IMPLEMENTASI ELK STACK UNTUK PEMANTAUAN KEAMANAN SERVER PADA CV LANIS IT SUPPORT AND MAINTENANCE

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Informatika

disusun oleh

ACH. FAISAL CHOIRUL ISMAIL

16.11.0753

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

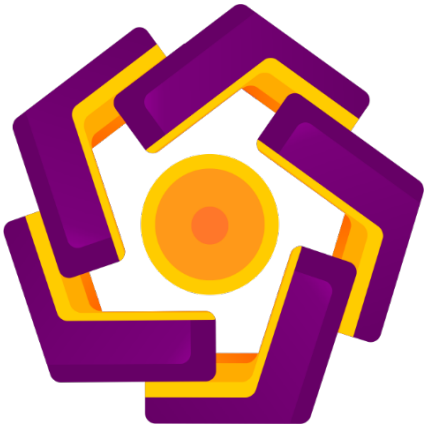
2023

IMPLEMENTASI ELK STACK UNTUK PEMANTAUAN KEAMANAN SERVER PADA CV LANIS IT SUPPORT AND MAINTENANCE

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Informatika



disusun oleh

ACH. FAISAL CHOIRUL ISMAIL

16.11.0753

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2023

HALAMAN PERSETUJUAN

SKRIPSI

IMPLEMENTASI ELK STACK UNTUK PEMANTAUAN KEAMANAN SERVER PADA CV LANIS IT SUPPORT AND MAINTENANCE

yang disusun dan diajukan oleh

Ach. Faisal Choirul Ismail

16.11.0753

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 1 maret 2023

Dosen Pembimbing,

Subektiningsih, S.Kom, M.Kom
NIK. 190302413

HALAMAN PENGESAHAN

SKRIPSI

IMPLEMENTASI ELK STACK UNTUK PEMANTAUAN KEAMANAN SERVER PADA CV LANIS IT SUPPORT AND MAINTENANCE

yang disusun dan diajukan oleh

Ach. Faisal Choirul Ismail

16.11.0753

Telah dipertahankan di depan Dewan Penguji
pada tanggal 1 maret 2023

Nama Penguji	Tanda Tangan
Arif Akbarul Huda, S.Si, M.Eng **NIK.** 190302287	
Anggit Ferdita Nugraha, S.T., M.Eng **NIK.** 190302480	
Subektiningsih, M.Kom **NIK.** 190302413	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 1 maret 2023

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Ach. Faisal Choirul Ismail
NIM : 16.11.0753

Menyatakan bahwa Skripsi dengan judul berikut:

Implementasi Elk Stack Untuk Pemantauan Keamanan Server Pada Cv Lanis It Support And Maintenance
Dosen Pembimbing : Subektiningsih, S.Kom, M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 1 maret 2023

Yang Menyatakan,

Ach. Faisal Choirul Ismail

HALAMAN PERSEMBAHAN

Segala puji syukur penulis penjatkan kepada Allah SWT, Yang Maha Kuasa dan telah memberikan berkah anugerahnya-Nya kepada penulis sehingga penulis mampu melaksanakan tugas untuk menyelesaikan skripsi ini dengan sebaik-baiknya.Saya juga sangat berterima kasih kepada orang-orang yang telah secara langsung maupun tidak langsung yang telah membantu saya dalam menyelesaikan skipsi ini.

Skripsi ini saya persembahkan kepada :

1. Almarhum kakek suja'i yang selalu memberikan kasih sayang dan juga doa yang tak ada batasnya.
2. Kedua orang tua Nurul Choiriyah dan nurtam dan juga adik perempuan Alsurotin dwi nur choirina yang selalu memberi dukungan finansial maupun dukungan lainnya. Semoga selalu dalam keadan sehat dan selalu dalam lindungan-Nya.
3. Nenek Maslikah yang selalu memberikan doa yang tak ada batasnya, semoga selalu dalam keadan sehat dan selalu dalam lindungan-Nya.
4. Ibu Subektiningsih, S.Kom, M.Kom selaku Dosen pembimbing yang sabar membimbing dan memberi masukan positif hingga skripsi ini dapat terselesaikan.
5. Serta semua pihak yang telah membantu serta mendukung saya yang tidak bisa saya sebutkan satu persatu.

KATA PENGANTAR

Segala puji syukur penulis penjatkan kepada Allah SWT, Yang Maha Kuasa dan telah memberikan berkah anugerahnya-Nya kepada penulis sehingga penulis mampu melaksanakan tugas untuk menyelesaikan skripsi ini dengan sebaik-baiknya.

Melalui proses dan tahap demi tahap dilalui sehingga penulis dapat menyelesaikan penulisan skripsi dengan judul "Implementasi Elk Stack Untuk Pemantauan Keamanan Server Pada Cv Lanis It Support And Maintenance" untuk memenuhi salah satu persyaratan dalam menyelesaikan Program Strata-I informatika di Universitas Amikom Yogyakarta.

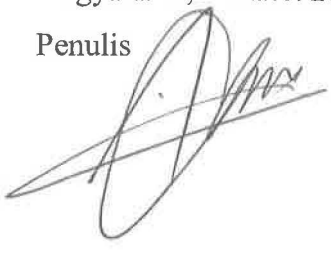
Pada kesempatan ini, penulis mengucapkan terima kasih kepada pihak-pihak yang telah membantu penulis menyelsaikan skripsi ini :

1. Bapak Prof. Dr. M. Suyanto, MM selaku Rektor Univeristas Amikom Yogyakarta.
2. Ibu Subektiningsih, S.Kom, M.Kom selaku Dosen pembimbing yang sabar membimbing dan memberi masukan positif hingga skripsi ini dapat terselesaikan.
3. Bapak / Ibu Dosen Universitas Amikom Yogyakarta yang telah mengajarkan kepada penulis berbagai ilmu yang dapat penulis terapkan dalam penulisan skripsi ini.
4. Teman-Teman seperjuangan 16-S1 Informatika 12, terima kasih atas semua doa dan dukungannya.

Penulis menyadari masih banyak terdapat kekurangan dalam penulisan skripsi ini, baik dalam penulisan dan keteledoran dalam proses pengerjaan skripsi. Oleh karena itu penulis mohon maaf atas segala kesalahan, semoga laporan skripsi ini dapat bermanfaat dan menjadi inspirasi.

Yogyakarta, 1 Maret 2023

Penulis



DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR LAMBANG DAN SINGKATAN

DDoS	Distributed Denial of Service
ELK	Elasticsearch, Logstash, Kibana
DSR	Dynamic Source Routing
PHP	Hypertext Preprocessor
TCP	Transmission Control Protocol
IDPS	Intrusion Detection and Prevention System
MS	Microsoft Windows
SIEM	Security Information and Event Management
IDS	Intrusion Detection System
UTM	Urchin Tracking Module
API	Application Programming Interface
HTTP	Hypertext Transfer Protocol
SSH	Secure Shell
RAM	Random Access Memory
CPU	Central Processing Unit
vCPU	Virtual Central Processing Unit
HDD	Hard Disk Drive
SSD	Solid-state drive
GB	Gigabyte
DDR4	Double Data Rate 4
TB	Terabyte
LTS	Long Term Support

DAFTAR ISTILAH

Administrator	Orang yang bertugas untuk mengelola hal-hal yang berhubungan dengan komputer.
Server	Sistem komputer yang menyediakan sumber daya untuk penyimpanan data.
Service	Layanan pada server jaringan
Log	Catatan yang merekam segala aktifitas suatu aplikasi dijalankan.
real time	Sebuah respon secara langsung di saat itu juga dalam suatu program atau sistem.
Program	Suatu rancangan struktur, desain, kode skema, maupun bentuk yang lainnya dengan yang disusun sesuai alur Algoritma dengan tujuan mempermudah suatu permasalahan.
Hacker	Orang yang skill pemrogramannya mampu menerobos sistem keamanan komputer atau jaringan komputer untuk tujuan tertentu.
Virus	Merupakan suatu program atau aplikasi yang dapat memperbanyak, dan menyebar dengan sendirinya, dan menyebabkan efek negatif pada komputer yang terjangkit.
Trojan	Salah satu jenis malware yang bisa mengancam situs web.
Support	Dukungan.
Data log	Proses otomatis pengumpulan dan perekaman data dari sensor untuk tujuan pengarsipan atau tujuan analisis.
Log management	Proses pengumpulan, konsolidasi, analisis, penyimpanan, visualisasi, dan pemecahan masalah log volume besar dari berbagai server, aplikasi, dan kerangka kerja. infrastruktur IT.
Tool	Alat.

Prometheus	Aplikasi perangkat lunak gratis yang digunakan untuk memantau dan mengingatkan event.
Splunk	Aplikasi Perangkat lunak untuk monitoring jaringan.
Open Source	Perangkat lunak yang kode sumber atau kode dasarnya dapat digunakan oleh banyak orang.
Data	Adalah kumpulan informasi yang telah diubah supaya bisa dioperasikan dengan komputer.
Planning	Proses perencanaan sistem
Modelling	Proses desain sistem
Construction	Proses membangun sistem
Deployment	Proses peluncuran sistem
Log Service	Merupakan platform observasi dan analitik cloud-native yang menyediakan layanan berskala besar dan real-time untuk memproses berbagai jenis data seperti log, metrik, dan pelacakan.
Monitoring	Merupakan proses rutin pengumpulan data dan pengukuran kemajuan atas objektif program, memantau perubahan yang fokus pada proses dan keluaran.
Syslog	Adalah protokol standar yang digunakan untuk mengirim pesan peristiwa atau log sistem ke server tertentu, server Syslog.
Auth log	Adalah log file yang merekam aktivitas authorization seperti perintah sudo dan remote login SSH.
Topologi	Adalah cara menghubungkan sebuah komputer dengan komputer lainnya hingga membentuk suatu jaringan.
Log-Access	Adalah log merekam semua request yang diproses oleh web server.
Katalog Online	Adalah katalog yang data bibliografinya disimpan dalam database komputer.

Perpustakaan Digital	Adalah perpustakaan yang sebagian besar koleksi bukunya tersedia dalam format digital dan bisa diakses melalui komputer.
File log	Adalah file yang berisi daftar acara, yang telah dicatat oleh komputer.
Website	Merupakan kumpulan dari halaman-halaman situs yang terdapat dalam sebuah domain atau subdomain yang berada di dalam World Wide Web (WWW) di internet.
Port Scanning	Adalah aktivitas yang dilakukan untuk memeriksa status port TCP dan UDP pada sebuah mesin.
Network admin	Adalah orang yang bertanggung jawab untuk selalu mengawasi sistem komunikasi di kantor agar tetap berjalan lancar.
Workstation	Adalah perangkat komputer dengan spesifikasi tinggi yang memiliki fungsi membantu melakukan pekerjaan berat.
Client	Adalah sebuah aplikasi atau sistem yang mengakses sebuah sistem layanan yang berada di sistem atau komputer lain yang dikenal dengan server melalui jaringan komputer.
Cluster	Merupakan suatu sistem perangkat keras dan perangkat lunak yang menggabungkan beberapa komputer dalam suatu jaringan dimana komputer tersebut dapat bekerjasama dalam pemrosesan suatu masalah.
Node	Adalah komputer yang mandiri artinya mampu memproses tugas komputasi tanpa node lain.
Shipping agent	Sebagai pelaku pengangkut yang akan di tujukan ke suatu tempat.
error.log	Adalah sebuah teks yang berisi aktivitas error pada sebuah server hosting maupun website.
access.log	Adalah log merekam semua request yang diproses oleh web server.

Timestamp	Adalah urutan karakter, yang menunjukkan tanggal dan / atau waktu di mana peristiwa tertentu terjadi.
Bandwidth	Adalah maksimal besar transfer yang dapat dilakukan pada satu waktu dalam pertukaran data.
Multiuser	Adalah Sebuah sistem dimana dua atau lebih user dapat bekerja sama menggunakan perangkat yang sama untuk saling berbagi pakai penggunaan aplikasi dan sumber daya yang ada pada komputer.
Multitasking	Merupakan suatu kemampuan dalam mengerjakan dua atau lebih pekerjaan secara sekaligus.
Software	Merupakan perangkat lunak pada sebuah komputer.
Platform	Adalah sebuah wadah digital yang banyak dipakai manusia untuk beragam keperluan.
Analyzer	Yang bertugas sebagai peng-analisa.
Decoding	Merupakan proses penerimaan menggunakan kode-kode untuk mengartikan sebuah pesan.
Directory	Adalah lokasi/alamat file atau dokumen yang tersimpan pada suatu media penyimpanan.
Memory Type	Merupakan sebuah tipe Memory.
Storage	Adalah media penyimpanan data atau file yang memanfaatkan teknologi komputasi.
Attacker	Istilah lain untuk Hacker
Host	Merupakan suatu perangkat yang terhubung ke komputer.
Install	Merupakan proses pemasangan dan penyetingan perangkat keras/lunak agar bisa digunakan oleh sistem.

INTISARI

CV Lanis IT Support and Maintenance merupakan sebuah Badan Usaha yang bergerak dibidang layanan jasa *support* teknis perangkat teknologi informasi, sebagai penyedia layanan *service on call* mempunyai *server* yang bekerja 24 jam penuh, maka *administrator* CV Lanis IT Support and Maintenance akan membutuhkan suatu sistem yang dapat *monitoring server* secara *realtime*, sehingga *administrator* akan lebih mudah dalam mengidentifikasi jika terjadi serangan semacam *DDoS (Distributed Denial of Service)*. Untuk itu peneliti akan membangun *log event management server* menggunakan *ELK (Elasticsearch, Logstash, Kibana)* yang dapat memudahkan dalam membaca sekaligus manganalisa *log service* pada *server*. Implementasi *log event management* pada penelitian ini menggunakan 2 *Ubuntu Server LTS,* satu sebagai ELK server dan satu untuk *server client*. Dari hasil pengujian *ELK Stack* yang sudah di bangun dapat mengidentifikasi serangan yang terjadi secara *realtime* dan berhasil merekam semua *log* yang sudah terjadi sehingga *administrator* mendapat info terkait serangan seperti kapan serangan terjadi, dan *ip address* penyerang.

Kata kunci: *log event management server*, *ELK*, *server*, *monitoring server*, *DDoS*.

ABSTRACT

CV Lanis IT Support and Maintenance is a Business Entity engaged in technical support services for information technology devices, as a service provider on call has a server that works 24 hours a day, the administrator of CV Lanis IT Support and Maintenance will need a system that can monitor server in real time, so that it will be easier for administrators to identify if an attack such as DDoS (Distributed Denial of Service) occurs. For this reason, researchers will build an event management server log using ELK (Elasticsearch, Logstash, Kibana) which can make it easier to read as well as analyze service logs on the server. The implementation of log event management in this study uses 2 Ubuntu Server LTS, one as an ELK server and one for client servers. From the test results the ELK Stack that has been built can identify attacks that occur in real time and successfully record all logs that have occurred so that the administrator gets information regarding attacks such as when the attack occurred, and the attacker's IP address.

Keyword: *event management server log*, *ELK*, *server*, *monitoring server*, *DDoS*.