

**ANALISIS PERBANDINGAN PERFORMA PLATFORM ELK
STACK DAN GRAFANA LOKI PADA HONEYPOT SERVER**

SKRIPSI



Disusun oleh:

Ach Izalul Haq

17.83.0084

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

**ANALISIS PERBANDINGAN PERFORMA PLATFORM ELK
STACK DAN GRAFANA LOKI PADA HONEYPOT SERVER**

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:

Ach Izalul Haq

17.83.0084

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

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS PERBANDINGAN PERFORMA PLATFORM ELK STACK DAN GRAFANA LOKI PADA HONEYPOT SERVER

yang dipersiapkan dan disusun oleh

Ach Izalul Haq

17.83.0084

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 05 Juni 2021

Dosen Pembimbing,

Banu Santoso, S.T., M.Eng

NIK. 190302327

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS PERBANDINGAN PERFORMA PLATFORM ELK STACK DAN GRAFANA LOKI PADA HONEYPOT SERVER

yang dipersiapkan dan disusun oleh

Ach Izatul Haq

17.83.0084

Telah dipertahankan di depan Dewan Penguji
pada tanggal 22 Juni 2021

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Wahid Miftahul Ashari, S.Kom., MT
NIK. 190302452

Ferry Wahyu Wibowo, S.Si, M.Cs
NIK. 190302235

Banu Santoso, S.T., M.Eng
NIK. 190302327

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

DEKAN FAKULTAS ILMU KOMPUTER

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

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini,

Nama mahasiswa : Ach Izalul Haq

NIM : 17.83.0084

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis Perbandingan Performa Platform ELK Stack dan Grafana Loki pada Honeypot Server

Dosen Pembimbing : Banu Santoso, S.T., M.Eng

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 Juni 2021

Yang Menyatakan,



Ach Izalul Haq

HALAMAN MOTTO

Ilmu lebih utama karena dia mengajak manusia untuk mengabdikan kepada Tuhan mengingat makhluk-Nya yang lemah dan terbatas, sedang harta mendorong manusia menganggap dirinya sebagai Tuhan dengan memandang rendah orang – orang yang lebih miskin darinya.

(Ali Bin Abi Thalib)

Saingan mu bukanlah orang yang lebih pandai dari mu, tetapi umur kedua orang tuamu. Semangat lah untuk sukses dan menjadi orang bernilai dan bermanfaat bagi agama bangsa dan negara.

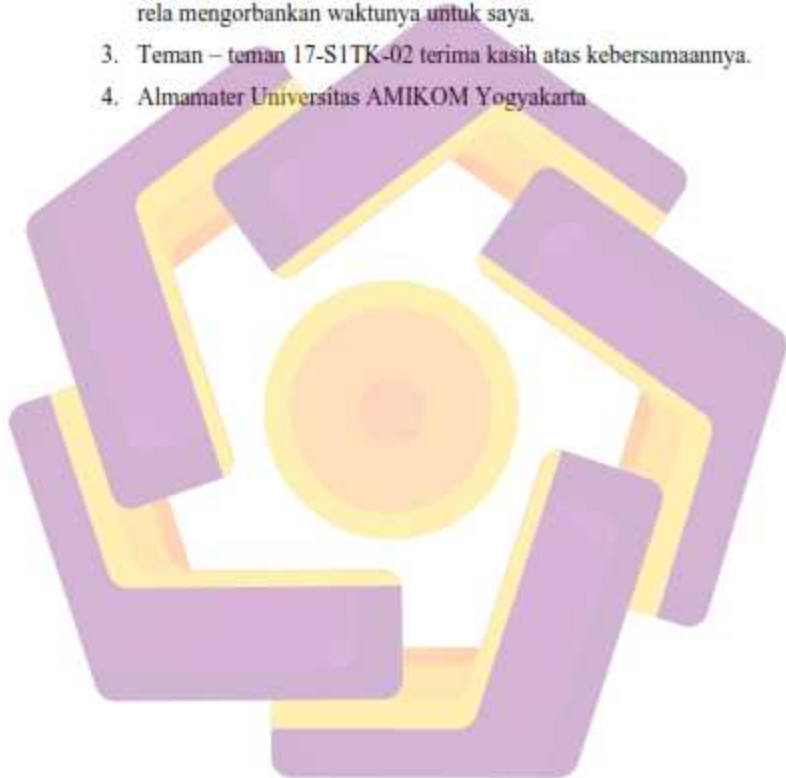
(Anonim)



HALAMAN PERSEMBAHAN

Tulisan ini dipersembahkan untuk :

1. Uwak dan Emak atas cinta, kasih sayang, doa, nasihat dan pengorbanan yang se tulusnya tcurahkan untukku.
2. Bapak Dosen pembimbing yang telah membimbing saya dengan sabar, rela mengorbankan waktunya untuk saya.
3. Teman – teman 17-S1TK-02 terima kasih atas kebersamaannya.
4. Almamater Universitas AMIKOM Yogyakarta



KATA PENGANTAR

Alhamdulillah Segala puji dan syukur kehadiran Allah AWT, Tuhan Semesta Alam, atas limpahan Rahmat dan Hidayah-Nya sehingga penulis mampu menyelesaikan penyusunan skripsi ini. Skripsi ini disusun sebagai salah satu syarat untuk mendapatkan gelar strata satu Universitas AMIKOM Yogyakarta.

Dalam penyusunan skripsi ini tidak lepas dari bantuan beberapa pihak, oleh karena itu penulis hendak mengucapkan terima kasih kepada :

1. Kedua orang tua yang telah memberikan dukungan dan doa sehingga penulis dapat menyelesaikan penyusunan skripsi ini.
2. Bapak Banu Santoso, S.T., M.Eng selaku pembimbing atas waktu dan kesabarannya memberikan arahan , bimbingan dan 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. Semua pihak yang tidak dapat disebutkan satu persatu.

Semoga amal kebaikan semua pihak tersebut mendapatkan imbalan dari Allah SWT. Penulis menyadari bahwa penulisan skripsi ini masih jauh dari sempurna, untuk itu kritik dan saran yang membangun dari pembaca sangat diharapkan. Semoga skripsi ini dapat bermanfaat bagi perkembangan ilmu pengetahuan.

Yogyakarta, 09 Mei 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.....	xi
DAFTAR GAMBAR.....	xii
INTISARI.....	xiv
<i>ABSTRACT</i>	xv
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah.....	2
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 Honeypot.....	6
2.3 Platform Manajemen Log	8
2.3.1 ELK Stack	8
2.3.1.1 Elasticsearch	9
2.3.1.2 Logstash.....	9
2.3.1.3 Kibana.....	9
2.3.2 Grafana Loki	9
2.3.2.1 Promtail	10
2.3.2.2 Loki.....	11
2.3.2.3 Grafana	11
2.3.3 Klasifikasi Platform Manajemen Log	12
2.6 SSH (Secure-Shell).....	12
2.7 Ubuntu Server.....	13
2.8 Digital Ocean	13
2.9 Glances.....	13
BAB III METODOLOGI PENELITIAN	14
3.1 Alur Kerja Perancangan.....	14

3.2	Desain Sistem.....	15
3.2.1	Skema Sistem Grafana Loki	15
3.2.2	Skema Sistem ELK Stack	16
3.2.3	Arsitektur Honeypot Server	18
3.2.4	Arsitektur Monitoring Server.....	20
3.2.5	Rancangan Pengujian.....	21
3.2.5.1	Skenario Serangan.....	21
3.2.5.2	Pengujian Performa.....	23
3.2.5.3	Rancangan Visualisasi	23
BAB IV PEMBAHASAN.....		26
4.1	Diagram Jaringan.....	26
4.2	Persiapan Data	27
4.3	Implementasi Sistem.....	28
4.3.2.1	Loki	29
4.3.2.2	Grafana.....	31
4.3.2.3	Promtail.....	33
4.3.2.4	Elasticsearch.....	34
4.3.2.5	Kibana	37
4.3.2.6	Logstash	38
4.3.2.7	Filebeat.....	42
4.4	Proses Pengujian.....	43
4.4.1	Proses Scanning Pada Honeypot Server	43
4.4.2	Serangan DoS menggunakan LOIC.....	45
4.4.3	Serangan MS17-10 menggunakan Metasploit.....	46
4.4.4	Serangan Brute Force Menggunakan Hydra	48
4.5	Hasil Pengujian	49
4.5.1	Hasil Pengujian Serangan DoS	49
4.5.2	Hasil Pengujian Serangan MS17-10	52
4.5.3	Hasil Pengujian Serangan Brute Force	55
BAB V PENUTUP.....		58
5.1	Kesimpulan	58
5.2	Saran	59
DAFTAR PUSTAKA		60
LAMPIRAN.....		63

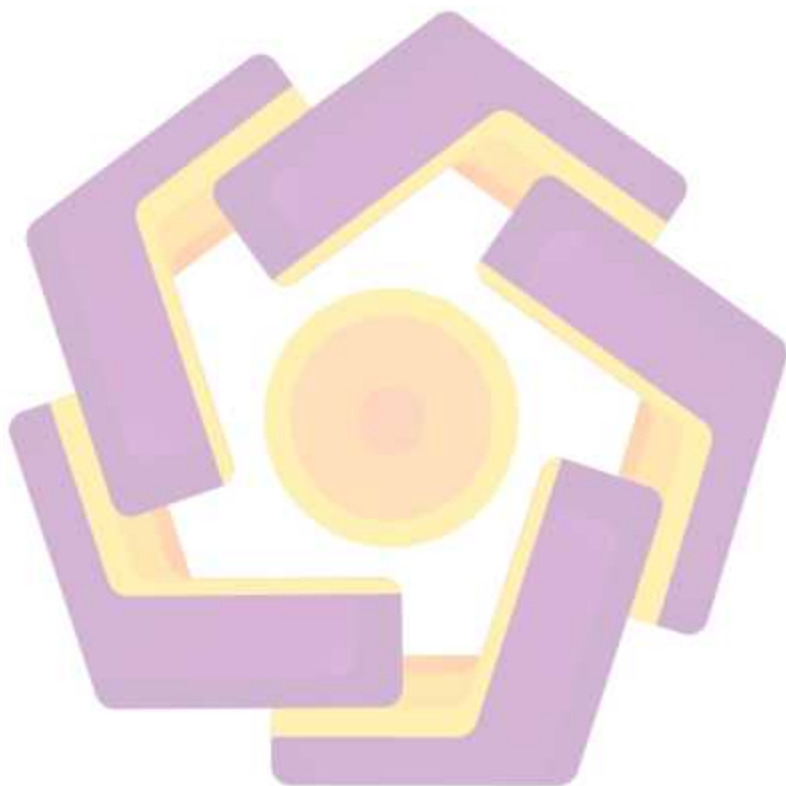
DAFTAR TABEL

Tabel 2.1 Daftar Penelitian Terkait	6
Tabel 2.2 Perbandingan Splunk, Graylog, Grafana Loki, dan ELK Stack [24],[26],[27]	12
Tabel 3.1 Daftar Port Grafana Loki	19
Tabel 3.2 Daftar Port ELK Stack	19
Tabel 3.3 Nama Serangan dan Perintah yang Digunakan untuk Honeypot Server 01	22
Tabel 3.4 Nama Serangan dan Perintah yang Digunakan untuk Honeypot Server 02	23
Tabel 4.1 Hasil Pengujian Serangan DoS	49
Tabel 4.2 Penggunaan Resource CPU Rata-rata pada Serangan DoS	50
Tabel 4.3 Penggunaan Resource Memori Rata-rata pada Serangan DoS	50
Tabel 4.4 Hasil Uji T (P-Value) Resource CPU pada Serangan DoS	51
Tabel 4.5 Hasil Uji T (P-Value) Resource Memori pada Serangan DoS	51
Tabel 4.4 Hasil Pengujian Serangan MS17-10	52
Tabel 4.6 Penggunaan Resource CPU Rata-rata pada Serangan MS17-10	53
Tabel 4.7 Penggunaan Resource Memori Rata-rata pada Serangan MS17-10	53
Tabel 4.8 Hasil Uji T (P-Value) Resource CPU pada Serangan MS17-10	53
Tabel 4.9 Hasil Uji T (P-Value) Resource Memori pada Serangan MS17-10	54
Tabel 4.7 Hasil Pengujian Serangan Brute Force	55
Tabel 4.10 Penggunaan Resource CPU Rata-rata pada Serangan Brute Force	56
Tabel 4.11 Penggunaan Resource Memori Rata-rata pada Serangan Brute Force	56
Tabel 4.12 Hasil Uji T (P-Value) Resource CPU pada Serangan Brute Force	56
Tabel 4.13 Hasil Uji T (P-Value) Resource Memori pada Serangan Brute Force	57

DAFTAR GAMBAR

Gambar 3.1	Flowchart Penelitian	14
Gambar 3.2	Desain Sistem Platform Grafana Loki	15
Gambar 3.3	Flowchart Sistem Grafana Loki	16
Gambar 3.4	Desain Sistem Platform ELK Stack	17
Gambar 3.5	Flowchart Sistem ELK Stack	18
Gambar 3.6	Arsitektur Honeypot Server untuk Grafana Loki	19
Gambar 3.7	Arsitektur Honeypot Server untuk ELK Stack	19
Gambar 3.8	Arsitektur Monitoring Server Grafana Loki	20
Gambar 3.9	Arsitektur Monitoring Server ELK Stack	21
Gambar 3.10	Skenario Serangan Honeypot Server	22
Gambar 3.11	Rancangan Dashboard Grafana	24
Gambar 3.12	Rancangan Dashboard Kibana	25
Gambar 4.1	Diagram Jaringan Simulasi	26
Gambar 4.2	Proses Pemilihan Image Droplets	28
Gambar 4.3	Proses Pemilihan Spesifikasi Droplets	29
Gambar 4.4	Server yang telah di Buat	29
Gambar 4.5	Proses Instalasi Loki Binary	30
Gambar 4.6	Loki yang Sudah Berjalan	31
Gambar 4.7	Install libfontconfig	31
Gambar 4.8	Download Grafana	32
Gambar 4.9	Install Grafana	32
Gambar 4.10	Grafana yang Sudah Berjalan	33
Gambar 4.11	Proses Instalasi Promtail Binary	34
Gambar 4.12	Promtail yang Sudah Berjalan	34
Gambar 4.13	Install Java 8	35
Gambar 4.14	Proses Menambahkan Repository Elastic	36
Gambar 4.15	Instalasi Elasticsearch	36
Gambar 4.16	Instalasi Kibana	37
Gambar 4.17	Konfigurasi Kibana	37
Gambar 4.18	Install Logstash	38
Gambar 4.19	Konfigurasi logstash-cowrie.conf	39
Gambar 4.20	Konfigurasi logstash-dionaea.conf	40
Gambar 4.21	Konfigurasi logstash-suricata.conf	41
Gambar 4.22	Install filebeat	42
Gambar 4.23	Konfigurasi Filebeat	43
Gambar 4.24	Hasil Scanning Honeypot Server 01	44
Gambar 4.25	Hasil Scanning Honeypot Server 02	45
Gambar 4.26	Proses Serangan DoS pada HoneypotServer01	45
Gambar 4.27	Proses Serangan DoS pada HoneypotServer02	46
Gambar 4.28	Proses Serangan MS17-10 pada HoneypotServer01	47
Gambar 4.29	Proses Serangan MS17-10 pada HoneypotServer02	47
Gambar 4.30	Proses Serangan Brute Force pada HoneypotServer01	48
Gambar 4.31	Proses Serangan Brute Force pada HoneypotServer02	49

Gambar 4.32 Grafik Penggunaan CPU pada Serangan DOS.....	51
Gambar 4.33 Grafik Penggunaan Memori pada Serangan DOS.....	52
Gambar 4.34 Grafik Penggunaan CPU pada Serangan MS17-10.....	54
Gambar 4.35 Grafik Penggunaan Memori pada Serangan MS17-10	55
Gambar 4.36 Grafik Penggunaan CPU pada Serangan Brute Force.....	57
Gambar 4.37 Grafik Penggunaan Memori pada Serangan Brute Force.....	57



INTISARI

Seiring perkembangan teknologi yang begitu pesat, telah muncul banyak platform untuk manajemen dan analisis log dari sebuah komputer diantaranya platform *Grafana Loki* dan *ELK Stack*. Sehingga dampak dari perkembangan ini menimbulkan banyak variasi dan ketidaktahuan para administrator dalam menentukan platform mana yang sesuai dengan kebutuhan mereka.

Pada penelitian ini menganalisis performa dari kedua platform tersebut terhadap server *honeypot* saat terjadi serangan dengan parameter penggunaan *CPU* dan *Memori*, kedua parameter tersebut merupakan standar untuk para administrator dalam mempertimbangkan platform yang akan dipilih.

Kesimpulan dari penelitian ini bahwa berdasarkan parameter yang digunakan platform *Grafana Loki* lebih efisien dari segi pemakaian *CPU* dan *Memori* dibandingkan platform *ELK Stack*, *Grafana Loki* sangat ringan untuk diimplementasikan tetapi dengan fitur yang terbatas, sedangkan *ELK Stack* lebih banyak memakai resource *CPU* dan *Memory* tetapi mempunyai fitur yang lebih lengkap.

Kata kunci: Performa, Honeypot, ELK Stack, Grafana Loki

ABSTRACT

Along with the rapid development of technology, many platforms for log management and analysis from a computer have emerged, including the Grafana Loki platform and the ELK Stack. So that the impact of this development causes a lot of variation and ignorance of administrators in determining which platform suits their needs.

In this study, we analyze the performance of the second platform against the honeypot server during an attack with CPU and Memory usage parameters, the second parameter is the standard for administrators in considering which platform to choose.

The conclusion of this study is that based on the parameters used the Grafana Loki platform is more efficient in CPU and Memory usage than the ELK Stack platform, Grafana Loki is very light to implement but with limited features, while the ELK Stack uses more CPU and Memory resources but has features that more complete.

Keyword: *Performance, Honeypot, ELK Stack, Grafana Loki*

