BAB V
SIMPULAN, IMPLIKASI, DAN REKOMENDASI

5.1 Simpulan

Berdasarkan hasil penelitian yang telah dilakukan, berikut merupakan beberapa kesimpulan yang dapat penulis uraikan:

1. Implementasi sistem keamanan IPS suricata dalam penelitian ini dengan berdasarkan pada tabel 4.1 berhasil melakukan pendeteksian terhadap delapan jenis serangan secara efektif dengan nilai rata-rata waktu deteksi yang dibutuhkan kurang dari 1 detik dan serangan berhasil terdeteksi sesuai dengan *rules* yang ditentukan . Dengan hasil tingkat deteksi yang tinggi dan kemampuan untuk menganalisis pola serangan yang akurat, maka menunjukkan bahwa sistem keamanan IPS suricata ini dapat digunakan untuk menjaga lalu lintas jaringan. Dalam pengujian IPS suricata berhasil mengidentifikasi dan memberikan peringatan *(alert)* terhadap delapan serangan yang diuji yaitu ICMP *Flood*, DDoS *Attack*, *Port Scanning*, IP *Spoofing*, XSS, SQLi, *Slow HTTP*, dan *SYN Flood Attack.*
2. Kinerja suricata menunjukkan hasil yang stabil dan konsisten. Meskipun pada umumnya bahwa beban lalu lintas jaringan tentunya akan meningkat selama proses serangan berlangsung, namun sistem keamanan suricata mampu dalam memproses dan menganalisis data tanpa mengalami performa yang signifikan. Hal ini menunjukkan bahwa sistem keamanan IPS suricata cocok untuk diterapkan dalam berbagai skala jaringan, baik dalam skala jaringan kecil maupun dalam skala jaringan besar.
3. Integrasi sistem notifikasi pada penelitian ini menggunakan aplikasi telegram dan whatsapp yang terbukti pada hasil pengujian dapat meningkatkan responsivitas terhadap ancaman serangan siber. Dalam proses mendeteksi serangan pada lalu lintas jaringan, suricata juga dapat secara *real-time* mengirimkan notifikasi ke perangkat *mobile*, sehingga memungkinkan administrator untuk mengambil tindakan lebih lanjut terhadap aktivitas yang terjadi pada lalu lintas jaringan. Dengan itu

menunjukkan bahwa sistem notifikasi *real-time* menjadi komponen penting dalam menjaga jaringan secara proaktif.

5.2 Implikasi

Implikasi dari hasil penelitian ini adalah sebagai berikut:

1. Institusi atau organisasi yang mempunyai rencana dalam meningkatkan keamanan jaringan dapat mempertimbangkan untuk menggunakan sistem keamanan IPS suricata. Sistem ini tidak hanya efektif dalam mendeteksi dan memitigasi berbagai jenis serangan siber, tetapi dapat diintegrasikan dengan sistem notifikasi *real-time* melalui aplikasi komunikasi seperti telegram dan whatsapp. Sehingga memungkin administrator jaringan untuk mendapatkan peringatan dalam bentuk notifikasi ketika terjadi serangan. Dengan memanfaatkan teknologi ini, institusi dan organisasi tentunya dapat meningkatkan keamanan siber secara signifikan, dengan mengurangi resiko pencurian data, dan mencegah *downtime* yang dapat mengganggu operasional bisnis.
2. Pengembangan lebih lanjut dapat dilakukan dengan mengintegrasikan untuk mengintegrasikan suricata dengan sistem keamanan yang lebih komprehensif, seperti *firewall, System Information and Event Management* (SIEM) dan perangkat lunak pemantauan jaringan lainnya.

5.3 Rekomendasi

Berdasarkan temuan pada penelitian ini, beberapa rekomendasi yang dapat diberikan untuk penelitian dan implementasi masa depan adalah sebagai berikut:

1. Pengujian IPS suricata dapat dilakukan dengan baik jika dilakukan dalam lingkunga jaringan yang lebih kompleks, untuk mengukur performa dalam skala yang lebih besar. Pengujian juga dapat melibatkan berbagai jenis perangkat jaringan seperti topologi yang lebih kompleks, serta volume lalu lintas yang lebih tinggi untuk menilai sejauh mana kemampuan suricata dalam mempertahankan efektivitasnya ketika kondisinya lebih menantang. Akan tetapi, penting juga untuk memastikan bahwa solusi yang diusulkan dapat diandalkan di berbagai situasi dan mampu menghadapi tantangan operasional yang mungkin dihadapi oleh institusi besar.

2. Pengujian terhadap jenis serangan siber lainnya juga perlu dilakukan untuk memperluas cakupan keamanan yang dapat disediakan oleh IPS suricata. Serangan seperti *man-in-the-middle* (MITM), DNS *poisoning*, dan *malware* dapat dijadikan fokus penelitian selanjutnya. Hal tersebut dapat menjadikan sistem lebih efektif dalam melindungi jaringan dari berbagai ancaman yang semakin berkembang.