RINGKASAN

RIZKI ADE MAULANA. Penerapan Sistem Pendeteksi dan Pencegah Serangan *Malware* dengan Sensor Maltrail pada Jaringan *Server* di Diskominfo Tangerang Selatan. *Implementation of Malware Attack Detection and Prevention System with Maltrail Sensor on Server Network at Diskominfo of South Tangerang*. Dibimbing oleh FAOZAN AHMAD.

Diskominfo Kota Tangerang Selatan merupakan suatu perangkat daerah yang dibentuk untuk membantu Walikota Kota Tangerang Selatan dalam melaksanakan urusan pemerintahan dibidang Komunikasi, bidang Informatika, bidang Persandian dan bidang Statistik. Diskominfo Kota Tangerang Selatan bertugas mengurus dan menjamin keamanan TIK, khususnya dibidang *networking support*, seperti menginstalasi perangkat jaringan, memperluas jaringan internet, perawatan perangkat jaringan secara berkala, dan peningkatan kualitas keamanan jaringan.

Dalam usaha peningkatan kualitas keamanan jaringan, dibutuhkan sebuah sistem yang dapat mendeteksi dan memblokir *malware-malware* yang berusaha masuk ke dalam jaringan pemerintahan dan pelayanan publik di Kota Tangerang Selatan. Sistem Pendeteksi dan Pencegah Serangan *Malware* dengan Sensor Maltrail merupakan solusi dari permasalahan tersebut. *Software* yang digunakan untuk melakukan pendeteksian *malware*, yakni bernama Maltrail (Malware Trail). Cara kerja dari *software* ini mirip dengan mekanisme "sensor" yang memindai seluruh aktivitas *traffic* pada jaringan *server*. Kemudian, s*oftware* yang digunakan untuk melakukan *blocking* 'pencegahan' dari serangan *malware*, yaitu Fail2Ban. Kedua sistem tersebut dikolaborasikan dan disesuaikan dengan jaringan *server*.

Metode yang digunakan dalam pembuatan sistem ini adalah PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize). Metode ini cocok utnuk mendesain pengembangan keamanan jaringan yang pendekatannya terpusat pada administrator. Metode ini memiliki 6 tahapan, yaitu persiapan, perencanaan, desain, implementasi, operasi dan optimasi. Tahap persiapan, meliputi penentuan kebutuhan untuk pengembangan keamanan jaringan berdasarkan konsep arsitektur yang akan diterapkan. Tahap perencanaan, diidentifikasian persyaratan jaringan berdasarkan tujuan, dan kebutuhan pengguna. Tahap desain, meliputi desain pengembangan berdasarkan persyaratan teknis yang diperoleh dari kondisi di lapangan. Tahap implementasi, dilakukan instalasi dan konfigurasi berdasarkan spesifikasi desain. Pada tahap operasional, meliputi pengelolaan dan *monitoring* komponen-komponen jaringan, mengelola pemeliharaan *upgrade* dan mengelola kinerja sistem. Tahap optimasi meliputi pengujian sistem dan penyelesaian masalah terkait sistem keamanan jaringan yang diterapkan.

Penerapan Sistem Pendeteksi dan Pencegah Serangan *Malware* dengan Sensor Maltrail pada Jaringan *Server* di Diskominfo Tangerang Selatan telah berhasil dilakukan sesuai dengan tujuan awal pembuatan sistem. Fungsionalitas utama dari *security networking software*, yakni Maltrail telah dapat dikolaborasikan dengan sistem Fail2Ban.

Kata Kunci: Fail2Ban, Maltrail, *malware*, pencegah, dan pendeteksi.