ABSTRACT

Nowadays, almost all of the devices which are connected to internet have a high chances to be attacked by hackers. The birth of the new attacks in every year also makes them more suffered. Intrusion Detection System Snort (IDS) provides good ways to answer all of those needs. But the problem is, Snort as the IDS can not provide basic ability such as intrussion notification in a user-friendly environment of Dashboard Application to do the monitoring easily. Snort doesn't have a basic ability to block IP address automatically using firewall in the provided hardware if there are intrussions by a certain IP address.

In this final project, a system was created to integrate Snort's abilities as IDS such as Dashboard Application to show detected signature, giving Snort ability to block intrussion in a various firewall, and ClamAV's ability in virus filtering which is expected to increase the performance and Snort's reliability.

According to experiment result and analysis to the created system, it is able to detect intrussion, showing signature in the Dashboard Application, and can block detected intruding IP address automatically. But the IDS Server performance is decreasing as the amount of security services which are running in IDS Server is increasing.

Keywords : ***Network Intrusion Detection Prevention System ,Dahsboard System, Snort , ACL Router, ClamAV.***