

**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

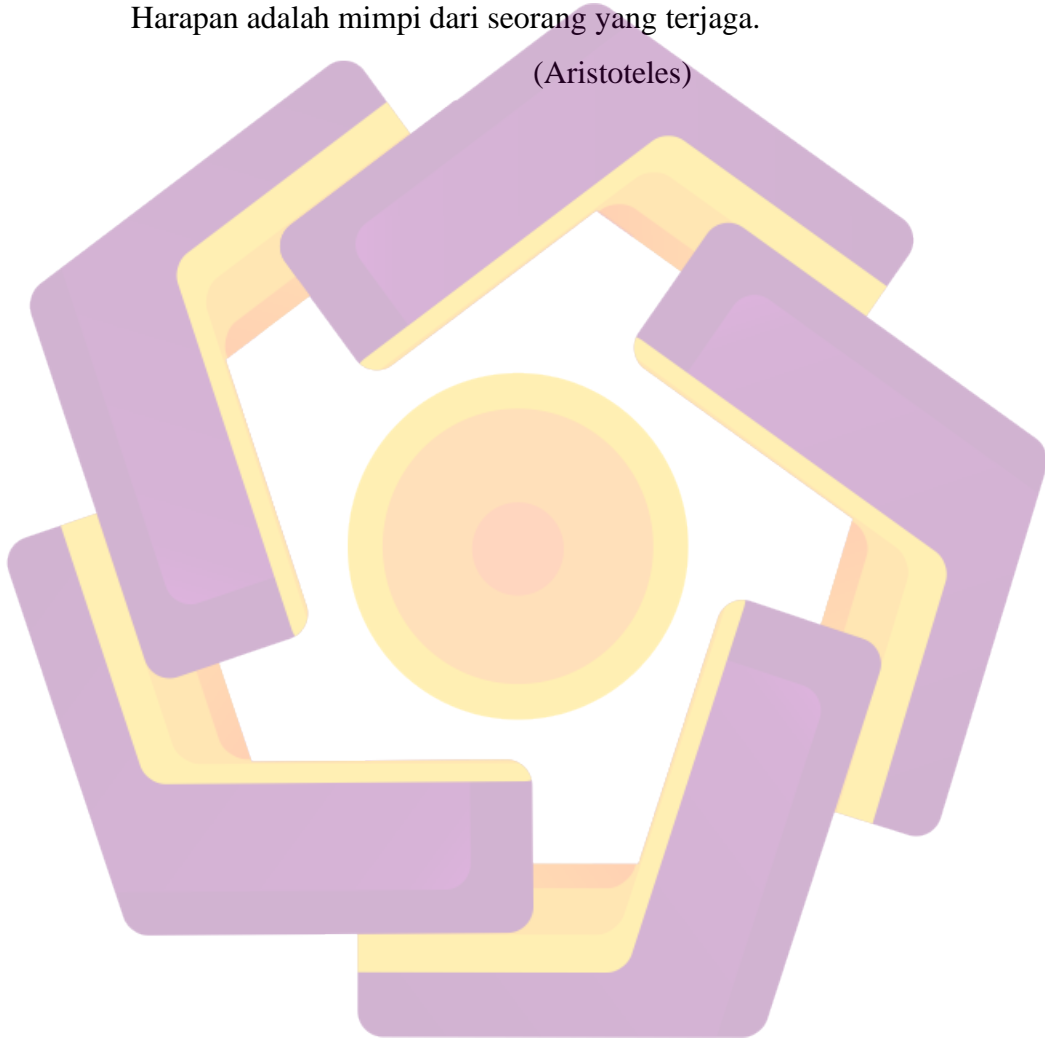
HALAMAN MOTTO

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

(Abu Bakar Asshidiq)

Harapan adalah mimpi dari seorang yang terjaga.

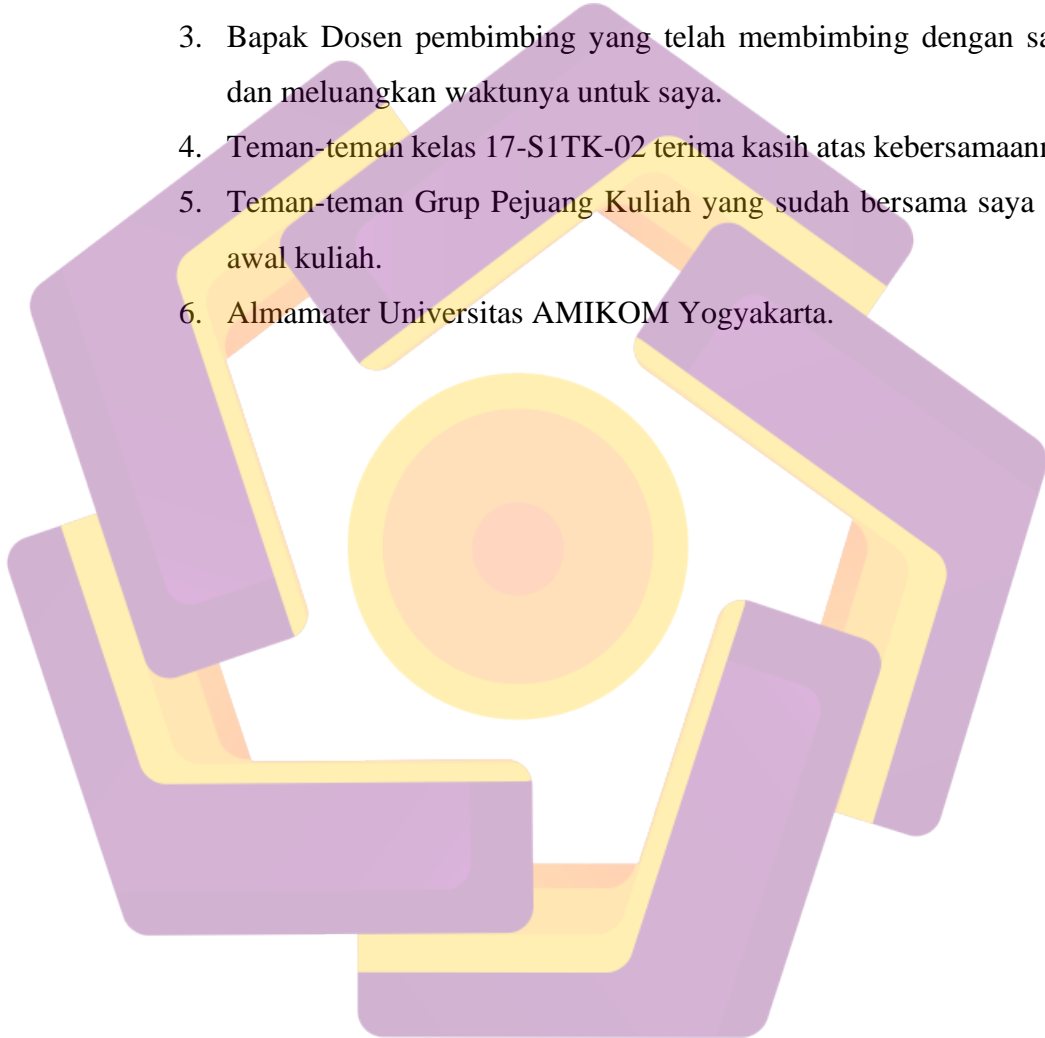
(Aristoteles)



HALAMAN PERSEMBAHAN

Tulisan ini dipersembahkan untuk :

1. Allah SWT dengan segala rahmat serta karunia-Nya yang memberikan kekuatan 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 kekuatan 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 skripsi 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



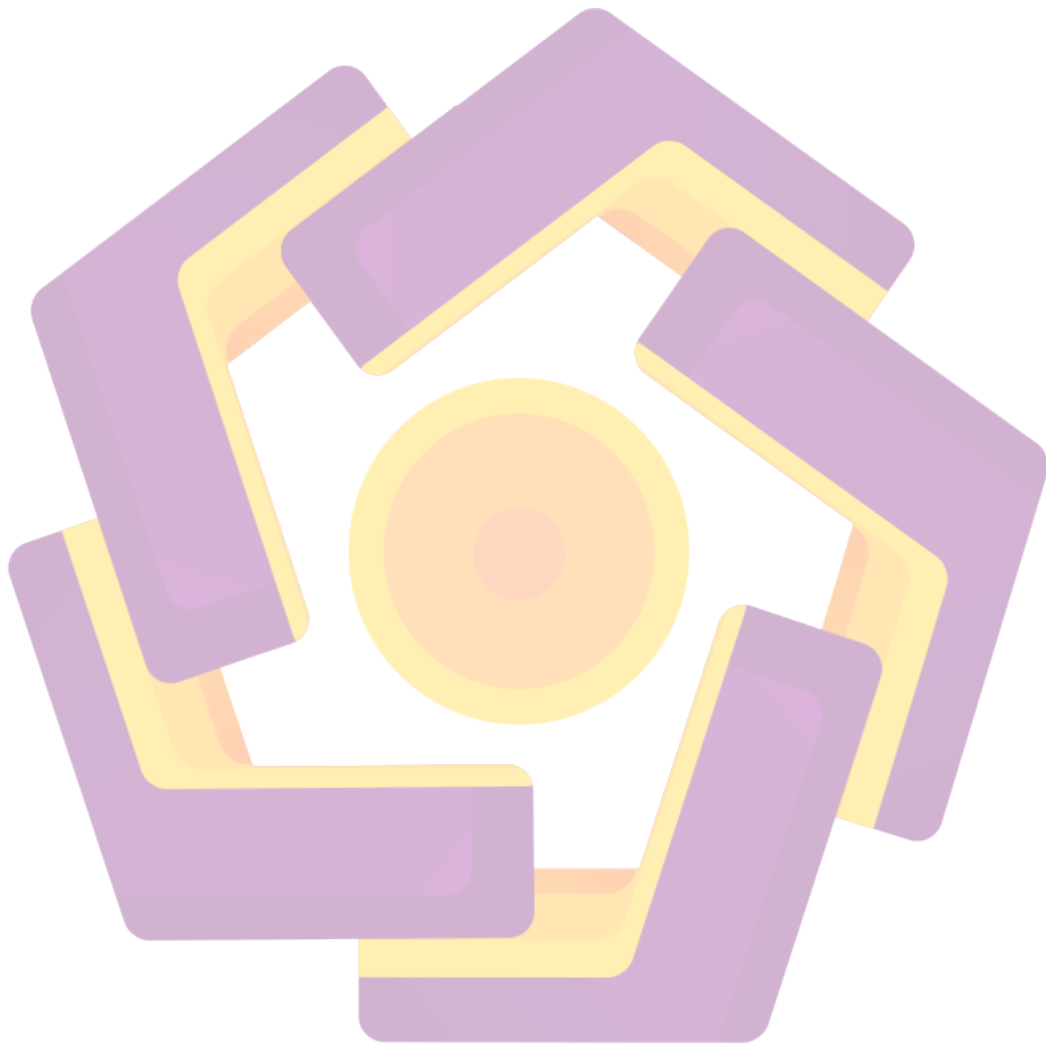
Penulis

DAFTAR ISI

HALAMAN JUDUL.....	2
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENGESAHAN.....	iv
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	v
HALAMAN MOTTO	vi
HALAMAN PERSEMBAHAN	vii
KATA PENGANTAR	viii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xii
DAFTAR GAMBAR	xiii
DAFTAR ISTILAH	xv
INTISARI.....	xvi
<i>ABSTRACT</i>	xvii
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Sistematika Penulisan	4
BAB II LANDASAN TEORI	5
2.1 Tinjauan Pustaka	5
2.2 Asterisk	8
2.3 Platform Managemen Log.....	9
2.3.1 ELK Stack.....	9
2.3.1.1 Elasticsearch	10
2.3.1.2 Logstash.....	11
2.3.1.3 Kibana.....	11
2.3.2 Splunk	12
2.3.3 Perbandingan Beberapa Tools Management Log.....	13
2.4 Sistem Operasi.....	13
2.4.1 Ubuntu Server 18.10	13
2.4.2 Debian 10.....	14
2.5 Google Cloud Platform (GCP)	14

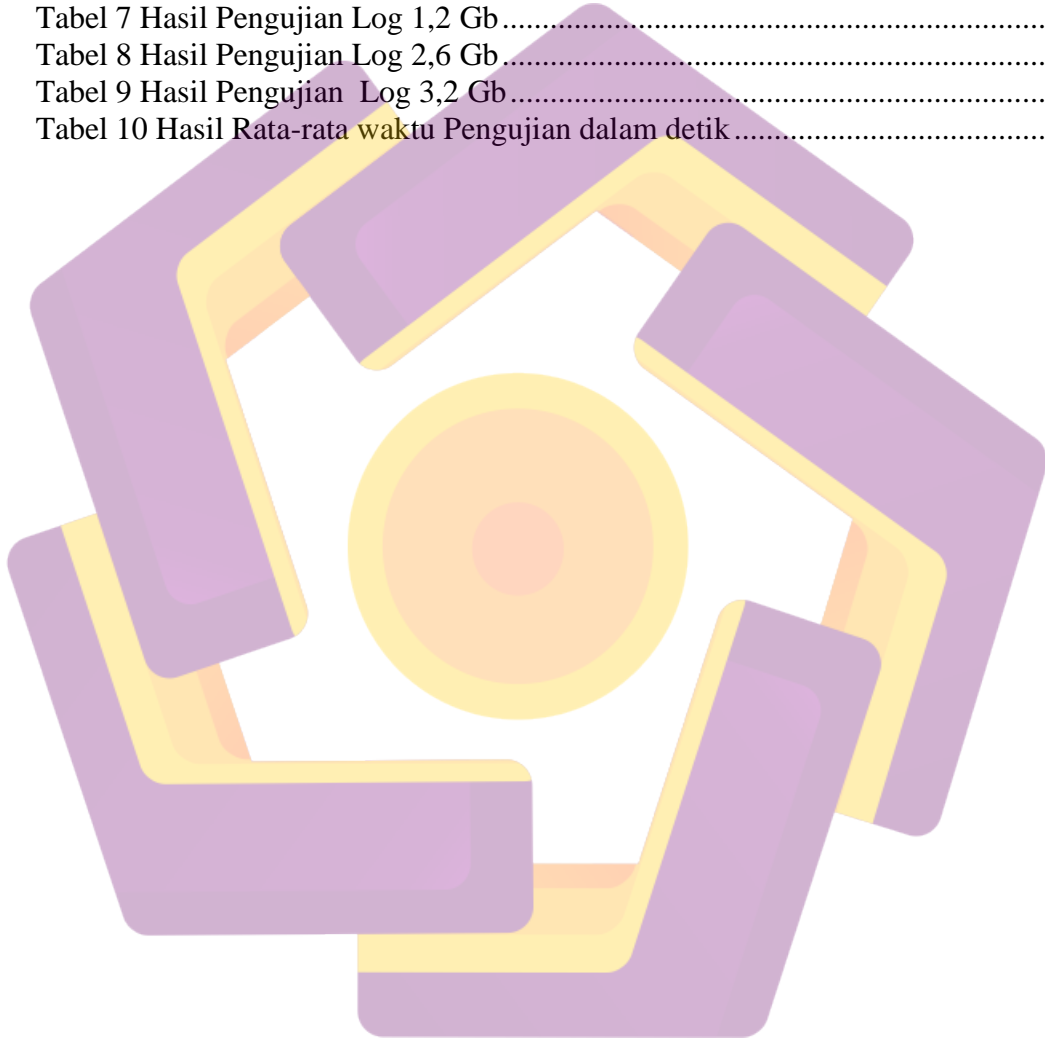
BAB III METODOLOGI PENELITIAN	15
3.1 Desain Alur Kerja Penelitian	15
3.2 Desain Sistem.....	17
3.2.1 Desain Sistem ELK Stack	17
3.2.2 Desain Splunk.....	18
3.2.3 Desain Asterisk.....	19
3.3 Rencana Pengujian	20
3.4 Skenario & Bentuk Serangan	20
3.6 Filter Search	22
3.6.1 Filter Search ELK Stack	22
3.6.2 Filter Search Splunk	23
3.7 Rancangan Visualisasi	24
3.7.1 Visualisasi ELK Stack	24
3.7.2 Visualisasi Splunk	24
BAB IV PEMBAHASAN.....	26
4.1 Diagram Simulasi.....	26
4.2 Persiapan Data	27
4.3 Implementasi Sistem	27
4.3.1 Instalasi Server	28
4.3.2 Instalasi Asterisk	28
4.3.3 Instalasi ELK Stack	32
4.3.3.1 Instalasi Elasticsearch	32
4.3.3.2 Instalasi Kibana	33
4.3.3.3 Instalasi Logstash.....	34
4.3.3.4 Instalasi Filebeat	36
4.3.4 Instalasi Splunk	36
4.3.5 Perbandingan Uji Proses Instalasi Tools Monitoring	37
4.4 Proses Pengujian	38
4.4.1 Pengujian ELK Stack	38
4.4.2 Pengujian Splunk.....	39
4.5 Hasil Pengujian	40
4.5.1 Hasil Pengujian Log Size 227 Mb.....	40
4.5.2 Hasil Pengujian Log Size 786 Mb.....	42
4.5.3 Hasil Pengujian Log Size 1 Gb	44
4.5.4 Hasil Pengujian Log Size 2,6 Gb	46
4.5.5 Hasil Pengujian Log Size 3,2 Gb	48
BAB V PENUTUP.....	52

5.1 Kesimpulan	52
5.2 Saran	52
DAFTAR PUSTAKA	53
LAMPIRAN.....	55



DAFTAR TABEL

Tabel 1 Penelitian Terkait	6
Tabel 2 Perbandingan Tools Management Log	13
Tabel 3 List & Ukuran File Log	22
Tabel 4 Perbandingan Uji Proses Instalasi Tools Monitoring	38
Tabel 5 Hasil Pengujian Log Size 227 Mb	40
Tabel 6 Hasil Pengujian Log 786 Mb	42
Tabel 7 Hasil Pengujian Log 1,2 Gb	44
Tabel 8 Hasil Pengujian Log 2,6 Gb	46
Tabel 9 Hasil Pengujian Log 3,2 Gb	48
Tabel 10 Hasil Rata-rata waktu Pengujian dalam detik	50



DAFTAR GAMBAR

Gambar 1 Serangan VoIP dari beberapa Negara	2
Gambar 2 Alur sistem Asterisk server	9
Gambar 3 Alur Data ELK Stack	10
Gambar 4 Alur Splunk	12
Gambar 5 Flowchart Penelitian.....	16
Gambar 6 Desain Sistem ELK Stack	17
Gambar 7 Desain Sistem Splunk	18
Gambar 8 Proses dari Asterisk ke Server ELK.....	19
Gambar 9 Proses dari Asterisk Ke Sever Splunk.....	19
Gambar 10 Contoh Serangan Bruteforce pada Asterisk	20
Gambar 11 Contoh Serangan Bruteforce	21
Gambar 12 Contoh Serangan lain	21
Gambar 13 Contoh Query Pencocokan Data	22
Gambar 14 Contoh Query Boolean.....	23
Gambar 15 Contoh Pencarian Splunk	23
Gambar 16 Rancangan Dashboard ELK Stack	24
Gambar 17 Rancangan Dashboard Splunk	25
Gambar 18 Flow Diagram Simulasi.....	26
Gambar 19 Fitur <i>Compute Engine</i> pada GCP	28
Gambar 20 Hasil Download & Ekstrak Source Asterisk.....	29
Gambar 21 Proses cek dependensi asterisk.....	29
Gambar 22 Proses konfigurasi Asterisk	30
Gambar 23 Proses Kompiling Asterisk.....	31
Gambar 24 Proses Instalasi Asterisk	31
Gambar 25 Proses Pembuatan Grup Asterisk	31
Gambar 26 Proses Edit User dan Grup	32
Gambar 27 Output Asterisk	32
Gambar 28 Proses menambahkan Repositori Elasticsearch	32
Gambar 29 Output Hasil dari Elasticsearch.....	33
Gambar 30 Output dari Kibana	34
Gambar 31 Konfigurasi file <i>02-beats-input.conf</i>	34
Gambar 32 Konfigurasi file <i>/etc/logstash/conf.d/10-syslog-filter.conf</i>	35
Gambar 33 Konfigurasi file <i>"/etc/logstash/conf.d/30-elasticsearch-output.conf</i>	35
Gambar 34 Konfigurasi file <i>/etc/filebeat/filebeat.yml</i>	36
Gambar 35 Download paket splunk binary.....	36
Gambar 36 Instalasi Splunk	37
Gambar 37 Output Splunk	37
Gambar 38 Contoh Curl ELK Stack	38
Gambar 39 Contoh Proses Curl & Output	39
Gambar 40 Proses Search & Output Splunk	40
Gambar 41 Grafik Pencarian Log Size 227 Mb.....	42
Gambar 42 Grafik Pencarian Log Size 786 Mb.....	44
Gambar 43 Grafik Pencarian Log Size 1,2 Gb	46
Gambar 44 Grafik Pencarian Log Size 2,6 Gb	48

Gambar 45 Grafik Pencarian Log Size 3,2 Gb50
Gambar 46 Grafik Rata-rata Pengujian.....51



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 mempunyai 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