ANALISIS PERFORMA PLATFORM ELK STACK DAN SPLUNK PADA LOG SERANGAN BRUTEFORCE ASTERISK

SKRIPSI

Disusun oleh:

Nurhalis Jusman
17.83.0079

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021

ANALISIS PERFORMA PLATFORM ELK STACK DAN SPLUNK PADA LOG SERANGAN BRUTEFORCE ASTERISK

SKRIPSI

Diajukan kepada Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
untuk memenuhi salah satu syarat memperoleh gelar Sarjana Komputer
Pada Jenjang Program Sarjana – Program Studi Teknik Komputer

Disusun oleh:

Nurhalis Jusman
17.83.0079

PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS PERFORMA PLATFORM ELK STACK DAN SPLUNK PADA LOG SERANGAN BRUTEFORCE ASTERISK

yang dipersiapkan dan disusun oleh

Nurhalis Jusman

17.83.0079

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 08 November 2021

Dosen Pembimbing,

Dony Ariyus, M.Kom
NIK. 190302128

HALAMAN PENGESAHAN
SKRIPSI

ANALISIS PERFORMA PLATFORM ELK STACK DAN SPLUNK PADA LOG SERANGAN BRUTEFORCE ASTERISK

yang dipersiapkan dan disusun oleh

Nurhalis Jusman

17.83.0079

Telah dipertahankan di depan Dewan Penguji
pada tanggal 22 November 2021

Susunan Dewan Penguji

Nama Penguji	**Tanda Tangan**
Rini Indrayani, M.Eng **NIK. 190302417**	_____
Ria Andriani, M.Kom **NIK. 190302458**	_____
Dony Ariyus, M.Kom **NIK. 190302128**	_____

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 22 November 2021

DEKAN FAKULTAS ILMU KOMPUTER

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

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Nurhalis Jusman
NIM : 17.83.0079

Menyatakan bahwa Skripsi dengan judul berikut:

Tuliskan Judul Skripsi

Dosen Pembimbing : Dony Ariyus, 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, 22 November 2021

Yang Menyatakan,

Nurhalis Jusman

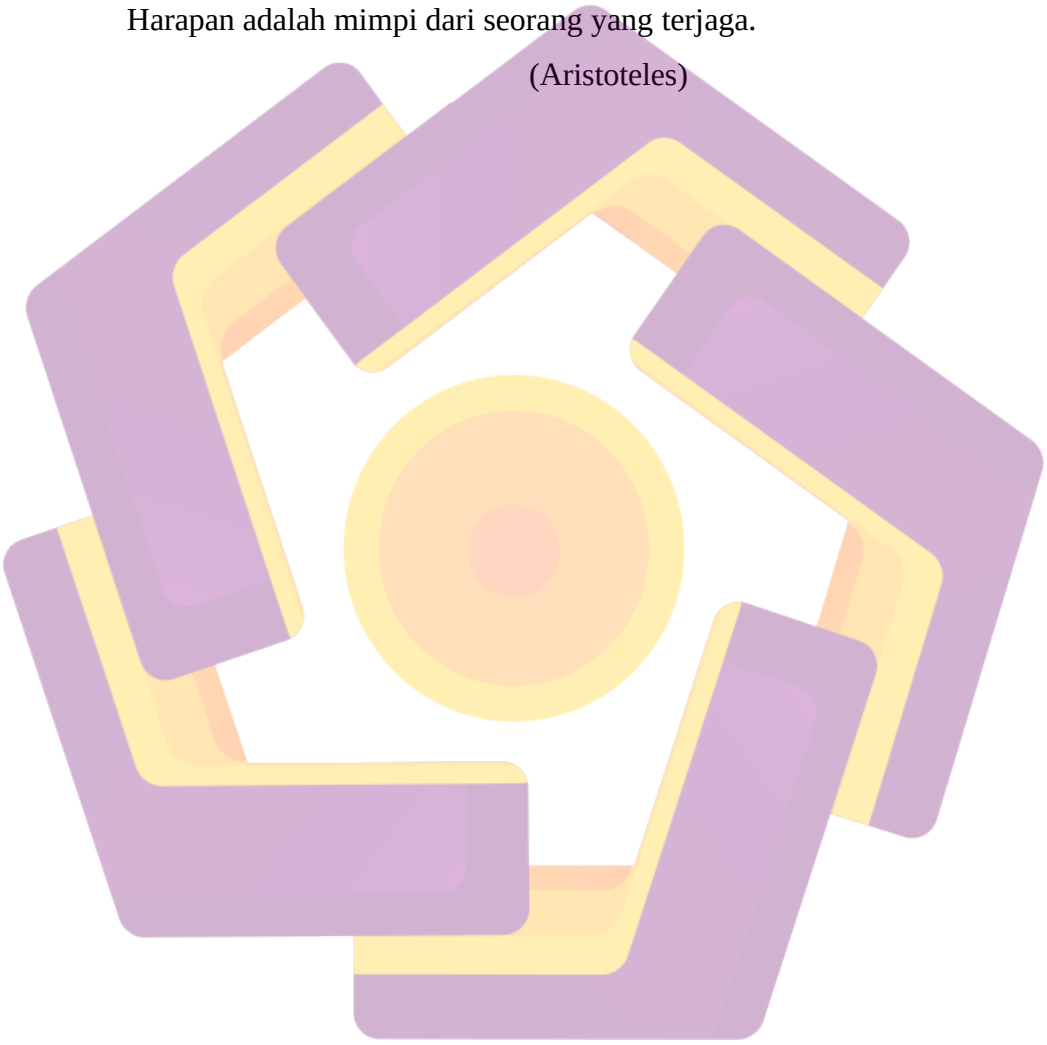
HALAMAN MOTTO

Tanpa Tindakan, pengetahuan tidak ada gunanya dan pengetahuan tanpa tidakan itu sia-sia.

(Abu Bakar Asshidiq)

Harapan adalah mimpi dari seorang yang terjaga.

(Aristoteles)



HALAMAN PERSEMBAHAN

Tulisan ini dipersembahkan untuk :

1. Allah SWT dengan segala rahmat serta karunia-Nya yang memberikan kekuattan bagi peneliti dalam menyelesaikan skripsi ini
2. Bapak ,Mama dan Adik yang selalu berdoa dan mendukung untuk keberhasilan anaknya.
3. Bapak Dosen pembimbing yang telah membimbing dengan sabar dan meluangkan waktunya untuk saya.
4. Teman-teman kelas 17-S1TK-02 terima kasih atas kebersamaannya.
5. Teman-teman Grup Pejuang Kuliah yang sudah bersama saya dari awal kuliah.
6. Almamater Universitas AMIKOM Yogyakarta.

KATA PENGANTAR

Dalam penyusunan skripsi ini tidak terlepas dukungan dari berbagai pihak. Peneliti secara khusus mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu. Peneliti banyak menerima bimbingan, petunjuk dan bantuan serta dorongan dari berbagai pihak baik yang bersifat moral maupun material. Pada kesempatan ini penulis menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

1. Allah SWT dengan segala rahmat serta karunia-Nya yang memberikan kekuattan bagi peneliti dalam menyelesaikan skripsi ini.
2. Kepada Bapak Dony Ariyus, M.Kom selaku pembimbing pada penelitian ini atas waktu dan bimbingannya yang telah memberikan arahan, masukan dalam penyusunan skiripsi ini.
3. Bapak dan Ibu dosen Program Studi Teknik Komputer yang telah memberikan ilmu selama penulis belajar di Universitas AMIKOM Yogyakarta.
4. Teman-teman Teknik Komputer, khususnya angkatan 2017 terima kasih atas bantuan, Kerjasama, dan motivasi nya selama ini.
5. Teman-teman Grup Pejuan Kuliah yang telah menemani penulis dari awal kuliah.
6. Semua pihak yang tidak dapat disebutkan satu persatu.

Yogyakarta, 22 November 2021

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR ISTILAH

INTISARI

Seiring dengan majunya teknologi komunikasi antar perangkat mengalami perkembangan yang sangat signifikan. Saat ini kita dapat berkomunikasi melalui jaringan dengan memanfaatkan teknologi yang disebut Voice over Internet Protocol (VoIP). VoIP dapat digunakan sebagai jaringan komunikasi yang dijalankan menggunakan aplikasi Asterisk. Pada sistem asterisk terdapat ribuan bahkan jutaan baris log mulai dari log call, serangan hacker, brutoforce, warning, debug. Untuk membuat dan membaca log yang sangat banyak dilakukan dengan memusatkan log tersebut. Pada penelitian ini menganalisis bagaimana kecepatan performa dalam membaca log pada ELK Stack dan Splunk dan untuk memudahkan sistem administrator memilih metode yang sesuai dengan kebutuhannya.

Pada penelitian ini dilakukan pengumpulan data dari log Asterisk dengan menyimpan log pada file dengan ukuran yang berbeda-beda. Ukuran file yang dianalisa yaitu 227 Mb, 784 Mb, 1Gb, 2.6 Gb dan 3 Gb. Hasil yang dari penelitian ini dalam melakukan proses pengecekan log pada ELK Stack didapatkan hasil dengan waktu rata-rata sekitar 1-2 detik, sedangkan pada Splunk membutuhkan waktu sekitar 2-3 detik. Pada ELK Stack dan Splunk mempunya perbedaan selilih waktu sekitar 1 detik.

Kesimpulan dari penelitian ini bahwa berdasarkan hasil yang didapatkan platform ELK Stack lebih efisien digunakan sebagai tools monitoring log karena dari segi waktu yang lebih cepat dan hasil log lebih lengkap dibandingkan dengan Splunk yang jika tidak dibatasi outputnya dapat memakan waktu yang sangat lama dibandingkan dengan ELK Stack.

Kata kunci: Asterisk, Bruteforce, Log, ELK Stack, Splunk

ABSTRACT

Along with the advancement of communication technology between devices, there has been a very significant development. Currently we can communicate over a network by utilizing a technology called Voice over Internet Protocol (VoIP). VoIP can be used as a communication network that is run using the Asterisk application. On the asterisk system there are thousands and even millions of log lines ranging from call logs, hacker attacks, gross force, warnings, debug. To create and read very large logs is done by centralizing the logs. In this study, we analyze how fast the performance is in reading logs on the ELK Stack and Splunk and to make it easier for system administrators to choose the method that suits their needs.

In this study, data was collected from Asterisk logs by storing logs in files of different sizes. The analyzed file sizes are 227 Mb, 784 Mb, 1Gb, 2.6 Gb and 3 Gb.The results of this study in the process of checking the logs on the ELK Stack obtained results with an average time of about 1-2 seconds, while in Splunk it takes about 2-3 seconds. ELK Stack and Splunk have a time difference of about 1 second.

The conclusion of this study is that based on the results obtained, the ELK Stack platform is more efficient to use as a log monitoring tool because in terms of faster time and more complete log results compared to Splunk which, if not limited, its output can take a very long time compared to ELK Stack.

Keyword: *Asterisk, Bruteforce, Log, ELK Stack, Splunk*