Analisis Perbandingan Performa Metode ELK Stack dan Grafana Loki Pada Honeypot Server

Ach Izalul Haq[1], Banu Santoso[2]*
Program Studi Teknik Komputer[1], [2]
Universitas AMIKOM Yogyakarta
Jl. Ring Road Utara, Condong catur, Kec. Depok, Kabupaten Sleman, DI Yogyakarta 55284
ach.0084@students.amikom.ac.id[1], banu@amikom.ac.id[2]
*) *Corresponding Author: Banu Santoso*

Abstract*— Along with the rapid development of technology, many methods have emerged to manage and analyze logs from computers, including the Grafana Loki method and the ELK Stack. So the impact of this development causes a lot of variation and ignorance of the managers in determining which method suits their needs. This research analyzes the performance of both methods against the honeypot server when an attack occurs with CPU and Memory usage parameters; these two parameters become the standard for administrators in considering the method to be chosen. This study concludes that based on the parameters used, the Grafana Loki method is more efficient in terms of CPU and Memory usage compared to the ELK Stack method; Grafana Loki is very light to implement but with limited features, while the ELK Stack uses more CPU and Memory resources but has more complete features.

***Keywords*— Performance, Honeypot, ELK Stack, Grafana Loki**

Abstrak*— Seiring perkembangan teknologi yang begitu pesat, telah muncul banyak metode untuk manajemen dan analisis log dari sebuah komputer diantaranya metode *Grafana Loki* dan *ELK Stack*. Sehingga dampak dari perkembangan ini menimbulkan banyak variasi dan ketidaktahuan para administrator dalam menentukan metode mana yang sesuai dengan kebutuhan mereka. Pada penelitian ini menganalisis performa dari kedua metode tersebut terhadap server *honeypot* saat terjadi serangan dengan parameter penggunaan *CPU* dan *Memori*, kedua parameter tersebut merupakan standar untuk para administrator dalam mempertimbangkan metode yang akan dipilih. Kesimpulan dari penelitian ini bahwa berdasarkan parameter yang digunakan metode *Grafana Loki* lebih efisien dari segi pemakaian CPU dan Memori dibandingkan metode *ELK Stack*, *Grafana Loki* sangat ringan untuk diimplementasikan tetapi dengan fitur yang terbatas, sedangkan *ELK Stack* lebih banyak memakai resource *CPU* dan *Memori* tetapi mempunyai fitur yang lebih lengkap.

***Kata Kunci*— Performa, Honeypot, ELK Stack, Grafana Loki**

I. PENDAHULUAN

Keamanan merupakan hal yang sangat penting dalam dunia teknologi dan informasi. Jumlah serangan siber terus meningkat seiring berjalannya waktu, baik di dunia maupun di indonesia. Hal tersebut dapat dilihat dari data Badan Siber dan Sandi Negara, jumlah serangan yang terjadi pada tahun 2018 tercatat di angka 12.895.554 serangan, dan serangan *malware* tercatat di angka 512.863 serangan [1].

Tidak mungkin untuk melindungi jumlah serangan yang meningkat secara eksplosif dengan cara yang sempurna. Tetapi penting untuk meminimalisir akibatnya dengan mendeteksi sumber serangan dan menerapkan reaksi yang sesuai. Ponemon Institute mengatakan bahwa dibutuhkan biaya rata-rata $8.76 juta untuk menangani serangan [2].

Sebagai solusi untuk menangani masalah tersebut, dibutuhkan *tools* untuk membaca serangan yang mencoba masuk ke dalam server. *Honeypot* merupakan salah satu *tools* dalam keamanan komputer yang biasa digunakan, honeypot merupakan sistem yang dirancang untuk menjebak penyerang dengan harapan penyerang akan masuk dan mengeksploitasi server. *Honeypot* mempunyai keunggulan dalam investigasi untuk menganalisis ancaman, intensitas dan kerentanan keamanan server, Administrator sistem dapat menganalisa serangan menggunakan *honeypot*. secara garis besar, *honeypot* memiliki tiga tingkatan, yaitu interaksi rendah, interaksi menengah dan interaksi tinggi. Tingginya intensitas serangan pada *honeypot*, maka *log* yang dapat dianalisis semakin besar dan risiko yang diterima semakin besar pula [3].

Log merupakan komponen penting dalam sebuah sistem, pada implementasinya log berperan sebagai kolektor informasi yang terjadi di sebuah sistem, log menyimpan segala informasi yang terjadi pada sistem sehingga menyebabkan jumlah log akan semakin banyak, analisis log perlu dilakukan untuk mempermudah mendapatkan informasi dari ribuan bahkan jutaan baris log yang ada.

Bertepatan dengan tidak mudahnya menganalisis *log* yang dihasilkan oleh honeypot, maka dibutuhkan *tools* visualisasi untuk memudahkan dalam menganalisa *log honeypot dengan* cepat. Log management tool yang digunakan pada penelitian ini adalah *Grafana Loki* dan *ELK Stack*, hasil catatan *log honeypot* divisualisasikan menggunakan kedua metode tersebut, dimana *Grafana loki* ini merupakan kombinasi dari *Grafana, loki dan promtail* dan *ELK Stack* merupakan kombinasi dari *Elasticsearch, Logstash, Kibana.*

Tujuan dari penelitian ini adalah untuk membandingkan performa CPU dan Memori *Grafana Loki* dan *ELK Stack* sebagai platform yang digunakan untuk manajemen log dan sebagai acuan untuk mempermudah Sistem administrator memilih platform yang sesuai dengan kebutuhannya.

Beberapa penelitian yang terkait dengan penelitian ini terutama dari basis software, kemiripan metode yang digunakan dan juga objek yang digunakan, Perbedaan dari penelitian saat ini dengan penelitian yang sudah pernah dibuat yaitu akan

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v10i3.1177, Copyright ©2020
Submitted : June 7, 2021; Revised : October 30, 2021; Accepted : November 1, 2021; Published : December 1, 2021

membandingkan dua metode yang akan digunakan dalam penelitian ini yaitu ELK Stack dengan Grafana Loki untuk mengetahui keunggulan dan kelemahan dari kedua metode tersebut.

Pada Tabel 1 yang berisikan Ikhtisar Penelitian yang dilakukan oleh peneliti- peneliti sebelumnya menggunakan alat dan metode yang cukup beragam sehingga penelitian terlihat unik dan berbeda.

TABEL 1. IKHTISAR PENELITIAN

Peneliti/tahun	Lokasi	Kontribusi Penelitian	Metode
Son, S. J., & Kwon, Y. (2017) [4]	Mesin Virtual	Analisis Performa ELK Stack dan Splunk saat melakukan penanganan log	ELK Stack, Splunk
Li, T., Wu, J., Xue, L., Bao, D., Jiang, Y., Zeng, C., … Zhang, L. (2017) [5]	Mesin Virtual	Efisiensi waktu dalam mengelola dan menganalisis log	FLAP
Bandari Swamy Devender, Vamshi Krishna (2019) [6]	Mesin Virtual	Menganalisis performa ELK Stack saat melakukan Analisa Log dari perangkat jaringan	ELK Stack
Sukma, N., Srisawat, W., Sa-nga-ngam, P., & Leelasantitham, A. (2019) [7]	Mesin Virtual	Mempercepat Proses Analisis Log mengurangi biaya operasional IT	ELK Stack, Fluentd
Rochim, A. F., Aziz, M. A., & Fauzi, A. (2019) [8]	Mesin Virtual	Mempercepat Proses Analisa Log pada infrastruktur jaringan	ELK Stack
Penelitian ini	Digital Ocean	Menganalisis performa antara metode ELK Stack dan Grafana Loki dalam Menganalisis Log Honeypot	ELK Stack, Grafana Loki

A. Honeypot

Honeypot merupakan suatu tools keamanan yang dikembangkan untuk diserang dan di analisis, pada umumnya honeypot merupakan komputer, data, atau situs jaringan yang terlihat seperti bagian yang sesungguhnya, tetapi sebenarnya di isolasi dan dimonitor. Ketika dilihat dari sisi attacker yang akan menyerang, *honeypot* terlihat seperti layaknya sistem yang patut di serang, padahal penyerang tidak melakukan serangan ke sistem yang sebenarnya [9].

B. ELK Stack

ELK Stack adalah tools *open-source* yang berfungsi sebagai alat pengindeks data dan menampilkannya menjadi sebuah data yang menarik. *ELK Stack* terdiri dari tiga aplikasi, yaitu *Elasticsearch*, *Logstash*, *Kibana*. Ketiga aplikasi ini memiliki peran yang berbeda – beda:

1) *Elasticsearch*

Elasticsearch adalah sebuah mesin penyimpanan dan pencari data untuk dianalisis [10]. Dua proses yang sering digunakan untuk menganalisis data yaitu mengatur urutan data, dan mengorganisasikan nya kedalam suatu pola, kategori serta uraian dasar, Elasticsearch juga melakukan tahapan yang sama untuk menganalisis data. Pada *Elasticsearch* mempunyai proses *data ingestion*. Pada proses ini data baru diolah melalui beberapa tahapan yaitu penguraian, normalisasi, dan penambahan data sebelum dilakukan proses pengindeks, Pengindeks berfungsi untuk mempercepat aplikasi untuk mengorganisasikan data [11].

2) *Logstash*

Logstash merupakan salah satu komponen utama dari *ELK Stack*. *Logstash* berfungsi untuk melakukan pemrosesan data dan melakukan agregat kemudian mengirimkannya ke *Elasticsearch [12]*

3) *Kibana*

Kibana merupakan tools visualisasi dan manajemen untuk *Elasticsearch* yang dapat memberikan grafik, histogram, secara *real-time*, Kibana juga menyediakan fitur dashboard, fitur ini berfungsi untuk mengumpulkan data yang telah di visualisasi ke dalam halaman dashboard [13].

C. Grafana Loki

Grafana Loki merupakan platform open-source visualisasi dan logging untuk mengatur dan menganalisis log, Grafana Loki terdiri dari tiga aplikasi utama yaitu: Promtail, Loki, dan Grafana. Ketiga aplikasi ini memiliki peran yang berbeda beda

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v10i3.1177, Copyright ©2020
Submitted : June 7, 2021; Revised : October 30, 2021; Accepted : November 1, 2021; Published : December 1, 2021

[14].

1) *Promtail*

Promtail merupakan agen yang mengirimkan konten dari log lokal ke *instance* loki pribadi atau grafana *cloud* [15].

2) *Loki*

Loki merupakan komponen yang dapat disusun menjadi tumpukan *logging* memiliki fitur lengkap dengan hanya mengindeks label untuk log dan membiarkan pesan log asli tidak terindeks [16].

3) *Grafana*

Grafana merupakan software open-source untuk visualisasi dan analisis yang memungkinkan untuk memberikan peringatan dan menjelajahi metrik dimanapun disimpan [17].

D. Digital Ocean

Digital ocean adalah layanan komputer berbasis *cloud* dan *scalable*. Ini bukan hanya mesin virtual sederhana tetapi juga menawarkan layanan berbasis cloud yang berbeda, penyimpanan tambahan, keamanan, dan pemantauan serta menjalankan aplikasi yang berbeda secara efektif.

Berikut ini adalah fitur dan fungsi inti Digital ocean, *Deployment custom image*, aplikasi sekali klik, atau distribusi standar dimungkinkan dengan layanan Digital ocean. Koneksi yang andal dan harga tetap di 8 wilayah pusat data dimungkinkan dengan layanan cloud Digitalocean. Rencana Kinerja sesuai dengan kebutuhan bisnis pengguna ditawarkan oleh layanan cloud Digitalocean dengan baik [18].

II. METODE PENELITIAN

A. Alur Kerja Perancangan

Alur kerja perancangan merupakan tahapan – tahapan atau perancangan yang digunakan untuk merancang objek rancangan, alur kerja perancangan dibutuhkan untuk memudahkan dalam melakukan perancangan. Alur kerja perancangan dalam penelitian ini dapat dilihat pada Gambar 1.

B. Skema Sistem

1) *Skema Sistem Grafana Loki*

Dalam desain ini menjabarkan rencana secara umum tentang mekanisme sistem yang sudah dibuat. Desain yang telah dibuat pada Gambar 2.

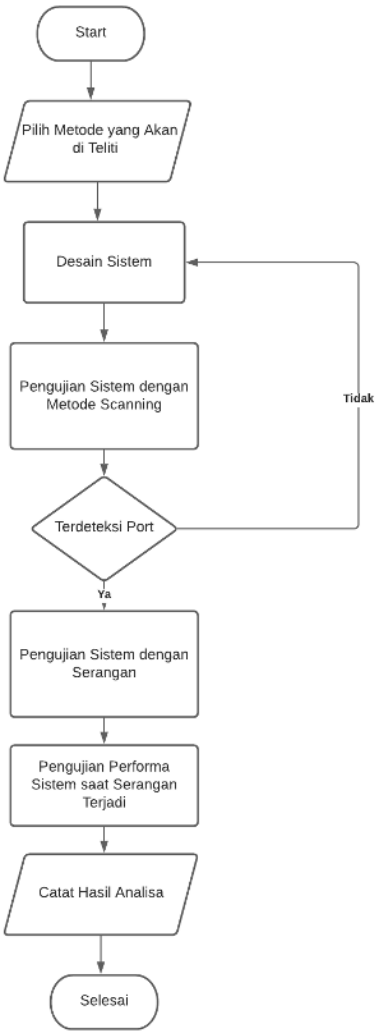
Pada desain diatas mengilustrasikan infrastruktur, *software* dan alur yang digunakan untuk metode Grafana Loki. Ada satu honeypot dipasang pada Ubuntu server, log yang dihasilkan honeypot akan berisi data serangan. Grafana Loki akan mengelola log dari honeypot yang dikirimkan kepada loki dan menampilkannya berupa visualisasi yang mudah dipahami di Grafana.

2) *Skema Sistem ELK Stack*

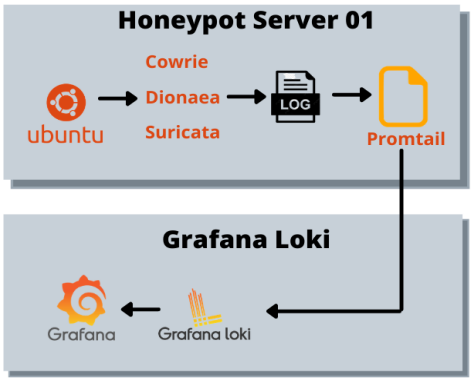
Dalam desain ini menjabarkan rencana secara umum tentang mekanisme sistem yang sudah dibuat. desain yang telah dibuat ditunjukkan pada Gambar 3.

3) *Skema Sistem Honeypot Server*

Ubuntu server digunakan sebagai server untuk menempatkan honeypot pada desain ini. Desain honeypot server ditunjukkan pada Gambar 4 dan Gambar 5.

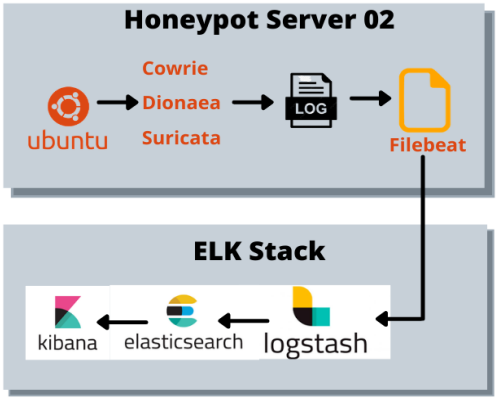


Gambar 1. Flowchart Penelitian

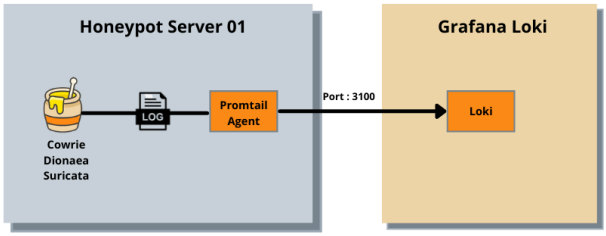


Gambar 2. Desain Sistem Metode Grafana Loki

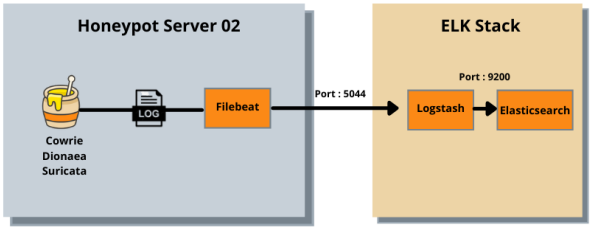
p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v10i3.1177, Copyright ©2020
Submitted : June 7, 2021; Revised : October 30, 2021; Accepted : November 1, 2021; Published : December 1, 2021



Gambar 3. Desain Sistem Metode ELK Stack



Gambar 4. Desain Sistem Honeypot Server untuk Grafana Loki



Gambar 5. Desain Sistem Honeypot Server untuk ELK Stack

Honeypot server terdiri dari satu honeypot yaitu cowrie honeypot dengan cara membuat lingkungan SSH untuk menjebak penyerang seolah-olah lingkungan tersebut merupakan SSH yang asli. *Cowrie* bekerja dengan cara mencatat serangan yang masuk dan mencoba masuk kedalam sistem melalui SSH oleh penyerang. *Log* yang tercatat dapat dianalisis, *log* yang tercatat akan di kirim honeypot server ke Grafana Loki melalui promtail sebagai agent di honeypot server mengirimkan ke Grafana Loki dengan port 3100, sedangkan filebeat akan mengirimkan log yang tercatat ke Logstash dengan port 5044 dan Logstash akan mengirimkan log tersebut ke Elasticsearch dengan port 9200.

Pada Tabel 2 terdapat port yang digunakan oleh cowrie honeypot beserta port yang digunakan oleh Grafana Loki dan pada Tabel 3 terdapat port yang digunakan oleh ELK Stack

TABEL 2. DAFTAR PORT GRAFANA LOKI

Nama Program	Port
Cowrie	22
Dionaea	21, 445, 3000, 3389
Suricata	80, 21, 22, 445
Loki	3100
Promtail	9080
Grafana	3000

TABEL 3. DAFTAR PORT ELK STACK

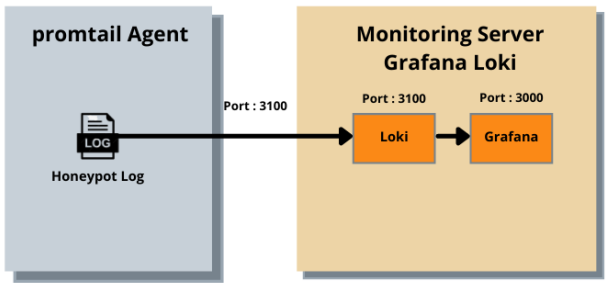
Nama Program	Port
Cowrie	22
Dionaea	21, 445, 3000, 3389
Suricata	80, 21, 22, 445
Filebeat	-
Logstash	5044
Elasticsearch	9200
Kibana	5601

4) *Skema Sistem Monitoring Server*

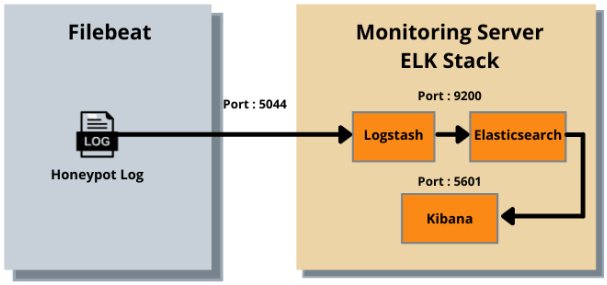
Grafana akan digunakan untuk mengelola log yang dicatat oleh cowrie honeypot pada arsitektur ini menjadi visualisasi yang mudah dipahami. Arsitektur monitoring server Grafana Loki ditunjukkan pada Gambar 6. Log yang dikirim dari promtail agent akan diterima oleh loki menggunakan port 3100. Promtail melakukan push data kepada loki dan loki mengumpulkan data tersebut dan menjadi penghubung antara promtail dengan grafana menggunakan port 3100. Pada grafana data akan diolah dan dianalisis dan ditampilkan melalui dashboard. Menggunakan Grafana mempermudah dalam memvisualisasikan data dalam bentuk tabel, grafik maupun log dan lain-lain. Pada penelitian ini akses grafana melalui IP local dari monitoring server Grafana Loki dengan port 3000, jadi hanya memungkinkan akses dari satu jaringan. Selain itu, grafana mempunyai validasi untuk user dan admin yang sudah ter registrasi untuk memvalidasi user dan admin yang berhak mengakses Grafana.

Kibana akan digunakan untuk mengelola log yang dicatat oleh cowrie honeypot pada arsitektur ini menjadi visualisasi yang mudah dipahami. Arsitektur monitoring server ELK Stack ditunjukkan pada Gambar 7. Log yang dikirim dari filebeat akan diterima oleh Logstash menggunakan port 5044. Logstash melakukan push data kepada Elasticsearch menggunakan port 9200. Pada Kibana data akan diolah dan dianalisis dan ditampilkan melalui dashboard. Menggunakan Kibana mempermudah dalam memvisualisasikan data dalam bentuk tabel, grafik maupun log dan lain-lain. Pada penelitian ini akses Grafana melalui IP local dari monitoring server *ELK Stack* dengan port 5601, jadi hanya memungkinkan akses dari satu jaringan. Selain itu, Kibana mempunyai validasi untuk user dan admin yang sudah ter registrasi untuk memvalidasi user dan admin yang berhak mengakses Kibana.

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v10i3.1177, Copyright ©2020
Submitted : June 7, 2021; Revised : October 30, 2021; Accepted : November 1, 2021; Published : December 1, 2021



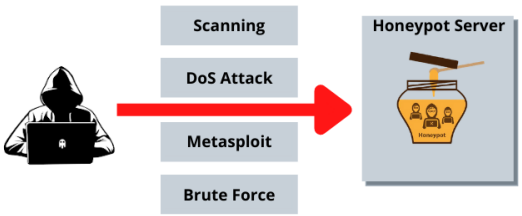
Gambar 6. Desain Sistem Monitoring Server untuk Grafana Loki



Gambar 7. Desain Sistem Monitoring Server untuk ELK Stack

5) *Skenario Serangan*

Honeypot server akan mendapat serangan pada tahapan simulasi kali ini. Pada pengujian kali ini akan dilakukan serangan dengan cara melakukan serangan langsung pada *cowrie honeypot*. Dalam tahap ini attacker akan berperan sebagai penyerang pada serangan tahap pertama dalam pengujian ini, ditunjukkan pada Gambar 8.



Gambar 8. Skenario Serangan Honeypot Server

Opsi serangan dan perintah yang digunakan untuk menyerang server honeypot dapat dilihat pada Tabel 4 dan Tabel 5, opsi serangan yang digunakan yaitu scanning menggunakan Nmap, Brute Force SSH menggunakan Hydra, Serangan DoS menggunakan LOIC, dan Serangan MS17-10 menggunakan Metasploit. Alasan menggunakan beberapa metode serangan berdasarkan tipe serangan yang umum digunakan oleh attacker.

TABEL 4. NAMA SERANGAN DAN PERINTAH UNTUK HONEYPOT SERVER 01

Opsi Serangan	Deskripsi
Scanning menggunakan Nmap	IP Target Serangan : 159.203.100.207 IP Penyerang : 182.1.77.146 Perintah : akses https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap# kemudian paste 159.203.100.207
Serangan Brute Force SSH menggunakan Hydra	IP Target Serangan : 159.203.100.207 IP Penyerang : 182.1.77.146 Perintah : hydra -L username.txt -P passwd.txt 159.203.100.207 ssh
Serangan DoS menggunakan (LOIC) Low Orbit Ion Cannon	IP Target Serangan : 159.203.100.207 IP Penyerang : 182.1.77.146 Perintah : flooding dengan ip tujuan 159.203.100.207 port 80, metode tcp, jumlah flood 10
Serangan MS17-10 menggunakan Metasploit	IP Target Serangan : 159.203.100.207 IP Penyerang : 182.1.77.146 Perintah : msf exploit(eternalblue_doublepulsar)> use auxiliary/scanner/smb/smb_ms17_010

TABEL 5. NAMA SERANGAN DAN PERINTAH UNTUK HONEYPOT SERVER 02

Opsi Serangan	Deskripsi
Scanning menggunakan *Nmap*	IP Target Serangan : 167.99.123.146 IP Penyerang : 182.1.77.146 Perintah : akses https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap# kemudian paste 167.99.123.146
Serangan *Brute Force* SSH menggunakan *Hydra*	IP Target Serangan : 167.99.123.146 IP Penyerang : 182.1.77.146 Perintah : hydra -L username.txt -P passwd.txt 167.99.123.146 ssh
Serangan DoS menggunakan *(LOIC) Low Orbit Ion Cannon*	IP Target Serangan : 167.99.123.146 IP Penyerang : 182.1.77.146 Perintah : flooding dengan ip tujuan 167.99.123.146 port 80, metode tcp, jumlah flood 10
Serangan MS17-10 menggunakan *Metasploit*	IP Target Serangan : 167.99.123.146 IP Penyerang : 182.1.77.146 Perintah : msf exploit(eternalblue_doublepulsar)> use auxiliary/scanner/smb/smb_ms17_010

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v10i3.1177, Copyright ©2020
Submitted : June 7, 2021; Revised : October 30, 2021; Accepted : November 1, 2021; Published : December 1, 2021

6) *Pengujian Performa*

Pengujian performa dilakukan untuk melihat performa sistem pada saat terjadi serangan pada honeypot server dan performa sistem ketika proses pengiriman log dari server honeypot menuju ELK Stack dan Grafana Loki. Parameter yang digunakan adalah penggunaan resource CPU dan Memori Pada masing-masing metode. Untuk mendapatkan data tersebut yang sedang diuji menggunakan Glances.

7) *Perancangan Visualisasi*

Visualisasi pada penelitian ini menggunakan Grafana dan Kibana untuk menampilkan log yang diproduksi cowrie honeypot menjadi lebih menarik. Rancangan dashboard Grafana ditunjukkan pada Gambar 9. Dashboard Grafana akan memiliki empat panel terdiri dari log panel, login gagal, login berhasil, dan jumlah percobaan login. Pada Grafana data akan diambil dari data source loki kemudian akan ditampilkan di setiap panel menggunakan *LogQL* untuk memberikan filter sesuai dengan yang ingin tampilkan.

Rancangan dashboard Kibana ditunjukkan pada Gambar 10. Dashboard Kibana akan memiliki empat panel terdiri dari log panel, login gagal, login berhasil, dan jumlah percobaan login. Pada Grafana data akan diambil dari *index pattern* filebeat kemudian akan ditampilkan di setiap panel menggunakan filter Kibana untuk memberikan filter sesuai dengan yang ingin tampilkan.

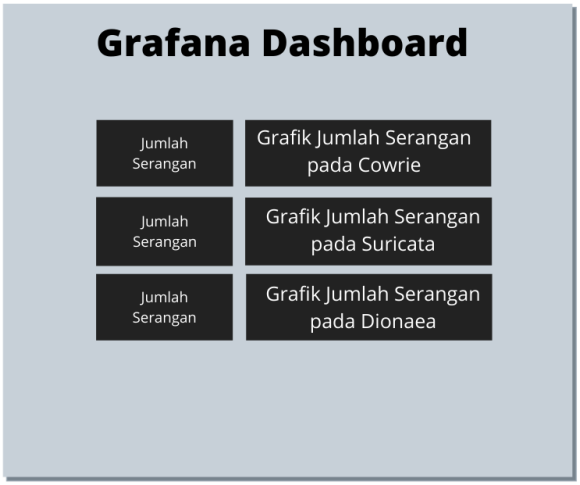
III. HASIL DAN PEMBAHASAN

A. Hasil Pengujian

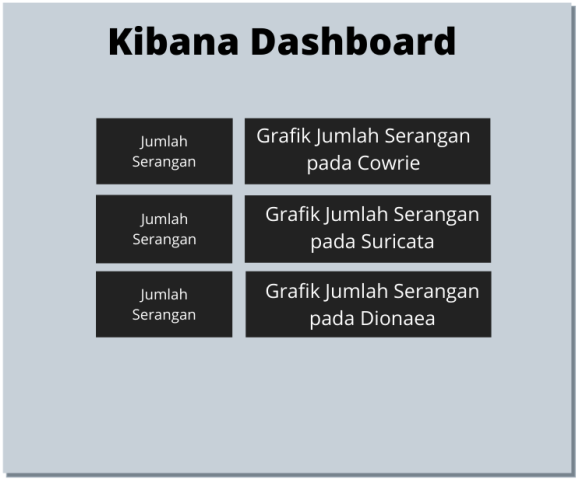
Setelah proses implementasi sistem dilakukan, uji coba penyerangan dijalankan. Pada tahap ini dilakukan pengujian sebanyak 30 kali dengan metode yang sama untuk mendapatkan data yang akurat. Pengujian dilakukan untuk mengetahui performa dari Grafana Loki dan ELK Stack saat menangani serangan adapun parameter yang diambil adalah penggunaan *CPU* dan *Memory*.

1) *Hasil Pengujian Serangan DOS*

Hasil pengujian pada Tabel 6 menunjukkan bahwa penggunaan CPU tertinggi pada loki terjadi pada serangan ke 19 dengan CPU terpakai 25.1 pada Loki, sedangkan pada Logstash pemakaian CPU tertinggi terjadi pada serangan kelima dengan jumlah pemakaian CPU 42.9 dan pada Elasticsearch pemakaian CPU tertinggi 87.8 terjadi pada serangan ke 29, Kibana di angka 45.3 pada serangan ke 14.



Gambar 9. Rancangan Dashboard Grafana



Gambar 10. Rancangan Dashboard Grafana

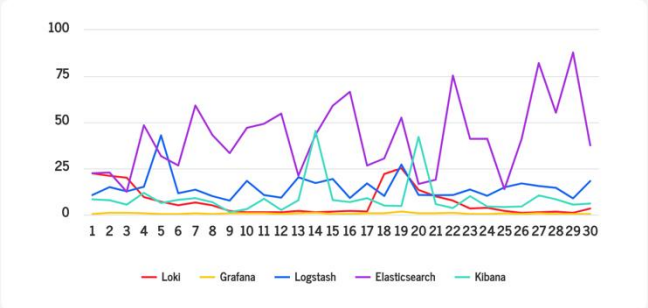
TABEL 6. HASIL PENGUJIAN SERANGAN DOS

No	SURICATA(DOS)									
	GRAFANA LOKI				ELK STACK					
	CPU %		MEM %		CPU %			MEM %		
	Loki	Grafana	Loki	Grafana	Logstash	Elastic	Kibana	Logstash	Elastic	Kibana
1	22.3	0.3	3.6	1.7	10.6	22.4	8.3	20.1	35.9	8.1
2	21.0	1.0	3.6	1.7	14.9	22.8	7.8	20.1	36.0	8.1
3	20.0	1.0	3.6	1.7	12.6	12.4	5.4	20.1	35.9	8.0
4	9.5	0.7	3.6	1.7	15.1	48.4	11.8	20.1	36.0	8.0
5	7.0	0.3	3.6	1.7	42.9	31.7	6.3	20.1	36.0	8.0
6	5.1	0.3	3.6	1.7	11.6	26.6	8.0	20.1	36.0	7.6
7	6.6	0.7	3.6	1.7	13.5	59.1	8.9	20.1	36.0	7.6
8	5.0	0.3	3.6	1.7	10.0	43.0	6.7	20.1	36.0	7.6
9	2.0	0.7	3.6	1.7	7.6	33.3	1.4	20.1	35.9	7.6
10	1.3	0.7	3.6	1.7	18.3	47.0	3.0	20.1	35.9	7.6
11	1.3	0.7	3.6	1.7	10.6	49.2	8.6	20.1	35.9	7.6
12	1.3	0.3	3.6	1.7	9.2	54.7	2.5	20.1	35.9	7.6

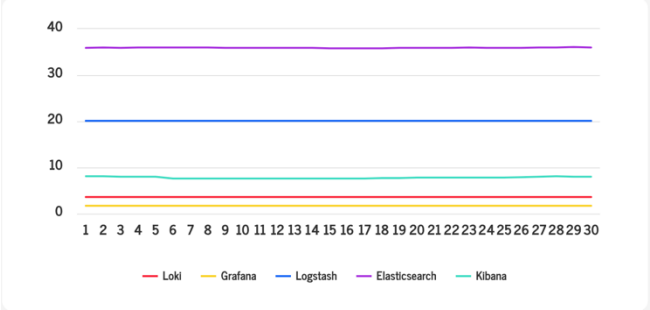
p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v10i3.1177, Copyright ©2020
Submitted : June 7, 2021; Revised : October 30, 2021; Accepted : November 1, 2021; Published : December 1, 2021

13	2.0	0.7	3.6	1.7	20.2	21.1	7.8	20.1	35.9	7.6
14	1.3	1.0	3.6	1.7	17.1	43.3	45.3	20.1	35.9	7.6
15	1.6	0.3	3.6	1.7	19.3	59.0	7.9	20.1	35.8	7.6
16	2.0	0.3	3.6	1.7	9.0	66.5	6.8	20.1	35.8	7.6
17	1.7	0.7	3.6	1.7	16.9	26.6	8.9	20.1	35.8	7.6
18	22.0	0.7	3.6	1.7	10.1	30.4	4.9	20.1	35.8	7.7
19	25.1	1.7	3.6	1.7	27.1	52.5	4.7	20.1	35.9	7.7
20	13.4	0.7	3.6	1.7	10.7	16.6	42.1	20.1	35.9	7.8
21	9.9	0.7	3.6	1.7	10.5	18.9	5.7	20.1	35.9	7.8
22	7.6	1.0	3.6	1.7	10.6	75.3	3.6	20.1	35.9	7.8
23	3.3	0.3	3.6	1.7	13.6	41.0	10.0	20.1	36.0	7.8
24	3.7	0.3	3.6	1.7	10.2	41.1	4.4	20.1	35.9	7.8
25	2.0	0.7	3.6	1.7	14.8	13.8	4.1	20.1	35.9	7.8
26	1.0	0.3	3.6	1.7	16.9	40.9	4.4	20.1	35.9	7.9
27	1.3	0.7	3.6	1.7	15.5	82.1	10.4	20.1	36.0	8.0
28	1.6	0.3	3.6	1.7	14.5	55.2	8.3	20.1	36.0	8.1
29	1.0	0.3	3.6	1.7	8.8	87.8	5.4	20.1	36.1	8.0
30	3.3	0.3	3.6	1.7	18.2	37.5	6.0	20.1	36.0	8.0

Untuk pemakaian memori pada loki sangat stabil di angka 3.6 dan Grafana di angka 1.7. untuk pemakaian memori Logstash stabil di angka 20.1 dan Elasticsearch di angka 35.9 sedangkan Kibana mencatat pemakaian memori tertinggi di angka 8.1. Grafik hasil pengujian dapat dilihat pada Gambar 11 dan Gambar 12.



Gambar 11. Grafik Penggunaan CPU pada Serangan DOS



Gambar 12. Grafik Penggunaan Memori pada Serangan DOS

2) *Hasil Pengujian Serangan MS17-10*

Hasil pengujian pada Tabel 7 menunjukkan bahwa penggunaan CPU tertinggi pada loki terjadi pada serangan ke 24 dan 30 dengan CPU terpakai 8.6 pada Loki, sedangkan pada Logstash pemakaian CPU tertinggi terjadi pada serangan kelima dengan jumlah pemakaian CPU 84.0 dan pada Elasticsearch pemakaian CPU tertinggi 99.3 terjadi pada serangan ke 29, Kibana 11.7 pada serangan ke 11.

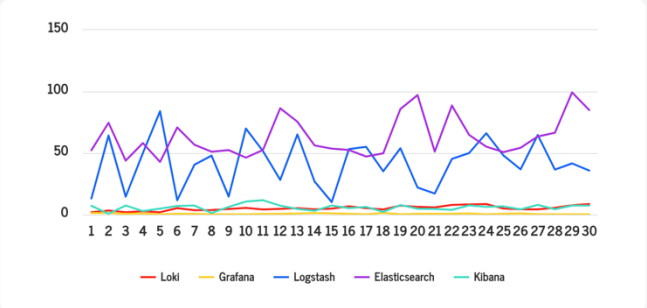
TABEL 7. HASIL PENGUJIAN SERANGAN DOS MS17-10

No	DIONAEA(MS17-10)									
	GRAFANA LOKI				ELK STACK					
	CPU %		MEM %		CPU %			MEM %		
	Loki	Grafana	Loki	Grafana	Logstash	Elastic	Kibana	Logstash	Elastic	Kibana
1	2.0	1.3	2.7	1.7	13.1	52.3	7.2	20.2	35.7	7.7
2	3.3	1.3	2.7	1.7	64.2	74.6	0.7	20.2	35.6	7.6
3	2.0	0.7	2.7	1.7	14.6	43.9	7.4	20.2	35.6	7.7
4	2.7	1.0	2.7	1.7	50.0	58.1	2.9	20.3	35.6	7.7
5	2.0	0.3	2.7	1.7	84.0	42.8	4.9	20.3	35.6	7.8
6	5.3	0.7	2.7	1.7	11.7	70.8	7.0	20.3	35.6	7.8
7	3.6	0.7	2.7	1.7	40.5	56.8	7.4	20.3	35.6	7.9
8	3.7	0.3	2.7	1.7	47.9	51.1	1.3	20.3	35.7	7.9
9	4.6	0.3	2.7	1.7	14.7	52.4	6.3	20.3	35.8	8.0
10	5.5	0.3	2.7	1.7	69.9	46.3	10.6	20.3	35.8	7.9
11	4.2	0.6	2.7	1.7	51.5	52.6	11.7	20.3	35.7	7.9
12	4.7	0.7	2.7	1.7	28.2	86.4	7.3	20.3	35.7	7.9
13	5.3	0.9	2.7	1.7	65.1	75.5	4.6	20.3	35.7	7.9
14	4.3	1.3	2.7	1.7	26.9	56.2	3.1	20.3	35.7	7.9
15	4.9	1.0	2.7	1.7	10.2	53.6	7.4	20.3	35.6	7.6
16	6.7	0.7	2.7	1.7	53.2	52.5	5.3	20.3	35.6	7.6

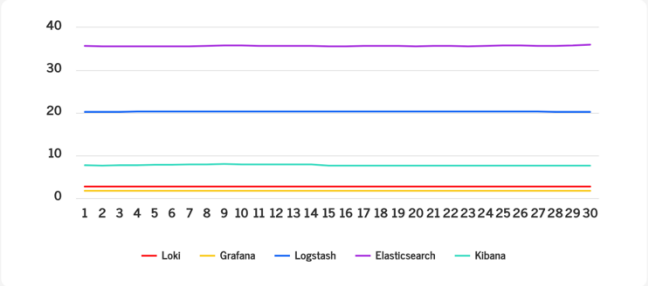
p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v10i3.1177, Copyright ©2020
Submitted : June 7, 2021; Revised : October 30, 2021; Accepted : November 1, 2021; Published : December 1, 2021

17	5.3	0.3	2.7	1.7	55.1	47.2	6.3	20.3	35.7	7.6
18	4.2	1.4	2.7	1.7	35.2	49.8	2.2	20.3	35.7	7.6
19	7.3	0.3	2.7	1.7	53.9	85.8	7.8	20.3	35.7	7.6
20	6.3	0.7	2.7	1.7	22.0	97.1	4.8	20.3	35.6	7.6
21	5.9	0.7	2.7	1.7	17.1	51.2	4.6	20.3	35.7	7.6
22	7.9	0.7	2.7	1.7	45.3	88.6	3.9	20.3	35.7	7.6
23	8.3	1.0	2.7	1.7	50.0	64.8	7.5	20.3	35.6	7.6
24	8.6	0.3	2.7	1.7	66.1	55.2	6.3	20.3	35.7	7.6
25	5.0	0.7	2.7	1.7	48.1	50.8	6.7	20.3	35.8	7.6
26	4.3	1.0	2.7	1.7	36.8	54.3	4.3	20.3	35.8	7.6
27	4.3	0.3	2.7	1.7	64.7	63.5	7.9	20.3	35.7	7.6
28	5.6	0.3	2.7	1.7	36.6	66.5	4.4	20.2	35.7	7.6
29	7.6	0.3	2.7	1.7	41.6	99.3	7.3	20.2	35.8	7.6
30	8.6	0.3	2.7	1.7	35.8	84.9	7.3	20.2	36.0	7.6

Untuk pemakaian memori pada loki stabil di angka 2.7 dan Grafana di angka 1.7. untuk pemakaian memori Logstash stabil di angka 20.3 dan Elasticsearch di angka 35.7 sedangkan Kibana mencatat pemakaian memori tertinggi di angka 8.0. Grafik hasil pengujian dapat dilihat pada Gambar 13 dan Gambar 14.



Gambar 13. Grafik Penggunaan CPU pada Serangan MS17-10



Gambar 14. Grafik Penggunaan Memori pada Serangan MS17-10

3) *Hasil Pengujian Serangan Brute Force*

Hasil pengujian pada Tabel 8 menunjukkan bahwa penggunaan CPU tertinggi pada loki terjadi pada serangan ke 26 dengan CPU terpakai 3.0 pada Loki, sedangkan pada Logstash pemakaian CPU tertinggi terjadi pada serangan ke 22 dengan jumlah pemakaian CPU 9.4 dan pada Elasticsearch pemakaian CPU tertinggi 22.0 terjadi pada serangan ke 1, Kibana di angka 25.7 pada serangan ke 17.

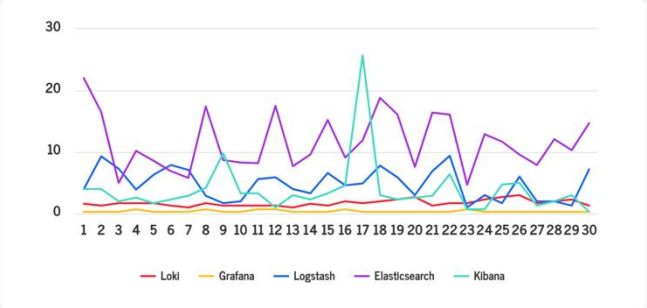
TABEL 8. HASIL PENGUJIAN SERANGAN BRUTE FORCE

No	COWRIE(Brute Force)									
	GRAFANA LOKI				ELK STACK					
	CPU %		MEM %		CPU %			MEM %		
	Loki	Grafana	Loki	Grafana	Logstash	Elastic	Kibana	Logstash	Elastic	Kibana
1	1.6	0.3	3.6	1.8	4.0	22.0	4.0	17.9	35.6	7.4
2	1.3	0.3	3.6	1.8	9.3	16.5	4.0	17.9	35.6	7.4
3	1.7	0.3	3.6	1.8	7.3	5.0	2.0	17.9	35.6	7.4
4	1.7	0.7	3.6	1.8	3.9	10.2	2.6	17.9	35.6	7.4
5	1.7	0.3	3.6	1.8	6.3	8.6	1.7	17.9	35.6	7.4
6	1.3	0.3	3.6	1.8	7.9	6.9	2.3	17.9	35.6	7.4
7	1.0	0.3	3.6	1.8	7.1	5.8	2.9	17.9	35.6	7.4
8	1.7	0.7	3.6	1.8	2.9	17.4	4.2	17.9	35.6	7.4
9	1.3	0.3	3.6	1.8	1.7	8.7	9.8	17.9	35.6	7.4
10	1.3	0.3	3.6	1.8	2.0	8.3	3.3	17.9	35.6	7.4
11	1.3	0.7	3.6	1.8	5.6	8.2	3.3	17.9	35.6	7.4
12	1.3	0.7	3.6	1.8	5.9	17.5	1.0	17.9	35.6	7.4
13	1.0	0.3	3.6	1.8	4.0	7.7	3.0	17.9	35.6	7.4
14	1.6	0.3	3.6	1.8	3.3	9.6	2.3	17.9	35.6	7.4
15	1.3	0.3	3.6	1.8	6.6	15.2	3.3	17.9	35.6	7.4
16	2.0	0.7	3.6	1.8	4.6	9.1	4.6	17.9	35.6	7.4
17	1.7	0.3	3.6	1.8	4.9	11.9	25.7	17.9	35.6	7.4
18	2.0	0.3	3.6	1.8	7.8	18.8	3.0	17.9	35.6	7.4
19	2.3	0.3	3.6	1.8	5.9	16.1	2.3	17.9	35.6	7.4
20	2.7	0.3	3.6	1.8	3.0	7.6	2.6	17.9	35.5	7.4
21	1.3	0.3	3.6	1.8	6.9	16.4	2.9	17.9	35.5	7.4
22	1.7	0.3	3.6	1.8	9.4	16.1	6.4	17.9	35.5	7.4
23	1.7	0.7	3.6	1.8	1.0	4.7	0.7	17.9	35.5	7.4

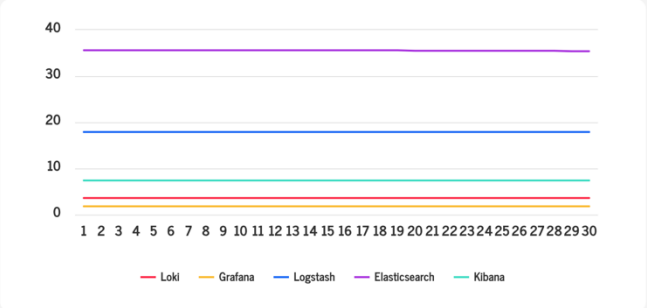
p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v10i3.1177, Copyright ©2020
Submitted : June 7, 2021; Revised : October 30, 2021; Accepted : November 1, 2021; Published : December 1, 2021

24	2.3	0.3	3.6	1.8	3.0	12.9	0.7	17.9	35.5	7.4
25	2.7	0.3	3.6	1.8	1.7	11.7	4.7	17.9	35.5	7.4
26	3.0	0.3	3.6	1.8	6.0	9.6	5.0	17.9	35.5	7.4
27	1.7	0.3	3.6	1.8	2.0	7.9	1.3	17.9	35.5	7.4
28	2.0	0.3	3.6	1.8	2.0	12.1	2.0	17.9	35.5	7.4
29	2.3	0.3	3.6	1.8	1.3	10.3	3.0	17.9	35.4	7.4
30	1.3	0.3	3.6	1.8	7.2	14.7	0.3	17.9	35.4	7.4

Untuk pemakaian memori pada loki stabil di angka 3.6 dan Grafana di angka 1.8. untuk pemakaian memori Logstash stabil di angka 17.9 dan Elasticsearch di angka 35.6 sedangkan Kibana stabil di angka 7.4. Grafik hasil pengujian dapat dilihat pada Gambar 15 dan Gambar 16.



Gambar 15. Grafik Penggunaan CPU pada Serangan Brute Force



Gambar 16. Grafik Penggunaan Memori pada Serangan Brute Force

IV. KESIMPULAN

Kesimpulan yang dapat diambil setelah menyelesaikan penelitian ini menunjukkan bahwa metode *Grafana Loki* sangat efisien dalam penggunaan *CPU* dan *Memory* berdasarkan hasil percobaan pada bab sebelumnya, penggunaan *CPU* tertinggi *Loki* mencatat angka 25.1 sedangkan Grafana mencatat penggunaan *CPU* tertinggi di angka 1.7. Sedangkan penggunaan *Memory* tertinggi *Loki* tercatat 3.6 dan Grafana 1.8. Metode *ELK Stack* berhasil mencatat penggunaan *CPU* tertinggi pada *Logstash* 84.0, *Elasticsearch* 99.3 dan Kibana 45.3, Sedangkan penggunaan *memory* tertinggi *Logstash* 20.3, *Elasticsearch* 36.1, dan *Kibana* 8.1.

Berdasarkan hasil uji coba *Grafana Loki* sangat ringan untuk diimplementasikan tetapi memiliki fitur yang terbatas sedangkan *ELK Stack* lebih banyak memakan *resource CPU* dan *Memory* tetapi memiliki fitur yang lebih lengkap.

Keterbatasan akses pada platform enterprise menyebabkan kendala dalam membandingkan antara platform opensource dan enterprise, untuk pengguna dari platform monitoring dan manajemen log agar memilih sesuai dengan kebutuhan untuk efisiensi biaya saat proses implementasi.

REFERENSI

[1] D. Hariyadi and F. Fazlurrahman, 'MEMBANGUN TELEGRAMBOT UNTUK CRAWLING MALWARE OSINT MENGGUNAKAN RASPBERRY PI', *IJUBI*, vol. 2, no. 1, p. 18, Jun. 2019, doi: 10.21927/ijubi.v2i1.996.

[2] M. Aldairi, L. Karimi, and J. Joshi, 'A Trust Aware Unsupervised Learning Approach for Insider Threat Detection', in *2019 IEEE 20th International Conference on Information Reuse and Integration for Data Science (IRI)*, Los Angeles, CA, USA, Jul. 2019, pp. 89–98. doi: 10.1109/IRI.2019.00027.

[3] D. K. Rahmatullah, S. M. Nasution, and F. Azmi, 'Implementation of low interaction web server honeypot using cubieboard', in *2016 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC)*, Bandung, Indonesia, Sep. 2016, pp. 127–131. doi: 10.1109/ICCEREC.2016.7814970.

[4] S. J. Son and Y. Kwon, 'Performance of ELK stack and commercial system in security log analysis', in *2017 IEEE 13th Malaysia International Conference on Communications (MICC)*, Johor Bahru, Nov. 2017, pp. 187–190. doi: 10.1109/MICC.2017.8311756.

[5] T. Li *et al.*, 'FLAP: An End-to-End Event Log Analysis Platform for System Management', in *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Halifax NS Canada, Aug. 2017, pp. 1547–1556. doi: 10.1145/3097983.3098022.

[6] S. Adike, V. Krishna, and B. S. Devender, 'Design and Performance of an Event Handling and Analysis Platform for vSGSN-MME event using the ELK stack', p. 65.

[7] N. Sukma, W. Srisawat, P. Sa-nga-ngam, and A. Leelasantitham, 'An Analysis of Log Management Practices to reduce IT Operational Costs Using Big Data Analytics', in *2019 4th Technology Innovation Management and Engineering Science International Conference (TIMES-iCON)*, Bangkok, Thailand, Dec. 2019, pp. 1–5. doi: 10.1109/TIMES-iCON47539.2019.9024400.

[8] A. F. Rochim, M. A. Aziz, and A. Fauzi, 'Design Log Management System of Computer Network Devices Infrastructures Based on ELK Stack', in *2019 International Conference on Electrical Engineering and Computer Science (ICECOS)*, Batam Island, Indonesia, Oct. 2019, pp. 338–342. doi: 10.1109/ICECOS47637.2019.8984494.

[9] M. M. Mustofa and E. Aribowo, 'PENERAPAN SISTEM KEAMANAN HONEYPOT DAN IDS PADA JARINGAN NIRKABEL (HOTSPOT)', vol. 1, p. 8, 2013.

[10] A. P. Atmaja and S. V. Yulianto, 'Pemanfaatan Elasticsearch untuk Temu Kembali Informasi Tugas Akhir', *TEKNOSI*, vol. 4, no. 3, pp. 160–167, Jan. 2019, doi: 10.25077/TEKNOSI.v4i3.2018.160-167.

[11] M. Bajer, 'Building an IoT Data Hub with Elasticsearch, Logstash and Kibana', in *2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, Prague, Aug. 2017, pp. 63–68. doi: 10.1109/FiCloudW.2017.101.

[12] W. Sholihah, S. Pripambudi, and A. Mardiyono, 'Log Event Management Server Menggunakan Elastic Search Logstash Kibana (ELK Stack)', *jtim*, vol. 2, no. 1, pp. 12–20, May 2020, doi: 10.35746/jtim.v2i1.79.

[13] P. H. Putra, 'IMPLEMENTASI LOG MANAGEMENT SERVER MENGGUNAKAN ELK (ELASTIC SEARCH, LOGSTASH DAN KIBANA) STACK PADA SERVER WEB SNORT DI PT.XYZ', p. 7, 2020.

[14] O. Márton, 'Integration of standard datasources with interactive data visualization solutions', p. 51.

[15] M. Brattstrom and P. Morreale, 'Scalable Agentless Cloud Network Monitoring', in *2017 IEEE 4th International Conference on Cyber*

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v10i3.1177, Copyright ©2020
Submitted : June 7, 2021; Revised : October 30, 2021; Accepted : November 1, 2021; Published : December 1, 2021

Security and Cloud Computing (CSCloud), New York, NY, USA, Jun. 2017, pp. 171–176. doi: 10.1109/CSCloud.2017.11.

[16] A. H. C. Mukai *et al.*, 'Architecture of the data aggregation and streaming system for the European Spallation Source neutron instrument suite', *J. Inst.*, vol. 13, no. 10, pp. T10001–T10001, Oct. 2018, doi: 10.1088/1748-0221/13/10/T10001.

[17] E. Betke and J. Kunkel, 'Real-Time I/O-Monitoring of HPC Applications with SIOX, Elasticsearch, Grafana and FUSE', in *High Performance Computing*, vol. 10524, J. M. Kunkel, R. Yokota, M. Taufer, and J. Shalf, Eds. Cham: Springer International Publishing, 2017, pp. 174–186. doi: 10.1007/978-3-319-67630-2_15.

[18] P. K. Paul, P. S. Aithal, R. Saavedra, B. Aremu, and P. Baby, 'Cloud Service Providers: An Analysis of Some Emerging Organizations and Industries', p. 12.

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v10i3.1177, Copyright ©2020
Submitted : June 7, 2021; Revised : October 30, 2021; Accepted : November 1, 2021; Published : December 1, 2021