BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada masa kini perkembangan tekno*log*i menjadi suatu kebutuhan dalam kehidupan manusia dalam mengakses informasi. Perkembangan tekno*log*i juga bisa memudahkan pekerjaan dalam kehidupan sehari hari. Namun dibalik itu terdapat sisi positif negatif dari adanya perkembangan tekno*log*i terutama dalam aspek keamanan. Dengan perkembangan tekno*log*i saat ini yang sangat pesat sering terjadi masalah ataupun ancaman serangan *cyber* yang dilakukan oleh orang yang tidak bertanggung jawab. Oleh karena itu, seorang administrator jaringan harus selalu memastikan bahwa sistem jaringan komputer selalu tetap aman dan terlindungi dari serangan intrusi, sangat penting bagi sebuah jaringan komputer untuk terus menjaga keamanannya dengan baik. Jika tidak kelemahan tersebut yang dapat memungkinkan akses tanpa izin dari pihak yang tidak bertanggung jawab, sehingga berpotensi menyebabkan kerugian seperti kehilangan data, kerusakan pada sistem *server*, atau bahkan aset berharga bagi institusi[1].

Perkembangan jaringan komputer di era digital sekarang masih terus berlanjut, jaringan komputer merupakan interkoneksi antara dua atau lebih komputer dengan media wired maupun wireless. Terdapat istilah *Client-Server* yang umum digunakan dalam jaringan komputer. *Client* merupakan *user* yang menggunakan atau meminta layanan kepada *server*, sedangkan *server* merupakan *user* yang menyediakan atau mengirim layanan yang di minta oleh *user client*[2]. Keamanan jaringan merupakan suatu sistem yang berfungsi untuk mencegah adanya aktivitas yang tidak diinginkan dengan cara mendeteksi *user* yang tidak memiliki hak akses terhadap *server*[3]. Dengan adanya aktivitas tersebut keamanan pada

jaringan menjadi suatu hal yang sangat krusial dalam perkembangan teknologi saat ini.

Keamanan jaringan komputer dan *server* menjadi poin penting yang harus dijaga terutama bagi seorang administrator yang dimana sangat penting bagi mereka untuk bisa melakukan pencegahan dan identifikasi serangan yang mencoba untuk mengakses jaringan komputer. Adanya keamanan jaringan komputer ini bertujuan untuk menjaga agar data dalam *server* tersebut bisa tetap aman dan utuh. Dengan selalu menjaga keamanan jaringan kita dapat selalu melindungi informasi, data bahkan memastikan bahwa infrastruktur di dalam tersebut bisa berjalan dengan baik, hal ini dapat membantu adanya resiko penyusupan atau serangan intrusi yang bisa menyebabkan kerusakan pada fungsi jaringan[4].

Jaringan komputer akan kurang optimal digunakan jika jaringan tersebut mendapatkan serangan intrusi atau hacker yang dimana mereka mencoba untuk bisa mendapatkan akses dari sebuah sistem keamanan yang ada, serangan intrusi terjadi ketika orang yang tidak punya wewenang mencoba untuk mendapatkan akses dari sistem sehingga membuat sistem tersebut mengalami penurunan performa atau bahkan overload yang menyebabkan sistem tidak berjalan dengan normal. Untuk dapat memahami sistem apa yang ingin digunakan untuk mencegah itu semua perlu dilakukan identifikasi terhadap spesifikasi sistem tersebut[5].

Untuk mengatasi hal tersebut sangat dibutuhkan sistem keamanan jaringan yang dapat mendeteksi serangan secara efektif. Salah satu nya adalah dengan memanfaatkan *Intrusion Detection System* (IDS) [6]. IDS dapat dibedakan menjadi dua kategori yaitu *Network-based Intrusion Detection Sistems* (NIDS) dan *Host-based Intrusion Detection Sistem* (HIDS). NIDS menganalisis *Traffic* jaringan untuk mendeteksi serangan sedangkan HIDS melakukan *monitoring* pada sistem individu[4]. Dalam kasus ini peneliti menggunkan salah satu kategori dari IDS yaitu *Network-based Intrusion Detection Sistem* (NIDS).

Intrusion Detection Sistem merupakan sebuah sistem yang dirancang untuk mendeteksi serangan dan ancaman yang terjadi pada sistem jaringan komputer baik itu local maupun global. IDS mampu melakukan *monitoring* terhadap *Traffic* jaringan dengan tujuan untuk melakukan identifikasi serangan yang dapat merusak sistem keamanan jaringan.[7] Aspek keamanan tersebut meliputi stabilitas, integritas dan validasi data yang sangat penting. Dalam melakukan analisis IDS berbasis *signature* akan melalukan deteksi dan kemudian membandingkan *signature* dengan paket yang ditangkap dari *Traffic* tersebut kemudian mengenali adanya kemungkinan serangan intrusi[8].

Salah satu aplikasi *IDS* yang digunakan yaitu *Snort*. *Snort* merupakan software open-source yang dapat digunakan untuk melakukan *monitoring* pada sebuah *Traffic* jaringan dengan kelebihan yang dimiliki oleh snort yaitu bisa membuat rules sendiri yang bisa dimanfaatkan untuk menerapkan *signature based detection* yaitu dimana snort dapat mendeteksi adanya serangan intrusi melalui port yang digunakan. Metode *signature based detection* bekerja dengan mencocokkan rules-rules dengan *Traffic* yang sedang dideteksi, jika ada kecocokan maka itu menandakan bahwa adanya serangan intrusi yang sedang terjadi[9].

Alasan peneliti memilih Snort sebagai sistem keamanan untuk mendeteksi serangan *Brute Force* karena Snort memiliki kecepatan deteksi yang tinggi dalam konteks serangan *Brute Force SSH* yang dimana serangan ini bersifat cepat dan berulang, oleh karena itu kemampuan sistem untuk mendeteksi dan merespons intrusi secara *real-time* sangat menentukan pertahanan keamanan jaringan. Berdasarkan penelitian yang membahas hal serupa yang dimana di penelitian tersebut dilakukan analisis perbandingan performa Snort dan IDS lainnya yaitu Suricata, dalam hal ini peneliti memilih Suricata sebagai perbandingannya karena dari kedua IDS tersebut memiliki kelebihan dan kekurangan di setiap skenario penyerangannya. Dalam penelitian tersebut juga dinyatakan bahwa

Suricata memiliki tingkat akurasi deteksi yang tinggi jika dibandingkan dengan snort tetapi di sisi lain kecepatan deteksi Snort lebih tinggi dibandingkan Suricata[10].

Dari uraian di atas peneliti menemukan suatu masalah Ketika adanya serangan *Brute Force* yang terjadi pada port *SSH* dan bagaimana *Snort* mendeteksi serangan tersebut. *Brute Force* merupakan jenis serangan yang masuk dalam sistem dengan mencoba semua opsi yang tersedia, seperti kombinasi antara huruf, angka dan symbol. *Brute Force* adalah sebuah algoritma yang bisa menemukan semua solusi, karena algoritma ini akan melakukan percobaan dari semua kemungkinan solusi yang ada[11]. Dengan melakukan analisis implementasi intrusion detection sistem snort dalam mendeteksi serangan *Brute Force* pada protocol *SSH*, penelitian ini bertujuan untuk menganalisis bagaimana implementasi *Snort* dalam mendeteksi serangan *Brute Force*.

1.2 Rumusan Masalah

Berdasar latar belakang yang sudah dijelaskan sebelumnya, permasalahan yang akan dibahas dalam penelitian ini adalah sebagai berikut :

1. Bagaimana cara kerja Snort dalam mendeteksi serangan *Brute Force* pada protocol *SSH* ?
2. Bagaimana tingkat kecepatan respons deteksi Snort dalam mengidentifikasi serangan *Brute Force* pada protocol *SSH*?
3. Bagaimana hasil analisis dari implementasi Snort dalam mendeteksi serangan *Brute Force* pada protocol *SSH*?

1.3 Batasan Masalah

Agar penelitian ini bisa lebih terarah perlu adanya Batasan masalah sebagai berikut :

1. Penelitian ini hanya membahas Implementasi Intrusion Detection Sistem (IDS) Snort khususnya pada deteksi serangan *Brute Force*

terhadap protocol *SSH* yang dimana serangan *Brute Force* ini hanya sebagai skenario pengujian serangan untuk mengamati bagaimana kinerja IDS dalam mendeteksi serangan tersebut.

2. Analisis difokuskan pada Konfigurasi Rules Snort yang digunakan serta hasil pendeteksian serangan dengan penekanan pada respons IDS Snort terhadap pola serangan yang diberikan oleh *Brute Force*.
3. Pengujian dilakukan pada jaringan lokal dengan scenario serangan *Brute Force* yang dilakukan untuk menguji kemampuan IDS snort dalam melakukan deteksi secara *real-time*.
4. Snort di operasikan hanya menggunakan sistem operasi Linux Ubuntu
5. Jenis serangan yang dideteksi oleh snort hanya serangan *Brute Force* yang dilakukan pada protocol *SSH*
6. Password yang digunakan dibatasi hanya menggunakan 12 karakter dengan kombinasi huruf, angka, dan simbol khusus. Pembatasan ini bertujuan untuk mensimulasikan penggunakan strong password.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang sudah diuraikan sebelumnya, tujuan yang akan dicapai oleh peneliti dalam penelitiannya adalah sebagai berikut :

1. Untuk mengetahui bagaimana cara kerja snort dalam mendeteksi serangan *Brute Force* pada protocol *SSH*.
2. Untuk mengetahui seberapa cepat Snort mampu mendeteksi dan memberikan *alert* terhadap serangan *Brute Force* pada protokol *SSH*.
3. Untuk mengetahui hasil analisis dari implementasi intrusion detection sistem (IDS) snort dalam mendeteksi serangan *Brute Force* pada protocol *SSH*.

1.5 Manfaat Penelitian

Hasil dari penelitian ini diharapkan dapat memberikan manfaat baik secara teoritis maupun praktis diantaranya adalah sebagai berikut :

1. Menambah wawasan dan pemahaman mengenai penerapan intrusion detection sistem snort dalam konteks keamanan jaringan khususnya pendeteksian serangan *Brute Force* pada protocol *SSH*.
2. Memberikan kontribusi pada kajian ilmu keamanan informasi dan sistem jaringan terutama pada mekanisme deteksi serangan dan analisis
3. Membantu administrator jaringan untuk memahami konfigurasi dan penggunaan snort dalam meningkatkan keamanan jaringan.
4. Menjadi bahan rekomendasi dalam pengoptimalan sistem pertahanan jaringan terhadap serangan *Brute Force*.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN, berisi Latar Belakang Masalah, Rumusan Masalah, Batasan Masalah, Tujuan Penelitian, Manfaat Penelitian, Sistematika Penulisan.

BAB II TINJAUAN PUSTAKA, berisi Tinjauan Pustaka, Studi Literatur, Dasar Teori.

BAB III METODE PENELITIAN, berisi Objek Penelitian, Alur Penelitian, Alat dan Bahan

BAB IV HASIL DAN PEMBAHASAN, bab ini berisi tahapan yang penulis lakukan dalam menganalisis hasil deteksi serangan dari snort terhadap serangan *Brute Force* pada protocol *SSH*.

BAB V KESIMPULAN, bab ini berisi kesimpulan dan saran yang sudah dirangkum oleh peneliti berdasarkan uraian penjelasan diatas.