BAB 5
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil pengujian sistem IDS Snort terhadap serangan DoS yang telah dilakukan, dapat disimpulkan sebagai berikut:

1. Penelitian ini menunjukkan bahwa penggunaan SDN dengan *Floodlight Controller* rentan terhadap serangan DoS. Serangan ini dapat menyebabkan penurunan performa jaringan dan meningkatkan risiko gangguan layanan. Identifikasi jenis-jenis serangan dan pemahaman mendalam terhadap vektor serangan merupakan langkah awal yang penting untuk meningkatkan keamanan jaringan.
2. Simulasi IDS berbasis *Snort* dalam lingkungan SDN dengan *Floodlight Controller* terbukti efektif dalam mendeteksi serangan DoS. IDS *Snort* mampu mengidentifikasi pola lalu lintas mencurigakan yang mengindikasikan adanya serangan. Integrasi antara IDS *Snort* dan *Floodlight* memungkinkan pemantauan jaringan yang lebih responsif dan proaktif terhadap potensi ancaman keamanan.
3. Sistem IDS berbasis *Snort* menunjukkan kemampuan yang baik dalam menangani kasus *true positives* dan *true negatives*. IDS *Snort* berhasil mendeteksi serangan di semua skenario, sekaligus meminimalkan kesalahan deteksi yang dapat menyebabkan alarm palsu (*true negatives*). Efektivitas ini mendukung keandalan IDS dalam memberikan perlindungan terhadap serangan DoS pada jaringan virtual.

5.2 Saran

Berdasarkan hasil penelitian ini, beberapa saran yang dapat diberikan adalah:

1. Meningkatkan kinerja sistem, kapasitas memori RAM harus ditingkatkan dari 16GB menjadi minimal 64GB, dan CPU diganti dengan prosesor *Intel Xeon* terbaru dengan minimal 16 core dan kecepatan 3.5 GHz. Peningkatan ini akan

mengurangi waktu respons dan memungkinkan pemrosesan data besar secara efisien, meningkatkan kemampuan deteksi dan respons terhadap serangan intensitas tinggi. Langkah ini mencakup evaluasi kebutuhan, pengadaan perangkat keras, dan penyesuaian konfigurasi sistem untuk kompatibilitas dan optimalisasi kinerja.

2. Lakukan monitoring dan pemeliharaan secara berkala untuk memastikan kinerja optimal sistem IDS. Pembaruan aturan deteksi secara rutin juga diperlukan untuk mengatasi ancaman baru yang muncul.
3. Lakukan pengujian sistem IDS Snort pada jaringan dengan skala yang lebih besar dan variasi jenis serangan lainnya untuk mendapatkan evaluasi yang lebih komprehensif.
4. Kembangkan sistem IDS hybrid yang menggabungkan metode deteksi berbasis tanda tangan dan anomali untuk meningkatkan akurasi dan efisiensi deteksi serangan.