ANALISIS KEAMANAN JARINGAN LAN DALAM MENGATASI ANCAMAN TERHADAP SITUS JUDI ONLINE : STUDI PADA PENYUSUPAN DAN PERLINDUNGAN DATA PENGGUNA

Harry Pribadi Fitrian, Ghinnia Nuraulia Zani, Tini Meilani,
Rizky Rifaldi Wahab, Muhammad Fathurrahman Abdillah
Informatika, Universitas Teknologi Digital
Jl. Raya Janti Karang Jambe No.143, Yogyakarta
harrypribadi@digitechuniversity.ac.id

ABSTRAK

Perkembangan dunia internet semakin meningkat yang membawa dampak positif dan negatif bagi masyarakat, salah satunya meningkatnya iklan situs perjudian online yang meresahkan bagi pengguna internet karena sering kali menyusup ke jaringan *Local Area Network* (LAN) untuk mencuri data atau melakukan aktivitas ilegal. Keamanan jaringan LAN kita menjadi hal yang penting untuk dilindungi. Tujuan dari penelitian adalah untuk menganalisis kerentanan jaringan LAN terhadap serangan situs judi online serta menyediakan solusi perlindungan untuk memitigasi ancaman tersebut. Penelitian ini menggunakan metode studi literatur yaitu dengan mengumpulkan data dan informasi dari jurnal dan artikel sebelumnya, menganalisis berbagai pendekatan seperti pemblokiran DNS, implementasi firewall, enkripsi protokol, dan penguatan keamanan jaringan nirkabel. Dengan mengetahui titik lemah jaringan LAN kita dapat lebih mengantisipasi dari serangan hacker judi online. Hasil penelitian menunjukan bahwa langkah-langkah ini efektif dalam meningkatkan keamanan LAN, tetapi keberhasilannya tergantung pada penerapan teknologi yang tepat, peningkatan kesadaran pengguna, serta harmonisasi regulasi.

Kata Kunci *: Keamanan LAN, perjudian online, kerentanan jaringan, pencegahan peretas, keamanan internet.*

1. PENDAHULUAN

Dalam era digital yang semakin maju, jaringan komputer, khususnya jaringan Local Area Network (LAN), memainkan peran penting dalam menunjang aktivitas bisnis, pendidikan, dan kehidupan sehari-hari. Keamanan jaringan LAN menjadi salah satu aspek yang harus diperhatikan dengan serius, mengingat potensi ancaman yang semakin kompleks. Salah satu ancaman yang signifikan adalah serangan dari situs judi online yang dapat memanfaatkan celah keamanan untuk menyebarkan malware, mencuri data, atau melakukan aktivitas ilegal lainnya.

Dengan meningkatnya pengguna internet, maka pasti kebocoran data pribadi warga negara kita sangatlah krusial. Situs judi online sering kali menjadi pintu masuk bagi ancaman keamanan karena mereka menggunakan berbagai teknik manipulasi, seperti phishing, malware injection, dan botnet, untuk menyerang jaringan yang kurang terlindungi. Ancaman terhadap keamanan informasi semakin kompleks dan beragam, mulai dari serangan siber hingga kebocoran data internal.

Keamanan sistem informasi merupakan fokus utama dalam kemajuan teknologi dan komunikasi. Perlindungan aset informasi organisasi dianggap penting untuk keberlangsungan bisnis, dan dibutuhkannya penerapan pendekatan yang sistematis untuk mencapai tujuan. Pendekatan ini dirancang untuk melindungi organisasi dari berbagai serangan yang mungkin dihadapinya. Untuk menyelesaikan masalah keamanan ini, diperlukan solusi yang mencakup seluruh komponen sistem informasi. Ini mencakup keamanan komunikasi dan transaksi di dalam organisasi serta perlindungan integritas, kerahasiaan, dan aksesibilitas data. Ada kebutuhan untuk menerapkan metode keamanan yang holistik yang melibatkan serangkaian tindakan yang menyeluruh dan berlapis-lapis selain melindungi satu aspek. Penting untuk memahami bahwa seiring dengan kemajuan teknologi, ancaman keamanan sistem informasi terus meningkat. Akibatnya, strategi yang digunakan harus dapat mengantisipasi perubahan ini dengan memasukkan strategi keamanan yang dapat mengidentifikasi, mencegah, dan menangani berbagai jenis ancaman. [1]

Dengan meningkatnya kesadaran akan pentingnya keamanan siber, Phishing merupakan ragam tindakan kejahatan yang membangun halaman situs website yang mana pelaku akan melakukan penyalinan sikap halaman situs web yang legal dan mendistribusikan url kepada seseorang yang sudah dijadikan sasaran dengan cara spam, teks, ataupun jejaring sosial seperti yang dipaparkan oleh Abdul Basil dan teman-temannya di dalam
jurnal nya. [2]

Penelitian ini diharapkan dapat memberikan wawasan tentang metode terbaik untuk melindungi jaringan LAN dari ancaman saat ini dan meminimalkan kemungkinan kebocoran data pengguna. [3]

2. TINJAUAN PUSTAKA

Perkembangan teknologi informasi dan komunikasi yang pesat telah membawa berbagai kemudahan, namun juga meningkatkan kompleksitas ancaman siber terhadap jaringan lokal (LAN). Penelitian-penelitian terkini menunjukkan perlunya pendekatan multi-faceted untuk melindungi jaringan LAN dari berbagai ancaman, mulai dari kerentanan teknis hingga perilaku pengguna yang rentan. Tinjauan pustaka ini akan membahas beberapa penelitian relevan yang menyoroti berbagai aspek keamanan jaringan LAN dan implikasinya.

Penelitian oleh Tahir menekankan pentingnya penerapan metode Infiltration Testing Execution Standard (PTES) dalam analisis kerentanan site. Metode ini menawarkan pendekatan terstruktur untuk mengidentifikasi dan mitigasi celah keamanan, yang krusial dalam melindungi infrastruktur online [1]. Sementara itu, Ladayya mengkaji ancaman-ancaman sosial rekayasa (phishing, smishing, vishing), menyoroti pentingnya edukasi dan peningkatan kesadaran pengguna sebagai lapisan pertahanan pertama. Penelitian ini menunjukkan bahwa teknologi semata tidak cukup, perilaku pengguna yang waspada sangat penting [2].

Peneliti lain juga menyoroti dampak ekonomi signifikan dari situs judi online dan menganjurkan penggunaan teknologi seperti pemblokiran DNS dan firewall untuk membatasi akses [4]. Ini menunjukkan bahwa pendekatan berbasis teknologi dapat efektif dalam mengurangi paparan terhadap konten berbahaya. Sejalan dengan itu, Hidayat meneliti dampak iklan judi online terhadap minat pengguna web, memperkuat argumen untuk pendekatan proaktif dalam memblokir konten tersebut [3]. Frangky juga menambahkan perspektif tata kelola keamanan informasi dengan menekankan pentingnya implementasi standar ISO/IEC 27001:2022 untuk melindungi aset advanced organisasi secara komprehensif [3].

Penelitian lain juga mengeksplorasi penggunaan Bound together Danger Administration (UTM) pada firewall. UTM mengintegrasikan berbagai fungsi keamanan seperti Interruption Detection/Prevention Framework (IDS/IPS), antivirus, dan web shifting dalam satu stage, menawarkan solusi yang efisien dan terintegrasi [6]. Sutiman menambahkan perspektif lain dengan meneliti efektivitas Firewall Harbour Security Switch dalam melindungi jaringan dari ancaman inner dan eksternal. Penelitian ini menunjukkan bahwa pemilihan perangkat keras yang tepat juga berperan penting dalam keamanan jaringan [8].

Penelitian oleh Yoga juga menyoroti pentingnya review keamanan sistem informasi secara berkala berdasarkan standar yang telah ditetapkan. Evaluasi reguler ini memastikan efektivitas kontrol keamanan yang telah diimplementasikan dan memungkinkan identifikasi serta mitigasi kerentanan yang mungkin muncul seiring waktu [17].

Untuk melindungi jaringan LAN, diperlukan pendekatan holistik yang menggabungkan berbagai pendekatan. Ini mencakup menerapkan teknologi keamanan canggih seperti UTM dan firewall, mematuhi standar keamanan informasi seperti ISO/IEC 27001:2022, melakukan analisis kerentanan secara berkala dengan metode seperti PTES, dan memberikan instruksi kepada pengguna untuk menjadi lebih waspada terhadap ancaman siber. Penting untuk diingat bahwa keamanan jaringan terdiri dari berbagai lapisan pertahanan yang saling melengkapi daripada satu solusi.

3. METODE PENELITIAN

Penelitian ini bertujuan untuk menganalisis ancaman jaringan LAN dari serangan hack situs judi online dan memberikan solusi untuk melindungi keamanan jaringan dari serangan cyber.

Adapun tahapan penelitian ini dilakukan sebagai berikut:

3.1. Analisis Ancaman

Mengidentifikasi ancaman umum pada jaringan LAN berdasarkan literatur, termasuk intrusi, serangan DDoS, dan kebocoran data. Analisis ini mencakup studi kasus, laporan insiden siber, dan statistik serangan untuk memahami pola ancaman yang ada.

3.2. Arsitektur Keamanan jaringan

Mengkaji pendekatan seperti pemblokiran DNS, firewall, dan sistem deteksi intrusi (IDS/IPS). Penelitian juga menyoroti penerapan sistem segmentasi jaringan untuk meminimalkan dampak dari potensi serangan. Segmentasi jaringan memungkinkan pemisahan sumber daya berdasarkan tingkat keamanan, sehingga serangan tidak dapat menyebar dengan mudah.

3.3. Implementasi Teknik Perlindungan

Mengevaluasi efektivitas teknologi seperti enkripsi data, protokol keamanan terbaru, dan penguatan pengaturan jaringan nirkabel. Simulasi serangan dilakukan untuk menguji ketahanan berbagai teknik perlindungan. Teknik enkripsi modern seperti AES-256 dan protokol seperti WPA3 diuji dalam simulasi untuk melihat sejauh mana mereka dapat mencegah akses tidak sah.

3.4. Pengujian Keamanan Berbasis Alat

Menggunakan perangkat lunak pengujian keamanan seperti Wireshark untuk memantau lalu lintas jaringan, serta Metasploit untuk mensimulasikan serangan pada lingkungan virtual. Langkah ini memberikan wawasan tentang efektivitas teknologi keamanan yang diimplementasikan.

3.5. Evaluasi Kebijakan dan Regulasi

Mengkaji relevansi regulasi seperti UU ITE dalam mendukung upaya keamanan jaringan. Analisis ini mencakup identifikasi celah regulasi dan

rekomendasi untuk peningkatan kebijakan keamanan. Selain itu, evaluasi terhadap inisiatif kerja sama internasional dilakukan untuk memahami bagaimana standar global dapat diadopsi secara lokal.

3.6. Peningkatan Kesadaran Pengguna:

Mengevaluasi metode edukasi dan pelatihan yang dapat meningkatkan kesadaran pengguna terhadap ancaman siber. Penelitian mengkaji efektivitas kampanye kesadaran melalui media sosial, webinar, dan pelatihan langsung. Pendekatan ini dirancang untuk membantu pengguna memahami risiko dan langkah-langkah mitigasi yang dapat diambil.

3.7. Pengumpulan Data Sekunder:

Data yang digunakan dalam penelitian ini diperoleh dari jurnal ilmiah, laporan industri, serta studi kasus yang relevan dengan topik. Data ini dianalisis menggunakan pendekatan kualitatif untuk mendapatkan gambaran mendalam tentang permasalahan keamanan jaringan.

3.8. Metode yang digunakan

Penelitian ini menggunakan metode Studi Literatur untuk menganalisis dan mengidentifikasi berbagai teknik perlindungan yang digunakan untuk melindungi jaringan LAN dan mencegah serangan cyber.

Tahapan penelitian yang berlapis ini dirancang untuk memberikan pandangan yang lebih menyeluruh dan komprehensif terhadap perlindungan jaringan LAN dari ancaman situs perjudian online.

4. HASIL DAN PEMBAHASAN

Penelitian ini memuat banyak hasil penting untuk dianalisis dalam hal peningkatan keamanan LAN, khususnya terhadap ancaman dari situs game online. Detailnya sebagai berikut

4.1. Pengaruh pemblokiran DNS

Keamanan jaringan LAN sangat dipengaruhi oleh penerapan berbagai teknologi dan pendekatan strategis, salah satu langkah efektifnya adalah pemblokiran DNS. Studi menunjukan bahwa pemblokiran DNS menggunakan Router OS v6.48.3 terbukti efektif mencegah akses ke hingga 10 situs web perjudian besar tanpa mengurangi kinerja jaringan secara signifikan [4]. Pendekatan ini sejalan dengan upaya pemerintah untuk meminimalkan dampak negatif negatif situs perjudian online terhadap penggunaan internet. Namun, penerapan pemblokiran DNS memerlukan analisis mendalam terkait kompatibilitas perangkat dan kondisi jaringan.

Cegah akses ke situs web tidak sah tanpa mengurangi kinerja jaringan.

Penelitian ini membahas berbagai praktik dan tantangan dalam melindungi jaringan lokal (LAN) dari ancaman situs perjudian online. Analisis terhadap literatur sebelumnya menjelaskan teknologi keamanan termasuk pemblokiran DNS, implementasi firewall, enkripsi protokol web, dan keamanan jaringan nirkabel.

Relevansi pemblokiran DNS semakin meningkat dalam melindungi jaringan lokal dari serangan yang berasal dari situs perjudian online, yang sering menjadi titik awal bagi distribusi malware, phishing, dan ancaman merugikan lainnya. Dengan memblokir akses ke situs-situs ini, administrator jaringan dapat mengurangi risiko infeksi malware, kebocoran data, dan eksposur terhadap ancaman keamanan lainnya, sekaligus memberikan perlindungan tambahan bagi pengguna yang secara tidak sengaja mengakses konten berbahaya melalui perangkat kerja. Sebagai bagian dari strategi keamanan yang lebih luas, pemblokiran DNS perlu diintegrasikan dengan langkah-langkah lain, seperti pendidikan pengguna dan pengawasan lalu lintas jaringan. Kampanye kesadaran yang mengedukasi pengguna tentang risiko situs perjudian online dapat memperkuat upaya teknis yang dilakukan oleh administrator jaringan. Pendekatan ini, yang menggabungkan teknologi, kebijakan, dan kesadaran pengguna, bertujuan menciptakan lingkungan digital yang lebih aman, di mana ancaman dapat dikelola secara proaktif.

4.2. Pentingnya firewall dalam melawan ancaman cyber di website.

Penerapan firewall berbasis teknologi seperti Cloudflare telah terbukti mencegah serangan berbahaya yang mengarah pada eksploitasi situs web. Dalam sebuah penelitian, 126 URL berbahaya berhasil diblokir selama 8 hari, menunjukkan peran firewall yang sangat efektif dalam mengurangi ancaman [6]. Firewall ini memainkan peranan penting dalam melindungi jaringan LAN dari aktivitas mencurigakan. Teknologi firewall tidak hanya mencegah ancaman eksternal tetapi juga mendeteksi aktivitas tidak sah di dalam jaringan lokal. Dalam studi lain, Firewall Port Security Switch berhasil meningkatkan perlindungan terhadap ancaman internal dan eksternal melalui pengaturan akses yang lebih ketat [8].

Relevansi firewall dalam infrastruktur jaringan LAN semakin nyata ketika dikaitkan dengan ancaman yang berasal dari situs perjudian online. Situs-situs ini sering kali menjadi pintu masuk bagi malware dan perangkat lunak berbahaya lainnya yang dirancang untuk mencuri data atau melakukan tindakan sabotase. Dalam studi lain, firewall terbukti efektif dalam mengidentifikasi pola akses mencurigakan yang terkait dengan aktivitas perjudian online, memungkinkan administrator jaringan untuk mengambil langkah-langkah pencegahan sebelum kerusakan lebih lanjut terjadi. Dengan fitur-fitur seperti analisis lalu lintas secara real-time dan pembaruan otomatis terhadap daftar ancaman yang diketahui, firewall modern mampu memberikan perlindungan yang adaptif dan tanggap terhadap ancaman yang terus berkembang.

Secara keseluruhan, peran firewall dalam melindungi jaringan LAN tidak dapat diremehkan. Sebagai komponen utama dari strategi keamanan yang komprehensif, firewall memberikan lapisan perlindungan yang kritis terhadap berbagai ancaman siber, baik yang berasal dari luar maupun dalam jaringan. Dengan terus berkembangnya teknologi firewall, termasuk integrasi dengan kecerdasan buatan untuk mendeteksi ancaman yang lebih canggih, peran ini diperkirakan akan semakin penting di masa mendatang. Hal ini menegaskan bahwa firewall bukan hanya alat teknis, tetapi juga bagian integral dari strategi pertahanan siber yang berkelanjutan.

Relevansi : Firewall dapat menjadi elemen penting dalam infrastruktur LAN untuk mendeteksi dan memblokir aktivitas mencurigakan terkait perjudian online.

4.3. Kerentanan Protokol Web

Penelitian keamanan siber menunjukkan bahwa protokol web yang tidak terlindungi secara optimal rentan terhadap serangan pelacakan, di mana informasi sensitif dapat terekspos dengan beralih dari HTTPS ke HTTP. Jenis serangan ini berpotensi mengekspos data sensitif para pengguna dari situs perjudian online. Oleh karena itu, enkripsi data serupa merupakan langkah penting untuk menjamin keamanan transmisi data di jaringan lokal. Studi ini juga menyoroti tantangan yang akan dihadapi oleh jaringan LAN dan nirkabel. Penelitian ini menunjukan bahwa jaringan nirkabel lebih rentan terhadap serangan dibandingkan dengan jaringan kabel. Untuk mengatasi ancaman ini, studi yang dilakukan Yoga merekomendasikan penggunaan protokol Transport Layer Security (TLS) yang lebih mutakhir. Penerapan TLS memungkinkan komunikasi data yang lebih aman dengan mencegah pengungkapan atau manipulasi data oleh pihak ketiga [17].

Serangan ini menyoroti pentingnya penerapan enkripsi data yang konsisten.

Relevansi : LAN harus memastikan bahwa semua komunikasi data dienkripsi untuk melindungi informasi sensitif dari potensi gangguan.

4.4. Keamanan LAN Nirkabel

Studi tentang keamanan Wi-Fi menunjukkan bahwa jaringan nirkabel secara inheren lebih rentan dibandingkan jaringan kabel. Praktik buruk seperti pengaturan default dan penggunaan enkripsi lama seperti WEP adalah kerentanan utama yang dieksploitasi oleh peretas [10]. Untuk mengatasi hal ini, protokol WPA 3 direkomendasikan sebagai standar enkripsi terkini. Selain itu, penghapusan pengaturan default perangkat jaringan seperti kata sandi bawaan, merupakan langkah sederhana tetapi krusial dalam meningkatkan keamanan jaringan.

Relevansi: Memastikan keamanan LAN nirkabel dengan memperbarui protokol enkripsi dan menghapus konfigurasi default dapat membantu melindungi jaringan dari serangan pengawasan atau intersepsi data.

Pembahasan keempat terhadap berbagai tantangan dan solusi dalam mengamankan jaringan lokal (LAN) dari ancaman keamanan, terutama pada jaringan tanpa kabel. Penelitian mengenai keamanan Wi-Fi menunjukan bahwa jaringan tanpa kabel secara alami lebih mudah diserang dibandingkan dengan jaringan berkabel. Kelemahan ini terutama diakibatkan oleh praktik yang kurang baik seperti pengaturan standar pada perangkat jaringan dan penggunaan protokol enkripsi usang seperti WEP, yang rentan terhadap serangan peretas.

Protokol enkripsi yang lebih canggih, seperti WPA3, telah direkomendasikan untuk menggantikan metode enkripsi lama yang kurang aman. WPA3 menyediakan fitur keamanan tambahan, termasuk perlindungan terhadap serangan brute force dan enkripsi yang lebih tangguh untuk menjaga integritas data dalam jaringan. Penelitian ini menunjukan bahwa penerapan WPA3 dapat secara signifikan menurunkan risiko serangan yang sering terjadi pada jaringan tanpa kabel. Di samping itu, penghapusan pengaturan standar, seperti kata sandi bawaan pada perangkat jaringan, merupakan tindakan sederhana tetapi krusial dalam meningkatkan keamanan. Kata sandi standar sering kali menjadi target serangan karena informasi ini biasanya tersedia untuk umum. Mengubah pengaturan standar menjadi konfigurasi yang lebih aman dapat mencegah akses yang tidak sah dan melindungi jaringan dari kemungkinan penyadapan atau pengawasan.

Relevansi dari temuan ini terletak pada pentingnya mengadopsi langkah-langkah perlindungan yang lebih mutakhir untuk jaringan LAN tanpa kabel. Memastikan pembaruan protokol enkripsi secara rutin dan menerapkan kebijakan keamanan seperti menggunakan kata sandi yang kuat dapat secara signifikan meningkatkan perlindungan terhadap serangan. Dengan pendekatan ini, jaringan tanpa kabel tidak hanya menjadi lebih aman tetapi juga mampu mendukung aktivitas pengguna tanpa mengorbankan privasi dan integritas data. Studi ini memberikan pemahaman bahwa peningkatan keamanan jaringan tanpa kabel memerlukan kombinasi teknologi mutakhir dan penerapan kebijakan yang tepat. Penerapan langkah-langkah tersebut diharapkan dapat menjadi solusi yang efektif untuk menghadapi ancaman terhadap jaringan LAN, termasuk yang berasal dari aktivitas situs perjudian online.

4.5. Unified Threat Management (UTM) Sebagai Solusi Keamanan Terpadu

Penelitian oleh Mulyana mengungkapkan bahwa penggunaan Unified Threat Management (UTM) sebagai solusi keamanan terpadu memberikan manfaat yang signifikan dalam menghadapi ancaman siber yang kompleks [9]. Dengan mengintegrasi berbagai fungsi keamanan seperti IDS/IPS, antivirus, dan pemfilteran web dalam satu platform. UTM memungkinkan pengelolaan yang lebih efisien dan terpusat. Dalam konteks LAN, teknologi ini dapat

menjadi pilar utama dalam meningkatkan keamanan jaringan. Studi oleh Tahir juga menekankan pentingnya audit keamanan reguler menggunakan metode seperti PTES. Pendekatan ini memastikan bahwa kerentanan baru dapat diidentifikasi dan mitigasi segera dilakukan [1]. Hal ini relevan dengan jaringan LAN yang sering menjadi target serangan siber karena konektivitas yang tinggi dan data sensitif yang dikelola.

Secara keseluruhan, Penelitian ini menyoroti betapa pentingnya mengambil pendekatan keamanan jaringan yang komprehensif dan berlapis untuk mengatasi ancaman jaringan area lokal (LAN). Menerapkan tindakan seperti melakukan pemblokiran DNS, firewall, enkripsi data, dan keamanan jaringan nirkabel tingkat lanjut dapat melindungi LAN anda dari serangan situs judi online. Namun, keberhasilan penerapan teknologi ini bergantung pada faktor lain, termasuk harmonisasi hukum, peningkatan teknologi keamanan, dan kesadaran pengguna terhadap keamanan siber saat penggunaan internet.

5. KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa pendekatan seperti pemblokiran DNS, firewall, enkripsi data, dan keamanan jaringan nirkabel tingkat lanjut efektif dalam melindungi jaringan LAN dari ancaman situs perjudian online. Langkah-langkah ini memberikan perlindungan yang komprehensif terhadap berbagai jenis ancaman siber yang memanfaatkan celah keamanan jaringan. Namun, keberhasilan implementasi teknologi ini tidak hanya bergantung pada aspek teknis, tetapi juga memerlukan dukungan regulasi yang kuat, kolaborasi internasional, dan peningkatan kesadaran pengguna. Dengan pendekatan yang terintegrasi, kita dapat memitigasi risiko secara signifikan, menciptakan ekosistem jaringan yang lebih aman dan andal untuk mendukung aktivitas bisnis dan operasional. Penelitian lebih lanjut diperlukan untuk mengevaluasi efektivitas pemblokiran DNS di berbagai jenis perangkat dan lingkungan jaringan. Selain itu, kajian mendalam terhadap penerapan regulasi seperti UU ITE dan penguatan kerja sama internasional juga perlu dilakukan untuk mendukung keamanan jaringan secara menyeluruh. Upaya seperti pengembangan teknologi keamanan yang lebih canggih, penerapan kebijakan yang adaptif, dan edukasi berkelanjutan bagi pengguna menjadi elemen kunci dalam menciptakan sistem yang tangguh terhadap ancaman siber.

DAFTAR PUSTAKA

[1] R. N. F. D. W. P. I. R. M. Muhlis Tahir1, "Analisis Kerentanan Keamanan Website Menggunakan Metode PTES," *NUANSA INFORMATIKA* , vol. Volume 18, no. 2, pp. 145-153, 2024

[2] D. P. M. S. R. H. N. W. A. Ulfa Ladayya*1, "Kesadaran Keamanan Informasi atas Phising, Smishing, dan Vishing," *NUANSA INFORMATIKA* , vol. 18, no. 2, pp. 109-119, 2024

[3] R. S. Frangky, "Penerapan ISO/IEC 27001:2022 dalam Tata Kelola," *NUANSA INFORMATIKA* , vol. 18, no. 2, pp. 46-54, 2024

[4] H. Asyidiqi, "The State and Online Gambling: The Economic Impact of Online Gambling -A Case Study of Indonesia," *Globalization and International Relations,* vol. 1, no. 1, pp. 13-27, 2024

[5] R. A. D. M. R. M Bayu Wibawa, "MANAGEMENT INFORMATION SYSTEM FOR STANDARD OPERATING," *Journal of Informatics and Computer Science,* vol. 10, no. 2, pp. 63-68, 2024

[6] F. P. Rifky Kurniawan, "Implementasi Metode IPS (Intrusion Prevention System) dan IDS (Intrusion Detection System) untuk Meningkatkan Keamanan Jaringan," *Jurnal SENTINEL, STMIK Indo Daya Suvan,* vol. 2, no. 2, pp. 231-242, 2020

A. Zein, "Analisa Penyerangan untuk Cyber Security Social Engineering," *Jurnal Informatika Universitas Pamulang,* vol. 8, no. 4, pp. 642-648, 2023

[7] G. Sutiman Sutiman, "FIREWALL PORT SECURITY SWITCH UNTUK KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN CISCO ROUTER 1600S PADA PT. TIRTA KENCANA TATA WARNA SUKABUMI," *Conten Computer and Network Technology,* vol. 1, no. 1, pp. 13-22, 2021

[8] F. A. N. H. A. Z. Dadang Iskandar Mulyana, "Network Security Optimization Against Online Gambling and Pornography," *MALCOM: Indonesian Journal of Machine Learning and Computer Science* , vol. 4, no. 2, pp. 647-655, 2024

[9] T. S. &. S. H. M. Yundha Kurniawan, "Law Enforcement by Polri Against The Performers Online," *ARBITER: Jurnal Ilmiah Magister Hukum,* vol. IV, no. 1, pp. 28-44, 2022

[10] D. S. N. S. U. Wahyu Hidayat, "PENGARUH TERPAAN IKLAN JUDI ONLINE DAN INTENSITAS KOMUNIKASI DENGAN TEMAN SEBAYA TERHADAP MINAT BERMAIN JUDI ONLINE," *Undip Electro Jounal System (EUJS),* vol. 4, pp. 1-10, 2024

[11] N. ,. M. A. R. ,. T. A. ,. B. S. Endi Sjaiful Alim, "Monitoring dan Pencegahan Serangan Judi Online (Slot Gacor) pada," *Edumatic: Jurnal Pendidikan Informatika* , vol. 8, no. 1, pp. 75-83, 2024

[12] P. K. Manaf, "Pengaturan Tindak Kejahatan Judi Online di Internet dalam Perspektif," *Jurnal Hukum, Politik dan Ilmu Sosial* , vol. III, no. 4, pp. 301-309, 2024.

[13] P. Dora Sandova, "ANALISIS TRAFFIC PADA JARINGAN LAN," *JSAI : Journal Scientific and*

Applied Informatics , vol. 4, no. 3, pp. 329-337, 2021

[14] L. H. A. M. D. P. M. B. W. Rizka Albar 1, "ANALYSIS AND IMPLEMENTATION OF DOMAIN NAME SYSTEM (DNS)," *Journal of Informatics and Computer* , vol. 10, no. 1, pp. 2615-5346, 2024

[15] W. S. Yacob Hae, "Analisis Keamanan Jaringan Pada Web Dari Serangan," *Jurnal Teknik Informatika dan Sistem Informasi* , vol. 8, no. 4, pp. 2095-2105, 2021

[16] V. M. ,. N. D. M. Titan Parama Yoga, "Audit Keamanan Sistem Informasi Puskesmas Dengan Standar," *NUANSA INFORMATIKA* , vol. 18, no. 1, pp. 93-105, 2024