

**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**

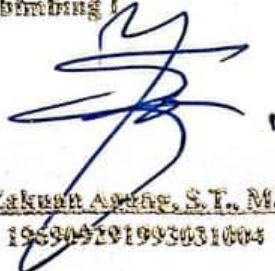


Oleh:

ERIK MARDIYAH NINGSIH
062210330725

Menyetujui,

Pembimbing I


M. Zakwan Arif, S.T., M. Kom
NIP. 196909291993031004

Pembimbing II


Ir. Suzan Zeti, 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 Zeti, 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 sebenarnya 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 kehadiran 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

HALAMAN JUDUL	i
LEMBAR PENGESAHAN	ii
SURAT PERNYATAAN	iii
MOTTO	iv
ABSTRAK	v
ABSTRACT	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	ix
DAFTAR GAMBAR.....	xi
DAFTAR TABEL	xiii
DAFTAR LAMPIRAN	xiv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah.....	3
1.4 Tujuan.....	3
1.5 Manfaat.....	4
1.6 Metode Penulisan	4
1.7 Sistematika Penulisan.....	5
BAB II TINJAUAN PUSTAKA.....	6
2.1 Keamanan Jaringan	6
2.2 <i>Packet Internet Gopher</i> (Ping)	7
2.3 <i>File Transfer Protocol</i> (FTP)	7
2.4 MikroTik	8
2.5 Aplikasi Winbox	9
2.6 Ubuntu	10
2.7 <i>Kali Linux</i> (Kali OS)	12
2.7.1 Pengertian <i>Kali Linux</i>	12
2.7.2 Sejarah <i>Kali OS</i>	13
2.7.3 Kelebihan dan Kekurangan <i>Kali OS</i>	13
2.7.4 Jenis-Jenis <i>Kali OS</i>	14
2.8 <i>VMware</i>	15
2.8.1 Pengertian <i>VMware</i>	15
2.8.2 Sejarah <i>VMware</i>	16
2.8.3 Komponen <i>VMware</i>	16
2.8.4 Manfaat Penggunaan <i>Vmware</i>	17
2.9 Aplikasi Telegram	17
2.10 <i>Firewall</i>	21
2.10.1 Pengertian <i>Firewall</i>	21
2.10.2 Fungsi <i>Firewall</i>	22
2.10.3 Cara kerja <i>Firewall</i>	23
2.10.4 Jenis-Jenis <i>Firewall</i>	23
2.11 <i>Intrusion Detection System</i> (IDS).....	24
2.11.1 Pengertian IDS	24

2.11.2	Arsitektur IDS	25
2.11.3	Sifat-Sifat IDS	26
2.11.4	Teknik Pada IDS	27
2.11.5	Cara Kerja IDS	28
2.11.6	Jenis-Jenis IDS	29
2.11.7	Kelebihan dan Kelemahan IDS	30
2.12	<i>Snort</i>	32
2.13	<i>Malicious Software</i> (Malware)	33
2.13.1	Pengertian Malware	33
2.13.2	Jenis-Jenis Malware	33
2.13.3	Model Analisa <i>Malware</i>	34
2.13.4	Pola Serangan Malware	36
2.14	<i>Flowchart</i>	37
2.15	Tabel Penelitian Sebelumnya	39
BAB III RANCANG BANGUN PERANGKAT		41
3.1.	Perancangan Perangkat	41
3.2.	Langkah-Langkah Perancangan Perangkat	42
3.2.1	<i>Flowchart</i>	42
3.2.2	Blok Diagram	43
3.2.3	Topologi Jaringan	44
3.3.	Prinsip Kerja	44
3.4.	Konfigurasi Mikrotik	45
3.4.1	Konfigurasi Dasar Mikrotik	45
3.4.2	Konfigurasi Mikrotik sebagai <i>Access Point</i>	49
3.5.	Instalasi dan Konfigurasi <i>Snort</i> sebagai IDS	52
3.6.	Instalasi <i>Kali Linux</i> untuk Simulasi Serangan Malware	57
BAB IV HASIL DAN PEMBAHASAN		59
4.1	Pengujian Perangkat	59
4.2	Tujuan Pengujian Perangkat	59
4.3	Alat dan Bahan Pengambilan Data	60
4.4	Prosedur Pengujian Perangkat	60
4.5	Data Hasil Pengujian	62
4.5.1	Pengujian Deteksi ICMP <i>Real-Time</i>	62
4.5.2	Pengujian Deteksi Setelah <i>Ping</i> ke-50 kali (<i>Ping Flood</i>)	64
4.5.3	Pengujian Deteksi Kiriman Malware dari Berbagai Pola Perintah	66
4.5.4	Pengujian Pemblokiran IP	69
4.6	Analisa Data Keseluruhan	70
4.6.1	Analisa Pengujian Deteksi ICMP <i>Real-Time</i>	70
4.6.2	Analisa Pengujian Deteksi Setelah <i>Ping</i> ke-50 Kali	71
4.6.3	Analisa Pengujian Deteksi <i>Malware</i>	71
4.6.4	Analisa Pemblokiran IP	71
BAB V PENUTUP		72
5.1	Kesimpulan	72
5.2	Saran	72
DAFTAR PUSTAKA		73
LAMPIRAN		

DAFTAR GAMBAR

Gambar 2. 1 MikroTik	8
Gambar 2. 2 Aplikasi Winbox	9
Gambar 2. 3 Ubuntu	11
Gambar 2. 4 Kali Linux	12
Gambar 2. 5 VMware	15
Gambar 2. 6 Aplikasi Telegram	18
Gambar 2. 7 Teknik Deteksi Anomali	27
Gambar 2. 8 Teknik Deteksi Penyalahgunaan	28
Gambar 2. 9 Diagram Struktur Kerja IDS	28
Gambar 3. 1 Flowchart	42
Gambar 3. 2 Blok Diagram	43
Gambar 3. 3 Topologi Jaringan	44
Gambar 3. 4 Instalasi Winbox	46
Gambar 3. 5 Reset MikroTik	46
Gambar 3. 6 Login Winbox	47
Gambar 3. 7 Mengubah Password dan Login Ulang	47
Gambar 3. 8 Konfigurasi IP dan DHCP Client	48
Gambar 3. 9 Pengaturan Firewall	48
Gambar 3. 10 Pengaturan Hotspot Setup	49
Gambar 3. 11 Mengaktifkan Antarmuka Wireless	49
Gambar 3. 12 Pembuatan Security Profile	50
Gambar 3. 13 Mengatur Interface Wireless sebagai Access Point	50
Gambar 3. 14 Setup Hotspot dan Konfigurasi Profil Hotspot	51
Gambar 3. 15 Menambahkan Akun Pengguna Hotspot	51
Gambar 3. 16 Mengatur Profil Pengguna Hotspot	52
Gambar 3. 17 Login Hotspot	52
Gambar 3. 18 Instalasi Ubuntu	52
Gambar 3. 19 Instalasi Telegram	53
Gambar 3. 20 Pembuatan Bot	53
Gambar 3. 21 Pengecekan IP Lokal Server IDS Melalui Perintah ifconfig	54
Gambar 3. 22 Instalasi dan Konfigurasi Snort	55
Gambar 3. 23 Integrasi Snort dengan Telegram	55
Gambar 3. 24 Pembuatan Skrip Notifikasi Menggunakan Python	56
Gambar 3. 25 Konfigurasi Local.Rules	57
Gambar 3. 26 Instalasi Kali Linux pada VMware Workstation	58
Gambar 3. 27 Login Kali Linux	58
Gambar 4. 1 Tampilan Awal Ubuntu Server	60
Gambar 4. 2 Mengaktifkan Snort	61
Gambar 4. 3 Menjalankan script Python3	61
Gambar 4. 4 Pengujian Ping Real-Time	63
Gambar 4. 5 Notifikasi Telegram dari deteksi ICMP Ping	63
Gambar 4. 6 Pengujian Ping via Handphone	64
Gambar 4. 7 Pengujian Ping 50 kali	65

Gambar 4. 8 Notifikasi Telegram dari deteksi ICMP Ping 50 kali.....	65
Gambar 4. 9 Pengujian Kirim Simulasi <i>Malware</i>	66
Gambar 4. 10 Pemblokiran IP	69
Gambar 4. 11 Notifikasi Telegram Saat Terjadinya Pemblokiran IP	70

DAFTAR TABEL

Tabel 2. 1 Simbol <i>Flowchart</i>	38
Tabel 2. 2 Tabel Penelitian Sebelumnya.....	39

DAFTAR LAMPIRAN

- Lampiran 1 Lembar Kesepakatan Bimbingan Laporan Akhir Pembimbing I
- Lampiran 2 Lembar Kesepakatan Bimbingan Laporan Akhir Pembimbing II
- Lampiran 3 Lembar Bimbingan Laporan Akhir Pembimbing I
- Lampiran 4 Lembar Bimbingan Laporan Akhir Pembimbing II
- Lampiran 5 Lembar Rekomendasi Ujian Laporan Akhir
- Lampiran 6 Lembar Revisi Laporan Akhir
- Lampiran 7 Lembar Pelaksanaan Revisi Laporan Akhir
- Lampiran 8 Lembar Bukti Penyerahan Hasil Karya Laporan Akhir
- Lampiran 9 Lembar *Logbook* Pembuatan Alat Laporan Akhir
- Lampiran 10 *Command Ubuntu Server*