ABSTRAK

Ancaman terhadap serangan siber seperti Malware, Phishing, dan DDoS menjadi masalah yang serius. Serangan tersebut semakin berkembang pesat dan terus berevolusi, menciptakan varian-varian baru yang lebih kompleks dan sulit dideteksi oleh sistem keamanan. Hal ini mejadi bentuk perhatian lebih dalam mempertahankan serta mengamankan suatu sistem dengan tujuan untuk melindungi data yang dianggap vital.

Sistem pencegahan serangan siber sudah dilakukan dari waktu ke waktu seperti menggunakan sistem *Intrusion Prevention System* (IPS), namun sistem seperti ini cenderung memiliki kerentanan seperti kurangnya pencegahan dari sistem tersebut untuk memeriksa log jaringan, dengan menggunakan Machine Learning pola serangan baru dapat dipelajari, sehingga penggunaan dari IPS memiliki sistem yang lebih kuat, aspek keamanan berbasis *realtime* diperlukan untuk pengawasan, *Security Information and Event Management* (SIEM) merupakan sistem keamanan, yang dapat digunakan untuk monitoring jaringan yang disebut, penggunaan sistem ini bertujuan untuk memberikan peringatan kepada pemilik dari perangkat untuk menindaklanjuti serangan yang terjadi.

Pengujian dilakukan dengan mengukur performa deteksi menggunakan parameter seperti Accuracy, Precision, Recall, dan F1-Score. Neural Network dan XGBoost mencatat akurasi sebesar 77%, K-Means 44%, dan Naïve Bayes 33%, dengan kemampuan generalisasi yang baik terhadap serangan minoritas. Perbandingan antara sistem berbasis rules dan machine learning menunjukkan bahwa ML mampu mendeteksi serangan yang tidak terdeteksi oleh rules. Pada serangan IP Sweep, sistem *rules* tidak menghasilkan deteksi, sementara Neural Network berhasil mendeteksi 6 *flow*. Untuk Full Port Scan, Naïve Bayes mendeteksi 436 dari 3.372 *flow*. Pada serangan DoS, Neural Network mendeteksi 90.947 dari 90.982 *flow* dan Naïve Bayes 81.770 dari 93.759 *flow* pada SYN Flood; serta 45.053 dari 68.530 flow dan 47.556 dari 62.157 flow pada UDP Flood. Pada serangan FTP Brute Force (R2L), hanya *rules-based* yang berhasil mendeteksi 400 flow, sementara ML gagal. Untuk U2R Exploit, Naïve Bayes mendeteksi 10 dari 14 flow, dibandingkan hanya 1 flow oleh rules.

Kata kunci : Keamanan Siber, *Intrusion Detection System, Intrusion Prevention System, Security Information and Event Management. Machine Learning*