BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan yang dapat diambil dari penelitian Analisis dan Perancangan *Intrusion Detection System* Menggunakan Mikrotik Berbasis SMS Gateway dan Mail Report (Studi Kasus: Undukunduk.net Wireless Internet Service) adalah sebagai berikut :

1. Administrator dapat melakukan quick respon terhadap adanya serangan jaringan berupa serangan *FTP Bruteforce, SSH Bruteforce, Port Scanning* dan *ICMP Flood (ping of death)* dengan memantau log ketika serangan terjadi.
2. Administrator dapat mengetahui jenis serangan *FTP Bruteforce, SSH Bruteforce, Port Scanning* dan *ICMP Flood (ping of death)* yang terjadi pada jaringan dengan memlihat setiap email dan sms yang dikirim sebagai respon sistem terhadap adanya serangan.
3. Dengan adanya laporan mingguan administrator dapat mengetahui *IP address* penyerang *FTP Bruteforce, SSH Bruteforce, Port Scanning* dan *ICMP Flood (ping of death)* selama satu minggu terakhir yang dikirim .

4. Seluruh kendali *IDS* dapat dilakukan secara terpusat.
5. Pada *fungsional test intrusion detection system* menggunakan mikrotik versi 5.20 dapat mendeteksi adanya serangan baik berupa *FTP Bruteforce, SSH Bruteforce, Port Scanning* dan *ICMP Flood (ping of death)* dan menghalau serangan tersebut serta melakukan respon dengan mengirimkan email dan sms.
6. Berdasarkan pengujian yang telah dilakukan, *intrusion detection system* menggunakan mikrotik versi 5.20 yang telah dibangun adalah jenis *interval based (batch mode)* dimana Informasi dikumpulkan terlebih dahulu dan kemudian dievaluasi menurut interval waktu yang telah ditentukan atau dengan jenis *realtime* dimana informasi dapat langsung dikirim.
7. Berdasarkan percobaan yang telah dilakukan dengan melakukan serangan secara berurutan *(Sekuensial)* dan Serentak *(simultan) respon time* sistem yang dihasilkan adalah tidak tentu *(fluktuasi)*.

5.2 Saran

Dari perancangan *intrusion detection system* menggunakan mikrotik versi 5.20 ini, Ada beberapa saran yang dapat dikembangkan untuk penelitian selanjutnya. Adapun sebagai berikut :

1. *Intrusion detection system* menggunakan mikrotik versi 5.20 ini dikembangkan menjadi *Anomaly Detection System*.
2. *Intrusion detection system* menggunakan mikrotik versi 5.20 ini akan lebih baik dikembangkan mengggunakan *Application Programmable*

Interface(API) untuk membuat perangkat lunak yang dapat dimodifikasi untuk berkomunikasi dengan *RouterOS* untuk mengumpulkan informasi.

3. Dikembangkan dengan menambah fitur update otomatis.
4. Pengujian serangan dapat lebih bervariasi.
5. Dapat dikembangkan ke *Intrusion Prevention System* (IPS).