LINIER
LITERATUR INFORMATIKA & KOMPUTER
e-ISSN: 3063-2218
DOI : 10.33096/linier.vxix.xxxx
Literatur Informatika & Komputer
Vol 1, No 3 (2024), pp 235-240

Perancangan Sistem Keamanan Jaringan Intrusion Prevention System Menggunakan Suricata Dan IPTables

Andi Rahmat Aulia[a], Erick Irawadi Alwi[b], Andi Widya Mufila Gaffar[c]
Universitas Muslim Indonesia, Makassar, Indonesia
[a]13020180182@umi.ac.id; [b]erick.alwi@umi.ac.id; [c]widya.mufila@umi.ac.id

Received: xx xx xxxx | Revised: xx xx xxxx | Accepted: xx xx xxxx | Published: xx xx xxxx

Abstrak
Server merupakan perangkat dalam jaringan telekomunikasi yang bertugas mendistribusikan perangkat lunak *IPTables* dan basis data. Salah satu tipe server yang rentan terhadap serangan *Denial of Service* (DoS) merupakan *web server*. Serangan DoS bekerja dengan menghabiskan sumber daya server sehingga menyebabkan server tersebut menjadi tidak dapat diakses atau *down*. Oleh karena itu, penelitian ini bertujuan untuk mengembangkan sistem pencegahan serangan dengan menggunakan *Intrusion Prevention System* (IPS) yang memanfaatkan *Suricata* dan *IPTables* sebagai mekanisme deteksi dan pencegahan serangan DoS pada *web server*. IPS bekerja dengan menganalisis lalu lintas jaringan yang masuk dan keluar, melakukan inspeksi mendalam terhadap setiap *paket data* yang melintasi jaringan. Dengan penerapan *Suricata* dan *IPTables* pada *web server*, administrator jaringan dapat memastikan keamanan *web server* dari ancaman serangan. Penelitian ini akan menunjukkan bahwa aturan *Suricata* dan *IPTables* efektif dalam mendeteksi serangan yang dilakukan dengan alat *Hping3*, sebuah perangkat lunak yang digunakan untuk melakukan pemindaian jaringan dan secara *default* tersedia di *Kali Linux* yang akan dimanfaatkan untuk simulasi serangan DoS.

Kata kunci: IPS, *Suricata*, *IPTables*, DoS, *Hping3*.

Pendahuluan

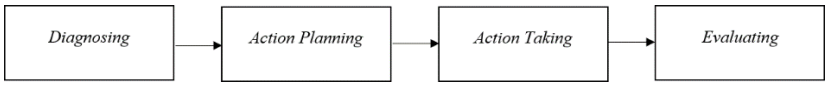
Server merupakan alat telekomunikasi dalam jaringan yang mendistribusikan peralatan *software* dan database diantara berbagai terminal kerja dalam jaringan server [1]. Server merupakan pusat layanan dan pengolahan data dalam suatu jaringan atau sistem komputer yang menjalankan layanan tertentu. Server dapat diskalakan dan didukung oleh prosesor yang dilengkapi dengan sistem operasi jaringan [2]. Penggunaan *web server* sering kali digunakan untuk kegunaan atau popularitas konten berdasarkan jumlah kunjungan atau pengunjung. Maka diperlukan suatu sistem keamanan jaringan yang dapat memantau apakah *web server* sedangdiserang atau tidak [3]. Perangkat lunak administratif yang digunakan oleh server juga memiliki kemampuan untuk mengatur akses ke jaringan dan sumber daya, seperti mengakses berkas dan memberikan akses kepada anggota jaringan yang bekerja. di mana banyak sistem keamanan server bergantung pada administrator, membuat sistem bergantung pada administrator untuk mengatasi gangguan dan bergantung pada seberapa cepat administrator dapat memperbaiki jaringan. Gangguan tersebut dapat membuat *server down*, membuat administrator tidak dapat memperbaiki jaringan dengan cepat [2].

Serangan DoS merupakan salah satu serangan *cyber* populer yang ditargetkan pada situs web organisasi terkenal dan berpotensi memiliki biaya ekonomi dan waktu yang tinggi. Dalam penelitian ini, beberapa metode pembelajaran mesin termasuk model *ensemble* dan pengklasifikasi *deep learning* berbasis autoencoder dibandingkan dan disetel menggunakan optimasi Bayesian. Kerangka autoencoder memungkinkan untuk mengekstrak fitur baru dengan memetakan input asli ke ruang baru. Metode tersebut dilatih dan diuji baik untuk klasifikasi biner dan multi-kelas pada kumpulan data Digiturk dan Labris yang baru-baru ini diperkenalkan untuk mendeteksi berbagai jenis serangan DDoS. Semakin penting koneksi data melalui Internet membuat kebutuhan akan keamanan jaringan data semakin meningkat. Salah satu tools yang penting merupakan *Intrusion Detection Systems* (IDS) [4]. Jenis serangan DoS yang menyebabkan habisnya sumber daya pada sistem merupakan UDP*Flooding* yang menggunakan protokol UDP sebagai akses penyerangan dan SYN *Flooding* yang terjadi saatdua komputer berkomunikasi. Penyerang akan mengirimkan banyak pesan "*syn ack*" ke komputer tujuan [5].

Perangkat keamanan jaringan *Intrusion Prevention System* (IPS) merupakan salah satu *tool* pengamanan pada jaringan. Pada penelitian ini Suricata sebagai IPS untuk melindungi *web server* dari serangan SQL *Injection* menggunakan SQLMap dengan melihat efektifitas *rules* dan parameter *response time* [6]. *Suricata* merupakan aplikasi pendeteksi yang sudah memiliki IDS yang memiliki kemampuan untuk

menghentikan serangan dengan mengirimkan *packet drop* yang dicurigai. *Suricata* berbeda dari *snort* karena memiliki dukungan untuk aturan yang luas, sehingga dapatberkomunikasi dengan bahasa aturan *snort* dengan cara yang sama [7]. Dan ada juga perangkat keamanan lainnya seperti *IPTables, IPTables* merupakan alat untuk menyaring atau mengatur lalu lintas data memiliki tiga jenis aturan dalam tabel filter: jalur firewall, jalur input, jalur output, dan jalur maju dan hanya dapat digunakan di sistem operasi *Linux* [8]. Karena teknologi ini berasal dari IDS yangdapat mendeteksi dan memblokir ancaman. Selain itu, teknologi ini dapat digabungkan dengan teknologi SMS yang memungkinkan *System* Administrator untuk mengidentifikasi dan menangani setiap masalah dengan cepat [9].

Metode



Gambar 1. Metode Penelitian

Gambar 1 menunjukkan bahan penelitian ini menggunakan metode *action research* yang menggabungkan teori dengan praktik. Untuk menyelesaikan penelitian ini, metode penelitian tindakan diperlukan untuk melakukan sebuah perancangan sistem, analisis, instalasi, dan pengujian. Perlu adanya identifikasi masalah pada masalah keamanan jaringan pada server. Untuk melakukan pengembangan pada tahap ini sehingga peneliti memahami pokok masalah yang ada kemudian membuat skema rencana tindakan yang tepat untuk menyelesaikan permasalahan yang ada. Seperti membuat topologi jaringan dan rancangan alur kerja sistem dan peneliti juga membuat skema rencana yang telah dibuat dengan harapan dapat menyelesaikan masalah. Pada tahap ini peneliti melakukan uji coba atau mengimplementasikan *Suricata* dan *IPTables* untuk mendeteksi serangan *DoS*.

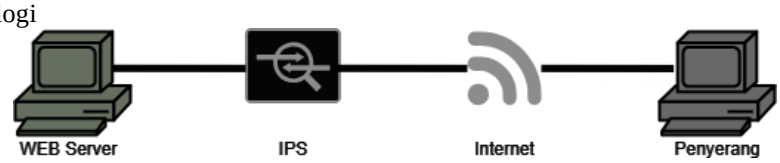
1. DoS merupakan singkatan dari *Denial of Service*, sebuah teknik penyerangan terhadap sebuah sistem dengan jalan menghabiskan sumber data sistem tersebut sehingga tidak dapat diakses lagi. Sumber daya dapat berupa CPU, RAM, Swap, *cache*, maupun *bandwidth*. Jenis serangan DoS: UDP Flood Attack, ICMPFlood, Ping Flood, Ping of Death, SYNFlood, dan HTTPFlood. Tools DoS meliputi: LOIC, *Hping3*, dan GoldeEye [10]
2. *Intrusion Prevention System* (IPS) merupakan sistem *hardware* atau *software* yang memiliki kemampuan untukmemantau trafik jaringan, menemukan aktivitas yang tidak diinginkan, dan mencegah atau mencegah pencurian atau kejadian lain yang dapat mengganggu jaringan. Dengan menggabungkan teknik *Firewall* dan metode IPS, IPS dapat digunakan sebagai piranti untuk mencegah aktivitas yang tidak diinginkan yanghendak masuk ke sistem jaringan yang dibangun. Mereka memeriksa, merekam, dan mencatat semua paketdata dan mengenali paket melalui sensor yang mengidentifikasi serangan atau memberikan pemberitahuan [11]. Cara kerja IPS didasarkan pada analisis lalu lintas jaringan yang masuk dan keluar. IPSakan melakukan inspeksi mendalam terhadap setiap paket data yang melewati jaringan, membandingkannya dengan basis pengetahuan yang luas tentang serangan yang diketahui, dan mengambil tindakan untuk memblokir atau menghentikan serangan tersebut. Peneliti sebelumnya juga menunjukkan bahwa sistem pencegahan serangan IPS dapat mencegah serangan atau penyusupan. Pola serangan yang ada dalam aturan IPS menyebabkan serangan terdeteksi, jadi perangkat IPS harus dikonfigurasi dengan benar dan sering mengembangkan aturan IPS [12]. Penelitian lainnya menyatakan bahwa IPS berbasis *Snort* dapat digunakan Bersama telegram dan *IPTables* sehingga dapat mendeteksi dan memblokir lima seranganyang terjadi secara otomatis; serangan *Ftp, Telnet, Bruteforce From Login* menggunakan serangan *Hydra,Rfi Fan Http Bruteforce* dengan menggunakan serangan *Hydra*. Melalui telegram, sistem dapat mengetahuiserangan pada server internet melalui pesan notifikasi yang berisikan informasi tentang jenis serangan dankapan terjadinya [13]. Penelitian ini membuat IPS dengan menggunakan *Suricata* dan *IPTables. Suricata* merupakan aplikasi pendeteksi yang sudah memiliki IDS yang memiliki kemampuan untuk menghentikan serangan dengan mengirimkan *packet drop*yang dicurigai. *Suricata* berbeda dari *snort* karena memiliki dukungan untuk aturan yang luas, sehingga dapat berkomunikasi dengan bahasa aturan *snort* dengan cara yang sama.
3. *IPTables* merupakan alat untuk menyaring atau mengatur lalu lintas data di sistem operasi *Linux*. Itu

memiliki tiga jenis aturan dalam tabel filter: jalur *firewall*, jalur *input*, jalur *output*, dan jalur maju [14].

4. *Hping3* yang merupakan alat yang digunakan untuk memindai jaringan. itu tersedia di *kali linux* secara *default* itu merupakan salah satu perangkat lunak serangan DoS, merupakan singkatan dari serangan *denial of service* [15].

Perancangan

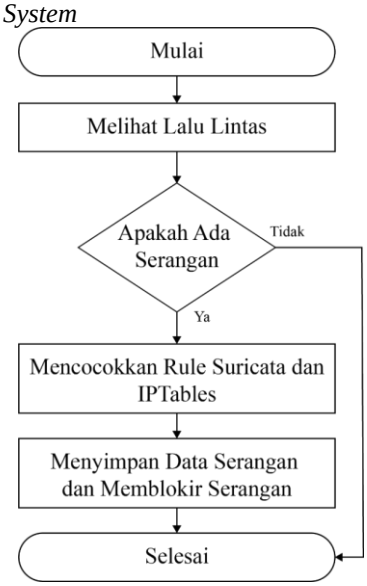
A. Desain Topologi



Gambar 2. Desain Topologi

Gambar 2 merupakan rangkaian topologi fisik sesuai dengan sistem yang akan dijalankan. Pada gambar topologi jaringan diatas terdapat 2 PC yaitu, PC 1 berperan sebagai pendeteksi adanya serangan pada server dan sekaligus menjadi server. Kemudian PC 2berperan sebagai *attacker* yang akan melakukan serangan pada server. Topologi ini mensimulasikan bahwa pengujian serangan dilakukan melalui komputer *attacker* yang terhubung pada jaringan. *Attacker* akan melakukan penyerangan dengan menggunakan serangan DoS yang menggunakan tools*Hping3*. IPS akan melakukan blok jaringan terhadap paket-paket yang masuk pada sistem dan memberikan pemberitahuan yang berupa serangan yang terjadi.

B. Cara Kerja *Intrusion Prevention System*



Gambar 3. Alur Kerja *Intrusion Prevention System*

Gambar 3 merupakan cara kerja sistem IPS *Suricata* dan *IPTables*. Langkah pertama yang dilakukan yaitu analisis lalu lintas jaringan yang masuk dan keluar setiap paket, melakukan inspeksi mendalam terhadap setiap paket data yang melewati jaringan, membandingkannya dengan basis pengetahuan yang luas tentang serangan yang diketahui,dan akan disaring apabila ada serangan yang sesuai dengan *rules* maka IPS *Suricata* dan *IPTables* akan memberikan peringatan serta memblokir serangan tersebut, dan menyimpan data dari serangan yang telah dilakukan.

C. Alur Skenario Serangan

Gambar 4, merupakan alur pengujian penyerangan menggunakan *tools Hping3* dengan serangan DoS jenis SYN Flood. Penyerangan ini dilakukan pada PC 2 (PC attacker). Proses pertama yang dilakukanyaitu menyiapkan *Hping3*, lalu jika berhasil maka langsung menguji serangan pada server, apabila terjadi serangan maka pengujian serangan telah berhasil.

Gambar 4. Alur Penyerangan

Pemodelan

A. Instalasi *Suricata*

Tahapan pertama yaitu menambahkan repository dari *Suricata* dengan *command sudo add-apt-repository ppa:oisf/Suricata-stable*, Gambar menambahkan repository dapat dilihat pada Gambar 5.

Gambar 5. Menambahkan Repository *Suricata*

Tahapan selanjutnya instalasi Suricata dengan command *dan sudo apt-get install Suricata*, instalasi *suricata* dapat dilihat pada Gambar 6.

Gambar 6. Instalasi *Suricata*

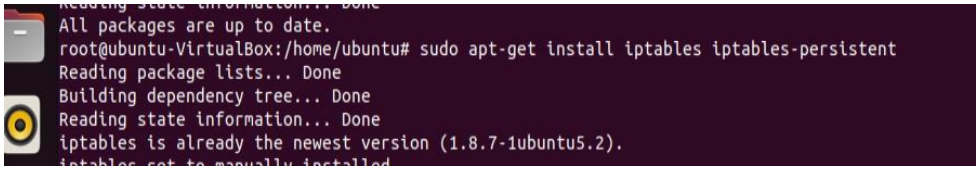
Langkah berikutnya mengecek status *Suricata*, Suricata akan langsung aktif setelah di install. Untuk tahapan enable dan melihat *Suricata* sudah aktif bisa dilakukan dengan *command sudo systemctl enable Suricata dan sudo systemctl status suricata.service* dapat dilihat pada Gambar 7.

Gambar 7. Pengecekan status *Suricata*

Gambar 8. Konfigurasi Suricata

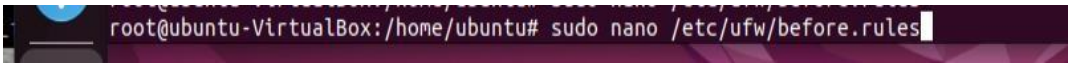
Gambar 8 merupakan konfigurasi *IP Address* komputer yang ingin dimonitoring. Pengeditan konfigurasi dari Suricata dapat dilakukan dengan *command sudo nano /etc/suricata/suricata.yaml*,

B. Instalasi *IPTables*



Gambar 9. Instalasi *IPTables*

Gambar 9 merupakan langkah berikutnya dengan menginstall *IPTables*, dengan *command sudo apt-get install iptables iptables-persistent.*



Gambar 10. Konfigurasi *IPTables*

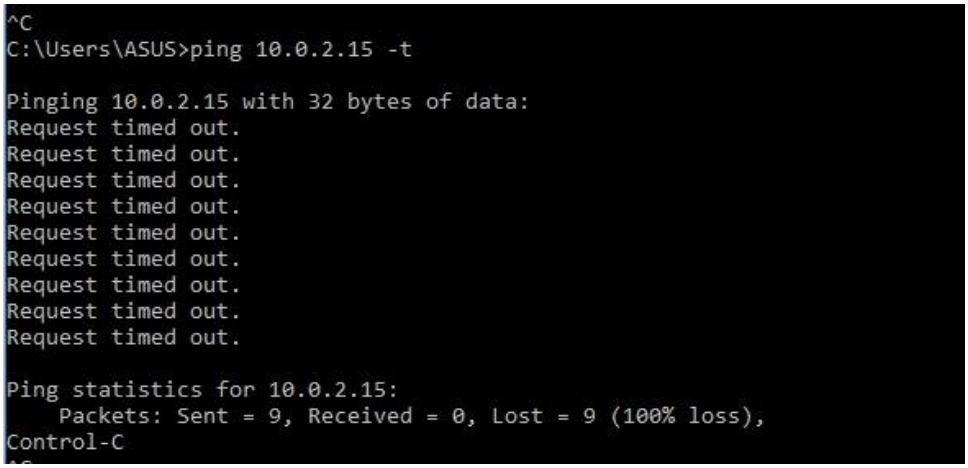
Gambar 10 merupakan tahapan konfigurasi rules yang ingin diterapkan di *IPTables* dengan *command sudo nano /etc/ufw/before.rules.*

C. Uji Coba

Pengujian Sistem Keamanan Jaringan merupakan proses untuk mengevaluasi efektivitas Sistem Keamanan Jaringan dalam mencegah, mendeteksi, dan merespons serangan. Tujuan pengujian ini merupakan untuk menentukan apakah sistem keamanan jaringan dapat mencegah serangan yang dicobakan. Penelitian ini melakukan pengujian untuk mengambil data dengan skenario serangan yang sudah dilakukan untukmengetahui kinerja dari Suricata dan *IPTables*. Pengambilan Data dilakukan oleh peneliti dengan melakukan pengamatan secara langsung dari log Suricata pada saat terjadi Serangan ICMP ping.

1. Skenario Pertama dan Hasil

   Dalam Skenario Pertama ini serangan yang dilakukan berupa satu laptop penyerang akan melakukan serangan dengan jenis serangan ICMP Ping yang dapat dilihat pada Gambar 11.



Gambar 11. Uji Coba

IPS memberikan *alert* serta melakukan drop paket yang dilakukan penyerang, untuk memastikan Suricata bekerja secara *real time*. Tampak waktu yang di tampilan di log Suricata sama dengan waktupenyerangan dan IPS telah berhasil mencegah serangan ICMP Ping.

Berdasarkan Gambar 12 yang telah dilakukan yaitu instalasi suricata dan *IPTables* telah berhasil dilakukan dan berjalan sesuai konfigurasi telah kita lakukan. Adapun sistem pencegahan serangan IPS dapat memberikan pemberitahuan serangan dan mencegah serangan terjadi. Pola serangan yang ada dalam aturanIPS menyebabkan serangan terdeteksi, sehingga perangkat IPS harus dikonfigurasi dengan benar dan sering mengembangkan aturan IPS. Hasil dari yang telah dilakukan percobaan dapat dilihat pada Gambar 12.

Gambar 12. Log Serangan

Kesimpulan

Berdasarkan perancangan dan pengujian diatas. Maka dapat dikatakan *Suricata* memiliki kemampuan untuk melakukan pemantauan lalu lintas jaringan yang lebih akurat dan memiliki kemampuan pemrosesan yang lebih baik. Pengujian sistem yang telah dibuat menggunakan *Suricata* dan *IPTables* dapat mendeteksi dan memblokir sebuah serangan yang dapat dilihat di Log file *Suricata*. *Suricata* dan *IPTables* dapat berfungsi dengan baik apabila pengaturan dan penerapan aturan yang dapat meningkatkan performa dan kemampuan deteksi serangan pada jaringan.

Daftar Pustaka

[1] K. F. I. Ilham, E. I. Alwi, and F. Fattah, "Penerapan dan Analisis Network Security Snort Menggunakan Intrusion Detection System pada Serangan UDP Flood," *INFORMAL: Informatics Journal*, vol. 8, no. 1, p. 94, Apr. 2023, doi: 10.19184/isj.v8i1.34003.

[2] E. Stephani, F. Nova, E. Asri, and N. Fitri, "Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server," 2020. [Online]. Available: http://jurnal-itsi.org

[3] S. Anraeni, E. I. Alwi, P. L. L. Belluano, A. W. M. Gaffar, R. Satra, and L. Syafie, "Pendampingan Pengelolaan Website UPT.PJP UMI (Pusat Jurnal dan Publikasi) untuk Peningkatan Pemeringkatan Webometrics," *Jurnal Abdidas*, vol. 5, no. 1, pp. 1–7, Feb. 2024, doi: 10.31004/abdidas.v5i1.870.

[4] R. G. Gunawan, Erik Suanda Handika, and Edi Ismanto, "Pendekatan Machine Learning Dengan Menggunakan Algoritma Xgboost (Extreme Gradient Boosting) Untuk Peningkatan Kinerja Klasifikasi Serangan Syn," *Jurnal CoSciTech (Computer Science and Information Technology)*, vol. 3, no. 3, pp. 453–463, Dec. 2022, doi: 10.37859/coscitech.v3i3.4356.

[5] M. Dehan Pratama, F. Nova, and D. Prayama, "Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos," 2022. [Online]. Available: http://jurnal-itsi.org

[6] F. Tanang Anugrah, S. Ikhwan, and J. Gusti A.G, "Implementasi Intrusion Prevention System (IPS) Menggunakan Suricata Untuk Serangan SQL Injection," *Techné : Jurnal Ilmiah Elektroteknika*, vol. 21, no. 2, pp. 199–210, Sep. 2022, doi: 10.31358/techne.v21i2.320.

[7] Z. A. Tyas, A. Firdonsyah, and W. Ramdhani, "Analisis Keamanan Jaringan dari Serangan DoS pada Sistem Inventaris Sanggar Tari Natya Lakshita menggunakan IDS," *INFORMAL: Informatics Journal*, vol. 7, no. 3, p. 258, Dec. 2022, doi: 10.19184/isj.v7i3.34943.

[8] O. Rivaldi and N. L. Marpaung, "Penerapan Sistem Keamanan Jaringan Menggunakan Intrusion Prevention System Berbasis Suricata," vol. 8, no. 1, p. 2023.

[9] H. Awal and A. P. Gusman, "Implementasi Intrusion Detection Prevention System Sebagai Sistem Keamanan Jaringan Komputer Kejaksaan Negeri Pariaman Menggunkan Snort Dan Iptables Berbasis Linux," Bulan Juni, Jun. 2023.

[10] E. Stephani, F. Nova, E. Asri, and N. Fitri, "Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server," Jun. 2020. [Online]. Available: http://jurnal-itsi.org

[11] R. Artikel, N. Christianto, and W. Sulistyo, "Model Pemantauan Keamanan Jaringan Melalui Aplikasi Telegram Dengan Snort," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 7, pp. 2443–2229, Dec. 2021, doi: 10.28932/jutisi.v7i1.4088.

[12] A. Muhaimi, I. P. Hariyadi, and A. Juliansyah, "Analisa Penerapan Intrusion Prevention System (IPS) Berbasis Snort Sebagai Pengaman Server Internet Yang Terintegrasi Dengan Telegram," *Jurnal Bumigora Information Technology (BITe)*, vol. 1, no. 2, pp. 167–176, Dec. 2019, doi: 10.30812/bite.v1i2.611.

[13] F. Wahyudi and L. T. Utomo, "Perancangan Security Network Intrusion Prevention System Pada PDTI Universitas Islam Raden Rahmat Malang," *Edumatic: Jurnal Pendidikan Informatika*, vol. 5, no. 1, pp. 60–69, Jun. 2021, doi: 10.29408/edumatic.v5i1.3278.

[14] F. Bagaskara Perdana, R. Munadi M.T., and I. Arif Indra, "Implementasi Sistem Keamanan Jaringan Menggunakan Suricata dan NTOPNG," *Implementasi Sistem Keamanan Jaringan Menggunakan Suricata dan NTOPNG*, pp. 4076–4083, Aug. 2019.

[15] O. Dwi Prasetyo, P. Hari Trisnawan, and A. Bhawiyuga, "Uji Kinerja Host-Based Intrution Detection System WAZUH terhadap Serangan Brute Force dan Dos," Jun. 2023. [Online]. Available: http://j-ptiik.ub.ac.id