IMPLEMENTASI SISTEM MONITORING KEAMANAN JARINGAN BERBASIS SURICATA DAN ELASTIC STACK DI INSTANSI ABC

TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer

ALFREDO JULIANSA SITOHANG

1202921003

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK ILMU KOMPUTER

UNIVERSITAS BAKRIE

JAKARTA

2023

HALAMAN PERNYATAAN ORISINALITAS

Tugas Akhir adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Alfredo Juliansa Sitohang

NIM : 1202921003

Tanda Tangan : 

Tanggal : 20 Juli 2023

HALAMAN PENGESAHAN

Tugas Akhir ini diajukan oleh:

Nama	:	Alfredo Juliansa Sitohang
NIM	:	1202921003
Program Studi	:	Informatika
Fakultas	:	Fakultas Teknik dan Ilmu Komputer
Judul Skripsi	:	Implementasi Sistem Monitoring Keamanan Jaringan Berbasis Suricata dan Elastic Stack di Instansi ABC

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer (S.Kom) pada Program Studi Informatika Fakultas Teknik dan Ilmu Komputer Universitas Bakrie.

DEWAN PENGUJI

Pembimbing I	: Prof. Dr. Hoga Saragih, S.T, M.T	( )
Pembimbing II	: Ihsan Ibrahim, S.T, M.T	( )
Penguji I	: Iwan Adhicandra, SMIEEE, MIET, MBCS	( )
Penguji II	: Albert Sembiring, S.T, M.T	( )
Ditetapkan di	: Jakarta	
Tanggal	: 20 Juli 2023	

UCAPAN TERIMA KASIH

Puji dan syukur kehadirat Tuhan Yang Maha Esa karena telah memberikan berkat dan kasihya dalam pembuatan tugas akhir yang berjudul "Implementasi Sistem Monitoring Keamanan Jaringan Berbasis Suricata dan Elastic Stack di Instansi ABC" sehingga penelitian ini dapat diselesaikan. Penyusunan tugas akhir ini tidak terlepas dari berbagai kesulitan, rintangan, dan hambatan dari awal hingga akhir penyusunan. Oleh karena itu, dengan segala hormat dan kerendahan hati, penulis mengungkapkan terima kasih kepada:

1. Bapak dan Mama serta saudara yang selalu memberikan dukungan dan semangat untuk menyelesaikan penelitian ini.
2. Bapak Prof. Dr. Hoga Saragih S.T., M.T selaku pembimbing I yang telah mendukung dan membantu dalam menyelesaikan penelitian ini
3. Bapak Ihsan Ibrahim S.T., M.T selaku pembimbing II yang telah meluangkan banyak waktunya dalam menjawab pertanyaan saya mengenai penelitian dan membantu dalam penyelesaiaan penelitian.
4. Bapak Iwan Adichandra, MIEE, MIET, MBCS selaku pembahas I dan Kepala Program Studi Informatika yang memberikan masukan terhadap penulisan saya.
5. Bapak Albert A. Sembiring, S.T, M.T selaku pembahas II yang memberikan saran dan masukan terhadap penelitian saya.
6. Bang Alfonso Brolin Sihite, S.Tr.TP, M.T selaku senior saya yang selalu memberikan referensi, saran dan bantuan dalam menyelesaikan penelitian ini.
7. Silvia Veronika Nababan, S.E selaku pacar yang selalu mendengarkan keluh kesah saya serta memberikan dukungan dan semangat untuk menyelesaikan penelitian ini.
8. Bang Khairil, Bang Anton, dan Mas Lingga Maulana selaku senior yang selalu memberikan referensi, saran dan bantuan dalam menyelesaikan penelitian ini.
9. Senior dan rekan-rekan SOC yang telah memberikan dukungan dan fasilitas untuk menyelesaikan penelitian ini.

10. Seluruh Dosen Informatika yang telah memberikan ilmunya semasa kuliah sehingga saya mendapatkan berbagai pengetahuan yang dapat saya cantumkan dalam penelitian ini.
11. Teman –teman Informatika khususnya kelas karyawan yang yang telah memberikan dukungan untuk menyelesaikan penelitian ini.
12. Seluruh pihak Universitas Bakrie yang terlibat langsung maupun tidak langsung yang telah memberikan bantuan, dukungan dan fasilitas yang sangat membantu selama masa perkuliahan.

Semoga Tuhan Yang Maha Esa selalu memberikan keberkahan dan rahmatnya untuk kita semua dan semoga tugas akhir ini memberikan manfaat kepada berbagai pihak khususnya di bidang Keamanan Siber.

Jakarta, 20 Juli 2023

Penulis,

Alfredo Juliansa Sitohang

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI

Sebagai sivitas akademik Universitas Bakrie, saya yang bertanda tangan di bawah ini:

Nama : Alfredo Juliansa Sitohang

NIM : 1202921003

Program Studi : Informatika

Fakultas : Teknik dan Ilmu Komputer

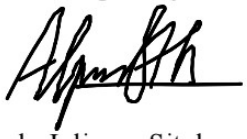
Dengan pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Bakrie Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-free Right*) atas karya ilmiah sata yang berjudul:

" Implementasi Sistem Monitoring Keamanan Jaringan Berbasis Suricata dan Elastic Stack di Instansi ABC "

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Bakrie berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta untuk kepentingan akademis.

Demikian pernyataan ini saya buat sebenarnya.
Dibuat di : Jakarta
Pada tanggal : 20 Juli 2023

Yang Menyatakan



(Alfredo Juliansa Sitohang)

IMPLEMENTASI SISTEM MONITORING KEAMANAN JARINGAN
BERBASIS SURICATA DAN ELASTIC STACK
DI INSTANSI ABC

Alfredo Juliansa Sitohang

ABSTRAK

Instansi ABC merupakan instansi pemerintah yang terdiri dari masing-masing unit kerja, dimana salah satu unit kerja memiliki tugas dalam pengamanan jaringan. Instansi ABC membentuk tim *Security Operation Center* (SOC) dalam menyelenggarakan pengamanan jaringan yang memiliki salah satu tugas yaitu melakukan monitoring *traffic* jaringan. Tim SOC mengalami kesulitan dalam mendeteksi dan menganalisis anomali *traffic* sehingga membutuhkan sistem monitoring keamanan jaringan yang dapat mendeteksi anomali *traffic* yang berpotensi menjadi serangan siber. Anomali *traffic* dan serangan siber dapat dideteksi menggunakan *Intrusion Detection System* (IDS) dengan metode pendeteksian yaitu *signature-based*. Pada penelitian ini dilakukan implementasi sistem monitoring keamanan jaringan yang terdiri dari IDS Suricata dan *Security Information and Event Management* (SIEM) yang terdiri dari Elasticsearch, Filebeat, dan Kibana dari Elastic Stack. Dari penelitian yang telah dilakukan dihasilkan bahwa sistem monitoring keamanan jaringan berbasis Suricata dan Elastic Stack dapat mendeteksi serangan siber berupa SQL *injection* dan *Cross Site Scripting* (XSS) dan menghasilkan sebuah visualisasi dalam bentuk Dashboard dan Discover sehingga mempermudah tim SOC dalam mendeteksi dan menganalisis anomali *traffic* dan serangan siber. Dari penelitian yang telah dilakukan dihasilkan bahwa penerapan *rules default* Suricata dengan penambahan *rules custom* lebih efektif dalam mendeteksi berbagai serangan SQL *injection* dan XSS dibandingkan dengan hanya penerapan *rules default* Suricata.

Kata Kunci: Serangan Siber, Suricata, Elastic Stack, SQL *Injection*, XSS.

IMPLEMENTATION OF NETWORK SECURITY MONITORING SYSTEM
BASED ON SURICATA AND ELASTIC STACK
AT ABC AGENCY

Alfredo Juliansa Sitohang

ABSTRACT

ABC agency is a government agency consisting of each work unit, where one of the work units has duties in network security. ABC agency formed a Security Operation Center (SOC) team in organizing network security which has one of the tasks of monitoring network traffic. The SOC team has difficulty detecting and analyzing traffic anomalies, so they need a network security monitoring system that can detect traffic anomalies that have the potential to become cyber attacks. Traffic anomalies and cyber attacks can be detected using an Intrusion Detection System (IDS) with a detection method that is signature-based. In this research, a network security monitoring system consisting of IDS Suricata and Security Information and Event Management (SIEM) consisting of Elasticsearch, Filebeat, and Kibana from Elastic Stack was implemented. From the research that has been done, it is found that the network security monitoring system based on Suricata and Elastic Stack can detect cyber attacks in the form of SQL injection and Cross Site Scripting (XSS) and produce a visualization in the form of Dashboard and Discover, making it easier for the SOC team to detect and analyze traffic anomalies and cyber attacks. From the research that has been done, it is found that the application of Suricata default rules with the addition of custom rules is more effective in detecting various SQL injection and XSS attacks compared to only applying Suricata default rules.

Keywords: Cyber Attacks, Suricata, Elastic Stack, SQL Injection, XSS.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL