ABSTRAK

Sistem keamanan jaringan pada kenyataanya sudah sangat banyak macam nya sesuai dengan keadaan dan kondisi yang bersangkutan. Dan hampir keseluruhannya hanya berbicara tentang melindungi dan menghalau serangan tanpa adanya nilai lebih yang dapat kita manfaatkan. Sehingga kita hanya dapat melindungi sistem tanpa kita dapat menganalisanya lebih lanjut. Untuk itu perlu dibuat sebuah sistem yang dapat membuat sebuah serangan mampu memberikan nilai yang bermanfaat bagi kita.

Tugas akhir ini mengujikan performansi suatu sistem keamanan jaringan yang berfungsi sebagai perangkap dan pendeteksi serangan. Kelebihan dari *Honeypot Dionaea* adalah bisa mendapatkan salinan *malware* yang dikirim oleh penyerang. Sehingga seorang *administrator* dapat mengambil langkah berikutnya, seperti menganalisis *malware* tersebut menggunakan *Malware Analisys Toolkit*.

Dari hasil pengujian, dapat dilihat bahwa *Dionaea* sebagai perangkap mampu menangkap *malware* dan menyimpannya dalam folder *binaries.* Pengujian dilakukan di jaringan publik selama 14 hari, dan *malware* yang tertangkap sebanyak 11 buah. *Service* yang paling banyak diserang adalah Mssql, sedangkan yang paling sedikit adalah HTTP. Lalu baik pada jaringan publik maupun lokal, pendeteksi serangan pun mampu mendeteksi adanya serangan dengan *real time* dan stabil¸ namun masih memiliki *false negative* dan *false positif*. Dan *Cuckoo Sandbox* sebagai *Malware Analisys Toolkit*, mampu memberikan informasi mengenai *malware* tersebut sehingga mampu memberikan informasi yang bermanfaat untuk kedepannya.

Kata Kunci : *Honeypot, Dionaea, IDS, Malware, Malware Analisys Toolkit, Cuckoo Sandbox*