ABSTRAK

Dinas Komunikasi dan Informatika Persandian dan Statistik (Diskominfo) Kota Sumedang, merupakan organisasi pelayanan publik yang bertanggung jawab menangani bidang data dan jaringan komunikasi yang menghubungkan semua lembaga pemerintahan seperti kelurahan, kecamatan dan dinas-dinas yang terhubung ke server Diskominfo Sumedang. Tugas server yaitu melayani semua perangkat yang terhubung kejaringannya, seperti memonitoring seluruh keamanan aktivitas jaringan, perlindungan sistem, data, dan peningkatan kualitas keamanan jaringan. Melihat hal tersebut dibutuhkan sebuah sistem yang dapat mendeteksi dan memblokir malware-malware yang berusaha masuk ke jaringan server Diskominfo Sumedang.

Pada Proyek Akhir ini dirancang suatu sistem implementasi sensor Maltrail (Malware Trail) dan Fail2Ban untuk mendeteksi dan mencegah serangan malware pada jaringan server Diskominfo Sumedang dengan push notifikasi, yang merupakan solusi lain dari permasalahan tersebut. Software yang digunakan untuk melakukan pendeteksian yaitu Maltrail. Cara kerja dari software ini sebagai sensor yang memindai seluruh aktivitas trafik pada jaringan server. Kemudian, software yang digunakan untuk melakukan blocking atau pencegahan dari serangan malware, yaitu Fail2Ban. Sistem tersebut menggunakan bot telegram sebagai push notifikasi jika ada serangan malware ke server.

Dari hasil pengujian serangan malware pada server, terjadi penurunan throughput sebesar 56,28%, hasil implementasi sistem ini mampu mendeteksi dan memblokir malware trafik pada jaringan. Kemudian sistem mampu mendeteksi serangan selain malware yaitu scanning port dengan tingkat ancaman 2,7%. Sehingga sistem mampu meminimalisir ancaman serangan dan mampu meningkatkan nilai throughput pada jaringan server Diskominfo Sumedang dengan melihat perbandingan trafik malware sebelum dan sesudah penerapan sistem.

Kata Kunci: Maltrail, Fail2Ban, malware, mendeteksi, mencegah.