

**ANALISIS KEAMANAN JARINGAN DENGAN *HYBRID INTRUSION
DETECTION SYSTEM, FIREWALL, DAN VISUALISASI LOG ATTACKER***

TUGAS AKHIR

Oleh:

MUHAMMAD SULTHAN ALFARISY

NIM.1710817210013



**PROGRAM STUDI TEKNOLOGI INFORMASI
FAKULTAS TEKNIK
UNIVERSITAS LAMBUNG MANGKURAT
BANJARMASIN**

2024

**ANALISIS KEAMANAN JARINGAN DENGAN *HYBRID INTRUSION
DETECTION SYSTEM, FIREWALL, DAN VISUALISASI LOG ATTACKER***

TUGAS AKHIR

Diajukan Untuk Memenuhi Salah Satu Syarat
Sarjana Strata-1 *Teknologi Informasi*

Oleh:

MUHAMMAD SULTHAN ALFARISY

NIM.1710817210013



**PROGRAM STUDI TEKNOLOGI INFORMASI
FAKULTAS TEKNIK
UNIVERSITAS LAMBUNG MANGKURAT
BANJARMASIN, OKTOBER 2024**

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Muhammad Sulthan Alfarisy
NIM : 1710817210013
Fakultas : Teknik
Program Studi : Teknologi Informasi
Judul Tugas Akhir : Analisis Keamanan Jaringan Dengan *Hybrid Intrusion Detection System*, *Firewall*, dan *Visualisasi Log Attacker*
Pembimbing Utama : Andry Fajar Zulkarnain, S.ST., M.T.
Pembimbing Pendamping : Ir. Eka Setya Wijaya, S.T., M.Kom.

Dengan ini saya menyatakan bahwa dalam Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar akademik di suatu perguruan tinggi, dan sepanjang pengetahuan saya, juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar rujukan.

Banjarmasin, 11 Oktober 2024



Muhammad Sulthan Alfarisy

NIM. 1710817210013

LEMBAR PENGESAHAN

SKRIPSI PROGRAM STUDI S-1 TEKNOLOGI INFORMASI

**Analisis Keamanan Jaringan Dengan *Hybrid Intrusion Detection System, Firewall,*
Dan Visualisasi *Log Attacker***

Oleh

Muhammad Sulthan Alfariy (1710817210013)

Telah dipertahankan di depan Tim Penguji pada 25 Juni 2024 dan dinyatakan

L U L U S

Komite Penguji :

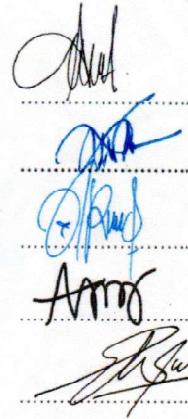
Ketua : Muti'a Maulida, S.Kom., M.T.I.
NIP 198810272019032013

Anggota 1 : Dr. Ir. Yuslena Sari, S.Kom., M.Kom., IPM.
NIP 198411202015042002

Anggota 2 : Nurul Fathanah Mustamin, S.Pd., M.T.
NIP 199110252019032108

Pembimbing Utama : Andry Fajar Zulkarnain, S.ST., M.T.
NIP 199007272019031018

Pembimbing Pendamping : Ir. Eka Setya Wijaya, S.T., M.Kom.
NIP 198205082008011010



Banjarbaru, 11 OCT 2024
diketahui dan disahkan oleh:

**Wakil Dekan Bidang Akademik
Fakultas Teknik ULM,**



Dr. Mahmud, S.T., M.T.
NIP 197401071998021001

**Koordinator Program Studi
S-1 Teknologi Informasi,**



Andreyan Rizky Baskara, S.Kom., M.Kom.
NIP 199307032019031011

PERSETUJUAN TUGAS AKHIR

ANALISIS KEAMANAN JARINGAN DENGAN *HYBRID INTRUSION
DETECTION SYSTEM, FIREWALL, DAN VISUALISASI LOG ATTACKER*

OLEH

MUHAMMAD SULTHAN ALFARISY

NIM. 1710817210013

Telah diperiksa dan terpenuhi semua persyaratan akademik, administrasi, dan
disetujui untuk dipertahankan di hadapan dewan penguji

Banjarmasin, 14 Juni 2024

Pembimbing Utama,



Andry Fajar Zulkarnain, S.ST., M.T.

NIP. 199007272019031018

Pembimbing Pendamping,



Ir. Eka Setya Wijaya, S.T., M.Kom.

NIP. 198205082008011010

ABSTRAK

Era digital saat ini memberikan kemudahan bagi masyarakat di berbagai sektor, terutama dalam akses informasi yang dapat diperoleh dari banyak sumber di internet. Namun, kebebasan berinternet juga menyebabkan meningkatnya kejahatan siber yang menjadi masalah serius. Menurut laporan monitoring dari Badan Siber dan Sandi Negara (BSSN), Indonesia mengalami total 2.479.875.997 anomali serangan siber antara Januari 2021 hingga Agustus 2022. Dengan banyaknya kasus serangan tersebut, diperlukan sistem yang efektif untuk mendeteksi, mencegah, dan memantau jaringan komputer. Penelitian ini menerapkan sistem *hybrid Intrusion Detection System* (IDS) yang menggunakan OSSEC dan Suricata, serta menggunakan Elastic Stack untuk manajemen *log* untuk *monitoring server*. Hasil penelitian menunjukkan bahwa sistem IDS hybrid ini mampu mendeteksi semua jenis serangan yang diuji, termasuk *port scanning*, *brute force*, *SQL injection*, dan *denial of service* (DoS). Selain itu, sistem ini juga dapat memblokir akses serangan dengan memanfaatkan fitur *firewall* seperti Iptables. Hasil deteksi dari IDS *hybrid* berhasil divisualisasikan menggunakan Elastic Stack, menunjukkan efektivitas sistem dalam meningkatkan keamanan jaringan komputer.

Kata Kunci: *Intrusion Detection System* (IDS), OSSEC, Suricata, *Firewall*, Elastic Stack

ABSTRACT

The current digital era provides convenience for people in various sectors, especially in accessing information that can be obtained from many sources on the internet. However, the freedom of the internet has also led to an increase in cybercrime, which has become a serious problem. According to a monitoring report from the National Cyber and Crypto Agency (BSSN), Indonesia experienced a total of 2,479,875,997 cyber attack anomalies between January 2021 and August 2022. With so many cases of these attacks, an effective system is needed to detect, prevent, and monitor computer networks. This research implements a hybrid Intrusion Detection System (IDS) system that uses OSSEC and Suricata, and uses Elastic Stack for log management for server monitoring. The results show that this hybrid IDS system is able to detect all types of attacks tested, including port scanning, brute force, SQL injection, and denial of service (DoS). In addition, this system can also block attack access by utilizing firewall features such as Iptables. The detection results of the hybrid IDS were successfully visualized using Elastic Stack, demonstrating the effectiveness of the system in improving computer network security.

Keywords: Intrusion Detection System (IDS), OSSEC, Suricata, Firewall, Elastic Stack

HALAMAN PERSEMBAHAN

Tugas Akhir ini saya persembahkan untuk:

1. Keluarga tercinta yang selama ini sangat membantu memberikan dukungan dan senantiasa mendoakan saya dalam keberlangsungan penyelesaian Tugas Akhir ini.
2. Bapak Andry Fajar Zulkarnain, S.ST., M.T. selaku Dosen Pembimbing Utama dan Bapak Ir. Eka Setya Wijaya, S.T., M.Kom. selaku Dosen Pembimbing Pendamping yang selalu meluangkan waktunya untuk memberi arahan, bimbingan, dan dukungan kepada saya dari awal hingga akhir penyelesaian Tugas Akhir ini.
3. Seluruh Dosen beserta Staf Program Studi *Teknologi Informasi* yang turut membantu dan mengarahkan serta memberikan semangat kepada saya selama proses penyelesaian Tugas Akhir.
4. Teman-teman seperjuangan dari masa perkuliahan sampai Tugas Akhir ini dan seluruh teman-teman Angkatan 2017 Program Studi *Teknologi Informasi* serta kakak tingkat dan adik tingkat lainnya yang selalu memberikan dukungan, motivasi, kritik dan saran agar saya mempunyai upaya untuk melakukan penyelesaian Tugas Akhir.
5. Seluruh pihak yang sudah membantu dalam penyelesaian Tugas Akhir.
6. Serta persembahkan kepada diri saya sendiri yang sudah bertahan dan berjuang sampai sejauh ini.

KATA PENGANTAR

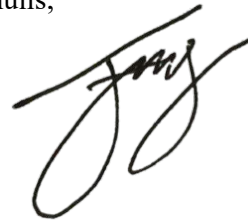
Puji syukur kehadiran Allah SWT, Tuhan Yang Maha Pengasih lagi Maha Penyayang yang telah memberikan kita berbagai macam nikmat dan rezeki, sehingga semua cita-cita serta harapan yang ingin kita capai menjadi lebih mudah dan bermanfaat untuk orang banyak. Sholawat dan salam tidak lupa penulis sampaikan kepada junjungan kita Nabi Besar Muhammad SAW yang telah membawa kita ke jalan yang terang benderang. Selain itu, atas limpahan rahmat serta karunia dari Allah SWT, penulis dapat menyelesaikan Tugas Akhir ini dengan Judul: “Analisis Keamanan Jaringan Dengan *Hybrid Intrusion Detection System, Firewall, dan Visualisasi Log Attacker*”. Tugas Akhir ini disusun dalam rangka memenuhi salah satu syarat untuk memperoleh gelar Sarjana Strata-1 Teknologi Informasi di Fakultas Teknik Universitas Lambung Mangkurat, Banjarmasin. Dalam kesempatan ini penulis menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Rektor Universitas Lambung Mangkurat, Bapak Prof. Dr. Ahmad, S.E., M.Si. yang memimpin dan memajemen jalannya seluruh perkuliahan yang ada di Universitas Lambung Mangkurat.
2. Dekan Fakultas Teknik, Bapak Prof. Dr. Ir. Irphan Fitriani Radam, S.T., M.T., IPU yang memberikan layanan terbaik dalam perkuliahan, terkhusus pada pelaksanaan Tugas Akhir di lingkungan Fakultas Teknik.
3. Ketua Program Studi Teknologi Informasi Bapak Andreyan Rizky Baskara S.Kom, M.Kom. yang telah memberikan arahan dan Solusi dalam penyelesaian Tugas Akhir.
4. Pembimbing Utama, Bapak Andry Fajar Zulkarnain yang telah bersedia membimbing, meluangkan waktu, dan memberikan arahan kepada penulis dalam penyelesaian Tugas Akhir ini.
5. Pembimbing Pendamping, Bapak Ir. Eka Setya Wijaya, S.T., M.Kom. yang telah memberikan waktu, pengarahan, dan saran kepada penulis dalam penyelesaian Tugas Akhir ini.
6. Dosen-dosen beserta staf dan teman-teman di Program Studi Teknologi Informasi yang telah membantu dalam proses penyelesaian Tugas Akhir.

Akhir kata, penulis menyampaikan terima kasih kepada semua pihak yang turut membantu dalam penyelesaian Tugas Akhir ini. Harapan yang paling besar dari penyusunan laporan ini adalah, semoga apa yang penulis susun bermanfaat, baik untuk pribadi, teman-teman, serta pembaca. Penulis juga mengharapkan saran dan kritik demi perbaikan dan penyempurnaan laporan ini. Semoga laporan ini dapat bermanfaat bagi para pembaca dan semua pihak yang membutuhkan.

Banjarmasin, 11 Oktober 2024

Penulis,

A handwritten signature in black ink, appearing to be 'Muhammad Sulthan Alfarisy', written in a cursive style.

Muhammad Sulthan Alfarisy

DAFTAR ISI

HALAMAN SAMPUL LUAR	i
HALAMAN SAMPUL DALAM	ii
LEMBAR PERNYATAAN	iii
LEMBAR PENGESAHAN	Kesalahan! Bookmark tidak ditentukan.
PERSETUJUAN TUGAS AKHIR	v
ABSTRAK	vi
<i>ABSTRACT</i>	vii
HALAMAN PERSEMBAHAN	viii
KATA PENGANTAR	ix
DAFTAR ISI	xi
DAFTAR TABEL	xiv
DAFTAR GAMBAR	xv
DAFTAR RIWAYAT HIDUP	xvii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	4
1.3 Batasan Masalah	4
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	5
BAB II TINJAUAN PUSTAKA	6
2.1 Penelitian Terkait	6
2.1.1 Deteksi Ancaman Keamanan Pada <i>Server</i> dan Jaringan Menggunakan OSSEC	6
2.1.2 Implementasi Intrusion Detection System (IDS) Suricata dan Management Log ELK Stack Untuk Pendeteksian Kegiatan Mining... 7	7
2.1.3 Implementasi <i>Intrusion Prevention System</i> (IPS) OSSEC dan Honeypot Cowrie	7
2.1.4 Penerapan Sistem Keamanan Jaringan Menggunakan <i>Intrusion Prevention System</i> Berbasis Suricata	8
2.1.5 Penerapan <i>Intrusion Prevention System</i> (IPS) Suricata Sebagai Pengamanan Dari Serangan <i>Distributed Denial of Service</i> (DDoS)..... 8	8
2.2 Landasan Teori	12
2.2.1 Keamanan Jaringan	12

2.2.2 <i>Intrusion Detection System (IDS)</i>	12
2.2.3 Firewall.....	13
2.2.4 <i>Log Management System</i>	13
2.2.5 OSSEC.....	14
2.2.6 Suricata.....	16
2.2.7 Iptables.....	16
2.2.8 Elasticsearch.....	16
2.2.9 Kibana.....	17
2.2.10 <i>Port Scanning</i>	17
2.2.11 <i>Brute Force</i>	17
2.2.12 <i>SQL Injection</i>	17
2.2.13 <i>Denial of Service (DoS)</i>	18
2.3 Kerangka Pemikiran.....	18
BAB III METODOLOGI PENELITIAN.....	20
3.1 Alat dan Bahan.....	20
3.2 Teknik Pengumpulan Data.....	22
3.3 Alur Penelitian.....	22
3.4 Rancangan Topologi Jaringan.....	24
3.5 Metode Pengujian.....	26
3.5.1 <i>Port Scanning</i>	26
3.5.2 <i>Brute Force</i>	26
3.5.3 <i>SQL Injection</i>	26
3.5.4 <i>Denial-of-Service (DoS)</i>	27
3.6 Skenario Pengujian.....	27
BAB IV HASIL DAN PEMBAHASAN.....	30
4.1 Implementasi.....	30
4.1.1 Suricata.....	30
4.1.2 OSSEC.....	33
4.1.3 Elastic Stack (Elasticsearch dan Kibana).....	36
4.1.5 Filebeat.....	40
4.2 Pengujian.....	42
4.2.1 Serangan <i>Port Scanning</i> ke 1.....	43
4.2.2 Serangan <i>Brute Force</i> ke 1.....	44
4.2.3 Serangan <i>SQL Injection</i> ke 1.....	46

4.2.4 Serangan <i>Denial of Service</i> (DoS) ke 1.....	48
4.2.5 Serangan <i>Port Scanning</i> ke 2	51
4.2.6 Serangan Brute Force ke 2	53
4.2.7 Serangan <i>SQL Injection</i> ke 2	55
4.2.8 Serangan <i>Denial of Service</i> (DoS) ke 2.....	57
4.2.9 Serangan <i>Port Scanning</i> ke 3	59
4.2.10 Serangan <i>Brute Force</i> ke 3.....	60
4.2.11 Serangan <i>SQL Injection</i> ke 3	61
4.2.12 Serangan <i>Denial of Service</i> (DoS) ke 3.....	62
4.3 Analisis Hasil Penelitian	65
4.3.1 Analisis Serangan <i>Port Scanning</i>	65
4.3.2 Analisis Serangan Brute Force.....	67
4.3.3 Analisis Serangan <i>SQL Injection</i>	69
4.3.4 Analisis Serangan <i>Denial of Service</i> (DoS)	71
4.4 Evaluasi Hasil Penelitian.....	73
BAB V KESIMPULAN DAN SARAN.....	76
5.1 Kesimpulan	76
5.2 Saran.....	77
DAFTAR PUSTAKA	78
LAMPIRAN.....	82

DAFTAR TABEL

Tabel 2.1 Penelitian Terkait	10
Tabel 2.2 Klasifikasi rules OSSEC	14
Tabel 3.1 Alat dan Bahan.....	20
Tabel 3.2 Pengalamatan Jaringan.....	25
Tabel 3.3 Perintah Simulasi Serangan	27
Tabel 4.1 Hasil Pengujian <i>Port Scanning</i>	66
Tabel 4.2 Hasil Pengujian Brute Force SSH.....	68
Tabel 4.3 Hasil Pengujian SQL Injection	70
Tabel 4.4 Hasil Pengujian Denial of Service (DoS)	72
Tabel 4.5 Hasil Pengujian Serangan	73

DAFTAR GAMBAR

Gambar 1.1 Laporan anomali nasional Januari 2021 - Agustus 2022	2
Gambar 2.1 Kerangka Pemikiran.....	19
Gambar 3.1 Alur Penelitian.....	23
Gambar 3.2 Rancangan Topologi Jaringan.....	25
Gambar 4.1 Instalasi Suricata	30
Gambar 4.2 Suricata Running	31
Gambar 4.3 Konfigurasi Suricata yml Bagian Address-Groups.....	31
Gambar 4.4 Konfigurasi Suricata yml Bagian Af-Packet.....	31
Gambar 4.5 Konfigurasi Suricata yml Bagian Rule-Files	32
Gambar 4.6 rules suricata pada custom.rules.....	32
Gambar 4.7 Suricata running IPS mode.....	33
Gambar 4.8 Mengunduh OSSEC	33
Gambar 4.9 OSSEC Running.....	34
Gambar 4.10 Proses menambahkan agen pada manage_agents	34
Gambar 4.11 Extract Key Untuk Agent OSSEC	35
Gambar 4.12 Import Key OSSEC Agent Manager.....	35
Gambar 4.13 Konfigurasi ossec.conf.....	36
Gambar 4.14 konfigurasi active response pada ossec.conf.....	36
Gambar 4.15 Penambahan Sumber Dan Package Elastic Stack	37
Gambar 4.16 Instalasi Elastic Stack.....	37
Gambar 4.17 Konfigurasi Elasticsearch.....	38
Gambar 4.18 Elasticsearch Running	38
Gambar 4.19 Tampilan Elasticsearch di CLI (Command Line Interface).....	39
Gambar 4.20 Konfigurasi Kibana	39
Gambar 4.21 Kibana Running	40
Gambar 4.22 Tampilan Kibana Di Web Browser	40
Gambar 4.23 Instalasi Filebeat.....	41
Gambar 4.24 Konfigurasi Elasticsearch Di Dalam Filebeat	41
Gambar 4.25 Konfigurasi Kibana Di Dalam Filebeat.....	42
Gambar 4.26 Konfigurasi Log OSSEC Di Dalam Filebeat.....	42
Gambar 4.27 Perintah Enable Modules Pada Filebeat.....	42
Gambar 4.28 Pengujian Port Scanning ke 1 Menggunakan Nmap	43
Gambar 4.29 Hasil Monitoring OSSEC Terhadap Serangan Port Scanning ke 1	44
Gambar 4.30 Hasil Monitoring Suricata Terhadap Serangan Port Scanning ke 1	44
Gambar 4.31 Pengujian Serangan SSH Brute Force ke 1 Menggunakan Hydra ..	45
Gambar 4.32 Hasil Visualisasi Log Serangan SSH Brute Force OSSEC ke 1	46
Gambar 4.33 Hasil Visualisasi Log Serangan SSH Brute Force Suricata ke 1 ...	46
Gambar 4.34 Pengujian SQL Injection ke 1 Menggunakan Sqlmap	47

Gambar 4.35 Informasi Users Yang Didapatkan Oleh Penyerang	47
Gambar 4.36 Hasil Visualisasi <i>Log</i> OSSEC Serangan SQL Injection ke 1.....	48
Gambar 4.37 Hasil Visualisasi <i>Log</i> Suricata Serangan SQL Injection ke 1.....	48
Gambar 4.38 Pengujian Denial Of Service (Dos) ke 1 Menggunakan Slowhttptest	49
Gambar 4.39 Grafik Serangan DoS Slowhttptest	49
Gambar 4.40 Hasil Visualisasi <i>Log</i> OSSEC Serangan Denial Of Service (DoS) ke 1.....	50
Gambar 4.41 Hasil Visualisasi <i>Log</i> Suricata Serangan Denial Of Service (DoS) ke 1.....	51
Gambar 4.42 Pengujian <i>Port Scanning</i> ke 2 Menggunakan Nmap	52
Gambar 4.43 Hasil Visualisasi <i>Log</i> OSSEC Serangan <i>Port Scanning</i> ke 2	53
Gambar 4.44 Hasil Visualisasi <i>Log</i> Suricata Serangan <i>Port Scanning</i> ke 2.....	53
Gambar 4.45 Pengujian SSH Brute Force ke 2 Menggunakan Hydra.....	53
Gambar 4.46 Visualisasi <i>Log</i> OSSEC Serangan SSH Brute Force ke 2.....	54
Gambar 4.47 Visualisasi <i>Log</i> Suricata Serangan SSH Brute Force ke 2.....	55
Gambar 4.48 Pengujian SQL Injection ke 2 Menggunakan Sqlmap	55
Gambar 4.49 Visualisasi <i>Log</i> OSSEC Serangan SQL Injection ke 2	56
Gambar 4.50 Visualisasi <i>Log</i> Suricata Serangan SQL Injection ke 2.....	57
Gambar 4.51 Pengujian Denial of Service (DoS) ke 2 Menggunakan Slowhttptest	57
Gambar 4.52 Grafik Serangan DoS Slowhttptest Dengan Kondisi IPS OSSEC Aktif	57
Gambar 4.53 Hasil Visualisasi <i>Log</i> OSSEC Serangan DoS ke 2	59
Gambar 4.54 Hasil Visualisasi <i>Log</i> Suricata Serangan DoS ke 2	59
Gambar 4.55 Pengujian <i>Port Scanning</i> ke 3 Menggunakan Nmap	60
Gambar 4.56 Tampilan Drop Suricata Terhadap Serangan <i>Port Scanning</i>	60
Gambar 4.57 Pengujian Serangan SSH Brute Force ke 3 Menggunakan Hydra..	61
Gambar 4.58 Tampilan Drop Suricata Terhadap Serangan SSH Brute Force.....	61
Gambar 4.59 Pengujian Serangan SQL Injection ke 3 Menggunakan Sqlmap	62
Gambar 4.60 Tampilan Drop Suricata Terhadap Serangan SQL Injection	62
Gambar 4.61 Pengujian Serangan Denial of Service (DoS) ke 3 Menggunakan Slowhttptest.....	63
Gambar 4.62 Tampilan Drop Suricata Terhadap Serangan DoS	64
Gambar 4.63 Grafik Serangan DoS Slowhttptest Dengan Kondisi IPS Suricata Aktif	64