ABSTRACT

Cyber-attack is an inevitable risk from any business in internet era. Cyber-attack can originate from both internal employees and external sources. The office network can be in danger due to cyber-attack and can disturb the workflow. This issue can be prevented by Host Intrusion Prevention System (HIPS) Snort that secures the network through smart security in a box system with Raspberry Pi as the firewall to protect the user devices against Denial of Service (DoS) attacks.

This thesis applies the Raspberry Pi to be the firewall with installing the HIPS Snort as a defence system to protect the user's work devices. The Raspberry Pi is also configured to work as a router. This thesis uses several components for the experiment which are one server uses the Linux Basic Pentesting Operation System (OS), two attackers use the Kali Linux OS, and one client uses Linux Ubuntu (OS) to access the web server. This smart security in a box is installed between the user's devices before connected to the office network. The smart security in a box detects the misuse in the network for all data packets that are suspected of being DoS attacks and drops them. DoS attacks using SYN Flood and UDP Flood are going to put Snort to the test.

The successful client connection when Snort is running are only the average of 48.60% and 46.31% for DoS SYN Flood and UDP Flood attack respectively. When Snort is running, the average incoming attack packets decreases for both DoS SYN Flood and UDP Flood attack. The HIPS Snort can drop the average of 41.48% of SYN Flood attack and 28.27% of UDP Flood attack packets. CPU and Memory usage are higher when Snort is running. DoS SYN Flood attack consumes more CPU and Memory usage of Raspberry Pi with the average of 83.60% and 76.75% respectively when Snort is running.

Keywords: smart security, HIPS snort, raspberry pi, web server, DoS attacks