BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan dapat dikatakan suatu hal yang vital dan harus diperhatikan karena itu merupakan hal yang sangat mendasar dalam keamanan jaringan, kelemahan di dalam jaringan komputer yang tidak dapat dilindungi tentunya dapat berdampak pada kerugian seperti kehilangan file data bahkan kerusakan sistem server, tidak maksimal dalam melayani *user* atau pengguna yang dapat menyebabkan kehilangan aset berharga suatu organisasi atau perusahaan. Keamanan jaringan harus sangat diperhatikan, tentunya dengan adanya perkembangan dari jaringan maka jenis ancaman serangan yang datang juga akan semakin canggih dan bervariatif terlebih jika jaringan lokal telah terhubung ke internet tentunya ancaman jaringan terhadap jaringan tersebut akan meningkat (Mulyanto et al., 2022).

Mengutip penelitian yang dilakukan (Saputro et al., 2020) belakangan ini ancaman serangan yang terjadi yakni *Port Scanning* dan *DDoS (Distributed Denial Of Service)* yang mana menurut *survey* Link 11 menunjukan lonjakan peningkatan sebanyak 81% maksimal *bandwidth* yang di tujukan dalam mengatasi DDoS ini, sedangkan volume paket yang tertinggi sebanyak 19 *packet* dengan lebih dari 50Gbps. Sehingga pentingnya keamanan jaringan. Dalam jaringan komputer tentunya ini harus menjadi fokus utama terlebih jika mengadakan sebuah *event*

secara *virtual* tentunya ancaman serangan ini akan lebih beragam mengingat *event virtual* ini dilaksanakan secara *online.*

Event Virtual adalah sebuah acara yang dilakukan secara *online* melalui perangkat elektronik secara digital, seperti yang kita ketahui di masa era digital sekarang ini, dengan adanya perkembangan teknologi yang ada, tidak menutup kemungkinan bagi kita untuk melaksanakan sebuah kegiatan secara *online*. Dengan ini akan memberikan opsi alternatif dalam melakukan kegiatan. Proses mekanisme jaringan membutuhkan router sebagai penghubung ISP *(Internet Service Provider)* menuju *switch,* salah satu router yang akan digunakan yakni router mikrotik pada *event virtual.* Router mikrotik digunakan untuk management, filtering jaringan dengan tujuan untuk menjaga kestabilan, efektifitas serta tingkat keamanan pada saat digunakan (Aji & Diniati, 2021).

Router mikrotik berfungsi untuk meringankan pekerjaan *administrator* dalam *mengkonfigurasi, monitoring,* dan *troubleshooting* pada sebuah sistem (Hidayat et al., 2022). Saat mengimplementasikan dalam acara *event virtual*, konfigurasi berfungsi untuk mengkonfigurasi sistem sesuai dengan kebutuhan. Fungsi *monitoring* untuk melihat sebuah sistem berjalan pada saat pengujian maupun pada saat acara sedang berlangsung, akan tetapi hal tersebut tidaklah dapat dilakukan setiap saat dikarenakan terkendala oleh tempat yang tidak bisa dijaga setiap saat, khususnya pada perangkat router mikrotik. Permasalahan yang muncul adalah ketika *administrator* tidak dapat mengetahui jika terjadi gangguan-gangguan yang dapat menghambat dan mengurangi kinerja dari router mikrotik, seperti percobaan untuk memasuki sebuah sistem keamanan jaringan secara *illegal (Brute*

Force, SSH, Telnet) dan *Scanning* pada *port router mikrotik* (Desmira & Wiryadinata, 2022b). Serangan tersebut merupakan suatu langkah awal dalam upaya proses pencurian data atau merusak data, apabila hal tersebut terjadi pada router mikrotik tentu saja akan mengganggu kinerja dari router mikrotik tersebut.

PT. Shanaya Creativo Innovation merupakan sebuah perusahaan perorangan yang bergerak dibidang *IT Consultant* yang berdiri sejak tahun 2019. Perusahaan ini memberikan layanan berupa jasa yang berhubungan dengan permasalahan teknologi informasi yang ada di perusahaan tentunya ini akan memberikan dampak positif dalam jangka panjang. Tetapi terdapat beberapa permasalahan yang dihadapi di perusahaan yaitu ketika hendak memonitoring keamanan jaringan administrator jaringan diharuskan menggunakan komputer dan laptop dalam *memonitoring* jaringan tentunya ini tidaklah efektif. Maka peneliti ingin melakukan penelitian untuk memberikan perubahaan dalam memonitoring keamanan jaringan menggunakan handphone dengan bantuan sosial media telegram.

Tahapan awal yang harus dilakukan adalah pemberian keamanan terhadap sistem router mikrotik. Penerapan fitur *port knocking* pada sistem login dengan autentifikasi kesepakatan dengan bertujuan untuk menghambat serta meminimalisir kemungkinan ketika terjadinya serangan *ssh, telnet* dan *winbox*, fitur *firewall* melakukan filtering terhadap jaringan apabila terdeteksi adanya kejanggalan pada saat proses login, melakukan pemblokiran ip secara otomatis, pengnonaktifan pada serangan dan pemberitahuan atau notifikasi serangan dengan memanfaatkan social media telegram sebagai platform yang terhubung ke router mikrotik terhadap

administrator (Rizal et al., 2020). Telegram merupakan sebuah aplikasi yang gratis, ringan dan bersifat multiplatform dengan kata lain telegram merupakan sebuah aplikasi yang bersifat *open source* yang memudahkan kita dalam membangun sebuah pengermbangan bot telegram bagi para pengembang.

Telegram Bot API *(Application Programming Interface)* terdiri dari sebuah perintah dan objek yang diperlukan dalam menyelesaikan instalasi bot telegram. Dengan menggunakan antar muka yang ada, maka dengan otomatis perintah yang dimasukan akan dieksekusi secara mandiri dan membuat asisten yang akan melakukan fungsi yang diberikan kepada mereka ketika telegram di jalankan, yang mana terdapat beberapa keunggulan yang ditawarkan oleh telegram ketika pengguna mengoperasikannya yakni dapat mengirim ataupun menerima file dari robot maupun klien tentunya dengan keunggulan ini akan memudahkan pengguna dalam memonitoring setiap aktivitas dalam rancangan yang akan dibuat nantinya (Sastrawangsa, 2017).

Berdasarkan permasalahan yang sering alami ketika mengadakan sebuah *event* secara *virtual* maka peneliti akan melakukan sebuah penelitian yang berjudul Rancang bangun sistem keamanan jaringan mikrotik menggunakan *firewall filtering* dan *port knocking* dengan notifikasi telegram pada *event virtual* yang bertujuan dapat memudahkan pekerjaan *administrator* dalam menjaga keamanan sebuah sistem sehingga dapat meminimalisir serangan dan memfiltering jaringan yang mencurigakan serta melakukan autentifikasi serta memberikan notifikasi melalui bantuan sosial media telegram dalam upaya mengantisipasi serangan pada router mikrotik.

1.2 Identifikasi Masalah

Berdasarkan penjelasan yang dijabarkan pada latar belakang maka dapat diuraikan beberapa beberapa masalah pada penelitian ini :

1. Belum adanya sistem keamanan yang menjamin sebuah sistem dapat berjalan dengan aman
2. Belum terdapat sarana pendukung dalam mengembangkan sistem keamanan jaringan dalam sebuah event yang dilakukan secara virtual
3. Belum adanya sistem pengingat ketika terjadi sebuah serangan terhadap sistem.

1.3 Batasan Masalah

Dalam penelitian ini peneliti berfokus pada permasalahan yang akan dibahas supaya penelitian ini lebih efisien dan tepat sasaran sehingga mampu dipahami, maka peneliti membuat batasan masalah sebagai berikut:

1. Sistem yang dikembangkan hanya pada jaringan LAN *(Local Area Network)*
2. Sistem dirancang dengan menggunakan 4 user yakni pada virtual mesin sebagai router (mikrotik versi 7.1.1), *attacker 1 (Putty), attacker 2* (*Filezilla),* dan *attacker 3 (Zenmap)*.
3. Penelitian ini hanya sampai tahap pengujian serangan pada sistem keamanan firewall filtering digunakan untuk mengatasi *(Port Scanning, Brute Force, ssh dan telnet)*
4. Penelitian ini hanya sampai tahap pengujian serangan pada sistem keamanan jaringan dan pengujian pada serangan *(ssh, telnet* dan *scanning)*

5. Notifikasi jika terjadi serangan melalui telegram versi 9.5.4

1.4 Rumusan Masalah

Berdasarkan latar belakang masalah maka dapat dijelaskan beberapa rumusan masalah dalam penelitian ini :

1. Bagaimana penerapan keamanan pada router mikrotik terhadap serangan jaringan ?
2. Bagaimana cara penerapan *filtering firewall* dan *port knocking* pada sebuah sistem ?
3. Bagaimana menjadikan telegram sebagai notifikasi sistem peringatan ?

1.5 Tujuan Penelitian

Dalam tujuan penelitian, peneliti akan memberikan gambaran dari setiap rancangan dari keamanan jaringan ini, yang mana tujuan dari penelitian ini adalah sebagai berikut:

1. Membuat sebuah rancang bangun sebuah sistem keamanan router mikrotik untuk mengantisipasi serangan terhadap pihak pihak yang tidak berhak dalam mengaksesnya
2. Menerapkan rancangan pada fitur fitur *filtering firewall, block ip, drop ip, port scanning , brute force, winbox, ssh* dan *telnet*
3. Implementasi telegram sebagai notifikasi awal dalam mengantisipasi serangan pada router mikrotik

1.6 Manfaat Penelitian

Dalam penelitian ini ditemukan manfaat-manfaat yang dapat memberi nilai tambahan teori pendukung bagi peneliti yang hendak mengangkat topik yang sama kedepannya berdasarkan beberapa aspek sebagai berikut :

1.6.1 Aspek Teoritis

Dengan adanya penelitian ini peneliti berharap dapat memberi dampak yang positif terhadap perusahaan atau organisasi lain yang membutuhkan referensi mengenai judul ini. Maka peneliti dapat menyebutkan beberapa aspek teoritis yang ada dalam penelitian ini :

1. Dengan adanya notifikasi melalui telegram maka akan mempercepat dalam upaya meminimalisir kemungkinan terjadinya penyerangan terhadap router mikrotik
2. Dapat mengetahui jika terjadinya penyerangan serta menjadi langkah dalam mengevaluasi dalam meningkatkan keamanan bagi administrator

1.6.2 Aspek Praktis

Dalam penelitian ini terdapat beberapa aspek praktis yang dalam dirasakan bagi beberapa pihak diantaranya :

1. Untuk Penyelenggara *event virtual* , dapat mengetahui serangan yang terjadi melalui notifikasi melalui social media telegram
2. Untuk Pembaca, menambah wawasan dan pengetahuan serta informasi mengenai keamanan router mikrotik berdasarkan penelitian yang dilakukan.

3. Untuk Univeritas, dapat menjadi referensi di perpustakaan
4. Untuk Peneliti, menjadi ilmu baru yang dapat digunakan dalam dunia kerja