BAB V

PENUTUP

5.1 Kesimpulan

Dari hasil penelitian yang dilakukan dengan tema Analisis dan Perancangan Keamanan Jaringan menggunakan *Intrusion Detection System* dan *Firewall* Pada Routerboard Mikrotik RB951Ui-2HnD Berbasis SMS *Gateway* berjalan sesuai seperti yang ada di perencanaan dan rancangan, sehingga didapat beberapa kesimpulan sebagai berikut :

1. Dengan mengimpelentasikan *Intrusion Detection System* dengan penambahan konfigurasi *Network Time Protocol, Scheduler,* serta *Script* dapat melakuakan *quick respon* terhadap adanya serangan di jaringan
2. Memanfaatkan *tool* sms yang ada pada Routerboard RB951Ui-2HnD dapat memberikan informasi secara *real time* pada *mobile* administrator.
3. Pada hasil *test intrusion detection system* menggunakan routerboard RB951Ui-2HnD dapat mendeteksi serangan berupa *ICMP Flood, SSH Bruteforce, FTP Bruteforce, Port Scanning* dan melakukan *packet drop* terhadap *ip address* pelaku.
4. Serangan berupa *ICMP Flood, SSH Bruteforce, FTP Bruteforce, Port Scanning* dapat tercatat di sistem *log* routerboard RB951Ui-2HnD.
5. Pada Pengamatan respon time system dan respon time sms gateway dari masing-masing serangan tersebut memiliki rata-rata respon sebagai berikut:

Tabel 5.1 Respon Time

No.	Jenis Serangan	Respon Time System	Respon Time SMS Gateway
1.	ICMP Flood	±00:01:58	±00:02:00
2.	SSH Bruteforce	±00:02:41	±00:02:46
3.	FTP Bruteforce	±00:02:43	±00:02:45
4.	Port Scanning	±00:02:43	±00:02:45

5.2 Saran

Tahapan saran merupakan evaluasi hasil dari penelitian yang dilakukan, sehingga dari penelitian yang dilakukan pada saat ini kedepannya dapat dilanjutkan untuk pengembangan sistem keamanan, beberapa saran yang bisa dikembangkan kedepanya sebagai berikut :

1. *Intrusion Detection System* menggunakan Routerboard RB951Ui-2HnD dapat dikembangkan dengan menambahkan *rule firewall* yang dapat menghalau serangan pada jaringan
2. Pemisahan sms gateway pada perangkat yang berbeda akan membantu meringankan kinerja dari Routerboard RB951Ui-2HnD melihat dari pengembangan jaringan tersebut.
3. Penambahan fitur sistem keamanan yang dipadukan dengan *intrusion detection system*, mengingat keamanan jaringan tidak dapat mengahalau serangan dengan satu sistem.
4. Pengembangan *Intrusion Detection System* dapat dikembangkan menjadi IPS *Intrusion Prevention System*.