BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan dalam dunia teknologi informasi membawa manfaat besar dalam hal efisiensi dan konektivitas, namun juga membawa tantangan serius terutama dalam hal keamanan jaringan. Sebagai infrastruktur inti berbagi data, penting untuk terus mengembangkan teknik keamanan yang lebih canggih dan efektif.[1]

Ada beberapa serangan jaringan berbahaya, termasuk spoofing, yang memanipulasi paket data dan identitas jaringan untuk menipu sistem keamanan. Selain itu, serangan *Distributed Denial of Service* (DDOS) adalah serangan yang bertujuan untuk mempengaruhi ketersediaan sistem atau layanan dengan mencegah pengguna yang berwenang mengakses sistem atau layanan.

Salah satu solusi untuk meningkatkan keamanan jaringan adalah dengan menerapkan metode *Firewall security port*. Dalam konteks ini, *Firewall security port* sangat penting dalam mendeteksi dan memblokir akses tidak sah ke jaringan. Namun, untuk memastikan hal ini harus memiliki sistem pemantauan yang dapat memberikan informasi tentang aktivitas jaringan. Oleh karena itu, penggunaan Bot Telegram sebagai alat monitoring membuat pemantauan jaringan menjadi lebih mudah.[2]

Penelitian ini bertujuan untuk melakukan analisis terhadap keamanan jaringan pada VLAN dengan menerapkan metode *Firewall security port*, serta mengintegrasikan Telegram Bot sebagai alat monitoring. Dengan demikian, dapat diperoleh pemahaman mengenai metode ini dalam melindungi data pada jaringan.

Dengan melihat pentingnya peran keamanan jaringan dan kebutuhan akan metode pemantauan yang canggih, dalam penelitian ini dapat memberikan kontribusi untuk meningkatkan keamanan jaringan dan memberikan solusi dengan membangun sebuah sistem monitoring melalui Telegram Bot dan dikendalikan oleh perangkat mobile maupun desktop untuk melakukan aktivitas monitoring jarak jauh.

1.2 Rumusan Masalah

Dalam konteks keamanan jaringan pada VLAN dengan penerapan metode Firewall Security Port dan penggunaan Telegram Bot sebagai alat monitoring, terdapat beberapa permasalahan yang perlu dipecahkan, yaitu:

1. Sejauh mana cara kerja metode Firewall dengan action drop dalam melindungi VLAN dari serangan?
2. Bagaimana penggunaan Telegram Bot dapat meningkatkan respons terhadap potensi ancaman dalam keamanan jaringan?

1.3 Batasan Masalah

Untuk menjamin agar penelitian ini tidak menyimpang dari tugas dan tujuan yang ingin dicapai, maka penulis membuat batasan rentang sebagai berikut :

1. Firewall security port
2. Menggunakan Mikrotik
3. Pengembangan sistem pendeteksi serangan menggunakan Telegram Bot Api

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Mengukur cara kerja metode Firewall dengan action drop dalam melindungi VLAN dari serangan.
2. Telegram Bot dalam meningkatkan respons terhadap potensi ancaman dalam keamanan jaringan.

1.5 Manfaat Penelitian

Manfaat penelitian yang dilakukan penulis adalah mendapat informasi berupa notifikasi pesan ketika terjadi serangan pada IP address karena menggunakan Telegram Bot sebagai sarana notifikasi serangan.

1.6 Metode Penelitian

Dalam tugas akhir skripsi ini, penulis menggunakan metode SPDLC

1.7 Sistematika Penulisan

Dalam penulisan ini, menggunakan sistematika penulisan sebagai berikut :

BAB I PENDAHULUAN

Bab ini menjelaskan latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, metode penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini mencakup tinjauan hasil pustaka dan dasar teori, tinjauan pustaka membahas mengenai uraian tentang kajian berbagai macam pustaka yang kemudian hasil dari kajian ini digabungkan dengan masalah yang sedang diteliti dalam proses penyusunan skripsi.

BAB III METODE PENELITIAN

Pembahasan ini berkaitan dengan penyampaian mengenai bahan dan peralatan yang akan digunakan dalam penelitian, serta metode dan perancangan sistem yang meliputi kebutuhan dalam membuat sistem keamanan jaringan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini membahas pengimplementasian dan menjelaskan apa saja yang dibutuhkan untuk membuat rancangan penelitian yang dilakukan penulis.

BAB V PENUTUP

Pada bab ini membahas hasil akhir dari rancangan sistem yang sudah dibuat kemudian dari hasil tersebut penulis menyampaikan beberapa saran yang bermanfaat untuk menambah sesuatu yang kurang supaya menjadi lengkap pada proses sistem keamanan jaringan tersebut.