**Analisis Keamanan Transaksi E-Commerce Menggunakan *Intrusion Detection System* (IDS) Berbasis Snort**

**Tri Lestari1, Imam Riadi2, Rusydi Umar3**

1Pascasarjana, 2Program Studi Magister Tekik Informatika, 3Universitas Ahmad Dahlan Jl. Prof. Dr. Soepomo, Janturan, Umbulharjo, Yogyakarta 1tri1907048008@webmail.uad.ac.id, 2imam.riadi@mti.uad.ac.id,3 rusydi@mti.uad.ac.id

## Abstract

*The digital age is a sign of the progress of the internet that has made everything easy and fast. Tix Id is one of the many e-commerce applications that have developed in the digital age. This application requires that consumers are satisfied with promotions and services. Even though the Tix Id application already provides the best service, there are still some customers who feel unsatisfied using the application, a problem that often occurs is that there is often a one-sided ticket booking cancellation by Tix Id, the transaction process has been successfully carried out, besides that the consumer is also harmed by Tix's complaints My ID-consumer refunds remain reduced, and there are also often errors that contain seats not available. One way to optimize this application in the transaction process, namely by improving the information infrastructure, before improving the technology infrastructure, security analysis will be done first by using the intrusion detection system (IDS) [1], and this IDS is the process of finding active solutions suspicious on a system or network so that it can be identified the cause that occurs in the Tix Id application transaction process. The results obtained from this study are errors that often occur in Tix Id applications can not be identified whether it is an attack or not, but this research has resulted in the design of the need to optimize network security in Tix Id applications.*

***Keywords****: Security, Transactions, Tix Id, Intrusion Detection System (IDS), Snort*

## Abstrak

*Era digital merupakan tanda kemajuan internet yang menyebabkan semua menjadi mudah dan cepat. Tix Id adalah salah satu dari sekian banyak aplikasi e-commerce yang berkembang di era digital. Aplikasi ini berusaha agar konsumen merasa puas dengan promosi dan pelayanan. Meskipun aplikasi Tix Id sudah berusaha memberikan pelayanan terbaik namun masih ada beberapa konsumen yang merasa kurang puas menggunakan aplikasi tersebut, masalah yang sering terjadi adalah sering terjadi pembatalan pemesanan tiket sepihak oleh Tix Id padahal proses transaksi sudah berhasil dilakukan, selain itu konsumen juga merasa dirugikan ketika pihak Tix Id me-refund konsumen namun saldo konsumen tetap berkurang, dan juga sering terjadi error yang berisi pesan kursi tidak tersedia. Salah satu cara untuk mengoptimasi aplikasi tersebut kususnya dalam proses transaksi, yaitu dengan memperbaiki infrastruktur teknologi informasi, sebelum diperbaiki infrastruktur teknologinya, akan dilakukan terlebih dahulu analisis keamanan dengan menggunakan metode intrusion detection system (IDS) [1], dimana IDS ini merupakan proses untuk mendeteksi aktivias mencurigakan pada sebuah sistem atau jaringan sehingga dapat diketahui penyebab kesalahan yang terjadi pada proses transaksi aplikasi Tix Id. Hasil yang diperoleh dari penelitian ini adalah kesalahan yang sering terjadi pada aplikasi Tix Id belum dapat teridentifikasi apakah merupakan serangan atau bukan, namun penelitian ini telah menghasilkan rancangan kebutuhan untuk mengoptimalisasi keamanan jaringan pada aplikasi Tix Id.*

**Kata Kunci***: Keamanan, Transaksi, Tix Id, Intrusion Detection System (IDS), Snort*

## Pendahuluan

Era digital merupakan masa dimana manusia telah memahami teknologi dan semuanya serba terkoneksi seperti saat ini. Era digital juga merupakan salah satu tanda kemajuan internet yang menyebabkan semuanya menjadi mudah dan cepat. Tix Id merupakan salah satu dari sekian banyak aplikasi yang berkembang di era digital, Tix Id merupakan aplikasi partner resmi Cinema 21 dan Dana dalam pembelian tiket bioskop di Indonesia tanpa perlu repot mengantri, bebas memilih kursi dimana saja dan kapan saja. Aplikasi Tix Id dikembangkan oleh PT Nusantara Elang dan mulai aktif sejak 2018.

Ada beberapa aplikasi lain yang kegunaannya sama dengan Tix Id diantaranya ada go-tix, m-tix, dan traveloka. Namun pada kenyataannya, saat ini aplikasi Tix Id sedang naik daun dan ramai diperbincangkan banyak orang dikarenakan aplikasi ini banyak sekali menghadirkan promo. Aplikasi Tix Id berusaha agar konsumen merasa puas dengan promosi dan pelayanan.

Tix Id sudah berusaha memberikan pelayanan terbaik namun masih ada beberapa konsumen yang merasa kurang puas menggunakan aplikasi tersebut, dilihat dari beberapa ulasan terkait aplikasi Tix Id diantaranya sering terjadi pembatalan pemesanan tiket sepihak oleh Tix Id padahal proses transaksi sudah berhasil dilakukan selain itu konsumen juga merasa dirugikan ketika pihak Tix Id me-refund konsumen namun saldo konsumen tetap berkurang, dan juga sering terjadi error yang berisi pesan kursi tidak tersedia.

Beberapa masalah yang ada pada aplikasi Tix Id ini terjadi pada proses transaksi. Ada salah satu cara untuk mengoptimasi aplikasi Tix kususnya dalam proses transaksi, yaitu dengan memperbaiki infrastruktur teknologi informasi. Namun sebelum diperbaiki infrastruktur teknologinya, alangkah lebih baik apabila dilakukan analisis keamanannya terlebih dahulu, dan analisis tersebut dapat dilakukan dengan menggunakan metode intrusion detection system (IDS), dimana IDS ini merupakan sebuah metode yang dapat digunakan untuk mendeteksi aktifitas mencurigakan pada sebuah sistem atau jaringan sehingga dapat diketahui penyebab kesalahan yang terjadi pada proses transaksi aplikasi Tix Id ini apakah mungkin ada percobaan intrusi (penyusupan) atau tidak. Intrusion IDS pada penelitian ini menggunakan tools Snort dimana Snort adalah software open source yang berguna untuk mendeteksi intruksi pada sistem, mampu menganalisa lalu lintas data secara real-time pada IP Address, Snort juga maampu mendeteksi serangan berdasarkan anomaly detection maupun misuse detection untuk menemukan segala ancaman serangan [1].

Langkah-langkah yang dilakukan dalam penelitian ini adalah sebagai berikut ini ; pertama dilakukan studi literatur dari masalah yang relevan dengan penelitian, kedua dilakukan deteksi penyusupan pada proses transaksi Tix Id menggunakan IDS berbasis Snort, kemudian merancang kebutuhan aplikasi yang diimplementasikan, disesuaikan dengan kebutuhan yang bertujuan untuk optimasi sistem yang dibangun dan untuk kemudahan proses pengembangan aplikasi Tix Id [2], terakhir adalah penutup yaitu berisi kesimpulan dari hasil dan pembahasan yang telah dilakukan dalam penelitian.

Tujuan dilakukannya penelitian ini adalah untuk mengoptimalisasi keamanan transaksi pada aplikasi Tix Id sehingga apabila penelitian ini berhasil dilakukan maka manfaat bagi instansi pendiri aplikasi Tix Id adalah mendapatkan rekomendasi perbaikan aplikasi kususnya pada proses transaksi agar dapat dilakukan perbaikan dan pengembangan, sehingga masalah-masalah yang sering terjadi pada aplikasi Tix Id dapat dikurangi. Selain itu, dengan adanya perbaikan dan pengembangan aplikasi Tix Id dapat memberikan pelayanan yang lebih optimal bagi konsumennya.

## Kajian Teori

**Kajian Peneliti Terdahulu**

Penelitian ini dilakukan dengan melakukan kajian beberapa peneliti terdahulu, diantaranya ;

Telah dilakukan penelitian terkait Implementasi Log dalam Forensik Router Terhadap Serangan Distributed Denial of Service (DDoS) yang menghasilkan terjadi peningkatan lalu lintas data yang menunjukkan bahwa telah terjadi serangan ddos melalui ICMP berdasarkan analisa log yang di lakukan. IDS dapat dimanfaatkan untuk mendeteksi, merekam lalu lintas data yang ada pada router kemudian di simpan pada log dengan format .pcap. Hasil Analisa dapat membantu administrator dan pihak terkait dalam menemukan bukti serangan untuk keperluan persidangan [17].

Telah dilakukan penelitian terkait Deteksi Serangan DDoS Menggunakan Neural Network dengan Fungsi Fixed Moving Average Window yang menghasilkan Pendekatan baru yang diusulkan dalam mendeteksi serangan DDoS dengan metode neural network dengan fungsi fixed moving average window (FMAW) menghasilkan prosentase ratarata pengenalan terhadap tiga kondisi jaringan (normal, slow DDoS, Dan DDoS) sebesar 90,52%. Prosentase pengenalan yang dihasilkan berada diatas 90%. Hal ini menunjukkan bahwa metode metode neural network dengan fungsi fixed moving average window (FMAW), mampu mengenali serangan DDoS dengan baik [3].

Telah dilakukan penelitian terkait Analisis Forensik Serangan Sql Injection Menggunakan Metode Statis Forensik yang menghasilkan pengamatan yang dilakukan dengan metode statis forensic Penyerang hanya melihat isi data belum mengubah database yang ada di website [4]. Telah dilakukan penelitian terkait Modelling And Design E-Commerce SMI Sector Using Zachman Framework yang menghasilkan analysis and design of the interface can be recommended for pembutan modeling and system design e-commerce field of domestic trade [5]. Telah dilakukan penelitian terkait Perancangan Sistem Remote Ip Table Dan Instrusion Detection System (Ids) dengan Snort Pada Jaringan Lan yang menghasilkan penerapan Intrusion Detection System (IDS) berhasil mendeteksi serangan melalui 5 (lima) tahapan, yaitu : konfigurasi snort, pembuatan rules snort, pembuatan syntax pemblokiran, konfigurasi gammu dan pembuatan sejulah scripts agar saling terintegrasi satu sama lain, sehingga menghasilkan alert berupa SMS dengan 4 (empat) jenis informasi, yaitu: waktu serangan, jenis serangan, IP tujuan, dan IP sumber [2].

## Tix Id

Tix Id Tix Id merupakan aplikasi partner resmi Cinema 21 dan Dana dalam pembelian tiket bioskop di Indonesia tanpa perlu repot mengantri, bebas memilih kursi dimana saja dan kapan saja. Aplikasi Tix Id dikembangkan oleh PT Nusantara Elang dan mulai aktif sejak maret 2018. Aplikasi ini bisa diunduh di playstore atau app store. Aplikasi ini bukan aplikasi berbayar sehingga pengguna dapat mengunduh aplikasi ini secara cuma- cuma. Tix id menawarkan banyak fitur yang dapat diakses dengan gampang selain pembelian tiket bioskop, salah satunya yaitu fitur dana.

Dana merupakan dompet digital indonesia yang maksudnya adalah tempat penyimpanan uang digital yang nantinya akan digunakan untuk pembayaran tiket bioskop, dengan hadirnya dana pengguna dimudahkan untuk langsung melakukan pembayaran secara online dengan menggunakan saldo yang telah ada atau telah diisi oleh pengguna dana. Ada juga aplikasi lain yang kegunaan nya hampir sama dengan Tix id yaitu ada go-tix, m-tix, traveloka, namun pada kenyataannya aplikasi Tix id sedang naik daun dan ramai diperbincangkan banyak orang dikarenakan Tix id adalah aplikasi yang banyak sekali menghadirkan promo, diantara nya adalah :

Promo beli 1 gratis 1 di setiap hari rabu

Promo beli 1 gratis 1 film tertentu dengan jangka waktu tertentu Mendapatkan voucher sebesar 25.000 untuk pengguna baru Tix id

Mendapatkan voucher sebesar 25.000 untuk pengguna baru Tix id yang pada saat medaftar memakai kode undangan dari teman.

 Mendapatkan voucher senilai 25.000 ketika kita mengundang teman dan teman tersebut menggunakan kode undangan dari kita.

Diskon 50% pada jangka waktu tertentu

Saat ini aplikasi Tix Id sudah diunduh lebih dari 5.000.000 pengguna smartphone di Indonesia, hal inilah yang menyebabkan Tix id sedang ramai diperbincangkan oleh banyak orang saat ini dan juga aplikasi Tix id menempati nomor 1 teratas aplikasi layanan hiburan di playstore . Langkah-langkah penggunaan Tix Id adalah sebagai berikut ini;

Pertama unduh aplikasi Tix id di playstore ataupun app store, Kemudian masuk ke konten aplikasi,

Klik profil dan daftar untuk mendapatkan akun baru,

Setelah daftar, kembali lagi ke halaman profil aktifkan dana dan ikutkan petunjuknya

Jika ingin langsung memesan tiket bioskop, masuk ke beranda pilih lokasi bioskop yang diinginkan, Pilih film yang akan ditonton,

Pilih kursi yang anda inginkan untuk duduk,

Setelah semua nya dipilih, tekan ringkasan order dan lanjutkan ke pembayaran, Jika memiliki voucher nanti akan otomatis terpotong jumlah pembayaran nya.

Jika belum memiliki saldo, lakukan top up dana dan bisa dilihat di profil cara top up sesuai jenis bank, Lakukan pembayaran dan jika sudah, anda akan mendapatkan pemberitahuan bahwa pembayaran berhasil di aplikasi maupun melalui SMS,

 Untuk cetak tiket di bioskop, lakukan scan barcode atau masukkan kode nonton serta nomor telfon di setiap monitor khusus yang ada di setiap bioskop XXI [6].

Langkah-langkah penggunaan aplikasi Tix Id dapat dilihat pada Gambar 1.



Gambar 1. Langkah penggunaan aplikasi Tix Id

***Intrusion Detection System* (IDS)**

IDS merupakan aplikasi software atau hardware yang digunakan untuk mendeteksi aktivitas yang mencurigakan dari sebuah sistem atau jaringan. IDS mampu menganalisis dan mendapatkan bukti dari percobaan penyusupan dengan melakukan pengamatan terhadap lalu lintas yang masuk dan keluar dari sebuah sistem atau jaringan. Ada dua cara kerja yang biasa digunnakan IDS untuk menganalisa sebuah paket sehingga dapat ditentukan apakah paket tersebut termasuk serangan atau bukan. Cara kerja tersebut adalah knowledge based dan behavior based[7][8][9]. Gambar 2 merupakan gambaran penerapan IDS secara umum.



Gambar 2. Penerapan IDS secara umum

Penyusupan dapat dikenali dengan cara menyadap paket data, kemudian paket data tersebut dibandingkan dengan aturan basis data yang ada pada IDS, apabila paket memiliki kesamaan maka paket tersebut dianggap sebagai serangan, cara ini disebut dengan *knowledge based*. Sedangkan penyusupan yang dikenali dengan cara mengamati kondisi aplikasi untuk menemukan kejanggalan yang membuat aplikasi berjalan tidak normal seperti penggunaan memori yang berlebihan secara terus-menerus atau bisa juga ditemukan koneksi pararel pada satu Ip, kondisi ini dapat dianggap sebagai kejanggalan yang kemudian dapat disimpulkan bahwa kejanggalan tersebut merupakan serangan [10][11][12], cara kerja ini dapat disebut dengan *behavior based*.

## Snort

Snort adalah IDS berbasis jaringan dengan menggunakan metode rule based yang digunakan untuk menganalisis data sesuai dengan jenis seranngan yang sudah diketahui [8][1]. Snort memiliki beberapa karakteristik diantaranya ;

Source code dan rules Snort berukuran 2256kb.

Snort telah diporting ke Linux, Windows, OSX, Solaris, dan BSD. Snort mampu mendeteksi serangan pada jaringan 100Mbps.

Snort dapat dikonfigurasi sesuai kebutuhan. Snort bersifat open source dan berlisensi GPL.

Komponen penyususn Snort diantaranya ;

Paket capture library (libcap) berfungsi untuk memisahkan paket data memalui ethernet card. Paket decoder berfungsi untuk mengambil data yang dikirim oleh layer sebelumnya.

Preprocessor yaitu analisis paket sebelum diproses oleh komponen berikutnya dengan cara menandai, mengelompokan atau menghentikan karena paket yang ditangkap tidak lengkap.

 Detection Engine yaitu proses pembandingan paket dengan rule yang ada atau sudah ditetapkan sebelumnya, rule berisi signature kategori serangan.

 Output nya berupa report dan alert dan variasi output yang dihasilkan yaitu teks ASCII, syslog, XML, binary, atau database.

Gambar 3 merupakan gambar Snort dan gambar 4 merupakan cara penerapan Snort.



Gambar 3. Snort



Gambar 4. Penerapan Snort

Snort memberi fasilitas kepada pengguna agar dapat membuat rule sendiri sesuai kebutuhan, namun Snort telah menyediakan banyak rule secara default sehingga tidak perlu dilakukan konfigurasi apapun. Berikut ini merupakan beberapa hal yang harus diperhatikan saat membuat *custom rule* Snort ;

Pass yaitu proses ketika Snort tidak memberikan aksi apapun terhadap paket.

Log yaitu proses Snort menulis paket secara penuh pada direktori yang sudah didefinisikan sejak awal. Alert yaitu notifikasi untuk memberitahukan kepada tim analisis bahwa ada aktivitas serangan.

Active yaitu proses pengiriman Alert sekaligus pengerjaan rule yang lain.

Dynamic yaitu opsi dalam kondisi diam dan akan aktif ketika rule yang bersangkutan telah aktif.

Snort memiliki kelebihan dan kekurangan, kelebihan dari Snort diantaranya [13] ; Merupakan IDS yang cukup matang karena memiliki dukungan komunitas yang kuat Kemungkinan mendeteksi serangan tergantung dari kelengkapan basis data

Kekurangan Snort diantaranya [13] ;

 Masih menggunakan *singletrack* menyebabkan performa tidak bertambah secara signifikan meskipun jumlah *core processor* bertambah.

 Belum bisa mendeteksi *zero day attack.*

## Metodologi Penelitian

Agar penelitian berjalan sesuai harapan maka pada bagian ini akan dijelaskan alur dan proses yang akan dilakukan. Berikut ini merupakan gambaran metedologi penelitian yang berupa flowchart [14], metedologi penelitian yang akan dilakukan dapat dilihat pada gambar 5.



Gambar 5. *Flowchart* metedologi penelitian

Pertama studi literatur merupakan proses yang dilakukan agar peneliti lebih memahami konteks yang akan diteliti, memahami permasalahan yang ada dan mampu menemukan solusi. Kemudian dilakukan analisis kebutuhan, yaitu peneliti menganalisis apa saja yang dibutuhkan agar penelitian dapat berjalan dengan lancar, termasuk juga menganalisis peralatan yang dapat menunjang keberhasilan penelitian. Selanjutnya adalah deteksi serangan yang mungkin terjadi pada aplikasi Tix Id, tujuannya adalah untuk mengetahui apakah beberapa masalah yang terjadi pada Tix Id merupakan serangan dari peretas atau bukan. Setelah deteksi serangan selesai maka dilanjutkan dengan merancang kebutuhan sistem, rancangan kebutuhan sistem ini dilakukan untuk memberikan solusi kepada pihak Tix id apabila memang ditemukan serangan, dengan adanya rancangan kebutuhan sistem ini nantinya dapat membantu jika Tix Id jika akan meningkatkan teknik pengamanannya dari serangan peretas.

## Hasil dan Pembahasan

Langkah pertama adalah studi literatur, pada proses ini sudah dilakukan studi literatur dengan cara mengumpulkan sebanyak 15 jurnal bahkan lebih terkait penerapan IDS, kemudian dipelajari dan dibandingkan metode mana yang sesuai dengan kebutuhan, dan akhirnya pada penelitian ini memilih IDS berbasis Snort untuk membantu menyelesaikan analisis keamanan yang dilakukan pada proses transaksi aplikasi Tix Id.

Langkah selanjutnya yaitu melakukan deteksi serangan yang mungkin terjadi pada aplikasi Tix Id [2], rancangan untuk mendeteksi serangan dapat dilihat pada Gambar 6.



Gambar 6. Diagram untuk mendeteksi serangan

Gambar 6 merupakan alur gambar sistem pendeteksi serangan dengan pembuatan IDS dan Remot Iptables serta pelaksanaan pencegahan filtering firewall yang digunakan untuk memantau jaringan sehingga dapat membantu administrator dalam mendeteksi dan menanggulangi serangan secara lebih cepat dan jaringan dapat beroperasi kembali secara optimal. IDS melakukan pendeteksian serangan berdasarkan rules yang ditentukan, sedangkan Remote Iptables melakukan pencegahan dengan cara pemutusan terhadap serangan tersebut .

Langkah selanjutnya adalah membuat rancangan kebutuhan aplikasi Tix Id dalam hal ini adalah perancangan penerapan IDS. Rancangan penerapan IDS pada aplikasi Tix Id dapat dilihat pada Gambar 7.



Gambar 7. Rancangan IDS pada aplikasi Tix Id

Rancangan kebutuhan sistem yang diimplementasikan, disesuaikan dengan kebutuhan yang bertujuan untuk optimasi sistem yang dibangun dan untuk kemudahan proses pengembangan sistem. IDS berbasis Snort meliputi perancangan perangkat keras (hardware) dan perangkat lunak (software) untuk keluaran (output) yang diinginkan [15]. IDS pada gambar tersebut bertugas untuk mengawasi trafik yang masuk dan keluar dari jaringan, kemudian IDS mengidentifikasi trafik yang mencurigakan atau membahayakan yang mungkin saja dapat melewati firewall atau bisa juga berasal dari dalam jaringan karena IDS tidak hanya mendeteksi serangan dari luar tetapi juga potensi serangan dari dalam jaringan.

IDS bekerja sebagai pendeteksi dan pemberi peringatan dini terhadap kondisi jaringan yang berpotensi merusak sistem jaringan, sedangkan firewall bekerja untuk mencari gangguan, apabila ditemukan gangguan maka firewall akan menghentikan gangguan tersebut sebelum masuk ke dalam sistem jaringan. Administrator Tix Id akan mendapatkan notifikasi apabila terjadi gangguan, setelah mendapat notifikasi administrator dapat memutuskan tindakan apa yang harus segera dilakukan agar gangguan dapat sesegera mungkin dicegah.

Validasi keamanan pada suatu sistem atau aplikasi dapat ditentukan dengan menganalisis sifat-sifat aplikasi, dimana aplikasi dapat dikatakan aman apabila aplikasi memenuhi kriteria aman. Kriteria aman dari suatu aplikasi dilihat dari sifatnya yaitu apakah aplikasi mempunyai sifat availability, confidentialiy, integrity data, control, dan audit. Apabila aplikasi tidak memenuhi kelima sifat tersebut maka aplikasi belum dapat dikatakan aman.

Aplikasi Tix Id belum memiliki integritas data yang maksimal, berdasarkan pengamatan yang dilakukan aplikasi Tix Id sering memberikan data yang masih kurang tepat, sebagai salah contoh terkadang kursi bioskop yang masih tersedia pada aplikasi namun setelah dipilih terdapat notifikasi “kursi tidak tersedia”, hal trsebut dapat membuat pengguna menjadi kurang nyaman.

## Kesimpulan

Berdasarkah hasil dan pembahasan yang sudah dilakukan maka dapat ditarik kesimpulan bahwa, analisis keamanan transaksi pada aplikasi Tix Id dapat dilakukan dengan penerapan IDS Snort yaitu dengan langkah- langkah sebagai berikut ini ; Studi literatur, deteksi serangan dengan penerapan IDS berbasis Snort, dan merancang penerapan IDS pada aplikasi Tix Id untuk pengembangan keamanan, dengan diterapkannya IDS berbasis Snort pada jaringan Tix Id ini maka dapat diketahui serangan apa yang mungkin terjadi pada aplikasi Tix Id, dengan begitu administrator dapat segera mengatasi masalah yang sering terjadi pada aplikasi Tix Id apabila memang kesalahannya berasal dari serangan peretas.

Aplikasi Tix Id dapat dikatakan aman apabila memenuhi kriteria aman yaitu memiliki sifat availability, confidentialiy, integrity data, control, dan audit, untuk sementara ini Aplikasi Tix Id belum bisa dikatakan aman

karena ada salah satu kriteria aman yang belum dimiliki aplikasi tix Id yaitu integritas data pada aplikasi Tix Id masih kurang maksimal.

Sekian penelitian ini disampaikan, apabila banyak kesalahan dalam pembuatan penelitian ini penulis mohon maaf yang sebesar-besarnya, dan juga peneliti sangat berharap agar mendapatkan komentar beserta saran yang nantinya dapat membuat penelitian ini menjadi lebih baik. Terimakasih.

## Daftar Pustaka (10pt, center, bold)

1. L. B. Becker, M. Gergeleit, S. Schemmer, and E. Nett, “Using a flexible real-time scheduling strategy in a distributed embedded application,” *IEEE Int. Conf. Emerg. Technol. Fact. Autom. ETFA*, vol. 2, no. January, pp. 652–657, 2003.
2. B. A. Prakosa, A. H. Hendrawan, and W. Apriana, “Perancangan Sistem Remote Ip Table Dan Instrusion Detection System (Ids) Dengan Snort Pada Jaringan Lan,” *Krea-Tif*, vol. 3, no. 2, p. 1, 2015.
3. A. W. Muhammad, I. Riadi, and S. Sunardi, “Deteksi Serangan DDoS Menggunakan Neural Network dengan Fungsi Fixed Moving Average Window,” *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 1, no. 3, p. 115, 2017.
4. I. Riadi, R. Umar, and W. Sukarno, “Analisis Forensik Serangan Sql Injection Menggunakan Metode statis Forensik,” *Pros. Interdiscip. Postgrad. Student Conf. 1st*, vol. I, no. I, pp. 102–103, 2016.
5. Y. Hendriana, “Modelling And Design E-Commerce SMI Sector Using Zachman Framework,” *Int. J. Comput. Sci. Inf. Secur.*, vol. 13, no. 8, pp. 9–14, 2015.
6. G. Umum *et al.*, “Bab 1 pendahuluan 1.1,” 2018.
7. Sutarti, P. Pancaro, Adi, and I. Saputra, Fembi, “Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal,” *J. PROSISKO*, vol. 5, no. 1, 2018.
8. E. Risyad, M. Data, and E. S. Pramukantoro, “Perbandingan Performa Intrusion Detection System ( IDS) Snort Dan Suricata Dalam Mendeteksi Serangan TCP SYN Flood,” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 9, pp. 2615–2624, 2018.
9. Ari, “Perancangan dan Implementasi Intrusion Detection System dengan Algoritma Data Mining Instance Based Learning Artikel Ilmiah Peneliti,” no. 672009307, p. 50381, 2014.
10. F. A. Masse, A. N. Hidayat, and Badrianto, “Penerapan Network Intrusion Detection System Menggunakan Snort Berbasis Database MySQL Pada Hotspot Kota,” *J. Elektron. Sist. Inf. Dan Komput.*, vol. 1, no. 2, pp. 1–16, 2015.
11. B. H. Izza, Khaerani. Lekso, “Implementasi Dan Analisa Hasil Data Mining Untuk Klasifikasi Serangan Pada Intrusion Detection (Ids) Dengan Algoritma C4.5,” *Techno.COM*, vol. 14, no. 3, pp. 181–188, 2015.
12. I. N. T. Wirawan and I. Eksistyanto, “Penerapan Naive Bayes Pada Intrusion Detection System Dengan Diskritisasi Variabel,” *JUTI J. Ilm. Teknol. Inf.*, vol. 13, no. 2, p. 182, 2015.
13. B. A. Pratomo and R. M. Ijtihadie, “Sistem Deteksi Intrusi Menggunakan N-Gram Dan Cosine Similarity,” *JUTI J. Ilm. Teknol. Inf.*, vol. 14, no. 1, p. 108, 2016.
14. A. Prasetyo, L. Affandi, and D. Arpandi, “Implementasi metode naive bayes untuk intrusion detection system (ids),” *J. Inform. Polinema*, vol. 4, pp. 280–284, 2018.
15. Y. Arta, “Implementasi Intrusion Detection System Pada Rule Based System Menggunakan Sniffer Mode Pada Jaringan Lokal,” *It J. Res. Dev.*, vol. 2, no. 1, p. 43, 2017.