BAB I
PENDAHULUAN

1.1 Latar Belakang

Jaringan komputer saat ini perkembangan dengan sangat pesat, kemudahan manusia mendapatkan informasi dari sejarah perkembangan komputer yang begitu panjang sehingga kita dapat menikmati fasilitas dari jaringan komputer. Begitu juga perkembangan jaringan wireless (nirkabel / tanpa kabel) semenjak hadirnya teknologi informasi dan komunikasi komputer, netbook, *Personal Digital Assistant* (PDA), *Telepon Seluler* (handphone) sangat mendominasi dalam pemakaian jaringan wireless. Penggunaan jaringan wireless yang diterapkan dalam suatu jaringan lokal sering disebut *wireless local area network* (WLAN), seiring perkembangan zaman teknologi jaringan wireless menjadi kebutuhan seseorang untuk dapat berkomunikasi data maupun suara. Jaringan *wireless* merupakan teknologi jaringan komputer tanpa menggunakan kabel, cara kerja teknologi ini mengandalkan gelombang berfrekuensi tinggi sehingga komputer-komputer bisa saling terhubung satu sama lain tanpa menggunakan kabel. Pada dasarnya ada beberapa jenis frekuensi *wireless* yaitu *IEEE 802.11b* dengan frekuensi *2.4GHz* frekuensi ini memiliki rate data sebesar 1Mbps sampai 11Mbps dengan daya jangkau maksimun 350ft atau 105 meter. *IEEE 802.11g* dengan frekuensi *2.4GHz* frekuensi ini memiliki rate data sebesar 6Mbps sampai 54Mbps dengan jangkauan maksimum kurang lebih 300ft atau 90meter. *IEEE 802.11a* adalah standar wifi dengan frekuensi *5GHz* frekuensi ini memiliki rate data sebesar 6 Mbps sampai 54Mbps dengan daya jangkau maksimum kurang lebih 60meter. [1]

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 *Address Resolution Protocol* (ARP) *Poison*, ARP *Poison* merupakan teknik penyerangan jaringan lokal komputer baik menggunakan media kabel maupun tanpa kabel,

yang memungkinkan penyerang bisa melakukan pengendusan pada *frame* data jaringan lokal, memodifikasi *traffic* dan menghentikan *traffic.* ARP *Poison* merupakan konsep dari serangan *Man in The Middle Attack (*MITM*)* prinsip serangan ini adalah dengan memanfaatkan kelemahan jaringan komputer itu sendiri yang menggunakan ARP *broadcast.*[2] Sedangkan *Domain Name Server* (DNS) *Spoofing* merupakan salah satu metode hacking MITM, konsep dari serangan ini hampir sama dengan ARP *Poison* namun yang membedakan adalah penyerang membedakan alamat IP dengan sebuah *domain.* DNS merupakan *Server* yang digunakan untuk mengetahui IP *address* suatu *host* lewat *host namenya.* Di dalam dunia internet komputer berkomunikasi satu sama lain dengan menggunakan IP *address,* tetapi bagi manusia tidak mungkin menghafal IP address tersebut, manusia sering menggunakan kata kata seperti *www.google.com*, *www.gmail.com*, *www.facebook.com.* DNS bertujuan untuk mengkonversikan nama yang bisa manusia ke dalam IP address host yang bersangkutan untuk melakukan sebuah komunikasi, pada dasarnya korban tidak akan mengenali dampak dari serangan tersebut. Umumnya di dalam dunia maya siapa saja bisa terserangan seperti serangan diatas oleh karena itu admin sebuah jaringan dan Pengguna harus tau sifat dalam serangan tersebut agar dapat menemukan solusi bertahan yang tujuan untuk mempertahankan diri serangan pencurian data ataupun perusakan jaringan.[3]

Sniffer paket (penyadapan paket) bisa disebut juga dengan *Network Analyzers* atau *Ethernet Sniffer* adalah sebuah aplikasi yang berfungsi sebagai melihat aktivitas lalu lintas sebuah jaringan. Sniffing merupakan aktivitas penyadapan paket data melalui lalu lintas sebuah jaringan. Contohnya, ada seorang pengguna memakai komputer yang terhubung dalam suatu jaringan lokal. Pada saat pengguna tersebut mengirimkan data kepada temannya yang berada di luar kota, maka data tersebut akan dikirimkan melalui komputer pengguna melewati gateway internet lokal, kemudian dari jaringan lokal diteruskan ke internet barulah data tersebut sampai ke temannya. Pada saat data melewati gateway jaringan lokal inilah aktifitas sniffing dapat dilakukan oleh pihak pihak yang tak bertanggung jawab. Dengan aktivitas ini data yang dikirimkan pengguna

tadi dapat di capture sehingga isinya dapat dibaca oleh pihak yang melakukan sniffing.[3] Aksi *sniffing* dibedakan menjadi dua yaitu *sniffing* aktif dan pasif, *sniffing* pasif melakukan penyadapan tanpa mengubah data atau paket apapun dalam jaringan sedangkan *sniffing* aktif melakukan penyadapan dengan mengubah atau merusak paket data dalam jaringan. Pada dasarnya cara kerja *sniffing* dibedakan ke beberabagain yaitu *collecting, conversion, analysis* dan pencurian data. Cara kerja *sniffing collection* dengan mengubah interface yang digunakan menjadi *promicius mode* dan mulai mengumpulkan data yang lewat dalam bentuk binary, *sniffing conversion* dengan mengubah data data yang berbentuk binary ke dalam bahasa yang mudah dipahami, *sniffing analysis* mengklasifikasikan data yang sudah di *conversion* ke dalam blok protokol yang berdasarkan sumber transmisi, sedangkan yang terakhir adalah tahapan pencurian data setelah melewati tahapan - tahapan *collecting, conversion, analysis* maka hacker dengan mudah mencuri informasi penting dalam jaringan.[4]

Saat ini Madrasah Aliyah (MA) Masalikil Huda Tahunan sekolah ini telah menerapkan sistem jaringan komputer menggunakan kabel maupun tanpa kabel sebagai media pertukaran data informasi dan akademik. Kondisi jaringan yang ada saat ini terpusat di MA Masalikil Huda, kemudian dibagi ke beberapa tempat yaitu ke Madrasah Tsanawiyah (MTS) Masalikil Huda, Madrasah Ibtidaiyah (MI) Masalikil Huda, dan yang terakhir Yayasan Masalikil Huda. Tiap-tiap bagian memiliki jumlah komputer yang berbeda, MA Masalikil Huda memiliki jumlah komputer sebanyak 37 yang di terbagi ke beberapa ruangan 30 untuk laboratorium, 2 komputer untuk server, 1 komputer untuk perpustakaan 5 komputer untuk kantor. MTS Masalikil Huda memiliki 33 komputer yang terbagi ke 2 ruangan yaitu 30 untuk laboratorium, 3 komputer untuk kantor. MI Masalikil Huda hanya memiliki 5 komputer yang terletak di kantor sedangkan yayasan Masalikil Huda hanya ada 2 komputer. Dalam jaringan tersebut sebagian besar digunakan oleh para siswa/siswi, guru staff dan karyawan. Dengan kondisi jaringan yang hanya berpusat di MA Masalikil Huda dirasa kurang efektif karena apa bila terjadi salah satu bagian gedung mengalami kerusakan jaringan maka staff IT akan kesulitan menelusuri alur pada bagian mana jaringan yang rusak,

Oleh karena itu peneliti perlu melakukan pengujian keamanan jaringan yang ada di MA Masalikil Huda dari serangan paket data atau sniffing.

Pada penelitian ini peneliti mengacu pada jurnal Irawan Dedi yang berjudul Analisis Dan Penyadapan Transmisi Paket Data Jaringan Komputer Menggunakan *Wireshark* (2017). Peneliti menjelaskan bahwa selama komunikasi data tidaklah penting seperti berkomunikasi menggunakan email, pesan ke wall facebook tidak ada masalah menggunakan koneksi HTTP. Misal ada aksi sniffing dan berhasil mengintipnya dampaknya tidak begitu berpengaruh, Namun bagaimana jika data data yang dikirimkan bersifat rahasia dan pribadi. Peneliti menggunakan *tool sniffing wireshark* yang sudah sangat terkenal karena dengan menggunakan tools ini bisa dengan mudah mendapatkan capture dengan paket data secara langsung dari sebuah *network interface*, mampu menampilkan informasi-informasi secara detail mengenai informasi yang sifatnya begitu penting dan rahasia seperti username dan password.[5]

Netcut merupakan salah satu aplikasi jenis interruption yang banyak digunakan oleh para pelaku serangan pada jaringan komputer. Netcut adalah aplikasi berfungsi untuk melakukan pemotongan terhadap akses jaringan wireless. Jika ada seseorang berada dalam jaringan wireless yang terhubung ke jaringan internet, penguna tersebut dapatmemutuskan koneksi *wireless* pengguna lain yang ada dalam satu jaringan, sehingga client yang lain tidak dapat terhubung ke jaringan. Alasan penggunaan netcut biasanya agar pelaku pengguna netcut dapat memanfaatkan seluruh fasilitas jaringan internet yang ada, seperti bandwidth, karena dalam satu jaringan, hanya terdapat satu user, sedangkan user yang lain aksesnya di potong.[6]

Dalam melihat permasalahan diatas peneliti akan menganalisa wifi yang terdapat di MA Masalikil Huda dari serangan paket data (*Sniffing)* dengan adanya penelitian ini diharapkan dapat memberikan rasa aman dan nyaman bagi pengguna yang menggunakan fasilitas jaringan wifi yang diberikan MA Masalikil Huda.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah dapat dirumuskan masalah sebagai berikut :

1. Bagaimana upaya untuk menghasilkan sebuah sistem keamanan pada lalu lintas jaringan wifi ?
2. Bagaimana melakukan upaya mendeteksi serangan pada lalu lintas jaringan wifi ?

1.3 Batasan Masalah

Dalam penyusunan tugas akhir ini peneliti membatasi masalah yang akan dianalisa yaitu :

1. Peneliti hanya melakukan analisa keamanan jaringan dengan metode *sniffing.*
2. Peneliti hanya melakukan analisa pada jaringan wifi yang berada di MA Masalikil Huda.
3. Peneliti hanya menggunakan tools *ettercap, sslstrips* dan *arp spoof*
4. Peneliti tidak melakukan penerapan pengamanan jaringan, hanya memberi saran skema jaringan guna mengantisipasi terjadinya serangan.

1.4 Tujuan Penelitian

Tujuan dalam penelitian analisa keamanan jaringan MA Masalikil Huda. menggunakan metode *sniffing* sebagai berikut:

1. Memberikan rekomendasi atau saran berupa *software* untuk mendeteksi apabila terjadi serangan jaringan
2. Melindungi pengguna yang terhubung pada jaringan dari serangan paket data *sniffing*

1.5 Manfaat Penelitian

1.5.1 Bagi Peneliti

1. Dapat menerapkan secara langsung ilmu keamanan jaringan.
2. Menambah kemampuan penetrasi testing dibidang keamanan jaringan.

1.5.2 Bagi Sekolah

1. Melindungi pengguna dari ancaman serangan yang terhubung pada jaringan.

1.5.3 Bagi Pengguna

1. Memberikan rasa aman dan nyaman saat terhubung kedalam jaring.
2. pengguna dengan nyaman menggunakan fasilitas jaringan internet tanpa ada gangguan dari pihak-pihak yang tidak bertanggung jawab.

1.6 Sistematika Penulisan

Sebagai acuan bagi penulis agar penulisan dapat terarah sesuai dengan penulis harapkan. Maka disusun sistematika penulisan sebagai berikut :

BAB I PENDAHULUAN

Bab ini mengemukakan latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan yang masing-masing dijelaskan tiap bab.

BAB II LANDASAN TEORI

Bab ini menguraikan tentang pengertian dan teori yang digunakan sebagai landasan atau dasar dari penelitian.

BAB III METODE PENELITIAN

Bab ini menjelaskan mengenai metode yang digunakan dalam penelitian yaitu metode pengumpulan data dan metode pengembangan sistem.

BAB IV PEMBAHASAN

Bab ini akan membahas tentang hasil penelitian tentang Penerapan Metode Sniffing dalam Analisa Keamanan MA Masalikil Huda Dengan Metode Sniffing.

BAB V PENUTUP

Bab ini berisi kesimpulan dari penelitian disertai saran untuk pengembangan lebih lanjut.