ABSTRAK

Teknologi jaringan nirkabel sebenarnya bukanlah suatu hal yang baru, namun maraknya penggunaan teknologi jaringan nirkabel baru dirasakan akhir-akhir ini saja. Banyak ISP saat ini membangun infrakstruktur nirkabel dalam menggelar jasanya, komunikasi internal perusahaan juga menggunakan jaringan nirkabel. Jaringan nirkabel ini menggunakan frekuensi 2,4 Ghz yang telah dibebaskan penggunaannya oleh pemerintah, karena bebas inilah maka jalur 2,4 Ghz ini tidak terlindungi secara hukum yang ironisnya justru banyak digunakan oleh banyak perusahaan untuk komunikasi perusahaan tersebut. Karena tidak terlindungi hukum maka jalur 2,4 Ghz ini pun tidak di dukung standarisasi keamanan seperti misalnya pada frekuensi 800/900/1800 Mhz (telepon genggam) sehingga hal ini menjadi celah keamanan yang empuk bagi para *hacker* untuk menyusup dan mencuri pada jaringan yang dituju.

Dalam tugas akhir ini, analisis pada sistem keamanan jaringan *wrielessLAN* dilakukan dengan menggunakan metode *wardriving.* Kegiatan *wardriving* sendiri merupakan kegiatan *scanning*. *Wardriving* dilakukan dengan menggunakan *laptop/notebook* yang dilengkapi dengan *wireless* NIC dengan mode *promiscuous* untuk menyadap sinyal *wirelessLAN*. Selanjutnya dengan menggunakan *tools* tertentu dapat tersambung ke jaringan *wirelessLAN* yang tidak diproteksi untuk menyusup kedalam jaringan tersebut untuk mencuri rahasia perusahaan tertentu karena jaringan nirkabel juga digunakan oleh perusahaan-perusahaan dalam menjalin komunikasi internal perusahaan tersebut atau untuk mendapatkan (“mencuri”) akses internet secara *anonymous.*

Hal yang diharapkan dalam tugas akhir ini adalah untuk mengetahui apakah sistem keamanan pada jaringan nirkabel yang ada pada saat ini dapat melindungi diri dari serangan penyusupan tersebut.

Kata kunci : *wardriving*, jaringan nirkabel, mode *promiscous*(*monitor),* sistem keamanan