

## **ABSTRACT**

*Network security is an important thing to do to prevent unauthorized use of resources. An intrusion Prevention System (IPS) is one of the security tools on the network. In this study, Suricata as an IPS to protect the webserver from SQL Injection attacks using SQLMap by looking at the effectiveness of the rules and response time parameters. This research was conducted in the PSD Laboratory using a LAN network topology that is set to static. Suricata is an IPS tool installed on a PC that functions as a router as well as an IPS server. Normal users and attackers use the Windows 10 operating system, while the web server and IPS server use the Ubuntu 20.04 operating system. The response time parameter testing was performed 30 times during the SQL Injection attack. The results of these tests show the average value when Suricata is applied at 4.260633 milliseconds. This means that Suricata takes 4.2 ms to respond to a packet. Suricata in this study acts as an IPS that works every time a SQL Injection attack occurs, it will be detected by Suricata by checking the packet's compatibility against the signature rules. Rules that are considered effective to deal with SQL Injection attacks are rules that use some ASCII code as keywords.*

**Keywords:** *Network Security, Intrusion Prevention System, Suricata Rules, SQL Injection*