ABSTRAK

Pertumbuhan jumlah pengguna dan perkembangan dari aplikasi-aplikasi yang memanfaatkan jaringan atau internet berdampak pada peningkatan jumlah data yang di transfer melalui jaringan. Semakin meningkatnya transfer data di dalam jaringan, maka *traffic* (arus) data juga mengalami peningkatan. Sehingga diperlukan sebuah sistem *monitoring* dan *analysis* terhadap sebuah sistem atau jaringan komputer dengan melakukan *capturing* pada aliran paket-paket data jaringan. Pengolahan paket data jaringan sangat penting buat para *sys admin* . Sistem *monitoring* dan *packet capturing* menganalisa dan mengidentifikasi adanya jenis *flooding* dan *packet loss* dengan menggunakan algoritma *random early detection* (RED) yang membandingkan nilai *counter* paket berdasarkan jenisnya dengan nilai ambang batas (*threshold value*) yang bersifat *user defined*. Sistem *monitoring* dan *packet capturing* diimplementasikan pada jaringan *wireless* LAN kampus Teknologi Informasi Universitas Sumatera Utara pada saat jam aktif. Hasil dari implementasi sistem yang dilakukan selama beberapa hari berturut diperoleh paket yang aktif jenis TCP , UDP dan *Ethernet*. Untuk jenis intrusi yang sering terjadi adalah TCP/SYN *flooding* dan *packet loss* pada TCP *packet*.

Kata Kunci: sistem monitoring , *packet capturing* , RED, intrusi, jpcap, *wireless* LAN.

ABSTRACT

The Growth in the number of users and the development of applications that utilize the network or the Internet, impact on increasing the amount of data transferred over the network. The increasing transfer of data in the network, then traffic (flow) data is also increased. So, we need a monitoring and analysis system to a computer system or network by capturing the flow of network data packets. Processing network data packets are very important for system administrators. System monitoring and packet capturing analyze and identify the types of flooding and packet loss algorithms using random early detection (RED) comparing the packet counter value by type with the threshold value (threshold value) that are user-defined. System monitoring and packet capturing implemented onwireless LAN of the campus of Information Technology University of North Sumatra during active hours.Results of the implementation of the system is done for several consecutive days obtained active packet type of TCP, UDP and Ethernet. For this type of intrusion that often occurs is the TCP / SYN flooding and TCP packet loss.

Keywords: monitoring system, packet capturing, RED, intrusion, jpcap, wireless LAN.