ABSTRACT

The increasing use of the internet and the growing number of cyber attacks, DoS attacks particularly have made WLAN security a critical issue. This research aims to prevent Denial of Service (DoS) attacks on Wireless Local Area Networks (WLAN) using Intrusion Prevention System (IPS) technology based on Snort. The literature review section discusses previous research on IPS technology and Snort, and identifies some of the challenges and limitations of using IPS and Snort for WLAN security. The project involves setting up a Virtual Machine using Virtual Box with the Ubuntu as an OS, and installing necessary tools including Snort, Libpcap, and hping3. The primary objective is to configure Snort to detect and prevent various types of DoS attacks such as TCP SYN Flood, UDP Flood, and combined TCP&UDP Flood. The results show that the proposed IPS architecture is effective in preventing DoS attacks and reducing the impact on the network performance. Through the simulation, the study evaluates Snort's capability to identify and mitigate these attacks, ensuring the system's resilience and providing a comprehensive analysis of its performance. The final results contribute to understanding the effectiveness of Snort IPS in real-world scenarios and offer insights for further enhancement of network security measures.

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