

## BAB V

### PENUTUP

#### 5.1 Kesimpulan

Kesimpulan yang dapat diambil dari penelitian Analisis dan Perancangan Keamanan Jaringan Menggunakan *Intrusion Detection System* dan *Firewall* di PT. Sujama Jaya Makmur adalah sebagai berikut :

1. Menerapkan metode PPDIIO (*Prepare, Plan, Design, Implementation, Operate* dan *Optimize*) dapat memudahkan dalam membangun dan mengembangkan keamanan yang ada jaringan berbasis *Intrusion Detection System* dan *Firewall* secara terstruktur.
2. Administrator dapat melakukan *quick respon* terhadap adanya serangan jaringan berupa serangan *FTP Bruteforce, SSH Bruteforce, SSH Bruteforce, ICMP Flood, dan Port Scanning* dengan 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 *Email* yang dikirim sebagai *Respon System* terhadap adanya serangan.
4. Seluruh kendali *Intrusion Detection System* dapat dilakukan secara terpusat
5. Pada *Functional Test IDS* menggunakan Mikrotik RB-941-2nD dapat mendeteksi adanya serangan baik berupa *FTP Bruteforce, SSH*

*Bruteforce*, *SSH Bruteforce*, *ICMP Flood*, dan *Port Scanning* dan menghalau serangan tersebut serta melakukan *respon* dengan mengirimkan *email* kepada admin jaringan.

6. Berdasarkan pengujian yang telah dilakukan, *IDS* menggunakan Mikrotik RB-941-2nD 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 serangan secara berurutan (*Sekvensional*) dan bersamaan (*Simultan*) *respon time* sistem yang dihasilkan adalah tidak menentu (*fluktuasi*).

## 5.2 Saran

Dari perancangan *IDS* menggunakan Mikrotik RB-941-2nD ini, 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. *Intrusion Detection System* menggunakan Mikrotik RB-941-2nD ini akan lebih baik dikembangkan menggunakan *Application Programmable Interface (API)* untuk membuat perangkat lunak yang dapat dimodifikasi untuk berkomunikasi dengan *RouterOS* untuk mengumpulkan informasi ataupun memberikan notifikasi lainnya.

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

