

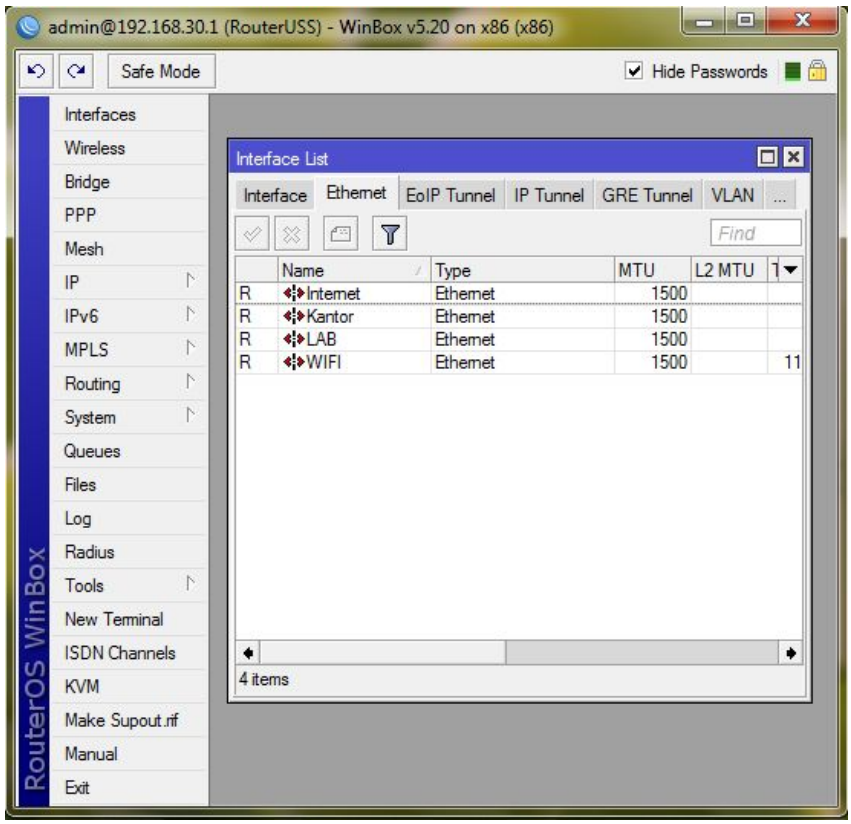
Berikut keterangan dari Gambar 3.1 yang menggambarkan struktur dan jalur jaringan yang ada di Universitas Sahid Surakarta, awal dari proses masuknya jaringan di Universitas Sahid Surakarta yaitu dari ISP yang bernama *Biznet* yang memberikan *bandwidth* sebesar 15 Mbps ke *router* Universitas Sahid Surakarta melalui *converter* (pengubah media transmisi basis kabel *fiber optic* ke jaringan berbasis kabel UTP) dari *router* Universitas Sahid Surakarta yang berperan sebagai pusat jaringan di Universitas Sahid Surakarta (*server*) akan didistribusikan ke setiap bagian-bagian yang membutuhkan pasokan jaringan internet yaitu sebagai pengguna jaringan maupun internet.

3.1.1.2. Analisis *Software*

Jaringan di Universitas Sahid Surakarta adalah jaringan yang berbasis jaringan terpusat, sehingga pusat atau *server* terletak pada *router* Mikrotik RB750. *Software* yang digunakan untuk mengatur atau setting *router* atau *server* tersebut adalah Winbox, peran Winbox ini adalah untuk mengatur *router* atau *server* dengan pengaturan atau *setting* secara umum. Dalam penelitian ini menggunakan Winbox versi 2.2.16 dengan tampilan seperti Gambar 3.2.

Gambar 3.2 Aplikasi Winbox v2.2.16

Aplikasi Winbox ini mempunyai fasilitas atau menu untuk pengaturan atau *setting* jaringan yang ada di Universitas Sahid Surakarta secara umum. Fasilitas atau menu yang disediakan oleh Winbox v2.2.16 ini diantaranya *interface*, *wireless*, IP, *Routing* dan lainnya, dapat dilihat pada Gambar 3.3.



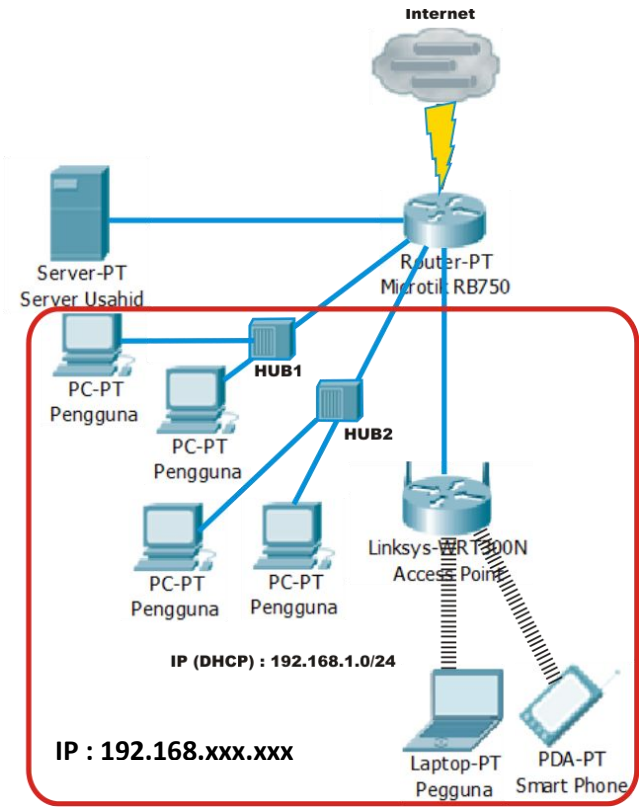
Gambar 3.3 Fasilitas atau Menu Pada Winbox V2.2.16

3.1.1.3. Analisis Jaringan Internet dan Keamanannya

Jaringan internet yang masuk melalui *router* Mikrotik RB750 sehingga akan disalurkan melalui 3 *port output* yang akan disalurkan ke *hardware* pendukung seperti HUB dan *acces point*. Kecepatan internet yang dimiliki Universitas Sahid Surakarta sebesar 15 Mbps dengan jumlah pengguna sekitar 90 jaringan LAN dan 40 melalui jaringan WIFI.

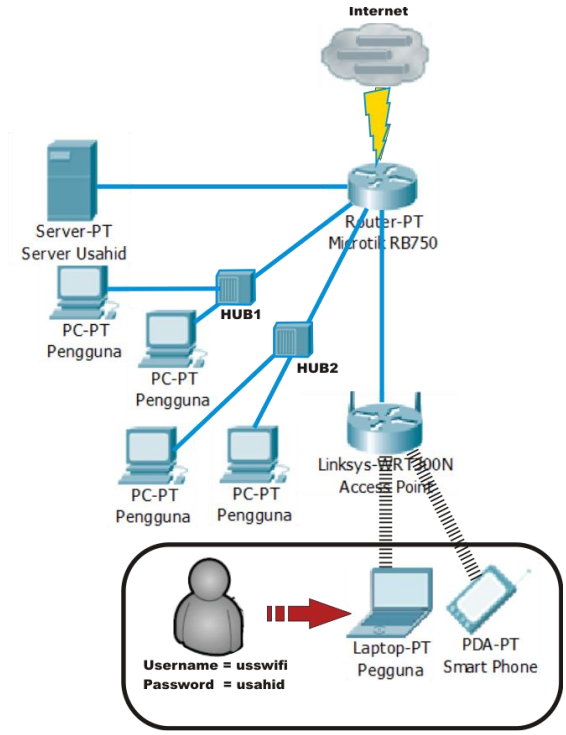
Penerapan keamanan jaringan yang ada di Universitas Sahid Surakarta untuk jaringan LAN menggunakan IP secara DHCP seperti desain Gambar 3.4, untuk pengguna WIFI harus melalui tahap pengamanan dengan memasukan *username*

dan *password* dapat dilihat pada Gambar 3.5. Sifat *password* tersebut bersifat umum dan setiap orang di lingkungan Universitas Sahid Surakarta berhak mengetahui *username* dan *password* tersebut.



Gambar 3.4 Desain Penggunaan IP Address

Sistem *login* melalui *username* dan *password* yang berlaku untuk pengguna melalui jaringan WIFI yang memiliki satu jumlah akun masuk yaitu dengan *username* "usswifi" dengan *password* "usahid" seperti Gambar 3.5, sehingga pengguna WIFI berhak mendapatkan akses internet yang sama, sehingga dari hak akses tersebut menjadi celah untuk melakukan penyalahgunaan. Pada celah tersebut sehingga perlu pengamanan yang harus ditingkatkan supaya jaringan di Universisitas Sahid Surakarta tidak memiliki kendala pada keamanan jaringan maupun akses internetnya.



Gambar 3.5 Desain Penggunaan Pengamanan Jaringan Melalui *Username* dan *Password*

3.1.1.4. Sistem Kerja Jaringan Komputer Yang Sedang Berjalan

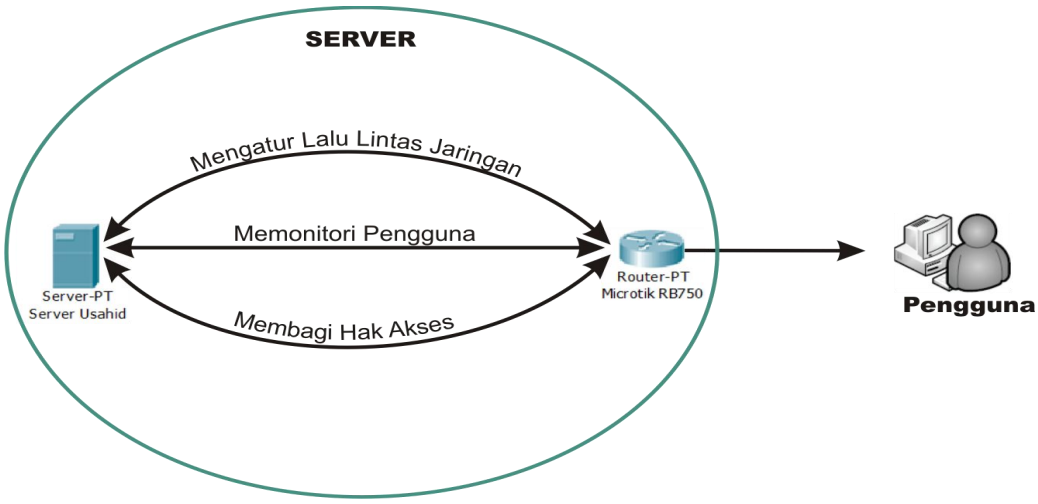
Berdasarkan pengamatan jalur jaringan komputer yang ada di Univesitas Sahid Surakarta mulai dari penerima sinyal dari ISP sampai pengguna internetnya maka desain seperti pada Gambar 3.1 dan menerapkan sistem pengamanan pada penggunanya seperti Gambar 3.5. Jaringan pada Universitas Sahid Surakarta dalam penerapannya menggunakan sistem jaringan terpusat yaitu pada *router* Mikrotik RB750 yang berperan sekaligus sebagai *server* pengendali jaringan yang ada didalam Universitas sahid Surakarta.

Dalam penerapan jaringan yang sudah ada tersebut dapat dikembangkan atau ditingkatkan dalam segi pengamanan jaringan sehingga proses kerja jaringan yanga ada di Universitas Sahid Surakarta jauh dari gangguan penyalahgunaan hak akses dan mencari sistem yang sesuai dan dapan diterapkan di Universitas Sahid Surakarta dan sesui dengan infrastruktur jaringan yang ada sehingga dengan pemanfaatkan alat yang sudah ada.

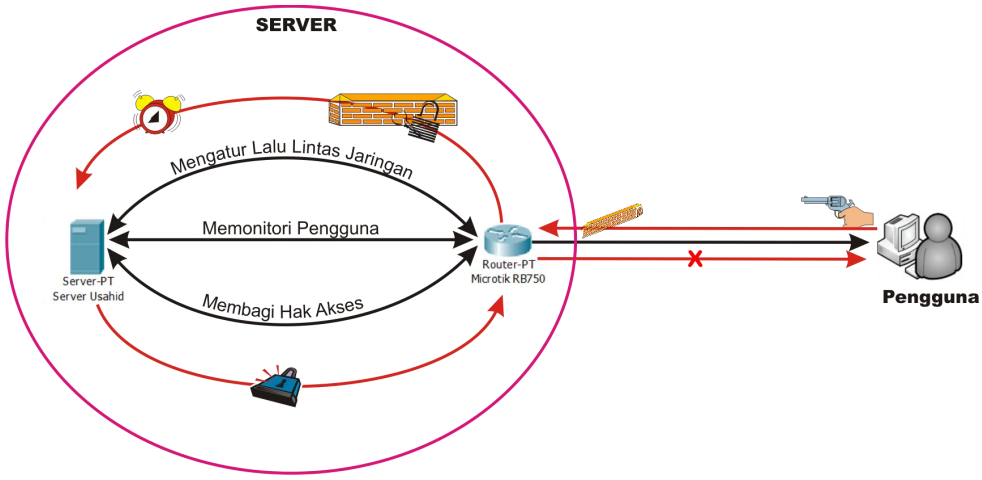
3.1.2. Analisis Sistem Yang Baru

Berdasarkan analisis pada sistem yang sedang berjalan saat ini yang dilakukan sehingga perlu peningkatan pengamanan jaringan yang ada di Universitas Sahid Surakarta melalui *server* jaringannya. Peningkatan pengamanan ini bertujuan untuk menghindari penyalahgunaan hak akses dan penyerangan, penyerangan disini dimaksutkan penyerangan dengan meminta atau memberi banyak serangan (*threads*) dalam waktu yang bersamaan pada jaringan yang ada di Universitas Sahid Surakarta, hal ini menggunakan sistem yang sesuai sesuai dengan infrastuktur jaringan yang ada di Universitas Sahid Surakarta. Hasil penelitian tersebut maka jaringan yang ada di Universitas Sahid Surakarta perlu peningkatan pengamanan yang dapat dilakukan pada *server* jaringan yang ada.

Fungsi *server* sendiri adalah sebagai pusat tujuan dari user-usernya atau komputer yang menggunakan fasilitas jaringan yang melewati *server* tersebut, selain itu *server* berperan sebagai pengontrol atau pengatur lalu lintas maupun jalur jaringan yang melaluinya seperti pada Gambar 3.6. Dari fungsi tersebut dapat dimanfaatkan untuk melakukan pengamanan atau menambahkan fungsi *firewall* didalamnya seperti pada Gambar 3.7.



Gambar 3.6 Fungsi dan Peran *Server*

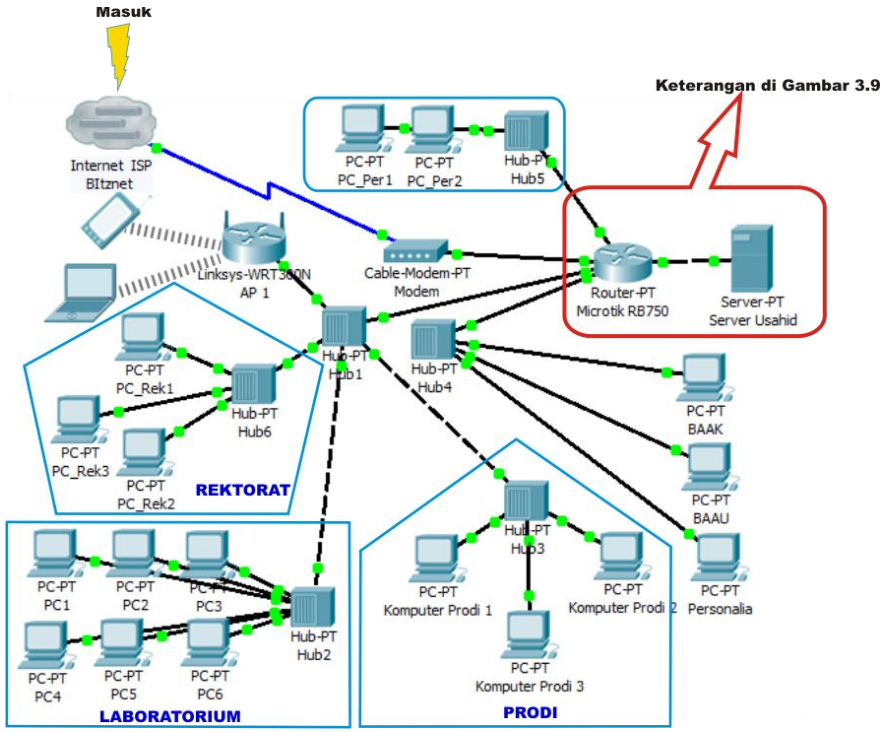


Gambar 3.7 Penambahan *Firewall* dan *Alert*

Gambar 3.7 menjelaskan bahwa fungsi dari *router* RB750 dapat ditambahkan fungsinya sebagai *firewall*, dimana fungsi peran *firewall* pengamanan dari *router* RB750 (*server*) yaitu sebagai pengamanan jaringan lokal yang ada di Universitas Sahid Surakarta dengan cara kerja apabila ada sebuah serangan atau *intrusion* yang otomatis akan melalui *firewall* yang ada pada *router* RB750 dan akan memberi peringatan kepada komputer *server* jika telah terjadi *intrusion* atau serangan, komputer *server* akan memberi pengaturan atau perintah ke *router* RB750 untuk melakukan pemutusan hak aksesnya, sehingga serangan tersebut berhenti dan jaringan tersebut akan normal kembali. Setiap pemberian tindakan tersebut tergantung pada komputer *server* memberikan tindakan apakah akan di putus hak akses seterusnya atau penurunan kecepatan akses.

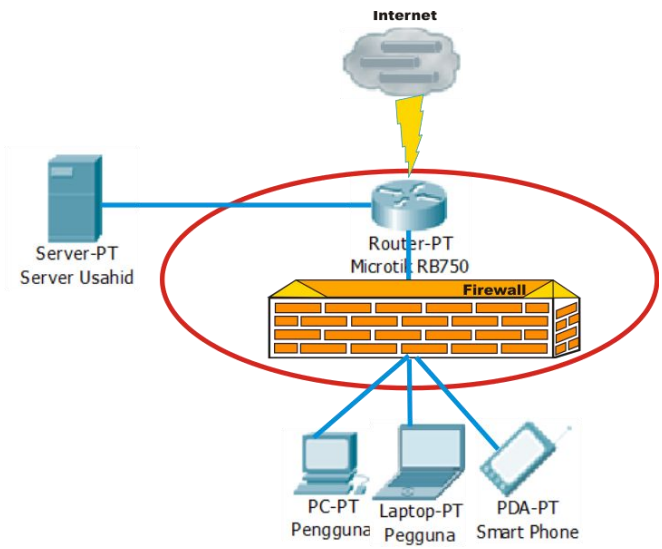
3.1.2.1. Analisis *Hardware* dan Struktur Jaringan Yang Baru

Penggunaan perangkat keras (*software*) pada sistem yang baru ini tidak memerlukan tambahan, melainkan memaksimalkan fungsi kerja dari alat tersebut untuk membuat sebuah pengamanan jaringan yang bersifat *intrusion detection system* yang berfungsi sebagai pendeteksi serangan dari *user* atau pengguna yang bertujuan untuk melemahkan fungsi *hardware* jaringan maupun memperlambat kinerja jaringan yang ada di Universitas Sahid Surakarta. Pemaksimalan *hardware* berada pada *router* Mikrotik RB750 seperti pada Gambar 3.8 yang menjelaskan *router* dimaksimalkan fungsinya sebagai *firewall* jaringan lokalnya.



Gambar 3.8 Struktur Perangkat Keras dan Jaringan di Usahid Yang Baru

Pemaksimalan fungsi *router* Mikrotik RB750 seperti Gambar 3.8 menunjukan bahwa *router* sebagai pusat pada jaringan lokal terhadap jaringan luar sehinga dapat difungsikan sebagai *firewall* untuk jaringan lokal dengan penjelasan lebih lanjut pada Gambar 3.9.



Gambar 3.9 Sistem Pada *Router* atau *Server*

Gambar 3.9 diatas menjelaskan bahwa fungsi *router* Mikrotik RB750 sebagai *firewall*, dimana *firewall* tersebut membatasi jalur akses *user* atau pengguna untuk mengakses jaringan melalui *router* tersebut sehinga *user* atau pengguna tersebut sebelum mengakses keluar dari jaringan lokal akan diteliti atau diperiksa oleh *firewall* apakan *user* atau pengguna tersebut melakukan sebuah serangan atau tidak.

3.1.2.2. Analisis Kebutuhan *Software* Pada Sistem Yang Baru

3.1.2.2.1. Snort dan IDScenter

Snort adalah aplikasi yang digunakan untuk mendeteksi atau mengendus suatu penyalahgunaan melalui kejanggalan-kejanggalan yang terjadi saat penyerang melakukan penyerangan. Laporan pendeteksian berupa *port*, IP, jalur akses (UDP, TCP, HTTP). Memiliki tampilan depan seperti gambar 3.10.

Gambar 3.10 Aplikasi Snort

Penerapan IDScenter ini digunakan untuk mendeteksi dan memberikan tindakan kepada pelaku penyerangan melalui jaringan. *Alert* pendeteksian dan pemberian tindakan harus dilakukan setting pada menu yang ada pada menu dan IDScenter *General* (konfigurasi umum), *Alert* (pengaturan pemberian peringatan), *Wizard (*konfigurasi letak *rule*), *Logs* (menyimpan *rule* dan aktivitas), *Rule* (menentuan dan memasukkan *rule*) dan *Explorer* (memperlihatkan hasil) pada menu untuk *Action Start* Snort (memulai Snort), *View Alert* (melihat peringatan), *Reset Alert* (atur ulang peringatan), *Test Alert* (mencoba fungsi peringatan),

Reload (memproses ulang) dan *Apply* (penerapan), tampilan dan menu dapat dilihat pada Gambar 3.11.

Gambar 3.11 Menu-menu Pada IDScenter

3.1.2.2.2. WinPcap

WinPcap adalah aplikasi berperan untuk penangkapan IP dan paket data yang lewat melalui atau menuju *router* atau *server* dan dapat di laporkan melalui Snort. WinPcap adalah aplikasi yang berada pada belakang layar dan tidak dapat di tampilkan karena sifat aplikasi ini berupa *platform* perekam yang berada pada *port* jaringan.

3.1.2.2.3. Winbox

Kebutuhan *software* yang berupa aplikasi untuk mengatur atau setting *router* tetap menggunakan Winbox dengan versi sama yaitu versi 2.2.16 dimana fungsi Winbox telah dijelaskan pada pembahasan **3.1.1.2**. selain dari fungsi tersebut, Winbox untuk *setting router* Mikrotik RB750 dapat dimaksimalkan sebagai bentuk pengamanan dan memonitori jaringan yang sedang berjalan di Universitas Sahid Suarakarta.

3.2. Perancangan Sistem

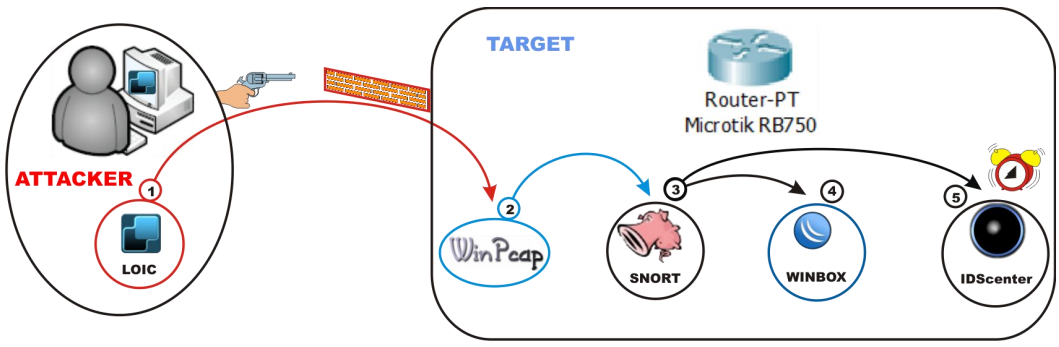
3.2.1. Perancangan Sistem Yang Akan Diterapkan

Perancangan sistem dimaksudkan untuk mengetahui cara kerja pengamanan dengan melakukan sebagai tindakan pengamanan dari proses terjadinya

penyerangan hingga cara penanganannya. Perancangan sistem ini dilakukan untuk memberikan gambaran dan struktur alur proses pengamanannya. Dari proses perancangan ini akan diterapkan pada sistem jaringan yang ada di Universitas Sahid Surakarta sebagai bentuk peningkatan keamanan jaringan berbasis *intrusion detection system.*

3.2.2. Cara Kerja Pengamanan Jaringan

Pengamanan dilakukan pada saat terjadi sebuah *intrusion* dimana dalam *intrusion* tersebut seorang *attacker* melakukan penyerangan dengan target *server* (*router*) dalam penyerangan tersebut bertujuan untuk melemahkan kinerja atau membebani *router* tersebut dengan memberikan sebuah *threads* dengan jumlah tertentu atau dapat dikatakan banyak dengan waktu yang bersamaan, sehingga fasilitas ataupun kinerja dari *router server* tersebut terhambat ataupun menurun kinerjanya, pada dasar permasalahan tersebut sehingga perlunya sebuah penanganan yang terletak pada *router atau server* tersebut dengan menggunakan aplikasi yang dapat membantu kinerja *router* sebagai alat pengamanan dari sebuah *intrusion* yang bersal dari *attacker* seperti pada Gambar 3.12.



Gambar 3.12 Alur Proses Penyerangan Hingga Penangananya

Pada gambar 3.12 diatas menggambarkan alur proses enyerangan hingga penanganan pada target penyerangan (pada jalur proses nomor 1) menggambarkan aplikasi Loic yaitu aplikasi untuk melakukan penyerangan oleh seorang pengguna yang berperan sebagai *attacker* dengan target *router* Mikrotik Rb750 dimana yang berperan sebagai *server* jaringan yang ada di dalam

Universitas Sahid Surakarta, kemudian pada target penyerangan yaitu *router* atau *server* akan melakukan sebuah penanganan penyerangan atau tahap antisipasi dengan menggunakan metode perekaman IP yang dilakukan oleh aplikasi WinPcap (pada jalur proses nomor 2). Hasil perekaman akan dibawa atau di masukan ke aplikasi Snort (pada jalur proses nomor 3) dimana Snort akan berfungsi sebagai penghitung jumlah IP yang masuk dan seberapa sering IP yang sama tersebut melintas atau menuju *router* atau *server*.

Proses dari aplikasi Snort akan terlihat bahwa seberapa cepat dan banyaknya sebuah arus jaringan yang melintas atau menuju pada *router* atau *server* sehingga laporan perekaman dan penghitungan akan disimpan pada *rule* Snort dan mengetahui jalur yang dilintasi oleh penyerang atau *attacker*, dari laporan tersebut aplikasi digunakan untuk melihat berapa besaran permintaan dan nomor IP yang melakukan penyerangan, sehingga dapat ditindaklanjuti akan di proses atau diberi tindakan pemutusan akses atau penurunan kecepatan *bandwidth* yng diberikan kepada IP *attacker*.

Tindak pengamanan dapat dilakukan dengan dua cara yaitu melalui Winbox *(*pada jalur proses nomor 4) atau menggunakan aplikasi IDScenter (pada jalur proses nomor 5). Aplikasi Winbox tersebut sudah dapat dilakukan penanganan penyerangan tetapi pada aplikasi Winbox tersebut harus dilakukan secara manual atau penanganan langsung pada *router* atau *server* yang ada tersebut dengan melakukan tindakan penghentian akses IP yang diinginkan, sehingga proses tersebut membutuhkan tenaga manusia yang harus siap siaga pada *router* atau *server* untuk melakukan tindakan pengamanan saat terjadi penyerangan, sehingga dari permasalahan tersebut harus ditambahkan aplikasi dengan fungsi melakukan pengamanan secara otomatis atau berjalan sendiri pada sistem *router* atau *server* tersebut.

Aplikasi yang tepat untuk penganganan *intrusion* tersebut adalah IDScenter (pada jalur proses nomor 5) dimana fungsi IDScenter ini akan memberikan peringatan pada saat terjadi penyerangan atau diduga sebagai *intrusion* berdasarkan IP yang melewati *router* atau *server* tersebut sehingga jika seorang *administrator* atau *operator server* dapat melakukan sebuah tindakan, IDScenter

juga dapat memberikan sebuah tindakan otomatis atau berjalan sendiri saat terjadi sebuah penyerangan atau diduga *intrusion* berdasarkan seberapa sering dan berapa besar sebuah IP melewati atau menuju *router* tersebut.

Cara kerja IDScenter yang secara otomatis ini dapat memberikan tindakan kepada IP yang melakukan penyerangan atau diduga *intrusion* tersebut akan dilakukan pemutusan akses seterusnya atau dapat dilakukan pemutusan selama waktu yang ditentukan dan akan tersambung lagi aksesnya dalam waktu tertentu.