JURNAL RISET SISTEM INFORMASI
Halaman Jurnal: https://journal.smartpublisher.id/index.php/jissi
Halaman UTAMA Jurnal : https://journal.smartpublisher.id

DOI: https://doi.org/10.69714/zxrv9q19

FORENSIK JARINGAN UNTUK INVESTIGASI KEJAHATAN CYBER

Rakhmadi Rahman[a*], Gina Latifa Akmal[b]
[a] Information System Department, rakhmadi.rahman@ith.ac.id, Institut Teknologi Bacharuddin Jusuf Habibie, Parepare Sulawesi Selatan
[b] Sistem informasi, ginalatifaa0@gmail.com, institut teknologi bacharuddin jusuf habibie, Parepare Sulawesi Selatan
[*] Korespondensi

ABSTRACT

This study investigates the application of Snort as an intrusion detection tool for addressing insider threats in network environments. The primary focus is on utilizing network forensic techniques to identify, analyze, and respond to suspicious activities conducted by internal users. The analysis method involves implementing Snort on a Linux platform to monitor network traffic in real-time and collect digital evidence that can be used in forensic investigations. The study successfully demonstrates that Snort is effective in detecting suspicious behavior patterns associated with insider threats, such as unauthorized access attempts and potentially malicious application usage. The digital evidence gathered by Snort aids in further forensic analysis, assisting in the identification of threat sources and facilitating a swift and appropriate response to security incidents. The discussion highlights the strengths and weaknesses of using Snort in the context of insider threat detection, emphasizing the importance of meticulous configuration and regular maintenance for optimal performance. The study concludes that employing Snort within a network forensic framework enhances an organization's ability to detect, analyze, and respond to insider threats, providing better protection for organizational assets and information from various internal cyber threats. This research lays the foundation for developing more effective security policies and improving cybersecurity awareness within organizations..

Keywords: *Insider threat, Snort, network forensics, digital evidence.*

Abstrak

Studi ini menginvestigasi penerapan Snort sebagai alat deteksi intrusi dalam menangani ancaman dari dalam (insider threat) di lingkungan jaringan. Fokus utama adalah pada penggunaan teknik forensik jaringan untuk mengidentifikasi, menganalisis, dan merespons aktivitas mencurigakan yang dilakukan oleh pengguna internal. Metode analisis melibatkan implementasi Snort pada platform Linux untuk memantau lalu lintas jaringan secara real-time dan mengumpulkan bukti digital yang dapat digunakan dalam proses penyelidikan forensik. Studi ini berhasil menunjukkan bahwa Snort efektif dalam mendeteksi pola perilaku mencurigakan yang terkait dengan ancaman dari dalam, seperti upaya akses tidak sah dan penggunaan aplikasi berpotensi berbahaya. Bukti digital yang dikumpulkan oleh Snort dapat digunakan untuk analisis forensik lebih lanjut, membantu identifikasi sumber ancaman dan memfasilitasi respon yang cepat dan tepat terhadap insiden keamanan. Diskusi menyoroti kelebihan dan kelemahan penggunaan Snort dalam konteks deteksi ancaman dari dalam, menekankan pentingnya konfigurasi yang cermat dan pemeliharaan teratur untuk kinerja optimal. Penelitian ini menyimpulkan bahwa penggunaan Snort dalam kerangka kerja forensik jaringan efektif dalam meningkatkan kemampuan organisasi dalam mendeteksi, menganalisis, dan merespons ancaman dari dalam, memberikan perlindungan yang lebih baik terhadap aset dan informasi organisasi dari berbagai ancaman siber internal. Studi ini memberikan landasan bagi pengembangan kebijakan keamanan yang lebih efektif dan peningkatan kesadaran keamanan siber di organisasi.

Kata Kunci: Ancaman dari dalam, Snort, forensik jaringan, bukti digital.

Received Juni 16, 2024; Revised Juni 19, 2024; Accepted Juli 23, 2024; Published Juli 25, 2024

1. PENDAHULUAN

Ancaman dari dalam bisa berasal dari karyawan, kontraktor, atau mitra bisnis yang memiliki berbagai motif, mulai dari ketidakpuasan, motif finansial, hingga kelalaian. Sebagai contoh, seorang karyawan yang tidak puas mungkin mencuri data sensitif sebagai tindakan balas dendam, sementara pelaku dengan motif finansial mungkin menjual informasi berharga kepada pihak ketiga. Kelalaian juga dapat menyebabkan ancaman dari dalam, di mana karyawan secara tidak sengaja mengungkapkan informasi sensitif atau membuka celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab.

Dampak dari ancaman dari dalam bisa sangat merusak bagi organisasi. Pencurian data sensitif seperti informasi pelanggan atau rahasia dagang dapat menyebabkan kerugian finansial yang signifikan, merusak reputasi perusahaan, dan menurunkan kepercayaan pelanggan. Selain itu, sabotase terhadap infrastruktur teknologi dapat mengganggu operasi bisnis dan menyebabkan kerugian operasional yang besar.

Untuk mengatasi ancaman dari dalam, penggunaan alat forensik jaringan seperti Snort menjadi sangat penting. Snort adalah alat open-source yang berfungsi sebagai sistem deteksi intrusi jaringan (NIDS) yang dapat menganalisis lalu lintas jaringan secara real-time untuk mendeteksi aktivitas mencurigakan. Dengan mengkonfigurasi Snort secara tepat, organisasi dapat memantau aktivitas jaringan, mengidentifikasi pola perilaku anomali, dan mengumpulkan bukti digital yang diperlukan untuk menyelidiki insiden keamanan.

Studi kasus ini mengeksplorasi bagaimana Snort dapat digunakan untuk mendeteksi dan menganalisis ancaman dari dalam di lingkungan jaringan Linux. Dengan memahami penerapan Snort dalam situasi nyata, organisasi dapat meningkatkan kemampuan mereka dalam melindungi aset dan informasi kritis dari ancaman internal yang berbahaya. Studi ini juga menyoroti pentingnya mengembangkan kebijakan dan prosedur keamanan yang efektif serta edukasi karyawan untuk mencegah ancaman dari dalam di masa depan.

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan eksperimental untuk menguji efektivitas Snort dalam mendeteksi dan menganalisis ancaman dari dalam (insider threat) di lingkungan jaringan Linux. Metode penelitian meliputi beberapa tahap, mulai dari persiapan lingkungan eksperimen, konfigurasi Snort, hingga pengujian dan analisis hasil. Berikut adalah tahapan detail yang dilakukan dalam penelitian ini:

2.1 Persiapan Lingkungan Eksperimen

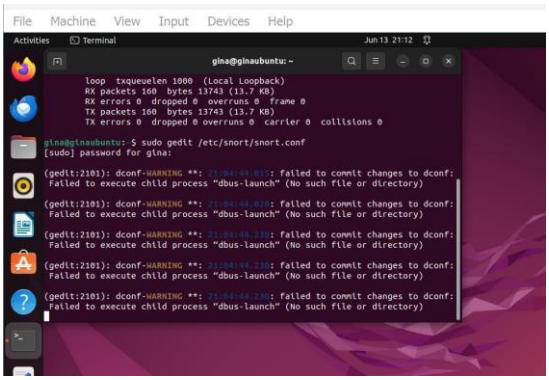
Langkah awal dalam penelitian ini adalah mempersiapkan lingkungan eksperimen yang mencakup:

a. Sistem Operasi: Menggunakan distribusi Linux (misalnya, Ubuntu) sebagai platform utama.
b. Perangkat Lunak: Menginstal Snort, sebuah sistem deteksi intrusi jaringan (NIDS) open-source.
c. Konfigurasi Jaringan: Menyusun topologi jaringan yang akan dipantau oleh Snort, termasuk menetapkan antarmuka jaringan yang relevan.

2.2 Instalasi dan Konfigurasi Snort

Snort diinstal dan dikonfigurasi untuk mendeteksi aktivitas mencurigakan yang terkait dengan ancaman dari dalam. Langkah-langkah yang dilakukan meliputi:

a. Instalasi Snort: Mengunduh dan menginstal Snort pada sistem Linux.
b. Konfigurasi Dasar: Mengedit file konfigurasi utama (`/etc/snort/snort.conf`) untuk menyesuaikan pengaturan sesuai kebutuhan, termasuk menentukan aturan yang akan digunakan untuk mendeteksi ancaman dari dalam.



Gambar 1 Konfigurasi Dasar

c. Aturan Khusus: Membuat dan mengedit file aturan khusus (misalnya, `/etc/snort/rules/ftp.rules`) untuk mendeteksi aktivitas mencurigakan yang terkait dengan protokol atau layanan tertentu.

Gambar 2 Aturan Khusus

2.3 Pengujian Konfigurasi

Setelah konfigurasi Snort selesai, dilakukan pengujian untuk memastikan semuanya berjalan dengan baik:

a. Perintah Pengujian: Menjalankan perintah `sudo snort -T -c /etc/snort/snort.conf -i enp0s3` untuk menguji konfigurasi Snort. Perintah ini memastikan bahwa file konfigurasi dan aturan yang digunakan tidak memiliki kesalahan.
b. Pemantauan Aktif: Setelah pengujian berhasil, Snort dijalankan dalam mode aktif dengan perintah `sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i enp0s3`. Perintah ini memulai Snort untuk memantau lalu lintas jaringan dan menampilkan peringatan di konsol.

2.4 Simulasi Serangan

Untuk mengevaluasi efektivitas Snort dalam mendeteksi ancaman dari dalam, dilakukan simulasi serangan menggunakan alat pemindaian jaringan:

a. Nmap: Menggunakan `nmap` untuk melakukan pemindaian terhadap alamat IP target (misalnya, mesin Ubuntu) guna meniru aktivitas mencurigakan yang mungkin dilakukan oleh pelaku ancaman dari dalam.
b. Pemantauan Respons Snort: Memantau bagaimana Snort mendeteksi dan merespons aktivitas pemindaian yang dilakukan oleh `nmap`.

2.5 Analisis Hasil

Setelah simulasi serangan, dilakukan analisis terhadap data yang dikumpulkan oleh Snort:

a. Peringatan Snort: Mengidentifikasi dan menganalisis peringatan yang dihasilkan oleh Snort selama simulasi serangan.
b. Bukti Digital: Mengumpulkan dan mengevaluasi bukti digital yang dikumpulkan oleh Snort untuk memastikan validitas dan relevansinya dalam konteks penyelidikan forensik.
c. Efektivitas Deteksi: Menilai efektivitas Snort dalam mendeteksi ancaman dari dalam berdasarkan respons terhadap simulasi serangan.

2.6 Penyusunan Laporan

Tahap akhir adalah penyusunan laporan penelitian yang mencakup:

a. Deskripsi Metodologi: Menjelaskan secara rinci metode penelitian yang digunakan.
b. Hasil dan Diskusi: Menyajikan hasil pengujian dan analisis, serta mendiskusikan temuan utama.
c. Kesimpulan: Menyimpulkan penelitian dan memberikan rekomendasi untuk pengembangan lebih lanjut.

3. METODOLOGI PENELITIAN

Metode penelitian ini bertujuan untuk memberikan pemahaman yang komprehensif tentang bagaimana Snort dapat digunakan untuk mendeteksi dan menganalisis ancaman dari dalam di lingkungan jaringan Linux, serta memberikan wawasan praktis bagi organisasi dalam mengimplementasikan strategi keamanan siber yang efektif.

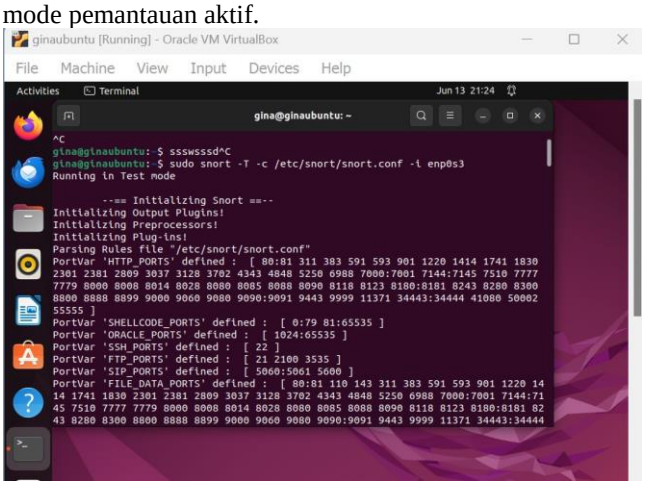
4. HASIL DAN PEMBAHASAN

4.1 Hasil

Penelitian ini menghasilkan beberapa temuan penting terkait dengan efektivitas Snort dalam mendeteksi dan menganalisis ancaman dari dalam di lingkungan jaringan Linux. Berikut adalah hasil dari setiap tahap yang telah dilakukan:

4.1.1. Pengujian Konfigurasi Snort

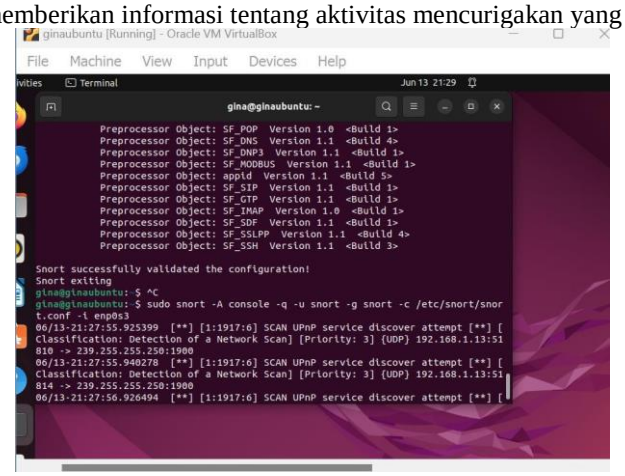
Pengujian konfigurasi Snort dengan perintah `sudo snort -T -c /etc/snort/snort.conf -i enp0s3` menunjukkan bahwa file konfigurasi dan aturan yang digunakan telah diatur dengan benar tanpa kesalahan. Snort siap untuk dijalankan dalam mode pemantauan aktif.



Gambar 3 Pengujian Konfigurasi Snort

4.1.2. Pemantauan Lalu Lintas Jaringan

Saat Snort dijalankan dalam mode aktif (`sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i enp0s3`), sistem berhasil memantau lalu lintas jaringan secara real-time. Peringatan yang dihasilkan ditampilkan di konsol, memberikan informasi tentang aktivitas mencurigakan yang terdeteksi.

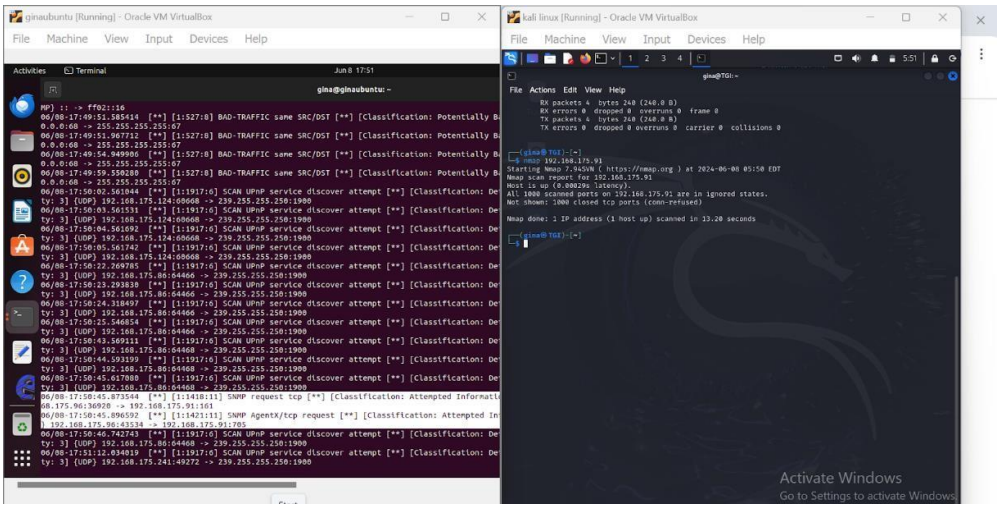


Gambar 4 Pemantauan lalulintas Jaringan

4.1.3. Simulasi Serangan dengan Nmap

Penggunaan `nmap` untuk memindai alamat IP target berhasil memicu sejumlah peringatan pada Snort. Contoh peringatan yang muncul termasuk deteksi pemindaian port yang mencurigakan dan upaya akses tidak sah terhadap layanan tertentu. Berikut adalah beberapa contoh peringatan yang dihasilkan:

a. Peringatan Pemindaian Port: Snort mendeteksi pemindaian port yang dilakukan oleh `nmap` dan mengidentifikasinya sebagai aktivitas mencurigakan.
b. Peringatan Akses Tidak Sah: Upaya untuk mengakses layanan tertentu tanpa otorisasi terdeteksi oleh Snort, memicu peringatan yang menunjukkan adanya kemungkinan ancaman dari dalam.



Gambar 5 Simulasi serangan dengan Namp

4.1.4. Pengumpulan Bukti Digital

Snort mengumpulkan bukti digital berupa log aktivitas jaringan yang mencurigakan. Log ini mencakup detail seperti alamat IP sumber, alamat IP tujuan, jenis protokol yang digunakan, dan timestamp kejadian. Bukti ini dapat digunakan dalam analisis forensik lebih lanjut untuk mengidentifikasi pelaku dan pola serangan.

4.2 Pembahasan

Hasil penelitian menunjukkan bahwa Snort efektif dalam mendeteksi aktivitas mencurigakan yang terkait dengan ancaman dari dalam. Beberapa poin penting dari pembahasan ini adalah:

4.2.1. Efektivitas Snort dalam Deteksi Ancaman dari Dalam

Snort terbukti mampu mendeteksi berbagai jenis aktivitas mencurigakan yang sering kali dilakukan oleh orang dalam, seperti pemindaian port dan upaya akses tidak sah. Peringatan yang dihasilkan memberikan informasi yang cukup untuk mengidentifikasi dan mengatasi ancaman tersebut.

4.2.2. Pentingnya Konfigurasi yang Tepat

Keberhasilan Snort dalam mendeteksi ancaman sangat bergantung pada konfigurasi yang tepat. File konfigurasi (`/etc/snort/snort.conf`) dan aturan deteksi harus disesuaikan dengan kebutuhan spesifik jaringan dan jenis ancaman yang diantisipasi. Konfigurasi yang tidak tepat dapat menyebabkan deteksi yang kurang efektif atau kesalahan positif.

4.2.3. Penggunaan Bukti Digital dalam Analisis Forensik

Bukti digital yang dikumpulkan oleh Snort sangat berharga dalam proses analisis forensik. Detail log yang lengkap memungkinkan penyelidik untuk melacak aktivitas mencurigakan, mengidentifikasi pelaku, dan memahami pola serangan. Hal ini membantu dalam penyusunan laporan penyelidikan yang akurat dan dapat digunakan untuk tindakan hukum atau penegakan kebijakan keamanan.

4.2.4. Keterbatasan dan Tantangan

Meskipun Snort efektif dalam mendeteksi banyak jenis ancaman, ada beberapa keterbatasan yang perlu diperhatikan:

a. Kesalahan Positif: Snort dapat menghasilkan sejumlah kesalahan positif yang memerlukan analisis lebih lanjut untuk memastikan bahwa peringatan yang dihasilkan benar-benar mencerminkan ancaman yang nyata.
b. Pemeliharaan dan Pembaruan: Snort membutuhkan pemeliharaan dan pembaruan aturan secara teratur untuk memastikan kinerjanya tetap optimal dan mampu mendeteksi ancaman terbaru.

4.3 Implikasi Praktis

Implementasi Snort sebagai bagian dari strategi keamanan siber organisasi dapat memberikan manfaat signifikan dalam mendeteksi dan mengatasi ancaman dari dalam. Organisasi harus memastikan bahwa tim keamanan mereka terlatih dalam mengkonfigurasi dan memantau Snort, serta mampu menganalisis bukti digital yang dikumpulkan untuk tindakan lebih lanjut.

4.4 Rekomendasi

Untuk meningkatkan efektivitas deteksi dan respon terhadap ancaman dari dalam, organisasi disarankan untuk:

a. Mengembangkan Kebijakan Keamanan yang Kuat: Menetapkan kebijakan dan prosedur yang jelas untuk menangani ancaman dari dalam.
b. Pelatihan dan Edukasi: Memberikan pelatihan yang memadai kepada karyawan tentang pentingnya keamanan siber dan bagaimana menghindari tindakan yang dapat menyebabkan ancaman dari dalam.
c. Pemeliharaan Berkala: Melakukan pemeliharaan berkala dan pembaruan aturan Snort untuk memastikan deteksi ancaman tetap optimal.

Pembahasan ini memberikan pemahaman mendalam tentang hasil penelitian dan implikasi praktis dari penggunaan Snort dalam mendeteksi dan menganalisis ancaman dari dalam, serta memberikan rekomendasi untuk meningkatkan strategi keamanan siber organisasi.

5. KESIMPULAN DAN SARAN

Penelitian ini telah menunjukkan bahwa Snort, sebagai sistem deteksi intrusi jaringan (NIDS), efektif dalam mendeteksi dan menganalisis ancaman dari dalam (insider threats) di lingkungan jaringan Linux. Beberapa poin penting yang dapat disimpulkan dari penelitian ini adalah: Efektivitas Snort dalam Deteksi Ancaman dari Dalam: Snort terbukti mampu mendeteksi aktivitas mencurigakan yang sering kali dilakukan oleh pelaku ancaman dari dalam, seperti pemindaian port dan upaya akses tidak sah. Peringatan yang dihasilkan memberikan informasi yang cukup untuk mengidentifikasi dan mengatasi ancaman tersebut. Pentingnya Konfigurasi yang Tepat: Keberhasilan Snort dalam mendeteksi ancaman sangat bergantung pada konfigurasi yang tepat. Pengaturan yang cermat pada file konfigurasi dan aturan deteksi sangat penting untuk memastikan bahwa Snort dapat berfungsi secara optimal. Penggunaan Bukti Digital dalam Analisis Forensik: Bukti digital yang dikumpulkan oleh Snort, termasuk log aktivitas jaringan yang mencurigakan, sangat berharga dalam proses analisis forensik. Log ini memungkinkan penyelidik untuk melacak aktivitas mencurigakan, mengidentifikasi pelaku, dan memahami pola serangan. Tantangan dan Keterbatasan: Meskipun Snort efektif dalam mendeteksi banyak jenis ancaman, kesalahan positif dan kebutuhan untuk pemeliharaan serta pembaruan aturan secara teratur tetap menjadi tantangan yang perlu diatasi.

Berdasarkan temuan penelitian ini, berikut adalah beberapa saran untuk meningkatkan efektivitas deteksi dan respon terhadap ancaman dari dalam menggunakan Snort: Pengembangan Kebijakan Keamanan yang Kuat: Organisasi harus menetapkan kebijakan dan prosedur keamanan yang jelas untuk menangani ancaman dari dalam. Kebijakan ini harus mencakup pedoman untuk penggunaan sistem, pelatihan karyawan, dan respon terhadap insiden keamanan. Pelatihan dan Edukasi: Memberikan pelatihan yang memadai kepada karyawan tentang pentingnya keamanan siber dan cara menghindari tindakan yang dapat menyebabkan ancaman dari dalam sangat penting. Edukasi yang berkelanjutan dapat membantu menciptakan kesadaran yang lebih baik tentang keamanan siber di seluruh organisasi. Pemeliharaan Berkala dan Pembaruan: Untuk memastikan Snort tetap efektif dalam mendeteksi ancaman terbaru, organisasi harus melakukan pemeliharaan berkala dan pembaruan aturan secara rutin. Ini termasuk memperbarui aturan deteksi untuk mengidentifikasi ancaman yang baru muncul. Integrasi dengan Sistem Keamanan Lain: Mengintegrasikan Snort dengan sistem keamanan lainnya, seperti SIEM (Security Information and Event Management), dapat meningkatkan kemampuan deteksi dan analisis. Integrasi ini memungkinkan pengumpulan data yang lebih komprehensif dan respon yang lebih cepat terhadap insiden keamanan. Evaluasi dan Audit Rutin: Melakukan evaluasi dan audit rutin terhadap sistem deteksi intrusi dan kebijakan keamanan organisasi dapat membantu mengidentifikasi kelemahan dan area yang perlu ditingkatkan. Evaluasi ini juga membantu memastikan bahwa langkah-langkah keamanan yang diambil tetap relevan dan efektif.

Dengan menerapkan saran-saran ini, organisasi dapat meningkatkan kemampuan mereka dalam mendeteksi, menganalisis, dan merespons ancaman dari dalam, sehingga memberikan perlindungan yang lebih baik terhadap aset dan informasi kritis mereka.

DAFTAR PUSTAKA

[1] Ahmad Sakhowi Amin, and Pipit Dewi Arnesia. “Pengembangan Sistem Keamanan Jaringan Menggunakan Network Forensics.” Bit, vol. 20, no. 1, 30 Apr. 2023, pp. 50–50, https://doi.org/10.36080/bit.v20i1.2180. Accessed 14 June 2024.

[2] Ashilah, A. P., & Rahman, R. (2024). FORENSIK JARINGAN UNTUK INVESTIGASI KEJAHATAN CYBER PADA STUDI KASUS PEMBOBOLAN DATA KOMINFO OLEH BJORKA. *Jurnal Riset Sistem Informasi*, *1*(3), 17-26.

[3] Julias Sulicdio, et al. "Comparative Analysis of Wireshark and Windump Software in Network Security Monitoring." Deleted Journal, vol. 1, no. 1, 25 Jan. 2022, https://doi.org/10.37676/jmcs.v1i1.1901. Accessed 14 June 2024.

[4] Rizdqi Akbar Ramadhan, et al. "Network Forensic: Analysis of Client Attack and Quality of Service Measurement by ARP Poisoning Using Network Forensic Generic Process (NFGP) Model." Sistemasi, vol. 13, no. 2, 23 Mar. 2024, pp. 713–713, https://doi.org/10.32520/stmsi.v13i2.3804 . Accessed 14 June 2024.

[5] R. Sanjeetha, "Mitigating HTTP GET FLOOD DDoS Attack Using an SDN Controller," International Conference on Recent Trends on Electronic, Information, Communictioan & Technology, pp. 6–10, 2020.

[6] suharti, sri, Yudhana, A., & Riadi, I. (2022). Forensik Jaringan DDoS menggunakan Metode ADDIE dan HIDS pada Sistem Operasi Proprietary. *MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, *21*(3), 567-582.

[7] Sutarti, et al. "ANALISIS WEB PHISHING MENGGUNAKAN METODE NETWORK FORENSIC DAN BLOCK ACCESS SITUS DENGAN ROUTER MIKROTIK." PROSISKO Jurnal Pengembangan Riset Dan Observasi Sistem Komputer, vol. 10, no. 1, 14 June 2024, pp. 71–83, https://doi.org/10.30656/prosisko.v10i1.7048.

[8] P. Bhale, S. Biswas, and S. Nandi, "LORD: Low Rate DDoS Attack Detection and Mitigation Using Lightweight Distributed Packet Inspection Agent in IoT Ecosystem," International Symposium on Advanced Networks and Telecommunication Systems, ANTS, vol. 2019-December, pp. 2–7, 2019.