Abstract

Intrusion Detection System (IDS) is a tool, a method, a resource which can monitor or observe activities to identify dangerous or suspicious event. Dangerous or suspicious event can be called intrusion or attack. In detecting a n intrusion, IDS uses 2 main technique which are Signature Based Detection and Anomaly Based Detection.

In this final project, 2 systems is built to detect intrusion, which are a signature based system and anomaly based system. Each system has different design. For signature based IDS, Snort tools is used, whereas for anomaly based IDS, Ourmon tools is used. Both of the system is tested with the same case study. There are 4 case study, which are 3 case study on port scanning attac, denial of service SYN Flood type, and exploit, then 1 case study that is not an attack type like file download activitiy. The analysis done is accuracy analysis, resource usage analysis, and error on detection (false positive and false negative).

From the 4 case testing, it can be concluded that for signature IDS can detect port scanning, denial of service and exploit, where anomaly IDS can only detect denial of service attack and download activity which is not an attack.

***Key Word** : Intrusion Detection System (IDS), Signature Based, and Anomaly Based*