DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Seiring berjalannya waktu, perkembangan teknologi amat sangat pesat. Hal itu tentu saja tidak terlepas dari peran jaringan yang dapat menghubungkan perangkat sarana untuk dapat bertukar informasi. Dengan adanya jaringan computer memudahkan pengguna untuk mencari maupun bertukar informasi yang bersifat penting dan rahasia. Keamanan jaringan merupakan aspek terpenting sebuah sistem dalam menjaga validitas dan integritas data, serta menjamin ketersediaan layanan bagi penggunaanya. Sistem keamanan jaringan komputer harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak (Anggreni and Jasa 2022).

Perkembangan ini tidak lepas dari perkembangan teknologi jaringan, software maupun hardwarenya. Jaringan komputer adalah kumpulan beberapa komputer yang saling terhubung satu sama lain, sehingga memungkinkan pengguna untuk saling bertukar informasi berupa suara, video, gambar dan data pada jaringan yang sama, jaringan komputer memerlukan keamanan agar

terhindar dari agar terhindar dari kejahatan *cyber* yang di lakukan oleh orang yang tidak bertanggung jawab yang mengakibatkan kehilangan data-data yang sangat penting. Karyawan dapat bekerja dari rumah, dan siswa dari segala usia mengambil kelas secara online. Semakin publik bergantung untuk tetap terhubung dengan jaringan, semakin besar potensi serangan jaringan yang terjadi.(Saputro, Saputro, and Wijayanto 2020)

Keamanan jaringan merupakan hal yang sangat penting untuk diperhatikan karena ancaman serangan yang semakin canggih dan beragam, terlebih ketika jaringan lokal sudah terhubung ke internet maka ancaman keamanan jaringan akan meningkat. Misalnya *Distributed Denial of Service* (DDoS), serangan *hacker*, *virus*, *trojan* yang semuanya merupakan ancaman yang tidak bisa dihindari. Pengamanan Jaringan merupakan salah satu tindakan untuk menjaga data yang terdapat di server selain menggunakan metode lain seperti enkripsi data, salah satu Teknik yang di gunakan untuk mengamankan jaringan adalah dengan menggunakan Teknik DMZ *(Demilitarized Zone)*. Teknik ini bekerja dengan memisahkan *traffic* data dari IP Publik internet dan IP Lokal di Regita Klinik Utama untuk melindungai *server* dengan membuat lingkungan khusus dalam jaringan, dalam penelitian ini *router* yang di gunakan adalah Router Mikrotik.(Anon n.d.)

Mikrotik RouterOS adalah salah satu sistem operasi jaringan yang populer dan menyediakan fitur *firewall* yang lengkap. Fitur *firewall* pada Mikrotik *RouterOS* meliputi fitur filter paket, fitur filter konten, fitur filter IP, dan fitur fitur yang lainnya.(Pratomo 2023)

Web server merupakan salah satu target *public* yang menyangkut sebuah organisasi. Keamanan web server sama pentingnya dengan keamanan website atau aplikasi web tersebut dan jaringan disekitarnya. Dengan adanya kemungkinan akses ilegal tersebut, maka dikembangkansuatu mekanisme yang dapat mengamankan *web server* dan *database server* dari akses yang dilakukan pihak ilegal. Untuk itu perlu adanya jaringan komputer yang memerlukan sistem *firewall* yang berfungsi sebagai sistem keamanan jaringan dan menjaga semua perangkat yang ada didalamnya. Dengan fasilitas yang dimiliki pada *firewall*, maka komunikasi melalui suatujaringan komputer dapat berfungsi dengan baik. (Arlis and Sahari 2019)

Firewall adalah perangkat lunak atau perangkat keras yang digunakan untuk melindungi jaringan dengan menganalisis data yang masuk dan keluar, berdasarkan sekumpulan aturan, apakah memiliki rangkaian berbahaya atau tidak. (Al Amien n.d.)

Firewall adalah sebuah sistem atau kelompok sistem yang menerapkan sebuah *access control policy* terhadap lalu lintas jaringan yang melewati titik-titik akses dalam jaringan. Tugas *firewall* untuk memastikan bahwa tidak ada tambahan diluar ruang lingkup yang diizinkan. Firewall untuk memastikan bahwa acces control policy diikuti oleh semua *user* di dalam jaringan. (Naufal et al. 2022)

Firewall mengamankan sistem jaringan komputer dengan menerapkan penyaringan *port-port* web. Salah satu aplikasi *firewall* yang memiliki fitur untuk dapat melakukannya yaitu aplikasi iptables pada linux. Dengan adanya *iptables*, pihak sekolah dapat melakukan penyaringan trafik pada server, mengatur lalu

lintas jaringan, termasuk mengizinkan atau memblokir koneksi yang masuk, keluar, atau sekedar melewati server. (Dwipoyono et al. 2023)

Pada penelitian sebelumnya dilakukan oleh M.Agus Syamsul Arifin, Antoni Zulius pada tahun 2019 dengan menggunakan judul Perancangan Sistem Keamanan Jaringan Pada Universitas Bina Insan Lubuk Linggau Menggunakan Teknik *Demilitarized Zone* menjelaskan bahwa Lalulintas data pada Jaringan Universitas Bina Insan di Lubuk Linggau tidak terfilter sehingga system internal yang ada dalam hal ini adalah perangkat server tidak memiliki pengamanan selain system keamanan *built in* yang ada pada sistem operasi yang di gunakan oleh server Universitas (*Firewall Sistem Operasi*) pengguna yang mengakses jaringan Internet menggunakan *IP Address* yang biasa di gunakan mahasiswa dapat juga memasuki jaringan yang di gunakan oleh server secara langsung tanpa terfilter, dengan menggunakan Teknik DMZ lalulintas data server yang ada akan dipisah dari Jaringan yang di gunakan oleh mahasiswa dan Jaringan Luar, sehingga mahasiswa dan pengguna hanya akan dapat mengakses port yang sudah di tentukan saja (Agus, Arifin, and Zulius 2019).

Klinik Regita Utama memilik permasalahan dalam keamanan jaringan yang kurang baik, yang dimana lalulintas data jaringan tersebut tidak mempunyai filterisasi sehingga system internal pada Klinik Regita Utama hanya memiliki system keamanan built in yang ada pada system operasi yang dimiliki. Jadi pengguna dapat mengakses jaringan tersebut hanya menggunakan *IP Address* biasa dan dapat memasuki jaringan yang digunakan oleh server secara langsung.

Untuk menyelesaikan permasalahan diatas, maka pada penelitian ini akan digunakan konsep *Keamanan Jaringan.* Keamanan Jaringan merupakan

merupakan salah satu tindakan untuk menjaga data yang terdapat di server (Agus et al. 2019).

Untuk menunjang konsep *Network Security*, pada penelitian ini untuk mengamankan system dari perusahaan. DMZ adalah metode yang digunakan pada penelitian ini, DMZ merupakan interface yang berada diantara area jaringan internal dan eksternal Teknik ini bekerja dengan memisahkan *traffic* data dengan *IP Public* internet dan *IP Local* untuk melindungi *server* dengan membuat lingkungan khusus dalam jaringan (Suteja, Kumalasari, and Raharjo 2021).

Dan kombinasi dari konsep tersebut menggunakan Firewall Rules, *Firewall Rules* merupakan sekelompok sistem yang menetapkan kebijakan kendali akses antara dua jaringan, dengan prinsip sepasang mekanisme memblok lalu lintas, dan mengizinkan lalu lintas jaringan. Dengan menggunakan firewall, pengelola jaringan dapat membatasi hak akses terhadap *IP Address* yang dianggap kurang baik bagi pengguna jaringan (Putra and Ramdhani 2021)

Tujuan Dari penelitian ini ialah merancang sistem keamanan jaringan dan menerapkan beberapa metode seperti DMZ dan *Firewall Rules*, dengan harapan jaringan yang ada di Klinik Regita Utama akan lebih aman dari serangan luar. Dan juga penelitian ini sudah dilakukan terdahulu bisa dijadikan sebagai acuan serta memperoleh perbandingan-perbandingan yang sesui dengan topik yang di teliti. Teknik DMZ pada layanan server jaringan LAN dapat melakukan filter terhadap serangan DDOS, ICMP *flooding attack* dan UDP *flooding attack*. Dan juga penelitian ini hanya menjelaskan tentang serangan yang dihadapi tidak menjelaskan cara mengatasi serangan tersebut (Suteja et al. 2021).

1.2 Perumusan Masalah

Latar belakang masalah yang telah diuraikan dapat disimpulkan permasalahan adalah sebagai berikut :

a) Apakah metode DMZ dan *Firewall Rules* dapat mengatasi keamanan jaringan pada Klinik Regita Utama ?
b) Bagaimana cara DMZ melindungi *system* keamanan jaringan Klinik Regita Utama?
c) Bagaimana agar dapat memonitoring keamanan jaringan yang telah dibuat ?

1.3 Hipotesa

Hipotesa sebagai berikut :

a) Diharapkan Penggunaan metode *Demilitarized Zone* dan *Firewall Rules* dapat mengatasi ada nya problem dari klinik Regita Utama
b) DMZ menggunakan *Firewall Rules* agar bisa mengontrol lalulintas jaringan internal tersebut.
c) Diharapkan dengan adanya metode DMZ ini dapat memonitoring peretas yang mencoba masuk ke jaringan yang ada.

1.4 Batasan Masalah

Untuk menghindari adanya penyimpangan maupun pelebaran pokok dalam masalah penyusunan penlitian ini maka penelitian akan membantu memberikan batasan masalah yaitu dalam memberikan sebuah pengaplikasi atau berupa web yang nantinya mempermudah dalam penginputan data evaluasi kinerja pegawai.

a) Rancangan bangun keamanan jaringan komputer dengan memanfaatkan metode DMZ dan *Firewall Rules* yang menyangkut tentang topologi jaringan dengan spesifikasi perangkat keras yang ada.
b) Menggunakan metode DMZ dan *Firewall Rules* untuk membuat jaringan pribadi yang dapat bertukar informasi hanya melalui jaringan tertentu saja.
c) Dalam implementasi menggunakan media Router board mikrotik, dan winbox.

1.5 Tujuan Penelitian

Dalam melakukan penilitian ini tujuan yang ingin dicapai diantaranya adalah

a) Merancang dan menganalisa keamanan jaringan DMZ dan *firewall* untuk dapat mangatasi *system* keamanan jaringan pada klinik Regita Utama.
b) Untuk melindungi system keamanan jaringan dari Klinik Regita Utama DMZ mengontrol pengaturan akses lalu lintas jaringan yang diizinkan masuk agar tidak terjadinya peretasan.
c) Dapat *memonitoring* peretas yang mencoba masuk ke system, serta menguji dan menganalisa kinerja jaringan DMZ berdasarkan parameter *throughput.*

1.6 Manfaat Penelitian

Adapun beberapa manfaat yang didapatkan dari penelitian ini adalah:

a) Penelitian ini bermanfaat untuk menambah wawasan dalam dunia Networking, dan juga bisa berbagi pendapat tentang metode yang digunakan saat ini.
b) Keamanan Jaringan saat ini juga perlu pada zaman teknologi canggih, dan salah satunya juga membantu memprivasikan data-data yang dimiliki beberapa instansi.
c) Dapat dijadikan solusi alternatif bagi Klinik Regita Utama sebagai peningkatan kualitas keamanan jaringan dengan menggunakan metode DMZ dan *Firewall Rules*