BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan komputer dan server menjadi poin utama yang harus di rawat dan dijaga, bagi seorang administrator jaringan sangat penting untuk bisa melakukan pencegahan dan identifikasi pengguna yang tidak berhak untuk mengakses jaringan komputer. Keamanan jaringan komputer bertujuan untuk menjaga agar data di dalamnya tetap aman, utuh, dan valid. Dengan menjaga keamanan jaringan, kita bisa melindungi informasi, data, dan memastikan bahwa infrastrukturnya berjalan dengan baik. Ini membantu mencegah risiko seperti penyusupan atau ancaman yang dapat merusak fungsi jaringan. Jika keamanan jaringan tidak dijaga, bisa muncul masalah seperti gangguan, pengintipan, perubahan, atau pemalsuan pada jaringan komputer [2].

Penting sekali untuk memperhatikan keamanan jaringan, karena banyak hal yang dapat mengganggu keamanan dan stabilitas koneksi komputer. Beberapa contoh masalah yang umum terjadi dalam keamanan jaringan termasuk gangguan sistem yang bisa disebabkan oleh kesalahan tak disengaja dari pengelola. Namun, tidak sedikit pula masalah yang timbul akibat upaya merusak, menyusup, atau menyalahgunakan data dan sistem oleh pihak ketiga [4]. Salah satu solusinya adalah dengan memanfaatkan sistem pendeteksi intrusi (*Intrusion Detection System*/IDS) [5]. *Intrusion Detection System* (IDS) adalah sebuah sistem yang dirancang untuk mendeteksi serangan dan ancaman yang terjadi pada jaringan komputer, baik itu terkait dengan jaringan lokal maupun internet. IDS mampu melakukan pengawasan terhadap aktivitas jaringan dengan tujuan untuk mengidentifikasi tindakan yang mencurigakan atau tidak sah yang dapat merusak keamanan sistem jaringan [6]. Aspek keamanan jaringan meliputi stabilitas, integritas, dan validasi data yang sangat penting. Program *Intrusion Detection System* (IDS) berbasis jaringan yang dapat mendeteksi upaya penyusupan pada sistem jaringan computer salah satunya yaitu snort.

Snort adalah sebuah perangkat lunak yang digunakan untuk mendeteksi penyusup dan dapat menganalisis lalu lintas jaringan secara *real-time*. Snort memiliki kemampuan untuk mendeteksi berbagai jenis serangan [7]. Kelebihan Snort adalah mendukung berbagai platform dan sistem operasi, termasuk Linux dan Windows. Snort juga termasuk perangkat lunak open source dengan dukungan komunitas yang luas di internet. Hal ini memungkinkan pengguna Snort untuk dengan mudah memperbarui aturan (*rule*) Snort dibandingkan dengan perangkat lunak IDS lainnya [8]. Metode *Signatures* bekerja dengan mencocokkan aturan-aturan dengan lalu lintas yang sedang dideteksi, jika ada kecocokan, itu menandakan adanya serangan yang terjadi. Sementara itu, metode Anomaly Detection menggunakan aturan-aturan yang mengidentifikasi lalu lintas yang tidak biasa atau anomali dengan lalu lintas yang sedang dideteksi [6].

Namun, keefektifan *rule snort* dalam mendeteksi serangan jaringan masih menjadi pertanyaan yang perlu diteliti lebih lanjut. Meskipun *rule snort* telah dikembangkan dan diperbarui secara teratur, serangan jaringan juga terus berkembang dan mungkin memiliki pola yang belum terdeteksi oleh *rule snort* yang ada. Keberhasilan pendeteksian dan efektivitasnya sangat tergantung pada kemampuannya untuk mengenali dan merespons serangan dengan cepat. Beberapa organisasi telah mengintegrasikan notifikasi melalui platform komunikasi instan seperti Telegram ke dalam sistem Snort mereka. Tujuannya adalah untuk meningkatkan kemampuan Snort dalam mendeteksi dan merespons serangan dengan lebih baik.

Dengan menggunakan notifikasi Telegram, respons terhadap serangan menjadi lebih efisien karena pesan notifikasi dapat segera diteruskan ke pihak yang berwenang untuk mengatasi serangan secara tepat waktu. Penggunaan Telegram sebagai saluran notifikasi dipilih karena popularitas nya sebagai aplikasi pesan instan yang cepat dan andal dengan dukungan lintas platform, sehingga memudahkan administrator dan tim keamanan untuk berkoordinasi dan merespons serangan dari perangkat apa pun. Dalam konteks ini, analisis efektivitas *rule snort* mengacu pada penilaian sejauh mana rule yang diterapkan pada Snort mampu mendeteksi serangan yang dihadapi. Pada analisis tersebut, penting untuk

memastikan bahwa rule yang diterapkan sesuai dengan jenis serangan yang paling mungkin terjadi dalam lingkungan jaringan tertentu. Selain itu, evaluasi *rule snort* juga harus mempertimbangkan tingkat keakuratan deteksi (minimal *false positive* dan *false negative*) serta kemampuan sistem untuk menangani ancaman dengan respons yang tepat[5].

Selain menyediakan aplikasi Telegram juga menyediakan API bagi pengguna untuk membuat bot yang dapat digunakan dan dikembangkan untuk sistem informasi. Telegram dapat digunakan untuk melakukan kegiatan pemantauan jaringan sebagai penerima pemberitahuan jika terjadi serangan dari luar. Salah satu penggunaan Telegram untuk kegiatan pemantauan ini dengan menerima pesan dari IDS yang langsung terkirim menuju ke akun pengguna sehingga dapat mengetahui serangan yang terjadi walaupun sedang tidak di depan komputer server. Bot API yang terus berkembang sehingga dapat membuat bot yang dinamis dan dapat merespon pesan dari administrator jaringan. Implementasi bot mulai banyak digunakan karena mempunyai keunggulan yaitu dapat menyediakan data ke pengguna yang tidak terbatas oleh waktu dan dapat dikembangkan oleh siapa saja. Pada penelitian ini menghasilkan sistem pemantauan sebuah server yang lebih fleksibel karena dapat dipantau dari mana saja, sehingga seorang administrator tidak perlu selalu di depan komputer server untuk mengawasi server. Penggunaan model pemantauan seperti ini dapat mengefisienkan dari aspek waktu dan tenaga bagi seorang administrator server. Pengiriman pemberitahuan yang cepat dari server menuju Telegram juga akan membantu administrator dalam melakukan tindakan ketika server sedang terjadi sesuatu.[9]

1.2 Permasalahan

Berdasarkan latar belakang di atas permasalahan yang muncul pada penelitian ini adalah penerapan rule snort pada jaringan komputer tidak mampu dalam melakukan intrusi serangan yang belum pernah ada sebelumnya, sehingga perlu dilakukan pengembangan rule snort dengan penerapan aturan baru untuk memfilter serangan yang belum pernah ada sebelumnya.

1.3 Tujuan

Tujuan penelitian ini adalah sebagai berikut:

1. Mengembangkan dan menganalisis efektivitas *rule snort* dalam mendeteksi pola serangan pada jaringan
2. Mengirimkan notifikasi serangan ke administrator melalui aplikasi telegram.

1.4 Manfaat

Penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. Menyediakan pemahaman yang lebih baik tentang efektivitas *rule snort* dalam mendeteksi serangan jaringan.
2. Memberikan informasi mengenai kecepatan respons IDS menggunakan *rule snort*, yang penting dalam menghadapi serangan yang memerlukan deteksi dan respons yang cepat.
3. Pemantauan fleksibel memberikan fleksibilitas pemantauan jaringan dari mana saja dengan integrasi Telegram, memungkinkan administrator untuk mengawasi server tanpa harus berada di depan komputer fisik.

1.5 Sistematika Penulisan

Jelaskan tentang sistematika pembahasan dalam buku proyek akhir yang meliputi:

Bab 1 Pendahuluan

Penjelasan yang berisi latar belakang, permasalahan, tujuan, dan sistematika penulisan.

Bab 2 Kajian Pustaka

Penjelasan tentang teori-teori, konsep dan penelitian terkait yang berkaitan dengan penelitian yang di lakukan

Bab 3 Desain Sistem

Penjelasan tentang tahapan- tahapan penelitian yang di lakukan dan teknik-teknik yang di gunakan dalam pengujian Analisis Efektivitas *Rule snort* dalam Mendeteksi Serangan Jaringan

Bab 4 Eksperimen dan Analisis

Jelaskan tentang apa saja yang dibahas pada Bab 4. Penjelasan memuat bagian-bagian penting pada Eksperimen dan Analisis.

Bab 5 Penutup

Jelaskan tentang apa saja yang dibahas pada Bab 5. Penjelasan memuat bagian-bagian penting pada Penutup.