ABSTRAK

Penggunaan akan teknologi informasi yang diaplikasikan dalam segala bidang dalam kehidupan sehari-hari telah menjadi sesuatu yang tidak asing lagi saat ini. Dari berbagai umur bisa dengan mudah mengakses internet. Salah satu alat bantu yang bisa kita andalkan sebagai sistem keamanan virtual adalah *Honeypot*. 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.

Pada tugas akhir ini implementasi *honeypot honeyd* di letakkan pada server utama, yang fungsinya sebagai 'jaring' untuk mengelabuhi serangan penyusup. Pada server utama akan dibuat layanan *File Transfer Protocol*, seberapa kuat layanan FTP bertahan jika ada serangan dari penyusup. Dalam hal ini penyusup berupa penguji serangan memakai *Denial of Services* (DoS) Sehingga *administrator* akan mengetahui perbandingan performansi saat tidak ada serangan, saat ada serangan, dan saat dibelokkan ke port palsu yang dijalankan oleh HoneyD dan Snort IDS. Sebelum dilakukan percobaan kita uji dulu ketahanan server FTP dengan ping flooding attack untuk menentukan threshold pada rules Snort IDS. Agar seperti jaringan riil dibangkitkan trafik di jaringan sebesar 5 Mbps. Kemudian dilakukan analisis performansi, pada 3 kali percobaan dengan kondisi yang berbeda. Pada sisi server performansi yang dilihat yaitu *CPU history*, *RAM usage*, *bitrate data*, dan *processing time*. Akibat dari serangan dari DoS, *CPU history* mencapai 94,7% dan system akan down jika mencapai 100%. Setelah ada *HoneyD*, CPU history menurun dibawah 85%, sehingga layanan FTP akan berjalan normal kembali. *Respon time* yang dibutuhkan HoneyD untuk mengembalikan kondisi normal sekitar 20 sampai 25 detik.

Kata kunci*:* ***HoneyD, Snort IDS, File Transfer Protocol, Ping Flooding Attack, Iperf, Performance***