# Implementasi dan Efektivitas Pengendalian Keamanan Jaringan Menggunakan *Tools* Honeypot KFSENSOR

**Benoni Manase Tarigan[1], Sinta Juliyanti[2], Sapriani Gustina[3]**
[123]Universitas Proklamasi 45,
[123]Yogyakarta-Indonesia,
Email: [1]benonimanase488@gmail.com, [2]sintajuliyanti267@gmail..com,
[3]sagustina@up45.ac.id

***Abstract***

*The threat of cyber security continues to rise alongside the rapid development of digital technology, presenting significant challenges for companies in protecting their systems from various attacks, such as malware, ransomware, and DDoS assaults. This study discusses the implementation and effectiveness of using the KFSensor honeypot as a tool to detect and analyze cyber threats. By deceiving attackers into interacting with decoy ports, KFSensor can record attack activities without posing risks to the main system. The findings indicate that KFSensor can detect attacks in real-time, providing valuable information for security teams to respond swiftly and develop more effective defense strategies. Additionally, KFSensor aids in identifying attack patterns and conducting risk assessments, enabling companies to focus their resources on the most vulnerable areas. In conclusion, the implementation of the KFSensor honeypot enhances network security by proactively monitoring, analyzing, and anticipating cyber-attacks, thereby mitigating potential damage and strengthening corporate protection systems.*

***Keywords:*** *attack detection, defense strategies, network security, threat analysis.*

***Abstraksi***

*Ancaman keamanan siber terus meningkat seiring dengan pesatnya perkembangan teknologi digital, yang menciptakan tantangan besar bagi perusahaan dalam melindungi sistem mereka dari berbagai serangan, seperti malware, ransomware, dan serangan DDoS. Penelitian ini membahas implementasi dan efektivitas penggunaan honeypot KFSensor sebagai alat untuk mendeteksi dan menganalisis ancaman siber. Dengan menipu penyerang agar berinteraksi dengan port palsu, KFSensor mampu merekam aktivitas serangan tanpa menimbulkan risiko bagi sistem utama. Hasil penelitian menunjukkan bahwa KFSensor dapat mendeteksi serangan dalam waktu nyata, menyediakan informasi berharga bagi tim keamanan untuk merespons secara cepat dan menyusun strategi pertahanan yang lebih efektif. Selain itu, KFSensor membantu dalam mengidentifikasi pola serangan dan melakukan penilaian risiko, sehingga perusahaan dapat memfokuskan sumber daya pada area yang paling rentan. Kesimpulannya, implementasi honeypot KFSensor secara signifikan meningkatkan keamanan jaringan melalui pemantauan, analisis, dan mitigasi serangan siber secara proaktif, sehingga mengurangi potensi kerusakan dan memperkuat sistem perlindungan perusahaan.*

***Kata Kunci:*** *analisis ancaman, deteksi serangan, keamanan jaringan, strategi pertahanan.*

## 1. PENDAHULUAN

Teknologi berperan sebagai pendukung utama dalam berbagai aktivitas, termasuk penafsiran dan pengambilan keputusan. Awalnya, teknologi informasi hanya digunakan untuk mengolah data. Namun, seiring berkembangnya teknologi informasi, hampir seluruh aktivitas organisasi saat ini terotomasi dan bergantung pada penerapannya. Dalam era digital, ancaman terhadap keamanan jaringan meningkat dengan cepat, baik dari segi frekuensi maupun kompleksitas serangan. Perusahaan yang bergerak di bidang transformasi digital menjadi sangat rentan terhadap berbagai jenis serangan siber, seperti *malware*, *ransomware*, hingga serangan DDoS. Oleh karena itu, penting bagi perusahaan untuk memiliki sistem pengendalian keamanan jaringan yang kuat dan efektif. Salah satu metode yang terbukti mampu mendeteksi dan menganalisis serangan adalah honeypot. Honeypot dapat memberikan informasi palsu kepada penyerang, sehingga mereka merasa telah berhasil menyusup ke server utama, sementara aktivitas mereka dipantau secara cermat. Dengan kemampuan ini, honeypot menjadi solusi penting dalam memahami pola serangan dan memperkuat keamanan jaringan.

Topik "Implementasi dan Efektivitas Pengendalian Keamanan Jaringan Menggunakan Honeypots KFSensor" dipilih karena relevansinya dengan kebutuhan perusahaan untuk memantau dan mengendalikan ancaman keamanan jaringan secara efektif. KFSensor, sebagai salah satu jenis honeypot, menawarkan solusi praktis dan efisien dalam mendeteksi serta menganalisis serangan siber. Dengan fitur pemantauan *real-time*, KFSensor memungkinkan perusahaan untuk mempelajari pola serangan dan meningkatkan strategi pertahanan. Hal ini menjadikan KFSensor pilihan yang strategis dibandingkan solusi lainnya dalam mendukung keamanan jaringan perusahaan di tengah meningkatnya ancaman siber.

## 2. TINJAUAN PUSTAKA

Pada penelitian pertama yang menganalisis serangan dan tindakan pada keamanan jaringan. Pada penelitian ini tentang " Ancaman, Serangan dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi: *Systematic Review*)." Fokus penelitian adalah Melakukan pemetaan antara jenis ancaman atau serangan dengan teknologi keamanan yang ada haruslah berdasarkan pada aspek dasar dari keamanan jaringan atau sistem informasi, yaitu: kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*). Hasilnya yakni menerapkan teknologi keamanan yang sesuai sebagai antisipasi dari beraneka ragam jenis ancaman atau serangan pada jaringan [1].

Penelitian kedua meneliti teknik mitigasi serangan Slowloris menggunakan framework Kali Linux. Studi ini mengungkapkan bahwa serangan Slowloris berdampak negatif terhadap kinerja server, tetapi dapat dikenali melalui pola lalu lintas jaringan. Strategi mitigasi, seperti membatasi koneksi server dan menggunakan firewall aplikasi web, terbukti efektif dalam mengurangi dampak serangan. Kesimpulannya, pemahaman

teknik serangan dan metode mitigasi sangat penting untuk meningkatkan keamanan jaringan[2].

Penelitian ketiga yang berjudul " Keamanan Jaringan Komputer Pada Era Big Data " membahas bentuk dan faktor ancaman keamanan komputer, juga beberapa saran untuk meningkatkan pencegahan dari ancaman keamanan komputer. Hasilnya melakukan pembersihan situs-situs phishing, tautan ilegal, spam, dan sebagainya dalam komputer. Jangan pernah memberikan kesempatan kepada penjahat karena hal itu merupakan kelalaian yang bisa berdampak serius terhadap kemanan komputer. Selain itu, pengembangan teknologi keamanan jaringan komputer harus terus menerus dilakukan sesegera mungkin dan mengurangi elemen ilegal secara teknis. Masih ada jalan panjang yang harus ditempuh untuk perkembangan teknologi keamanan jaringan komputer dimasa depan [3].

Penelitian keempat yang mengimplementasikan honeypot kipo pada sistem keamanan server dan menghasilkan persentase keberhasilan penanganan serangan oleh sistem yang dibangun sebesar 99%. Waktu rata-rata yang dibutuhkan oleh aplikasi website dalam mengirim notifikasi otomatis adalah 2.8 detik. Kinerja server akan meningkat 7.6% untuk CPU dan 562607.2K untuk memori apabila serangan ditangani oleh sistem yang dibangun [4].

Penelitian kelima yang berjudul " Implementasi Honeypot Pada Jaringan Internet Laboratorium Fakultass Teknik Uniks Menggunakan Dionaea Sebagai Keamanan Jaringan ". Temuan menjelaskan bagaimana cara kendali dan kontrol penuh terhadap *system,* dan hasilnya cukup memuaskan karena berhasil mendapatkan 63 dari 70 jenis virus yang ada dengan menggunakan bantuan virustotal.com. bantuan dari virus total yakni untuk membantu mendeteksi virus yang tidak dapat dikenali oleh honeypot [5].

Penelitian keenam tentang “Forensik Jaringan DDoS menggunakan Metode ADDIE dan HIDS pada Sistem Operasi Proprietary” menunjukkan bahwa tool DDoS Slowloris pada protokol HTTP merupakan alat yang sangat merusak dengan peningkatan trafik sebesar 92,84% dan penurunan performa server hingga 78%, menyebabkan server mengalami gangguan yang lebih parah dibandingkan dengan alat lain seperti LOIC UDP, LOIC TCP, dan PoD[6].

Penelitian yang ketujuh dengan judul “Penerapan dan Mitigasi Teknik Slowloris dalam Serangan Distributed Denial-of-Service (DDos) terhadap Website Ilegal dengan Kali Linux”. Penelitian ini berhasil menerapkan teknik Slowloris untuk melancarkan serangan Distributed Denial-of-Service (DDoS) terhadap website ilegal menggunakan Kali Linux. Hasil simulasi menunjukkan bahwa serangan Slowloris efektif dalam menghabiskan sumber daya server dan menyebabkan penurunan kinerja yang signifikan [7].

Penelitian kedelapan “Analisis Keamanan Jaringan Sistem Informasi Sekolah Menggunakan Penetration Test dan ISSAF” melakukan pengujian menggunakan Kali Linux dan Metasploit, yang menunjukkan bahwa semua port terdeteksi tertutup dengan

hasil Loss 100%. WireShark, yang juga digunakan dalam penelitian ini, tidak mendukung pengujian penetration test pada localhost, sehingga tidak dapat menangkap data. [8].

Penelitian yang kesembilan dengan judul"Implementasi Honeypot Dengan Metode Honeytrap". Penelitian ini melakukan implementasi pengujian terhadap Honeypot dengan metode Honeytrap dan meyimpulkan bahwa: Honeytrap yang dibangun berhasil memperkuat keamanan Web Server yaitu dengan cara mengalihkan penyerang ke server palsu serta Honeytrap yang dibangun dapat mendeteksi dari serangan port SSH, IP Address Target, dan Tanggal Waktu [9].

Penelitian kesepuluh, "Pemantauan dan Analisis Performa Sistem Honeypot dengan Simple Network Management Protocol (SNMP)", menyimpulkan bahwa pemantauan performa Honeypot dengan SNMP memungkinkan pengambilan data sensor. Analisis menunjukkan bahwa serangan yang masuk ke sensor Honeypot berdampak pada peningkatan beban CPU dan penggunaan memori perangkat.[10].

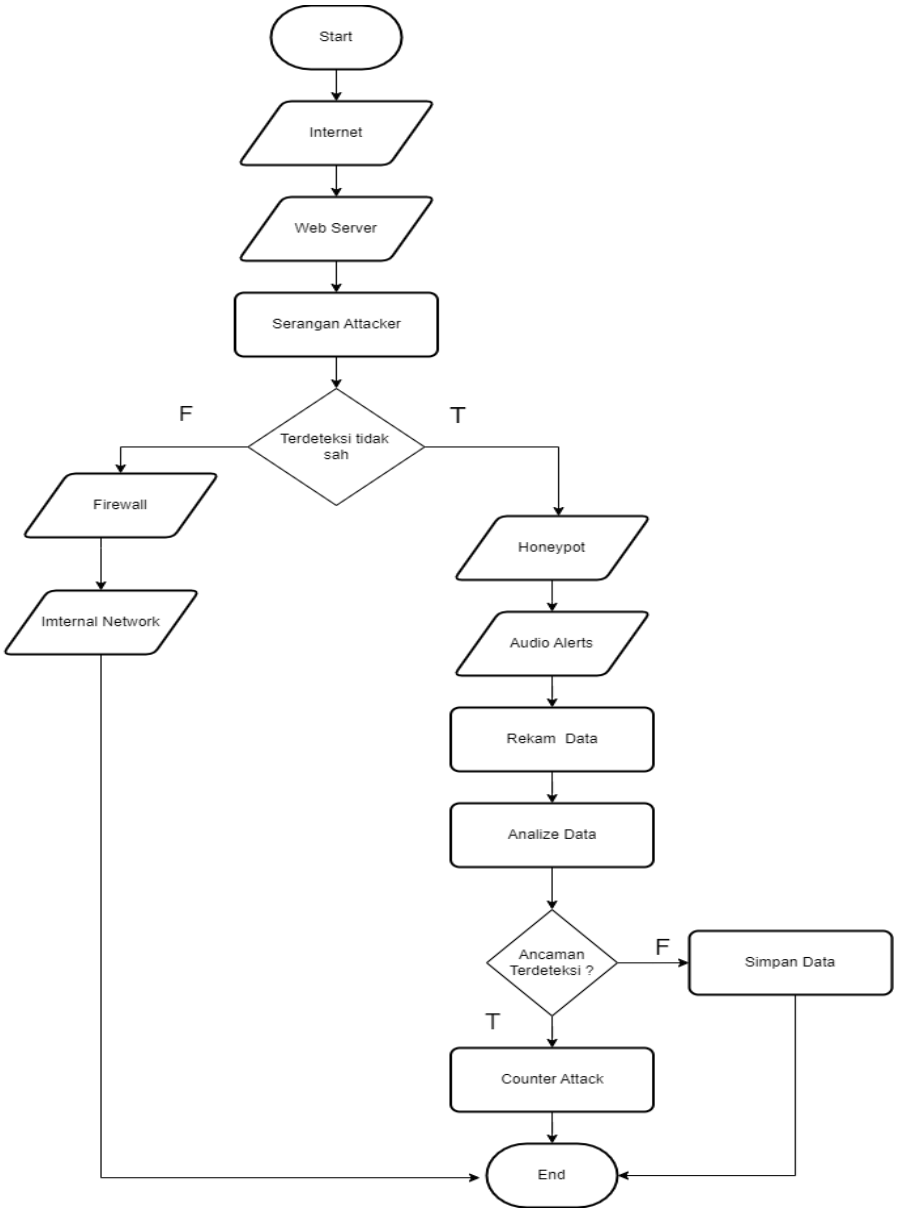
Berdasarkan tinjauan terhadap penelitian-penelitian sebelumnya, terdapat beragam pendekatan dalam mengatasi ancaman keamanan jaringan, mulai dari pemetaan ancaman [1], mitigasi serangan spesifik [2][7], hingga pencegahan dan pengujian keamanan [3][5][8]. Penelitian lain mengeksplorasi performa sistem [4][6] dan penggunaan honeypot untuk deteksi dasar [9][10], namun masih terbatas dalam hal penggabungan pemantauan real-time dengan analisis pola serangan serta strategi respons taktis. Penelitian ini, *"Pengendalian Keamanan Jaringan Menggunakan Tools Honeypot KFSENSOR"*, memberikan kontribusi lebih lanjut dengan mengintegrasikan penggunaan KFSensor untuk mendeteksi, menjebak, dan menganalisis aktivitas penyerang secara real-time. Solusi ini tidak hanya memantau, tetapi juga menyediakan data rinci guna evaluasi risiko dan perencanaan respons keamanan adaptif, menjadikannya lebih unggul dibandingkan pendekatan terdahulu dalam literatur.

## 3. METODE PENELITIAN

Pada diagram alir, proses deteksi dan respons terhadap serangan siber menggunakan kombinasi honeypot dan firewall dijelaskan secara sistematis. Proses dimulai ketika pengguna mengakses internet dan masuk ke web server. Jika terjadi serangan oleh attacker melalui internet, paket data diperiksa oleh honeypot. Paket data yang terdeteksi tidak sah diarahkan ke port honeypot untuk direkam dan dianalisis. Analisis ini bertujuan menentukan apakah paket data tersebut merupakan ancaman. Jika ancaman teridentifikasi, sistem memberikan peringatan audio kepada administrator, melakukan counter attack untuk mencegah kerusakan lebih lanjut, dan menyimpan data serangan sebagai referensi untuk evaluasi di masa mendatang. Paket data yang sah atau dianggap sah diteruskan ke *firewall* untuk diproses lebih lanjut sebelum diarahkan ke jaringan internal atau web server. Proses berakhir ketika paket data mencapai tujuan dengan aman atau ketika serangan berhasil direspons dan dihentikan. Diagram ini menunjukkan bagaimana sistem keamanan jaringan dapat mendeteksi, merekam, menganalisis, dan merespons serangan siber secara efektif.

Untuk mengukur efektivitas honeypot KFSensor, penelitian ini menggunakan parameter pengujian berupa:

1. Deteksi Waktu Nyata (*Real-Time Detection*): Kemampuan sistem untuk mendeteksi serangan secara langsung saat terjadi.
2. Tingkat Akurasi Analisis: Ketepatan honeypot dalam mengidentifikasi ancaman nyata dan membedakannya dari *false positive*.
3. *Respons Counter Attack*: Efektivitas respons terhadap serangan, termasuk waktu respons dan dampak mitigasi.
4. Rekam Data**:** Kualitas data serangan yang direkam untuk analisis lebih lanjut, meliputi detail seperti IP *attacker*, waktu serangan, dan metode yang digunakan.




Gambar 3. 1 *Flowchart* Penelitian

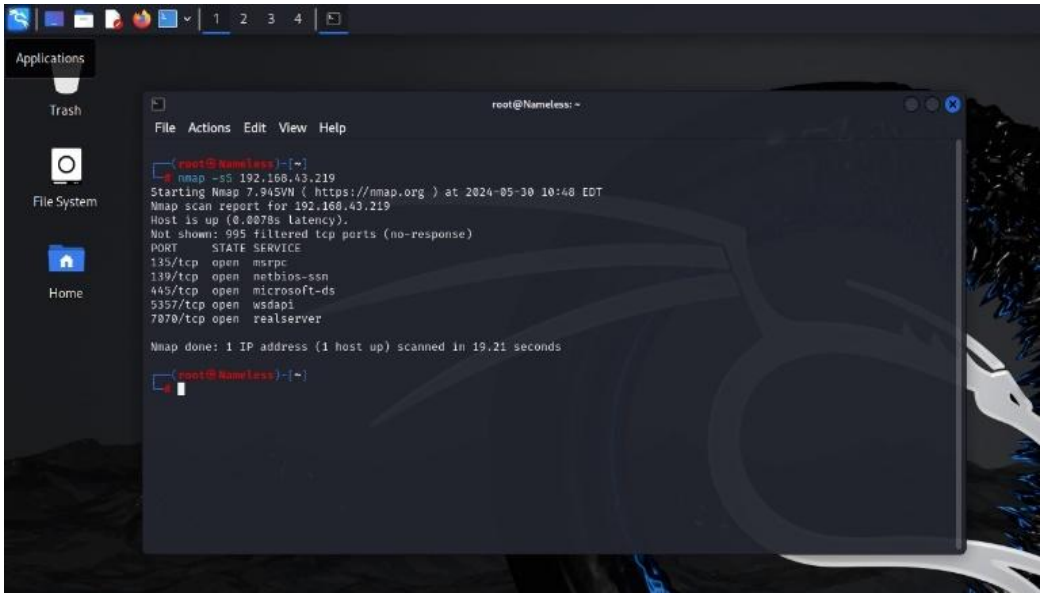
**Penjelasan Flowchart**

## 4. HASIL DAN PEMBAHASAN

### 4.1 Implementasi Honeypot KFSensor

1. Tanpa Honeypot KFSensor

Berikut ialah hasil *scanning* menggunakan Kali Linux menggunakan tools Nmap pada IP *Address device* yang dituju. Dibawah ini terdapat 5 *port* yang terbuka pada saat *scanning*, dengan *port* yang rentan seperti ini sang *attacker* sangat leluasa melakukan apa yang mereka inginkan terhadap target mereka dengan *port* yang tersedia.



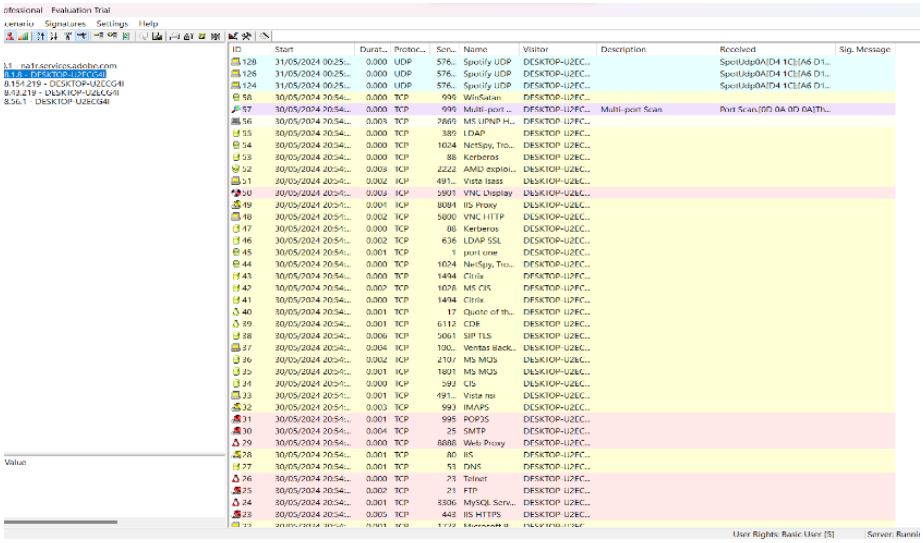

Gambar 4. 1 Hasil Nmap Scanning Tanpa Menggunakan Honeypot

2. Menggunakan Honeypot KFSensor

Berikut Ini Ialah hasil dari scanning pada IP *device* yang dituju, hasil dari scanning tersebut yakni mendapat total 13 port yang terbuka. Dimana Port yang terbuka ini ialah *Port* pengalihan/jebakan dari Honeypot KFSensor itu sendiri dan bukanlah *port* sebenarnya dari *device* yang akan di serang oleh sang *attacker*.


Gambar 4. 2 Hasil Nmap Scanning Menggunakan Honeypot

Setelah sang penyerang melakukan pemindaian (*scanning*) terhadap IP perangkat yang dituju, peran besar Honeypot KFSensor pun mulai terlihat. Di sinilah KFSensor memainkan perannya dengan mengalihkan perhatian atau menjebak penyerang untuk masuk ke dalam port yang telah disiapkan oleh KFSensor. Dengan cara ini, KFSensor dapat mengumpulkan informasi berharga mengenai metode serangan yang digunakan oleh penyerang tanpa menimbulkan risiko bagi sistem asli. Penyerang akan terkecoh dan menganggap bahwa mereka telah menemukan celah yang dapat dieksploitasi, padahal sebenarnya mereka hanya berinteraksi dengan sistem yang dirancang khusus untuk memonitor dan menganalisis perilaku *attacker* dan dapat dilihat lebih lanjut pada gambar di bawah ini untuk memahami bagaimana KFSensor melakukan tugas penting ini dalam menjaga keamanan jaringan. Coba kita lihat pada gambar dibawah ini;



Gambar 4. 3 Gambar detail scanning sang attacker di KFSensor

Sangat jelas di gambar diatas bahwa sang *visitor/attacker* masuk kedalam port yang tersedia di honeypot, dan di honeypot kita juga dapat melihat detail dari serangan sang *attacker* seperti *IP* sang *attacker* serta *port* yang yang mereka scan. Selanjutnya setelah penyerang melihat *port* yang tersedia dan tanpa menyadari bahwa *port* tersebut merupakan *port* pengalihan/jebakan dari honeypot, berikut adalah beberapa langkah yang mungkin mereka ambil dari sudut pandang penyerang:

1. Pemindaian Lebih Lanjut: Penyerang akan melakukan pemindaian lebih mendalam terhadap *port* yang terbuka untuk mengidentifikasi layanan apa yang berjalan di *port* tersebut. Mereka mungkin menggunakan alat seperti Nmap untuk mendapatkan lebih banyak informasi.
2. Pemeriksaan Kerentanan: Setelah mengetahui layanan apa yang berjalan di *port* tertentu, penyerang akan mencoba menemukan kerentanan yang diketahui pada layanan tersebut.

## 4.1 Efektivitas Honeypot KFSensor

### 4.1.1 Deteksi Cepat

Kecepatan Deteksi KFSensor mampu mendeteksi serangan dalam waktu nyata, memberikan notifikasi instan yang memungkinkan tim keamanan untuk merespons dengan cepat. Deteksi *real-time* ini sangat penting untuk mencegah potensi kerusakan lebih lanjut dan mengambil langkah-langkah mitigasi segera. Dengan honeypot sang pengguna dapat mengetahui secara *real time* serangan yang sedang terjadi.

### 4.1.2 Penanganan Serangan

1. *Respons* Taktis: Informasi yang diperoleh dari honeypot memungkinkan tim keamanan untuk merencanakan dan mengimplementasikan langkah-langkah taktis dalam menangani serangan. Misalnya, memblokir alamat IP yang mencurigakan atau memperkuat konfigurasi keamanan pada layanan yang disimulasikan, Serta memastikan bahwa potensi kelemahan dieksploitasi oleh honeypot diperbaiki sebelum dapat digunakan oleh penyerang nyata. Selain itu, tim dapat mengembangkan aturan dan kebijakan keamanan yang lebih adaptif, melakukan penyesuaian pada *firewall* dan sistem deteksi intrusi, serta meningkatkan pelatihan bagi staf keamanan untuk menghadapi skenario serangan yang teridentifikasi. Dengan respons taktis yang tepat, organisasi dapat meningkatkan postur keamanan mereka secara signifikan, mengurangi risiko serangan berhasil, dan memitigasi dampak dari setiap insiden yang terjadi.
2. Penilaian Risiko: Data serangan membantu dalam melakukan penilaian risiko yang lebih akurat dan menentukan prioritas dalam perlindungan aset kritis, memastikan bahwa sumber daya dan upaya keamanan difokuskan pada area yang paling rentan dan berisiko tinggi. Data ini juga

membantu dalam mengidentifikasi tren dan pola serangan, memungkinkan tim untuk mengantisipasi potensi ancaman di masa depan dan mengambil tindakan *preventif* yang diperlukan. Selain itu, penilaian risiko berbasis data serangan memungkinkan organisasi untuk mengalokasikan anggaran dan sumber daya dengan lebih efisien, dan memastikan bahwa investasi dalam keamanan memberikan hasil yang optimal dan sesuai dengan kebutuhan perlindungan yang diidentifikasi.

### 4.1.3 Analisis Ancaman

1. Identifikasi Pola Serangan: Hasil analisis data dari KFSensor menunjukkan bahwa alat ini mampu mendeteksi serangan dalam waktu nyata dengan tingkat akurasi yang cukup tinggi. Dalam contoh kasus yang ditampilkan, KFSensor berhasil mencatat aktivitas mencurigakan, termasuk jenis serangan, waktu kejadian, dan sumber serangan. Informasi yang diperoleh meliputi data detail seperti IP pengunjung (Visitor IP), port yang digunakan, domain, dan deskripsi aktivitas serangan. Sebagai contoh, dalam log serangan yang terdeteksi, terlihat aktivitas dari IP lokal (127.0.0.1) dengan jenis koneksi ke protokol TCP pada *port* 80, yang menunjukkan adanya upaya akses tidak sah ke server IIS. Data ini memberikan gambaran penting tentang bagaimana serangan dirancang dan dilakukan oleh attacker.
2. Analisis Pola dan Karakteristik Serangan:
   a. Frekuensi Serangan

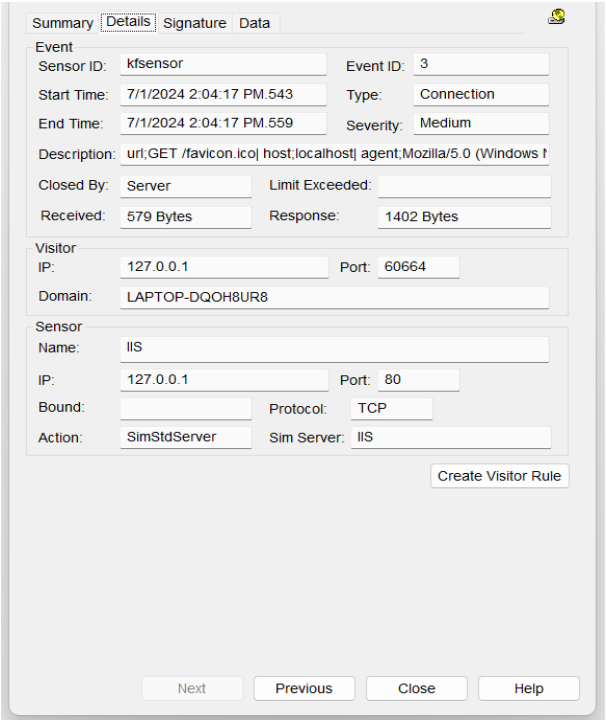
      Dari data yang dikumpulkan, serangan terjadi dengan pola tertentu, seperti peningkatan aktivitas pada waktu-waktu tertentu (misalnya, di jam kerja atau tengah malam). Hal ini menunjukkan bahwa serangan dirancang untuk memanfaatkan kelemahan dalam pengawasan sistem.

   b. Jenis Serangan

      Sebagian besar serangan yang terdeteksi melibatkan upaya eksploitasi port yang terbuka dan pemanfaatan skrip otomatis untuk mencoba akses ke server. Pola ini mengindikasikan bahwa serangan bersifat umum tetapi cukup berbahaya jika tidak segera diatasi.

   c. Karakteristik Penyerang

      Karakteristik yang diidentifikasi melalui KFSensor mencakup penggunaan agen pengguna (*user agent*) yang dimodifikasi untuk menyamar sebagai permintaan sah, serta upaya berulang untuk melebihi batas akses yang ditentukan.




Gambar 4. 4 Detail Serangan

## 5. KESIMPULAN

Pemberian pemahaman mendalam tentang pentingnya keamanan siber dan bagaimana berbagai serangan umum dapat dideteksi dan ditangani, berdasarkan data yang telah dikumpulkan dan dianalisis menggunakan honeypot KFSensor, dapat disimpulkan:

1. Efektivitas Honeypot KFSensor:

   Honeypot KFSensor terbukti efektif dalam mendeteksi serangan siber. Tanpa honeypot,5 *port* dari *device* yang dituju terdeteksi dan terbuka oleh alat pemindaian seperti Nmap, menunjukkan kerentanan yang jelas. Dengan honeypot, 13 *port* pengalihan terbuka, menipu penyerang dan mengalihkan mereka dari target sebenarnya. Honeypot membantu dalam merekam aktivitas penyerang, memberikan wawasan berharga tentang metode dan pola serangan yang digunakan.

2. Peningkatan Keamanan Jaringan:

   Penggunaan honeypot memungkinkan deteksi dini dan analisis mendalam terhadap berbagai jenis serangan siber, termasuk *phishing*, *brute force, malware injection*, dan SQL *injection*.

Kontribusi Penelitian:

Penelitian ini menunjukkan bahwa honeypot KFSensor bukan hanya alat deteksi serangan, tetapi juga sistem pendukung yang dapat meningkatkan keamanan jaringan secara keseluruhan. Kemampuan untuk memantau dan menganalisis serangan

memberikan peluang untuk memahami ancaman secara lebih mendalam dan menyusun kebijakan keamanan yang lebih tangguh.

Rekomendasi untuk Penelitian Lanjutan:

1. Penggunaan Lebih Lanjut Honeypot dalam Sistem Kompleks
   Implementasi honeypot dapat diperluas ke infrastruktur yang lebih kompleks, seperti jaringan multi-layer, untuk mengevaluasi keefektifannya di berbagai skenario serangan.
2. Integrasi dengan Sistem Keamanan Lain
   Kombinasi honeypot dengan teknologi keamanan lainnya, seperti *machine learning* untuk analisis pola serangan secara otomatis, dapat meningkatkan efektivitas sistem deteksi dan respons.

## DAFTAR PUSTAKA

[1] Bustami, A. and Bahri, S, 2020, Ancaman, Serangan dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi: Systematic Review.

[2] Sumayyah, Z. I., Permana S.,D.,S.,Tsabit, M. And Setiawan, A, 2024, Penerapan dan Mitigasi Teknik Slowloris dalam Serangan Distributed Denial-of-Service (DDos) terhadap Website Ilegal dengan Kali Linux, *Journal of Internet and Software Engineering*, vol. 1, no. 2, p. 14, Jun., doi: 10.47134/pjise.v1i2.2694.

[3] Munawar, Z., M. Kom, and Putri, N.,I, 2020, Keamanan Jaringan Komputer Pada Era Big Data.

[4] Ruslianto, I.,U. Ristian, J. Rekayasa Sistem Komputer, and F. H. MIPA Universitas Tanjungpura Jl Hadari Nawawi, 2019, Implementasi Honeypot Kipo pada Sistem Keamanan Server Berbasis Web Monitoring dengan Notifikasi Otomatis menggunakan API Telegram.

[5] Dermawati, R., and Siregar,M,H, 2020, Implementasi Honeypot Pada Jaringan Internet Labor Fakultas Teknik Uniks Menggunakan Dionaea Sebagai Keamanan Jaringan.

[6] Suharti, S. Yudhana, A and Riadi, A, 2022, Forensik Jaringan DDoS menggunakan Metode ADDIE dan HIDS pada Sistem Operasi Proprietary, *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 21, no. 3, pp. 567–582, Jul., doi: 10.30812/matrik.v21i3.1732.

[7] Sumayyah, Z.,I., Permana, S.,D.,S., Tsabit, M and Setiawan, A, 2024 Penerapan dan Mitigasi Teknik Slowloris dalam Serangan Distributed Denial-of-Service (DDos) terhadap Website Ilegal dengan Kali Linux, *Journal of Internet and Software Engineering*, vol. 1, no. 2, p. 14, Jun., doi: 10.47134/pjise.v1i2.2694.

[8] Silmina, E.,P, Firdonsyah, A and Amanda, R.,A.,A, 2022, Analisis Keamanan Jaringan Sistem Informasi Sekolah Menggunakan Penetration Test Dan Issaf, *Transmisi*, vol. 24, no. 3, pp. 83–91, Aug.

[9] Hassan, R.,H and Ismail S.,J,.I. 2020, Implementasi Honeypot Dengan Metode Honeytrap.

[10] Hariri, I.,K and Subardono, A. 2021, Pemantauan Dan Analisis Performa Sistem Honeypot Dengan Simple Network Management Protocol (SNMP).