ABSTRAK

RANCANG BANGUN *INTRUSION DETECTION SYSTEM* (IDS) UNTUK DETEKSI SERANGAN MALWARE BERBASIS *SNORT* DAN NOTIFIKASI TELEGRAM
(2025 : xiv + 72 HALAMAN + 44 GAMBAR + 2 TABEL + LAMPIRAN)

ERIK MARDIYAH NINGSIH
062230330728
JURUSAN TEKNIK ELEKTRO
PROGRAM STUDI D3 TEKNIK TELEKOMUNIKASI
POLITEKNIK NEGERI SRIWIJAYA

Perkembangan teknologi informasi telah membawa dampak signifikan terhadap keamanan jaringan komputer, terutama terkait ancaman malware yang semakin kompleks dan sulit dideteksi oleh sistem konvensional. Dalam laporan ini, dirancang dan dibangun sebuah sistem *Intrusion Detection System* (IDS) berbasis aplikasi *Snort* yang diintegrasikan dengan perangkat MikroTik sebagai router dan aplikasi Telegram sebagai media notifikasi. Sistem ini dirancang untuk mendeteksi berbagai jenis aktivitas mencurigakan seperti serangan ICMP *real-time*, ICMP *Flood*, pengiriman *file .exe*, *signature hex*, hingga pola konten Malware lainnya. Sistem diuji dengan berbagai simulasi serangan menggunakan *Kali Linux* dan menghasilkan deteksi *real-time* yang langsung dikirim sebagai peringatan ke Telegram, sekaligus melakukan pemblokiran otomatis terhadap IP sumber serangan. Hasil pengujian menunjukkan bahwa sistem IDS yang dibangun mampu bekerja secara responsif dan efektif dalam mendeteksi serta mencegah serangan malware. Sistem ini juga memberikan solusi keamanan jaringan yang adaptif, dengan fleksibilitas pengembangan *rule* tambahan untuk menghadapi ancaman baru di masa depan.

Kata Kunci: *Intrusion Detection System*, *Snort*, Malware, Telegram, Keamanan Jaringan.

ABSTRACT

DESIGN AND DEVELOPMENT OF AN INTRUSION DETECTION SYSTEM (IDS) FOR MALWARE ATTACK DETECTION BASED ON SNORT AND TELEGRAM NOTIFICATIONS
(2025: xiv + 72 PAGES + 44 FIGURES + 2 TABLES + APPENDICES)

ERIK MARDIYAH NINGSIH
062230330728
JURUSAN TEKNIK ELEKTRO
PROGRAM STUDI D3 TEKNIK TELEKOMUNIKASI
POLITEKNIK NEGERI SRIWIJAYA

The advancement of information technology has significantly impacted computer network security, especially concerning increasingly complex malware threats that are difficult to detect using conventional systems. This report presents the design and development of an Intrusion Detection System (IDS) based on the Snort application, integrated with a MikroTik device as the router and Telegram as the notification platform. The system is designed to detect various types of suspicious activities such as real-time ICMP attacks, ICMP Floods, .exe file transfers, hexadecimal signatures, and other malware content patterns. The system was tested through multiple simulated attacks using Kali Linux and demonstrated real-time detection with immediate alerts sent to Telegram, along with automatic blocking of the attacker's IP address. The test results show that the implemented IDS is capable of operating responsively and effectively in detecting and preventing malware attacks. This system also offers an adaptive network security solution, with the flexibility to expand detection rules to address future threats.

Keywords*: Intrusion Detection System, Snort, Malware, Telegram, Network Security.*