ABSTRAK

Perkembangan teknologi yang pesat di bidang komunikasi data telah membuat banyak kemudahan di masa sekarang ini. Hal ini diiringi pula dengan meningkatnya kebutuhan akan kehandalan, kecepatan dan efektivitas pertukaran data antar belahan dunia. Setelah beberapa tahun terkonstruksi dan teranyam dengan baik di banyak negara, jaringan komputer yang masih kebanyakan berbasis kabel dihadang oleh tuntutan *user* yang mulai cenderung menyukai layanan mobile. Peningkatan dan kemajuan yang pesat ini sayangnya kurang ditunjang dengan perkembangan sistem pertahanan terhadap serangan yang baik pula. Lebih lagi, sistem kemanan teknologi *wireless* yang ada saat ini membuat *user* masih khawatir dan menjadi relatif kurang nyaman dalam menggunakan teknologi *wireless*.

Beberapa kelemahan IDS (Intrusion Detection System) antara lain kesulitan membedakan aktivitas legal dengan trafik *malicious*, serta belum dapat mendeteksi serangan jika data yang dikirim berupa data terenkripsi. Merangkak naiknya angka kejahatan di Internet diharapkan mampu diminimalisasi dengan hadirnya *honeypot*. Sederhananya, *honeypot* merupakan suatu sistem yang memang didesain untuk disusupi penyerang, baik itu oleh *hacker*, *cracker*, ataupun *script kiddy*. Karena *honeypot* yang sejatinya merupakan suatu sistem tiruan, maka setiap interaksi dengan *honeypot*, semacam *probe*, *scan* dan yang lainnya akan dianggap sebagai usaha penyusupan.

Pada tugas akhir ini, akan di implementasikan suatu sistem *wireless* honeypot yang menyerupai *production system* yang sesungguhnya pada jaringan Telkom PDC, lalu diujicobakan beberapa tipe serangan pada sistem yang telah dirancang hingga dapat menganalisis kehandalan *wireless honeypot* berdasarkan data yang didapat dari *log*, untuk dianalisis secara berkelanjutan untuk meningkatkan sistem keamanan jaringan.