ABSTRAK

Sistem keamanan jaringan sudah sangat banyak macamnya sesuai dengan keadaan dan kondisi yang bersangkutan. Sistem keamanan jaringan sangatlah penting perannya dalam menjaga suatu keamanan jaringan sehingga dapat mencegah terjadinya penyerangan dan melindungi kita ketika terjadi penyerangan. Sering terjadi penyerangan terhadap sebuah perangkat melalui suatu jaringan baik dalam hal pemberian malware, dan pencurian data.

Proyek akhir ini berfokus pada sejauh mana IDS yang berbasis HIDS dapat mendeteksi serangan serangan yang umum terjadi dalam jaringan. Dengan bantuan Honeypot Dionaea yang dijadikan sebagai penarik perhatian penyerang, serta informasi apa saja yang akan didapatkan ketika melakukan malware analysis menggunakan Cuckoo Sandbox. Implementasi ini dilakukan dengan enam user aktif yang berada dalam satu jaringan dan memperhatikan apakah penyerang dapat terdeteksi oleh IDS atau tidak.

Hasil dari proyek akhir ini didapatkan bahwa IDS yang berbasis HIDS memiliki kelebihan dalam memonitoring data digital serta berdasarkan hasil percobaan penyerangan dengan bruteforce didapatkan 65.55% terdeteksi adanya percobaan *log in* menggunakan username yang tidak terdaftar, 29.16% terdeteksi adanya percobaan *log in* gagal, 4.17% terdeteksi *log in* ganda dalam waktu yang berdekatan, dan 1.11% terdeteksi adanya percobaan *bruteforce* untuk mendapatkan akses ke sistem. Cuckoo Sandbox dapat memberikan informasi malware berupa jenis malware apa yang dianalisis, bagaimana tingkahlaku malware tersebut, dan bagaimana dampak malware tersebut pada sistem yang diserang.

Kata kunci : *Honeypot, IDS, Malware, Malware Analysis System*