BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Perkembangan ilmu teknologi diiringi dengan meningkatnya kebutuhan akan teknologi jaringan komputer dan internet. Selain sebagai penyedia informasi, jaringan internet dapat digunakan untuk bertukar data. Salah satu dampak dari kemajuan teknologi yaitu informasi dan data dapat diperoleh dari pengguna ke pengguna yang lain dengan mudahnya. Kemudahan bertukar informasi tersebut juga menyebabkan munculnya kejahatan *cyber* atau biasa disebut *cybercrime*. Penyusupan pada jaringan juga termasuk *cybercrime*. Banyak cara untuk melakukan penyusupan mulai dari sekedar tes jaringan hingga berusaha mencuri data penting dan bahkan merusak sistem yang ada [1].

SQL *Injection* merupakan salah satu cara untuk melakukan penyusupan ke dalam sebuah webserver. SQL *Injection* dilakukan dengan menggunakan kode SQL untuk memanipulasi database. Serangan ini akan merugikan banyak orang karena penyerang dapat mencuri maupun mengubah data yang ada. Salah satu upaya untuk mencegah terjadinya penyusupan SQL *Injection* tersebut yaitu dengan menerapkan keamanan jaringan [2]. Keamanan jaringan merupakan hal yang penting untuk dilakukan agar dapat mengantisipasi risiko ancaman baik secara langsung maupun tidak langsung. Terdapat beberapa sistem keamanan jaringan yang dapat dimanfaatkan seperti firewall untuk menghentikan paket yang tidak diizinkan, dan *cryptography* dengan enkripsi data. Selain itu juga terdapat sistem pendeteksian penyusup atau *Intrusion Detection System* (IDS) dan sistem pencegahan penyusup atau *Intrusion Prevention System* (IPS). Suricata merupakan salah satu IDPS dan juga alat monitoring keamanan jaringan yang berbasis *open-source*. Suricata yang bekerja sama dengan firewall akan mencegah serangan yang masuk jika menerapkan aturan yang sesuai [3].

Berdasarkan pemaparan tersebut, IPS dapat menjadi solusi yang dapat diterapkan untuk menangani serangan SQL *Injection*. Penelitian tentang implementasi *Intrusion Prevention System* (IPS) menggunakan Suricata dengan

fokus serangan SQL *Injection* ini diharapkan mampu menjaga layanan yang diberikan server terhadap pengguna.

1.2 RUMUSAN MASALAH

Rumusan masalah dari penelitian ini adalah:

1. Bagaimana melakukan perancangan sistem keamanan dengan mengimplementasikan Suricata?
2. Bagaimana cara mengetahui *rules* Suricata yang efektif agar dapat mendeteksi dan juga mencegah adanya ancaman SQL *Injection*?
3. Bagaimana kinerja dari Suricata berdasarkan parameter *response time*?

1.3 BATASAN MASALAH

Batasan masalah dari penelitian ini adalah:

1. Penerapan Suricata sebagai IPS hanya untuk menghadapi serangan SQL *Injection*.
2. IPS diterapkan dalam mode *inline* pada jaringan LAN.
3. Menggunakan metode *Signature-based*.
4. Menggunakan linux ubuntu sebagai OS IPS.
5. Menggunakan *tool* SQLMap sebagai penyerang.
6. Parameter yang akan diukur yaitu *response time*.
7. Pengujian penelitian hanya sebatas jaringan lokal di Laboratorium PSD.

1.4 TUJUAN

Tujuan dari penelitian ini adalah:

1. Mengetahui proses perancangan sebuah sistem keamanan dengan menerapkan Suricata sebagai IPS.
2. Mengetahui penerapan *rules* yang efektif pada Suricata untuk menghadapi serangan SQL *Injection*.
3. Mengetahui kinerja Suricata berdasarkan parameter *response time*.

1.5 MANFAAT

Penelitian ini diharapkan dapat meningkatkan keamanan jaringan dari serangan yang terdeteksi oleh Suricata, mampu merancang sebuah sistem keamanan yang dapat mempermudah administrator jaringan dalam mewujudkan sistem yang aman dan handal. Penulis juga mengharapkan adanya penelitian ini dapat menunjang berbagai pengembangan dalam meningkatkan keamanan jaringan dengan mengimplementasikan *Intrusion Prevention System.*

1.6 SISTEMATIKA PENULISAN

Penelitian ini dibagi menjadi lima bab. Bab pertama meliputi latar belakang, rumusan masalah, Batasan penelitian, tujuan penelitian, manfaat penelitian, dan sistematika penulisan. Bab selanjutnya membahas tentang tinjauan pustaka dan dasar teori yang berisikan jaringan komputer, keamanan jaringan, *Intrusion Detection System* dan *Intrusion Prevention System*, firewall, *IPTables*, Suricata, SQL *Injection*, SQLMap, serta parameter *response time*. Prosedur penelitian seperti perancangan sistem, alat yang digunakan, konfigurasi jaringan maupun konfigurasi server IPS dan skenario pengujian dipaparkan pada bab ketiga. Bab keempat membahas tentang hasil dan analisis berdasarkan hasil implementasi. Bab terakhir berisikan kesimpulan dan saran pengembangan untuk penelitian kedepannya