ANALISIS dan IMPLEMENTASI MENCEGAH VIRUS MALWARE PADA JARINGAN DENGAN METODE BLOCKING PORT MENGGUNAKAN MIKROTIK

SKRIPSI

Oleh:
Christophorus Heru M
130210032

PROGRAM STUDI TEKNIK INFORMATIKA
UNIVERSITAS PUTERA BATAM

ANALISIS dan IMPLEMENTASI MENCEGAH VIRUS MALWARE PADA JARINGAN DENGAN METODE BLOCKING PORT MENGGUNAKAN MIKROTIK

SKRIPSI
Untuk memenuhi syarat
guna memperoleh gelar Sarjana

Oleh:
Christophorus Heru M
130210032

PROGRAM STUDI TEKNIK INFORMATIKA
UNIVERSITAS PUTERA BATAM
2018

ANALISIS dan IMPLEMENTASI MENCEGAH VIRUS MALWARE PADA JARINGAN DENGAN METODE BLOCKING PORT MENGGUNAKAN MIKROTIK

SKRIPSI
Untuk memenuhi syarat
guna memperoleh gelar Sarjana

Oleh:
Christophorus Heru M
130210032

PROGRAM STUDI TEKNIK INFORMATIKA
UNIVERSITAS PUTERA BATAM
2018

PERNYATAAN

Dengan ini saya menyatakan bahwa:

1. Skripsi ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (sarjana, dan/atau magister), baik di Universitas Putera Batam maupun di perguruan tinggi lain.

2. Skripsi ini adalah murni gagasan, rumusan, dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing.

3. Dalam skripsi ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan oranglain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.

4. Pernyataan ini saya buat dengan sesungguhnya dan apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di perguruan tinggi.

Batam, 5 Agustus 2019

Yang membuat pernyataan,

Christophorus Heru M
130210032

ANALISIS dan IMPLEMENTASI MENCEGAH VIRUS MALWARE PADA JARINGAN DENGAN METODE BLOCKING PORT MENGGUNAKAN MIKROTIK

Oleh
Christophorus Heru M
130210032

SKRIPSI
Untuk memenuhi salah satu syarat
guna memperoleh gelar Sarjana

Telah disetujui oleh Pembimbing pada tanggal
Seperti tertera di bawah ini

Batam, 5 Agustus 2019

Cosmas Eko Suharyanto, S.Kom.,M.MSI.
Pembimbing

ABSTRAK

Jaringan komputer sudah menjadi kebutuhan pokok di berbagai bidang, yang terhubung ke *internet* akan memperbesar kemungkinan terjadinya ancaman atau gangguan terhadap keamanan sistem. Kurangnya pengetahuan dari pengguna komputer terhadap masalah keamanan sistem menjadi salah satu penyebab timbulnya masalah terhadap komputer, sering dijumpai komputer yang program anti virusnya tidak di *update,* atau bahkan tidak dilengkapi dengan program anti virus sama sekali. Hal tersebut menyebabkan komputer atau *host* dapat terinfeksi *malware* tanpa sepengetahuan dari pengguna. Kemudian malware tersebut dapat menyebar ke komputer lainnya dalam jaringan, dan pada akhirnya dapat merugikan banyak pihak. *Malicious Software* (*malware)* adalah program yang diciptakan dengan tujuan mencari kelemahan atau bahkan merusak *software* serta sistem operasi komputer, mereka dapat masuk melalui *port-port* terbuka yang tidak digunakan dalam jaringan. Setelah penulis melakukan observasi di Sekolah Charitas Batam dan melakukan studi pustaka dari berbagai sumber, maka dibutuhkan Router Mikrotik untuk mencegah hal tersebut serta *Honeypot Dionaea* sebagai alat bantu deteksi *malware* pada jaringan lokal. Penelitian ini bertujuan untuk membangun sistem keamanan jaringan komputer dengan metode *blocking port* di Sekolah Charitas Batam dengan menggunakan metode penelitian observasi, studi pustaka dan analisis. Setelah selesai penelitian ini, maka sistem keamanan jaringan Sekolah Charitas Batam dapat memaksimalkan kinerja sistem, mencegah masuknya *Malicious Software* (*malware).*

Kata kunci : Malware, Block port, Honeypot, Dionaea

ABSTRACT

Computer networks have become a major requirement in various fields, which is connected to the internet will increase. Lack of knowledge about computer users regarding system security problems is one of the causes of problems with computers, often found computers whose anti-virus programs are not updated, or even not equipped with anti-virus programs at all. This causes the computer or host to use malware without the user's knowledge. Malware can then spread to other computers in the network, and in the end can affect many parties. Malicious Software (malware) is a program created with the aim of finding weaknesses or damaging software and computer operating systems, they can enter through open ports that are not used in the network. After the author made observations at the Batam Charitas School and conducted a literature study from various sources, it would require a Router Router to prevent this and Honeypot Dionaea as a tool for detecting malware on the local network. This study aims to build a computer network security system by blocking the port at Batam's Charitas School by using observational research, library research and analysis. After completing this research, the Batam Charitas School security system can maximize the system, preventing the entry of Malicious Software (malware).

Keywords: Malware, Block Port and ,Honeypot Dionaea

KATA PENGANTAR

Puji dan syukur kepada Tuhan Yang Maha Esa yang telah melimpahkan segala rahmat dan karuniaNya, sehingga penulis dapat menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Program Studi Teknik Informatika Universitas Putera Batam.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati.

Dengan segala keterbatasan, penulis menyadar, bahwa skripsi ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Rektor Universitas Putera Batam.
2. Ketua Program Studi Andi Maslan, S.T., M.SI.
3. Bapak Cosmas Eko Suharyanto, S.Kom.,M.MSI. selaku pembimbing Skripsi pada Program Studi Teknik InformatikaUniversitas Putera Batam.
4. Dosen dan Staff Universitas Putera Batam.
5. Ibu, Adik, dan seluruh keluarga yang telah memberikan semangat serta dukungannya.
6. Alm. Ayah yang telah mendukung saya selama 4 semester semasa hidupNya sebelum beliau pergi menghadap sang pencipta Allah Bapa di Surga.

7. Rekan Mahasiswa yang telah memberikan saran dan informasi. Semoga Tuhan Yang Maha Esa membalas kebaikan dan selalu mencurahkan rahmat dan kasihnya, Amin.

Batam, 5 Agustus 2019

Christophorus Heru M

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

1.1 Latar Belakang

Jaringan komputer sudah menjadi fasilitas yang sangat penting di berbagai bidang. yang terhubung ke *internet* akan memperbesar kemungkinan terjadinya ancaman atau gangguan terhadap keamanan sistem jaringan. *Malicious Software* (*malware)* adalah program yang diciptakan dengan tujuan mencari kelemahan atau bahkan merusak *software* serta sistem operasi komputer (Mada R. Perdhana, 2011). *Malware* dalam bentuk *virus, trojan, worm*, atau memasang *backdoor* merupakan ancaman utama bagi keamanan sistem jaringan komputer. Kurangnya pengetahuan dari pengguna komputer terhadap masalah keamanan sistem menjadi salah satu penyebab timbulnya masalah terhadap komputer. sering dijumpai komputer yang program anti virusnya tidak di *update*, atau bahkan tidak dilengkapi dengan program anti virus sama sekali. Hal tersebut menyebabkan komputer atau *host* dapat terinfeksi *malware* tanpa sepengetahuan dari pengguna. Kemudian malware tersebut dapat menyebar ke komputer lainnya dalam jaringan, dan pada akhirnya dapat merugikan banyak pihak. *Malware* dan serangan dari luar dapat masuk melalui *port – port* terbuka yang tidak digunakan dalam sistem jaringan.

Teknik pengamanan jaringan biasanya dengan *memblokade* serangan dengan mendeteksi serangan yang ada dengan IDS. Selain menggunakan cara konvensional tersebut, pengamanan sistem jaringan dapat dibantu dengan menggunakan *Honeypot* untuk mendeteksi *malware* pada jaringan kemudian dilakukan metode *blocking port* atau lebih dikenal dengan istilah *firewall filter*. Dengan menggunakan metode ini seorang pengamat serangan akan dapat memblok *port-port* tidak terpakai atau digunakan yang menjadi jalur masuknya *malware* yang sebelumnya dilakukan pendeteksian dengan menggunakan *Honeypot*. Salah satu hal yang bisa didapat dengan *blocking port* atau *firewall filter* adalah memblok port yang tidak digunakan agar dapat mencegah masuknya serangan *malware* melalui *port-port* dalam jaringan yang telah terdeteksi oleh *Honeypot*.

Di lingkungan Sekolah Swasta Charitas Batam saat ini telah menggunakan akses internet yang berbasis *wireless* (*hotspot*) dan kabel pada jaringannya. layanan provider M-link yang berkecepatan 10 Mbps pun digunakan untuk layanan *internet* 24 jam, jumlah user yang mengakses pada jaringan di Sekolah Swasta Charitas Batam adalah 50 user yang terus menggunakan akses internet sebagai sarana untuk pencarian informasi dan komunikasi baik berada di Laboratorium maupun bagian Kantor Guru dan Kantor Administrasi, namun jaringan di lingkungan Sekolah Swasta Charitas ini tidak memiliki keamanan jaringan yang memadai, ini ditunjukkan dengan berdasarkan wawancara dengan pimpinan Sekolah Charitas serta beberapa pengguna jaringan yang mengeluhkan PC atau Laptop yang digunakan sering mengalami kerusakan pada bagian

software akibat serangan *Malware*, dan tidak adanya *management* jaringan didalam Sekolah Charitas.

Metode *blocking port* atau *firewall filter* dijalankan menggunakan *Router* mikrotik agar *port-port* yang tidak terpakai dapat segera dilakukan tindakan agar tidak diserang oleh *malware* yang menyerang port-port, dengan aplikasi pendukung honeypot dapat dilakukan pendeteksian agar port-port yang diserang dapat terlihat sehingga dapat dilakukan tindakan pada host yang terinfeksi agar dihentikan penyebaran *malware* tersebut ke *host* lain dalam jaringan maka masalah ini diangkat penulis kedalam skripsi yang berjudul **"Analisis dan Implementasi Mencegah Virus Malware Pada Jaringan Dengan Metode Blocking Port Menggunakan Mikrotik".**

1.2 Identifikasi Masalah

Agar penulis mudah dalam melakukan analisis serta pembahasan pada penelitian ini, dengan didasarkan pada latar belakang permasalahan yang telah diuraikan, maka penulis melakukan identifikasi permasalahan yang ada sebagai berikut:

1. Rendahnya management sistem keamanan jaringan di Sekolah Charitas Batam.
2. Serangan *malware* mampu merusak *software* atau sistem operasi komputer pada Sekolah Charitas Batam.

3. Banyaknya *port-port* yang terbuka memungkinkan *malware* dengan mudah masuk ke dalam jaringan komputer.

1.3 Batasan Masalah

Dalam penelitian ini penulis membatasi permasalahan agar tetap terarah dan tidak menyimpang dari apa yang sudah direncanakan sebelumnya. adapun batasan masalah pada penelitian ini :

1. Metode *blocking port* atau *firewall filter* diterapkan pada *local area network* (LAN) di Sekolah Swasta Charitas Batam.
2. Menggantikan Router yang dimiliki oleh Sekolah Swasta Charitas Batam dengan Router Mikrotik Rb750, setingan router sebelumnya diterapkan pada Router Mikrotik yang akan digunakan, serta tidak merubah susunan jaringan yang ada.
3. Menambahkan server *Honeypot* sebagai alat deteksi *malware* pada *Local Area Network*.
4. Menjalankan Metode *Blocking Port* atau *firewall filter* yang mana metode ini dijalankan menggunakan Mikrotik RB750.
5. *Memblock port* dengan menggunakan Router mikrotik Rb750, kemudian *port-port* yang tidak terpakai dapat segera dilakukan tindakan agar tidak diserang oleh *malware* yang menyerang *port-port* kosong dan tidak terpakai.

1.4 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka penulis merumuskan permasalahan dalam penelitian ini, yaitu:

1. Bagaimana Metode *Blocking port* mampu menjadi penunjang keamanan jaringan pada Sekolah Charitas Batam?
2. Bagaimana *Metode Blocking port* atau *firewall filter* menghambat serangan *malware* pada jaringan komputer?
3. Bagaimana *memblocking port-port* yang kosong atau tidak terpakai dalam jaringan dengan menggunakan router mikrotik?

1.5 Tujuan Penelitian

Berdasarkan rumusan masalah di atas maka tujuan dari penelitian ini yaitu:

1. Untuk memaksimalkan kinerja serta kemampuan sistem keamanan jaringan pada Sekolah Charitas Batam
2. Untuk mengetahui *metode Blocking Port* menghambat serangan *malware* pada jaringan komputer.
3. Untuk mencegah masuknya serangan *malware* dari *port-port* yang kosong dan tidak terpakai dalam jaringan komputer dengan metode *blocking port* router mikrotik.

1.6 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah sebagai berikut:

A. Aspek Teoritis

1. Dapat menambah pengetahuan dan pemahaman *malware* dan serangan-serangan dalam suatu jaringan komputer.
2. hasil penelitian ini diharapkan dapat menjadi bahan referensi guna penelitian lebih lanjut yang berkaitan dengan sistem keamanan jaringan komputer dan berbagai serangan-serangan yang dilakukan oleh *malware* terhadap suatu sistem jaringan.

B. Aspek Praktis

1. Bagi sekolah, agar dapat meningkatkan keamanan jaringan yang ada. dengan tidak adanya penyebaran *Malware* dan serangan dari luar sehingga jaringan komputer pada jaringan tersebut dapat stabil dan pertukaran data menjadi aman dan lancar.
2. Bagi peneliti, hasil penelitian ini dapat menjadi pelajaran dan pemahaman tentang keamanan jaringan komputer dan berbagai macam serangan *malware* serta melakukan metode *blocking port* menggunakan Router Mikrotik.

BAB II

KAJIAN PUSTAKA

2.1 Teori Dasar

2.1.1 Jaringan Komputer

Menurut Habib-Ur Rehman (2016: 1), Sebuah jaringan komputer biasanya terdiri dari tiga komponen: perangkat, menengah, dan topologi. Komputer, *smartphone*, laptop, *router*, *switch*, dan *repeater* adalah jenis berbeda dari perangkat yang mungkin ada dalam sebuah jaringan komputer. Dalam rangka untuk berkomunikasi satu sama lain, perangkat ini dihubungkan oleh media, baik nirkabel atau kabel. Sehingga menghasilkan skema dari perangkat yang terhubung melalui media topologi jaringan. Dalam jaringan komputer, komunikasi yang sebenarnya terjadi antara perangkat. Dalam konteks percakapan manusia, komunikasi mencakup dialog lengkap antara dua orang. Aturan yang sama berlaku untuk jaringan komputer, komunikasi antara dua atau lebih perangkat terdiri dari lebih dari satu pesan dipertukarkan di antara peserta perangkat. Sesi adalah istilah teknis lebih banyak digunakan untuk menggambarkan serangkaian pesan berkorelasi dipertukarkan antara perangkat.

2.1.1.1 Protokol

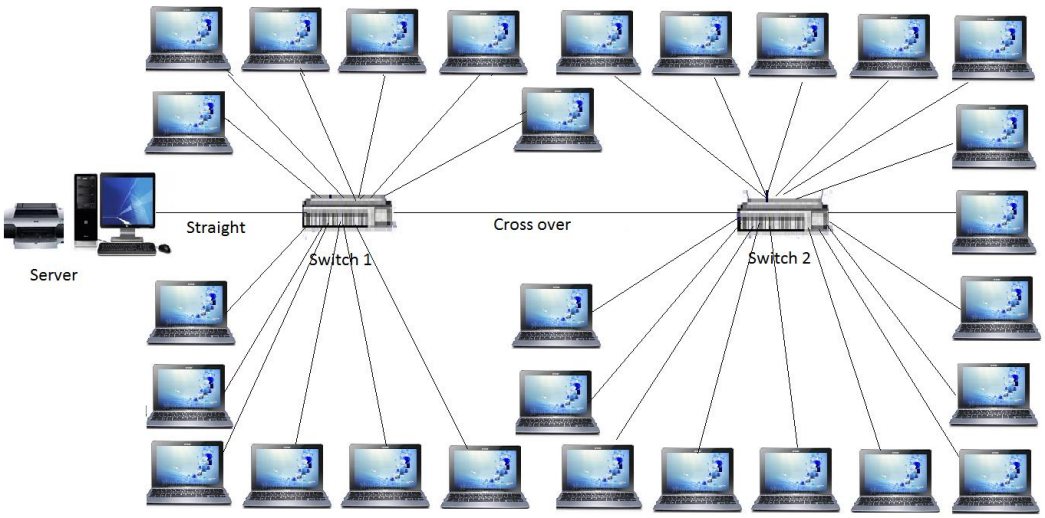
Menurut (Rehman, 2016), protokol menjelaskan tindakan yang harus dilakukan dan pedoman yang harus diikuti dengan perangkat selama komunikasi. Model referensi *OSI* adalah dokumen dasar komunikasi dalam jaringan komputer. Protokol di sebagian besar kasus menargetkan pekerjaan rencana model *OSI*. Namun, tidak ada protokol tunggal yang menargetkan semua tujuh lapisan dari model *OSI*. Sebuah protokol tunggal biasanya menargetkan pekerjaan lapisan individu dan protokol selalu dikaitkan dengan masing-masing lapisan *OSI*. Dalam rangka untuk melakukan komunikasi, perangkat berikut beberapa protokol, yang bekerja dengan cara yang mengharuskan bahwa protokol harus sesuai satu sama lain. Disebabkan oleh fakta ini, protokol berevolusi dalam bentuk kelompok, di mana Keluarga merupakan protokol milik berbeda lapisan *OSI* dan *compliant* satu sama lain. ia kategori protokol dan standar sangat luas. Standar istilah dalam jaringan komputer mengacu pada protokol, model, arsitektur dan kombinasi yang dirancang oleh beberapa otoritas yang didirikan atau organisasi.

2.1.2 Jenis Jaringan Komputer

Menurut (Sopandi, 2008), luas jaringan komputer ada beberapa bagian secara wilayah dibedakan menjadi tiga kelompok:

2.1.2.1 Local Area Network (LAN)

Local area network (LAN), Merupakan jaringan yang bersifat internal dan biasanya milik pribadi di dalam sebuah perusahaan kecil atau menengah dan berukuran sampai beberapa kilometer.

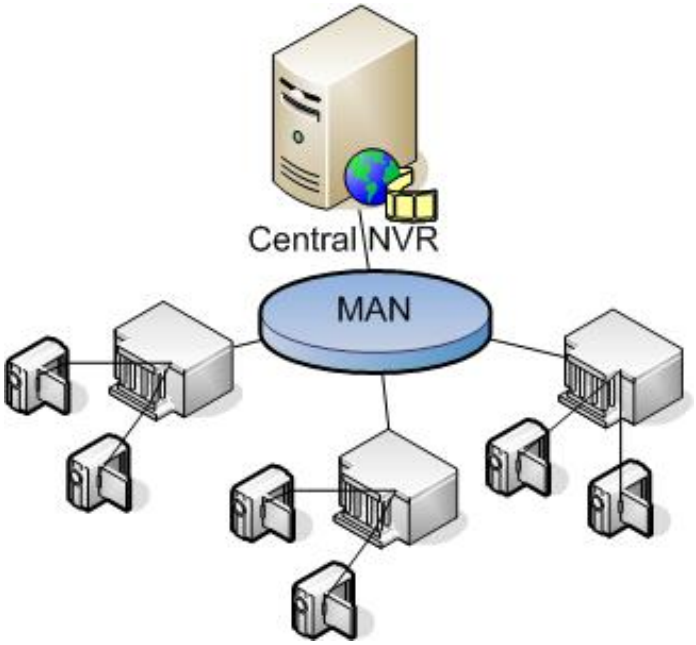


Gambar 2.1 *Local Area Network (LAN)*

Sumber: Dede Sopandi 2008

2.1.2.2 Metropolitan Area Network (MAN)

Metropolitan Area Network (*MAN*), merupakan sebuah jaringan dengan teknologi yang sama dengan *LAN*, hanya *MAN* lebih luas dari pada *LAN*. *MAN* mencakup kantor-kantor perusahaan yang letaknya berdekatan atau antar kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum.

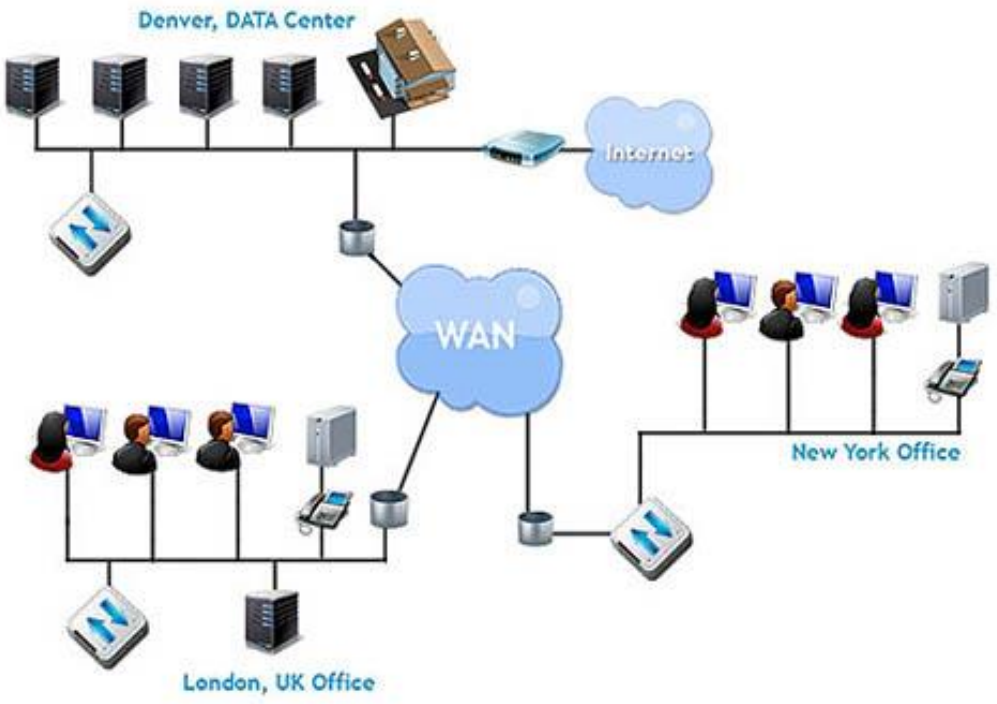


Gambar 2.2 ***Metropolitan Area Network (MAN)***

Sumber: Dede Sopandi 2008

2.1.2.3 Wide Area Network (WAN)

Wide Area Network (*WAN*) mencakup daerah dengan wilayah yang luas, seringkali mencakup sebuah negara atau benua. *WAN* terdiri dari kumpulan server yang bertujuan untuk menjalankan program-program aplikasi. Seperti *LAN* (*Local Area Network*), terdapat sejumlah perangkat yang dilewati aliran informasi data dalam sebuah *WAN*. Penggabungan perangkat tersebut menciptakan infrastruktur *WAN*.



Gambar 2.3 ***Wide Area Network (WAN)***

Sumber: Dede Sopandi 2008

2.1.2.4 Internet

Merupakan gabungan dari berbagai *LAN* dan *WAN* yang berada di seluruh jaringan Komputer di dunia. Sehingga terbentuk jaringan dengan skala yang lebih luas dan *global* jaringan *internet* biasanya menggunakan *protocol TCP/IP* dalam mengirimkan paket data *internet* berasal dari (*interconnected network*) yang berarti hubungan dari beragam jaringan komputer di dunia yang saling terintegrasi membentuk suatu komunikasi global.

2.1.2.5 Jaringan Tanpa Kabel

Komputer *mobile* seperti komputer *notebook* dan *Personal Digital Assistant* (*PDA*), merupakan cabang industri komputer yang paling cepat pertumbuhannya. Banyak pemilik jenis komputer tersebut yang sebenarnya telah memiliki mesin-mesin *desktop* yang terpasang pada *LAN* atau *WAN* tetapi karena koneksi kabel tidaklah mungkin dibuat di dalam mobil atau pesawat terbang, maka banyak yang tertarik untuk memiliki komputer dengan jaringan tanpa kabel ini.

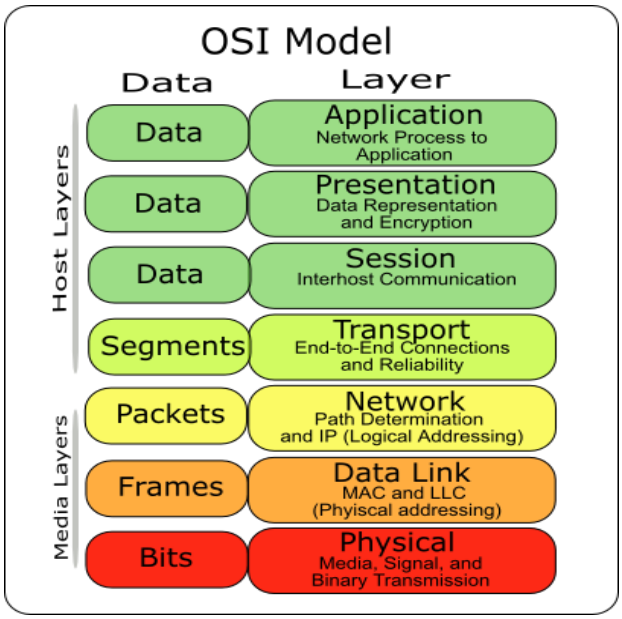
Jaringan tanpa kabel mempunyai berbagai manfaat, yang telah umum dikenal adalah kantor *portable*. Orang yang sedang dalam perjalanan seringkali ingin menggunakan peralatan elektronik *portable*-nya untuk mengirim atau menerima telepon, fax, e-mail, dan sebagainya, serta dapat digunakan dimana saja, darat, laut, udara. Jaringan tanpa kabel sangat bermanfaat untuk mengatasi masalah-masalah di atas.

Walaupun jaringan tanpa kabel dan sistem komputasi yang dapat berpindah-pindah sering kali berkaitan erat, sebenarnya tidaklah sama. Komputer *portable* kadang-kadang menggunakan kabel juga, yaitu disaat seseorang yang sedang dalam perjalanan menyambungkan komputer *portable*-nya ke jack telepon di sebuah hotel, maka kita mempunyai mobilitas yang bukan jaringan tanpa kabel. Sebaliknya, komputer-komputer yang menggunakan jaringan tanpa kabel tetapi bukan portabel, hal ini dapat terjadi disaat komputer-komputer tersebut terhubung pada *LAN* yang menggunakan fasilitas komunikasi *wireless* (radio).

Meskipun jaringan tanpa kabel ini cukup mudah untuk di pasang, tetapi jaringan seperti ini memiliki banyak kekurangan. Biasanya jaringan tanpa kabel mempunyai kemampuan 1-2 Mbps, yang mana jauh lebih rendah dibandingkan dengan jaringan berkabel. Kesalahan juga sering kali lebih besar, dan transmisi dari komputer yang berbeda dapat mengganggu satu sama lain.

2.1.3 Model OSI Layer

Menurut (Wangdra, 2012), Suatu jaringan komputer *LAN* dibangun dengan memperhatikan arsitektur standar yang dibuat lembaga standar industri dunia. Standar jaringan yang saat ini di akui adalah *The Open System Connection* atau *OSI* yang dibuat oleh lembaga *ISO* (*The International Standard Organization*), Amerika Serikat. Seluruh fungsi kerja jaringan komputer dan komunikasi antar terminal diatur dalam standar ini. *OSI* adalah suatu standar komunikasi antar mesin yang terdiri dari 7 lapisan. Ketujuh lapisan tersebut mempunyai peran dan fungsi yang berbeda satu dengan yang lain. Model dibagi menjadi 7 *layer*, dengan karakteristik dan fungsinya masing-masing. Tipe *layer* harus dapat berkomunikasi dengan *layer* diatasnya maupun dibawahnya secara langsung melalui serentetan *protocol* dan *standard*.



Gambar 2.4 *OSI Layer*

Sumber: Iwan Sofana 2017

1. *Physical Layer*

   Menangani pengiriman bit-bit data melalui saluran komunikasi, memastikan jika *entity* satu mengirimkan bit 1, maka *entity* yang lain juga harus menerima bit 1. Fungsi utama layer ini untuk menentukan berapa volt bit 1 dan 0, *nanoseconds* bit dapat bertahan di saluran komunikasi, kapan koneksi awal dibuat dan diputuskan ketika dua *entity* selesai melakukan pertukaran data, dan pin yang digunakan oleh *network connector* dan fungsi dari setiap pin.

2. *Data Link Layer*

   Menyediakan prosedur pengiriman data antar jaringan, mendeteksi dan mengoreksi *error* yang mungkinterjadi di *physical layer*, memiliki address secara fisik yang sudah di-kode-kan secara langsung ke *network*

card pada saat pembuatan *card* tersebut yaitu MAC *address*. Perangkat yang beroperasi di layer ini adalah *bridge* dan layer-2 *switch*.

3. *Network Layer*

   Menentukan prosedur pengiriman data sekuensial dengan berbagai macam ukuran, dari sumber ke tujuan, melalui satu atau beberapa jaringan, dengan tetap mempertahankan *quality of service* (QOS) yang diminta oleh *transport layer*. Fungsi dari layer ini adalah routing menentukan jalur pengiriman dari sumber ke tujuan, bisa statis atau *transit time*, *jitter*, dll), dan menyediakan *interface* untuk dinamis, pengendalian kongesti, mempertahankan QoS (*delay*, jaringan-jaringan yang berbeda agar dapat saling berkomunikasi.

4. *Transport Layer*

   Fungsi *layer* ini adalah menerima data dari *layer* diatasnya, memecah data menjadi unit-unit yang lebih kecil yang sering disebut *packet*, meneruskan ke *network layer* dan memastikan semua *packet* tiba diujung penerima tanpa *error*.

5. *Session Layer*

   Mengijinkan *user-user* yang menggunakan mesin yang berbeda untuk membuat dialog (*session*). Fungsi nya adalah pengendalian dialog guna memantau pengiriman, pengelolaan token adalah mencegah dua pihak untuk melakukan operasi yang sangat kritis dan penting secara bersamaan, dan melakukan sinkronisasi yang menandai bagian data

yang belum terkirim sesaat *crash* pengiriman terjadi, sehingga pengiriman bisa dilanjutkan tepat ke bagian tersebut.

6. *Presentation Layer*

   Layer ini mengatur tentang *syntax* dan *semantics* dari data yang dikirimkan, dan manipulasi data seperti MIME encoding, kompresi, dan enkripsi dilakukan *layer* ini.

7. *Application layer*

   Layer ini sangat dekat *user*, menyediakan *user interface* ke jaringan melalui aplikasi, contoh *protocol* aplikasi yang banyak digunakan: *hypertext transfer protocol* (*HTTP*) yang digunakan di *world wide web, file transfer protocol* (*FTP*) untuk pengiriman file antar komputer, *simple mail transfer protocol* (*SMTP*) untuk *email*.

2.2 Teori Khusus

2.2.1 Malware

Menurut (Mada R. Perdhana, 2011), *Malware* merupakan singkatan dari *malicious software*, yaitu sebuah sebutan bagi *software* yang di desain sedemikian rupa agar dapat menyusup ke dalam sebuah sistem komputer tanpa diketahui pemilik sistem, dimana di dalam *software* tersebut terdapat perintah-perintah khusus yang dibuat dengan tujuan khusus, seperti menyebarkan *virus, trojan,*

worm, atau memasang *backdoor*. Secara umum dapat dikatakan bahwa, *malware* merupakan aplikasi yang dapat atau akan membuat celah pada keamanan sebuah sistem komputer.

2.2.1.1 Macam Malware

Pada awal perkembangannya, banyak aplikasi *malware* seperti *worm* dan *virus* yang dibuat hanya untuk tujuan eksperimen dan lelucon untuk menjahili orang lain. Namun dalam beberapa kasus, pencipta aplikasi *malware* tersebut tidak menyadari seberapa dalamnya kerugian yang didapatkan pengguna oleh karena ciptaan mereka. Dalam beberapa kasus, program *malware* yang berisi perintah-perintah mematikan banyak ditemukan berkeliaran di dalam jaringan publik, beberapa diantaranya mengakibatkan kerusakan serius pada data bahkan hingga pada terhapusnya data dari dalam sistem. *Malware* yang melakukan perusakan pada sistem kebanyakan menyerang pada sistem operasi berbasis *DOS* dan *Windows*. Kebanyakan malware tersebut dirancang untuk menghancurkan *file* yang berada pada *harddisk*, atau untuk merusak *system* yang ada di dalam sistem operasi.

Sejak meningkatnya penggunaan teknologi *internet*, para pembuat *malware* mulai meningkatkan pola serangan dan penyebaran *malware* yang dibuat. Salah satu teknik yang digunakan adalah memanfaatkan komputer yang terinfeksi untuk mengirimkan pesan masal kepada pihak lain yang nantinya akan dijadikan host

baru bagi *malware*. Pesan yang terkirim biasanya berupa pesan *email* iklan pesan IM melalui aplikasi IM ang popular seperti *Yahoo messenger*. Bahkan beberapa *malware* dirancang untuk menjadikan *host* yang *terinfeksi* sebagai tempat untuk melakukan serangan *DOS massal* terhadap *system*.

Kelompok *malware* lainnya adalah kelompok *malware* yang mengambil keuntungan financial dari korban yang sistemnya telah terinfeksi. Ada beberapa cara yang dilakukan *malware* untuk menjebak korbannya agar mengirimkan uang kepada pembuat *malware*, yaitu :

1. Memantau lalu lintas *internet web browser* dan menyusupkan halaman iklan atau halaman khusus yang akan mengarahkan ke dalam halaman produk si pemilik *malware*.
2. Memunculkan pesan palsu, bahwa *system* telah terinfeksi *virus* dan korban dapat menghapusnya dengan produk khusus yang hanya dapat dipesan pada pembuat *malware*.

Malware memiliki 3 tipe yaitu :

1. *Malware* tipe infeksi, *malware* ini akan melakukan infeksi pada *system* dan menggandakan diri ketika *system* atau *file* yang telah terinfeksi di eksekusi. *Malware* tipe ini merupakan *malware* yang paling terkenal yaitu *virus* dan *worm*. Sejak awal *virus* dan *worm* dikenal karena cepatnya mereka menyebar dari *system* satu ke *system* lainnya. Perbedaan yang mendasar dari kedua *malware* ini adalah mengenai bagaimana teknik penyebarannya. *Virus* biasanya, melakukan penyebaran dengan melakukan infeksi pada *file-file* yang dapat dieksekusi (dijalankan). Ketika *user* melakukan eksekusi pada *file* yang

telah terinfeksi oleh *virus*, maka *virus* yang telah menginfeksi *file* akan menyebar dan mulai menginfeksi *file-file* lainnya yang ada di dalam *system* tempat dieksekusi. Sedangkan *worm*, melakukan penyebaran secara aktif dengan berjalan di dalam jaringan, menginfeksi *file-file* tertentu yang ada di dalam *system* kemudian mencari koneksi ke dalam jaringan dan mulai bergerak pindah ke dalam *host* lain yang ada di dalam jaringan tersebut. Baik *virus* maupun *worm*, keduanya sama-sama membawa *payload* yang memiliki perintah-perintah tertentu, seperti melakukan exploitasi pada system atau mengumpulkan data tertentu dan mengirimkannya ke pada pembuat *malware*.

2. *Malware* tipe terselubung, *malware* ini biasanya akan diproteksi dengan beberapa teknik penyelamatan diri, salah satunya adalah melakukan kamuflase di dalam *system*, sehingga *user* pemilik *system* tidak akan sadar apabila sistemnya telah terinfeksi oleh *malware*. Dalam prakteknya, selain melindungi diri dengan menyerupai proses asli dari sebuah sistem operasi, ada juga *malware* yang melakukan konfigurasi sedemikian rupa pada sistem operasi, sehingga apabila sistem dimatikan dan kemudian dinyalakan kembali, *malware* pun akan ikut aktif dan kembali berjalan di dalam sistem. Berikut adalah *malware* yang termasuk ke dalam tipe *malware* terselubung :
    a. *Rootkit* adalah *malware* khusus yang dirancang untuk menjaga aktifitas dari proses menjadi tidak tertangkap secara normal oleh pemilik sistem. *Rootkit*, merupakan tipe *malware* yang berjalan atas *control* langsung pemilik *malware*.
    b. *Trojan horse* adalah *malware* yang dikamuflasekan dengan *file-file*

yang tampaknya tidak berbahaya dan terlihat umum oleh pengguna komputer atau *system antivirus*. Namun ketika *file* tersebut dieksekusi, maka *malware* berbahaya yang berada di dalamnya akan keluar dan mulai melakukan infeksi ke dalam sistem dengan cepat. Beberapa *malware Trojan horse*, akan mematikan sistem proteksi yang ada pada *host* yang terinfeksi, seperti *firewall, antivirus*, atau *removal.*

c. *Backdoor* adalah salah satu jenis *malware* yang mampu berkamuflase dalam sistem. Seperti namanya yang berarti pintu belakang, *malware* ini akan membuka akses khusus ke dalam sistem bagi pembuat *malware.* Biasanya *backdoor* digunakan setelah *malware* lain menginfeksi terlebih dahulu sistem target, missal menggunakan *worm, Trojan horse* atau lainnya. Dengan adanya *backdoor* pada sistem, memungkinkan pembuat *malware* leluasa untuk keluar masuk sistem yang terinfeksi, dan melakukan aktifitas di dalam sistem sebagaimana yang dilakukan oleh *user* sistem yang normal.

3. *Malware* tipe *profit-oriented* adalah *malware* yang dirancang untuk tujuan mencari keuntungan, baik financial maupun non-financial. *Malware* tipe ini biasanya didistribusikan menggunakan *Trojan horse*. Beberapa contoh *malware* tipe ini adalah *spyware, botnet, keylogger malware* dan *dialer*.

2.2.1.2 Tingkah Laku *Malware*

Pada umumnya *malware* memiliki pola penyebaran/penginfeksian melalui beberapa cara, seperti: *email attachment, script* dari halaman *web, link* ke dalam halaman *web* yang terkadang berupa *file* yang siap di *install*, malakukan exploitasi bug pada sistem operasi, *USB drive*, *file sharing*, serta aplikasi bajakan yang telah ditanami *loader malware*.

Secara umum kinerja *malware* di dalam sebuah sistem yang telah terinfeksi dapat dikelompokkan menjadi dua bagian, yaitu :

1. *Malware* pada sistem, umumnya *malware* akan melakukan beberapa kegiatan rutin pada sistem yang telah berhasil diinfeksi. Berikut adalah beberapa kegiatan *malware* pada sistem sebuah sistem :
    a. Menggandakan diri sebanyak-banyaknya pada sistem yang terinfeksi, dengan tujuan untuk saling melindungi antara proses *malware* satu dengan proses *malware* lainnya
    b. Menyamarkan diri, dengan melakukan kamuflase pada sistem, seperti menginfeksi *file* pada sistem utama aplikasi, mengubah attribute *file* yang telah terinfeksi dan atribut *malware* itu sendiri.
    c. Pada sistem *windows*, *malware* akan melakukan konfigurasi pada *registry*, sehingga *malware* dapat mengontrol alur kerja sistem operasi dan aplikasi yang berjalan di dalamnya.
    d. Membuat proses baru pada sistem, berupa *service* yang berjalan di *background process* pada sistem informasi.

e. Mematikan *service-servirce* standar pada sistem, dan menggantikan dengan *service* palsu yang telah diinfeksi oleh *malware.*

f. Menyiapkan *file* sistem palsu yang nantinya akan di *load* oleh sistem aplikasi, seperti .dll, .sys, dan .so.

Malware pada jaringan umumnya selain melakukan kegiatan yang berhubungan dengan sistem, sebuah *malware* setelah berhasil menginfeksi sebuah sistem biasanya juga akan melakukan aktifitas yang berhubungan dengan jaringan. Aktifitas umum sebuah *malware* yang berhubungan dengan jaringan adalah sebagai berikut :

1. Mencoba untuk melakukan exploitasi pada *service* tertentu yang berhubungan dengan jaringan.
2. Mengirimkan informasi kepada pembuat *malware* melalui jaringan.
3. Mengontrol alur data sebuah sistem dari dalam dan ke dalam jaringan.
4. Menyimpan komunikasi data yang berada di dalam jaringan.

2.3 Tools

2.3.1 Linux Ubuntu

Menurut (Eko Koswara, 2012) nama “Linux” berasal dari nama pembuatnya, yang diperkenalkan 1991 oleh Linus Torvalds. Sistemnya, peralatan

sisten dan pustaka umumnya berasal dari sistem operasi *GNU*, yang diumumkan tahun 1983 oleh Richard Stallman.

Ubuntu pertama kali dirilis pada 20 Oktober 2004, versi-versi Ubuntu akan dirilis setiap 6 bulan sekali agar dapat memperbaharui sistem keamanan dan *update* program. Ubuntu didasarkan pada paket-paket dari Debian yang tidak stabil keduanya menggunakan distro Debian's deb format dan alamat manejemen paket, *APT* dan *Synaptic* walaupun Debian dan Ubuntu merupakan paket-paket yang belum tentu (biner kompatibel) satu sama lain, dan mungkin perlu dibangun ulang dari sumber. Kelebihan menggunakan Ubuntu :

1. Tidak perlu membeli *license* dan boleh digunakan dibanyak komputer hanya dengan satu *CD*.
2. Stabil, bebas *virus, malware, worm*, dan sebagainya sehingga tidak perlu memasang program anti *virus*.
3. Sangat ringan dan boleh digunakan pada komputer dengan *hardware* yang rendah.
4. Tidak sulit untuk installasi driver karena kebanyakan *driver* telah ada di dalam *CD* seperti *LAN, Wifi, Audio* dan sebagainya.
5. Banyak aplikasi seperti untuk *browsing internet, office*, mendengar musik, memainkan *video, photo viewer*, kalkulator dan sebagainya.
6. Terdapat *Live CD*, yang memperbolehkan untuk mencoba menggunakan Ubuntu tanpa perlu installasi ke dalam *harddisk*, hanya perlu *boot* menggunakan *CD* Ubuntu untuk masuk ke *Live CD session*.

Kelemahan menggunakan Ubuntu:

1. Masih belum *user friendly*, terkadang pengguna biasa agak kaku dalam pengoperasiannya terutama yang belum dengan linux.
2. Aplikasi di *windows* mungkin tidak dapat digunakan di Ubuntu sehingga tidak semua aplikasi *Compatible* dapat dijalankan dengan *wine (windows emulator)*.

2.3.2 *Router* Mikrotik

Menurut (Athailah, 2013) *Router* mikrotik adalah sebuah merek dari sebuah perangkat jaringan, pada awalnya mikrotik hanyalah sebuah perangkat lunak atau *software* yang diinstal dalam komputer yang digunakan untuk mengontrol jaringan, tetapi dalam perkembangannya saat ini telah menjadi sebuah *device* atau perangkat jaringan yang handal dan harga yang terjangkau, serta banyak digunakan pada *level* perusahaan penyedia jasa *internet*.

Pada awalnya dimulai saat dua orang ahli jaringan, yaitu Jhon Trully dan Arnis Riekstins berhasil membuat routing jaringan ke jaringan yang lebih luas, sehingga hal ini menjadi visi mikrotik sampai saat ini, yaitu "*Routing The Word*". John Trully bersama Arnis Riekstins bekerja sama untuk membuat sebuah perangkat yang benar-benar dapat diandalkan untuk pekerja routing jaringan. Dimulai dengan membuat mikrotik yang berbasiskan kernel Linux, mereka berdua

membangun sebuah *ISP* berkecepatan 2 Mbps dan bernama Aeronet, di Moldova, sebuah negara tetangga Latvia.

2.3.2.1 Jenis-Jenis Mikrotik

1. Mikrotik *Router* OS yang berbentuk software yang dapat didownload di www.mikrotik.com dapat diinstal pada komputer atau *PC*.
2. *Built-in Hardware* Mikrotik dalam bentuk perangkat keras yang khusus dikemas dalam *board router* yang didalamnya sudah terinstal mikrotik *router* OS.

2.3.2.2 Fitur-Fitur Mikrotik

Menurut (Herlambang, M.L., 2008) dalam bukunya menyebutkan beberapa fitur mikrotik, berikut merupakan fitur-fitur mikrotik:

1. *Address List*
2. *Asynchronous*
3. *Bonding*
4. *Bridge*
5. Data *Rate Management*
6. *multiple network*
7. *Firewall* dan *NAT*
8. *Hotspot*

9. *IPSec*
10. *ISDN*
11. M3P
12. MNDP
13. Monitoring / *Accounting*
14. *NTP*
15. *Point to Point Tunneling Protocol*
16. *Proxy*
17. Routing
18. SDSL
19. *Simple Tunnel*
20. *SNM* : *Simple Network Monitoring Protocol* mode akses *read-only*.
21. *Synchronous*
22. *Tool*
23. *UPnP*
24. *VLAN*
25. *VoIP*
26. *VRRP*

2.3.2.3 Mikrotik Rb 750

Mikrotik RB750 adalah salah satu jenis *Router Board* Mikrotik yang paling banyak digunakan karena harganya yang murah meriah. Mikrotik RB 750 memiliki 5 buah *port ethernet* 10/100, dengan prosesor baru Atheros 400MHz dan sudah termasuk dengan lisensi *level* 4. Sayangnya RB750 tidak memiliki *interface Wireless*, sehingga tidak dapat langsung digunakan untuk membuat *wireless Hotspot*. Agar dapat membuat *wireless Hotspot* perlu ditambahkan perangkat tambahan sebagai *Access Point*.

2.3.3 Honeypot

Menurut (Rehman, 2016), berbicara tentang sejarah *honeypot*, banyak definisi dari *honeypot*. Dengan kata lain, ada beberapa definisi *honeypot* pada peneliti yang berbeda, mungkin mereka memiliki definisi sendiri tentang apa honeypot, beberapa berpikir bahwa *honeypot* adalah alat untuk penipuan, sedangkan yang lain menganggapnya sebagai senjata untuk memikat para hacker, dan yang lain percaya bahwa hal itu hanya alat deteksi intrusi lain. Definisi formal *honeypot* adalah sumber daya keamanan yang nilainya terletak pada pendeteksian, penyusupan, dan jebakan.

Honeypot dapat mengumpulkan informasi tentang siapa saja yang mencoba membobol sistem.

Honeypot dapat memberikan informasi tentang alat dan taktik yang digunakan oleh penyerang untuk membobol sebuah sistem. Informasi tersebut dapat ditemukan dalam teknik yang telah digunakan dalam *honeypot* seperti *firewall log*, sistem deteksi intrusi (IDS), dan sistem log. Dengan mendapatkan informasi ini, dapat menghindari serangan tersebut yang terjadi pada sistem jaringan. Dengan meningkatkan sistem terhadap serangan yaitu, mengumpulkan informasi tentang alat dan taktik, dianggap sebagai tujuan yang paling penting dari sebuah *honeypot*.

Dengan menggunakan *honeypot*, bisa didapatkan serangan *zero-day* (tanpa diketahui penyerang). *honeypot* menyediakan informasi yang luas tentang berbagai serangan dan pola dari penyerang.

Fakta yang menarik tentang honeypot adalah bahwa tidak berguna jika honeypot tidak diserang oleh penyerang, karena untuk menangkap informasi tentang penyerang, *honeypot* harus dibobol atau disusupi. Jika tidak, *honeypot* tidak memiliki utilitas, karena tidak dapat memberikan informasi yang diperlukan.

Honeypot berbeda dari kebanyakan alat-alat atau sistem keamanan jaringan lainnya. Sebagian besar teknologi keamanan yang digunakan saat ini, dirancang untuk mengatasi masalah spesifik. Misalnya, *firewall* adalah teknologi yang melindungi sistem dengan mengendalikan tinggi rendah *traffic*, atau sebagai alat kontrol akses. *Firewall* yang paling umum digunakan di sekeliling sistem untuk memblokir aktivitas yang tidak sah. Sedangkan jaringan IDS dirancang untuk

mendeteksi serangan, pemantauan baik sistem atau aktivitas jaringan. *Honeypot* berbeda karena tidak terbatas pada pemecahan tunggal, masalah spesifik. Sebaliknya, *honeypot* adalah alat yang *flexible*, dapat diterapkan dalam berbagai situasi yang berbeda. Sebabnya definisi *honeypot* mungkin pada awalnya membingungkan, karena dapat digunakan untuk mencapai begitu banyak tujuan yang berbeda dan dapat datang dalam berbagai bentuk berbeda. Sebagai contoh, *honeypot* dapat digunakan untuk mencegah serangan, dengan menggabungkan bersama dengan sistem *firewall*. *Honeypot* juga dapat digunakan untuk mendeteksi serangan, mirip dengan fungsi dari *IDS*. *honeypot* dapat digunakan untuk menangkap dan menganalisa serangan otomatis, seperti *worm*, atau bertindak sebagai awal indikasi dan peringatan. Penggunaan *honeypot* menyesuaikan dengan kebutuhan. Hal ini tergantung pada apa yang akan dicapai atau diinginkan.

Honeypot ditempatkan di 3 lokasi, Setiap lokasi mempunyai kelebihan dan kekurangannya masing-masing. Sehingga membutuhkan pertimbangan–pertimbangan sebelum menerapkannya pada lokasi yang ada, *honeypot* ditempatkan pada lokasi berikut :

1. Di depan *gateway* (dekat dengan jaringan)

   Kelebihan dari penempatan *honeypot* di lokasi ini adalah *honeypot* akan dianggap sama seperti dengan sistem eksternal sehingga akan mengurangi resiko terhadap jaringan *private* apabila *honeypot* telah berhasil disusupi/diambil alih oleh penyerang. Kekurangannya adalah trafik–trafik yang mencurigakan dideteksi oleh *honeypot* tidak akan

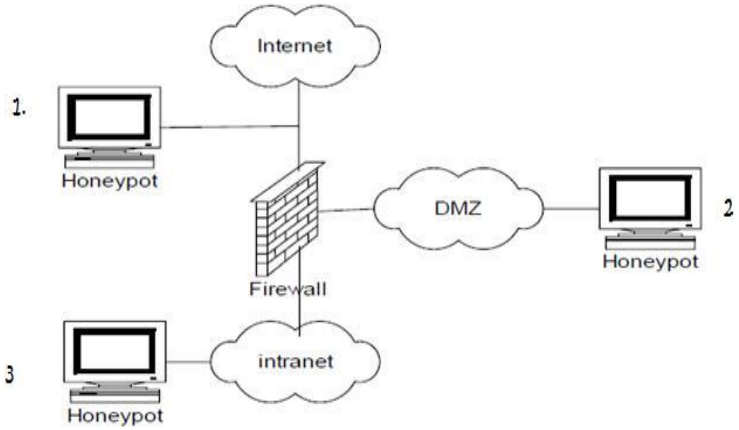
terdeteksi pada *firewall* atau IDS sehingga informasi yang diperoleh sangat sederhana.

2. Di dalam *DMZ (Demilitarized Zone*).

   Pada gateway biasanya juga terdapat sistem pengaman seperti *firewall*. Di lokasi ini, kelebihan yang didapatkan adalah trafik yang sah biasanya menuju ke *honeypot* akan melewati *firewall* dan akan tercatat pada *firewall log*. Dengan demikian informasi dapat cepat terkumpulkan. Kekurangan dari letak *honeypot* di lokasi ini adalah sistem lain yang terdapat pada *DMZ* harus diamankan dari *honeypot*.

3. Di belakang *gateway* (dekat dengan jaringan *intranet*)

   Alasan *honeypot* ditempatkan di lokasi ini adalah untuk mendeteksi penyerang yang berasal dari dalam atau untuk mendeteksi *firewall* yang tidak terkonfugurasi dengan baik sehingga menyebabkan adanya trafik tidak diketahui yang menuju jaringan privat. Penempatan *honeypot* pada lokasi ini akan mengakibatkan betambahnya resiko pada jaringan *private* karena bila *honeypot* telah berhasil disusupi/diambil alih maka penyerang akan mendapat akses menuju jaringa *private* melalui *honeypot*. Dengan kata lain, *honeypot* akan digunakan sebagai batu loncatan untuk menyerang jaringan *private*.



Gambar 2.5 *Skema Honeypot*

Sumber: Habib ur-Rehman 2016

Tingkat interaksi memberi skala yang bisa diukur dan dibandingkan. Berdasarkan tingkat interaksi, *honeypot* terbagi ke dalam tiga kategori :

1. *Low Interaction Honeypot* yang paling sederhana dalam hal pelaksanaan, biasanya yang paling mudah dalam hal instalasi, konfigurasi, dan desain yang sederhana karena *Honeypot* ini hanya meniru berbagai layanan. Sebagai contoh, *low interaction honeypot* bisa meniru server Unix standar dengan beberapa layanan yang berjalan, seperti *Telnet* dan *FTP*. Seorang penyerang bisa Telnet ke honeypot, mendapatkan informasi yang menyatakan OS, dan mungkin mendapatkan *prompt login*. Penyerang bisa mencoba untuk *login* dengan *brute-force* atau dengan menebak *password*. *honeypot* akan menangkap dan mengumpulkan informasi tersebut. Jadi, interaksi penyerang terbatas untuk dapat login. Bahkan, fungsi utama dari *low interaction honeypot* adalah melakukan scan pada jaringan yang

dianggap mencurigakan atau mencoba memasuki sistem dengan cara yang tidak sah. Seperti yang telah disebutkan di atas, *low interaction honeypot* sebagian besar dapat ditiru oleh program. Program hanya diinstal pada sistem *host* dan konfigurasi untuk layanan apapun, serta honeypot mampu membuat kedua penyebaran dan pemeliharaan honeypot mudah. *Low interaction honeypot* memiliki risiko terendah, karena ada tidak ada OS yang nyata bagi penyerang untuk berinteraksi yaitu, semua layanan yang ditiru tidak nyata. Jadi, *honeypot* ini tidak dapat digunakan untuk merusak atau memonitor sistem lain. *Low interaction honeypot* memiliki fungsi yang terbatas informasi dan dirancang untuk menangkap aktivitas yang diketahui. Penyerang dapat mendeteksi *low interaction honeypot* dengan mengeksekusi perintah yang hanya mampu memeriksa dan terkoneksi kebeberapa *port* saja.

2. *Medium Interaction Honeypot* adalah penggabungan kedua level (*low dan high interaction honeypot*) sehubungan dengan deteksi dan pengumpulan informasi *malware*. Kunci dari fitur *honeypot* level ini adalah aplikasi virtualisasi lapisan. *Medium interaction honeypot* tidak bertujuan sepenuhnya kepada simulasi operasional pada sistem, dan juga tidak menerapkan semua rincian dari aplikasi protokol. *Medium interaction honeypot* memberikan informasi bahwa eksploitasi berada pada *port* tertentu yang akan menjeratnya. Setelah *payload* tersebut telah diterima, *shellcode* diekstrak dan dianalisis entah. *Medium interaction honeypot*

kemudian mengemulasi tindakan *shellcode* yang akan men-*download* informasi tentang *malware*. *Honeypot* menyediakan beberapa sistem file virtual baik sebagai virtual Windows standar *download* utilitas. *Honeypot* level ini kemudian dapat men-download malware dan menyimpannya secara lokal atau mengirimkannya ke tempat lain untuk dilakukan analisis.

3. *High Interaction Honeypot* sangat berbeda dari *low interaction honeypot* dalam hal pelaksanaan dan mengumpulkan informasi. Level ini memanfaatkan *OS* yang sebenarnya bukan sebuah emulasi. Dalam level *honeypot* ini dapat mengumpulkan informasi lebih lanjut tentang serangan yang dimaksudkan. *High interaction honeypot* berguna jika seseorang administrator jaringan ingin menangkap rincian kelemahan atau eksploitasi yang belum dikenal. Eksploitasi tersebut dikenal sebagai eksploitasi *zero-day*. Cara tersebut sangat penting untuk mendapatkan informasi dengan cepat, sehingga sistem administrator dapat bekerja di sekitar masalah tersebut. Kelemahan *high interaction honeypot* dilevel ini, penyerang dapat menggunakan atau mengambil alih sistem untuk merusak sistem lain. Untuk mengurangi kelemahan tersebut, *high interaction honeypot* sering ditempatkan dalam lingkungan yang terkendali, seperti di belakang *firewall*. Seperti yang telah disebutkan di atas, *high interaction honeypot* perlu mekanisme kontrol yang luas sehingga bisa sangat dificult dan dapat memakan waktu untuk menginstal dan melakukan konfigurasinya. Untuk menjalankan level *high interaction honeypot,* berbagai teknologi berbeda harus digabungkan di dalam level ini, seperti *firewall* dan *IDS*.

Pemeliharaan juga memakan waktu, karena harus memperbarui *firewall* dan database signature *IDS*. Karena kompleksitas ini, *high interaction honeypot* memiliki resiko tinggi.

2.4 Penelitian Terdahulu

Sebagai bahan pertimbangan dan rujukan dalam penelitian ini, penulis mengacu pada beberapa penelitian terdahulu yang diantaranya adalah:

1. (Sumardi, 2013) dengan judul: "*Rancang Bangun Keamanan Jaringan Dengan Metode Blocking Port Pada Sekolah Menengah Kejuruan Karya Nugraha Boyolali*". Pada penelitian *PC Router Mikrotik* dapat digunakan untuk memblokir *port* yang tidak terpakai pada jaringan komputer, sehingga meminimalkan risiko masuknya *malware* dan serangan dari luar yang dapat memicu terjadinya kelumpuhan jaringan lokal.
2. (Wilman, 2018) dengan Judul: *"Port Knocking dan Honeypot Sebagai Keamanan Jaringan Pada Server Ubuntu Virtual"*. hasil penelitian ini Port Knocking dengan Fitur Limit per-IP connection Rate dan honeypot sebagai keamanan jaringan pada Server Ubuntu Virtual mampu mengamankan server dengan cara mengalihkan penyusup dan seolah – olah penyusup sudah masuk ke server utama, selain itu dengan adanya honeypot bias memonitoring yang dilakukan penyusup selama berada di

server banyangan dan bias dijadikan sebagai acuan untuk memperkuat system keamanan.

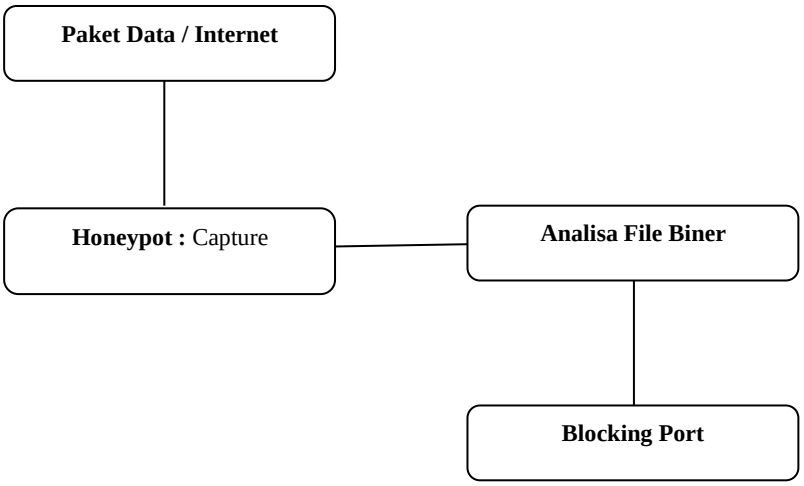
3. (Prihasmoro, 2014) dengan judul: "*Simulasi Sistem Deteksi Penyusup Dalam Jaringan Komputer Berbasis Web Interface Serta Perancangan Untuk Meningkatkan Keamanan*". Hasil penelitian ini *IDS* mampu memberikan informasi serangan melalui *web* untuk dapat dianalisa oleh *administrator*, perpaduan antara sistem deteksi dengan *firewall* merupakan suatu metode yang dinamakan *Intrusion Detection* and *Prevention System (IDPS).*
4. (Harjono, 2013) dengan judul: "*Deteksi Malware Dalam Jaringan Menggunakan Dionaea*". Pada Hasil penelitian adanya kekurangan dan kelemahan dari keamanan jaringan yang ada yaitu tidak adanya sistem untuk mendeteksi adanya serangan. Untuk meningkatkan keamanan jaringan dibutuhkan sistem yang dapat mendeteksi serta mengindentifikasi ancaman atau serangan, khususnya serangan malware. Rancangan sistem yang baru menggunakan *Honeypot Dionaea* untuk melakukan deteksi terhadap ancaman atau serangan dari *malware*, yang merupakan ancaman utama bagi keamanan sistem jaringan komputer.
5. (Muhammad Masuri Mustofa, 2013) dengan judul: "*Penerapan Sistem Keamanan Honeypot dan IDS pada Jaringan Nirkabel (Hotspot)*". Pada Hasil penelitian ini Implementasi *Honeypot* pada jaringan *nirkabel hotspot* yang sangat berkembang akan memberikan tambahan kesulitan kepada penyerang yang mencoba melakukan penyerangan, kombinasi *Honeypot*

dan *IDS* dengan *Honeyd* dan *Snort* memberikan sebuah sistem keamanan berlapis dengan menipu dan mendeteksi serangan yang ditujukan ke jaringan *hotspot*.

6. (Nugroho, 2013) dengan judul "*Analisis Dan Implementasi Honeypot Menggunakan Honeyd Sebagai Alat Bantu Pengumpulan Informasi Aktivitas Serangan Pada Jaringan".* Dengan demikian, implementasi honeypot dapat digunakan sebagai alat bantu administrator untuk melihat laporan aktivitas yang dihasilkan Honeyd agar dapat membantu dalam menentukan kebijakan keamanan jaringan.

2.5 Kerangka Pemikiran

Kerangka pemikiran adalah konstruksi berfikir yang bersifat logis dengan argumentasi yang konsisten dengan pengetahuan sebelumnya yang telah berhasil disusun (Suryana, 2010:23). Didasari dengan teori yang diperoleh dan dijelaskan, maka kerangka berpikir penilitian ini digambarkan pada gambar berikut ini:



Gambar 2.6 ***Kerangka Pemikiran***

Sumber: Penelitian 2018

2.6 Hipotesis

Hipotesis adalah kesimpulan sementara tentang hubungan antara *variable* dan fenomena penelitian. Hipotesis merupakan kesimpulan tentatif yang diterima secara sementara sebelum diuji (Nazir, 2013: 40). Berdasarkan rumusan permasalahan di atas, maka hipotesis utama yang penulis ajukan adalah sebagai berikut :

1. Kinerja dan kemampuan sistem keamanan jaringan pada Sekolah Charitas Batam mampu dimaksimalkan.
2. *Blocking Port* dapat menghambat serangan *malware* pada jaringan komputer.
3. Router mikrotik mampu mencegah masuknya serangan *malware* dari *port-port* yang kosong dan tidak terpakai dalam jaringan komputer.

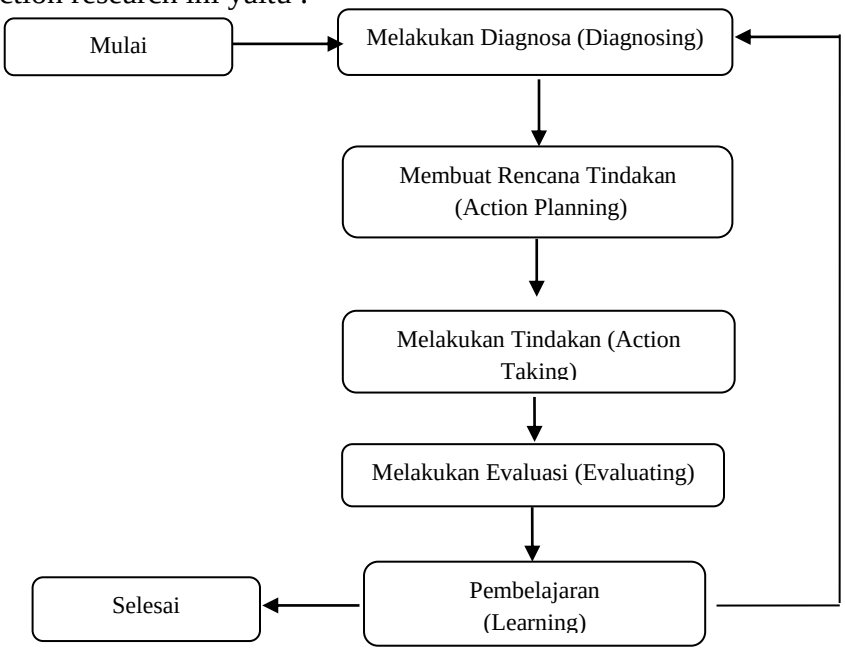
BAB III

METODE PENELITIAN

Dalam penelitian ini penulis menggunakan metode *Action Research* (penelitian tindakan). Menurut (Widi, 2010), Penelitian tindakan adalah suatu penyelidikan atau penelitian dalam konteks usaha yang berfokus pada peningkatan kualitas organisasi atau kinerjanya.

3.1 Desain Penelitian

Penulis melakukan terapan atau tahapan penelitian yang merupakan bagian dari action research ini yaitu :



Gambar 3.1 ***Alur Penelitian***

Sumber : Data Olahan Sendiri

3.1.1 Melakukan diagnosa (*diagnosing*)

Melakukan identifikasi masalah-masalah pokok yang ada guna menjadi dasar kelompok atau organisasi sehingga terjadi perubahan, untuk pengembangan keamanan jaringan Sekolah Charitas pada tahap ini peneliti mengidentifikasi masalah akan keamanan pada jaringan komputer Sekolah Charitas dengan metode *Signature* dibantu dengan aplikasi *Honeypot Dionaea* sebagai penunjang analisis seberapa banyak *malware* yang menyerang system jaringan di Sekolah Charitas.

3.1.2 Membuat rencana tindakan (*action planning*)

Peneliti mendalami pokok masalah yang ada kemudian dilanjutkan dengan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada, pada tahap ini pengembangan keamanan jaringan memasuki tahapan desain dengan melihat topologi jaringan Sekolah Charitas. Dengan memperhatikan kebutuhan terhadap penggunanan jaringan dan keamanan jaringan penelitian memulai melakukan beberapa persiapan seperti daftar alat- alat yang akan dipakai, *Operating System* yang digunakan dan Aplikasi-aplikasi pendukung seperti aplikasi *honeypot dionaea* dan lain-lain. Adapun rincian alat-alat dan bahan sebagai berikut :

Tabel 3.1 *Daftar Hardware*

Sumber: Data Olahan Sendiri

No	*Hardware*	
	Nama Perangkat	Spesifikasi
1	PC Server	Processor Intel Xeon E3-1200, Motherboard Asus Server TS110, Memory RAM 8 GB
2	Laptop	Acer Aspire 4738Z Intel(R) Pentium (R) CPU P6200 2,13GHz (2 CPUs), Memory RAM 2 GB

Tabel 3.2 Daftar *Operating System*

Sumber: Data Olahan Sendiri

No	*Operating System*	
	Nama	Spesifikasi
1	Linux Ubuntu	14.04 LTS
2	Windows 7	Windows 7 Ultimate 64-bit (6.1, Build 7601)

Tabel 3.3 Daftar *Software*

Sumber: Data Olahan Sendiri

No	*Software*	
	Nama	Versi
1	Dionaea	0.8.0
2	Liblcfg	-
3	Libemu	-
4	Libnl	-
5	Libev	-
6	Python 3.2	3.2

7	Cython	3.2
8	Libcurl	14
9	Libpcap	-
10	Winbox Mikrotik	2.2.18

Tabel 3.4 Daftar Perangkat Jaringan

Sumber: Data Olahan Sendiri

No	Perangkat Jaringan	
	Nama Perangkat	Spesifikasi
1	Router Mikrotik	Mikrotik Rb750
2	Konektor RJ45	-
3	Kabel UTP	-

3.1.3 Melakukan tindakan (*action taking*)

Peneliti mengimplementasikan rencana tindakan dengan harapan dapat menyelesaikan masalah. Selanjutnya setelah rencana dibuat, dilanjutkan dengan tahapan tindakan berdasarkan rencana yang ada kemudian peneliti melakukan pemasangan alat-alat yang dibutuhkan seperti penggantian *router* menjadi router mikrotik dengan menyesuaikan settingan jaringan yang sudah ada, kemudian melakukan penginstalan *operating system Ubuntu* pada Pc yang nantinya akan dijadikan server, kemudian penginstalan aplikasi *dionaea* dan beberapa aplikasi pendukung pada *OS* Ubuntu, kemudian menjalankan *dionaea* pada *linux ubuntu*,

lalu melihat hasil dari menjalankan aplikasi *dionaea* tersebut, kemudian setelah mendapatkan hasil dari aplikasi *dionaea,* selanjutnya melakukan *blocking port* pada jaringan Sekolah Charitas dengan menggunakan router mikrotik.

3.1.4 Melakukan evaluasi (*evaluating*)

Setelah melakukan implementasi (*action taking*) dianggap cukup kemudian peneliti melaksanakan evaluasi hasil dari implementasi yang telah dilakukan, dalam tahap ini dilihat bagaimana aplikasi *dionaea* dapat menelusuri *port* mana saja yang sering dilalui oleh *malware* dan dengan menggunakan *router* mikrotik dapat melakukan *blocking port* yang dilalui oleh *malware*.

3.1.5 Pembelajaran (*learning*)

Tahap ini merupakan bagian akhir siklus yang telah dilalui dengan melaksanakan review tahap-pertahap yang telah berakhir kemudian penelitian ini dapat berakhir. Seluruh kriteria dalam prinsip pembelajaran harus dipelajari, perubahan dalam situasi atau keadaan dievaluasi oleh peneliti dan dikomunikasikan kepada klien, peneliti dan klien merefleksikan terhadap hasil penelitian ini, yang nampak akan dilaporkan secara lengkap dan hasilnya

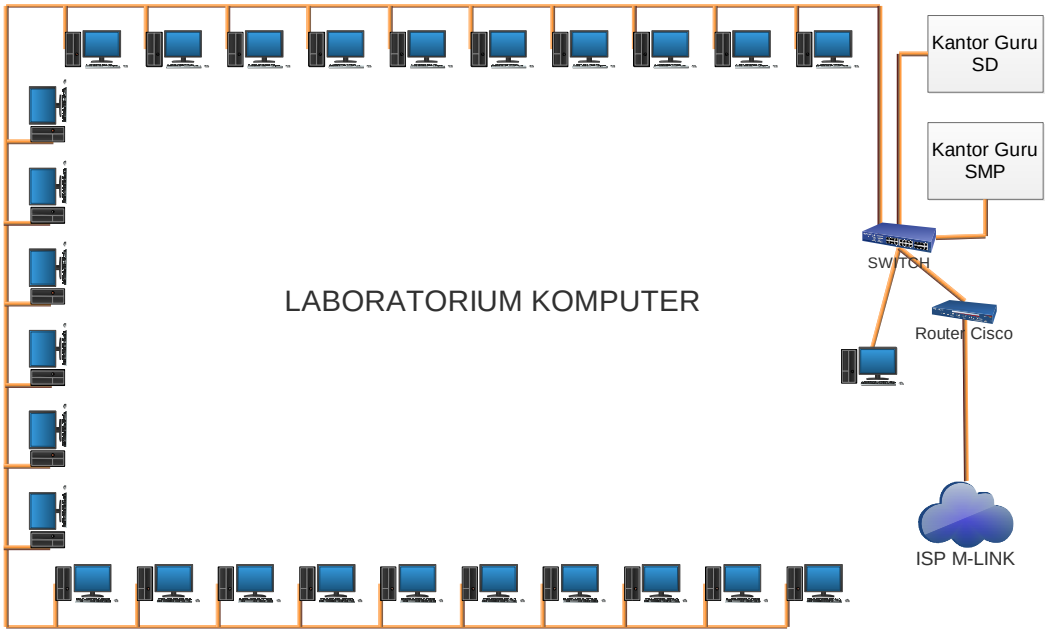
secara eksplisit dipertimbangkan dalam hal implikasinya terhadap penerapan *Canonical Action Reaserch* (*CAR*). Untuk hal tertentu, hasilnya dipertimbangkan dalam hal implikasinya untuk tindakan berikutnya dalam situasi organisasi lebih-lebih kesulitan yang dapat dikaitkan dengan pengimplementasian perubahan proses. Jika ditemukan kegagalan maka akan dilakukan kembali dari Diagnosa dan seterusnya menurut dengan langkah penelitian yang digunakan sampai mendapatkan hasil dari penelitian ini.

3.2 Analisis Jaringan Lama

Pada saat ini jaringan Sekolah Charitas Batam menggunakan topologi star yang komputer-komputer pada setiap ruang di sekolah tersebut antara lain: kantor TU, kantor Guru/Kepala sekolah, Lab.Bahasa dan Lab komputer terhubung dengan menggunakan switch sebagai alat penghubung untuk setiap jalur jaringan.

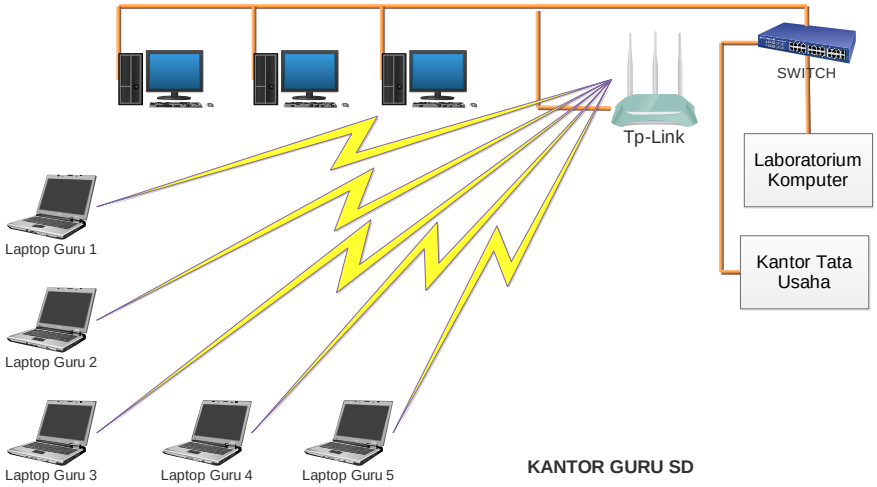
Di lingkungan Sekolah Swasta Charitas Batam saat ini juga menggunakan akses internet yang berbasis *wireless* (*hotspot*) dan kabel pada jaringannya. layanan provider M-link yang berkecepatan 10 Mbps pun digunakan untuk layanan *internet* 24 jam, jumlah user yang mengakses pada jaringan di Sekolah Swasta Charitas Batam adalah 50 user yang menggunakan akses internet sebagai sarana untuk pencarian informasi dan komunikasi baik berada di Laboratorium maupun bagian Kantor Guru/Kepala Sekolah, dan Kantor Administrasi, namun jaringan di lingkungan Sekolah Swasta Charitas ini tidak memiliki keamanan

jaringan yang cukup memadai. Adapun penulis mencantumkan rancangan jaringan pada Sekolah Charitas Batam yang saat ini digunakan, seperti gambar di bawah ini :



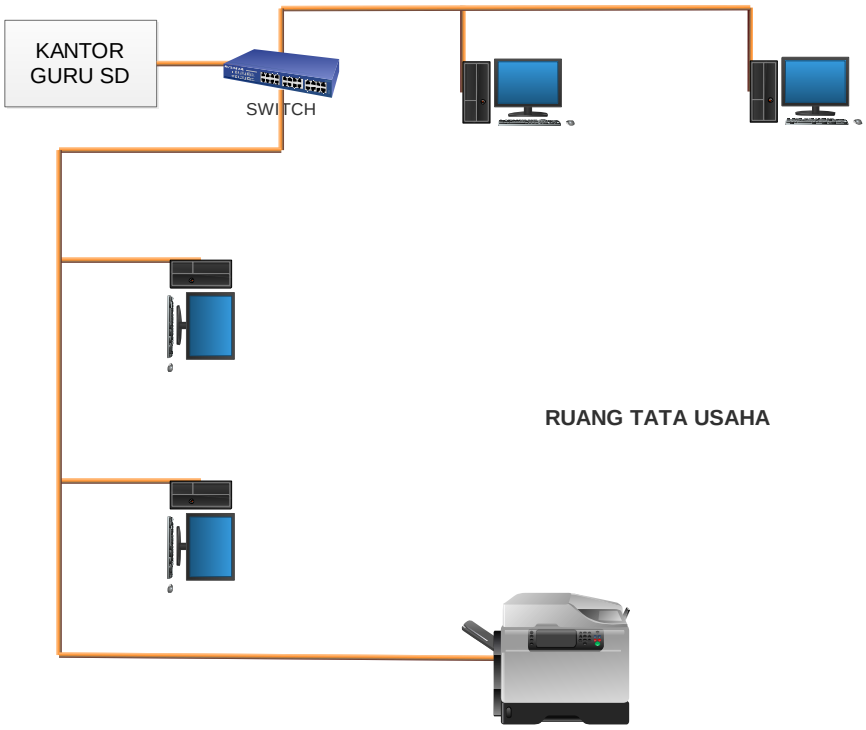
Gambar 3.2 Struktur Jaringan Lama Laboratorium Komputer

Sumber: Data Olahan Sendiri



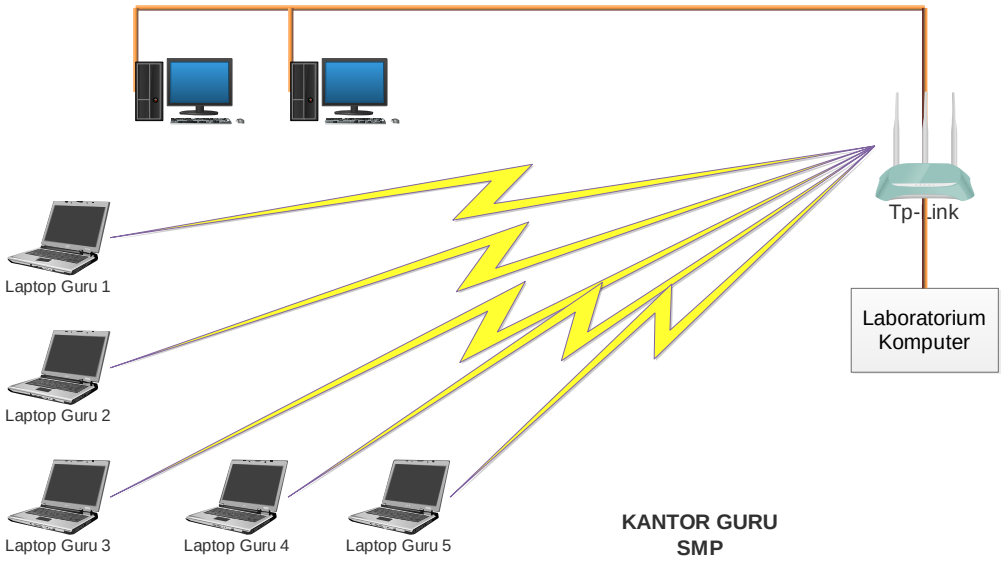
Gambar 3.3 Struktur Jaringan Kantor Guru SD

Sumber: Data Olahan Sendiri



Gambar 3.4 Struktur Jaringan Kantor Tata Usaha

Sumber: Data Olahan Sendiri

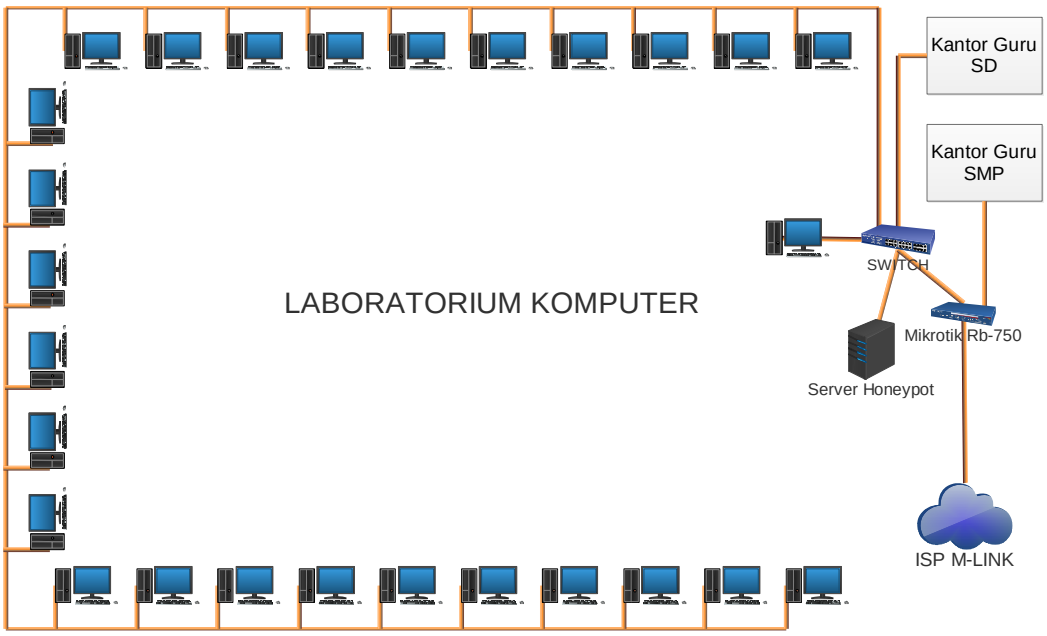


Gambar 3.5 Struktur Jaringan Kantor Guru SMP

Sumber: Data Olahan Sendiri

3.3 Rancangan Jaringan Yang Dibangun

Dalam perancangan jaringan yang dibangun akan mengalami perubahan pada alat yang digunakan tanpa merubah topologi yang sudah diterapkan sebelumnya pada jaringan Sekolah Charitas Batam. Perubahan yang dilakukan adalah menggantikan router biasa dengan router mikrotik RB750, dan penambahan server yang telah disiapkan untuk penunjang sistem keamanan jaringan dengan menggunakan *honeypot dionaea* yang ditempatkan pada ruang laboratorium komputer. Berikut adalah rancangan jaringan yang telah mengalami perubahan:



Gambar 3.6 Struktur Jaringan Baru Laboratorium Komputer

Sumber: Data Olahan Sendiri

3.4 Lokasi dan Jadwal

Berikut ini adalah Lokasi dan Jadwal kegiatan berdasarkan alur yang sudah dijelaskan sebelumnya.

Lokasi Penelitian : Sekolah Charitas Batam

Alamat : Jalan Kaktus Giwang No.1A, Bukit Indah Sukajadi

Tabel 3.5 Jadwal Kegiatan

Sumber: Data Olahan Sendiri

No	Jenis Kegiatan	Waktu Penelitian tahun 2018																			
		September				Oktober				Nopember				Desember				Januari 2019			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Pengajuan Topik																				
2	Studi Literatur																				
3	Pengumpulan Data																				
4	Analisis Data																				
5	Pengolahan Data																				
6	Implementasi																				
7	Penyusunan Draf Laporan																				
8	Monitoring																				
9	Evaluasi																				
10	Perbaikan																				
11	Penulisan Laporan																				