ABSTRAK

Kebutuhan dan penggunaan akan teknologi informasi yang diaplikasikan dalam segala bidang dalam kehidupan sehari-hari telah menjadi sesuatu yang tidak asing lagi.

Honeypot merupakan alat bantu yang menghasilkan nilai palsu saat sumber daya dicoba diakses oleh seseorang/sistem yang tidak sah atau tidak dizinkan. Sistem dengan honeypot akan 'menipu' atau memberikan data palsu apabila ada orang yang memiliki maksud yang tidak baik ketika ia masuk ke suatu sistem informasi. *Honeypot* dirancang untuk meniru sistem yang lemah dimana biasanya *worm* menyebar, dan untuk menangkap *worm* tersebut.

Pada tugas akhir ini implementasi *honeypot* di letakkan pada jaringan *internet* menggunakan *ip public*, yang fungsinya untuk mengobservasi *malware* yang masuk pada jaringan. Sehingga *administrator* hanya menunggu serangan yang datang menuju *honeypot*.

Hasil akhir dalam pengerjaan proyek akhir ini adalah *honeypot* behasil menangkap 8 (delapan) *malware* pada jaringan *internet* menggunakan *virtual private server* dalam jangka waktu observasi selama 2 (dua) hari.

Kata Kunci: ***honeypot, ip public, worm, malware, virtual private server.***

ABSTRACT

The need and usage of information technology that is applied in everyday lives has been something that isn't odd anymore.

Honeypot is a tool to create a fake value as the main source is attempted to be accessed by unauthorized person or system. An employed honeypot in a system will deceit or provides a wrong data when someone with bad intention is entering an information system. Honeypot Nepethes is designed to imitate weak system where worm is usually spread out and also to quarantene those worms.

In this final project honeypot is being implemented on internet network using ip public, which its function is to observe malware that attack the network. So the administrator just has to wait the attacker to come to honeypot.

The results on this final project are that honeypot has succeeded to capture 8 (eight) malware on internet network using virtual private server which is been monitored for 2 (two) days period of observation.

Key Words: honeypot, ip public, worm, malware, virtual private server.