



## **BERITA ACARA SIDANG PENDADARAN TUGAS AKHIR**

S/UBL/FTI/1000/VII/26

Pada hari ini, Kamis 16 Juli 2026 telah dilaksanakan Ujian Sidang Pendadaran Tugas Akhir sebagai berikut:

Judul: PROTOTIPE SISTEM DETEKSI DAN RESPON KEAMANAN JARINGAN BERBASIS MACHINE LEARNING MENGGUNAKAN METADATA ZEEK, INTEGRASI SIEM DAN NOTIFIKASI TELEGRAM BOT

Nama : Septian Tri Mahendra  
NIM : 2211501453  
Dosen Pembimbing : Joko Christian Chandra, S.Kom., M.Kom.

Berdasarkan penilaian pada Presentasi + Demo, Penulisan, Penguasaan Materi, Penguasaan Program maka Mahasiswa tersebut di atas dinyatakan:

**LULUS**

dengan nilai angka : **87** huruf : **A**

Mahasiswa tersebut di atas wajib menyerahkan hasil perbaikan tulisan Tugas Akhir dalam bentuk terjilid sesuai dengan Panduan Perbaikan Tugas Akhir, selambat-lambatnya Kamis 30 Juli 2026.

### Panitia Penguji:

- 1 Ketua Sri Mulyati, S.Kom., M.Kom.
- 2 Anggota Painem, S.Kom., M.Kom.
- 3 Moderator Joko Christian Chandra, S.Kom., M.Kom.

### Keterangan:

Nilai Huruf: A:85-100 A-:80-84,99 B+:75-79,99 B:70-74,99 B-:65-69,99 C:60-64,99 D:40-59,99 E-:0-39,99



UNIVERSITAS BUDI LUHUR  
FAKULTAS TEKNOLOGI INFORMASI

Kartu Bimbingan Tugas Akhir

NIM: 2211501453

Nama: Septian Tri Mahendra

Pembimbing: Joko Christian Chandra, S.Kom., M.Kom.

| No. | Tanggal    | Materi                                         |
|-----|------------|------------------------------------------------|
| 1   | 16-04-2026 | bimbingan tema dan konsep riset                |
| 2   | 04-05-2026 | draft bab 1, perbaikan terkait rumusan masalah |
| 3   | 19-05-2026 | draft bab 2 dan metodologi                     |
| 4   | 27-05-2026 | perbaikan bab 1-2 dan draft bab 3              |
| 5   | 09-06-2026 | Perbaikan bab 3 dan gambar                     |
| 6   | 17-06-2026 | Draft bab 4 dan demo                           |
| 7   | 29-06-2026 | demo aplikasi perbaikan                        |
| 8   | 02-07-2026 | perbaikan bab 4, diskusi bab 5                 |



LEMBAR PENGESAHAN

Nama : Septian Tri Mahendra  
Nomor Induk Mahasiswa : 2211501453  
Program Studi : Teknik Informatika  
Bidang Peminatan : Cyber Security  
Jenjang Studi : Strata 1  
Judul : PROTOTIPE SISTEM DETEKSI DAN RESPON KEAMANAN JARINGAN  
BERBASIS MACHINE LEARNING MENGGUNAKAN METADATA  
ZEEK, INTEGRASI SIEM DAN NOTIFIKASI TELEGRAM BOT



Laporan Tugas Akhir ini telah disetujui, disahkan dan direkam secara elektronik sehingga tidak memerlukan tanda tangan tim penguji.

Jakarta, Kamis 16 Juli 2026

Tim Penguji:

Ketua : Sri Mulyati, S.Kom., M.Kom.  
Anggota : Painem, S.Kom., M.Kom.  
Pembimbing : Joko Christian Chandra, S.Kom., M.Kom.  
Ketua Program Studi : Dr. Indra, S.Kom., M.T.I.

**PROTOTIPE SISTEM DETEKSI DAN RESPON KEAMANAN  
JARINGAN BERBASIS *MACHINE LEARNING*  
MENGUNAKAN METADATA ZEEK, INTERGRASI SIEM  
DAN NOTIFIKASI TELEGRAM BOT**

**TUGAS AKHIR**



**Oleh:**

**Septian Tri Mahendra**

**2211501453**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNOLOGI INFORMASI  
UNIVERSITAS BUDI LUHUR**

**JAKARTA  
2026**

**ABSTRAK**  
**PROTOTYPE SISTEM DETEKSI DAN RESPON KEAMANAN**  
**JARINGAN BERBASIS *MACHINE LEARNING* MENGGUNAKAN**  
**METADATA ZEEK, INTEGRASI SIEM DAN NOTIFIKASI TELEGRAM**  
**BOT**

**Oleh: Septian Tri Mahendra (2211501453)**

Ancaman keamanan jaringan komputer terus berkembang seiring meningkatnya kompleksitas dan frekuensi serangan siber, sehingga pendekatan deteksi berbasis *signature* konvensional memiliki keterbatasan dalam mengenali serangan baru (*zero-day*). Penelitian ini bertujuan merancang dan membangun prototipe Sistem Deteksi dan Respons Keamanan Jaringan menggunakan pendekatan deteksi hibrida yang mengintegrasikan Suricata, Zeek, algoritma Isolation Forest, ELK Stack, dan Telegram Bot. Metode yang digunakan adalah *Prototype* meliputi analisis kebutuhan, perancangan, implementasi, serta pengujian. Sistem diimplementasikan pada empat *virtual machine* menggunakan VirtualBox. Lapisan deteksi memanfaatkan Suricata dengan *ruleset Emerging Threats Open* dan *custom rule*, serta Isolation Forest berbasis metadata Zeek. Hasil deteksi disimpan di Elasticsearch, divisualisasikan melalui Kibana, dan dikirimkan melalui Telegram Bot. Pengujian terhadap enam skenario serangan menunjukkan *detection rate* 100%, menghasilkan 738 alert Suricata dan 388 anomali. Rata-rata latensi notifikasi sebesar 31,2 detik, sedangkan mekanisme anti-spam menurunkan volume notifikasi hingga 98,3%. Integrasi *signature*, *machine learning*, SIEM, dan notifikasi *real-time* menghasilkan sistem keamanan jaringan yang efektif, komprehensif, dan hemat biaya.

**Kata Kunci:** Network Intrusion Detection System, *Hybrid Detection*, Suricata, Zeek, *Isolation Forest*, ELK Stack, SIEM, Telegram Bot, *Machine Learning*, Keamanan Jaringan.

## DAFTAR ISI

|                                                                     |      |
|---------------------------------------------------------------------|------|
| LEMBAR PENGESAHAN .....                                             | iii  |
| ABSTRAK.....                                                        | iv   |
| SURAT TIDAK PLAGIAT .....                                           | v    |
| KATA PENGANTAR .....                                                | vi   |
| DAFTAR TABEL.....                                                   | vii  |
| DAFTAR GAMBAR.....                                                  | viii |
| DAFTAR SIMBOL .....                                                 | ix   |
| DAFTAR ALGORITMA .....                                              | x    |
| DAFTAR ISI.....                                                     | xi   |
| BAB I PENDAHULUAN.....                                              | 1    |
| 1.1 Latar Belakang.....                                             | 1    |
| 1.2 Perumusan Masalah .....                                         | 2    |
| 1.3 Batasan Masalah .....                                           | 2    |
| 1.4 Tujuan .....                                                    | 3    |
| 1.5 Manfaat .....                                                   | 3    |
| 1.6 Sistematika Penulisan .....                                     | 3    |
| BAB II LANDASAN TEORI.....                                          | 5    |
| 2.1 Keamanan Jaringan Komputer.....                                 | 5    |
| 2.1.1 Klasifikasi Ancaman Jaringan .....                            | 5    |
| 2.2 <i>Intrusion Detection System (IDS)</i> .....                   | 6    |
| 2.2.1 Jenis-jenis IDS .....                                         | 6    |
| 2.2.2 Metode Deteksi IDS.....                                       | 7    |
| 2.3 Security Information and Event Management (SIEM).....           | 8    |
| 2.3.1 Arsitektur dan Komponen SIEM .....                            | 8    |
| 2.4 Suricata .....                                                  | 9    |
| 2.5 Zeek .....                                                      | 9    |
| 2.5.1 Tipe-tipe Log Zeek .....                                      | 9    |
| 2.6 ELK Stack (Elasticsearch, Logstash, Kibana) .....               | 10   |
| 2.6.1 Elasticsearch .....                                           | 10   |
| 2.6.2 Logstash .....                                                | 11   |
| 2.6.3 Kibana .....                                                  | 11   |
| 2.7 Filebeat.....                                                   | 11   |
| 2.8 Machine Learning untuk Keamanan Jaringan .....                  | 12   |
| 2.9 Algoritma Isolation Forest .....                                | 12   |
| 2.9.1 Mekanisme Kerja Isolation Forest .....                        | 13   |
| 2.9.2 Keunggulan Isolation Forest untuk NIDS .....                  | 13   |
| 2.10 Telegram Bot API.....                                          | 14   |
| 2.11 Metodologi Pengembangan Purwarupa ( <i>Prototyping</i> ) ..... | 14   |
| 2.11.1 Jenis-jenis Model Purwarupa ( <i>Prototyping</i> ) .....     | 15   |
| 2.11.2 Keunggulan dan Keterbatasan Metodologi Prototyping.....      | 15   |
| 2.12 Pengujian Black Box .....                                      | 16   |
| 2.13 Penelitian Terdahulu .....                                     | 16   |
| BAB III METODOLOGI PENELITIAN .....                                 | 19   |

|                                   |                                                         |    |
|-----------------------------------|---------------------------------------------------------|----|
| 3.1                               | Metode Penelitian Prototype.....                        | 19 |
| 3.1.1                             | Tahapan Metodologi Prototype dalam Penelitian Ini ..... | 19 |
| 3.2                               | Arsitektur Sistem .....                                 | 20 |
| 3.3                               | Topologi Jaringan Lab .....                             | 21 |
| 3.4                               | Spesifikasi Lingkungan Pengujian.....                   | 22 |
| 3.4.1                             | Spesifikasi Virtual Machine.....                        | 22 |
| 3.4.2                             | Spesifikasi Perangkat Lunak.....                        | 23 |
| 3.5                               | Use Case Diagram .....                                  | 23 |
| 3.5.1                             | Identifikasi Aktor .....                                | 24 |
| 3.5.2                             | Diagram Use Case .....                                  | 24 |
| 3.6                               | Activity Diagram .....                                  | 24 |
| 3.6.1                             | Activity Diagram Proses Deteksi Hybrid .....            | 25 |
| 3.6.2                             | Activity Diagram Pengiriman Notifikasi Telegram.....    | 25 |
| 3.7                               | Perancangan Alur Kerja Sistem.....                      | 26 |
| 3.7.1                             | Alur Data Suricata .....                                | 26 |
| 3.7.2                             | Alur Data Zeek.....                                     | 26 |
| 3.8                               | Perancangan Hybrid Detection .....                      | 27 |
| 3.8.1                             | Deteksi Berbasis Signature (Suricata) .....             | 27 |
| 3.8.2                             | Deteksi Anomali Berbasis ML (Isolation Forest).....     | 27 |
| 3.8.3                             | Korelasi Hasil Deteksi .....                            | 27 |
| 3.9                               | Perancangan Notifikasi Telegram.....                    | 28 |
| 3.9.1                             | Format Pesan Alert Suricata .....                       | 28 |
| 3.9.2                             | Format Pesan Alert ML Anomaly .....                     | 28 |
| 3.9.3                             | Mekanisme Anti-Spam .....                               | 28 |
| 3.10                              | Feature Engineering ML .....                            | 29 |
| 3.10.1                            | Pemetaan Field conn.log ke Fitur ML .....               | 29 |
| 3.11                              | Perancangan Pengujian .....                             | 29 |
| 3.11.1                            | Kriteria Keberhasilan Pengujian.....                    | 30 |
| 3.11.2                            | Matriks Pengujian .....                                 | 30 |
| 3.11.3                            | Metriks Evaluasi .....                                  | 30 |
| BAB IV HASIL DAN PEMBAHASAN ..... |                                                         | 32 |
| 4.1                               | Hasil Implementasi Sistem .....                         | 32 |
| 4.1.1                             | Hasil Implementasi Infrastruktur Virtual.....           | 32 |
| 4.1.2                             | Hasil Implementasi Suricata .....                       | 34 |
| 4.1.3                             | Hasil Implementasi Zeek .....                           | 35 |
| 4.1.4                             | Hasil Implementasi Log Pipeline.....                    | 36 |
| 4.1.5                             | Hasil Implementasi ML Isolation Forest .....            | 38 |
| 4.1.6                             | Hasil Implementasi Telegram Bot .....                   | 38 |
| 4.2                               | Hasil dan Pembahasan Pengujian Serangan .....           | 39 |
| 4.2.1                             | Skenario Network Scanning (Nmap).....                   | 39 |
| 4.2.2                             | Skenario SSH Brute Force (Hydra) .....                  | 42 |
| 4.2.3                             | Skenario FTP Brute Force (Hydra).....                   | 44 |
| 4.2.4                             | Skenario HTTP Directory Traversal (Nikto + curl).....   | 45 |
| 4.2.5                             | Skenario SQL Injection (curl Manual) .....              | 47 |
| 4.2.6                             | Skenario ICMP Flood / DoS (hping3) .....                | 48 |
| 4.3                               | Algoritma .....                                         | 49 |

|                                 |                                                                  |    |
|---------------------------------|------------------------------------------------------------------|----|
| 4.3.1                           | Algoritma Machine Learning.....                                  | 49 |
| 4.3.2                           | Algoritma Notifikasi Telegram Bot.....                           | 50 |
| 4.4                             | Analisis Performa Sistem Deteksi .....                           | 50 |
| 4.4.1                           | Rekap Komprehensif Seluruh Skenario Pengujian.....               | 50 |
| 4.4.2                           | Analisis Detection Rate .....                                    | 50 |
| 4.4.3                           | Analisis False Positive .....                                    | 51 |
| 4.4.4                           | Analisis Latensi Notifikasi Telegram .....                       | 51 |
| 4.4.5                           | Analisis Anomaly Score Distribution .....                        | 52 |
| 4.5                             | Pembahasan Efektivitas Pendekatan Hybrid Detection.....          | 53 |
| 4.5.1                           | Komparasi Kuantitatif Layer Signature-based vs Anomaly-based.... | 53 |
| 4.5.2                           | Analisis Sinergi dan Komplementaritas Kedua Layer.....           | 54 |
| 4.5.3                           | Pembahasan Potensi Deteksi Zero-Day .....                        | 55 |
| 4.6                             | Pembahasan Hasil Visualisasi Dashboard Kibana.....               | 55 |
| 4.6.1                           | Analisis Nilai Informasional Setiap Panel .....                  | 55 |
| 4.7                             | Pembahasan Sistem Notifikasi Real-time Telegram .....            | 55 |
| 4.7.1                           | Efektivitas Deduplication .....                                  | 55 |
| 4.7.2                           | Efektivitas Rate Limiting.....                                   | 55 |
| 4.8                             | Flowchart .....                                                  | 56 |
| 4.8.1                           | Flowchart Notifikasi Alert Telegram .....                        | 56 |
| 4.8.2                           | Flowchart Deteksi Machine Learning.....                          | 57 |
| 4.9                             | Temuan Penelitian dan Keterbatasan Sistem.....                   | 58 |
| 4.9.1                           | Temuan Utama Penelitian.....                                     | 58 |
| 4.9.2                           | Keterbatasan Sistem yang Teridentifikasi .....                   | 58 |
| BAB V PENUTUP .....             |                                                                  | 60 |
| 5.1                             | Kesimpulan .....                                                 | 60 |
| 5.2                             | Saran .....                                                      | 61 |
| DAFTAR PUSTAKA .....            |                                                                  | 62 |
| LEMBAR SURAT SELESAI RISET..... |                                                                  | 63 |
| LAMPIRAN.....                   |                                                                  | 64 |

## DAFTAR PUSTAKA

- Ahmad, Z., Khan, A. S., Shiang, C. W., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, 32(1), e4150.
- Akbari, I., Tahoun, M., & Khoukhi, L. (2022). Machine learning for network intrusion detection: A survey. *IEEE Access*, 10, 45230–45258.
- Bertoli, G. C., Pereira Júnior, L. A., Saotome, O., dos Santos, A. L., Verri, F. A. N., Marcondes, C. A. C., Barbieri, S., Rodrigues, M. S., & Parente de Oliveira, J. M. (2021). An End-to-End Framework for Machine Learning-Based Network Intrusion Detection System. *IEEE Access*, 9, 106790–106805.
- Buczak, A. L., & Guven, E. (2021). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*.
- Elastic. (2025). Elastic machine learning documentation.
- Elastic. (2025). Elastic Security documentation.
- Kumar, S., Gupta, S., & Arora, S. (2021). Research Trends in Network-Based Intrusion Detection Systems: A Review. *IEEE Access*, 9, 157761–157779.
- Le Jeune, L., Goedemé, T., & Mentens, N. (2021). Machine Learning for Misuse-Based Network Intrusion Detection: Overview, Unified Evaluation and Feature Choice Comparison Framework. *IEEE Access*, 9, 63995–64015.
- Open Information Security Foundation. (2025). Suricata User Guide (Version 7.x).
- Pacheco, J., Benitez, V., Felix-Herran, L. C., & Satam, P. (2023). Toward a Reliable Evaluation of Machine Learning Schemes for Network-Based Intrusion Detection. *IEEE Transactions on Network and Service Management*.
- Sarhan, M., Layeghy, S., & Portmann, M. (2021). Towards a Standard Feature Set for Network Intrusion Detection System Datasets. *IEEE Access*.
- Sarhan, M., Layeghy, S., Moustafa, N., & Portmann, M. (2022). NetFlow Datasets for Machine Learning-Based Network Intrusion Detection Systems. *Data*, 7(7).
- Scarfone, K., & Mell, P. (2021). Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology (NIST).
- Stallings, W. (2022). *Network Security Essentials: Applications and Standards* (7th ed.). Pearson.
- Telegram. (2025). Telegram Bot API.
- The Zeek Project. (2025). Zeek Documentation (Book of Zeek).