

## **BAB V**

### **PENUTUP**

#### **5.1 Kesimpulan**

Dari penelitian dan pengujian yang telah dilakukan, dapat disimpulkan bahwa *Network Intrusion Detection System* (NIDS) menggunakan Snort mampu bekerja secara efektif memberikan peringatan terhadap serangan *TCP Port Scanning* dan *ICMP flooding*. Selain itu, sistem notifikasi menggunakan bot telegram juga terbukti dapat menerima notifikasi serangan secara *real-time*. Pada penelitian ini juga telah dibuktikan bahwa system *Iptables* yang dirancang efektif dalam pencegahan serangan *TCP Port Scanning* dan *ICMP Flooding*. Oleh karena itu, hasil dari pengujian membuktikan bahwa IDS dan IPS dapat memberi pertahanan yang kuat terhadap berbagai serangan tersebut terutama pada *ICMP Flooding*. Karena *ICMP Flooding* sekedar mengirimkan serangan berbentuk packet yang banyak dan proses penyerangan melalui protokol dan tidak masuk ke port secara langsung. IDS dan IPS adalah solusi yang efektif untuk menghadapi serangan tersebut.

#### **5.2 Saran**

Simulasi yang dilakukan hanya menggunakan serangan *TCP Port Scanning* dan *ICMP Flooding*, maka penelitian selanjutnya diharapkan dapat menggunakan serangan serangan yang lain untuk menguji IDS dan IPS.