SEMINAR NASIONAL TEKNOKA

Vol. 9, 2024
ISSN No. 2502-8782

Analisis Keamanan Jaringan *Wifi* di MI Inwanul Huda

Arif Nur Iman, Muchammad Sholeh*

Universitas Muhammadiyah Prof. DR. HAMKA, Jl. Tanah Merdeka No. 6, Jakarta Timur, DKI Jakarta, Indonesia.
Email: mafiawhite25@gmail.com
Corresponding author: mafiawhite25@gmail.com

Abstrak

Penelitian ini bertujuan untuk menganalisis tingkat keamanan jaringan Wi-Fi di MI Inwanul Huda menggunakan metode kuantitatif, dengan pendekatan pengujian teknis jaringan dan survei pengguna. Hasil pengujian menunjukkan bahwa jaringan Wi-Fi di MI Inwanul Huda memiliki beberapa celah keamanan, antara lain penggunaan enkripsi WPA2 yang tidak optimal, lemahnya kata sandi yang digunakan, serta firmware perangkat yang belum diperbarui. Evaluasi konfigurasi perangkat juga menemukan bahwa firewall belum diaktifkan dengan baik, dan beberapa perangkat menggunakan pengaturan kata sandi bawaan yang rentan terhadap eksploitasi. Survei kepada 30 pengguna jaringan menunjukkan bahwa 70% pengguna tidak memahami langkah-langkah keamanan dasar jaringan, sementara 65% menggunakan kata sandi yang sama untuk berbagai layanan. Hal ini mengindikasikan rendahnya kesadaran pengguna terhadap keamanan jaringan. Rekomendasi yang diajukan mencakup peningkatan keamanan teknis melalui implementasi WPA3, pembaruan perangkat secara berkala, serta edukasi pengguna terkait praktik keamanan jaringan. Dengan langkah-langkah ini, diharapkan jaringan Wi-Fi di MI Inwanul Huda dapat mendukung pembelajaran berbasis teknologi dengan lebih aman.

***Kata Kunci**: Keamanan Jaringan, Wi-Fi, Metode Kuantitatif, MI Inwanul Huda*

Abstract

This study aims to analyze the level of Wi-Fi network security at MI Inwanul Huda using quantitative methods, with a technical network testing approach and user surveys. The test results show that the Wi-Fi network at MI Inwanul Huda has several security gaps, including the use of suboptimal WPA2 encryption, weak passwords used, and device firmware that has not been updated. The device configuration evaluation also found that the firewall had not been properly activated, and some devices used default password settings that were vulnerable to exploitation. A survey of 30 network users showed that 70% of users did not understand basic network security measures, while 65% used the same password for various services. This indicates low user awareness of network security. Recommendations proposed include improving technical security through the implementation of WPA3, regular device updates, and user education regarding network security practices. With these steps, it is hoped that the Wi-Fi network at MI Inwanul Huda can support technology-based learning more safely.

***Keywords**: Network Security, Wi-Fi, Quantitative Methods, MI Inwanul Huda*

1. PENDAHULUAN

Kemajuan teknologi informasi telah membawa perubahan besar dalam dunia pendidikan, terutama melalui penggunaan internet sebagai media pembelajaran. Salah satu fasilitas yang mendukung proses tersebut adalah jaringan Wi-Fi, yang memberikan akses cepat dan mudah ke berbagai sumber belajar daring. Di lembaga pendidikan seperti MI Inwanul Huda, Wi-Fi menjadi salah satu infrastruktur penting yang digunakan untuk mendukung kegiatan pembelajaran berbasis teknologi [1].

Namun, kemudahan akses Wi-Fi juga diiringi dengan tantangan keamanan yang semakin kompleks. Serangan siber, seperti pencurian data, akses tidak sah, dan eksploitasi jaringan, dapat terjadi jika keamanan jaringan

tidak dikelola dengan baik. Berdasarkan pengamatan awal, beberapa perangkat jaringan di MI Inwanul Huda menggunakan pengaturan keamanan dasar seperti enkripsi WPA2 tanpa konfigurasi optimal, dan kata sandi Wi-Fi yang lemah. Hal ini meningkatkan risiko ancaman terhadap data pengguna dan kestabilan jaringan [2].

Selain itu, rendahnya pengetahuan pengguna tentang praktik keamanan jaringan memperburuk situasi. Sebagian besar pengguna tidak memahami pentingnya menjaga kerahasiaan kata sandi, memperbarui perangkat, atau menggunakan perangkat yang aman. Hal ini dapat membuka peluang bagi pihak yang tidak bertanggung jawab untuk mengakses jaringan secara ilegal.

Melalui penelitian ini, analisis dilakukan untuk mengidentifikasi tingkat keamanan jaringan Wi-Fi di MI Inwanul Huda, baik dari sisi teknis maupun perilaku pengguna. Temuan dari penelitian ini diharapkan dapat memberikan rekomendasi yang relevan untuk meningkatkan keamanan jaringan Wi-Fi di lingkungan sekolah, sehingga dapat mendukung pembelajaran berbasis teknologi secara lebih aman dan efektif [3].

Kesimpulan dari penelitian ini ditujukan untuk membantu madrasah meningkatkan keamanan jaringan, sehingga memungkinkan mereka menciptakan lingkungan belajar yang aman dan terlindungi dari segala ancaman digital.

2. DASAR TEORI

2.1 Keamanan Jaringan

Keamanan jaringan merupakan bagian penting dari manajemen teknologi informasi yang berupaya mengamankan arsitektur dan data jaringan dari serangan internal maupun eksternal. Keamanan jaringan mencakup berbagai langkah, kebijakan, dan proses teknologi yang bertujuan untuk memastikan kerahasiaan, integritas, dan ketersediaan informasi yang beredar di dalam jaringan. Penerapan keamanan jaringan di sekolah atau madrasah sangat penting untuk melindungi data siswa, guru, dan administrasi dari penggunaan yang tidak sah [4].

2.2 WIFI

WIFI (Wireless Fidelity) adalah teknologi nirkabel yang menghubungkan perangkat listrik ke internet tanpa menggunakan kabel. Jaringan WIFI memainkan peran penting dalam pendidikan dengan memungkinkan akses informasi yang cepat dan mudah. Jaringan WIFI menggunakan gelombang radio, sehingga lebih rentan terhadap berbagai ancaman dunia maya daripada jaringan konvensional. Oleh karena itu, keamanan jaringan WIFI harus ditangani dengan hati-hati untuk menghindari pencurian data, peretasan, dan akses yang tidak sah [5].

2.3 Protokol Keamaan WIFI

Jaringan nirkabel dilindungi menggunakan protokol keamanan Wi-Fi seperti WEP, WPA, dan WPA2. WPA2 (Wi-Fi Protected Access 2) merupakan protokol yang paling banyak digunakan saat ini karena dianggap lebih aman daripada pendahulunya. WPA2 menggunakan Advanced Encryption Standard (AES), yang lebih efektif dalam mengenkripsi data tetapi masih dapat rentan jika tidak dirawat dengan baik, seperti dengan menggunakan kata sandi yang lemah atau melakukan pembaruan sistem yang jarang. Protokol keamanan ini harus diterapkan dengan tepat di lingkungan pendidikan seperti madrasah untuk melindungi data dan jaringan dari ancaman eksternal [6].

2.4 Ancaman terhadap Keamanan Jaringan WIFI

Berikut merupakan berbagai jenis ancaman yang dapat mengganggu keamanan jaringan WIFI, antara lain:

1. Serangan Man-in-the-Middle (MitM), di mana penyerang mencegat komunikasi antara dua perangkat.
2. Serangan Denial of Service (DoS), yang bertujuan untuk membuat jaringan tidak dapat digunakan dengan menghabiskan sumber daya.
3. Serangan brute force, yang mencoba menebak kata sandi melalui berbagai kombinasi hingga menemukan yang tepat [7].

Ancaman-ancaman ini menjadi perhatian khusus di lingkungan pendidikan, karena banyaknya pengguna dengan tingkat kesadaran keamanan yang rendah, seperti siswa yang sering tidak memperhatikan pentingnya kata sandi yang kuat.

ISSN No. 2502-8782

2.5 Pengelolaan Keamanan Jaringan di Lingkungan Pendidikan

Manajemen keamanan jaringan di lembaga pendidikan memerlukan rencana komprehensif yang mencakup kebijakan keamanan, edukasi pengguna, dan penerapan teknologi mutakhir. Perguruan tinggi dan sekolah dasar/madrasah memerlukan solusi keamanan yang menggabungkan teknologi (firewall dan enkripsi) dan manajemen sumber daya manusia yang lebih baik. Salah satu bagian penting dari keamanan jaringan adalah kesadaran dan pelatihan pengguna tentang kemungkinan risiko dan cara mengatasinya [8].

3. METODOLOGI

Penelitian ini dilakukan untuk menganalisis keamanan jaringan WIFI di Madrasah Ibtidaiyah Inwanul Huda dengan fokus pada identifikasi kelemahan dan potensi ancaman terhadap jaringan tersebut. Metode yang digunakan akan disajikan secara detail sebagai berikut:

3.1 Alur Penelitian

Penelitian ini menggunakan metode kuantitatif untuk menganalisis tingkat keamanan jaringan Wi-Fi di MI Inwanul Huda. Pendekatan ini dipilih karena memungkinkan pengumpulan dan analisis data secara sistematis untuk mengidentifikasi kerentanan dan mengevaluasi efektivitas langkah-langkah keamanan yang telah diterapkan.

3.2 Desain Penelitian

Desain penelitian ini bersifat deskriptif, dengan fokus pada evaluasi kondisi jaringan Wi-Fi. Penelitian dilakukan melalui pengujian teknis jaringan, survei pengguna, dan analisis konfigurasi perangkat jaringan untuk memperoleh gambaran komprehensif terkait keamanan jaringan [9].

3.3 Popuulasi dan Sampel

Populasi dalam penelitian ini mencakup perangkat jaringan yang digunakan di MI Inwanul Huda serta pengguna jaringan Wi-Fi, termasuk guru, staf, dan siswa. Sampel penelitian diambil secara purposive, melibatkan:

1. 2 perangkat jaringan utama (router dan access point).
2. 30 pengguna jaringan Wi-Fi.

3.4 Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan meliputi:

1. Pengujian Penetrasi: Dilakukan untuk mengidentifikasi potensi celah keamanan pada jaringan Wi-Fi [10].
2. Kuesioner: Kuesioner diberikan kepada pengguna jaringan untuk mengukur persepsi mereka terhadap keamanan dan kebiasaan mereka dalam menggunakan Wi-Fi.
3. Analisis Konfigurasi: Evaluasi konfigurasi perangkat jaringan, seperti pengaturan enkripsi, firewall, dan manajemen kata sandi.

3.5 Teknik Analisis Data

Data yang diperoleh dianalisis menggunakan langkah-langkah berikut:

1. Analisis Kuantitatif: Data survei diolah menggunakan statistik deskriptif untuk menggambarkan pola penggunaan dan persepsi pengguna terhadap keamanan jaringan.
2. Evaluasi Keamanan Teknis: Hasil pengujian penetrasi dan analisis konfigurasi perangkat diinterpretasikan untuk menilai tingkat kerentanan dan rekomendasi perbaikan.

3.6 Validitas dan Reliabilitas

Untuk memastikan validitas dan reliabilitas, penelitian ini menggunakan:

1. Validasi Instrumen: Uji coba kuesioner dilakukan sebelum digunakan untuk memastikan relevansi dan kejelasan pertanyaan.
2. Reliabilitas Data: Pengujian teknis dilakukan lebih dari satu kali untuk memastikan konsistensi hasil [11].

4. HASIL DAN PEMBAHASAN

4.1 Hasil Pengujian Keamanan Jaringan Wi-Fi

Pengujian penetrasi terhadap jaringan Wi-Fi di MI Inwanul Huda dilakukan dengan menggunakan beberapa alat dan teknik untuk mengidentifikasi potensi kerentanannya. Hasil pengujian menunjukkan bahwa jaringan Wi-Fi di MI Inwanul Huda memiliki beberapa celah keamanan yang perlu diperbaiki. Beberapa temuan utama dari pengujian ini adalah sebagai berikut:

ISSN No. 2502-8782

Tabel 1. Hasil Pengujian Keamanan Jaringan Wi-Fi

Temuan	Deskripsi	Tingkat Kerentanan
Enkripsi Lemah	Penggunaan enkripsi WPA2 pada sebagian besar perangkat, rentan terhadap serangan brute-force	Tinggi
Kata Sandi Lemah	Penggunaan kata sandi yang mudah ditebak dan tidak sesuai dengan standar keamanan yang baik	Tinggi
Perangkat Tidak Terupdate	Beberapa perangkat jaringan menggunakan firmware lama yang meningkatkan potensi eksploitasi	Menengah

Pembahasan :

1. Enkripsi yang Lemah: Sebagian besar perangkat di jaringan menggunakan enkripsi WPA2, yang meskipun aman, dapat rentan terhadap serangan brute-force dan dictionary attack jika kata sandi yang digunakan lemah.
2. Penggunaan Kata Sandi yang Lemah: Kata sandi yang digunakan untuk mengakses jaringan Wi-Fi ditemukan mengandung pola yang mudah ditebak dan tidak memenuhi standar keamanan yang baik.
3. Perangkat yang Tidak Terupdate: Beberapa perangkat jaringan, seperti router dan access point, menggunakan firmware yang tidak terupdate, yang meningkatkan risiko terhadap eksploitasi kerentanan yang telah diketahui.

4.2 Hasil Survei Pengguna

Survei yang dilakukan kepada 30 pengguna Wi-Fi di MI Inwanul Huda menunjukkan beberapa temuan terkait persepsi dan kebiasaan pengguna dalam menggunakan jaringan Wi-Fi.

Tabel 2. Survei Pengguna

Aspek	Temuan	Persentase (%)
Pengetahuan Keamanan Jaringan	Pengguna tidak mengetahui langkah-langkah keamanan dasar jaringan Wi-Fi	70%
Penggunaan Jaringan untuk Pembelajaran	Pengguna menggunakan Wi-Fi untuk kegiatan pembelajaran online	90%
Kebiasaan Penggunaan Kata Sandi	Pengguna menggunakan kata sandi yang sama untuk berbagai layanan	65%

Pembahasan :

1. Pengetahuan Keamanan Jaringan: Sebagian besar responden (70%) mengaku tidak mengetahui langkah-langkah keamanan dasar yang seharusnya diterapkan pada jaringan Wi-Fi, seperti penggunaan enkripsi yang kuat dan pengelolaan kata sandi yang baik.
2. Penggunaan Jaringan Wi-Fi untuk Kegiatan Pendidikan: 90% pengguna mengandalkan jaringan Wi-Fi untuk kegiatan pembelajaran online, namun hanya 30% yang mengetahui adanya kebijakan keamanan yang jelas terkait akses jaringan.
3. Kebiasaan Penggunaan Kata Sandi: Mayoritas pengguna (65%) menggunakan kata sandi yang sama untuk berbagai layanan, yang meningkatkan risiko keamanan jika kata sandi tersebut bocor atau terdeteksi oleh pihak yang tidak bertanggung jawab.

4.3 Evaluasi Konfigurasi Perangkat Jaringan

Evaluasi konfigurasi perangkat jaringan di MI Inwanul Huda menunjukkan beberapa kelemahan dalam pengaturan keamanan, antara lain:

Tabel 3. Evaluasi Konfigurasi Perangkat Jaringan

Aspek	Temuan	Kondisi
Pengaturan Enkripsi	Penggunaan WPA2, beberapa perangkat tidak terkonfigurasi dengan WPA2-AES, tidak ada WPA3	Lemah
Firewall dan Pengaturan Akses	Firewall tidak diaktifkan secara optimal, beberapa port tidak dibatasi dengan benar	Lemah
Manajemen Pengguna dan Kata Sandi	Pengelolaan kata sandi yang buruk, tidak ada kebijakan penggantian kata sandi secara berkala	Lemah

Pembahasan :

1. Pengaturan Enkripsi: Sebagian besar perangkat menggunakan WPA2, namun tidak semua router terkonfigurasi dengan WPA2-AES, yang lebih aman

ISSN No. 2502-8782

dibandingkan WPA2-TKIP. Penggunaan WPA3, yang menawarkan enkripsi lebih kuat, tidak ditemukan di perangkat yang diuji.

2. Firewall dan Pengaturan Akses: Firewall pada perangkat-perangkat jaringan tidak diaktifkan secara optimal, yang membuka potensi akses tidak sah ke jaringan. Beberapa port penting juga tidak dibatasi dengan benar, memungkinkan kemungkinan terjadinya eksploitasi oleh pihak luar.
3. Manajemen Pengguna dan Kata Sandi: Proses pengelolaan kata sandi untuk mengakses perangkat jaringan tidak menerapkan kebijakan penggantian kata sandi secara berkala, dan beberapa perangkat menggunakan kata sandi default yang dapat dengan mudah ditebak.

4.4 Hasil Uji Validitas dan Reliabilitas

Uji validitas dilakukan untuk memastikan setiap butir dalam kuesioner mengukur variabel yang dimaksud. Uji validitas dilakukan menggunakan korelasi Pearson Product Moment dengan bantuan perangkat lunak SPSS. Kriteria validitas adalah nilai r hitung harus lebih besar dari nilai r tabel (pada taraf signifikan 5% dan N = 30, r tabel = 0,361).

Tabel 4. Hasil Uji Validitas

No. Butir Pertanyaan	r hitung	r tabel	Keterangan
1. Saya merasa jaringan Wi-Fi di MI Inwanul Huda aman digunakan.	0,550	0,361	Valid
2. Saya mengetahui pentingnya menggunakan kata sandi yang kuat untuk mengakses Wi-Fi.	0,472	0,361	Valid
3. Jaringan Wi-Fi di MI Inwanul Huda memiliki perlindungan yang cukup untuk mencegah akses tidak sah.	0,620	0,361	Valid
4. Saya memahami risiko keamanan jika menggunakan jaringan Wi-Fi tanpa perlindungan yang memadai.	0,440	0,361	Valid
5. Pihak sekolah telah memberikan edukasi terkait keamanan jaringan Wi-Fi kepada pengguna.	0,590	0,361	Valid

Uji reliabilitas dilakukan untuk mengukur konsistensi instrumen dalam mengukur variabel. Uji reliabilitas menggunakan metode Cronbach's Alpha dengan kriteria:

1. Cronbach's Alpha ≥ 0,70: Reliabel
2. Cronbach's Alpha < 0,70: Tidak Reliabel

Tabel 5. Hasil Uji Reliabilitas

Variabel	Cronbach's Alpha	Keterangan
Persepsi Keamanan Jaringan	0,785	Reliabel

Hasil uji reliabilitas menunjukkan bahwa kuesioner memiliki nilai Cronbach's Alpha sebesar 0,785, yang berarti instrumen tersebut reliabel dan konsisten dalam mengukur persepsi keamanan jaringan.

4.5 Pembahasan Hasil Penelitian

Berdasarkan hasil pengujian dan survei, dapat disimpulkan bahwa keamanan jaringan Wi-Fi di MI Inwanul Huda masih rentan terhadap beberapa potensi ancaman. Celah-celah yang ditemukan, seperti penggunaan enkripsi yang lemah dan pengelolaan kata sandi yang buruk, dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mengakses jaringan dan mengganggu kegiatan pembelajaran online. Beberapa faktor yang memengaruhi tingkat keamanan jaringan adalah kurangnya pengetahuan tentang praktik keamanan siber di kalangan pengguna, serta kurangnya pembaruan dan pengelolaan perangkat jaringan yang teratur. Oleh karena itu, perlu dilakukan langkah-langkah untuk meningkatkan konfigurasi perangkat jaringan.

Rekomendasi untuk meningkatkan keamanan jaringan Wi-Fi di MI Inwanul Huda antara lain:

1. Penerapan WPA3: Mengganti pengaturan enkripsi WPA2 dengan WPA3 untuk meningkatkan perlindungan terhadap serangan berbasis kata sandi.
2. Pendidikan Keamanan Siber: Menyelenggarakan pelatihan dan sosialisasi kepada pengguna mengenai pentingnya keamanan kata sandi dan penggunaan jaringan yang aman.
3. Pemutakhiran Firmware dan Pengelolaan Perangkat: Melakukan pembaruan firmware secara berkala dan memastikan bahwa semua perangkat jaringan

ISSN No. 2502-8782

dilengkapi dengan pengaturan keamanan yang optimal, termasuk pengaturan firewall dan kontrol akses yang lebih ketat.

4. Penggunaan Manajemen Kata Sandi yang Kuat: Menerapkan kebijakan kata sandi yang kuat dan menggantinya secara berkala untuk mengurangi risiko akses yang tidak sah.

5. SIMPULAN

Berdasarkan hasil penelitian mengenai keamanan jaringan Wi-Fi di MI Inwanul Huda, dapat disimpulkan sebagai berikut:

1. Tingkat Keamanan Jaringan Wi-Fi
   Pengujian menunjukkan bahwa jaringan Wi-Fi memiliki beberapa celah keamanan. Temuan utama meliputi:
   1) Penggunaan enkripsi WPA2, yang meskipun masih umum, tidak sepenuhnya aman jika dikonfigurasi secara tidak optimal (misalnya, menggunakan WPA2-TKIP).
   2) Kata sandi Wi-Fi yang lemah dan mudah ditebak, memperbesar risiko serangan seperti brute-force.
   3) Perangkat jaringan yang belum diperbarui menggunakan firmware terbaru, membuka potensi eksploitasi kerentanan yang telah diketahui.
2. Persepsi dan Pengetahuan Pengguna
   Dari survei terhadap pengguna, ditemukan bahwa mayoritas pengguna memiliki pengetahuan yang rendah tentang keamanan jaringan. Sebanyak 70% pengguna tidak memahami langkah-langkah dasar untuk menjaga keamanan data, dan 65% menggunakan kata sandi yang sama untuk berbagai layanan. Kebiasaan ini meningkatkan risiko pelanggaran keamanan jaringan.
3. Konfigurasi Perangkat Jaringan
   Evaluasi konfigurasi perangkat menunjukkan bahwa firewall dan pengaturan akses tidak dioptimalkan, serta pengelolaan kata sandi tidak memiliki kebijakan rotasi yang memadai. Upaya peningkatan keamanan perangkat masih diperlukan untuk melindungi jaringan dari ancaman eksternal.

SARAN

Peneliti mengusulkan untuk menerapkan prosedur keamanan yang tegas di madrasah. Sebaiknya ada kebijakan terdokumentasi yang mengatur penggunaan jaringan WiFi. Kebijakan ini harus berisi panduan untuk memperbarui kata sandi secara berkala, mencegah berbagi kata sandi, dan mengenakan denda kepada mereka yang melanggar peraturan keamanan.

Menggunakan teknologi keamanan modern: Solusi keamanan seperti VPN untuk akses eksternal, firewall yang lebih baik, dan sistem deteksi intrusi (IDS) harus digunakan untuk mengurangi bahaya serangan eksternal.

Dengan mengambil prosedur ini, keamanan jaringan WIFI di Madrasah Ibtidaiyah Inwanul Huda diproyeksikan akan meningkat, mengurangi ancaman keamanan saat ini dan memungkinkan seluruh komunitas sekolah untuk memanfaatkan jaringan dengan aman dan efektif.

DAFTAR REFERENSI

[1] E. Putri Primawanti and H. Ali, “Pengaruh Teknologi Informasi, Sistem Informasi Berbasis Web Dan Knowledge Management Terhadap Kinerja Karyawan (Literature Review Executive Support Sistem (Ess) for Business),” *Jurnal Ekonomi Manajemen Sistem Informasi*, vol. 3, no. 3, pp. 267–285, 2022, doi: 10.31933/jemsi.v3i3.818.

[2] S. Faisal, “Perancangan Jaringan Wifi Rt / Rw Net Pada Desa Kutawargi,” *Konferensi Nasional Penelitian dan Pengabdian (KNPP) Ke-1 Karawang, 25 Februari 2021 Universitas Buana Perjuangan Karawang*, pp. 20–38, 2021.

[3] R. J. Sarjanoko, “Rancang Bangun Sistem Keamanan Lingkungan Berbasis Wifi Menggunakan Ip Camera,” *Teknois : Jurnal Ilmiah Teknologi Informasi dan Sains*, vol. 12, no. 1, pp. 79–84, 2022, doi: 10.36350/jbs.v12i1.132.

[4] M. Krisdianto, *Rancangan Keamanan Jaringan Komputer*. 2022.

[5] S. N. ARINZE, G. N. ONOH, and D. O. ABONYI, “Performance of Light Fidelity and Wireless Fidelity

Networks in a Wlan," *International Journal of Research in Engineering & Science*, vol. 4, no. 1, 2020, doi: 10.26808/rs.re.v4i1.02.

[6] M. Z. E. Kalam, N. M. A. E. D. Wirastuti, and I. M. O. Widyantara, "Analisa Kinerja Penerapan Standard Protokol Keamanan IEEE 802.11 Pada Layanan Wireless Fidelity," *Majalah Ilmiah Teknologi Elektro*, vol. 20, no. 1, p. 89, 2021, doi: 10.24843/mite.2021.v20i01.p10.

[7] A. Y. F. Azmi, J. Gusti A G, and E. Wahyudi, "Analisis Network Security pada Layanan Wifi Indihome Terhadap Serangan Denial of Service (DOS)," *Jurnal Litek : Jurnal Listrik Telekomunikasi Elektronika*, vol. 19, no. 1, pp. 8–12, 2022, doi: 10.30811/litek.v19i1.18.

[8] D. Rahmat, Z. Muharraran, and M. A. Agustian, "Analisis Efisiensi Dan Keamanan Konfigurasi Web Proxy Dalam Mengelola Trafik Internet Di Lingkungan Pendidikan," *INFOTECH journal*, vol. 10, no. 1, pp. 132–140, 2024, doi: 10.31949/infotech.v10i1.9774.

[9] A. Riyanto and D. P. Arini, "Analisis Deskriptif Quarter-Life Crisis Pada Lulusan Perguruan Tinggi Universitas Katolik Musi Charitas," *Jurnal Psikologi Malahayati*, vol. 3, no. 1, pp. 12–19, 2021, doi: 10.33024/jpm.v3i1.3316.

[10] R. N. Dasmen, R. Rasmila, T. L. Widodo, K. Kundari, and M. T. Farizky, "Pengujian Penetrasi Pada Website Elearning2.Binadarma.Ac.Id Dengan Metode Ptes (Penetration Testing Execution Standard)," *Jurnal Komputer dan Informatika*, vol. 11, no. 1, pp. 91–95, 2023, doi: 10.35508/jicon.v11i1.9809.

[11] B. Darma, *Statistika Penelitian Menggunakan SPSS (Uji Validitas, Uji Reliabilitas, Regresi Linier Sederhana, Regresi Linier Berganda, Uji t, Uji F, R2*. Guepedia, 2021.