ABSTRACT

Information security serves to avoid damage or loss caused by attack activities during the communication process. Information security aspects are Confidentiality, Integrity and Availability. Web server is a service provider that is used to receive HTTP requests that work on port 80 which is most vulnerable to attack threats. Threats of attacks that can occur on the web server are Port Scanning, Brute Force and DDoS. Intrusion Prevention System is a solution that can maintain network security from various attacks. Intrusion Prevention System acts as a protector on the network by detecting and preventing suspicious traffic on a network. In this study, the Intrusion Prevention System uses the Snort and IPTables tools as well as the signature based detection method. The test is carried out using two scenarios, namely before IPS is activated and after IPS is activated. The results of the study are that the three attacks tested have different characteristics of cause and effect. Port Scanning and Brute Force attacks can be prevented by IPS because the characteristics of both attacks are easily recognized by rules in the Snort database. In DDoS attacks, Snort only speeds up the attack time to be accessible again because the characteristics of Slow HTTP attacks are sending incomplete packets in large numbers gradually and maintaining connection session times so that it is difficult for Snort to recognize. In a DDoS attack with an action rule drop, the web server can be accessed again at 160 seconds while the reject rule action can be accessed again at 145 seconds where the normal attack time can be accessed again at 165 seconds. In CPU usage, IPS can reduce usage by 9 .2% on DDoS attacks.

***Keywords**: Intrusion Prevention System, Snort, CIA Triad.*