RINGKASAN

NURUL HANIFAH PRATIWI. Implementasi Suricata Sebagai IDS dan Elastic Stack Sebagai SIEM pada Lab Development BPPT. *Implementation of Suricata as IDS and Elastic Stack as SIEM at BPPT Development Lab*. Dibimbing oleh RINGGA GILANG BASKORO.

Sebuah keamanan jaringan merupakan suatu aspek penting dalam membangun sebuah jaringan. Aliran data pada jaringan memiliki kerentanan terhadap berbagai paket data yang keluar maupun yang masuk pada lalu lintas jaringan. Kerentanan pada aliran data tersebut menjadi celah bagi seorang *hacker* untuk melakukan kejahatan terhadap lalu lintas jaringan. Kejahatan tersebut dapat berupa penyalahgunaan hak akses, maupun kegiatan ilegal lainnya.

Pembuatan implementasi Suricata sebagai IDS dan Elastic Stack sebagai SIEM merupakan salah satu solusi untuk mengamankan dan mengelola *log* pada sebuah jaringan. IDS (*Intrusion Detection System*) merupakan sebuah teknologi yang dapat mendeteksi serangan-serangan pada aliran data sebuah jaringan dengan memberikan *alert* dan informasi kepada administrator, salah satu perangkat lunak untuk membangun IDS yaitu Suricata. *Log* pada IDS akan dikelola oleh Elastic Stack yaitu perangkat lunak untuk membangun SIEM. SIEM (*Security Information and Event Management*) adalah teknologi yang digunakan untuk mengelola *log* dan *monitoring* lalu lintas jaringan. Pada implementasi ini SIEM digunakan untuk mengelola *log* data dari IDS.

Kata Kunci: *Intrusion Detection System, Suricata, Security Information and Event Management, Elastic Stack*