ABSTRAK

Keamanan suatu jaringan merupakan isu yang sangat penting untuk diprioritaskan keberadaannya. Banyak cara dilakukan untuk melakukan penyusupan kedalam jaringan internal untuk sekedar melakukan tes terhadap jaringan tersebut seperti *scanning* atau pun membuat jaringan menjadi lumpuh dengan melancarkan *Denial of Service*(DoS) terlebih usaha untuk mendapatkan informasi penting dari server. Salah satu cara yang dapat digunakan untuk me-*monitoring* tindakan penyusupan tersebut adalah dengan mengimplementasikan IPS(*Intrusion Prevention System*). Sistem IPS akan mendeteksi penyusupan dengan metode *signature-based* menggunakan IDS Snort dan mengeluarkan *alert* untuk setiap tindakan penyusupan yang dikenali oleh IDS Snort. Selanjutnya IPS engine akan membaca *alert* yang telah di-*generate* dan melakukan pemblokiran akses IP dari intruder menggunakan iptables *firewall* berdasarkan informasi ip yang tersimpan pada *alert* yang di-*generate* oleh Snort IDS.

Setelah sistem IPS berhasil berjalan, perlu dibuat suatu aplikasi antarmuka untuk mengatur sistem IPS seperti managemen *alert*, pengaturan konfigurasi IDS Snort, dan lainnya. Untuk itu akan dibuat suatu aplikasi dashboard web sebagai antarmuka untuk mengatur sistem IPS seperti tersebut diatas. IDS Snort akan menyimpan data *alert* kedalam database untuk diolah selanjutnya dan akan ditampilkan ke dalam aplikasi dashboard web. Dengan adanya sistem IPS ini diharapkan mampu mengenali tindakan-tindakan penyusupan sehingga dapat meningkatkan tingkat keamanan jaringan

Kata kunci: IPS(*Intrusion Prevention System*), Snort IDS, iptables *Firewall*, *alert*, *signature-based*

ABSTRACT

Security of a network is already become the most important issue to be noticed and should be our priority. There are so many ways which can be done to penetrate into internal network in order to test the network, such as scanning or even make the network to be down using Denial of Services (DoS) furthermore to gain important informations from server. One of the ways to monitor the penetration is Intusion Prevention System (IPS). IPS system will detect penetration with signature based method using IDS Snort and display alert to each penetration activities which is identified by snort. IPS engine will read alert which has been generated and it is going to block IP access from intruder using iptables firewall based ip information stored of the generated alert by snort IDS.

After IPS system is already running, an interface applicaton to arrange IPS system like management alert, IDS Snort configuration, etc is needed. Based on that reason, it needs dashboard web application as interface to arrange IPS system like already mentioned above. IDS Snort will store data alert into database to be processed and it will be displayed through dasjboard web. By using this IPS system, it is expected to be able to identify each penetration so that security of network can be increased.

Key Words: IPS(Intrusion Prevention System), Snort IDS, iptables Firewall, alert, signature-based