BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi dan informasi berkembang sangat pesat. Kemajuan sistem informasi memberikan banyak keuntungan bagi manusia. Pada era digital ini manusia tidak terlepas dari komputer atau laptop. Manusia menggunakan komputer atau laptop untuk menunjang kebutuhan pada pekerjaan, pendidikan maupun hiburan. Kebutuhan akan jaringan komputer semakin bertambah penting karena dengan banyaknya akses ke jaringan tersebut maka akan banyak pula peluang untuk pihak-pihak yang tidak bertanggung jawab melakukan kejahatan komputer atau penyerangan yang berupa penyadapan data di jaringan komputer.

Keamanan jaringan sebagai bagian dari sebuah sistem sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Sistem keamanan jaringan komputer harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak.

Sistem keamanan firewall tidaklah cukup untuk meminimalkan terjadinya serangan terhadap suatu jaringan komputer. Banyak serangan yang terjadi pada jaringan komputer dapat diketahui setelah adanya kejadian-kejadian yang aneh pada jaringan. Para administrator jaringan tidak bisa mengetahui dengan pasti apa yang sedang terjadi, sehingga dibutuhkan waktu yang cukup lama untuk diatasi.

Pada jurnal Asep Fauzi Mutaqin yang berjudul Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMS Alert dengan Snort yang dimana dalam perancangannya masih menggunakan media SMS (*Short Message Service)* Pada *Handphone* administrator jaringan sehingga diperlukan biaya tambahan. Sedangkan jika pada telegram memiliki keunggulan jika dibandingkan dengan SMS yaitu dapat diakses dari berbagai perangkat secara bersamaan dan lebih ringan dijalankan.[1]

Oleh karena itu dibutuhkan suatu sistem yang dapat menanggulangi ancaman yang mungkin terjadi secara optimal dalam waktu yang cepat dan secara otomatis sehingga memungkinkan administrator mengakses sistem walaupun terjadi jaringan. Hal ini akan mempercepat proses penanggulangan gangguan serta pemulihan sistem atau layanan.

Raspberry PI dapat difungsikan sebagai server untuk menjaga keamanan infromasi data jaringan serta memonitoring keamanan jaringan dengan tujuan meminimalisir jika terjadi percobaan penyusupan dan percobaan intrusi.

Percobaan penyusupan tersebut dapat memanfaatkan aplikasi instan *messaging* sebagai media untuk memberitahu kepada administrator di jaringan komputer serta dapat dilakukan antisipasi awal dengan kontrol langsung terhadap *server* secara *real time*.

Aplikasi instan *messaging* saat ini populer digunakan oleh berbagai kalangan. Salah satu aplikasi tersebut yang memiliki berbagai fitur adalah *telegram.* Aplikasi tersebut selain untuk *chatting*, terdapat fitur pertukaran dokumen. Fitur tersebut dapat dimanfaatkan untuk memberikan laporan keamanan sistem jaringan komputer.

Berdasarkan latar belakang dari permasalahan di atas, penulis mengangkat judul tugas akhir "RANCANG BANGUN SISTEM KEAMANAN JARINGAN MENGGUNAKAN RASPBERRY PI DAN TELEGRAM BOT API".

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, penulis dapat merumuskan permasalahan sebagai berikut:

1. Bagaimana cara merancang sistem keamanan jaringan komputer yang dapat mendeteksi gangguan secara otomatis dan melakukan tindakan lebih lanjut?
2. Bagaimana cara mengintegrasikan aplikasi yang terkait dengan sistem keamanan jaringan komputer?

1.3 Batasan Masalah

Agar pembahasan masalah tidak menyimpang dari pokok permasalaan, maka penulis akan membuat batasan masalah sebagai berikut:

1. Sistem keamanan jaringan komputer pada sistem operasi raspbian jessie.
2. Merancang sebuah sistem keamanan jaringan berbasis IDS dengan menggunakan *snort*.
3. Blocking IP pada IP Tables bersifat permanen.
4. Pengujian serangan hanya pada protokol ICMP, UDP, dan TCP.
5. Hanya membahas sistem sebatas yang digunakan.
6. *Rules* yang ditulis pada *snort* hanya untuk membaca serangan DdoS dan *floading attack*.
7. Rancang bangun ini hanya diterapkan pada IP lokal.

1.4 Tujuan Penelitian

1. Untuk merancang sistem keamanan jaringan komputer berupa notifikasi pencegahan penyusupan.
2. Untuk mengetahui cara perancangan sistem keamanan jaringan komputer dengan Rasberry PI.

1.5 Manfaat Penelitian

1. Memberikan manfaat bagi penulis untuk mempelajari lebih dalam tentang rancang bangun sistem keamanan jaringan komputer.
2. Memberikan kemudahan pengguna untuk melindungi jaringan komputer beserta data-data yang ada di dalamnya.

1.6 Metodologi Penelitian

Dalam penulisan Proyek Akhir ini, penulis menggunakan beberapa macam metode penelitian, sebagai berikut:

1. Studi Literatur

   Merumuskan teori secara analisis dengan studi kepustakaan dan kajian dari buku-buku teks pendukung.
2. Perancangan Sistem dan Implementasi

   Pada tahap ini akan dilakukan perencanaan dan implementasi terhadap alat berdasarkan hasil studi literatur dan pada tahap ini pula akan dilakukan proses pembuatan alat sesuai dengan data-data yang telah ditentukan.
3. Uji Coba Alat

   Pada tahap ini akan dilakukan uji coba alat dan pengujian terhadap perancangan alat.

1.7 Sistematika Penulisan

Sistematika penulisan Proyek Akhir ini terdiri dari bab-bab dengan metode penyampaian sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini akan membahas latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini dibahas teori-teori dasar dari alat yang akan dibuat beserta komponen penunjang yang digunakan pada perancangan alat.

BAB III SIMULASI KEAMANAN JARINGAN

Pada bab ini membahas tentang tahap-tahap yang dilakukan dalam perancangan alat.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Pada bab ini berisikan analisa masalah-masalah yang dihadapi pada saat perancangan alat dan pada saat uji coba perangkat.

BAB V PENUTUP

Pada bab ini dikemukakan kesimpulan dan saran-saran yang konstruktif untuk kesempurnaan Proyek Akhir ini.