

ABSTRAK

ANALISIS PERBANDINGAN PERFORMANSI *INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS)* OSSEC DAN SNORT MENGGUNAKAN *QUALITY OF SERVICE (QoS)*

Oleh
Arifah Ramadhan
20102270

Jaringan yang bersifat publik akan dengan mudah diakses oleh semua orang dari berbagai negara, hal inilah yang membuat jaringan ini rentan terhadap penyerangan. Meskipun setiap jaringan sudah menggunakan *firewall* sekalipun pasti bisa dengan mudah diserang oleh penyerang. Dalam menyelesaikan permasalahan ini, dibutuhkanlah sistem yang lebih kuat daripada *firewall* yaitu *Intrusion Detection and Prevention System* atau lebih dikenal dengan *IDPS*. Pengamanan sistem tersebut dapat dilakukan dengan mengintegrasikan OSSEC dan Snort dimana sistem ini akan memberikan *log* untuk mencatat kegiatan yang dilakukan oleh penyerang. OSSEC akan bertindak seperti *firewall* yang dapat melakukan *allow* dan *block*. Sementara Snort akan menganalisis semua lalu lintas jaringan untuk menyadap dan mencari beberapa jenis penyusupan dalam sebuah jaringan. Dalam penelitian ini, dilakukan pengujian serangan *Distributed Denial of Service (DDoS)* terhadap server jaringan yang telah dipasangkan OSSEC dan Snort. Setelah dilakukan pengujian serangan akan dilakukan pengukuran kualitas jaringan menggunakan *Quality of Service (QoS)* untuk mengetahui keadaan jaringan saat sebelum dilakukan penyerangan dan setelah dilakukan penyerangan. Dalam perbandingan performansi antara Snort dan OSSEC dalam mendeteksi serangan, untuk serangan *ICMP Flood*, Snort lebih unggul dalam hal *throughput* dan *Packet loss*, sedangkan OSSEC lebih baik dalam *delay* dan *jitter*. Dalam mendeteksi serangan *TCP Flood*, Snort menunjukkan performa superior dalam *throughput*, *delay*, dan *packet loss*, sementara OSSEC unggul dalam *jitter*. Untuk serangan *UDP Flood*, Snort lebih baik dalam *throughput* dan *delay*, sedangkan OSSEC memiliki performa lebih baik dalam *jitter* dan *packet loss*.

Kata Kunci: *Intrusion Detection and Prevention System, OSSEC, Snort, Quality of Service*