Abstrak

Intrusion Detection System (IDS) adalah *tool*, metode, sumber daya yang dapat memonitor atau mengamati aktifitas-aktifitas untuk mengidentifikasi peristiwa berbahaya atau mencurigakan. Peristiwa yang berbahaya atau mencurigakan itu bisa disebut dengan intrusi atau serangan. Dalam mendeteksi intrusi, IDS menggunakan 2 teknik utama yaitu *Signature Based Detection* dan *Anomaly Based Detection*.

Pada tugas akhir ini, dibangun 2 buah sistem untuk mendeteksi adanya intrusi, yaitu sistem yang berbasis *signature* dan sistem yang berbasis *anomaly*. Masing-masing sistem memiliki rancangan yang berbeda. Untuk IDS yang berbasis *signature* digunakan *tools* Snort, sedangkan untuk IDS yang berbasis *anomaly* menggunakan *tools* Ourmon. Kedua sistem tersebut diuji dengan studi kasus yang sama. Studi kasus yang diuji ada 4 macam, yaitu 3 macam studi kasus yang berupa serangan *port scanning*, *denial of service* jenis *SYN Flood*, dan *exploit* serta 1 studi kasus yang bukan berupa serangan seperti aktifitas *download* suatu *file*. Analisis yang dilakukan adalah analisis akurasi, penggunaan *resource*, dan kesalahan dalam pendeteksian (*false positive* dan *false negative*).

Dari pengujian keempat studi kasus tersebut, dapat disimpulkan bahwa untuk IDS Signature bisa mendeteksi serangan *port scanning*, *denial of service*, dan *exploit*, sedangkan IDS Anomaly hanya bisa mendeteksi serangan *denial of service* dan mendeteksi aktifitas *download* yang sebenarnya bukan merupakan serangan.

Kata Kunci : *Intrusion Detection System* (IDS), *Signature Based*, dan *Anomaly Based*