JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika

[E-ISSN 2656-0321]
[Vol 19 No 1]
[Januari 2025]

SISTEM KEAMANAN JARINGAN KOMPUTER BERDASARKAN AHLI FORENSIK

Jalu Muhammad Abror[1], Robiatul Adawiah[2], Ahmad Tabrani[3]
[a,b,c 1]Informatika, Fakultas Sains, UIN Sultan Maulana Hasanuddin, Banten, Indonesia
jaluabrorr@gmail.com [1], robiatuladawiahayu@gmail.com [2] Ahmad.tabrani@uinbanten.ac.id [3]
* Jalu Muhammad Abror

ARTICLE INFO

Keywords
DDoS, Router, Safety system of Security Network

ABSTRACT

Network Forensics is like a computer detective. Forensics helps find out who is trying to damage a computer network by looking at clues and information from computer records. One way someone attacks a computer is called a Distributed Denial of Service (DDoS) attack. This occurs when multiple computers send too many requests to one computer, so that computer is so busy that it cannot help anyone else. At Ahmad Dahlan University in Yogyakarta, researchers are studying how to spot these attacks. They used special software called Winbox RouterOS to see things like who was attacking, how many data requests were sent, and when the attacks occurred. They also tested their computer security system with another program called LOIC to see how well it could protect against DDoS attack.

1. Pendahuluan

Host Intrusion Prevention System (HIPS) adalah alat keamanan lain yang dipasang di komputer individual. Alat ini mengawasi segala hal yang mencurigakan dan dapat menghentikan serangan dengan segera, seperti memutuskan sambungan dari jaringan atau memblokir akses ke berkas tertentu. Untuk menjaga keamanan jaringan komputer, kita memerlukan sistem yang dapat mendeteksi serangan ini, seperti Network-Based Intrusion Detection System (NIDS). NIDS mengawasi semua data yang masuk ke jaringan untuk menemukan aktivitas yang buruk. Alat ini sangat bagus dalam memeriksa lalu lintas antar komputer. Biasanya, NIDS ditempatkan di sekitar firewall dan VPN untuk melihat seberapa baik keamanan bekerja, Salah satu ancaman utama yang perlu dicatat adalah serangan DDoS (Distributed Denial of Service), yang memiliki potensi merusak dan mengganggu operasional sistem dan jaringan.[2]

Keamanan jaringan mencakup banyak hal, seperti perangkat fisik yang kita gunakan, yang sama pentingnya. Ini berarti kita perlu menjaga komputer, sistem penyimpanan, dan peralatan lainnya agar tidak seorang pun dapat mengaksesnya dengan mudah. Dengan pentingnya sebuah keamanan pada jaringan, maka hal ini menjadi aspek krusial dalam teknologi informasi saat ini[3]. Kita juga memerlukan sistem yang dapat mengawasi aktivitas yang buruk dan menghentikan serangan, seperti Intrusion Detection Systems (IDS) dan Intrusion Prevention Systems (IPS). Studi lain meneliti jenis serangan yang disebut "Ping of Death," di mana terlalu banyak paket data dikirim ke server, yang dapat menyebabkan masalah. Mereka menggunakan program bernama Snorby untuk merekam apa yang terjadi selama serangan ini sehingga mereka dapat menganalisisnya nanti.

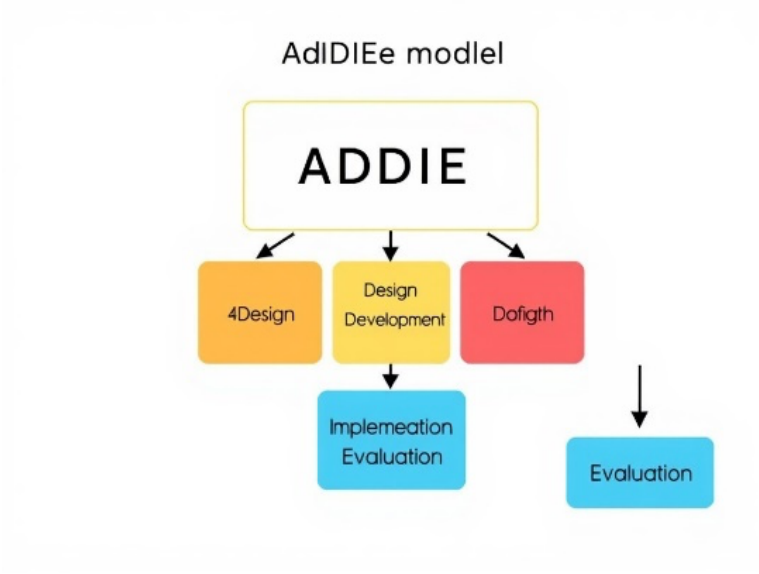
Studi ketiga menguji alat yang disebut OPNsense, yang membantu melindungi server web dengan memeriksa masalah secara real-time dan menyaring data yang buruk. Mereka menyiapkan jaringan virtual untuk melihat seberapa baik NIDS dan sistem lain yang disebut Host Intrusion Prevention System (HIPS) bekerja sama untuk menghentikan serangan. Mereka menguji seberapa baik sistem ini dapat mendeteksi dan

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 19 No 1]
[Januari 2025]

mencegah serangan "Ping of Death" dan melihat bagaimana serangan ini dapat memengaruhi komputer. Tujuannya adalah untuk melihat seberapa efektif sistem keamanan ini dalam menjaga keamanan komputer,.[1] Kegiatan merusak, mengganggu, mencuri data, dan segala hal yang merugikan pemilik sistem pada jaringan komputer adalah suatu tindak ilegal dan dapat dijatuhkan sangsi secara hukum di pengadilan[4]

Metodologi Penelitian

Tujuan utamanya adalah pemecahan masalah sehingga hasil penelitian dapat dimanfaatkan untuk kepentingan manusia baik secara individu atau kelompok, IDS merupakan security tools yang dapat digunakan untuk menghadapi aktivitas hackers[5], Langkah-langkah ini membantu mereka menciptakan sistem yang dapat mendeteksi saat sesuatu yang buruk terjadi pada komputer, baik di rumah maupun di tempat yang lebih besar. Mengikuti langkah-langkah ini dengan saksama membantu mereka memperoleh hasil terbaik dari penelitian mereka.[6]



Gambar 1. Alur Metode ADDIE

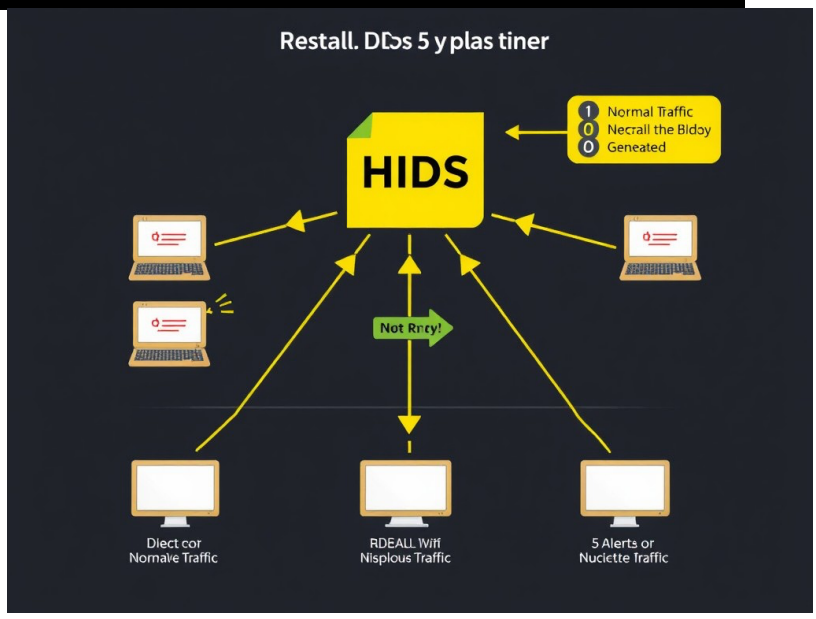
2.1. Analysis

Analisis seperti mengamati dengan saksama jalan yang ramai untuk mengetahui bagaimana lalu lintas bergerak saat ini. Analisis membantu kita memahami perbedaan antara apa yang kita harapkan terjadi dan apa yang sebenarnya terjadi pada jaringan. Ketika hal buruk terjadi, seperti serangan komputer, kita perlu menggunakan metode yang berbeda untuk memperbaiki masalah tersebut. Salah satu masalah yang sangat besar disebut serangan DDoS, yaitu ketika banyak komputer yang buruk mencoba membanjiri server, sehingga tidak dapat membantu orang yang membutuhkannya.

2.2. Design

Mereka juga akan melihat seberapa baik alat keamanan berbiaya rendah, yang disebut firewall buatan Mikrotik, dapat membantu menjaga keamanan jaringan. Dengan membandingkan waktu saat tidak ada serangan dengan waktu saat ada serangan DDoS, mereka berharap dapat melihat seberapa efektif firewall dalam menghentikan masalah ini. Secara sederhana, mereka ingin mempelajari cara menjaga komputer tetap aman dari serangan jahat!

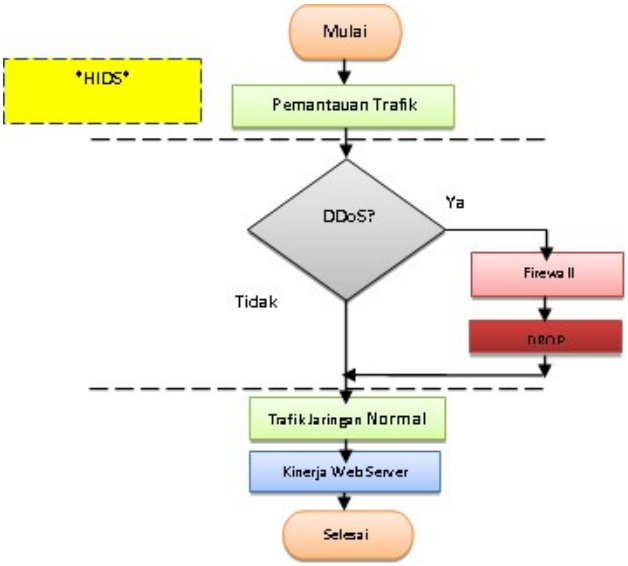
JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 19 No 1]
[Januari 2025]



Gambar 2. Metode HIDS Deteksi Serangan DdoS

2.3. Develop

Kami sedang menguji cara melindungi komputer dan situs web dari serangan jahat yang disebut DDoS, yang mencoba membanjiri komputer dan situs web dengan lalu lintas yang terlalu banyak. Untuk melakukannya, kami menggunakan tiga alat khusus bernama LOIC, Slowloris, dan Ping of Death. Kami mengawasi apakah serangan ini terjadi dengan menggunakan metode yang membantu kami mendeteksi masalah, yang melibatkan dua alat yang disebut Wireshark dan Snort. Kami mengaturnya di dua situs web: satu adalah www.srisuharti1212.sch.id dan yang lainnya adalah www.smknxxxx.sch.id. Jika semuanya berfungsi dengan baik dan tidak ada serangan, situs web www.srisuharti1212.sch.id dapat membantu orang yang mengunjunginya. Namun jika terjadi serangan, firewall akan memblokirnya untuk menjaga situs web tetap aman.

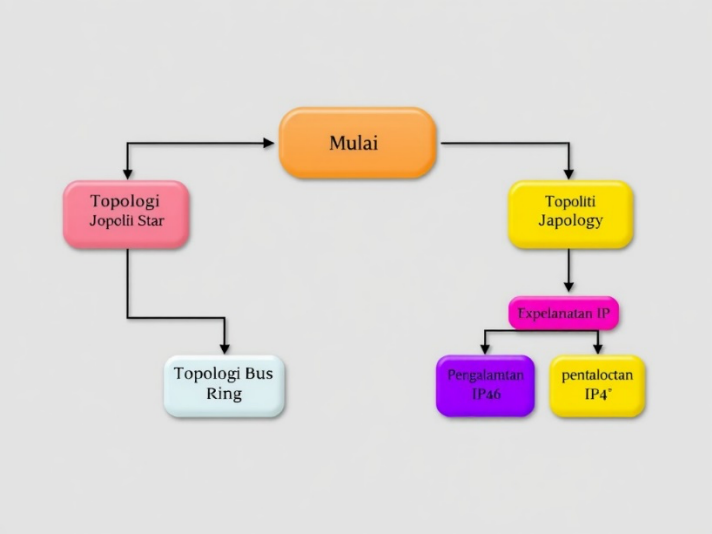


Gambar 3. Alur Metode HIDS pada DdoS

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 19 No 1]
[Januari 2025]

2.4. Implementasi

Beberapa pertempuran pura-pura (atau simulasi) menunjukkan bagaimana orang jahat dapat menggunakan alat khusus untuk mencoba menguasai komputer dan membuatnya berhenti bekerja. Alat-alat ini menggunakan berbagai cara untuk mengirim pesan melalui internet. Misalnya, satu alat yang disebut LOIC mengirim banyak pesan ke komputer menggunakan sesuatu yang disebut TCP/IP, sementara alat lain yang disebut Slowloris mencoba menjaga koneksi tetap terbuka untuk waktu yang lama menggunakan HTTP. Ada juga sesuatu yang disebut Ping of Death yang mengirim terlalu banyak pesan menggunakan ICMP. Semua ini terjadi berdasarkan pada bagaimana komputer disiapkan dan apa alamat IP-nya. Ketika kita berbicara tentang "implementasi," kita berbicara tentang menempatkan berbagai hal pada tempatnya, seperti menyiapkan kabel dan mencari tahu bagaimana komputer dapat terhubung ke internet. Setiap komputer memiliki nomor khusus yang disebut alamat IP yang membantu mengidentifikasinya, seperti alamat rumah tetapi untuk komputer. Dalam kasus ini, ada komputer yang mencoba menyerang komputer lain, dan keduanya memiliki alamat IP yang sama, yaitu 192.168.100.20.



Gambar 4. Topologi Jaringan dan pengalamatan IP

2.5. Evaluate

Mengevaluasi berarti memeriksa seberapa banyak data yang bergerak di internet, baik di jaringan rumah Anda maupun dalam skala yang lebih besar. Kami menggunakan alat khusus yang disebut Host-based Intrusion Detection System (HIDS) yang membantu kami melihat semua informasi kecil, yang disebut paket, dan seberapa banyak ruang yang mereka gunakan, yang dapat kami lihat menggunakan program yang disebut Wireshark. Setelah kami mengumpulkan informasi ini, kami membandingkannya untuk melihat paket mana yang normal dan mana yang mungkin buruk. Kami juga menggunakan persamaan matematika untuk membantu kami mengetahui seberapa akurat temuan kami.[2]

Hasil dan Pembahasan

Penelitian ini dilakukan pada waktu dan lokasi yang telah direncanakan. Sebelum memulai penelitian, orang yang melakukan penelitian berbicara dengan manajer lab komputer yang mengurus internet sekolah. Mereka ingin mengetahui beberapa masalah pada pengaturan internet sekolah. Karena tidak ada kesibukan selama bagian pengecekan masalah keamanan, hal itu memudahkan orang-orang dari luar sekolah untuk menggunakan internet tanpa izin.

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 19 No 1]
[Januari 2025]

Implementasi Hardware

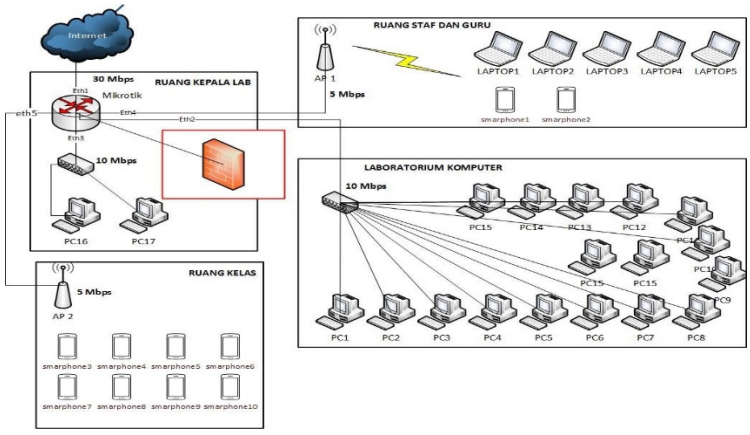
Setelah semuanya terhubung dengan benar, kita dapat mulai menguji seberapa baik jaringan komputer bekerja menggunakan metode khusus kita. Dalam jaringan kita, kita menggunakan sistem alamat khusus yang disebut alamat IP. Untuk pengaturan kita, kita menggunakan alamat 192.168.10.0/26. Mikrotik menggunakan alamat 192.168.10.1, dan laptop serta perangkat lain yang terhubung ke titik akses akan mendapatkan alamat dari 192.168.50.2 hingga 192.168.50.254. Semua alamat ini diberikan ke perangkat secara otomatis oleh Mikrotik.

Implementasi Perangkat Lunak

Pada bagian ini, penulis bersiap untuk menggunakan program khusus yang disebut LOIC untuk menguji keamanan jaringan komputer. Program ini digunakan untuk melihat apakah komputer yang terhubung ke jaringan sekolah aman. Jaringan menghubungkan komputer melalui switch dan juga melalui titik akses nirkabel. Tujuannya adalah untuk memastikan bahwa komputer di SMK Negeri 1 Palopo terlindungi dengan baik.

Topologi Jaringan

Setelah mencermati dengan seksama bagaimana hal-hal tersebut diatur, kami menemukan bahwa sebuah perangkat khusus bernama Mikrotik telah ditambahkan ke jaringan komputer sekolah. Perangkat ini berfungsi seperti perisai untuk melindungi jaringan sekolah dari hal-hal buruk yang dapat datang dari dalam maupun luar sekolah.



Gambar 5. Topologi Jaringan yang Diusulkan

Gambar Ini adalah gambar tentang bagaimana jaringan komputer disiapkan di SMK Negeri 1 Palopo. Jaringan ini menggunakan sesuatu yang disebut jaringan bintang, yang berarti semua ruangan terhubung ke lab komputer seperti titik-titik bintang. Mereka melakukan beberapa pengujian untuk melihat seberapa aman jaringan tersebut. Mereka memeriksa cara kerjanya sebelum dan sesudah mereka menambahkan sistem keamanan khusus yang disebut MikroTik. Hasilnya menunjukkan bahwa jaringan tersebut jauh lebih aman sekarang setelah mereka menerapkan sistem keamanan baru.

Dalam situasi ini, kami menggunakan program khusus yang disebut Winbox RouterOS untuk mengetahui apakah ada orang yang mencoba membuat masalah pada jaringan SMK Negeri 1 Palopo. Ketika kami melihat layar, kami melihat lampu hijau untuk orang yang memiliki izin untuk menggunakan jaringan dan lampu merah untuk mereka yang tidak. Untuk memeriksanya, kami mengklik tab "Interface" dan kemudian memilih "Interface ether2" di program Winbox. Ini memunculkan kotak khusus yang menunjukkan kepada kita apa yang terjadi. Selanjutnya, kami mencari informasi tersembunyi dan memeriksa beberapa detail menggunakan program Winbox. Kami dapat melihat berapa banyak data yang dikirim dan dalam urutan apa dengan memeriksa urutan paket dan menghitung paket data. Pada gambar yang kami lihat, kami dapat melihat jumlah paket yang dikirim dan dari alamat mana paket tersebut berasal menggunakan koneksi ether2.

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 19 No 1]
[Januari 2025]

Ketika seseorang mencoba menyelinap ke dalam sistem komputer tanpa izin, sebuah program khusus bernama Winbox RouterOS mendeteksinya. Di bagian program yang disebut menu Torch, program tersebut menunjukkan lokasi terjadinya aktivitas jahat, yaitu pada komputer dengan alamat 192.168.50.253, pada tanggal 8 Oktober 2021. Aktivitas jahat tersebut terjadi melalui sesuatu yang disebut port 80, yang terbuka dan memungkinkan hal-hal jahat masuk. Untuk menghentikan hal ini terjadi lagi, program tersebut memblokir alamat komputer jahat tersebut sehingga tidak dapat menyerang lagi. Oleh karena itu, serangan baru tidak dapat terjadi karena alamat 192.168.50.253 telah dihentikan. Program tersebut juga memastikan bahwa tidak ada lagi pesan jahat dari alamat tersebut yang dapat masuk. Selain itu, program tersebut memblokir alamat penting lainnya, seperti 192.168.10.1 dan 192.168.0.1, untuk menjaga semuanya tetap aman dan terlindungi.

Hasil Pengujian Jaringan

Kami melakukan banyak pengujian dan menemukan bahwa semuanya berjalan dengan baik! Pengujian menunjukkan bahwa klien tidak dapat terhubung ke Alamat IP yang telah kami blokir. Ini berarti bahwa penggunaan Mikrotik membantu menjaga jaringan tetap aman dari serangan, baik yang datang dari dalam maupun luar, baik melalui kabel maupun Wi-Fi. Semuanya berjalan dengan baik, dan Anda dapat melihat semua hasil pengujian pada tabel di bawah ini!

Tabel 2. Hasil pengujian implementasi keamanan jaringan

No	Pengujian	Hasil Pengujian		Keterangan
		Berhasil	Gagal	
1	Akses Mikrotik Lewat winbox		Ö	Tidak dapat akses mikrotik lewat Winbox
2	Akses modem lewat browser		Ö	Tidak dapat akses modem lewat Winbox
3	Serangan DDOS lewat Loic		Ö	Tidak dapat melakukan serangan DDOS lewat Loic

Kami melakukan serangkaian pengujian untuk melihat seberapa baik peralatan internet kami, seperti router dan modem Mikrotik, dapat melindungi dari orang jahat yang mencoba menyerang jaringan kami di SMK Negeri 1 Palopo. Kami akan menjalankan beberapa eksperimen menggunakan alat khusus yang disebut LOIC untuk memeriksa apakah kami dapat menghentikan serangan ini. Kami ingin memastikan bahwa jaringan kami aman, baik untuk orang yang menggunakan kabel (LAN) maupun untuk mereka yang menggunakan Wi-Fi. Untuk melakukannya, kami akan memblokir beberapa alamat khusus yang disebut alamat MAC dan alamat IP milik orang yang mencoba terhubung ke jaringan kami tanpa izin. Setelah memblokir alamat ini, kami akan memeriksa untuk melihat apakah pemblokiran berhasil dengan mencoba masuk ke router dan modem kami. [3]

3 Kesimpulan

Simpulan yang Dapat kita ambil bahwa Firewall next generation sebagai solusi utama karena firewall ini bisa dibilang lebih efektif dibandingkan firewall tradisional, dan juga firewall ini memiliki fitur tambahan yang mampu memantau dan mengontrol lalu lintas jarungan dengan baik, serta mencegah akses tidak sah yang dapat mengakibatkan kebocoran data. Selain firewall, penggunaan Intrusion Detection System

(IDS) juga ditekankan sebagai alat penting untuk mendeteksi dan merespons serangan jaringan secara real-time. IDS berfungsi untuk memantau aktivitas mencurigakan dan memberikan peringatan kepada administrator jika terdeteksi adanya pelanggaran aturan. penelitian ini menekankan perlunya pemantauan berkelanjutan terhadap sistem keamanan jaringan. Administrasi harus secara proaktif mengidentifikasi kelemahan dan melakukan tindakan perbaikan untuk mencegah potensi serangan di masa depan

.

Daftar Pustaka

[1] A. Satria and F. Ramadhani, "Analisis Keamanan Jaringan Komputer dengan Menggunakan Switch Port Security di Cisco Packet Tracer," *sudo J. Tek. Inform.*, vol. 2, no. 2, pp. 52–60, 2023.

[2] D. Suprihadi and I. Magfira, "Forensik Pada Jaringan Komputer Lokal Dengan Klasifikasi Svm Berbasis Framework Taara Universitas Kebangsaan Republik Indonesia," *J. Rev. Pendidik. dan Pengajaran*, vol. 7, no. 1, pp. 666–673, 2023.

[3] Z. Abdillah and P. Adytia, "Implementasi Intrusion Detection System (IDS) Suricata Untuk Mendeteksi Serangan DDoS Menggunakan Metode TAARA Pada Jaringan Internet di Pixel Esport Arena Samarinda Implementation of Suricata Intrusion Detection System (IDS) for Detecting DDoS Attacks Using the TAARA Method on the Internet Network at Pixel Esport Arena Samarinda," pp. 1–7.

[4] M. Aziz, R. Umar, and F. Ridho, "Implemetasi Jaringan Saraf Tiruan Untuk Mendeteksi Serangan DDoS Pada Forensik Jaringan," *J. Sist. Inf.*, vol. 5341, no. April, pp. 2579–5341, 2019.

[5] I. Ramadhan, "Monitoring Keamanan Jaringan Dengan Snort Ids Menggunakan Metode Forensic Jaringan (Studi Kasus: Cv.Triem Gunung Mas Sejahtera)," *J. Ilm. MIKA AMIK Al Muslim*, vol. 3, no. 1, pp. 13–18, 2019.

[6] T. Widodo and A. S. Aji, "Pemanfaatan Network Forensic Investigation Framework untuk Mengidentifikasi Serangan Jaringan Melalui Intrusion Detection System (IDS)," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 7, no. 1, pp. 46–55, 2022.