STT TERPADU
NURUL FIKRI

SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

PERANCANGAN DAN IMPLEMENTASI DASHBOARD MONITORING DAN ANALISIS SERANGAN APLIKASI WEB MENGGUNAKAN ELK STACK

TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer

MUHAMMAD ILHAM
0110217025

PROGRAM STUDI TEKNIK INFORMATIKA
DEPOK
MARET 2023

HALAMAN PERNYATAAN ORISINALITAS

Tugas aAkhir ini adalah hasil karya penulis,
dan semua sumber baik yang dikutip maupun dirujuk
telah saya nyatakan dengan benar.

Nama	**: Muhammad Ilham**
NIM	**: 0110217025**
Tanda Tangan	**: .....**
Tanggal	**: .....**

HALAMAN PENGESAHAN

Tugas Akhir ini diajukan oleh :

Nama	: Muhammad Ilham
NIM	: 0110217025
Program Studi	: Teknik Informatika
Judul Tugas Akhir	: Perancangan dan Implementasi Dashboard Monitoring Serangan Aplikasi Web Menggunakan ELK Stack

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Teknik Informatika, Sekolah Tinggi Teknologi Terpadu Nurul Fikri

DEWAN PENGUJI

Pembimbing I

Henry Saptono, S.Si. M.Kom.

Penguji

Ahmad Rio Adriansyah, S.Si. M.Si.

Ditetapkan di : Depok
Tanggal : **.....**

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT, karena atas berkat dan rahmat-Nya, penulis dapat menyelesaikan Tugas Akhir ini. Penulisan tugas akhir ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana komputer Program Studi Teknik Informatika pada Sekolah Tinggi Teknologi Terpadu Nurul Fikri Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan tugas akhir ini, sangatlah sulit bagi penulis untuk menyelesaikan tugas akhir ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Allah SWT.
2. Orang tua dan semua anggota keluarga yang telah memberikan dorongan baik secara moril maupun materil dalam penyelesaian tugas ini.
3. Bapak Dr. Lukman Rosyidi, M.T., M.M. selaku Ketua Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
4. Ibu Tifanny Nabarian., S.Kom., M.T.I. selaku Ketua Program Studi Teknik Informatika Sekolah Tinggi Teknologi Terpadu Nurul Fikri.
5. Bapak Henry Saptono., S.Si., M.Kom selaku Dosen Pembimbing Akademik yang telah membimbing penulis selama berkuliah di Sekolah Tinggi Teknologi Terpadu Nurul Fikri dan selaku Dosen Pembimbing Tugas Akhir penulis dalam menyelesaikan penulisan ilmiah ini.
6. Para Dosen di lingkungan Sekolah Tinggi Teknologi Terpadu Nurul Fikri yang telah membimbing penulis dalam menuntut ilmu yang telah diberikan.
7. Seluruh pihak yang telah membantu secara langsung maupun tidak langsung, yang tidak dapat penulis sertakan satu persatu namun tidak mengurangi rasa terima kasih penulis.
8. Teman-teman Sekolah Tinggi Teknologi Terpadu Nurul Fikri yang telah mendukung penulis dalam menyelesaikan penulisan ilmiah ini.

Dalam penulisan ilmiah ini tentu saja masih banyak terdapat kekurangan-kekurangan yang mungkin disebabkan oleh keterbatasan kemampuan dan pengetahuan yang

penulis miliki. Walaupun demikian, penulis telah berusaha menyelesaikan penulisan ilmiah ini sebaik mungkin. Oleh karena itu apabila terdapat kekurangan di dalam penulisan ilmiah ini, dengan rendah hati penulis menerima kritik dan saran dari pembaca.

Akhir kata, penulis berharap Allah SWT berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga tugas akhir ini membawa manfaat bagi pengembangan ilmu.

Depok, 02 Maret 2023

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Sekolah Tinggi Teknologi Terpadu Nurul Fikri, saya yang bertanda tangan di bawah ini:

Nama : Muhammad Ilham
NIM : 0110217025
Program Studi : Teknik Informatika
Jenis karya : Tugas Akhir

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada STT-NF **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty - Free Right*)** atas karya ilmiah saya yang berjudul :

"Perancangan dan Implementasi Dashboard Monitoring Serangan Aplikasi Web Menggunakan ELK Stack"

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini STT-NF 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.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok
Pada tanggal : 08 Maret 2023

Yang menyatakan

(Muhammad Ilham)

ABSTRAK

Nama : Muhammad Ilham
NIM : 0110217025
Program Studi : Teknik Informatika
Judul : Perancangan dan Implementasi Dashboard Monitoring Serangan Aplikasi Web Menggunakan ELK Stack

Tugas akhir ini berfokus pada perancangan dan implementasi dashboard monitoring dan analisis serangan aplikasi web menggunakan ELK stack dan Snort. Tujuan dari penelitian ini adalah untuk membantu organisasi dalam mengidentifikasi dan memitigasi serangan pada aplikasi web yang terjadi di lingkungan mereka.Metode yang digunakan dalam penelitian ini meliputi pengumpulan data dari Snort IDS yang telah diimplementasikan pada jaringan, kemudian data tersebut diolah menggunakan logstash dan diproses oleh Elasticsearch. Kibana digunakan untuk membuat dashboard visualisasi data yang memudahkan analisis serangan aplikasi web yang terjadi pada jaringan.Dalam penelitian ini, berhasil dirancang dan diimplementasikan sebuah dashboard yang mampu memonitoring dan menganalisis serangan pada aplikasi web secara real-time. Dashboard ini dapat menampilkan informasi yang berguna bagi tim keamanan seperti jenis serangan dan sumber serangan.Hasil pengujian menunjukkan bahwa dashboard yang dirancang mampu mengidentifikasi serangan aplikasi web dengan akurasi yang cukup tinggi. Dashboard ini juga membantu tim keamanan untuk mengambil tindakan yang cepat dan efektif dalam menangani serangan yang terdeteksi.Secara keseluruhan, penelitian ini membuktikan bahwa penggunaan ELK stack dan Snort sebagai alat bantu monitoring dan analisis serangan aplikasi web dapat membantu organisasi dalam meningkatkan keamanan jaringan mereka. Diharapkan hasil dari penelitian ini dapat memberikan manfaat bagi organisasi dalam memperkuat sistem keamanan jaringan mereka terhadap serangan aplikasi web yang berbahaya.

Kata kunci : ELK, Elasticsearch, Kibana, Logstash, Snort

ABSTRACT

Name : Muhammad Ilham
NIM : 0110217025
Study Program : Informatics Engineering
Title : Design and Implementation of Monitoring Dashboard Web Application Attacks Using ELK Stack

This research focuses on designing and implementing a dashboard for monitoring and analyzing web application attacks using the ELK stack and Snort. The purpose of this research is to assist organizations in identifying and mitigating attacks on web applications that occur in their environment. The methods used in this research include collecting data from Snort IDS that has been implemented on the network, then the data is processed using logstash and processed by Elasticsearch. Kibana is used to create a data visualization dashboard that facilitates the analysis of web application attacks that occur on the network.In this study, a dashboard was successfully designed and implemented that is able to monitor and analyze attacks on web applications in real-time. This dashboard can display useful information for the security team such as the type of attack and the *source* of the attack.The test results show that the designed dashboard is able to identify web application attacks with a fairly high accuracy. Overall, this research proves that using ELK stack and Snort as a tool for monitoring and analyzing web application attacks can help organizations improve their network security. It is expected that the results of this research can benefit organizations in strengthening their network security systems against malicious web application attacks.

Key words : ELK, Elasticsearch, Kibana, Snort

DAFTAR ISI

HALAMAN PERNYATAAN ORISINALITAS ii
HALAMAN PENGESAHAN iii
KATA PENGANTAR iv
ABSTRAK vii
ABSTRACT viii
DAFTAR ISI ix
DAFTAR GAMBAR xi
DAFTAR TABEL xiii
BAB I 1
PENDAHULUAN 1
1.1 Latar belakang 1
1.2 Rumusan Masalah 2
1.3 Tujuan dan Manfaat Penelitian 2
1.4 Batasan Masalah 3
1.5 Sistematika Penulisan 3
BAB II 5
KAJIAN LITERATUR 5
2. 1 Landasan Teori 5
2. 2 Penelitian Terkait 23
2. 3 Table Penelitian Terkait 24
BAB III 29
METODOLOGI PENELITIAN 29
3.1 Tahapan Penelitian 29
3.2 Rancangan Penelitian 31
BAB IV 33
ANALISA DAN PERANCANGAN 33
4.1 Analisis Kebutuhan 33
4.2 Rancangan Sistem 35

4.3 Perancangan sistem fisik 36
4.4 Rancangan Visualisasi 37
4.5 Rancangan Pengujian 38
BAB V 43
IMPLEMENTASI DAN PENGUJIAN 43
5.1 Impementasi System 43
5.2 Persiapan 43
5.3 Update Repositori Ubuntu 44
5.4 Instalasi Perangakat IDS 44
5.5 Instalasi Komponen ELK Stack 50
5.6 Pengujian 55
BAB VI 75
KESIMPULAN DAN SARAN 75
6.1 Kesimpulan 75
6.2 Saran 76
Daftar Pustaka 77
Lampiran 78

DAFTAR GAMBAR

Gambar 2. 1 Snort Workflow 15
Gambar 2. 2 Sistem Dashboard Menggunakan Kibana 18
Gambar 2. 3 ELK Stack Workflow 20
Gambar 2. 4 Pipelining Logstash 22
Gambar 2. 5 Kibana Status Dashboard 23
Gambar 3. 1. Diagram Tahapan Penelitian. 29
Gambar 4. 1 Perancangan sistem dashboard monitoring Snort & ELK Stack 35
Gambar 4. 2 Perancangan sistem fisik 36
Gambar 5. 1 *Development* Program 43
Gambar 5. 2 *Status snort running* 46
Gambar 5. 3 *Snort network configure* 47
Gambar 5. 4 *Snort alert configure* 47
Gambar 5. 5 *Snort running with rule* 50
Gambar 5. 6 *Elasticsearch Configuratio* 51
Gambar 5. 7. *Kibana Configuration* 52
Gambar 5. 8 Kibana Dashboard Status 53
Gambar 5. 9 *Logstash Configuration* 54
Gambar 5. 10 *Snort Logstash Configuration* 54
Gambar 5. 11 *Logstash Pipeline Configuration* 55
Gambar 5. 12 *Snort receiving Logs SQL Injection* 56
Gambar 5. 13 *Attack Result Cross Site Scripting* 58
Gambar 5. 14 *Snort receiving Logs* XSS 58
Gambar 5. 15 Hasil pengujian serangan *Cross Site Scripting* 58
Gambar 5. 16 *Attacking Process DDOS* 59
Gambar 5. 17 *Snort receiving Logs DDOS* 59
Gambar 5. 18 *Location snort log file* 60
Gambar 5. 19 Index pattern dalam kibana 62
Gambar 5. 20 Discovery menu Kibana 62
Gambar 5. 21 Dashboard Security *Website* Monitoring ELK Stack 66
Gambar 5. 22 Variasi Serangan 67

Gambar 5. 23 Total Serangan..... 67
Gambar 5. 24 Sumber IP Penyerang..... 68
Gambar 5. 25 Negara Penyerang..... 68
Gambar 5. 26 Top Serangan..... 69
Gambar 5. 27 Kota Penyerang..... 69
Gambar 5. 28 Filter Dashboard..... 70

DAFTAR TABEL

Tabel 2. 1 Penelitian Terkait 24
Tabel 2. 2 Posisi Penelitian 27
Tabel 4. 1 Detail Software 32
Tabel 4. 2 Server Snort & ELK stack 34
Tabel 4. 3 Rancangan Visualisasi 37
Tabel 4. 4 Pengujian pendeteksian serangan *SQL Injection* 39
Tabel 4. 5 Pengujian pendeteksian serangan *Cross Site Scripting* 39
Tabel 4. 6 Pengujian pendeteksian serangan DDoS Attack 39
Tabel 4. 7 Rancangan Uji Efektivitas Penggunaan 41
Tabel 4. 8 Rancangan Uji Efektivitas Kelayakan 42
Tabel 5. 1 Tabel rule snort 48
Tabel 5. 2 Hasil pengujian serangan *SQL Injection* 57
Tabel 5. 3 Hasil pengujian serangan *Cross Site Scripting* 58
Tabel 5. 4 Hasil pengujian serangan *DDOS* 60
Tabel 5. 5 Hasil pengujian efektifitas 63
Tabel 5. 6 Hasil Uji Visualisasi 64
Tabel 5. 7 Hasil Uji Efektivitas Penggunaan 70
Tabel 5. 8 Hasil Uji Efektivitas Kelayakan 71
Tabel 5. 9 Deskripsi dan Bobot nilai kuesioner/survey 71
Tabel 5. 10 Persentase Hasil Uji Efektivitas Penggunaan 72
Tabel 5. 11 Persentase Hasil Uji Efektivitas Kelayakan 73
Tabel 5. 12 Interprestasi Penilaian Efektivitas 74