ABSTRAK

Flooding Data adalah sejenis serangan *Denial of Service* (DOS) dimana *flooding data* melakukan serangan terhadap sebuah komputer atau *server* didalam jaringan lokal maupun internet dengan cara menghabiskan sumber *(resource)* yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut. Penelitian ini untuk menganalisis modikasi serangan dan menjaga keamanan sebuah sistem dari ancaman *flooding data*. Untuk itu diperlukan sebuah alat deteksi yang dapat mengenali adanya serangan *flooding data* dengan cara menyadap paket data kemudian membandingkannya dengan *database rule* IDS (berisi *signature* paket serangan). IDS *engine* akan membaca *alert* dari IDS (antara lain berupa jenis serangan dan *IP address* penyusup) agar dapat meminimalisasi serangan *flooding data* terhadap jaringan LAN *(Local Area Network)* dan *server*. Metode pengujian serangan *flooding data* dengan menggunakan metode *penetration testing*. Adapun tiga buah *sample* pengujian yaitu serangan *flooding data* terhadap protokol ICMP, UDP dan TCP dengan menggunakan aplikasi deteksi *flooding data*. Hasil yang diperoleh saat melakukan pengujian serangan *flooding data* dimana sensor alat deteksi dapat mendeteksi seluruh serangan dan seluruh sampel serangan dapat dicegah atau di *filtering* dengan menggunakan sistem keamanan jaringan berbasis *firewall*.

Kata kunci : *Intrusion Detection System* (IDS), *Denial of Service* (DOS), *Flooding Data, Firewall*, (LAN) *Local Area Network*

ABSTRACT

Flooding Data is a type of Denial of Service (DOS) attack in which flooding data attacks a computer or server in a local network or internet by spending resources owned by the computer until the computer can not perform it's function properly so that does not directly prevent other users from gaining access to services from the computer being attacked. This research is to analyze the indication of attack and maintain the security of a system from the threat of flooding data. For that we need a detection tool that can recognize the existence of data flooding attacks by tapping the data package and then compare it with IDS database rule (contains signature attack packets). IDS engine will read alerts from IDS (such as attack type and IP address intruder) in order to minimize flooding attack data against LAN (Local Area Network) and server. Method of testing flooding attack data by using penetration testing method. The three test samples are data flooding attacks against ICMP, UDP and TCP protocols using data Flooding applications. Results obtained when testing flooding attacks data where detection sensor sensors can detect all attacks and all attack samples can be prevented or filtered using a firewall-based network security system.

Keywords: *Intrusion Detection System (IDS), Denial of Service (DOS), Flooding Data, Firewall, (LAN) Local Area Network*