BAB II
LANDASAN TEORI

2.1 Tinjuan Studi

Tinjauan Studi berisikan jurnal yang berhubungan dengan penelitian untuk dijadikan sebagai referensi sekaligus media bertukar informasi dengan fakta yang ada :

Zakir Supratman (2015) yang berjudul Desain dan Implementasi *Network Security* Memanfaatkan *Security Configuration Wizard*. Penulis menjelaskan ancaman dapat dilakukan seseorang untuk mengeksploitasi suatu bagian yang lemah dalam bidang keamanan yang biasa disebut *vulnerability*. Masalah yang diangkat dalam penelitian ini adalah bagaimana *windows firewall* menerapkan rule rule dalam mengamankan sistem. Metode yang digunakan penulis adalah Studi Literatur, Survey, Analisis, Perancangan, Implementasi. Tahapan penelitian ini memeriksa *default setting* baik *server* maupun *client*. selanjutnya membuat aturan yang *meng-Allow Inbound Network Traffic*, dan *mem-Block Outbound Network Traffic*, dilanjutkan dengan menerapkan *Basic Domain Isolation Policy*, mengisolasi s*erver*, membuat s*ecurity group*, dan memodifikasi *Firewall Rule* untuk *Require Group Membership* dan *Encryption*. Pengujian yang dilakukan penulis adalah *Inbound Rule* untuk *mem-allow network traffic*, *menguji Rule* untuk spesifik komputer yang *di-allow inbound traffic*, *menguji Outbound Rule* untuk mengeblok *network traffic*, dan menguji *rule* ketika pengguna 1 bukan anggota member grup. Dari hasil pengujian rules yang telah dibuat untuk memblok *network traffic*, terlihat bahwa ketika salah satu *service* menggunakan *service telnet*, maka *service* tersebut akan gagal, hal ini dikarenakan *firewall* di *server* sekarang memblok seluruh *inbound traffic ke Telnet service*.[7]

Afrizal Feizil (2017), dkk yang berjudul Analisis Keamanan Lalu Lintas Paket Data Pada Ubuntu Menggunakan Metode *Attack Centric*. Penulis menjelaskan Dalam pengamanan lalu lintas keamanan jaringan internet terdapat dua sisi yang berbeda di satu sisi banyak usaha yang dilakukan untuk menjamin keamanan dan kenyamanan suatu jaringan internet sedangkan sisi lainya ada beberapa pihak tertentu yang berusaha melakukan pencurian data dan perusakan

lalu lintas jaringan internet. Bentuk dari serangan tersebut bisa juga disebut *ARP Poison, DNS Spoofing*, pada dasarnya korban tidak akan mengenali dampak dari serangan tersebut. Metode yang digunakan adalah a*ttack centrik* dalam metode ini terdapat tiga tahapan yang dilakukan tahap pertama menganalisa tujuan dari serangan, tahapan kedua menganalisa bagaimana serangan dapat terjadi sedangkan tahapan ketiga menentukan cara untuk menghindari serangan tersebut. Hasilnya penulis mampu melihat semua aktifitas yang ada pada jaringan dan dapat lakukan serangan *DNS Spoofing*.[3]

M. Ferdy Adriant dan Is Mardianto (2015) yang berjudul Implementasi *Wireshark* Untuk Penyadapan *(Sniffing)* Paket Data Jaringan. Penulis menjelaskan *Sniffing* merupakan aktivitas penyadapan paket data pada jaringan komputer, dampak negatif dari *sniffing* adalah seseorang dapat melihat informasi penting separti *username dan password* semetara dampak positif dari *sniffing* seorang admin jaringan dapat menganalisa paket-paket yang lewat pada jaringan untuk keperluan perbaikan pada jaringan. Untuk percobaan penulis menggunakan tools *wireshark* untuk melakukan aksi *sniffing*, dari hasil percobaan penulis kesulitan untuk menganalisa karena hasil capture dari *wireshark* menampilkan seluruh aktivitas yang ada di jaringan setelah itu penulis mencoba melakukan pemfilteran pada protokol *HTTP*. Setelah dilakukan *pen-capture-an* pada protokol *HTTP*, lakukan analisis pada paket yang berisikan data *POST*. Pada data *POST* tersebut penulis dapat melihat beberapa informasi seperti, alamat *IP, source* dan *destination, port TCP, source port destination*, lalu terdapat informasi HTTP yang berisi PO*ST, host, connection, content-length, origin, user-agent,* dan yang paling penting *HTML form URL* yang berisi *username dan password*.[8]

2.2 Tinjauan Pustaka

2.2.1 Jaringan Komputer

Jaringan komputer merupakan suatu sistem yang terdiri dari komputer dan perangkat jaringan lainya guna mencapai tujuan tertentu, jaringan komputer yang paling sederhana terdiri atas dua buah node. Jaringan tersebut dapat disusun dengan dua buah komputer atau perangkat keras.[9]

2.2.2 Jenis-Jenis Jaringan Komputer

Berdasarkan geografisnya jaringan komputer terbagi ke beberapa bagian diantaranya :

2.2.2.1 Local Area Network (LAN)

Merupakan sebuah jaringan yang bersifat pribadi atau lokal, jaringan ini pada umumnya digunakan pada ruang lingkup kecil seperti dalam suatu ruangan kantor, lab sekolahan, dan kampus. Tujuan penggunaan model. Jaringan seperti ini untuk berbagi sumber daya atau bertukar informasi.[9]

2.2.2.2 Metropolitan Area Network (MAN)

Merupakan sebuah jaringan komputer dengan ukuran menengah, jaringan MAN pada dasarnya tersusun dari beberapa gabungan jaringan LAN di dalamnya. Jaringan ini biasanya bertujuan untuk membangun hubungan antar kantor-kantor dalam satu kota antara pabrik/instansi dan kantor pusat yang berada dalam jangkauannya.[9]

2.2.2.3 Wide Area Network (WAN)

Merupakan jaringan dalam ruang lingkup besar, jaringan ini menghubungkan jaringan MAN menjadi suatu jaringan besar dengan beberapa macam layanan di dalamnya. Jaringan WAN dapat mencakup yang sangat luas bahkan bisa menghubungkan jaringan komputer antar negara, jaringan internet dapat juga dikategorikan sebagai jaringan WAN.[9]

2.2.3 Perangkat Keras Jaringan Komputer

Perangkat keras jaringan komputer merupakan alat yang dapat dilihat secara fisik yang saling terhubung sehingga dapat terciptanya suatu jaringan komputer. ada beberapa jenis perangkat keras jaringan komputer diantaranya :

2.2.3.1 Network Interface Card (NIC)

NIC bisa juga disebut LAN card merupakan suatu perangkat yang berfungsi sebagai penghubung dari sebuah komputer ke sebuah jaringan komputer, perangkat ini biasanya sudah terpasang secara langsung pada komputer maupun laptop.[10]

2.2.3.2 Kabel Jaringan

Kabel dalam jaringan bertujuan sebagai media penghubung, walaupun saat ini sudah ada teknologi *wireless* (tanpa kabel) namun kabel masih sering

digunakan karena mudah dalam pengoprasianya. Ada berapa macam tipe kabel dalam jaringan internet diantaranya :

1. **Kabel Twister Pair**

   Kabel ini terdiri dari beberapa kabel yang melilit, ada dua macam kabel yang termasuk kategori kabel ini yaitu Shielded Twisted Pair (STP) dengan lapisan alumunium foil dan Unshielded Twisted Pair (UTP). Kedua kabel ini pada dasarnya sama, perbedaanya hanya kabel UTP rentan terhadap medan magnet atau voltase yang tinggi sementara kabel STP tidak.[10]

2. **Kabel Coaxial**

   Bentuk kabel ini terdiri dari kawat tembaga sebagai inti kemudian dilapisi oleh isolator dalam lalu dilapisi dengan konduktor luar kemudian dibalut bahan semacam *Polivinil Clorida* (PVC) sebagai lapisan paling luar. Pada umumnya kabel ini sudah jarang digunakan, karena orang memilih membangu jaringan dengan kabel twisted pair. kabel coaxial terbagi menjadi dua macam yaitu :

   1. **Thick Coaxial**

      Digunakan untuk kabel backbone pada jaringan instalasi *Ethernet* antar gedung.[8]

   2. **Thin Coax**

      Kabel ini lebih dikenal dengan 10 Base 2 sangat cocok untuk network rumahan atau kantor dengan dua atau tiga komputer.[10]

   3. **Kabel Fiber Optic**

      Kabel ini terbuat dari serat kaca dengan teknologi canggih dan memiliki kecepatan mengirim file lebih cepat dari kabel biasa, kabel ini banyak digunakan oleh jaringan LAN, MAN, dan WAN karena dapat memberikan dampak yang lebih pada kecepatan.[10]

2.2.3.3 Konektor

Konektor berfungsi sebagai media penghubung antara kabel dan colokan NIC yang ada pada komputer.[10]

2.2.3.4 Hub

Hub merupakan perangkat jaringan yang beroperasi di *OSI layer* 1, *physical layer*. Perangkat tersebut sebagai penyambung atau concentrator, dan menguatkan sinyal di kabel UTP., jumlah port dalam hub mulai dari 8 - 32 port. Pada umumnya hub digunakan untuk menyatukan kan kabel-kabel network dari tiap workstation, server atau berangkat lainya.[10]

2.2.3.5 Switch

Switch merupakan perangkat jaringan yang beroperasi di OSI layer 2, data link layer. Switch pada dasarnya sama dengan hub, namun switch lebih canggih karena switch mampu menganalisa paket data yang dilewatkan padanya sebelum dikirim ke tujuan.[10]

2.2.3.6 Repeater

Repeater merupakan alat untuk memperkuat sinyal, sinyal yang diterima dari satu segmen kabel LAN ke kabel LAN berikutnya akan dipancarkan kembali dengan kekuatan sinyal asli pada segmen LAN pertama sehingga dengan adanya perangkat ini jarak antar komputer dapat diperluas.[10]

2.2.3.7 Router

Router mempunyai kemampuan untuk memfilter lalu lintas data berdasarkan aturan protokol tertentu, router juga dapat digunakan membangun jaringan LAN, MAN, dan WAN.[10]

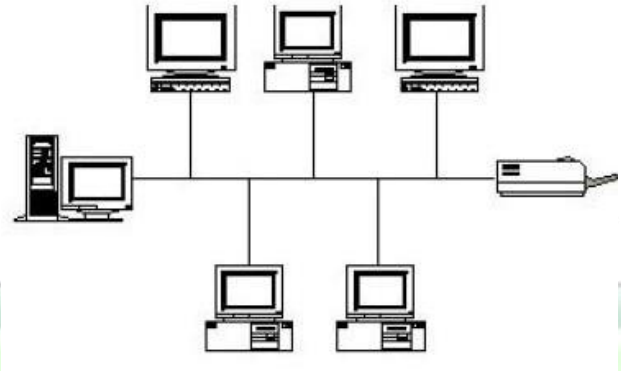
2.2.3.8 Modem

Modem berfungsi sebagai penghubung jaringan LAN dan Internet untuk melakukan tugasnya, modeng juga dapat mengubah data digital ke data analog agar bisa dipahami manusia begitu juga sebaliknya.[10]

2.2.4 Topologi Jaringan

Topologi jaringan merupakan suatu metode atau cara yang digunakan untuk menghubungkan komputer satu dengan komputer lainya, ada beberapa macam topologi jaringan diantaranya :

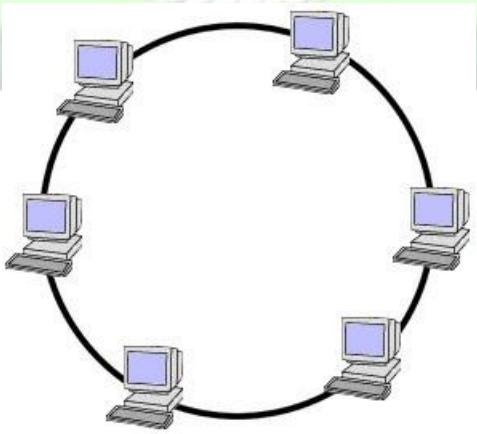
2.2.4.1 Topologi Bus



Gambar 2. 1 Topologi Jaringan Bus

Topologi Bus merupakan sebuah topologi yang menghubungkan semua node dengan kabel yang memiliki dua buah ujung, di dua ujung kabel dipasang terminator yang bertujuan mencegah hilangnya sinyal pada kabel. Keuntungan menggunakan topologi ini yaitu strukturnya yang terbilang sederhana dan tidak boros kabel, sedangkan kekurangannya menggunakan topologi ini adalah sulitnya menganalisa kesalahan pada kesalahan jaringan dan padatnya lalu lintas data pada jaringan. Jika ada satu node yang terputus, maka seluruh jaringan akan terkena dampaknya.[9]

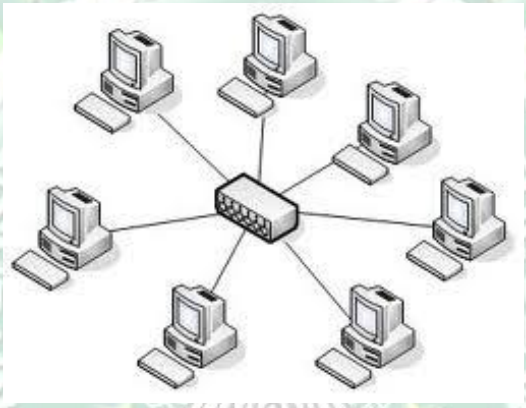
2.2.4.2 Topologi Ring



Gambar 2. 2 Topologi Jaringan Ring

Topologi Ring merupakan merupakan suatu metode menghubungkan komputer berbentuk lingkaran, topologi ini membuat data dikirim ke setiap node dalam jaringan. Informasi yang diterima oleh suatu akan diperiksa terlebih dahulu apakah data yang dikirim untuk node tersebut atau bukan. Keuntungan menggunakan topologi ini yaitu hematnya penggunaan kabel sedangkan kerugiannya adalah pekanya terhadap kesalahan dan kakunya dalam pengembangan jaringan.[9]

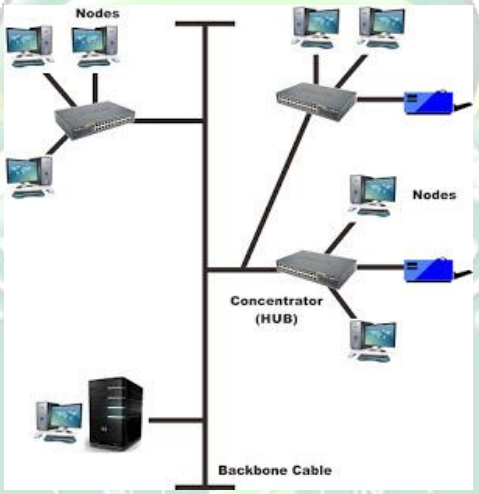
2.2.4.3 Topologi Star



Gambar 2. 3 Topologi Jaringan Star

Topologi Star merupakan suatu topologi yang di mana semua node dihubungkan melalui suatu node yang terpusat. Titik pusat jaringan ini atau *concentrator* berupa Hub atau Switch, semua data yang ditransmisikan antar node akan melalui titik pusat tersebut. Penggunaan topologi ini memberikan kontrol yang terpusat, perubahan atau gangguan tidak akan berdampak pada semua jaringan sedangkan kelemahan topologi ini jika perangkat *concentrator* mengalami kerusakan maka seluruh node akan terganggu.[9]

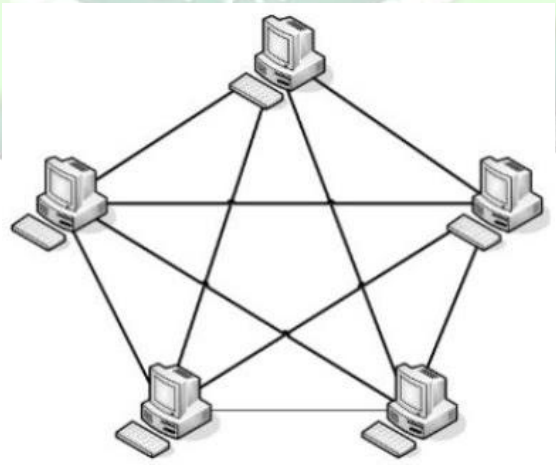
2.2.4.4 Topologi Tree



Gambar 2. 4 Topologi Jaringan Tree

Topologi Tree merupakan topologi yang dimana semua node-node terhubung secara tersusun dengan rapi.[9]

2.2.4.5 Topologi Mesh



Gambar 2. 5 Topologi Jaringan Mesh

Topologi Mesh merupakan topologi yang node dalam jaringan dapat terhubung dengan node-node lainya secara tidak beraturan. Satu node dalam jaringan ini memiliki lebih dari satu koneksi ke node lainya.[9]

2.2.5 Media Penghantar Jaringan

Pada dasarnya media penghantar yang digunakan komputer terbagi menjadi dua macam yaitu :

1. **Wire Network (Jaringan Berkabel)**

   Wire network merupakan jaringan komputer yang memanfaatkan kabel sebagai media penghantar, Kabel yang sering digunakan pada jaringan komputer biasanya berbahan dasar tembaga, ada juga yang menggunakan kabel berbahan dasar *fiber optik* atau serat optik. kebanyakan jaringan LAN menggunakan kabel berbahan dasar tembaga, sedangkan MAN dan WAN menggunakan gabungan kabel tembaga dan serat optik.[11]

2. **Wireless Network (Jaringan Tanpa Kabel)**

   Wireless network merupakan jaringan komputer tanpa kabel yang memanfaatkan gelombang radio atau cahaya sebagai media penghantar. Saat ini sudah banyak pusat perbelanjaan, airport, rumah sakit dan masih banyak lokasi lainya menyediakan layanan wireless network. sehingga mempermudah pengguna mengakses internet menggunakan *handphone,* laptop, PDA dan perangkat *mobile* lainya.[11]

2.2.6 Computer Security

Sebelum membahas tentang *network security* ada baiknya kita mengenal *computer security.* Menurut Garfinkel, seorang pakar *security,* keamanan komputer mencakup empat bagian yaitu :

1. ***Privacy atau Confidentiality***

   Privacy mencakup tentang kerahasian informasi, inti dari bagian ini adalah menjaga suatu informasi agar tidak dilihat atau diakses oleh orang yang tak berhak. Sebagai contoh email seorang pengguna tidak boleh dibaca oleh

orang lain bahkan seorang administrator. Maka salah satu usaha yang dapat dilakukan adalah menggunakan *enkripsi*.[11]

2. ***Integrity***

   Integrity mencakup tentang keutuhan informasi atau keaslian informasi, inti dari bagian ini adalah bagaimana cara untuk menjaga informasi agar tetap utuh dan dijamin keaslianya tidak boleh diubah baik ditambah atau dikurangi. Virus seperti *trojan horse* atau lainya dapat mengganggu bagian dari *integrity*, maka dengan menggunakan anti virus, *enkripsi*, dan *digital signature* merupakan sebuah usaha untuk mengatasi masalah ini.[11]

3. ***Authentication***

   Authentication merupakan hal berkaitan dengan pengesahan oleh sang pemilik informasi, harus ada cara supaya mengetahui bahwa informasi benar benar asli dan yang bisa mengaksesnya adalah orang yang berhak[11]. Penggunaan sistem login, *digital signature*, dan *watermarking* merupakan usaha yang dapat dilakukan agar yang bisa mengakses informasi tersebut hanya orang orang yang berhak saja.[11]

4. ***Availability***

   Availability merupakan sebuah tahapan yang berhubungan dengan ketersediaan informasi. informasi harus tetap tersedia manakala sedang dibutuhkan. Kasus serangan terhadap tahapan ini adalah *denial of service aspek.* Contohnya, server dikirimi *request* palsu secara bertubi tubi sehingga tidak dapat menjalankan permintaan lainnya. Kasus lainya yaitu *mailbomb*, dimana seorang pengguna dikirimi ribuan email secara serentak sehingga pengguna tersebut kesulitan bahkan tidak bisa membuka emailnya[11]

Berhubungan dengan tahapan keamanan diatas, menurut W. Stallings, ada beberapa hal yang memungkinkan terjadinya serangan pada keamanan sistem informasi yaitu :

1. ***Interruption***

Sistem diganggu sedemikian rupa sehingga informasi tidak dapat diakses. Serangan ini ditujukan terhadap tahapan *Availability.*[11]

2. ***Interception***

Pihak yang tidak berhak berhasil mendapat akses asset atau informasi. Contoh kasus serangan ini adalah "*wiretapping"*serangan ini ditujukan terhadap tahapan *privacy.*[11]

3. ***Modification***

Pihak yang tidak berhak berhasil mendapat akses informasi tidak hanya itu namun dapat juga mengubah isi informasi tersebut. Serangan ini ditujukan terhadap tahapan *integrity*.[11]

4. ***Fabrication***

Pihak yang tidak berhak menyisipkan informasi yang palsu ke sebuah sistem, contohnya mengirim pesan-pesan palsu ke dalam jaringan komputer. Serangan ini ditujukan terhadap aspek *authentication.*[11]

Ada beberapa orang yang beranggapan *computer security* sama dengan *information security* (keamanan informasi). Menurut G. J. Simons, keamanan informasi merupakan bagaimana cara kita mencegah adanya penipuan paling tidak mendeteksi adanya penipuan di sebuah sistem yang berisi informasi. Baik *computer security* maupun *information security* sama sama memiliki tujuan yang sama yaitu sama-sama melindungi. Akan tetapi, ada beberapa perbedaan diantara keduanya perbedaan yang paling utama terletak pada pendekatan *(approach),* metode yang digunakan *(methodology),* dan fokus pada tujuan *(areas of concentration). Informasi security* fokus pada *confidentiality, integrity,* dan *availability* berbagai data yang berkaitan dengan dimana data tersebut disimpan. Sedangkan *computer security* fokus pada *confidentiality, integrity,* dan *availability* yang berkaitan dengan proses yang dilakukan oleh komputer.[11]

2.2.7 Network Security

Network security merupakan suatu upaya atau usaha yang dilakukan guna mengamankan sebuah jaringan, khususnya melindungi usability, reliability,

integrity, dan safety dari jaringan data. Tujuan utama dari network security adalah mencegah dan menghentikan berbagai macam potensi terjadinya serangan. berbagai macam ancaman. Ada beberapa macam serangan serangan pada jaringan diantaranya :

1. ***Brute Force and Dictionary***

   Merupakan jenis serangan dengan target database, serangan ini bertujuan untuk menemukan password dari seorang pengguna secara sistematis menggunakan gabungan dari angka,huruf dan simbol. Untuk menghindari serangan ini hindari penggunaan password yang mudah ditebak contohnya seperti nama, tanggal lahir, nomor handphone dan sebagainya.[12]

2. ***Denial of service attacks (DoS)***

   Merupakan jenis serangan yang membuat segala jenis layanan pada jaringan terganggu, bentuk umum dari serangan ini adalah dengan cara mengirimkan sebuah paket ke sebuah server dalam jumlah yang sangat besar sehingga server tidak dapat memprosesnya. *DoS* merupakan salah satu dari beberapa jenis serangan yang paling menakutkan, karena dampak dari serangan ini adalah server bisa lumpuh dan tidak bisa memberikan layanan. Untuk mengatasi serangan ini sebaiknya :

   1. Menutup protokol yang dianggap tidak perlu melalui firewall.[12]
   2. Menonaktifkan IP directed broadcast untuk subnetwork dalam domain.[12]
   3. Gunakan filter paket hanya untuk mengijinkan paket paket dengan IP yang sah.[12]

3. ***Spoofing***

   Merupakan jenis serangan untuk memperoleh akses yang tidak sah sesuatu komputer atau informasi, hacker berpura pura bahwa mereka adalah host yang dapat dipercaya. Seorang hacker menaruh sebuah link palsu atau yang sudah mereka hack pada web yang populer, sementara kita menggunakan mesin pencari seperti google, yahoo, dan bing untuk mendapatkan sebuah informasi. Tanpa kita sadari beberapa link diantaranya mungkin milik seorang hacker.[12]

4. ***Man In The Middle Attack***

   Merupakan sebuah serangan yang berada di tengah-tengah sehingga seorang hacker bebas untuk mendengarkan percakapan oleh kedua pengguna. Serangan ini tidak hanya bisa mendengarkan tapi seorang hacker juga bisa mengubah jenis percakapan dari salah satu pihak.[12]

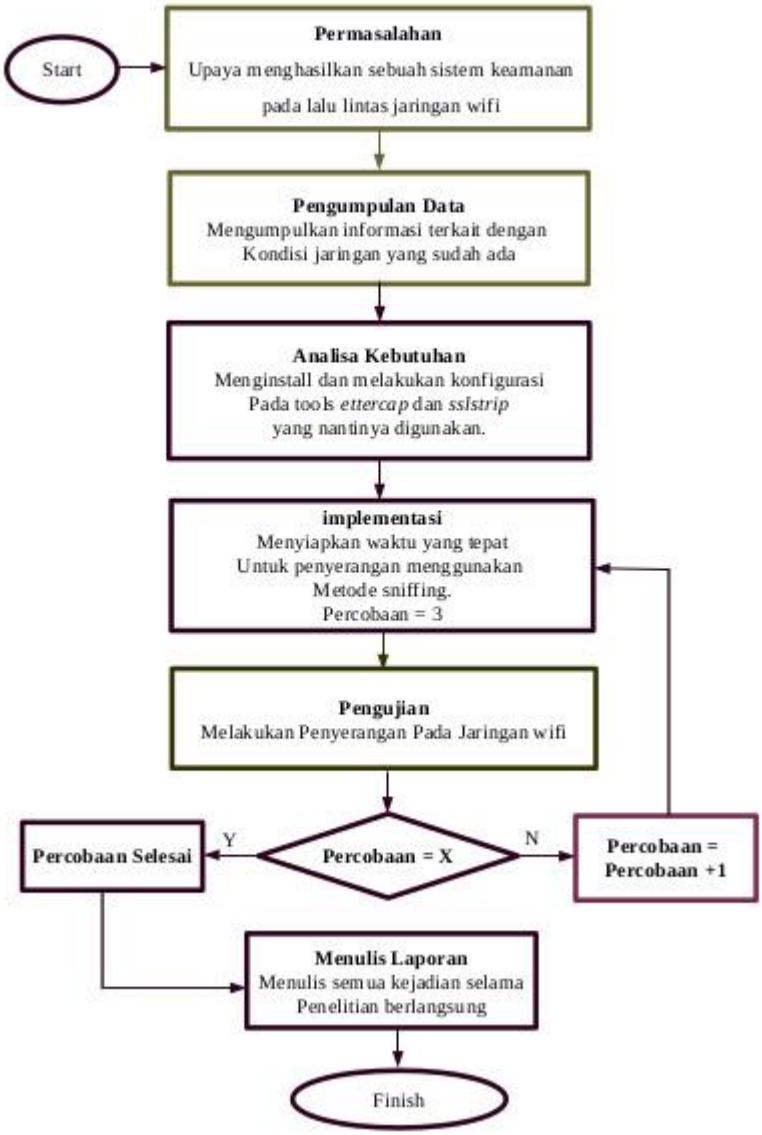
5. ***Sniffing***

   Sniffing merupakan penyadapan pada jaringan komputer, serangan ini sangat ditakuti karena dengan menggunakan teknik ini seorang hacker dapat dengan mudah mencuri informasi-informasi penting dari seorang pengguna dari sebuah jaringan.[12]

Berdasarkan ancaman serangan diatas maka tidak mungkin mencari solusi tunggal untuk melindungi jaringan kita dari ancaman serangan. Kita memerlukan berbagai lapisan keamanan, apabila lapisan pertama jebol maka masih ada lapisan kedua sebagai penjaga. Sebagai contoh misal sebuah jaringan sudah dilengkapi oleh sebuah firewall anti virus, mungkin saja dapat dijebol oleh virus-virus terbaru yang belum dikenali oleh firewall tersebut. Oleh karena itu komputer komputer yang ada di dalam jaringan tersebut perlu menjalankan aplikasi anti virus yang selalu terupdate guna meminimalisir terjadinya serangan. Cara yang baik digunakan untuk mengamankan sebuah jaringan adalah menggunakan *server proxy*. Karena *server proxy* dapat mengatur dan menyeleksi informasi yang keluar masuk dalam jaringan internal. Namun proxy bukanlah anti virus, jadi kalau kita ingin mengamankan jaringan dari virus yang kita butuhkan adalah membangun dua lapisan *security*. Lapisan pertama untuk akses kontrol di bangun dengan *proxy server*, Sedangkan lapisan kedua untuk mencegah virus dapat ditangani oleh aplikasi anti virus.[11]

2.3 Kerangka Pemikiran

Kerangka berpikir dibuat digunakan untuk mempermudah pemahaman sebuah penelitian, alur dalam penelitian tersaji dalam bentuk *flowchart.*



Gambar 2. 6 Kerangka Pemikiran