BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil pengujian dan pembahasan secara keseluruhan dalam penelitian implementasi *Intrusion Prevention System* (IPS) sebagai sistem keamanan jaringan dari serangan *Bruteforce*, SQL *Injection* dan DoS dengan notifikasi Telegram, dapat diambil kesimpulan sebagai berikut:

1. Dalam penelitian ini, telah berhasil diimplementasikan dan diuji sebuah sistem keamanan jaringan dengan metode *Intrusion Prevention System* (IPS) berbasis Suricata yang mampu secara efektif mengatasi serangan jaringan tipe *Bruteforce*, SQL *Injection*, dan DoS. Berdasarkan hasil pengujian dan analisis, dapat disimpulkan bahwa sistem yang dirancang memiliki kemampuan untuk mendeteksi dan mencegah berbagai upaya serangan yang dapat merusak kerahasiaan, integritas, dan ketersediaan data layanan pada jaringan.
2. Untuk menganalisis *rules Intrusion Prevention System* (IPS) berbasis Suricata dengan efektif guna mendeteksi dan mencegah ancaman yaitu dengan melakukan analisis data dan *log* yang relevan untuk setiap jenis serangan. Selanjutnya, penting untuk memahami pola dan karakteristik unik dari tiap serangan. Buatlah *rules* khusus untuk masing-masing jenis serangan berdasarkan informasi yang telah diidentifikasi sebelumnya. Selain itu, lakukan pengujian secara berkala untuk memastikan *rules* tersebut berfungsi dengan baik dan dapat memberikan *respons* yang tepat terhadap ancaman yang muncul.
3. Hasil analisis berdasrkan evaluasi kinerja *Intrusion Prevention System* (IPS) menunjukkan bahwa terjadi penurunan penggunaan CPU dari rata-rata 15,8% menjadi 7,7%, sementara terjadi peningkatan penggunaan *memory* dari 47,8% menjadi 61,7%. Pada serangan SQL *Injection*, penggunaan CPU menurun dari rata-rata 7,1% menjadi 5,5%, sementara penggunaan *memory* tetap pada 48,4%. Namun, pada serangan DoS, terjadi penurunan penggunaan CPU yang signifikan dari rata-rata 98,7% menjadi 7,1%,

dengan penggunaan *memory* tetap stabil pada 60,8%. Meskipun terdapat perubahan penggunaan sumber daya pada beberapa serangan, Suricata berhasil mempertahankan *response time* yang baik dengan rata-rata *response time* pada 2,6 ms. Secara keseluruhan, hasil pengujian menunjukkan bahwa Suricata efektif dalam melindungi sistem dari serangan *Bruteforce*, SQL *Injection* dan DoS, meskipun perlu perhatian khusus terhadap penggunaan sumber daya pada serangan DoS untuk meningkatkan efisiensi sistem.

4. Penelitian berhasil menggunakan Telegram *bot* untuk menginformasikan *administrator* jaringan tentang ancaman serangan dengan batasan penggunaan CPU lebih dari 70%. Mekanisme ini memungkinkan *administrator* merespons dan mengambil tindakan keamanan yang tepat untuk melindungi sistem.

5.2 Saran

Dalam rangka meningkatkan kualitas skripsi ini, terdapat beberapa saran yang dapat diberikan, antara lain:

1. Pertimbangkan untuk melakukan perluasan penelitian dengan mencakup lebih banyak skenario pengujian atau jenis serangan. Selain itu, lakukan verifikasi lebih lanjut terhadap hasil yang diperoleh untuk memastikan keakuratan dan validitasnya.
2. Untuk menguji efektivitas sistem secara menyeluruh, pertimbangkan untuk mengimplementasikan dan menguji coba sistem keamanan berbasis IPS Suricata di lingkungan nyata atau jaringan produksi.
3. Evaluasi lebih lanjut mengenai kecepatan *response* sistem dalam mendeteksi dan merespons ancaman. Memastikan juga bahwa sistem mampu memberikan notifikasi secara tepat waktu kepada *administrator*.
4. Pengembangan dan penyempurnaan skrip otomatisasi. Pertimbangkan untuk terus mengembangkan dan menyempurnakan skrip-skrip ini untuk memungkinkan pengujian lebih efisien dan akurat di masa depan. Skrip yang andal dan efisien dapat menghemat waktu dan usaha dalam pengujian keamanan yang berkelanjutan.