BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi nirkabel merupakan salah satu keutamaan sebagai faktor penunjang dunia informasi. informasi di dunia jaringan tidak semua terbuka untuk umum. Karena jaringan nirkabel yang bersifat terbuka diperlukan keamanan yang terjamin. Namun, disisi lain tetap saja ada pihak-pihak yang berusaha untuk menembus sistem internal pada jaringan nirkabel itu. Salah satu sisi untuk membuat jaringan itu menjadi aman yaitu menggunakan *firewall.*

Fakultas kedokteran Unsri kampus madang menyediakan jaringan nirkabel *(WiFi)* untuk karyawan, mahasiswa, tamu dan lainnya. Terlebih lagi jaringan yang disediakan adalah terbuka untuk umum. Jaringan yang terbuka memiliki banyak sekali kekurangan sehingga menyebabkan keamanan pengguna serta ketahanan perangkat penyedia dalam penggunaannya sering kali menjadi masalah. Sehingga dengan berbagai macam sifat pengguna dalam menggunakan jaringan terbuka dapat dipelajari untuk membaca kebiasaan hingga membantu pengguna lain dalam mengamankan datanya.

Meskipun disediakannya sebuah fasilitas yang berupa perangkat yang melindungi dalam jaringan kampus tersebut, penulis akan melakukan ujicoba pada jaringan tersebut apakah benar perangkat pelindung yang tersedia itu dapat melindungi secara *high priority* atau tidak sama sekali. Dilihat dari hasil analisa dan bukti dari hasil percobaan pada jaringan apakah paket data yang dilewati itu apakah akan dianggap sebagai penyusup atau bukan, jika pedeteksian anomali pola paket tersebut dapat dibaca oleh mesin pengaman tersebut maka, akan di di arahkan degan *rules* yang sudah otomatis diatur oleh mesin *firewall* itu.

Pada saat ini sudah banyak persaingan dari *vendor* untuk membuat dan mengembangkan *firewall* baik berupa *hardware* ataupun *software* yang bersifat *realtime* aktif sehingga dapat melakukan tugas untuk melindungi jaringan itu dari serangan ketika terdeteksi, dengan menutupi celah-celah seperti *port* atau mem-filter beberapa *Internet Protocol (IP). Firewall* seperti ini pada umumnya disebut sebagai *Intrusion Prevention System (IPS).* IPS merupakan suatu metode yang digunakan untuk mencegah aktifitas dan percobaan penyusup. Fungsi IPS ada 2 dalam kemapuan mendeteksi penyusupan dan kemampuan mencegah akses penyusupan. Kemampuan inilah yang disebut *Interusion Detection System (IDS).*

Pada tugas akhir ini akan dilakukan ujicoba terhadap sistem jaringan nirkabel pada Fakultas Kedokteran Universitas Sriwijaya Kampus Madang, apakah mampu atau tidaknya untuk masalah keamanan jaringan tersebut. Sistem ujicoba tersebut akan dilakukan dengan metode *information gathering*, dimana tahapan ujicoba tersebut menggunakan *tools-tools* apakah akan berhasil atau tidak.

1.2 Perumusan Masalah

Rumusan masalah yang diangkat pada skripsi ini yaitu *information gathering* terhadap objek yang diteliti, bagaimana serangan dan penyusupan pada suatu sistem dapat dilakukan sedini mungkin. Dan apakah segi keamanan yang tersedia dapat melakukan pendeteksian serangan terhadap jaringan *wireless* pada kampus tersebut. Apa yang akan dilakukan oleh mesin yang mengamankan itu dan bagaimana sistem kerjanya itu sendiri.

1.3 Tujuan Penelitian

Penulis memiliki tujuan penelitian sebagai berikut :

a. Mengidetifikasi kerentanan untuk mengurangi resiko serangan
b. Mengukur efektifitas tingkat keamanan terhadap jaringan nirkabel

c. Membuat laporan hasil data yang bisa berguna bagi administrator dalam mengatur keamanan jaringan nirkabel
d. Memotivasi administrator untuk bisa mencari hal-hal baru agar berguna bagi banyak orang
e. Metode ,*penetrasi* akan menggunakan metode *information gathering*

1.4 Ruang Lingkup dan Batasan Masalah

Pada ujicoba ini digunakan batasan – batasan sebagai berikut :

a. Ujicoba yang dilakukan bertahap
b. Tingkat pertahanan *firewall* berdasarkan laporan data serangan
c. Fokus permasalahan hanya pada pengujian pencarian informasi dengan memberikan serangan *Low Attack*
d. Menggunakan sistem operasi Windows dan Kali Linux

1.5 Manfaat Penelitian

Pada penelitian ini diharapkan dapat memberikan manfaat :

a. Meningkatkan efesiensi penggunaan jaringan *wireless*
b. Membantu administrator dalam meningkatkan kualitas jaringan *wireless*
c. Meningkatkan konsep pengaturan *firewall* dan mengkonfigurasinya lagi