ABSTRACT

Network traffic is very important to maintain security because sending and receiving data occurs in network traffic. It is possible that network traffic is free from attack interference. The disruption in this research is called Distributed Denial of Service or commonly known as DDoS, DDoS floods network traffic so that the original client cannot access the internet. The attacks used in this research are TCP and UDP floods, TCP attacks flood network traffic by sending large amounts of data continuously, while UDP can flood ports on the host by sending data packets to many ports, causing the host to become unresponsive. A network security system such as IDS is needed that can detect incoming attacks. In order to run according to its function, IDS must be run with tools. This research uses zeek and suricata as tools, and a comparison will be made to the tools used against attacks that enter the system. To determine the accuracy of the number of attacks detected by the tools, this study uses confusion matrix parameters consisting of accuration, precision, and recall. The results shown that Suricata is better in detecting TCP flood attacks with accuration 93.36%, precision 100%, recall 93.36%, but in detecting UDP flood attacks Zeek is better with accuration 63.33%, precision 100%, recall 63.33%.

***Keywords*:** DDoS, IDS, Zeek, Suricata, *Confusion Matrix.*