BAB 1. PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan menjadi aspek krusial dalam era digital ini, mengingat meningkatnya ancaman keamanan yang terus berkembang. Implementasi sistem deteksi intrusi (IDS) menjadi langkah penting untuk mengidentifikasi dan menghadapi potensi ancaman tersebut.

IDS menganalisis paket data untuk menentukan apakah ada upaya intrusi telah terjadi. Dalam beberapa tahun terakhir, ancaman terhadap sistem komputer yang mencurigakan (*Cyber threat*) oleh oknum yang tidak bertanggung jawab berulang kali terjadi melalui internet. Dengan meningkatnya permasalahan itu menimbulkan beberapa kerugian. Salah satunya adalah kehilangan data, kerentanan sistem dan kerusakan sistem akibat ancaman cyber. Contoh ancamannya termasuk *Distributed Denial Of Service* (DDoS), virus komputer dan Trojan Horse.

Salah satu layanan IDS opensource yaitu Snort, yang tersedia untuk sistem operasi Linux maupun Windows. Snort adalah perangkat lunak IDS yang biasa digunakan untuk melindungi jaringan dari aktivitas berbahaya. Cara kerjanya dengan menganalisis paket yang melewati jaringan, kemudian hasil deteksi tersebut akan disimpan pada database.

Meskipun sistem deteksi intrusi seperti Snort telah terbukti efektif, masih ada tantangan dalam menerapkannya pada skala kecil atau sumber daya terbatas, seperti yang dimiliki oleh Raspberry Pi. Raspberry Pi, sebagai perangkat berbiaya rendah, memiliki keterbatasan sumber daya seperti CPU, RAM, dan penyimpanan. Hal ini menjadi tantangan dalam mengimplementasikan sistem deteksi intrusi yang memerlukan daya komputasi yang signifikan. Oleh karena itu, perlu dilakukan penelitian untuk mengoptimalkan kinerja Snort pada perangkat dengan sumber daya yang terbatas.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dicantumkan, maka dapat diambil rumusan masalah dalam penelitian ini adalah sebagai berikut :

1. Bagaimana merancang sistem keamanan berbasis IDS (*Intrusion Detection System*) menggunakan Raspberry Pi ?
2. Bagaimana mendeteksi aktivitas yang mencurigakan pada sebuah server secara otomatis ?
3. Bagaimana melakukan tindakan yang cepat dan efektif untuk melindungi server dari bahaya intrusi?

1.3 Tujuan

Sesuai dengan rumusan masalah, Penelitian ini dirancang menggunakan Snort IDS (*Intrusion Detection System*) pada Raspberry Pi sebagai peringatan awal ketika ada serangan pada sistem dan membantu *administrator* melakukan tindakan pencegahan dengan tepat. Raspberry Pi adalah perangkat berbiaya rendah yang cocok untuk implementasi skala kecil seperti jaringan rumah atau jaringan kantor kecil.

Tujuan utamanya dapat difokuskan pada penerapan sistem deteksi intrusi menggunakan Snort untuk meningkatkan keamanan jaringan dalam skala yang lebih terbatas.

1.4 Manfaat

Dengan adanya penelitian ini, penulis berharap dapat memberikan manfaat sebagai berikut :

1. Pemahaman lebih dalam tentang sistem deteksi intrusi

   Menerapkan Snort pada Raspberry Pi memungkinkan lebih memahami cara kerja sistem deteksi intrusi. Hal ini mencakup pemahaman aturan deteksi, analisis lalu lintas jaringan, dan konfigurasi sistem untuk mendeteksi potensi ancaman keamanan.

2. Optimasi Sumber Daya

   Mengintegrasikan Raspberry Pi dengan sumber daya terbatas memungkinkan optimalisasi penggunaan CPU, RAM, dan penyimpanan.

3. Keamanan Jaringan Kecil

   Berfokus pada penerapan Snort pada Raspberry Pi memberikan wawasan untuk meningkatkan keamanan jaringan kecil, seperti di rumah atau kantor kecil. Hal ini mungkin relevan dalam situasi di mana diperlukan solusi berbiaya rendah namun efektif. Ini adalah keterampilan yang berharga untuk menghadapi tantangan pengelolaan sumber daya di lingkungan komputasi terbatas.

1.5 Batasan Masalah

Dengan mengidentifikasi masalah-masalah yang ada, agar lebih terarah dan dapat dipahami dengan mudah. Maka pembatasan terhadap masalah yang ada pada pembuatan sistem ini antara lain :

1. Server yang digunakan berupa Board Raspberry Pi
2. Menjalankan sistem IDS Snort pada Raspberry Pi
3. Melakukakan serangkaian serangan untuk mengetahui kinerja dari Raspberry Pi