BAB 1

PENDAHULUAN

1.1 Latar Belakang Masalah

Faktor keamanan merupakan suatu hal yang mutlak dalam membangun suatu jaringan. Pada dasarnya sistem keamanan yang dimiliki oleh sistem operasi tidaklah cukup untuk mengamankan suatu jaringan computer, maka pengamanan yang berlapis-lapis pada suatu jaringan komputer perlu dilakukan, seperti firewall yang berfungsi mengatur TCP/IP dan port-port yang mana diizinkan atau tidak untuk melewati jaringan. Keamanan yang terdapat di sistem operasi juga berfungsi untuk menghalangi dan memperlambat suatu serangan untuk mendapatkan akses layaknya sebagai super user (Dony Ariyus,2006).

Untuk mengatasi masalah tersebut dibutuhkan suatu tool yang mampu mendeteksi lebih awal terjadinya intruder atau kegiatan yang merugikan suatu jaringan. Intrusion Detection System merupakan suatu solusi yang sangat tepat untuk keperluan tersebut. Salah satu IDS (Intrusion Detection System) yang sangat populer dalam keamanan IT adalah Snort. Snort dibuat dan dikembangkan pertama kali oleh Martin Roesh pada bulan November 1998, lalu menjadi sebuah open source project. Bahkan di situs resminya www.snort.org mereka berani mengklaim sebagai standar "intrusion detection/prevention".Snort

merupakan IDS yang sangat populer dan cukup ampuh digunakan para hacker dan admin di seluruh dunia.

Hal inilah yang melatar belakangi penulis untuk mendesain dan mengimplementasikan suatu sistem deteksi penyusupan jaringan yang memiliki kemampuan untuk mendeteksi adanya aktivitas jaringan yang mencurigakan.

1.2 TUJUAN PENELITIAN

Adapun tujuan dari penelitian dalam pembangunan sistem ini adalah sebagai berikut :

1. Membangun sistem keamanan jaringan yang handal berbasis IDS dengan menggunakan SNORT.
2. Memonitor serangan yang terjadi didalam jaringan sehingga dapat melakukan pendeteksian.

1.3 Batasan Masalah

Dari sekian banyak permasalahan yang telah dirumuskan, maka agar penelitian ini lebih fokus, penelitian ini dibatasi pada :

1. Sensor IDS dapat mendeteksi upaya *port scanning* menggunakan nmap
2. Aplikasi IDS berjalan pada sistem operasi Linux CentOS.
3. Pengujian sistem menggunakan nmap untuk *scanning port*
4. Hanya terbatas pada jaringan lokal.