ABSTRAK

RANCANG BANGUN SISTEM DETEKSI DAN KLASIFIKASI SERANGAN JARINGAN MENGGUNAKAN ALGORITMA RANDOM FOREST BERDASARKAN DATA IDS DAN HONEYPOT PADA SECURITY OPERATIONS CENTER (SOC)

(Yehaezkiel Ellzer Manoppo, 2026: 118)

Perkembangan jaringan komputer di berbagai lingkungan organisasi meningkatkan risiko terjadinya serangan siber yang dapat mengganggu ketersediaan layanan, mencuri data, dan merusak integritas sistem. Proses pemantauan keamanan jaringan yang masih dilakukan secara manual membuat administrator kesulitan dalam mengenali jenis serangan secara cepat dan terstruktur. Penelitian ini bertujuan untuk merancang dan membangun sistem deteksi dan klasifikasi serangan jaringan menggunakan algoritma *Random Forest* berdasarkan data dari *Intrusion Detection System* (IDS) dan *Honeypot* pada *Security Operations Center* (SOC). Sistem dibangun menggunakan Snort IDS sebagai pendeteksi *traffic* mencurigakan, Cowrie Honeypot sebagai perangkap penyerang, TShark untuk menangkap *traffic* jaringan, CICFlowMeter untuk mengubah *packet capture* menjadi dataset berbasis *flow*, Python 3 dan *Scikit-learn* untuk pelatihan model *Random Forest*, MariaDB sebagai basis data, serta Flask sebagai *web dashboard* dan Telegram sebagai media notifikasi. Hasil penelitian menunjukkan bahwa sistem yang dibangun mampu mengumpulkan log dari IDS dan honeypot, memproses data serangan, mengklasifikasikan jenis serangan jaringan, menyimpan hasil klasifikasi ke dalam database, serta menampilkan informasi monitoring secara real-time melalui *dashboard* dan Telegram alert. Dengan demikian, sistem ini dapat membantu administrator dalam melakukan pemantauan keamanan jaringan secara lebih cepat, terpusat, dan efisien.

Kata kunci: deteksi serangan jaringan, Random Forest, IDS, honeypot, SOC, klasifikasi serangan

ABSTRACT

DESIGN AND DEVELOPMENT OF A NETWORK ATTACK DETECTION AND CLASSIFICATION SYSTEM USING THE RANDOM FOREST ALGORITHM BASED IDS AND HONEYPOT DATA IN A SECURITY OPERATIONS CENTER (SOC)

(Yehaezkiel Ellzer Manoppo, 2026: 118)

The growth of computer networks in organizational environments has increased the risk of cyberattacks that may disrupt service availability, compromise data, and damage system integrity. Manual network security monitoring makes it difficult for administrators to identify attack types quickly and systematically. This final project aims to design and build a network attack detection and classification system using the Random Forest algorithm based on data collected from an Intrusion Detection System (IDS) and a Honeypot within a Security Operations Center (SOC). The system is developed using Snort IDS to detect suspicious traffic, Cowrie Honeypot to capture attacker activities, TShark to capture network traffic, CICFlowMeter to convert packet captures into flow-based datasets, Python 3 and Scikit-learn to train the Random Forest model, MariaDB as the database, and Flask as the web dashboard, with Telegram used for alert notifications. The results show that the system is able to collect IDS and honeypot logs, process attack data, classify network attack types, store classification results in the database, and display monitoring information in real time through the dashboard and Telegram alerts. Therefore, the proposed system can assist administrators in monitoring network security more quickly, centrally, and efficiently.

Keywords: Network Attack Detection, Random Forest, Intrusion Detection System, Honeypot, Security Operations Center, Attack Classification