

## ABSTRACT

---

*Information technology develops very quickly, especially the Internet. But the development of information technology used by hacker for getting certain information. To handle attacks such as scanning, sniffing and DDoS Attack a Network Intrusion Detection System (NIDS) is required. The solution offered is to build NIDS with Snort, Portsentry, and IPFilter. Snort is able to detect and log attacks such as DDoS Attack, Sniffing and Scanning. Portsentry is able to block an attacker who wants to do the scanning of the server. IPFilter used as a firewall to block IP addresses that have been detected by Snort as an attacker. The NIDS system is integrated with the web interface BASE to show all of the attacks that have been detected by the snort rules. The system is built on the FreeBSD operating system, known as the operating system that has a good security. This system can handle attacks such as port scanning and DDoS Attack.*

*Keywords: NIDS, Sniffing, Scanning, FreeBSD, Snort*