ABSTRACT

The very rapid development of technology demands an increase in the quality of network security. The more open knowledge about hacking and cracking is supported by tools that can be obtained easily and for free. Computer network security threats also come from viruses, malicious, trojans, worms, DOS, spoofing, sniffing, spamming, and others. Network security systems are very important in maintaining a network. To get security in a network, sometimes we have to feel the inconvenience of using it, this is what is often a consideration in implementing a network security system. Many methods can be done to be able to secure a network system. One of them is to use the Intrusion Detection System (IDS). IDS itself specifically functions as protection that cannot stand alone in protecting a system, because it requires an additional tool to handle attacks, namely by using Snort. Snort is a software to detect intruders and is able to analyze packets traversing the network in real time traffic and logging into the database as well as being able to identify shared attacks originating from outside the network.

Keywords: WEB Interface, Alert, Snort, Rule Snort, Hacking, Cracking