

## BAB V

### PENUTUP

#### 5.1 Kesimpulan

Kesimpulan yang dapat diambil dari penelitian ini adalah:

1. Menerapkan metode NDLC (*anaylis, design, simulation prototyping, implementasi, monitoring dan management*). dapat memudahkan dalam membangun dan mengembangkan keamanan yang ada pada jaringan berbasis *Intrusion Detection System* dan *Firewall* secara terstruktur.
2. Administrator dapat melakukan *quick respon* terhadap adanya serangan jaringan berupa *FTP Bruteforce, SSH Bruteforce, ICMP Flood* dan *Port Scanning* dengan cara memantau *log* ketika serangan terjadi.
3. Administrator dapat mengetahui jenis serangan *FTP Bruteforce, SSH Bruteforce, ICMP Flood* dan *Port Scanning* yang terjadi pada jaringan dengan melihat setiap *e-mail* yang dikirim sebagai *Respon System* terhadap adanya serangan.
4. Pada *functional Test IDS* menggunakan Mikrotik RB-941-2nD dapat mendeteksi adanya serangan baik berupa *FTP Bruteforce, SSH Bruteforce, ICMP Flood* dan *Port Scannin* dan menghalau serangan tersebut serta melakukan *respon* dengan mengirimkan *alert* kepada administrator melalui Aplikasi *E-mail*.

5. Berdasarkan percobaan yang telah dilakukan dengan serangan secara berurutan (*Sekuensial*) dan bersamaan (*Simultan*) respon time yang dihasilkan adalah tidak menentu (*Fluktuasi*).
6. Seluruh kendali *Intrusion Detection System* dapat dilakukan secara terpusat.
7. Berdasarkan pengujian yang telah dilakukan, IDS menggunakan Mikrotik RB-941-2nD yang telah dibangun adalah *Interval Based (batch mode)*, dimana informasi dikumpulkan terlebih dahulu dan kemudian dievaluasi menurut interval waktu yang telah ditentukan atau jenis *realtime* dimana informasi dapat langsung dikirim.

## 5.2 Saran

Berdasarkan dari perancangan *intrusion Detection System* dengan menggunakan Mikrotik RB-941-2nD, ada beberapa saran yang dapat dikembangkan untuk penelitian selanjutnya, sebagai berikut:

1. *Intrusion Detection System* menggunakan Mikrotik RB-941-2nD ini dapat dikembangkan menjadi *Anomaly Detection System*.
2. Dikembangkan dengan menambahkan fitur update otomatis.
3. Pengujian serangan dapat bervariasi.