RANCANG BANGUN *INTRUSION DETECTION SYSTEM* (IDS) UNTUK DETEKSI SERANGAN MALWARE BERBASIS *SNORT* DAN NOTIFIKASI TELEGRAM

LAPORAN AKHIR

Disusun Untuk Memenuhi Persyaratan Menyelesaikan Pendidikan Diploma III Jurusan Teknik Elektro Program Studi DIII Teknik Telekomunikasi

Oleh :
ERIK MARDIYAH NINGSIH
062230330728

POLITEKNIK NEGERI SRIWIJAYA

PALEMBANG

2025

LEMBAR PENGESAHAN

RANCANG BANGUN *INTRUSION DETECTION SYSTEM* (IDS) UNTUK DETEKSI SERANGAN MALWARE BERBASIS *SNORT* DAN NOTIFIKASI TELEGRAM

Oleh:
ERIK MARDIYAN NINGSIH
0622030730728

Menyetujui,

Pembimbing I

M. Zakuan Arifin, S.T., M. Kom
NIP. 196904291993031004

Pembimbing II

Ir. Suzan Zefi, S.T., M. Kom
NIP. 197709252005012003

Mengetahui,

Ketua Jurusan Teknik Elektro

Dr. Ir. Selamat Muslimin, S.T., M.Kom., IPM
NIP. 197907222008011007

Koordinator Program Studi
DIII Teknik Telekomunikasi

Ir. Suzan Zefi, S.T., M.Kom
NIP. 197709252005012003

SURAT PERNYATAAN

Surat yang bertanda tangan di bawah ini menyatakan:

Nama	: Erik Mardiyah Ningsih
Jenis Kelamin	: Perempuan
Tempat, Tanggal Lahir	: Banyuasin, 14 Juni 2003
Alamat	: Sido Mulyo
NIM	: 062230330728
Program Studi	: DIII Teknik Telekomunikasi
Judul Skripsi/Laporan Akhir	: Rancang Bangun *Intrusion Detection System* (IDS) untuk Deteksi Serangan Malware Berbasis *Snort* dan Notifikasi Telegram

Menyatakan dengan sesungguhnya bahwa:

1. Skripsi/Laporan Akhir ini adalah hasil karya saya sendiri bebas dari tindakan plagiasi dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.
2. Dapat menyelesaikan segala urusan terkait pengumpulan revisi Skripsi/Laporan Akhir yang sudah disetujui oleh dewan penguji paling lama 1 bulan setelah ujian Skripsi/Laporan Akhir.
3. Dapat menyelesaikan segala urusan peminjaman/penggantian alat/buku dan lainnya paling lama 1 bulan setelah ujian Skripsi/Laporan Akhir.

Apabila kemudian hari diketahui ada pernyataan yang terbukti tidak benar dan tidak dapat dipenuhi, maka saya siap bertanggung jawab dan menerima sanksi tidak diikutsertakan dalam prosesi wisuda serta dimasukkan dalam daftar hitam oleh jurusan Teknik Elektro sehingga berdampak tertundanya pengambilan Ijazah dan Transkrip (ASLI & COPY). Demikian Surat pernyataan ini dibuat dengan sebenar-benarnya dan dalam keadaan sadar tanpa paksaan.

Palembang, Agustus 2025
Yang Menyatakan

Erik Mardiyah Ningsih
NIM. 062230330728

MOTTO

“Fa-inna ma'al 'usri yusrā. Inna ma'al 'usri yusrā”

(QS. Al-Insyirah: 5–6)

PERSEMBAHAN

Karya tulis ini merupakan bentuk rasa syukur saya kepada Tuhan Yang Maha Esa karena telah memberikan nikmat dan karunia pertolongan yang tiada henti hingga saat ini

- Kupersembahkan sebuah karya kecil ini untuk Almarhum Ayahanda dan Ibunda tercinta, yang selama ini senantiasa mendoakan, memberikan semangat, nasehat, kasih sayang, juga dukungan sepenuh hati dan pengorbanan yang tak tergantikan.
- Dosen pembimbingku, Bapak M. Zakuan Agung, S.T., M.Kom. dan Ibu Ir. Suzan Zefi, S.T., M.Kom. Terima kasih atas bimbingan dan ilmu yang telah bapak dan ibu berikan dalam menyelesaikan Laporan Akhir ini dan selalu meluangkan waktu disela kesibukan Bapak dan Ibu.
- Karya ini juga saya persembahkan kepada seluruh keluarga tercinta yaitu Kakak, Keponakan, Sepupu, Paman dan Bibi yang selalu menjadi sumber motivasi terbaik, selalu memberikan semangat dan dukungan baik moral maupun material.
- Terakhir, terima kasih kepada diri sendiri dan M. Agung Ade Anugerah, terima kasih karena telah mampu berkarya keras dan bertahan sejauh ini, mampu mengendalikan diri dari berbagai tekanan diluar keadaan, dan tetap berhasil bermuara di bundar doa untuk sama-sama menyelesaikan Laporan Akhir.

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.*

KATA PENGANTAR

Puji syukur Penulis panjatkan atas kehadirat Allah SWT, yang telah memberikan rahmat serta karunia-Nya sehingga penulis dapat menyelesaikan Laporan Akhir yang berjudul **"Rancang Bangun *Intrusion Detection System* (IDS) untuk Deteksi Serangan Malware Berbasis *Snort* dan Notifikasi Telegram"**.

Penyusunan Laporan Akhir ini merupakan syarat wajib bagi Mahasiswa DIII Teknik Telekomunikasi serta sebagai wujud pertanggungjawaban Penulis atas sebuah tugas akhir yang telah dikerjakan dalam menggali dan mendapatkan ilmu serta mengasah kemampuan *softskill* maupun *hardskill* mahasiswa.

Pada pelaksanaan penyusunan Laporan Akhir, terdapat banyak kesulitan yang Penulis hadapi, namun pembuatan proposal ini dapat berjalan lancar dengan semestinya tidak terlepas dari dukungan segenap pihak yang telah memberikan bantuan kepada Penulis baik secara dukungan moral maupun material. Oleh karena itu, dalam kesempatan ini Penulis menyampaikan terima kasih kepada :

1. Allah SWT yang telah memberikan rahmat yang sangat luar biasa kepada Penulis sehingga Laporan Akhir ini dapat terselesaikan.
2. Bapak Ir. Irawan Rusnadi, M.T., selaku Direktur Politeknik Negeri Sriwijaya.
3. Bapak Dr. Ir. Selamat Muslimin, S.T., M.Kom., IPM., selaku Ketua Jurusan Teknik Elektro Politeknik Negeri Sriwijaya.
4. Ibu Lindawati, S.T., M.T.I., selaku Sekretaris Jurusan Teknik Elektro Politeknik Negeri Sriwijaya.
5. Ibu Ir. Suzan Zefi, S.T.,M.Kom., selaku Ketua Program Studi DIII Teknik Telekomunikasi Politeknik Negeri Sriwijaya.
6. Bapak M. Zakuan Agung, S.T., M. Kom, selaku Dosen Pembimbing I yang telah memberikan arahan, petunjuk dan bimbingan kepada Penulis dalam penyusunan dan pengerjaan Laporan Akhir ini.

7. Ibu Ir. Suzan Zefi, S.T., M. Kom, selaku Dosen Pembimbing II yang telah memberikan arahan, petunjuk dan bimbingan kepada Penulis dalam penyusunan dan pengerjaan Laporan Akhir ini.
8. Bapak Achmad Aflah Jamazy, S.Tr., selaku Dosen Teknisi yang membantu dalam penyelesaian Laporan Akhir ini.
9. Bapak/Ibu Dosen Program Studi DIII Teknik Telekomunikasi Politeknik Negeri Sriwijaya.
10. Kedua Orang Tua, Kakak, serta seluruh Keluarga Besar penulis yang senantiasa memberikan do'a dan dukungan yang tiada henti dalam proses penyelesaian laporan ini.
11. Rekan-rekan satu bimbingan, kelas TB PRIDE 2022, sahabat 'hasil seleksi alam' (Puput, Indu, Ojan, Lilis, Ditak, Indah), sahabat 'rempong girl' (Bitak, Aul, Inces, Cin, Puti) sahabat serta rekan kamar kost, rekan ambis (Cintya), Ibu kost yang selalu pengertian dan baik sekali (Bu Jamilah) dan semua pihak yang telah membantu dalam penyelesaian Laporan Akhir ini.
12. M. Agung Ade Anugerah yang selalu ada dalam membantu, memberikan do'a dan dukungan yang tiada henti dalam penyelesaian Laporan Akhir ini.

Dalam penyusunan Laporan Akhir ini Penulis menyadari bahwa masih banyak kekurangan. Maka dari itu, Penulis mengharapkan kritik dan saran yang bersifat membangun guna perbaikan dimasa mendatang.

Palembang, Juli 2025

Erik Mardiyah Ningsih

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN