Evaluasi Keamanan Jaringan Wi-Fi Menggunakan *Penetration Testing* Berdasarkan ISO 27001 (Studi Kasus: LPD XYZ)

I Nyoman Kasna[1a)], Roy Rudolf Huizen [2b)], Ni Made Rai Masita Dewi [3c)]
[1)]Sistem Komputer, Institut Teknologi dan Bisnis STIKOM Bali, Bali, Indonesia
[2)]Magister Sistem Informasi, Institut Teknologi dan Bisnis STIKOM Bali, Bali, Indonesia
[3)]Sistem Informasi, Institut Teknologi dan Bisnis STIKOM Bali, Bali, Indonesia
e-mail: [a)]220010116@stikom-bali.ac.id, [b)]roy@stikom-bali.ac.id, [c)]raimasita@stikom-bali.ac.id

Abstrak

Penelitian ini dilakukan untuk mengevaluasi keamanan jaringan Wi-Fi pada LPD XYZ dengan menelaah kesenjangan antara pengamanan teknis yang diterapkan dan tata kelola keamanan informasi berdasarkan standar ISO/IEC 27001:2022. Metode penelitian yang digunakan adalah pendekatan kualitatif dengan desain studi kasus. Pengumpulan data dilakukan melalui observasi langsung terhadap infrastruktur jaringan, pelaksanaan penetration testing pada jaringan Wi-Fi, wawancara dengan pihak pengelola, dan telaah terhadap dokumen internal yang berkaitan dengan keamanan informasi. Analisis data dilakukan dengan memetakan seluruh temuan dari Technical audit dan management audit serta kontrol yang terdapat dalam Annex A ISO/IEC 27001:2022. Hasil audit menunjukkan bahwa secara teknis jaringan Wi-Fi telah memiliki tingkat keamanan yang cukup baik dan mampu bertahan dari serangan dasar. Namun demikian, aspek manajerial dan kebijakan keamanan informasi belum diterapkan secara formal dan terstruktur. Kelemahan utama yang ditemukan meliputi ketiadaan kebijakan tertulis, rendahnya kesadaran keamanan pengguna, serta belum adanya mekanisme evaluasi dan peningkatan keamanan secara berkelanjutan. Penelitian ini menegaskan pentingnya integrasi pengamanan teknis dengan sistem manajemen keamanan informasi untuk meningkatkan keamanan organisasi.

Kata kunci: *Keamanan Wi-Fi, ISO/IEC 27001:2022, ISMS, Penetration Testing, Lembaga Keuangan Desa.*

1. Pendahuluan

Perkembangan teknologi informasi telah mempercepat transformasi digital di berbagai sektor, termasuk layanan keuangan. Jaringan *Wireless Fidelity* (Wi-Fi) menjadi infrastruktur penting karena mendukung konektivitas dan operasional harian organisasi. Namun, peningkatan ketergantungan terhadap Wi-Fi juga diikuti oleh eskalasi ancaman keamanan siber. [1] mencatat lebih dari 370 juta anomali serangan siber di Indonesia, dengan sebagian besar memanfaatkan kelemahan konfigurasi jaringan nirkabel. Temuan [2] menunjukkan bahwa banyak titik akses Wi-Fi belum menerapkan autentikasi dan enkripsi yang memadai, sementara [3] menegaskan efektivitas *Penetration Testing Execution Standard* (PTES) dalam mengidentifikasi kerentanan sebelum dieksploitasi. Risiko ini tidak hanya bersifat teknis, tetapi juga berdampak pada kepercayaan publik terhadap institusi digital.

kajian keamanan jaringan Wi-Fi berbasis ISO IEC 27001 di Indonesia masih berfokus pada pengujian teknis kuantitatif, dengan perhatian terbatas pada aspek proses dan praktik implementasi di tingkat organisasi [4], [5]. Beberapa Penelitian telah menyoroti pentingnya integrasi manajemen risiko dan evaluasi keamanan jaringan [6], namun kajian pada organisasi lokal seperti Lembaga Perkreditan Desa masih terbatas. Berdasarkan celah penelitian tersebut, penelitian ini bertujuan untuk mengevaluasi keamanan jaringan Wi-Fi pada LPD XYZ melalui *penetration testing* yang dipetakan terhadap standar ISO/IEC 27001 dengan pendekatan kualitatif. Kontribusi penelitian ini terletak pada integrasi hasil pengujian teknis dengan evaluasi tata kelola keamanan informasi, sehingga memberikan gambaran mengenai kesenjangan antara pengamanan teknis dan penerapan Sistem Manajemen Keamanan Informasi pada lembaga keuangan mikro.

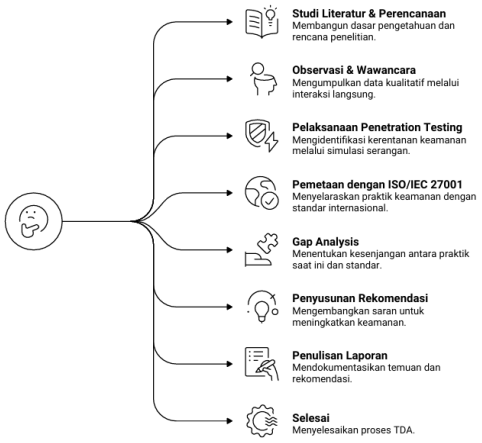
2. Metode Penelitian

Penelitian ini menerapkan metode *penetration testing* untuk mengidentifikasi celah keamanan yang berpotensi dieksploitasi pihak tidak berwenang [7]-[9]. Metode ini mensimulasikan serangan siber

secara terkontrol guna menilai tingkat keamanan jaringan secara nyata [10], [11]. Ruang lingkup pengujian terbatas pada jaringan Wi-Fi LPD XYZ dengan jenis serangan umum, yaitu *deauthentication*, *packet capturing*, dan *dictionary attack*, untuk mengevaluasi kekuatan konfigurasi teknis dan kerentanan yang dapat dimanfaatkan. Hasil pengujian kemudian dipetakan terhadap standar ISO IEC 27001 untuk menilai kesesuaian penerapan kontrol keamanan jaringan Wi-Fi di LPD XYZ.

2.1 Alur penelitian

Alur penelitian mencakup beberapa tahapan yang dimulai dari identifikasi masalah hingga pelaporan hasil penelitian. Tahapan tersebut ditunjukkan pada Gambar 1. Alur Penelitian.



Gambar 1. Alur Penelitian

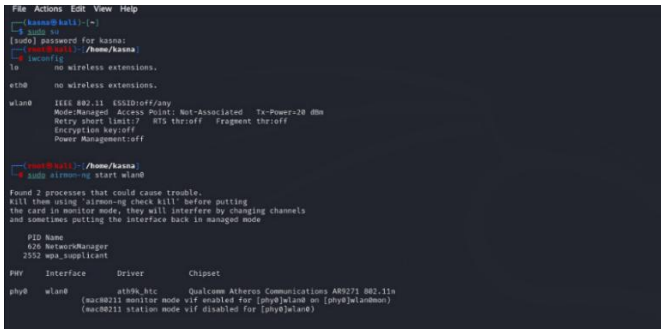
a. Studi Literatur dan Perencanaan
   Dilakukan penelaahan literatur mengenai keamanan jaringan Wi-Fi, *penetration testing*, serta standar ISO/IEC 27001:2022 yang merupakan versi terbaru dari sistem manajemen keamanan informasi (ISMS). Versi ini mencakup tujuh klausul utama (4–10) dan empat domain kontrol utama pada *Annex* A (A.5–A.8).
b. Observasi dan Pengumpulan Data
   Tahap ini melibatkan observasi kondisi jaringan Wi-Fi tersebut, wawancara dengan pengelola jaringan, dan studi dokumen pada kebijakan dan prosedur keamanan jaringan di LPD XYZ.
c. Pelaksanaan *Penetration Testing*
   Pengujian dilakukan menggunakan *tools Aircrack-ng suite* pada sistem operasi *Kali Linux* untuk mengidentifikasi celah keamanan, melakukan simulasi serangan, dan menguji kekuatan konfigurasi keamanan jaringan.
d. Pemetaan Hasil dengan ISO/IEC 27001
   Hasil *penetration testing* kemudian dipetakan terhadap kontrol keamanan yang relevan dalam ISO/IEC 27001, terutama pada aspek pengendalian akses dan keamanan jaringan.
e. Analisis Kesenjangan (*Gap Analysis*)
   Dilakukan perbandingan antara kondisi keamanan jaringan yang ada dengan kontrol ISO/IEC 27001.
f. Penyusunan Rekomendasi
   Rekomendasi disusun berdasarkan hasil *gap analysis* agar sistem keamanan jaringan Wi-Fi lebih sesuai dengan ISO/IEC 27001:2022.

3. Hasil dan Pembahasan

Pengujian dilakukan pada jaringan Wi-Fi LPD XYZ menggunakan sistem operasi *Kali Linux* versi 2024.4 dengan rangkaian *tools Aircrack-ng suite*. Proses pengujian dilakukan melalui beberapa tahap yaitu *scanning*, identifikasi kerentanan, dan simulasi serangan.

3.1 *Interface Monitoring (airmon-ng)*

Tahapan ini bertujuan untuk mengaktifkan mode monitor pada *wireless interface*, sehingga perangkat dapat memantau semua lalu lintas jaringan di sekitar area uji. Perintah *airmon-ng start wlan0* digunakan untuk menginisialisasi mode ini. Hasil dapat dilihat pada Gambar 2.

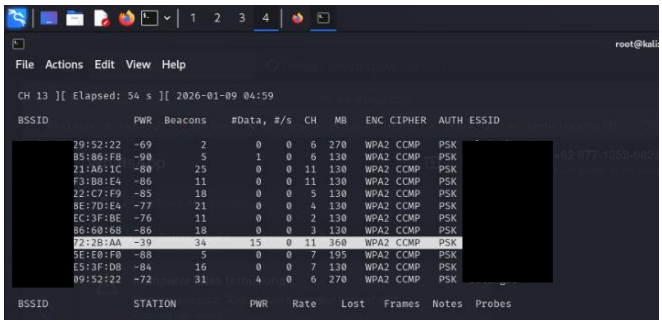


Gambar 2. *Interface Monitoring*

Gambar 2. menunjukkan *interface wlan0* berhasil diubah ke mode monitor dengan nama baru *wlan0mon*. Mode ini memungkinkan perangkat melakukan pemantauan sinyal Wi-Fi di sekitar area LPD XYZ untuk tahap pengujian selanjutnya.

3.2 *Packet Capturing* (*airodump-ng*)

Langkah ini digunakan untuk menangkap paket autentikasi antara *access point* dan klien agar dapat memperoleh WPA *handshake*, yang diperlukan dalam proses analisis kunci jaringan. Perintah yang dijalankan: *airodump-ng wlan0mon.* Hasilnya ditampilkan pada Gambar 3.

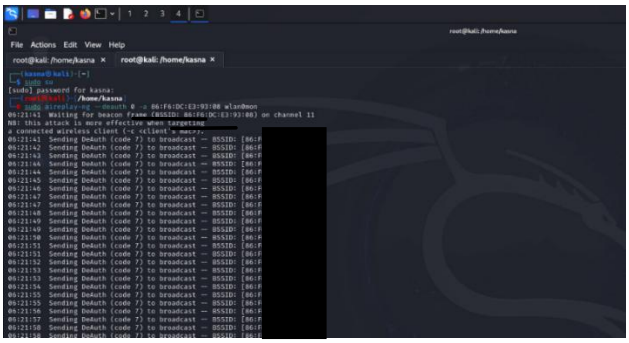


Gambar 3. *Packet Capturing*

Gambar 3. menunjukkan hasil eksekusi perintah *airodump-ng wlan0mon* yang menampilkan daftar jaringan Wi-Fi di sekitar area uji. Tabel tersebut memuat informasi seperti BSSID, *channel* (CH), *enkripsi* (ENC) dan ESSID dari masing-masing *access point*.

3.3 *Deauthentication Injection* (*aireplay-ng*)

Tahapan ini dilakukan untuk menguji ketahanan jaringan terhadap serangan *Denial of Service* (DoS) dengan metode *Deauthentication Injection*. Tujuannya adalah untuk memutus sementara koneksi antara *access point* dan klien, serta mempercepat proses perolehan paket a*utentikasi* (*WPA handshake*) pada jaringan target. Hasil dapat dilihat pada gambar 4.



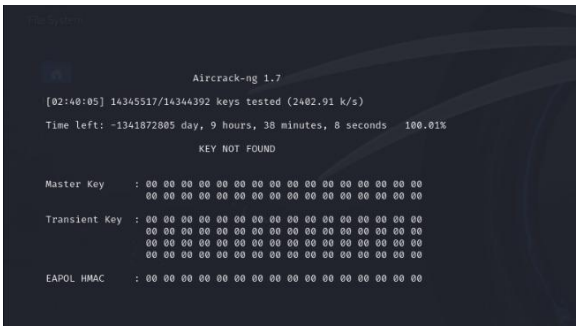
Gambar 4. *Deauthentication Injection*

Gambar 4. menunjukkan hasil eksekusi dari perintah *aireplay-ng* yang digunakan untuk melakukan *Deauthentication Injection* pada jaringan target. Proses ini bertujuan memutus koneksi antara *access point* dan *clien*, sehingga memicu proses *autentikasi* ulang yang memungkinkan penangkapan paket

WPA handshake. Pada gambar terlihat pengiriman berulang pesan *"Sending Deauth"* ke BSSID target LPD XYZ pada *channel* 11, menandakan serangan DoS berhasil dijalankan untuk keperluan pengujian keamanan jaringan.

3.4 *Proses Cracking Password (aircrack-ng)*

Tahapan ini merupakan bagian akhir dari proses penetration testing, di mana proses *penetration testing* bertujuan untuk menguji kekuatan kata sandi jaringan Wi-Fi dengan didasari *file handshake* yang telah diperoleh pada tahap sebelumnya. Pengujian ini dilakukan menggunakan metode *Dictionary Attack*. Hasilnya dapat dilihat pada Gambar 5.



Gambar 5. *Proses Cracking Password*

Gambar 5. menunjukkan hasil *tools aircrack-ng* pada tahap *cracking password* menggunakan metode *dictionary attack*. Proses ini bertujuan untuk menemukan kata sandi jaringan Wi-Fi berdasarkan *file handshake* yang telah diperoleh sebelumnya. Hasil *"KEY NOT FOUND"* Dalam hasil di atas menandakan bahwa tidak ada kata sandi yang cocok dengan yang ada di *wordlist*, jadi jaringan masih aman dari serangan ini.

3.5 Pemetaan Penilaian Berdasarkan *Klausul* ISO/IEC 27001

Pemetaan ini dilakukan untuk menilai sejauh mana LPD XYZ telah memenuhi klausul utama yang ditetapkan dalam standar ISO/IEC 27001:2022, khususnya pada aspek tata kelola sistem manajemen keamanan informasi (ISMS). Hasil pemetaan disajikan dalam Tabel 1.

Tabel 1. Pemetaan Penilaian Berdasarkan *Klausul* ISO/IEC 27001:2022 pada LPD XYZ

***Klausul* ISO/IEC 27001:2022**	**Deskripsi Kondisi di LPD XYZ**	**Target**	**Hasil**
4. *Context of the Organization*	Belum ada analisis konteks formal terhadap sistem jaringan Wi-Fi dan aset informasi.	3	2
5. *Leadership*	Dukungan pimpinan bersifat informal, belum ada kebijakan keamanan informasi tertulis.	3	2
6. *Planning*	Belum dilakukan perencanaan keamanan berbasis risiko secara formal.	3	2
7. *Support*	Pelatihan keamanan informasi dan kesadaran pegawai belum dilaksanakan.	3	1
8. *Operation*	Pengendalian operasional dilakukan manual tanpa SOP terdokumentasi.	3	3
9. *Performance Evaluation*	Belum ada evaluasi berkala atau *audit internal* terhadap sistem jaringan.	3	2
10. *Improvement*	Tidak ada *mekanisme* perbaikan dan peningkatan berkelanjutan terhadap sistem keamanan.	3	2

Berdasarkan Tabel 1, LPD XYZ belum menerapkan prinsip ISMS secara menyeluruh. Klausul 8 *Operation* memperoleh nilai tertinggi, yaitu 3, karena beberapa aktivitas operasional teknis sudah berjalan meskipun belum didukung prosedur tertulis. Sebaliknya, Klausul 7 Support memiliki nilai terendah, yakni 1, akibat tidak adanya pelatihan keamanan informasi dan

keterbatasan sumber daya manusia. Kondisi ini menunjukkan bahwa sistem manajemen keamanan informasi masih bersifat reaktif dan belum terdokumentasi secara formal.

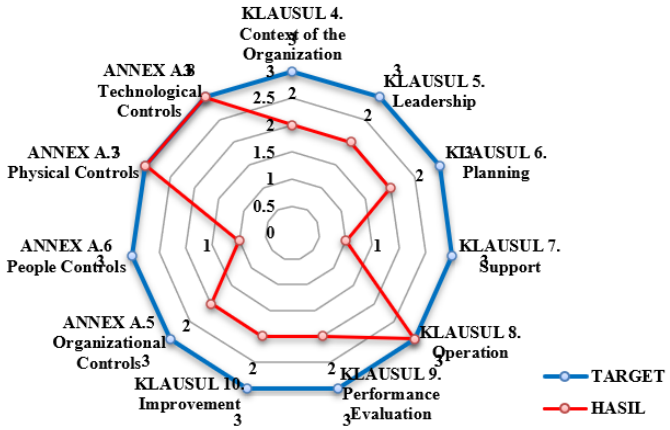
3.6 Evaluasi Penerapan Kontrol *Annex* A ISO/IEC 27001:2022

Selain klausul utama, evaluasi juga mencakup *Annex* A ISO IEC 27001:2022 yang terdiri dari empat *domain* kontrol, yaitu *Organizational*, *People*, *Physical*, dan *Technological Controls*. Penilaian ini digunakan untuk melihat tingkat kesesuaian penerapan kontrol keamanan jaringan Wi-Fi di LPD XYZ dengan ketentuan standar ISO IEC 27001:2022. Hasil evaluasi dapat dilihat dalam Tabel 2.

Tabel 2. Evaluasi Penerapan Kontrol Annex A ISO/IEC 27001:2022 pada LPD XYZ

***Annex* A ISO/IEC 27001:2022**	**Deskripsi *Implementasi***	**Target**	**Hasil**
A.5 *Organizational Controls*	Tidak ada kebijakan keamanan formal, belum ada pengelolaan risiko atau dokumentasi peran dan tanggung jawab keamanan.	3	2
A.6 *People Controls*	Belum ada pelatihan atau program kesadaran keamanan bagi *staf* dan pengguna jaringan.	3	1
A.7 *Physical Controls*	Fasilitas jaringan cukup aman, tetapi belum ada prosedur pengawasan dan dokumentasi keamanan fisik.	3	3
A.8 *Technological Controls*	Jaringan Wi-Fi menggunakan WPA2-CCMP yang aman; belum memiliki sistem logging otomatis dan kebijakan penggantian kata sandi.	3	3

Tabel 2. menunjukkan bahwa kontrol keamanan teknologi A.7 dan A.8 merupakan aspek terkuat, sejalan dengan hasil *penetration testing* yang membuktikan jaringan Wi Fi tahan terhadap *dictionary attack*. Sebaliknya, kontrol sumber daya manusia A.6 masih lemah akibat tidak adanya pelatihan dan rendahnya kesadaran keamanan. Secara umum, penerapan keamanan informasi di LPD XYZ masih berfokus pada aspek teknis dan belum menyentuh tata kelola keamanan secara menyeluruh. *Spider chart* semua *klausul* dan *annex* dapat dilihat pada gambar 6.



Gambar 6. *Spider chart Klausul* dan *Annex*

Technical audit dan *management audit* berbasis ISO IEC 27001 menunjukkan kesenjangan yang jelas. Audit teknis mencatat hasil lebih tinggi karena jaringan Wi-Fi telah dikonfigurasi aman dan terlindungi dari serangan dasar. Sebaliknya, audit manajemen menemukan kelemahan dalam kebijakan, dokumentasi, dan konsistensi kontrol keamanan. Dengan demikian, penguatan terintegrasi melalui implementasi ISMS berbasis ISO IEC 27001:2022, khususnya *pada klausul Support, Planning*, dan *Improvement*, dibutuhkan untuk memastikan keamanan jaringan yang berkelanjutan.

Secara keseluruhan, evaluasi ISO/IEC 27001:2022 menunjukkan bahwa keamanan jaringan Wi-Fi LPD XYZ sudah cukup kuat secara teknis melalui penerapan WPA2-CCMP, namun masih lemah pada aspek tata kelola keamanan informasi, khususnya pada kebijakan, dokumentasi, dan kesadaran keamanan oleh karena itu, peningkatan keamanan perlu difokuskan pada penyusunan kebijakan formal, pemenuhan dokumentasi sesuai ISO/IEC 27001:2022, serta pelatihan SDM agar sistem Wi-Fi dikelola dengan baik.

4. Kesimpulan

Keamanan teknis jaringan Wi-Fi LPD XYZ tergolong cukup kuat, dibuktikan dengan hasil *penetration testing* yang tidak menemukan kerentanan kritis dan efektivitas enkripsi WPA2-CCMP dalam menahan serangan dasar. Namun, penerapan Sistem Manajemen Keamanan Informasi belum berjalan menyeluruh karena aspek kebijakan, kepemimpinan, sumber daya manusia, dan tata kelola masih lemah. di mana kontrol keamanan sudah diterapkan tetapi belum terintegrasi, terdokumentasi, dan dikelola secara berkelanjutan sesuai ISO/IEC 27001:2022. penelitian ini mendorong integrasi sistem pengamanan teknologi dengan sistem manajemen keamanan informasi sesuai dengan standar ISO/IEC 27001 sebagai strategi yang lebih lengkap dan berkelanjutan bagi lembaga keuangan desa.

Daftar Pustaka

[1] B. S. dan S. N. (BSSN), "Laporan Tahunan BSSN 2023: Mengawal Ruang Siber Nasional," Badan Siber dan Sandi Negara, Jakarta, 2024. [Online]. Available: https://bssn.go.id/laporan-tahunan-2023

[2] M. A. Hanafi, "Analisa Keamanan Jaringan Wireless UNIMMA Menggunakan Metode Penetration Testing," 2024. [Online]. Available: http://repositori.unimma.ac.id/4139

[3] F. T. Huzaini, "Analisis Sistem Keamanan Jaringan Wireless dengan Metode PTES (Penetration Testing Execution Standard)," 2024. [Online]. Available: https://repository.nurulfikri.ac.id/id/eprint/612/

[4] Y. Y. Santika and R. Rianto, "Studi Komprehensif Keamanan Siber: Perbandingan Teknologi AI dengan Sistem Non-AI dalam Deteksi dan Pencegahan Ancaman," *Jurnal Komtika*, vol. 10, no. 2, 2025, doi: 10.31603/komtika.v10i2.13149.

[5] D. L. Jayanto, M. Herfin, M. Akbar, and S. Saputra, "Kesiapan dan Keamanan Infrastruktur Penyelenggaraan Rekam Medis Elektronik di RSUD Kabupaten Kediri," *Jurnal Sains, Nalar, dan Teknologi Informasi*, 2025, doi: 10.20885/snati.vol1.art40288.

[6] A. N. Fanani, B. T. Hanggara, and A. R. Perdanakusuma, "Manajemen Risiko Keamanan Informasi Menggunakan ISO/IEC 27005 Studi Kasus Pada Dinas Komunikasi dan Informatika Kabupaten Sidoarjo," 2025. [Online]. Available: http://j-ptiik.ub.ac.id

[7] A. Milenius, D. Marly, W. Ardiyasa, and W. K. Utama, "Analisis Keamanan Jaringan Dengan Menggunakan Metode Penetration Testing (Studi Kasus ITB STIKOM Bali)," vol. 2, no. 1, p. 2025, 2025.

[8] N. A. Santoso, M. Ainurohman, and R. D. Kurniawan, "PENERAPAN METODE PENETRATION TESTING PADA KEAMANAN JARINGAN NIRKABEL," *JURNAL RESPONSIF*, vol. 4, no. 2, pp. 162–167, 2022, [Online]. Available: https://ejurnal.ars.ac.id/index.php/jti

[9] D. Singasatia, M. Kom, ; M Hafid Totohendarto, S. M. M. Si, J. Saputro, and S. Kom, "PENETRATION TESTING UNTUK MENGUJI KERENTANAN PADA SISTEM INFORMASI AKADEMIK DI SEKOLAH TINGGI TEKNOLOGI XYZ." [Online]. Available: http://www.IANA.org,

[10] Wasti; Peggy Veronica Togas; Johan Reimon Batmetan; Arje Cerullo Djamen, "ANALISIS KEAMANAN JARINGAN WLAN MENGGUNAKAN METODE PENETRATION TESTING DI SMK KRISTEN GETSEMANI MANADO," *EduTIK: Jurnal Pendidikan Teknologi Informasi dan Komunikasi*, vol. 5, no. 1, pp. 31–41, Feb. 2025.

[11] Nurfanis; Zaenudin; Muhamad Masjun Efendi, "ANALISIS KEAMANAN JARINGAN WIRELESS MENGGUNAKAN METODE PENETRATION TESTING DI SMK BANGUN NEGERI HU'U," *Jurnal Rekayasa Sistem Informasi dan Teknologi*, p. 751, Nov. 2024.