BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada dunia digital saat ini, hampir semua orang menggunakan teknologi komputer yang terhubung dengan dunia internet. Dengan kemajuan teknologi internet saat ini kebutuhan serta pekerjaan dapat dengan mudah dikerjakan, semua informasi yang kita butuhkan dapat kita temui dengan internet menggunakan fitur "*Google Search"* . Dengan kemajuan internet pula kita dapat berkomunikasi dengan siapapun dari jarak yang jauh sekalipun, atau kita bisa juga membagikan sebuah informasi ,aktifitas atau hal apapun yang kita inginkan.

Dengan perkembangan teknologi internet yang sangat pesat , ada pula orang yang tidak bertanggung jawab memanfaatkan hal tersebut untuk melakukan sebuah penyerangan untuk bisa masuk kedalam sistem komputer kita sehingga mendapatkan data-data penting sehingga menjadi sebuah keuntungan bagi orang yang tidak bertanggung jawab tersebut. Berdasarkan artikel *writeup*(Aditya Gema Pratomo 2016, hlm. 1) yang terdapat pada laman *oketechno*, terjadi pada tahun 2016, dimana pada bulan Oktober videotron pada Kawasan Jakarta Selatan menayangkan sebuah video porno pada saat lalu lintas sedang ramai, sehingga pengendara yang melewati Kawasan tersebut banyak yang berhenti dan mengakibatkan kehebohan pada kawasan tersebut.

Kasus lainnya adalah berdasarkan artikel *writeup*(Oktariana Paramitha Sandy 2019, hlm.1) pada Cyberthreat.id bahwa terdapat seorang hacker yang dapat membobol 2.000 situs web hanya bermodal HP China. Oleh karena terdapat beberapa kasus yang sudah disebutkan , diperlukannya sebuah sistem keamanan komputer yang dapat mencegah sistem keamanan kita dibobol oleh penyerang. Terlebih lagi jika kita mengelola sebuah server sangat diperlukan sistem keamanan seperti *firewall* yang berfungsi mencegah terjadinya sebuah penyerangan untuk mengambil data-data kita

Didalam sebuah firewall, terdapat sebuah *Intrusion Detection System* yang berfungsi untuk mendeteksi adanya aktifitas jaringan yang sangat mencurigakan, sehingga jika terjadinya sebuah percobaan penyerangan terhadap sistem kita , dapat terdeteksi dan kita juga dengan cepat mengetahui hal tersebut sehingga kita dapat secara cepat melakukan pencegahan terhadap percobaan penyerangan tersebut.

Dengan menggunakan *Intusion Detection System* ini dapat menjadi tambahan keamanan tanpa harus kita selalu berada didepan layer komputer. Kita juga bisa mengetahui tipe tipe serangan yang sedang terjadi dalam bentuk sebuah laporan yang disimpan dalam sebuah log, sehingga kita bisa mengetahui celah mana pada sistem kita yang harus diperbaiki atau diperkuat sistem keamanannya.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang ada, maka penulis memiliki sebuah rumusan masalah sebagai berikut :

1. Apakah efektif menggunakan Intrusion Detection System dalam mengamankan sebuah server?
2. Bagaimana cara kerja *Intrusion Detection System* dalam mendeteksi sebuah *anomaly*?
3. Bagaimana pengaruh *Intrusion Detection System* dalam melindungi server komputer

1.3 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah:

- Untuk mengetahui bagaimana cara kerja *Intrusion Detection System* dengan metode *anomaly-based* pada suricara dalam mendeteksi sebuah serangan.
- Untuk mengetahui efektivitas *Intrusion Detection System* dalam mendeteksi sebuah serangan.

1.4 Manfaat

Manfaat yang didapatkan dalam penelitian ini adalah:

1. Menjadikan penelitian ini menjadi sebuah pengetahuan dasar mengenai cara kerja dari *Intrusion Detection System.*
2. Menjadikan penelitian ini sebagai pengetahuan dasar untuk melakukan penelitian yang mendalam mengenai topik penelitian ini.
3. Mengetahui sejauh mana Intrusion Detection System pada suricata dalam mendeteksi sebuah serangan.

1.5 Ruang Lingkup

Berdasarkan latar belakang yang telah disampaikan, maka ruang lingkup penelitian ini mencangkup sebagai berikut:

- Melakukan penelitian terhadap *Intrusion Detection System* pada Suricata dengan melakukan simulasi penyerangan terhadap sebuah server yang sudah terpasang suricata, lalu melakukan pemeriksaan hasil terdahap simulasi tersebut, apakah *Intrusion Detection System* pada suricata dapat bekerja dengan baik.

1.6 Luaran yang diharapkan

Luaran yang diharapkan *adalah Intrusion Detection System* pada suricata dengan metode Anomaly-based adalah analisis hasil dari pengujian berupa akurasi yang dapat terdeteksi oleh *Intrusion Detection System* dan waktu yang dapat dideteksi oleh *Intrusion Detection System.*

1.7 Sistematika Penulisan

Sistematika penulisan laporan penelitian ini berisi beberapa bagian sebagai berikut:

- **BAB 1 PENDAHULUAN**

  Berisi Latar belakang penelitian, tujuan, manfaat, ruang lingkup penelitian, luaran yang diharapkan, dan sistematika penulisan.

- **BAB 2 LANDASAN TEORI**

  Berisi teori-teori pendukung dalam melakukan penelitian.

- **BAB 3 METODOLOGI PENELITIAN**

  Berisi tentang Langkah kerja yang dilakukan pada penelitian ini, seperi identifikasi masalah, persiapan alat-alat , serta metode atau teknik yang dilakukan dalam melakukan simulasi penyerangan terhadap server, dan hasil dari simulasi penyerangan tersebut.

- **BAB 4 PEMBAHASAN**

  Berisi tentang proses pengujian yang dilakukan dan menambilkan hasil dari pengujian tersebut

- **BAB 5 KESIMPULAN DAN SARAN**

  Berisi tentang kesimpulan dan saran berdasarkan rumusan masalah serta hasil dari pengujian yang sudah dilakukan.

- **DAFTAR PUSTAKA**
- **LAMPIRAN**