ABSTRACT

Work From Home (WFH) as a result of the covid 19 pandemic force the digitalization advances. People do everything remotely because of the health protocol that force them not to interact with each other. Therefore, telecommunication engineer is demanded to supply the client needs for the internet and web server availability. However, the availability of the internet must be accompanied by a strong cyber security system to ensure the availability of web server.

This bachelor's thesis uses Snort as a defence system for a web server. Where, Snort can detect and drop the data packets that are suspected as DoS and DDoS attacks. Snort is tested with SYN and UDP flood attacks. This bachelor's thesis experiment deployed virtual network to implement the simulation. The implementation consists of several components which are one server uses the Linux Ubuntu Operation System (OS), four attackers use the Kali Linux OS, and one client accesses the information on the web server using the Linux Ubuntu OS. Testing is done by using the web server and HIPS Snort turned on so that it can be accessed by the client, then data can be obtained when the attacker attacks the web server.

The result is that all client requests can be accepted by the server when HIPS Snort is turned on, where HIPS Snort drop 96.65% of DoS SYN Flood attack packets, drop 97.92% DDoS SYN Flood attack packets, drop 95.54% DoS UDP Flood attack packets, and drop 95.07% DDoS UDP Flood attack packets. Thus, snort can prevent the server from DoS and DDoS attack in the form of SYN Flood or UDP Flood.

Keywords: Web server; Cyber attack; HIPS Snort; SYN flood; UDP flood