RANCANG BANGUN INTRUSION DETECTION SYSTEM MENGGUNAKAN SNORT UNTUK MONITORING KEAMANAN JARINGAN DENGAN VISUALISASI ELASTIC STACK DAN NOTIFIKASI TELEGRAM

SKRIPSI

MUHAMMAD HAFIZH

1907422024

PROGRAM STUDI TEKNIK MULTIMEIDA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA & KOMPUTER

POLITEKNIK NEGERI JAKARTA

2024

RANCANG BANGUN INTRUSION DETECTION SYSTEM MENGGUNAKAN SNORT UNTUK MONITORING KEAMANAN JARINGAN DENGAN VISUALISASI ELASTIC STACK DAN NOTIFIKASI TELEGRAM

SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk Memperoleh Diploma Empat Politeknik

MUHAMMAD HAFIZH

1907422024

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA & KOMPUTER

POLITEKNIK NEGERI JAKARTA

2024

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini :

Nama	: Muhammad Hafizh
NIM	: 1907422024
Jurusan/ProgramStudi	: T.Informatika dan Komputer / Teknik Multimedia dan Jaringan
Judul Skripsi	: Rancang Bangun Intrusion Detection System Menggunakan snort untuk monitoring keamanan dengan visualisasi elastic stack dan notifikasi telegram.

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandungg ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 30 Agustus 2024

Yang membuat pernyataan,

(Muhammad Hafizh)

NIM. 1907422024

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

LEMBAR PENGESAHAN

Skripsi diajukan oleh :

Nama : Muhammad Hafizh
NIM : 1907422024
Program Studi : Teknik Multimedia dan Jaringan
Judul Skripsi : Rancang Bangun Intrusion Detection System menggunakan Snort untuk Monitoring Keamanan Jaringan dengan visualisasi elastic stack dan notifikasi telegram.

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari senin, Tanggal 26, Bulan Agustus Tahun 2024 dan dinyatakan **LULUS**.

Disahkan oleh :

Pembimbing I : Fachroni Arbi Murad, S.Kom., M.Kom.
Penguji I : Dr. Indra Hermawan, S.Kom., M.Kom. ( )
Penguji II : Ariawan Andi Suhandana, S.Kom., M.T.I. ( )
Penguiji III : Syamsi Dwi Cahya, S.Kom., M.Kom. ( )

Mengetahui :
Jurusan Teknik Informatika dan Komputer
Ketua

Dr. Anita Hidayati, S.Kom., M.Kom.
NIP. 197908032003122003

KATA PENGANTAR

Puji Syukur saya panjatkan kepada Allah SWT, atas berkat dan Rahmatnya, Penulis dapat menyelesaikan Laporan Skripsi ini. Penulisan Laporan Skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar sarjana Politeknik. Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa Perkuliahan sampai Pada Penyusunan Laporan Skripsi, sangatlah sulit bagi penulis untuk menyelesaikan skripsi ini. Oleh karena itu, Penulis mengucapkan terima kasih kepada:

a. Bapak Fachroni Arbi Murad S.Kom., M.Kom Selaku Dosen Pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan penulis dalam penyusunan skripsi ini sampai selesai.
b. Ayah dan Bunda yang selalu memberikan motivasi dan semangat kepada penulis dalam rangka penyusunan laporan skripsi ini.
c. Seluruh Staf, Helper dan Administrasi Jurusan tik yang telah memberikan fasilitas serta prasarana kepada penulis dalam mengerjakan skripsi ini hingga larut malam.
d. Ibu Ayu Rosyida Zain, S.ST., M.T Selaku ketua Program Studi Teknik Multimedia dan Jaringan yang telah memberikan semangat, motivasi, kritikan, dan saran dalam mengerjakan serta penyusunan pada Laporan Skripsi ini.

Dalam Penulisan Skripsi ini masih banyak kekurangan dan kesalahan, oleh karena itu penulis menerima atas kritikan dan masukan yang membangun dalam menyempurnakan pada penulisan laporan skripsi ini serta bermanfaat bagi penulis serta para pembaca.

Depok, 3 0 Agustus 2024

Muhammad Hafizh

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan dibawah ini:

Nama : Muhammad Hafizh

NIM : 1907422024

Jurusan/ProgramStudi : Teknik Informatika dan Komputer / TMJ

Demi pengembangan ilmu pengetahuan , menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul:

RANCANG BANGUN INTRUSION DETECTION SYSTEM MENGGUNAKAN SNORT UNTUK MONITORING KEAMANAN JARINGAN DENGAN VISUALISASI ELASTIC STACK DAN NOTIFIKASI TELEGRAM.

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalihmediakan/formatkan,mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyatan ini saya buat dengan sebenarnya.

Depok, 30 Agustus 2024

Yang Membuat Pernyataan

(Muhammad Hafizh)

NIM.1907422024

RANCANG BANGUN INTRUSION DETECTION SYSTEM MENGGUNAKAN SNORT UNTUK MONITORING KEAMANAN JARINGAN DENGAN VISUALISASI ELASTIC STACK DAN NOTIFIKASI TELEGRAM

ABSTRAK

Keamanan jaringan komputer merupakan aspek krusial yang perlu diawasi secara terus menerus untuk mencegah serangan dan intrusi yang dapat merugikan. Namun, banyak organisasi masih menghadapi tantangan dalam mengidentifikasi dan merespon ancaman secara efisien. seiring dengan pesatnya perkembangan teknologi, keamanan jaringan komputer menjadi aspek yang sangat penting untuk terus memantau keamanan sistem. oleh karena itu mengingat berbagai ancaman dapat menyerang sistem kapan saja, maka diperlukan sebuah aplikasi yang mampu mendeteksi ancaman tersebut secara real time. Permasalahan tersebut mendorong penulis untuk memanfaatkan salah satu open source atau tools yaitu snort dengan menggunakan metode IDS untuk mendeteksi adanya serangan. Snort akan menampilkan alert ketika ada paket yang mencurigakan. alert yang dihasilkan dapat disimpan ke dalam log. tujuan dari penelitian ini adalah untuk mengimplementasikan serta membangun sistem IDS pada Snort yang dapat memantau keamanan jaringan dengan visualisasi elk (elasticsearch, logstash, dan kibana) stack yang dapat memudahkan administrator dalam membaca dan menganalisis log. alert yang muncul di ELK akan dikirimkan ke ponsel administrator melalui aplikasi telegram. Administrator jaringan akan menerima informasi secara real time terkait serangan yang terjadi pada jaringan. selain itu juga dilakukan konfigurasi sistem dan pengujian serangan dengan menggunakan port scanning, DDOS Attack, dan Brute force. Dari hasil penelitian yang telah dilakukan, Implementasi IDS Pada Snort dan Elk stack berhasil dilakukan untuk melakukan deteksi serangan pada server JTIK serta memvisualisasikan banyaknya data alert pada jaringan yang masuk pada Log yang berasal dari snort, kemudian untuk telegram berhasil menerima notifikasi yang diberikan kepada server JTIK dalam melakukan deteksi serangan yang diujikan. Penelitian ini menghasilkan nilai rata rata waktu untuk deteksi dan mengirimkan respon time notifikasi ke telegram saat terjadi serangan Port scanning, DDOS Attack, dan Brute force secara berurut adalah 17.77 detik untuk TCP Scan, 34.40 detik untuk fin scan, 34.38 detik untuk Xmas scan, dan 34.41 detik untuk null scan. sedangkan untuk serangan DDOS menghasilkan nilai respon time notifikasi secara berurut adalah 11.94 detik untuk Land Attack, 11.29 detik untuk TCP Syn Flood, dan 14.33 detik untuk Smurf Flooding. dan terakhir Pengujian serangan brute force menghasilkan nilai respon time lebih stabil untuk mendeteksi serangan, dimana nilainya adalah 8.43 detik.

Kata kunci : Intrusion Detection System, Snort, Elastic stack, DDOS.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era sekarang, peran network administrator sangat penting dalam menjaga keamanan jaringan yang menjadi tulang punggung operational dari berbagai sektor. Menurut Ketua Umum Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) Jamalul Izza, mengatakan bahwa peningkatan ini didorong oleh penyebaran infrastruktur internet cepat yang semakin merata dan transformasi digital yang masif akibat pandemi Covid-19 sejak Maret 2020 lalu (Bisnis.com,2020). seiring dengan semakin berkembangnya teknologi internet, kejahatan yang memanfaatkan teknologi juga semakin meningkat karena maraknya cybercrime akhir akhir ini yang bisa mencuri data dan penyadapan transmisi pada jaringan. Seorang administrator perlu memantau server JTIK agar mempermudah dalam mengamati dan mengontrol sistem. Server JTIK perlu mendapatkan perhatian yang lebih karena memiliki celah keamanan yang bisa dimanfaatkan oleh penyusup. Jika tidak segera diatasi hal tersebut dapat merugikan bagi *network administrator*. Salah satu cara untuk meningkatkan keamanan sistem informasi adalah dengan mengimplementasikan *Intrusion Detection System* (IDS).

Intrusion Detection System (IDS) adalah sistem yang berfungsi untuk mendeteksi aktivitas mencurigakan dalam suatu jaringan (Purnama, 2023). IDS mampu menginspeksi lalu lintas masuk dan keluar dalam sebuah sistem atau jaringan, melakukan analisis, dan mencari bukti adanya percobaan penyusupan (intrusi) (Paramitha et al., 2020). Walaupun pada sebuah jaringan biasanya sudah terdapat *firewall* yang bertindak sebagai penjaga pintu, mengatur lalu lintas jaringan berdasarkan aturan yang ditetapkan dan mencegah akses tidak sah dari luar. Namun, *firewall* tidak selalu mampu mendeteksi atau menghentikan seranganyang sudah berhasil melewati atau berasal dari dalam jaringan itu sendiri. Sehingga hanya mengandalkan *firewall* sebagai sistem keamanan jaringan internet saat ini tidaklah cukup karena semakin berkembang berbagai jenis serangan

jaringan. Maka implementasi satu keamanan yang dapat menjamin agar dapat meminimalisir ataupun bahkan menghilangkan kerugian yang disebabkan oleh serangan keamanan jaringan menjadi hal yang penting. Salah satunya adalah dengan menggunakan *Snort* (Purba & Efendi, 2020).

Snort adalah sebuah perangkat lunak yang dapat mendeteksi penyusup dan melakukan analisis lalu lintas secara *real-time* yang memungkinkan untuk mengenali berbagai jenis serangan. *Snort* tidak hanya berfungsi sebagai *Intrusion Detection System* (IDS) atau alat analisis protokol, tetapi merupakan kombinasi dari keduanya. Hal ini menjadikan sangat berguna dalam memberikan respon terhadap insiden serangan terhadap *host Host* dalam sebuah jaringan (Wijaya & Pratama, 2020). *Snort* memberikan notifikasi atau peringatan saat mendeteksi serangan, yang kemudian dicatat dalam *log*. Data *log* IDS *Snort* ini dapat dipergunakan oleh administrator jaringan untuk melakukan analisis pada kelemahan sistem keamanan jaringan (Paramitha et al., 2020). Hasil *log* tersebut perlu untuk diintegrasikan dan dilakukan analisis, sehingga dapat memberikan pemahaman yang lebih mendalam tentang aktivitas jaringan dan potensi ancaman yang terdeteksi. Hal itu dapat dilakukan dengan implementasi *Elastic Stack* untuk data *log* yang dihasilkan oleh *Snort*.

ELK merupakan singkatan yang terdiri dari tiga proyek *open-source* yaitu *Elasticsearch*, *Logstash*, dan *Kibana*. ELK memiliki kemampuan dalam pencarian, pemrosesan data, agregasi, dan visualisasi (Armend Gashi, 2020). Dengan menggunakan ELK, administrator jaringan dapat melakukan analisis yang lebih mendalam terhadap lalu lintas jaringan, mengidentifikasi pola serangan, dan merespon ancaman dengan lebih cepat dan efisien. Akan tetapi, administrator jaringan sering kali tidak bisa terus menerus memantau jaringan yang mereka kelola karena terdapat banyak tugas lain yang harus mereka selesaikan (Fernando & Asri, 2020). Sehingga diperlukan fitur tambahan agar administrator jaringan dapat selalu mengetahui aktivitas jaringan yaitu dengan menerapkan sistem notifikasi menggunakan aplikasi Telegram. Penggunaan Telegram sebagai aplikasi untuk pengiriman notifikasi dikarenakan sebagai aplikasi *instant messaging* yang populer, Telegram memiliki fitur keamanan seperti Secret Chat yang dienkripsi *end-to-end*, memastikan hanya pengirim dan penerima pesan yang dapat mengaksesnya (Panjaitan & Syafari, 2019). Implementasi fitur tersebut dapat membantu administrator jaringan dalam

mendapatkan pemberitahuan secara*real time* tentang kejadian penting dalam jaringan. Ketika terjadi aktivitas yang mencurigakan atau serangan yang terdeteksi oleh sistem IDS seperti *Snort* dan telah direkam dalam ELK, notifikasi Telegram dapat langsung mengirimkan pesan kepada administrator. Hal ini memungkinkan administrator untuk tetap terhubung dan memperoleh informasi yang diperlukan secara cepat, bahkan ketika mereka tidak dapat mengawasi jaringan secara langsung.

penelitian pertama yang berhasil penulis temukan dilakukan oleh Didik Rustandi dengan judul "Implementasi Intrusion Detection System menggunakan snort berbasis SMS Gateway untuk keamanan jaringan". pada penelitian ini berfokus dalam melakukan implementasi pada penerapan IDS Snort untuk mendeteksi serangan pada server dan memberikan notifikasi berupa SMS gateway kepada administrator saat ketika terjadi adanya serangan, lalu pada penelitian ini tidak memiliki Dashboard atau visualisasi yang memudahkan pengguna dalam memonitoring jaringan. Sehingga pada penelitian yang dilakukan sekarang menggunakan elastic stack sebagai alat untuk mengolah log, mengumpulkan, menyimpan data serta memudahkan dalam melakukan monitoring dan analisis lalu lintas jaringan. Penelitian kedua yang dilakukan oleh Wahyu dwi Romadhon dengan Judul "Implementasi IDPS Suricata untuk Monitoring Jaringan dengan Visualisasi Elk Stack dan Notifikasi melalui Bot telegram (2021)" membahas mengenai implementasi pada penggunaan IDS Suricata yang diintegrasikan dengan ELK dan notifikasi melalui bot telegram. Hasil penelitian ini menunjukkan bahwa suricata dapat mendeteksi adanya serangan jaringan, lalu ELK dapat memvisualisasikan log suricata sehingga mudah dimengerti dan terintegrasi dengan bot telegram secara real time untuk mengirimkan alert. Namun hal yang menjadi perbedaan dari penelitian ini yang dilakukan oleh penulis adalah dari penggunaan IDSnya. Jika penelitian sebelumnya menggunakan IDS Suricata , maka penelitian ini menggunakan IDS Snort. Penelitian ketiga yang dilakukan oleh Lukman & Suci pada tahun 2020 dengan judul analisis perbandingan kinerja IDS Snort 2 dan Suricata dalam mendeteksi serangan DoS Synchronize (SYN) flood dengan memperhatikan parameter jumlah deteksi serangan, CPU usage, memory usage, dan efektivitas deteksi serangan. Hasil penelitian tersebut menunjukan bahwa Snort lebih unggul dalam pendeteksian serangan, penggunaan CPU usage, dan fitur informasi data serangan. Sedangkan Suricata lebih unggul dalam efektivitas serangan dari data

uncaptured package dan penggunaan Random Access Memory (RAM) usage.

Berdasarkan penjelasan kedua literatur yang telah diuraikan di atas, hal inilah yang memperkuat dalam latar belakang penulis mengambil judul "Rancang Bangun Intrusion Detection System menggunakan Snort untuk Monitoring Keamanan Jaringan dengan Visualisasi Elastic Stack dan Notifikasi Bot Telegram". Pada Penelitian ini, penulis akan menawarkan penelitian dari IDS *Snort* yang diintegrasikan dengan *Elastic Stack* dan fitur notifikasi menggunakan aplikasi Telegram. Hasil penelitian diharapkan dapat memberikan solusi perbaikan bagi network administrator serta mempermudah dalam melakukan analisis dan *monitoring* jaringan.

1.2 Rumusan Masalah

Beberapa permasalahan yang dapat diambil dari latar belakang:

a. Bagaimana cara membangun *Intrusion Detection System* menggunakan *Snort*?
b. Bagaimana cara mengintegrasikan *Elastic Stack* untuk hasil visualisasi log pada *Intrusion Detection System Snort*?
c. Bagaimana cara mengimplementasikan sistem peringatan telegram dalam menotifikasikan kepada pengguna saat terjadi serangan?
d. Bagaimana cara kinerja snort dalam meningkatkan performa deteksi serangan port scanning, DDOS Attack, dan Brute force menggunakan parameter confusion matrix?

1.3 Batasan Masalah

Adapun batasan masalah yang ditentukan pada penelitian ini adalah:

1. Penelitian ini berfokus bagaimana cara implementasi *Intrusion Detection System Snort* dan visualisasi hasil *log server* pada *ElK;*
2. Notifikasi serangan menggunakan Telegram;
3. *Penelitian* ini menggunakan *Virtual Machine dari virtualbox* pada *Server JTIK dengan OS Ubuntu server 22.04,* dan *Attacker dengan OS Kali linux versi 2024.1* ;
4. Penelitian ini menggunakan *web server nginx* untuk menghubungkan ke dalam *ElK;*
5. Tools yang digunakan dalam penelitian ini adalah Nmap, Hping3, LOIC, dan Hydra;
6. Pengujian dilakukan pada jaringan Lokal;

7. Skenario pengujian serangan adalah *Port Scanning*, *DDOS Attack*, dan *Brute force password;*
8. Parameter yang digunakan pada penelitian ini yaitu confusion matrix yang terdiri dari TP, FP, TN, dan FN, kemudian diukur dengan waktu deteksi serangan, dan respon notifikasi telegram .
9. Log yang didapat hanya berasal dari snort yang diintegrasikan dengan ELK.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Adapun tujuan dari penelitian ini adalah:

a. Membangun *Intrusion Detection System* menggunakan *Snort;*
b. Mengimplementasikan hasil *log Snort* dengan visualisasi *Elastic Stack;*
c. Mendeteksi serangan *DDoS*, *Port Scanning* dan *Brute Force* dari *attacker* dengan notifikasi Telegram.
d. Mengukur seberapa handal dan efektif IDS Snort dalam mendeteksi serangan Port scanning, DDOS, dan Brute Force dengan parameter confusion matrix.

1.4.2 Manfaat

adapun manfaat dari penelitian ini adalah:

a. Memvisualisasikan hasil dari *log Snort* yang dapat mudah dipahami oleh administrator;
b. Dapat memonitoring serangan *Distributed Denial of Service* (*DDoS*), *Port Scanning*, dan *Brute Force* yang masuk pada perangkat keamanan jaringan Snort;
c. Mempermudah dalam pembacaan *log server* yang masuk ke dalam *ELK.*
d. Meningkatkan performa deteksi pada IDS Snort terhadap serangan Port scanning, DDOS Attack, dan Brute Force menggunakan parameter confusion matrix.

1.5 Sistematika Penulisan

Sistematika penulisan dalam penyusunan skripsi ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini akan membahas tentang latar belakang dari suatu permasalahan, rumusan

masalah, batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan pada skripsi ini.

BAB II TINJAUAN PUSTAKA

Bab ini akan membahas mengenai landasan teori yang relevan dengan kasus yang dipilih.

BAB III METODE PENELITIAN

Bab ini akan membahas tahapan penelitian mulai dari rancangan penelitian, tahapan penelitian, objek penelitian, dan teknik pengumpulan data yang digunakan dalam melakukan penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi penjabaran hasil yang telah didapatkan dari penelitian yang telah dilakukan.

BAB V PENUTUP

Bab terakhir di mana Bab penutup yang berisikan kesimpulan dan saran.

6. DAFTAR PUSTAKA

pada Bab ini melampirkan daftar sumber informasi termasuk jurnal dan situs web sebagai bukti atau referensi untuk proposal skripsi.

7. DAFTAR RIWAYAT HIDUP

pada Bab ini akan menyertakan biodata dan riwayat pendidikan Penulis

8. LAMPIRAN

pada bab ini akan disertakan berbagai lampiran yang relevan dengan penyusunan skripsi seperti foto, dokumen penting, dan lain-lain.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil dari penelitian yang telah dilakukan oleh penulis, maka dapat ditarik kesimpulan sebagai berikut:

1. Untuk membangun Intrusion detection system menggunakan snort, dibutuhkan beberapa modul tambahan seperti fitur multhreading memungkinkan sistem untuk memproses paket secara pararel serta meningkatkan kinerja dan efisiensi dalam menangani adanya pola aktivitas jaringan yang tinggi. selain itu pada penelitian ini juga dilakukan pembuatan script untuk memberikan notifikasi kepada administrator dengan aplikasi telegram serta melakukan uji deteksi pada snort apabila terjadi ancaman yang mencurigakan terhadap serangan yang masuk pada perangkat server JTIK. adapun pembuatan script yang dibuat akan diintegrasikan dengan IDS Snort dan Bot telegram dengan tujuan untuk mengirimkan notifikasi secara otomatis serta memantau jika muncul ada pesan informasi yang baru. selain itu sistem yang dibangun pada penelitian ini nantinya akan dijalankan secara bersamaan dengan ELK agar dapat menampilkan banyaknya visualisasi data alert yang masuk pada Log snort, dan kemudian secara otomatis, sistem tersebut bot telegram akan mengirimkan hasil notifikasi kepada administrator dengan jeda waktu 1 detik tiap masing masing jenis serangan yang telah diuji.
2. Pengintegrasilan log yang masuk melalui ELK dapat membuat visualisasi lebih terlihat menarik untuk dilihat oleh penulis, oleh karena itu ELK menyediakan beberapa fitur serta alat untuk visualisasi data yang lebih informatif dan dapat dianalisis oleh administrator jaringan saat terjadi serangan yang masuk pada perangkat server JTIK seperti line chart, pie chart, Gauge, table, dan lain lain. Untuk melakukan integrasi antara IDS Snort dan ELK dibutuhkan konfigurasi pada filebeat agar nantinya log yang dihasilkan oleh snort dapat dikirim ke elasticsearch, setelah log disimpan di elasticsearch, kemudian hasil log tersebut akan dilakukan proses parsing terlebih dahulu melalui logstash dan terakhir hasil log pada snort dapat divisualisasikan menggunakan kibana serta merancang dashboard sesuai kebutuhan.

3. Telegram bot yang dibuat berhasil diimplementasikan saat mengirimkan notifikasi secara real time kepada administrator ketika terjadi serangan yang masuk pada Server JTIK. adapun dari hasil data yang didapatkan pada 5 kali percobaan port scanning membutuhkan waktu rata rata respon time sebanyak 24,78 detik untuk snort mendeteksi, lalu bot telegram akan mengirimkan notifikasi secara otomatis. Kemudian pada 5 kali percobaan pada serangan DDOS membutuhkan waktu rata rata respon time sebanyak 12,52 detik untuk snort mendeteksi dan mengirimkan notifikasi secara otomatis kepada bot telegram. Dan terakhir akan dilakukan 5 kali percobaan pada serangan brute force yang membutuhkan waktu rata rata respon time sebanyak 8.43 detik, sehingga menghasilkan nilai respon time lebih stabil untuk mendeteksi serangan.
4. IDS Snort mampu mendeteksi serangan Port scanning, DDOS Attack dan Brute force dengan tingkat keberhasilan 100% dalam melakukan 5 kali percobaan, namun ditemukan false positive pada saat pengujian kedua hingga kelima untuk notifikasi yang diterima menunjukkan pesan "TCP Scan" meskipun serangan sebenarnya adalah *brute force* dengan tools *Hydra*. Hal ini menunjukkan bahwa IDS salah mengidentifikasi serangan *brute force* sebagai aktivitas IP Scanning untuk *TCP Scan*. Hal tersebut terjadi karena pola aktivitas *Hydra* yang digunakan dalam serangan *brute force* mirip dengan pola yang digunakan dalam *TCP Scan*, sehingga IDS salah dalam klasifikasi atau perlu dilakukan perbaikan *rules Snort* agar lebih akurat untuk mengatasi hal tersebut.
5. Berdasarkan hasil pengujian efektivitas IDS menggunakan parameter confusion matrix untuk TPR, FPR, FNR, dan TNR, kinerja snort memiliki performa sangat baik ketika mendeteksi serangan DDOS yang dilakukan dalam jaringan server JTIK pada skenario ke 2 dengan nilai akurasi persentase sebesar 100%, precision 100%, recall 100% dan F1 Score 100%. Dari hasil analisis data yang penulis dapatkan menunjukkan bahwa Snort memiliki performa deteksi yang sangat baik dalam mengidentifikasi serangan DDoS Syn Flood pada semua aktivitas dengan nilai yang mencapai performa ideal, Snort menunjukkan efektivitas yang tinggi dalam mendeteksi serangan ini tanpa ada kesalahan signifikan serta Tidak adanya False Positive dan kemampuan untuk mendeteksi semua serangan juga menunjukkan bahwa Snort adalah alat deteksi yang sangat handal untuk jenis serangan ini. Berdasarkan hasil skenario pengujian yang sudah dilakukan oleh penulis dari masing masing aktivitas yang sudah dilakukan, rata rata keseluruhan aktivitas 1 s.d 5 untuk port scanning adalah 80,0 % dengan nilai akurasi, 80,0 % untuk nilai precision, 100% dengan nilai recall atau true positive rate, dan 100% dengan penilaian F1 Score, yang dimana jika dimasukkan ke dalam klasifikasi penilaian pada parameter confusion matrix termasuk ke dalam kategori " baik" untuk accuracy, "tinggi" untuk precision, sangat tinggi untuk recall, dan sangat baik untuk Penilaian F1 Score. Untuk pengujian parameter confusion matrix rata rata keseluruhan pada aktivitas 1 s.d 5 untuk serangan brute force adalah 92,2% dengan nilai akurasi, 92,2 % untuk

nilai precision, 100% dengan nilai recall atau true positive rate, dan 100% dengan penilaian F1 Score, yang dimana jika dimasukkan ke dalam klasifikasi penilaian pada parameter confusion matrix termasuk ke dalam kategori " sangat baik" untuk accuracy, "sanga tinggi" untuk precision, sangat tinggi untuk recall, dan sangat baik untuk Penilaian F1 Score. Dengan begitu menunjukan bahwa kinerja snort dalam mendeteksi serangan berdasarkan hasil pengujian pada skenario 1 untuk port scanning, skenario ke 2 untuk DDOS Attack, dan Skenario ke 3 untuk Brute force menggunakan parameter confusion matrix terbilang baik dalam implementasi yang dilakukan pada jaringan yang ada pada server JTIK.

5.2 Saran

Saran yang dapat diusulkan pada penelitian ini adalah:

1. menambahkan lebih banyak jenis serangan lainnya yang dapat dideteksi oleh IDS pada Snort sehingga cakupan deteksi menjadi lebih luas seperti SQL Injection, Cross site scripting dan Malware.
2. Mengintegrasikan IDS Snort dengan lebih banyak alat atau tools keamanan lainnya untuk meningkatkan kapabilitas deteksi dan respons terhadap serangan.
3. notifikasi pada snort tidak hanya menggunakan bot telegram saja, tetapi bisa menambahkan opsi API lainnya seperti email, sms, dan whatsapp.
4. Diharapkan pengujian dapat dilakukan pada ruang lingkup yang lebih luas seperti menggunakan Cloud VPS .
5. menambahkan parameter QoS untuk melakukan perbandingan perfoma IDS yang lebih spesifik selain menggunakan parameter confusion matrix untuk penelitian selanjutnya, serta mengintegrasikan IDS dengan machine learning ke dalam alat IDS untuk mengoptimalkan keakuratan deteksi sekaligus meminimalkan adanya false positive.

DAFTAR PUSTAKA

Albert Yakobus Chandra. (2019). Analisis Performansi Antara Apache & Nginx Web Server dalam Menangani Client Request. Jurnal Sistem dan Informatika (JSI).

Alvana Noor Fariza. (2022). Topologi Jaringan: Pengertian, Cara Kerja, & 6 Jenis-Jenisnya.

Amira, DKK. (2023). Topologi Jaringan Komputer: Pengertian, Manfaat, dan Jenis-Jenisnya.

Armend Gashi. (2020, May 23). Forwarding Snort logs to ELK Stack. Medium.Com. https://medium.com/@armendgashx/forwarding-Snort-logs-to-elk-stack-371232699e7f

Assegaff, S. (2019). VIRTUAL PADA SMK NEGERI 2 KOTA JAMBI. Jurnal Manajemen Sistem Informasi, 4(2).

Bisnis.com, L. D. (2020, November 10). Teknologi. Retrieved from APJII: 196,7 Juta Warga Indonesia Sudah Melek Internet: https://teknologi.bisnis.com/read/20201110/101/1315765/apjii-1967-jutawarga-indonesia-sudah melekinternet#:~:text=Bisnis.com%2C%20JAKARTA%20%2D%20Jumlah,juta%20pengguna%20dibandingkan%20tahun%20lalu.

Dewaweb team. (2023). PENGERTIAN JARINGAN KOMPUTER, JENIS JENIS, DAN TOPOLOGINYA.

Didik Rustandi, (2023). Implementasi Intrusion Detection System (IDS) menggunakan Snort berbasis SMS gateway untuk keamanan Jaringan, Vol 3, (pp 37-44).

Elastic. (2019). What is Elasticsearch? [Online]. Available: https://www.elastic.co/what-is/elasticsearch. [Accessed 20 April 2022].

Elastic. (2021). What is Elasticsearch? Retrieved from https://www.elastic.co/what-is/elasticsearch

Fadhlillah, A. S., Karna, N. B. A., & Irawan, A. I. (2019). Analisis Performansi Ids Menggunakan Metode Deteksi Anomaly-based Terhadap Serangan Dos. eProceedings of Engineering, 6(2).

Fadhlillah, A., Karna, N., & Irawan, A. (2021, January). IDS performance analysis using anomaly-based detection method for DOS attack. In 2020 IEEE

International Conference on Internet of Things and Intelligence System (IoTaIS) (pp. 18-22). IEEE.

FARHAN, Ali. (2019). Implementasi Intrusion Detection System (Ids) Menggunakan Snort Untuk Mendeteksi Serangan Pada Server. PhD Thesis. Universitas Mataram.

Febrianto, H. I. (2022). PEMBANGUNAN SISTEM MONITORING NETWORK SECURITY MENGGUNAKAN INTRUSION DETECTION SYSTEM SNORT DENGAN LOG ANALISIS SPLUNK (Studi Kasus: PT. H-One Kogi Prima Auto Technologies Indonesia). Doctoral dissertation, Fakultas Teknik Unpas.

Fernando, N., & Asri, E. (2020). Monitoring Jaringan dan Notifikasi dengan Telegram pada Dinas Komunikasi dan Informatika Kota Padang. JITSI: Jurnal Ilmiah Teknologi Sistem Informasi, 1(4), 121–126.

Fily Fajrian. (2017). HAL BASIC YANG HARUS DIPELAJARI TENTANG JARINGAN KOMPUTER, Volume 1, pp. 1-56.

Fitriansyah, F. (2020). Penggunaan Telegram Sebagai Media Komunikasi Dalam Pembelajaran Online. Cakrawala: Jurnal Humaniora Bina Sarana Informatika, 20(2), 111-117.

Fuada, Z., & others. (2024). Penerapan keamanan jaringan menggunakan sistem Snort dan honeypot sebagai pendeteksi dan pencegah malware. UIN Ar-Raniry Fakultas Tarbiyah dan Keguruan.

Ihsana, A. N., & Maslan, A. (2020). Analisis Keamanan Jaringan Dari Serangan Paket Data Sniffing Di PT Raden Syaid Kantor POS PIAYU KOTA BATAM. Jurnal Comasie, 3(5).

Indrarto, S. A., & Basuki, A. (2022). Penerapan Platform Visualisasi dan Analisis Trafik Jaringan menggunakan Elastic Stack. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 6(9), 4562-4570.

Lucas Theodorus. (2022). Implementasi Intrusion Detection System menggunakan zeek dan suricata untuk network monitoring melalui SIEM Dashboard. Universitas Indonesia, Depok, 2022.

M. Hafidz. (2022). Perancangan dan Analisis Kinerja Intrusion Detection System (IDS) Suricata serta integrasi dengan sistem keamanan jaringan komputer Berbasis web. Universitas Indonesia, Depok, 2022.

Mahendrian, A. (2015). Intrusion detection and Prevention System: Technologies and Challenges. International Journal of Applied Engineering Research, pp. 1-12.

Muhammad, A. R., Mochammad, F. R., & Tedi, G. (2017). IMPLEMENTASI HACKING WIRELESS DENGAN KALI LINUX MENGGUNAKAN KALI NETHUNTER. e-Proceeding of Applied Science, 3(3).

Mulyanto, A. D. (2020). Pemanfaatan Bot Telegram Untuk Media Informasi Penelitian. MATICS: Jurnal Ilmu Komputer dan Teknologi Informasi, 12(1), 49-54.

Panjaitan, F., & Syafari, R. (2019). Pemanfaatan Notifikasi Telegram Untuk Monitoring Jaringan. Simetris: Jurnal Teknik Mesin, Elektro Dan Ilmu Komputer, 10(2), 725–732.

Paramitha, I. A. S. D., Sasmita, G. M. A., & Raharja, I. M. S. (2020). Analisis Data Log IDS Snort dengan Algoritma Clustering Fuzzy C-Means. Maj. Ilm. Teknol. Elektro, 19(1), 95.

Prayoga Haditya Putra. (2020). Implementasi Log Management Server menggunakan ELK (Elasticsearch, Logstash, dan Kibana) Stack pada server web snort di PT XYZ. Politeknik Negeri Jakarta, Depok, 2020.

PRATAMA, I. Putu Agus Eka & HANDAYANI, NI Kade Mega. (2019). IMPLEMENTASI IDS MENGGUNAKAN SNORT PADA SISTEM OPERASI UBUNTU: Implementasi IDS Menggunakan Snort Pada Sistem Operasi Ubuntu. Jurnal Mantik, 3(1), 176-182.

Prabowo, A. A., Fakhruddin, F., Pradana, C. S., & Haq, R. S. A. (2021). Sistem Pendeteksi Kerusakan Pada Motor Dan Mobil Berbasis Bot Telegram. Doctoral dissertation, Universitas Pembangunan Nasional Veteran Jawa Timur.

Purnama, T. (2023). Implementasi Intrusion Detection System (IDS) Snort Sebagai Sistem Keamanan Menggunakan Whatsapp Dan Telegram Sebagai Media Notifikasi. Jurnal Teknologi Informasi Dan Komunikasi, 14(2), 358–369.

Putra, M. J. R., & Saptono, H. (2022). Penerapan Log Analyzer untuk Mengetahui Lalu Lintas Jaringan berbasis Elasticsearch, Logstash, dan Kibana. Jurnal Informatika Terpadu, 8(1), 21-25.

Rahmadani, M. A., Rizal, M. F., & Gunamawan, T. (n.d.). IMPLEMENTASI HACKING WIRELESS DENGAN KALI LINUX MENGGUNAKAN KALI NETHUNTER WIRELESS HACKING IMPLEMENTATION USING KALI LINUX KALI NETHUNTER.

Setiawan, R. (2021, August 4). Flowchart Adalah: Fungsi, Jenis, Simbol, dan Contohnya. Dicoding.Com.

Subramanian, K., & Meng, W. (2021, December). Threat hunting using elastic stack: An evaluation. In 2021 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI) (pp. 1-6). IEEE.

Sutarti, Pancaro, A. P. & Saputra, F. I. (2018). Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal. Jurnal PROSISKO, 5, 1-8.

Tambunan, G., & Mantra, I. (2020). Implementasi Keamanan IDS/IPS Dengan SNORT dan IPTables Pada Server. SENAMIKA, pp. 10-16.

Waleed, A., Jamali, A. F., & Masood, A. (2022). Which open-source IDS? Snort, Suricata or Zeek. Computer Networks, 213, 109116.

WIDODO, Tri, et al. Peer review artikel IJCA: Implementation of Intrusion Detection System (IDS) and Snort Community Rules to Detect Types of Network Attacks.

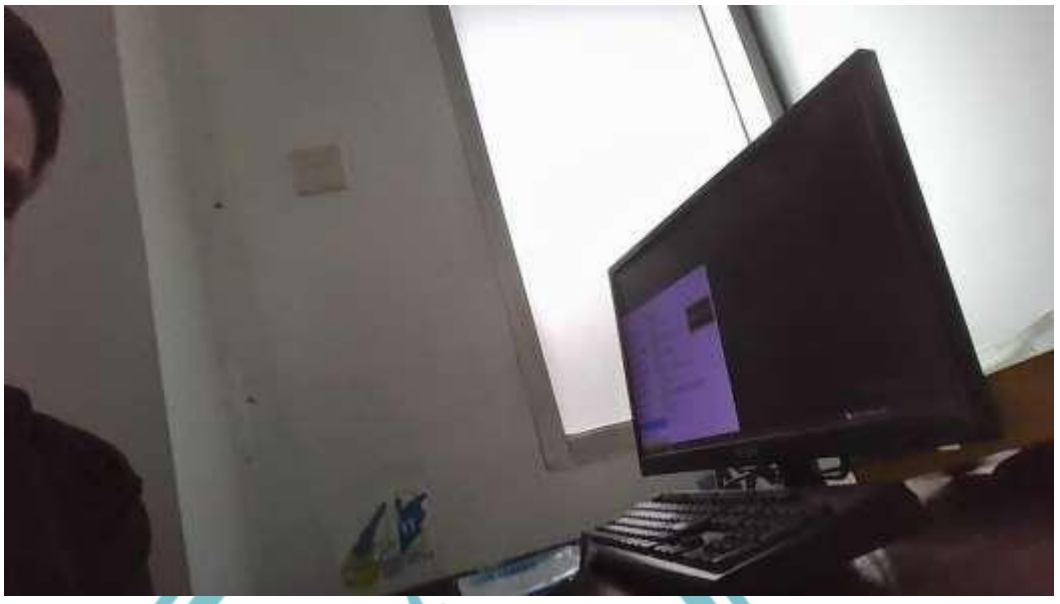
LAMPIRAN

L-1 Daftar Riwayat Hidup

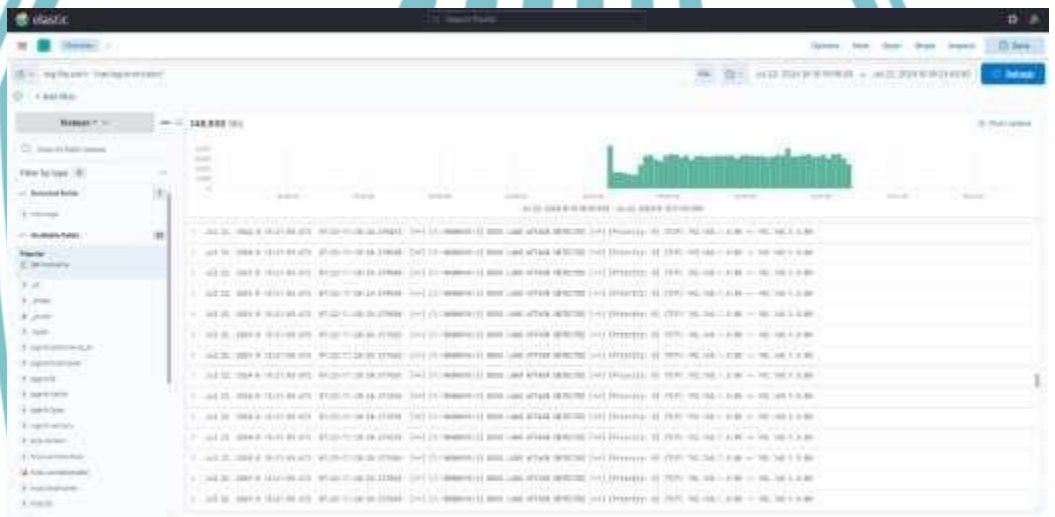
Muhammad Hafizh

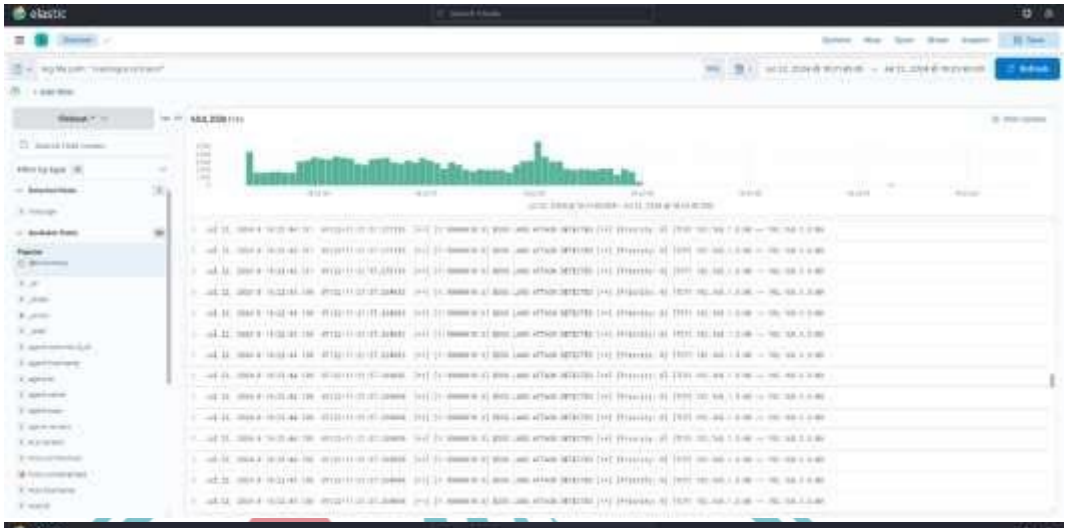
Lulus dari SDN Semplak 02 Kota Bogor tahun 2013, SMP Negeri 5 Bogor tahun 2016, dan SMA Pembangunan Satu Bogor pada tahun 2019. Saat ini, penulis sedang menempuh Pendidikan Tinggi pada program kerja sama Politeknik Negeri Jakarta dengan CCIT Fakultas Teknik Universitas Indonesia pada program D4, jurusan Teknik Informatika dan Komputer, prodi Teknik Multimedia dan Jaringan

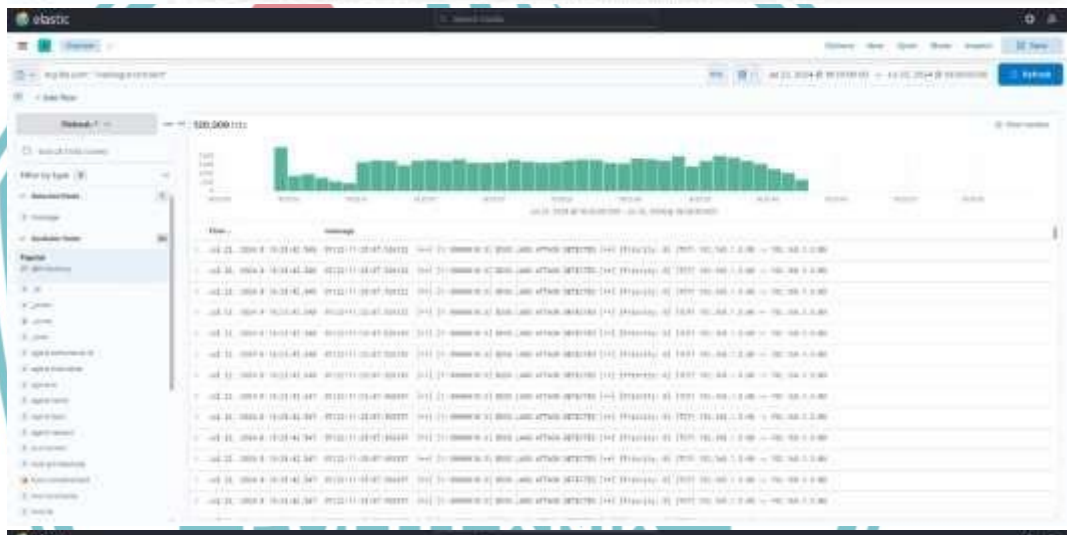
L-2 Pengerjaan Lab JTIK PNJ

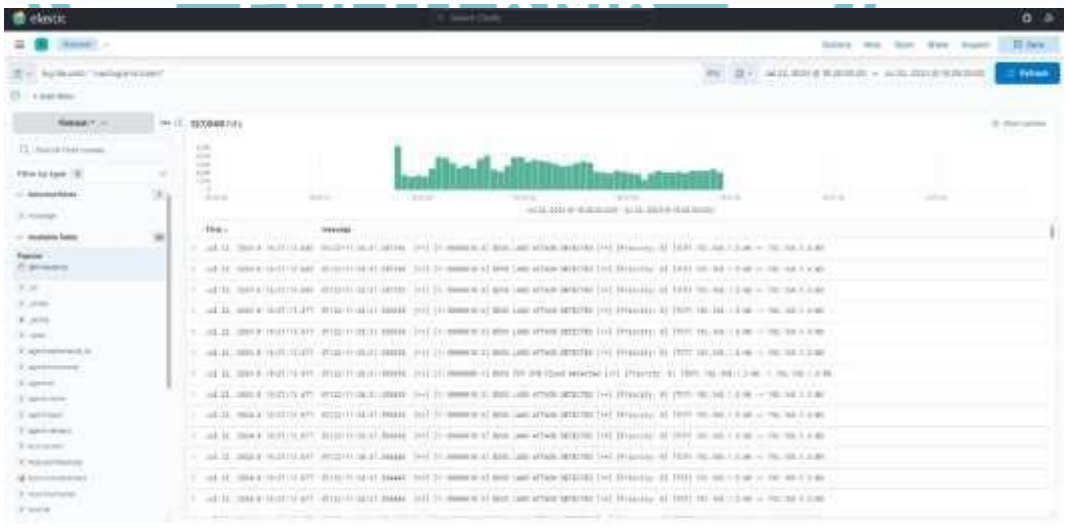


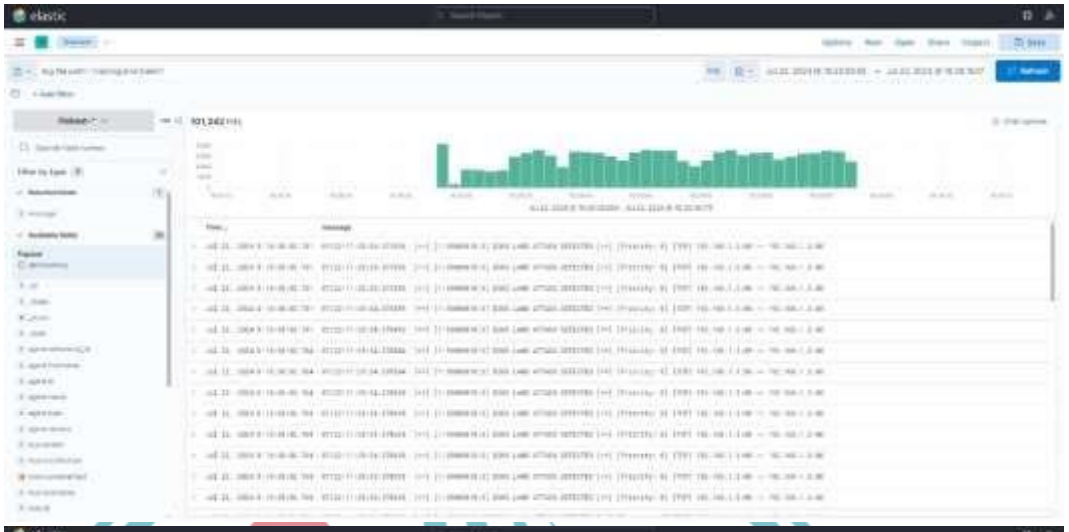
L-3 *Discovery Kibana DDoS* Hping3 Jumlah Hits

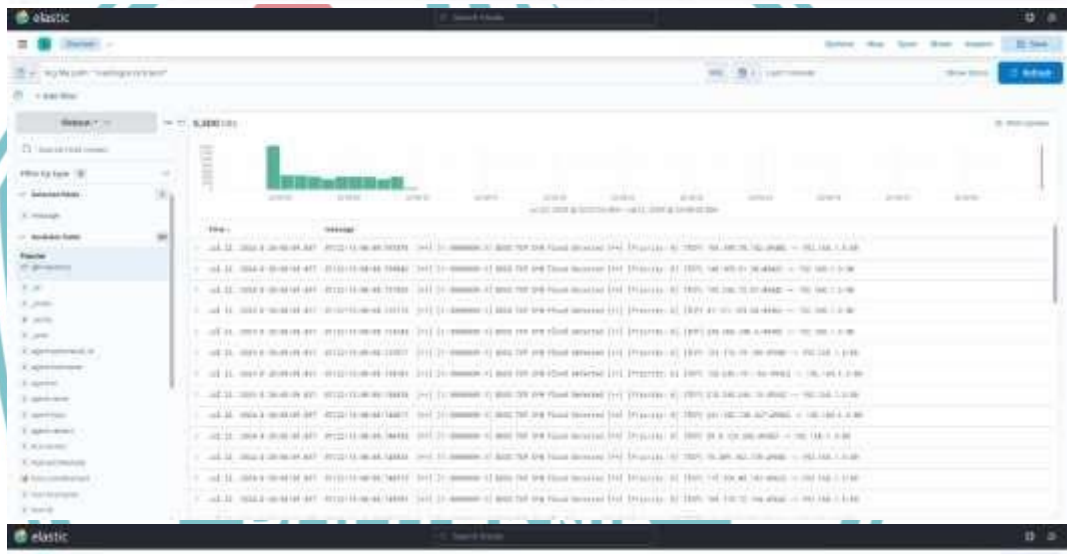


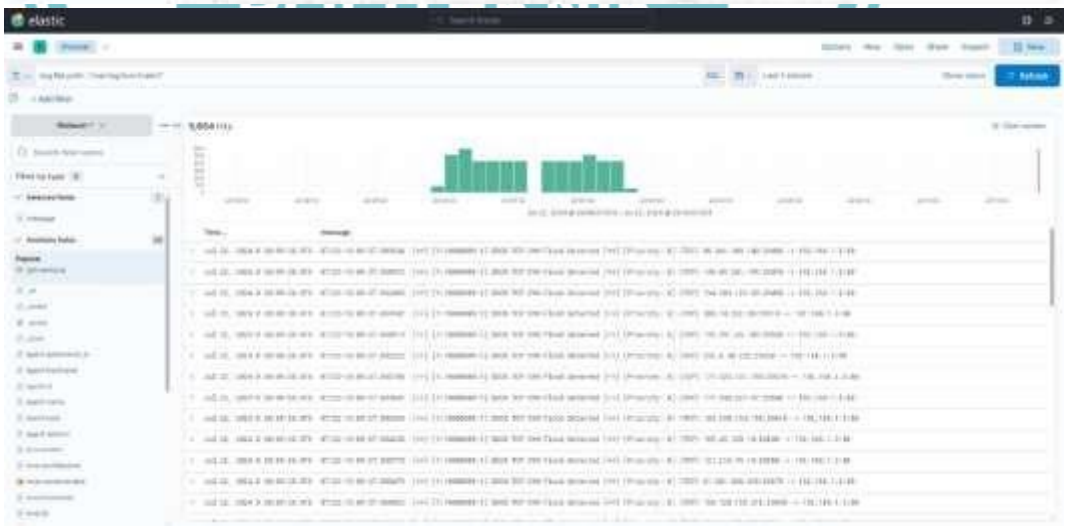


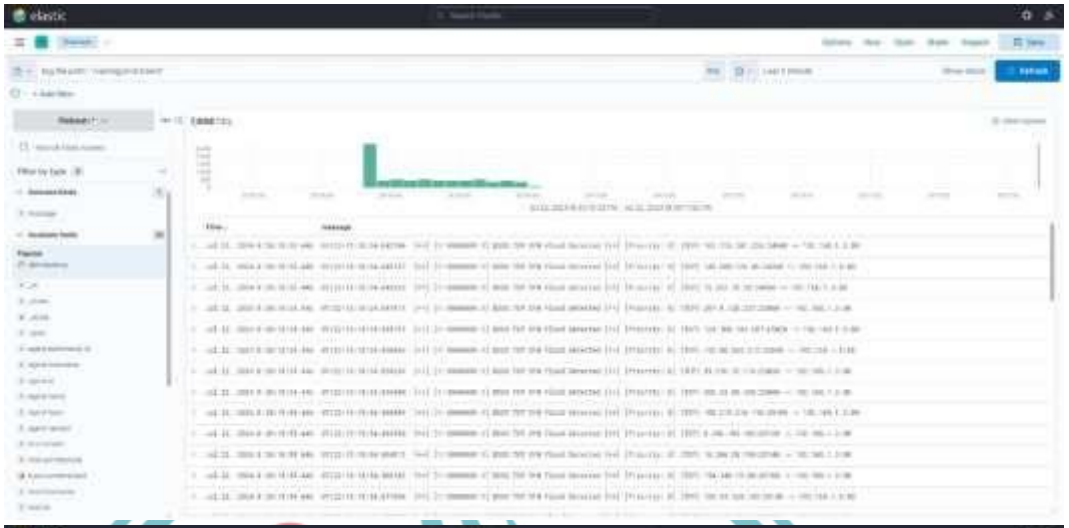


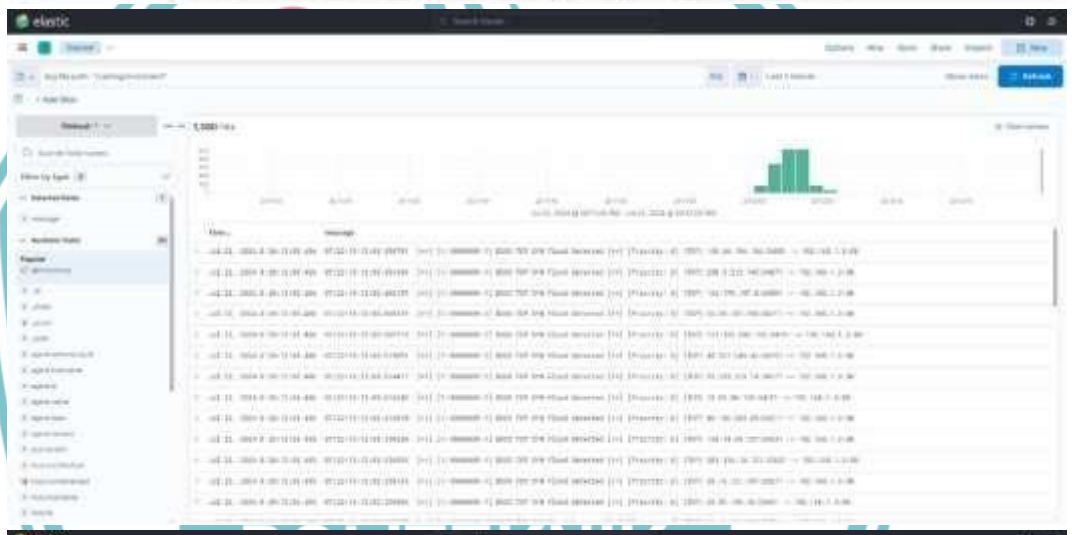


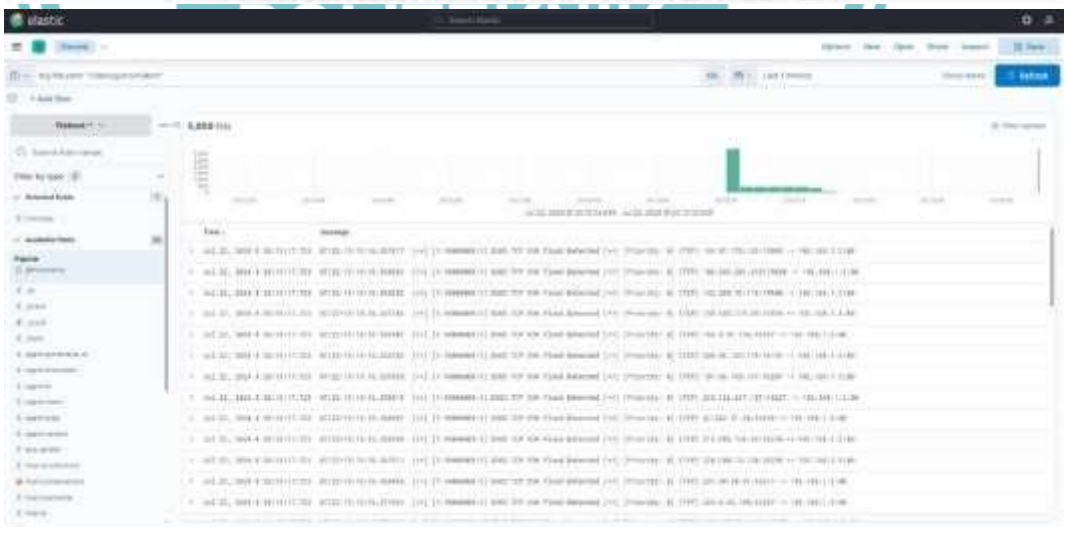


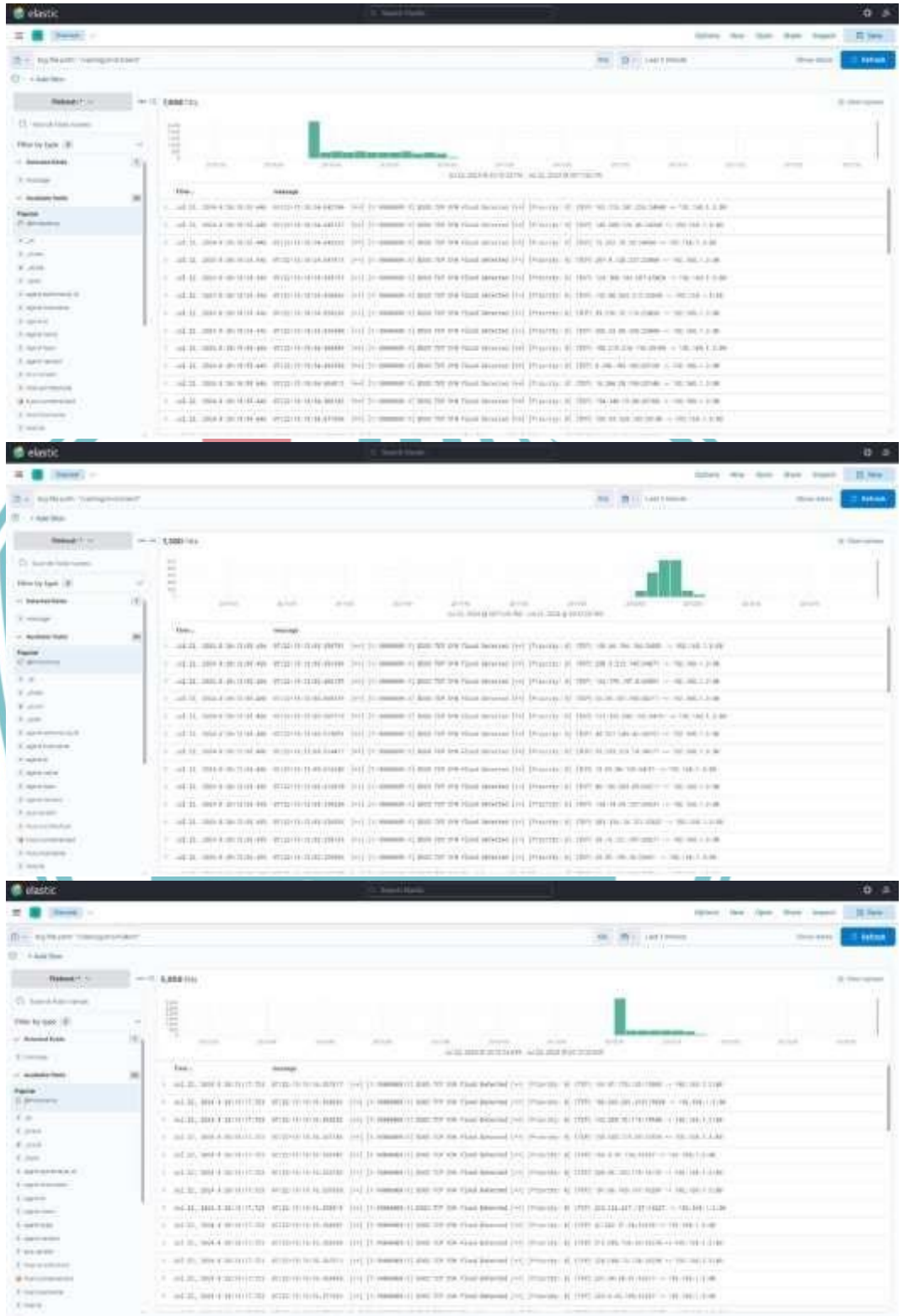


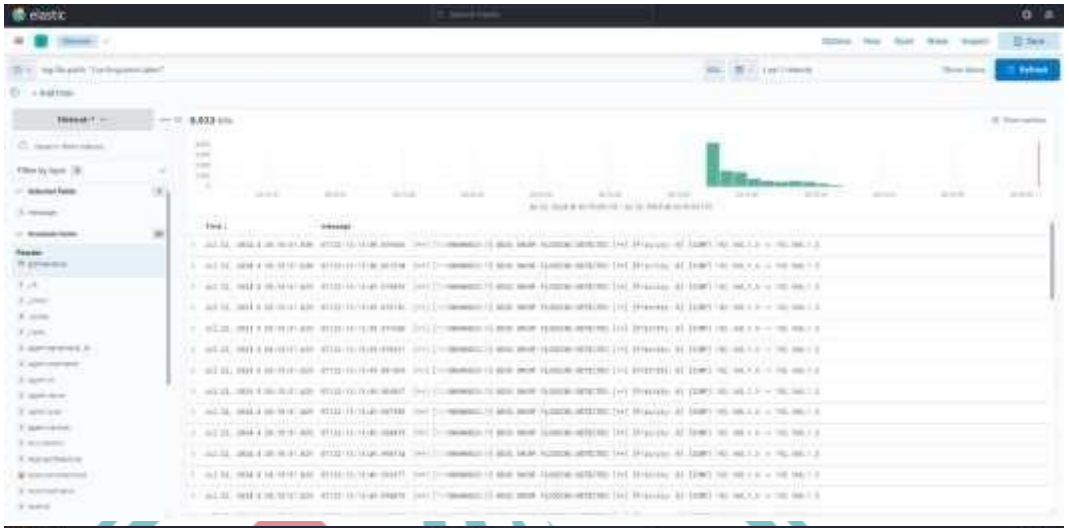


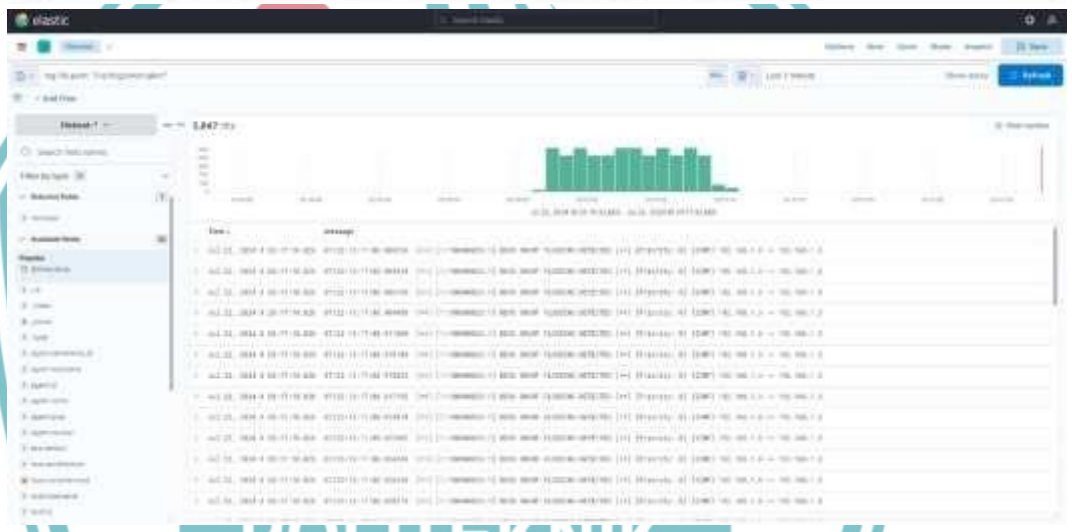


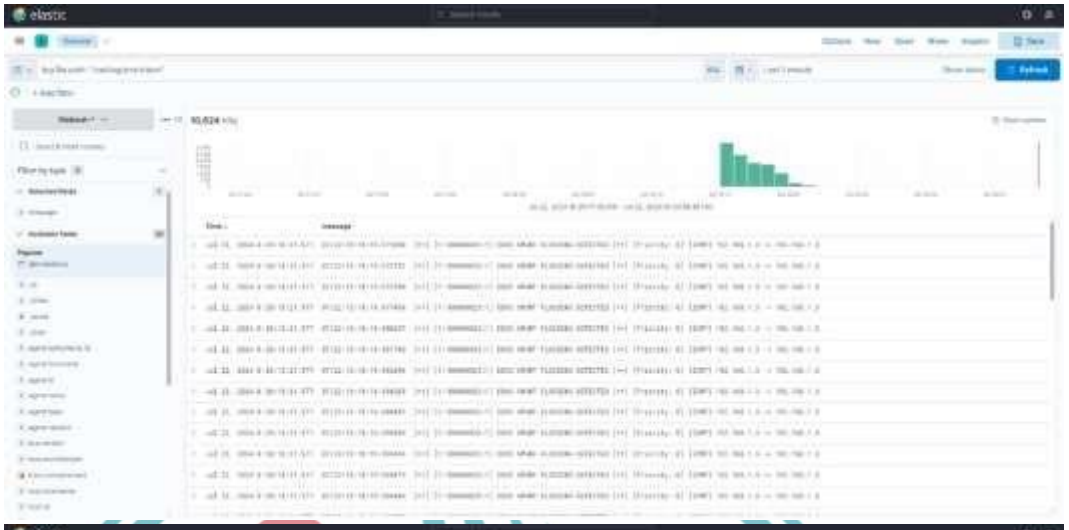


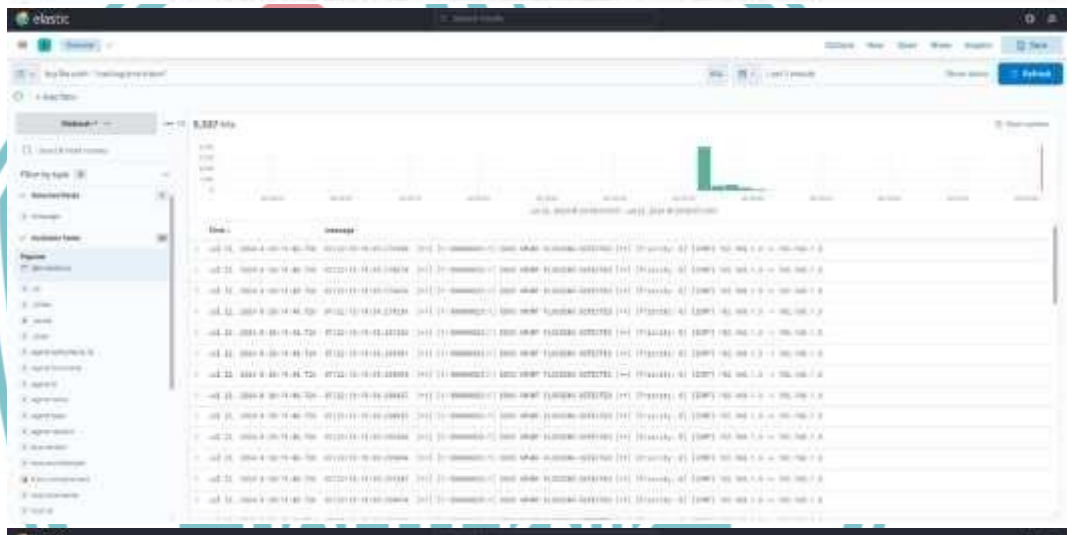


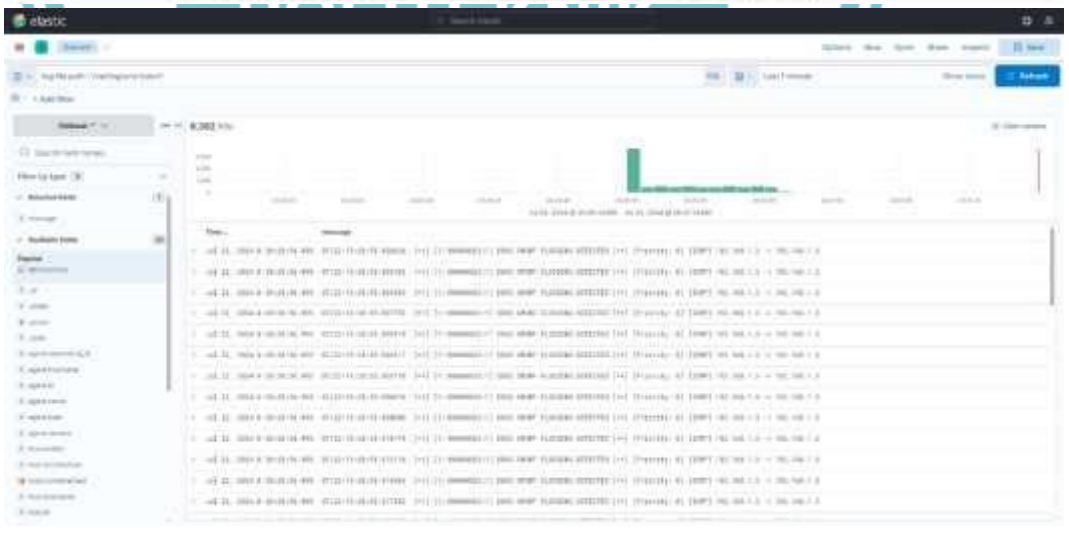












L-4 *Discovery Kibana DDoS* LOIC Jumlah Hits