BAB V

SIMPULAN DAN SARAN

5.1 Simpulan

Penelitian ini dilakukan untuk mengkaji pendekatan deteksi serangan SSH *slow-rate* yang selama ini tidak dapat ditangani secara efektif oleh sistem keamanan berbasis aturan, dengan studi kasus pada kebutuhan keamanan server PT Maro Anugrah Jaya. Penelitian berfokus pada pengembangan dan evaluasi model deteksi intrusi berbasis *Long Short-Term Memory* (LSTM) dengan memanfaatkan log autentikasi SSH yang memiliki karakteristik temporal. Berdasarkan hasil eksperimen yang telah dilakukan, model LSTM yang dibangun mampu melakukan deteksi serangan SSH *slow-rate* dengan performa yang lebih baik dibandingkan dengan Fail2Ban sebagai sistem deteksi berbasis aturan, yang terlihat dari peningkatan signifikan pada metrik *recall* dan penurunan *false negative* dibandingkan dengan Fail2Ban, dengan metrik akurasi, presisi, dan F1-score sebagai indikator pendukung pada tahap evaluasi. Analisis performa menunjukkan bahwa model mampu mempelajari pola aktivitas anomali dari log autentikasi secara adaptif dan tidak bergantung pada frekuensi percobaan login seperti yang menjadi batasan utama Fail2Ban.

Dari hasil analisis perilaku serangan, karakteristik serangan *slow-rate* diidentifikasi sebagai aktivitas *login* ilegal yang dilakukan dengan jeda waktu panjang antar percobaan, volume serangan rendah, serta pemanfaatan banyak *port* dan *username* yang berbeda. Karakteristik tersebut berbeda dengan *brute force* cepat yang memiliki lonjakan frekuensi percobaan *login* dalam jangka waktu singkat. Pendekatan ini berhasil membedakan pola serangan halus yang sebelumnya tidak terdeteksi oleh sistem keamanan berbasis aturan.

Model deteksi intrusi yang dikembangkan diuji melalui skenario pengujian eksperimental menggunakan dataset log autentikasi SSH eksternal untuk mengevaluasi kemampuan deteksi serangan *slow-rate* dibandingkan sistem berbasis aturan. Hasil pengujian menunjukkan bahwa model dapat memberikan notifikasi serangan secara lebih proaktif dan mampu mendeteksi

serangan *slow-rate* yang sebelumnya lolos dari pemblokiran otomatis oleh Fail2Ban. Namun demikian, implementasi di lingkungan nyata juga mengungkapkan adanya peningkatan *false positive*, yaitu sejumlah kecil aktivitas *benign* yang teridentifikasi sebagai serangan. Meskipun model secara signifikan meningkatkan tingkat deteksi ancaman, dibutuhkan mekanisme penyempurnaan lebih lanjut, baik pada sisi ambang batas keyakinan prediksi maupun logika kebijakan pemblokiran untuk meminimalkan gangguan pada aktivitas pengguna yang valid. Dengan demikian, sistem deteksi berbasis pembelajaran mesin ini tetap mampu meningkatkan perlindungan terhadap serangan adaptif, namun masih memerlukan penguatan tambahan agar lebih andal dalam konteks operasional secara jangka panjang.

5.2 Saran

Berdasarkan hasil penelitian dan implementasi sistem deteksi serangan SSH, terdapat beberapa saran yang dapat menjadi acuan dan pengembangan lebih lanjut:

- Pola serangan SSH dapat berubah dari waktu ke waktu. Maka penelitian selanjutnya disarankan untuk mengembangkan model dengan kemampuan *online learning* atau *incremental retraining* agar tetap efektif dalam menghadapi serangan yang beradaptasi.
- Adanya keterbatasan variasi pola serangan *slow-rate* pada dataset sehingga perlu dilakukan eksperimen generasi data serangan atau pengumpulan dataset *real-world* yang lebih kaya.
- Penelitian ini hanya memanfaatkan log autentikasi SSH sebagai sumber deteksi. Pengembangan lanjutan dapat mempertimbangkan integrasi seperti *Netflow*, *Packed-Based Telemetry*, serta *Application-Layer Behavior*.