1 PENDAHULUAN

1.1 Latar Belakang

Badan Pengkajian dan Penerapan Teknologi (BPPT) merupakan badan pemerintah dalam bidang teknologi yang terdiri atas beberapa subbagian dan masing-masing subbagian tersebut memiliki tugas pokok yang berbeda-beda.

Seorang administrastor jaringan seringkali mengalami masalah dalam keamanan lalu lintas jaringan. Salah satu masalah yang seringkali terjadi yaitu tidak diketahui adanya ancaman atau serangan yang masuk ke dalam sebuah sistem. Selain adanya ancaman yang tidak terdeteksi, seorang administrator harus memeriksa *log* dengan server langsung, dan ketika *log* yang masuk sangat banyak akan menyulitkan administrator dalam membaca *log*. Ancaman-ancaman yang seringkali terjadi salah satunya dapat menyebabkan kerusakan pada sebuah sistem jaringan. Ancaman yang sering terjadi diantaranya yaitu *port scanning*, penyusupan menggunakan *remote* SSH, dan *attacker* dapat menyerang web menggunakan SQL *injection* untuk mengetahui *database* pada sebuah web.

Karena adanya berbagai ancaman yang tidak terdeteksi oleh administrator jaringan tersebut, maka diperlukan sebuah sistem yang dapat mendeteksi adanya ancaman pada aliran data sebuah sistem. Sistem yang dapat mendeteksi adanya aktivitas yang mencurigakan pada aliran data tersebut yaitu IDS (*Intrusion Detection System*).

Untuk membuat IDS (*Intrusion Detection System*) diperlukan perangkat lunak yang dapat mendeteksi aktivitas pada sistem jaringan. Perangkat lunak IDS tersebut salah satunya yaitu suricata. Perangkat lunak suricata pada IDS akan diinstal sebagai sensor IDS.

Serangan maupun aktivitas yang terdeteksi oleh sensor IDS tersebut akan tersimpan berupa *log*. *Log* data pada IDS tersebut akan menjadi sulit untuk dibaca ketika *log* aktivitas yang masuk berjumlah sangat banyak. Oleh karena itu, diperlukan SIEM (*Security Information and Event Management*) sebagai *front-end* untuk *monitoring* dan mengelola *log* dari IDS. Perangkat lunak yang digunakan untuk membangun SIEM diantaranya Elasticsearch, Logstash, dan Kibana dari Elastic Stack.

1.2 Tujuan

Adapun tujuan dari pembuatan dari tugas akhir Implementasi Suricata sebagai IDS dan Elastic Stack sebagai SIEM pada Lab Development BPPT yaitu :

1. Menerapkan Suricata sebagai IDS untuk mendeteksi ancaman pada aliran data dengan memberikan sebuah peringatan/*alert* kepada administrator.
2. Menguraikan *log* data pada IDS dengan membangun sebuah sistem monitoring keamanan data menggunakan Elastic Stack

1.3 Manfaat

Adapun manfaat dari Implementasi Suricata sebagai IDS dan Elastic Stack sebagai SIEM pada Lab Development BPPT yaitu :

1. Mendeteksi adanya aktivitas mencurigakan maupun ancaman pada aliran data.
2. Membantu administrator dalam memonitor dan mengelola log data IDS dengan tampilan di web.

1.4 Ruang Lingkup

Ruang lingkup dari tugas akhir Implementasi Suricata sebagai IDS dan Elastic Stack sebagai SIEM pada Lab Development BPPT yaitu :

1. Implementasi Suricata sebagai IDS dibangun pada mini PC dengan NIC berjumlah dua.
2. Masing-masing NIC digunakan sebagai *mirroring* dan mengalirkan data menuju server Elastic Stack.
3. Sistem operasi yang digunakan pada sensor IDS yaitu Linux Ubuntu 16.04.
4. Pengujian dilakukan menggunakan sistem operasi Ubuntu, dan Windows sebagai penyerang.
5. Pengujian IDS menggunakan *rules* sederhana yaitu mendeteksi ping sebagai *alert,* dan mendeteksi remote SSH dari *default* Suricata.
6. Implementasi Elastic Stack sebagai SIEM dibangun pada mesin virtual VMware esxi.
7. Sistem operasi yang digunakan pada VM Server Elastic Stack yaitu Linux Ubuntu 18.04.
8. Pengujian SIEM pada Kibana meliputi menu Discover, Visualization, dan Dashboard.
9. Pengujian mengunakan remote VPN untuk mengakses jaringan di Lab Development BPPT.