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

LAPORAN TUGAS AKHIR

disusun sebagai salah satu syarat menyelesaikan pendidikan pada Program Studi D-III Teknik Komputer Jurusan Teknik Komputer Politeknik Negeri Sriwijaya

OLEH:
YEHAEZKIEL ELLZER MANOPPO
062330701568

POLITEKNIK NEGERI SRIWIJAYA
PALEMBANG
2026

LEMBAR PERSETUJUAN

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

LAPORAN TUGAS AKHIR

OLEH:

YEHAEZKIEL ELIZER MANOPPO
06233070156S

Palembang, 15 Juni 2026

Pembimbing I	Pembimbing II
Dr. Ahyar Supani, S.T., M.T.	Isnainy Azro, S.Kom., M.Kom.
NIP. 196802111992031002	NIP. 197310012002122007

Mengetahui,
Ketua Jurusan Teknik Komputer,

Dr. Slamet Widodo, S.Kom., M.Kom.
NIP. 197305162002121001

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

Telah Diuji dan dipertahankan di depan dewan penguji
Sidang Laporan Tugas Akhir pada hari Kamis, 25 Juni 2026

Ketua Dewan penguji	Tanda Tangan
Dr. Slamet Widodo, S.Kom., M.Kom. NIP. 197305162002121001	.....
Anggota Dewan penguji	
Dr. Ir. Alan Novi Tompunu, S.T., M.T., IPM., ASEAN Eng., APEC Eng. NIP. 197611082000031002	.....
Adi Sutrisman, S.Kom., M.Kom. NIP. 197503052001121005	.....
Fithri Selva Juneilah, S.Kom., M.T.I. NIP. 199005042020122013	.....

Palembang, 25 Juni 2026
Mengetahui,
Ketua jurusan,

Dr. Slamet Widodo, S.Kom., M.Kom.
NIP. 197305162002121001

KEMENTERIAN PENDIDIKAN TINGGI, SAINS,
DAN TEKNOLOGI
POLITEKNIK NEGERI SRIWIJAYA
JURUSAN TEKNIK KOMPUTER
Jalan Srijaya Negara, Palembang 30139. Telp. 0711-353414
Website : www.polsri.ac.id E-mail : info@polsri.ac.id

SURAT PERNYATAAN BEBAS PLAGIARISME

Yang bertanda tangan di bawah ini:

Nama	: Yehaezkiel Ellzer Manoppo
NIM	: 062330701568
Kelas	: 6 CN
Jurusan/Program Studi	: Teknik Komputer/D-III Teknik Komputer
Judul Laporan Akhir	: Rancang Bangun Sistem Deteksi dan Klasifikasi Serangan Jaringan Menggunakan Algoritma Random Forest Berdasarkan Data IDS dan Honeypot pada Security Operations Center (SOC)

Dengan ini menyatakan:

1. Laporan akhir yang saya buat dengan judul sebagaimana tersebut diatas beserta isinya merupakan hasil penelitian saya sendiri.
2. Laporan akhir tersebut bukan plagiat atau menyalin laporan akhir milik orang lain.
3. Apabila laporan ini di kemudian hari dinyatakan plagiat atau menyalin laporan akhir milik orang lain, maka saya bersedia menanggung konsekuensinya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya untuk diketahui oleh pihak-pihak yang berkepentingan.

Palembang, 21 Juli 2026

Yang membuat pernyataan,

Yehaezkiel Ellzer Manoppo
NIM. 062330701568

MOTTO

"Tidak harus menjadi yang paling hebat untuk memulai, tetapi harus berani memulai untuk menjadi lebih hebat."

"Sulit bukan berarti tidak bisa. Selama masih mau belajar dan terus mencoba, selalu ada jalan untuk menyelesaikannya."

"Selesaikan apa yang telah dimulai, karena setiap langkah kecil yang dilakukan dengan sungguh-sungguh akan membawa kita lebih dekat pada tujuan."

PERSEMBAHAN

Tugas Akhir ini saya persembahkan kepada:

1. Kedua Orang Tua Tercinta, Elizabeth Karyantina Ratoe dan Fentje Daniel Manoppo. Terima Kasih atas doa, kasih sayang, dukungan, pengorbanan, dan kepercayaan yang selalu diberikan. Tanpa dukungan kalian, perjalanan ini tentu tidak akan sampai pada titik ini.
2. Kakak dan Adik Tercinta, Felyna Deria Natalie Manoppo dan Sultan Yacobus Manuel Manoppo. Terima kasih atas perhatian, dukungan, semangat, serta kebersamaan yang selalu diberikan. Kehadiran kalian menjadi bagian penting dalam perjalanan saya hingga dapat menyelesaikan pendidikan dan Tugas Akhir ini.
3. Diri Saya Sendiri, Yehaezkiel Ellzer Manoppo. Yang telah bertahan melewati berbagai kesulitan, tekanan, keraguan, dan proses panjang selama menyelesaikan pendidikan dan Tugas Akhir ini. Terima kasih karena tetap memilih untuk melanjutkan ketika menyerah terasa lebih mudah. Semoga pencapaian ini bukan menjadi akhir, melainkan awal untuk terus belajar, berkembang, dan mengejar cita-cita yang lebih besar.

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

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Tuhan Yang Maha Esa karena atas rahmat dan karunia-Nya penulis dapat menyelesaikan Laporan Tugas Akhir yang berjudul **"RANCANG BANGUN SISTEM DETEKSI DAN KLASIFIKASI SERANGAN JARINGAN MENGGUNAKAN ALGORITMA RANDOM FOREST BERDASARKAN DATA IDS DAN HONEYPOT PADA SECURITY OPERATIONS CENTER (SOC)"** dengan baik dan tepat pada waktunya. Laporan Tugas Akhir ini disusun sebagai salah satu syarat untuk menyelesaikan pendidikan pada Program Studi D-III Teknik Komputer Jurusan Teknik Komputer Politeknik Negeri Sriwijaya.

Dalam proses penyusunan laporan ini, penulis menyadari bahwa banyak bantuan, dukungan, arahan, serta bimbingan dari berbagai pihak sehingga laporan ini dapat terselesaikan. Oleh karena itu, pada kesempatan ini penulis menyampaikan ucapan terima kasih kepada:

1. Bapak Ir. Irawan Rusnadi, M.T. selaku Direktur Politeknik Negeri Sriwijaya.
2. Bapak Dr. Slamet Widodo, S.Kom., M.Kom. selaku Ketua Jurusan Teknik Komputer Politeknik Negeri Sriwijaya.
3. Bapak Dr. Ahyar Supani, S.T., M.T. selaku Dosen Pembimbing I yang telah memberikan arahan, masukan, dan bimbingan selama proses penyusunan laporan tugas akhir ini.
4. Ibu Isnainy Azro, S.Kom., M.Kom. selaku Dosen Pembimbing II yang telah memberikan dukungan, saran, serta bimbingan kepada penulis dalam penyusunan laporan ini.
5. Kedua orang tua dan keluarga yang selalu memberikan doa, dukungan, serta semangat kepada penulis.
6. Rekan-rekan mahasiswa kelas 6 CN 23 Jurusan Teknik Komputer yang telah memberikan bantuan dan motivasi selama penyusunan laporan tugas akhir ini.

Penulis menyadari bahwa laporan tugas akhir ini masih memiliki kekurangan dan jauh dari kata sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun demi perbaikan di masa yang akan datang.

Akhir kata, penulis berharap semoga laporan tugas akhir ini dapat memberikan manfaat bagi penulis maupun para pembaca.

Palembang, 15 Juni 2026



Yehaezkiel Ellzer Manoppo
NIM. 062330701568

DAFTAR ISI

HALAMAN JUDUL ..... **i**
LEMBAR PERSETUJUAN ..... **ii**
LEMBAR PERSETUJUAN PENGUJI ..... **iii**
LEMBAR PERNYATAAN ..... **iv**
MOTTO DAN PERSEMBAHAN ..... **v**
ABSTRAK ..... **vi**
ABSTRACT ..... **vii**
KATA PENGANTAR ..... **viii**
DAFTAR ISI ..... **x**
DAFTAR GAMBAR ..... **xvii**
DAFTAR TABEL ..... **xx**

BAB I PENDAHULUAN
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Batasan Masalah 3
1.4 Tujuan 4
1.5 Manfaat 4

BAB II TINJAUAN PUSTAKA
2.1 Penelitian Terdahulu 6
2.1.1 Perbedaan Model Penelitian dengan Model Sebelumnya 9
2.2 Security Operations Center (SOC) 11
2.2.1 Pengertian Security Operations Center 11
2.2.2 Fungsi Security Operations Center 12
2.2.3 Komponen Security Operations Center 12
2.3 Keamanan Jaringan Komputer 13
2.3.1 Pengertian Keamanan Jaringan 13
2.3.2 Jenis-Jenis Serangan Jaringan 14
2.4 Intrusion Detection System (IDS) 15
2.4.1 Pengertian Intrusion Detection System (IDS) 15

2.4.2 Jenis-Jenis IDS 16
2.4.3 Snort IDS 16
2.5 Honeypot 17
2.5.1 Pengertian Honeypot 17
2.5.2 Fungsi Honeypot dalam Keamanan Jaringan 17
2.5.3 Jenis-Jenis Honeypot 18
2.5.4 Cowrie Honeypot 19
2.5.5 Honeypot sebagai Sumber Data Machine Learning 20
2.6 Machine Learning 21
2.6.1 Pengertian Machine Learning 21
2.6.2 Peran Machine Learning dalam Keamanan Jaringan 22
2.6.3 Jenis-Jenis Machine Learning 23
2.6.4 Machine Learning untuk Intrusion Detection System 24
2.6.5 Machine Learning pada Penelitian Ini 25
2.7 Algoritma Random Forest 26
2.7.1 Pengertian Random Forest 26
2.7.2 Cara Kerja Random Forest 27
2.7.3 Kelebihan dan Kekurangan Random Forest 27
2.7.4 Random Forest Untuk Deteksi Serangan Jaringan 28
2.7.5 Random Forest pada Penelitian Ini 29
2.8 Dataset CICIDS2017 30
2.8.1 Pengertian Dataset CICIDS2017 30
2.8.2 Karakteristik Dataset CICIDS2017 31
2.8.3 Jenis Serangan pada Dataset CICIDS2017 32
2.8.4 Fitur-Fitur pada Dataset CICIDS2017 32
2.8.5 Penggunaan Dataset CICIDS2017 pada Penelitian Ini 33
2.9 Database MariaDB 34
2.9.1 Pengertian Basis Data 34
2.9.2 MariaDB 34
2.9.3 Fungsi MariaDB pada Sistem Deteksi Serangan Jaringan 35
2.9.4 Struktur Penyimpanan Data pada Penelitian 35
2.9.5 MariaDB pada Penelitian Ini 35

2.10 Flask Framework 36
2.10.1 Pengertian Flask 36
2.10.2 Fungsi Flask pada Aplikasi Web 36
2.10.3 Peran Flask pada Sistem Monitoring Keamanan 37
2.10.4 Flask pada Penelitian Ini 37
2.11 Telegram Bot 37
2.11.1 Pengertian Telegram Bot 37
2.11.2 Telegram Bot API 38
2.11.3 Fungsi Telegram Bot pada Sistem Monitoring 39
2.11.4 Telegram Bot pada Sistem Deteksi Serangan Jaringan 39
2.11.5 Telegram Bot pada Penelitian Ini 40
2.12 Ubuntu Server 24.04 LTS 40
2.12.1 Pengertian Ubuntu Server 24.04 LTS 40
2.12.2 Karakteristik Ubuntu Server 24.04 LTS 41
2.12.3 Keunggulan Ubuntu Server24.04 LTS 42
2.12.4 Peran Ubuntu Server 24.04 LTS dalam Penelitian 42
2.13 Kali Linux 43
2.13.1 Pengertian Kali Linux 43
2.13.2 Fitur dan Tools Keamanan pada Kali Linux 43
2.13.3 Pemanfaatan Kali Linux untuk Pengujian Keamanan Jaringan 44
2.13.4 Peran Kali Linux dalam Penelitian 44
2.14 VirtualBox 45
2.14.1 Pengertian VirtualBox 45
2.14.2 Konsep Virtualisasi Menggunakan VirtualBox 46
2.14.3 Keunggulan VirtualBox sebagai Lingkungan Pengujian 46
2.14.4 Peran VirtualBox dalam Pengujian 47
2.15 TShark 47
2.15.1 Pengertian TShark 47
2.15.2 Cara Kerja TShark 48
2.15.3 Fungsi TShark dalam Analisis Lalu Lintas Jaringan 49
2.15.4 Peran TShark dalam Penelitian 49
2.16 CICFlowMeter 50

2.16.1 Pengertian CICFlowMeter 50
2.16.2 Cara Kerja CICFlowMeter 50
2.16.3 Feature Extraction pada CICFlowMeter 51
2.16.4 Peran CICFlowMeter 52
2.17 Python 3 53
2.17.1 Pengertian Python 3 53
2.17.2 Karakteristik Bahasa Pemrograman Python 54
2.17.3 Keunggulan Python untuk Pengembangan Sistem Keamanan Jaringan 54
2.17.4 Peran Python 3 dalam Penelitian 55
2.18 Scikit-learn 55
2.18.1 Pengertian Scikit-learn 55
2.18.2 Fitur dan Library pada Scikit-learn 56
2.18.3 Implementasi Algoritma Random Forest pada Scikit-learn 57
2.18.4 Peran Scikit-learn dalam Penelitian 58
2.19 Flowchart 58
BAB III METODE PENELITIAN/RANCANG BANGUN
3.1 Tujuan Perancangan 61
3.1.1 Tujuan Umum 61
3.1.2 Tujuan Khusus 61
3.2 Diagram Blok 62
3.2.1 Input Sistem 63
3.2.2 Proses Sistem 63
3.2.3 Output Sistem 64
3.2.4 Tabel Komponen Diagram Blok 64
3.3 Flowchart Sistem 64
3.3.1 Flowchart Sistem Keseluruhan 65
3.3.2 Penjelasan Flowchart Sistem 66
3.4 Metode Penelitian 67
3.4.1 Studi Literatur 69
3.4.2 Analisis Kebutuhan Sistem 69
3.4.3 Perancangan Sistem 70

3.4.4 Implementasi Sistem 70
3.4.5 Pengujian Sistem 70
3.5 Analisis Kebutuhan Sistem 71
3.5.1 Kebutuhan Perangkat Keras (Hardware) 72
3.5.2 Kebutuhan Perangkat Lunak (Software) 72
3.5.3 Kebutuhan Jaringan 73
3.6 Perancangan Arsitektur Sistem 74
3.6.1 Topologi Jaringan Sistem 74
3.6.2 Arsitektur Integrasi IDS, Honeypot, dan Machine Learning 75
3.6.3 Arsitektur SOC Dashboard 76
3.6.4 Arsitektur Teknik Serangan, Server, dan Monitoring Administrator 77
3.7 Perancangan Database 79
3.7.1 Struktur Tabel Snort Alerts 79
3.7.2 Struktur Tabel Cowrie Logs 79
3.7.3 Struktur Tabel ML Predictions 80
3.8 Perancangan Machine Learning 80
3.8.1 Dataset yang Digunakan 81
3.8.2 Preprocessing Data 82
3.8.3 Pelatihan Model Random Forest 84
3.8.4 Proses Klasifikasi Serangan 85
3.9 Perancangan Antarmuka Sistem 87
3.9.1 Rancangan Dashboard Utama 87
3.9.2 Rancangan Halaman IDS 87
3.9.3 Rancangan Halaman Honeypot 88
3.9.4 Rancangan Halaman Machine Learning 88
3.9.5 Rancangan Notifikasi Telegram 89
3.10 Skenario Pengujian Sistem 90
3.10.1 Pengujian Snort IDS 92
3.10.2 Pengujian Cowrie Honeypot 93
3.10.3 Pengujian Deteksi Port Scan 93
3.10.4 Pengujian Deteksi Brute Force 94

3.10.5 Pengujian Deteksi Web Attack 94
3.10.6 Pengujian Deteksi DDoS 95
3.10.7 Pengujian Dashboard dan Telegram Alert..... 95
BAB IV HASIL DAN PEMBAHASAN
4.1 Hasil 96
4.1.1 Hasil Implementasi Topologi Jaringan Sistem..... 96
4.1.2 Hasil Implementasi Snort IDS 97
4.1.3 Hasil Implementasi Cowrie Honeypot 97
4.1.4 Hasil Implementasi Database MariaDB..... 98
4.1.5 Hasil Implementasi Machine Learning Random Forest..... 99
4.1.6 Hasil Implementasi SOC Dashboard 100
4.1.6.1 Hasil Implementasi Dashboard Utama..... 100
4.1.6.2 Hasil Implementasi Halaman IDS..... 101
4.1.6.3 Hasil Implementasi Halaman Honeypot 101
4.1.6.4 Hasil Implementasi Halaman Machine Learning..... 102
4.1.7 Hasil Implementasi Telegram Alert..... 103
4.1.8 Hasil Pengujian Snort IDS 104
4.1.9 Hasil Pengujian Cowrie Honeypot..... 104
4.1.10 Hasil Pengujian Deteksi Port Scan..... 105
4.1.11 Hasil Pengujian Deteksi Brute Force 106
4.1.12 Hasil Pengujian Deteksi Web Attack 107
4.1.13 Hasil Pengujian Deteksi DDoS 107
4.1.14 Hasil Pengujian Dashboard dan Telegram Alert 108
4.2 Pembahasan..... 111
4.2.1 Analisis Kinerja Snort IDS 112
4.2.2 Analisis Kinerja Cowrie Honeypot 112
4.2.3 Analisis Kinerja Algoritma Random Forest..... 112
4.2.4 Analisis Hasil Klasifikasi Serangan Jaringan 113
4.2.5 Analisis Integrasi IDS, Honeypot, dan Machine Learning 113
4.2.6 Analisis Tampilan SOC Dashboard..... 114
4.2.7 Analisis Notifikasi Telegram Alert..... 114
4.2.8 Kelebihan dan Keterbatasan Sistem..... 115

BAB V PENUTUP

5.1 Kesimpulan 116

5.2 Saran..... 118

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR GAMBAR

Gambar 2.1 Arsitektur Umum Security Operations Center 11
Gambar 2.2 Alur Kerja Sistem Deteksi dan Klasifikasi Serangan Jaringan 13
Gambar 2.3 Jenis Serangan Jaringan 15
Gambar 2.4 Logo Snort IDS 16
Gambar 2.5 Mekanisme Kerja Snort IDS pada Sistem yang Diusulkan..... 17
Gambar 2.6 Ilustrasi Cara Kerja Honeypot..... 17
Gambar 2.7 Logo Cowrie Honeypot..... 19
Gambar 2.8 Arsitektur Kerja Cowrie Honeypot 20
Gambar 2.9 Konsep Machine Learning pada Keamanan Jaringan..... 22
Gambar 2.10 Konsep Machine Learning pada Intrusion Detection System.... 25
Gambar 2.11 Mekanisme kerja Algoritma Random Forest..... 26
Gambar 2.12 Penerapan Random Forest pada Deteksi Serangan Jaringan 29
Gambar 2.13 Dataset CICIDS2017..... 31
Gambar 2.14 Logo MariaDB 34
Gambar 2.15 Logo Flask Framework 36
Gambar 2.16 Logo Telegram 38
Gambar 2.17 Arsitektur Telegram Bot API..... 39
Gambar 2.18 Logo Ubuntu Server 24.04 LTS 41
Gambar 2.19 Logo Kali Linux..... 43
Gambar 2.20 Logo VirtualBox..... 45
Gambar 2.21 Arsitektur Virtualisasi Menggunakan VirtualBox 45
Gambar 2.22 Mekanisme Capture *Traffic* Menggunakan TShark 48
Gambar 2.23 Proses Konversi PCAP Menjadi Dataset CSV Menggunakan CICFlowMeter 52
Gambar 2.24 Logo Python 3 53
Gambar 2.25 Pemanfaatan Python pada Integrasi Sistem 53
Gambar 2.26 Logo Scikit-learn..... 56
Gambar 3.1 Diagram Blok Sistem 63
Gambar 3.2 Flowchart Sistem Keseluruhan..... 66
Gambar 3.3 Flowchart Metode Penelitian..... 68

Gambar 3.4 Topologi Jaringan Sistem 75
Gambar 3.5 Arsitektur Integrasi IDS, Honeypot, dan Machine Learning 76
Gambar 3.6 Arsitektur SOC Dashboard..... 77
Gambar 3.7 Arsitektur Teknik Serangan, Server, dan Monitoring Administrator 78
Gambar 3.8 Alur Perancangan Machine Learning..... 81
Gambar 3.9 Flowchart Preprocessing Data..... 83
Gambar 3.10 Flowchart Proses Pelatihan Model Random Forest 85
Gambar 3.11 Alur Klasifikasi Serangan Menggunakan Random Forest 86
Gambar 3.12 Rancangan Dashboard Utama 87
Gambar 3.13 Rancangan Halaman IDS 88
Gambar 3.14 Rancangan Halaman Honeypot 88
Gambar 3.15 Rancangan Halaman Machine Learning 89
Gambar 3.16 Rancangan Notifikasi IDS, Honeypot, dan Machine Learning.. 90
Gambar 3.17 Skenario Pengujian Sistem..... 91
Gambar 4.1 Hasil Implementasi Topologi Jaringan Sistem 97
Gambar 4.2 Hasil Implementasi Snort IDS..... 97
Gambar 4.3 Hasil Implementasi Cowrie Honeypot 98
Gambar 4.4 Hasil Implementasi Database MariaDB 99
Gambar 4.5 Hasil Implementasi Machine Learning Random Forest..... 100
Gambar 4.6 Hasil Implementasi Dashboard Utama..... 100
Gambar 4.7 Hasil Implementasi Halaman IDS 101
Gambar 4.8 Hasil Implementasi Halaman Honeypot..... 102
Gambar 4.9 Hasil Implementasi Halaman Machine Learning..... 102
Gambar 4.10 Hasil Implementasi Teegram Alert 103
Gambar 4.11 Hasil Pengujian Snort IDS pada Kali Linux..... 104
Gambar 4.12 Hasil Pengujian Snort IDS pada Ubuntu Server 24.04 LTS..... 104
Gambar 4.13 Hasil Pengujian Cowrie Honeypot pada Kali Linux 105
Gambar 4.14 Hasil Pengujian Cowrie Honeypot pada Ubuntu Server 24.04 LTS 105
Gambar 4.15 Hasil Pengujian Port Scan pada Kali Linux 106
Gambar 4.16 Hasil Pengujian Port Scan pada Ubuntu Server 24.04 LTS 106

Gambar 4.17 Hasil Pengujian Brute Force pada Kali Linux..... 106
Gambar 4.18 Hasil Pengujian Brute Force Pada Ubuntu Server 24.04 LTS.... 107
Gambar 4.19 Hasil Pengujian Web Attack pada Kali Linux 107
Gambar 4.20 Hasil Pengujian Web Attack pada Ubuntu Server 24.04 LTS 107
Gambar 4.21 Hasil Pengujian DDoS pada Kali Linux..... 108
Gambar 4.22 Hasil Pengujian DDoS pada Ubuntu Server 24.04 LTS..... 108
Gambar 4.23 Hasil Pengujian Halaman Dashboard Utama 109
Gambar 4.24 Hasil Pengujian Halaman IDS..... 109
Gambar 4.25 Hasil Pengujian Halaman Honeypot 110
Gambar 4.26 Hasil Pengujian Halaman Machine Learning..... 110
Gambar 4.27 Hasil Pengujian Telegram..... 111

DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu 8
Tabel 2.2 Perbedaan Model Penelitian dengan Model Sebelumnya 10
Tabel 2.3 Jenis Serangan Jaringan dan Karakteristiknya 15
Tabel 2.4 Perbandingan NIDS dan HIDS 16
Tabel 2.5 Fitur Utama Snort IDS 17
Tabel 2.6 Perbandingan Low Interaction dan High Interaction 18
Tabel 2.7 Perbandingan Jenis Machine Learning 23
Tabel 2.8 Kelebihan dan Kekurangan Random Forest 27
Tabel 2.9 Karakteristik Dataset CICIDS2017 31
Tabel 2.10 Jenis Serangan pada Dataset CICIDS2017 32
Tabel 2.11 Contoh Fitur Penting Dataset CICIDS2017 32
Tabel 2.12 File Dataset CICIDS2017 yang Digunakan 33
Tabel 2.13 Data yang Disimpan pada MariaDB 35
Tabel 2.14 Contoh Feature yang Dihasilkan CICFlowMeter 51
Tabel 2.15 Simbol dan Fungsi Flowchart 59
Tabel 3.1 Komponen Diagram Blok 64
Tabel 3.2 Tahapan Metode Penelitian 71
Tabel 3.3 Kebutuhan Perangkat Keras 72
Tabel 3.4 Kebutuhan Perangkat Lunak 72
Tabel 3.5 Kebutuhan Jaringan 73
Tabel 3.6 Kebutuhan Jaringan Mitra 74
Tabel 3.7 Komponen Arsiteiktur Teknik Serangan, Server, dan Monitoring 78
Tabel 3.8 Struktur Tabel Snort Alerts 79
Tabel 3.9 Struktur Tabel Cowrie Logs 80
Tabel 3.10 Struktur Tabel ML Predictions 80
Tabel 3.11 File Dataset CICIDS2017 yang Digunakan 82
Tabel 3.12 Skenario Pengujian Sistem 92
Tabel 4.1 Hasil Pengujian Dashboard dan Telegram Alert 111