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

TUGAS AKHIR

Oleh:

MUHAMMAD SULTHAN ALFARISY
NIM.1710817210013

PROGRAM STUDI TEKNO*LOGI* 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 Tekno*log*i Informasi

Oleh:
MUHAMMAD SULTHAN ALFARISY
NIM.1710817210013

PROGRAM STUDI TEKNO*LOG*I 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	:	Tekno*log*i 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 Alfarisy (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 Tekno*log*i 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 Tekno*log*i Informasi serta kaka 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 persembahan kepada diri saya sendiri yang sudah bertahan dan berjuang sampai sejauh ini.

KATA PENGANTAR

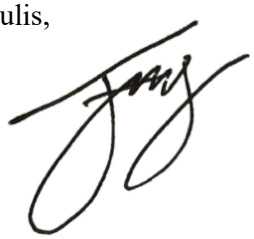
Puji syukur kehadirat Allah SWT, Tuhan Yang Maha Pengasih lagi Maha Penyayang yang telah memberikan kita berbagai macam nikmat dan rezeki, sehingga semua cita-cita serta harapan yang ingin kita capai menjadi lebih mudah dan bermanfaat untuk orang banyak. Sholawat dan salam tidak lupa penulis sampaikan 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 Tekno*log*i 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 memanajemen jalannya seluruh perkuliahan yang ada di Universitas Lambung Mangkurat.
2. Dekan Fakultas Teknik, Bapak Prof. Dr. Ir. Irphan Fitrian 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 Tekno*log*i 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 Tekno*log*i 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,



Muhammad Sulthan Alfarisy

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR