ABSTRAK

Jaringan komputer merupakan media informasi yang berkembang begitu pesat, hampir seluruh kegiatan komunikasi menggunakan jaringan komputer sebagai media transformasi informasi. Namun ada hal-hal yang harus diperhatikan dalam penggunaan jaringan komputer yaitu banyaknya arus data yang keluar masuk, *malicious traffic* merupakan suatu kejadian abnormal pada lalu lintas jaringan yang dapat membahayakan komputer. Untuk mengetahui kondisi normal dan abnormal pada jaringan dibutuhkan sistem monitoring untuk pengawasan, mengolah, dan mengontrol. Untuk mengatasi masalah tersebut pada Proyek Akhir ini dilakukanlah sistem monitoring dengan menggunakan aplikasi maltrail yang memanfaatkan daftar yang tersedia secara publik yang berisi jalur berbahaya atau secara umum mencurigakan, bersama dengan jejak statis yang dikumpulkan dari berbagai laporan AV dan daftar yang ditetapkan pengguna khusus, jejak tersebut dapat berupa apa pun dari nama domain, alamat URL atau IP. Aplikasi maltrail ter-integrasi dengan berbagai *tools* yaitu sensor, server, dan klien. Sensor merupakan komponen untuk pemantauan lalu lintas untuk mencari "jejak" yang telah ditandai dalam blacklist, dan server akan menyimpan semua peristiwa (yaitu entri log) dalam periode (24h) yang akan di transfer ke klien dalam bentuk CSV. Kemudian client berupa web browser sebagai web interface untuk monitoring via web yang menampilkan data berupa presentasi seperti ancaman, kejadian, sumber, dan jejak dengan cara mengakses http://127.0.0.1:8338.

Kata kunci : jaringan, malicious traffic, sistem monitoring, maltrail, sensor, server, klien.