BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

BLPT (Balai Latihan Pendidikan Teknik) Yogyakarta tepatnya di ICT terdapat sebuah server yang baru saja dibangun dan didalamnya terdapat sebuah penyimpanan berbasis *cloud*. Untuk itu server tersebut harus memiliki suatu sistem yang dapat mendeteksi serangan-serangan yang bisa kapan saja terjadi.

Sebagai langkah antisipasi untuk menghindari terjadinya serangan terhadap server. Oleh karena itu, peneliti terpikirkan untuk membuat suatu sistem yang dapat mendeteksi serangan-serangan seperti itu. IDS (*Instrusion detection system*) yang digunakan dalam usaha membangun sistem pendeteksi intrusi ini adalah aplikasi *open source* Suricata yang diinstal pada server Linux Debian .

IDS (*Instrusion detection system*) Suricata merupakan sebuah aplikasi berbasis *open source* yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah jaringan komputer. IDS Suricata memantau lalu lintas yang melewatinya dan menghasilkan output yang tersimpan dalam bentuk file log.

1.2 Tujuan Penelitian

Tujuan dari penelitian ini dimaksud untuk mencapai beberapa hal sebagai berikut:

1. Mendeteksi serangan yang kemungkinan akan terjadi di server ICT BLPT Yogyakarta.
2. Menghasilkan rekapitulasi output serangan yang tersimpan dalam bentuk file log.

1.3 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan, maka permasalahan yang dapat dirumuskan: "Membangun suatu sistem keamanan yang dapat

mendeteksi serangan yang masuk kedalam server jaringan dengan menggunakan aplikasi IDS (*Instrusion detection system*) Suricata di ICT BLPT (Balai Latihan Pendidikan Teknik) Yogyakarta serangan yang terjadi dan menghasilkan output yang tersimpan dalam bentuk file log".

1.4 Batasan Masalah

Beberapa batasan masalah yang digunakan dalam penelitian ini adalah sebagai berikut.

1. Sistem operasi yang digunakan adalah Debian 8.
2. Server yang digunakan hanya satu dan diletakan di ruang ICT BLPT (Balai Latihan Pendidikan Teknik) Yogyakarta.
3. Software yang digunakan sebagai sistem pendeteksi intrusi adalah Suricata.
4. Pengujian intrusi dilakukan dengan cara DOS (*denial of service*).
5. Daftar rule yang digunakan *rule management with Oinkmaster* yang diunduh.
6. IP *address* yang digunakan adalah IPv4.
7. Hanya mendeteksi serangan yang terjadi dan menghasilkan output yang tersimpan dalam bentuk file log .

1.5 Sistematikan Penulisan

Pada laporan Tugas Akhir ini menjelaskan tentang "Implementasi *Instruction Detection System* (IDS) Menggunakan Suricata Dalam Mendeteksi Serangan *Denial of Service* Pada Server Linux Debian 8.0 di BLPT Yogyakarta" yang terdiri dari lima bab, yang masing-masing bab akan dijelaskan secara singkat dari tiap bab.

1. **BAB I : PENDAHULUAN**

   Bab ini berisi latar belakang masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, metode penelitian, dan ssistematika penulisan.

2. **BAB II : LANDASAN TEORI**

   Dalam bab ini berisi tentang landasan teori yang berkaitan dengan suricata dengan aplikasi Loic yang digunakan referensi dalam pembuatan

Tugas Akhir ini dan kebutuhan system yang digunakan untuk membangun keamanan jaringan.

3. **BAB III : GAMBARAN UMUM**

Dalam bab ini akan menjelaskan mengenai studi kasus yang diangkat dalam laporan ini, berisi mengenai profil perusahaan, stuktur organisasi, masalah yang diambil dari studi kasus tersebut.

4. **BAB IV : PEMBAHASAN**

Dalam bab ini akan dijelaskan mengenai pembangunan keamanan jaringan dan konfigurasi yang dilakukan serta uji coba hasil dari keamanan jaringan tersebut.

5. **BAB : PENUTUP**

Dalam bab ini penulis akan menguraikan beberapa kesimpulan dari uraian bab-bab sebelumnya, dan penulis akan berusaha memberikan saran yang mungkin bermanfaat untuk pengembangan dari teknologi yang telah dibuat.