ABSTRAK

Kenaikan jumlah pengguna internet dan pertumbuhan jumlah serangan siber, khususnya serangan DoS telah menjadi isu yang sangat serius khususnya dalam jaringan WLAN. Penelitian ini bertujuan untuk mencegah serangan DoS pada jaringan WLAN menggunakan teknologi IPS berbasis Snort. Di dalam jurnal referensi penelitian sebelumnya membahas tentang teknologi IPS Snort dan mengidentifikasi beberapa tantangan dan batasan dalam menggunakan IPS Snort untuk keamanan jaringan WLAN. Penelitian ini dilakukan dengan memanfaatkan Virtual Machine menggunakan Virtual Box dengan OS Ubuntu, serta instalasi berbagai tools yang diperlukan termasuk Snort, Libpcap, dan hping3. Tujuan utama dari penelitian ini adalah untuk mengonfigurasi Snort agar dapat mendeteksi dan mencegah berbagai jenis serangan DoS seperti TCP SYN Flood, UDP Flood, dan kombinasi antara TCP & UDP Flood. Hasil penelitian ini menunjukkan bahwa mode Snort sebagai IPS dapat bekerja efektif dalam mencegah serangan DoS dan mengurangi dampaknya terhadap performansi jaringan. Melalui simulasi yang dilakukan, penelitian ini mengevaluasi kemampuan Snort dalam mengidentifikasi dan mengatasi serangan-serangan tersebut serta memastikan pertahanan sistem dan memberikan analisis yang komprehensif terhadap kinerjanya. Hasil akhir dari penelitian ini adalah dapat berkontribusi terhadap pemahaman tentang efektivitas Snort IPS dalam skenario dunia nyata dan memberikan wawasan untuk pengembangan lebih lanjut terhadap sistem keamanan jaringan.

Kata Kunci: *IPS, Snort, WLAN, Denial of Service (DoS), TCP Flood, UDP Flood, Rules, Alert, hping3, Dropped Packet*