ABSTRAK

Semakin meningkatnya ancaman siber mengakibatkan jumlah dan kompleksitas *malicious traffic* yang terekam di *honeypot* semakin tinggi sehingga diperlukan mekanisme analisis yang dapat mengidentifikasi tingkat risiko serangan secara terukur. Penelitian ini bertujuan membangun sistem analisis dan klasifikasi risiko *malicious traffic* pada log *honeypot* menggunakan algoritma *Random Forest*. Dataset yang digunakan berasal dari log *Honeypot* yang merekam aktivitas autentikasi dan interaksi penyerang. Tahapan penelitian meliputi *preprocessing data*, *feature engineering*, pembentukan label risiko menggunakan *pseudo labeling* berdasarkan *framework MITRE ATT&CK* dan *NIST SP* 800-30, penanganan ketidakseimbangan data menggunakan *Synthetic Minority Oversampling Technique (SMOTE)*, serta evaluasi model menggunakan *Stratified* 5-*Fold Cross Validation.* Hasil penelitian menunjukkan bahwa model *Random Forest* mampu mengklasifikasikan *malicious traffic* ke dalam kategori *Low Risk* dan *High Risk* dengan nilai *accuracy* sebesar 99,40%, *precision* sebesar 95,28%, *recall* sebesar 99,02%, *F1-score* sebesar 97,12%, dan *ROC-AUC* sebesar 99,95%. Selanjutnya model diimplementasikan ke dalam dashboard berbasis web untuk menampilkan hasil analisis, klasifikasi risiko, attack indication, dan security recommendation secara interaktif. Hasil penelitian menunjukkan bahwa kombinasi log *honeypot* dan *Random Forest* efektif digunakan untuk mendukung analisis risiko ancaman siber berdasarkan karakteristik perilaku serangan.

Kata kunci: *malicious traffic, honeypot, Random Forest,* klasifikasi risiko, keamanan siber

ABSTRACT

The increasing volume and sophistication of cyber threats have resulted in a growing amount of malicious traffic recorded by honeypots, creating the need for a mechanism capable of identifying attack risk levels in a measurable manner. This study aims to develop a risk analysis and classification system for malicious traffic based on honeypot logs using the Random Forest algorithm. The dataset was obtained from honeypot logs that record authentication activities and attacker interactions. The research process consisted of data preprocessing, feature engineering, risk label generation using pseudo labeling based on the MITRE ATT&CK framework and NIST SP 800-30, data balancing using the Synthetic Minority Oversampling Technique (SMOTE), and model evaluation through Stratified 5-Fold Cross Validation. The results show that the Random Forest model successfully classified malicious traffic into Low Risk and High Risk categories, achieving an accuracy of 99,40%, precision of 95,28%, recall of 99,02%, F1-score of 97,12%, and ROC-AUC of 99,95%. The model was subsequently implemented in a web-based dashboard to provide interactive analysis results, risk classification, attack indications, and security recommendations. These findings demonstrate that the combination of honeypot logs and Random Forest is effective in supporting cyber threat risk analysis based on attack behavior characteristics.

Keywords: malicious traffic, honeypot, Random Forest, risk classification, cybersecurity