LINIER
LITERATUR INFORMATIKA & KOMPUTER
e-ISSN: 3063-2218
DOI : 10.33096/linier.v2i1.2786
Literatur Informatika & Komputer
Vol 2, No 1 (2025), pp 50-57

Analisis Serangan *Jammer* Pada Jaringan *Wireless*

Maulana Nuruddin Djamin[a], Erick Irawadi Alwi[b], Syahrul Mubarak Abdullah[c]
Universitas Muslim Indonesia, Makassar, Indonesia
[a]13020200257@umi.ac.id; [b]erick.alwi@umi.ac.id; [c]syahrul.mubarak@umi.ac.id

Received: 21-08-2024 | Revised: 20-01-2025 | Accepted: 01-03-2025 | Published: 29-03-2025

Abstrak

Serangan *jammer* terhadap jaringan *wireless* telah menjadi Persoalan Penting dalam upaya menjaga keamanan dan kelancaran Pemeliharaan jaringan. *Jammer* berfungsi mengganggu dan merusak sinyal jaringan *wireless*, yang mengakibatkan Keterbatasan pengguna untuk terhubung dengan jaringan tersebut. Penelitian ini Bertujuan Untuk menjelaskan mekanisme kerja Serangan *Jammer*, dan mengidentifikasi metode-metode keamanan yang dapat digunakan untuk menghadapi ancaman ini secara efektif. Dengan menggabungkan pendekatan penelitian teoretis, analisis studi kasus, simulasi berbasis Laptop/Komputer, dan eksperimen praktis, penelitian ini mengevaluasi efektivitas serangan jamming dalam berbagai kondisi jaringan serta dampaknya terhadap performa dan keamanan. Penelitian ini menemukan bahwa serangan *jammer* dapat secara signifikan menurunkan kualitas layanan dan menyebabkan gangguan serius pada kestabilan jaringan. Hasil penelitian menunjukkan bahwa penerapan strategi keamanan yang menyeluruh dan berbasis pada pemahaman mendalam tentang mekanisme serangan dapat memberikan perlindungan yang signifikan terhadap ancaman *jammer*. Strategi tersebut meliputi penggunaan teknik mitigasi yang dapat mengurangi dampak serangan jamming dan memastikan keberlangsungan jaringan *wireless* yang aman dan stabil.

Kata kunci: Serangan *Jammer,* Jaringan *Wireless,* Deteksi, Mitigasi, Keamanan Jaringan

Pendahuluan

Di era digital yang semakin berkembang pesat seperti ini, jaringan *wireless* menjadi salah satu teknologi yang tak terpisahkan dari kehidupan sehari-hari [1]. Jaringan *wireless* memungkinkan pengguna untuk terhubung ke internet tanpa perlu menggunakan kabel fisik, sehingga memberikan banyak manfaat, seperti kemudahan akses internet, fleksibilititas dalam berkomunikasi, dan mobilitas tanpa batas [2], [3]. Terutama dengan kemajuan teknologi yang terus-menerus sehingga jaringan *wireless* semakin memikat dengan kemudahan dan fleksibilitasnya [4]. Dalam konteks ini, jaringan nirkabel telah menjadi sangat penting bagi banyak aspek kehidupan sehari-hari, dari kebutuhan pribadi hingga kebutuhan bisnis [5]. Teknologi ini memungkinkan pengguna untuk mengakses informasi, berkomunikasi, dan bertukar data dengan lebih mudah dan efektif. Sebagai contoh, *Wi-fi* telah menjadi standar untuk menghubungkan perangkat ke internet di rumah, kantor, dan area umum lainnya [6].

Namun, bersama dengan keuntungan-keuntungan tersebut, ada juga resiko penggunaan jaringan *wireless* yang perlu di waspadai. Salah satu resiko yang sering kali dihadapi adalah serangan *jammer* pada jaringan *wireless* [7]. Serangan ini dapat menyebabkan gangguan serius pada jaringan, seperti penurunan kualitas sinyal, kegagalan koneksi, ketidakstabilan dalam pengiriman data, bahkan memicu kebocoran data sensitive [8]. Sehingga, membuat pengguna tidak dapat mengakses internet atau menggunakan layanan lainnya. Hal ini bisa terjadi di tempat kerja, sekolah, atau bahkan di rumah. Oleh karena itu, Sangat penting untuk mengimplementasikan strategi keamanan yang efektif dan menerapkan langkah - langkah keamanan yang tepat Seperti menggunakan perangkat keras atau perangkat lunak yang dapat mengenali dan mengatasi serangan *jammer* [8][9].

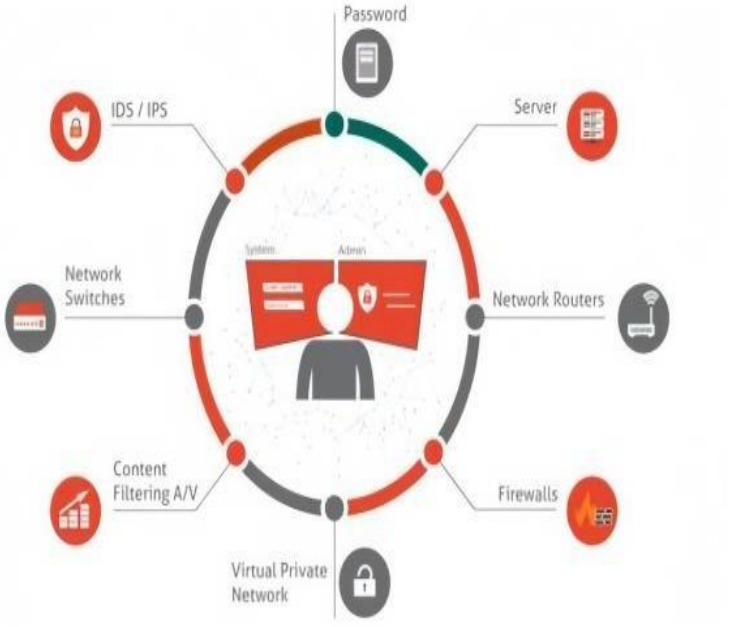
Perkembangan teknologi wireless tidak hanya membawa inovasi, tetapi juga memunculkan celah keamanan yang semakin kompleks. Serangan jammer, sebagai salah satu bentuk cyber-physical attack, bekerja dengan memancarkan sinyal gangguan pada frekuensi yang sama dengan jaringan wireless target, sehingga menimbulkan interferensi destruktif [10]. Teknik ini dapat dilakukan dengan perangkat sederhana yang mudah diakses, seperti software-defined radio (SDR) atau alat jamming komersial, membuat ancaman ini semakin sulit dideteksi dan diantisipasi [11]. Dampak serangan jammer juga meluas ke sektor kritis. Misalnya, di lingkungan industri yang mengandalkan IoT (Internet of Things), gangguan pada jaringan wireless dapat mengakibatkan malfungsi sistem otomasi, kerugian finansial, hingga risiko keselamatan [12]

Berdasarkan Penelitian Terdahulu, telah dilakukan Tinjauan tentang *A Review of Jamming Attacks in Wireless*

Systems [13]. penelitian ini membahas tentang berbagai jenis serangan jamming, teknik deteksi, dan metode mitigasi. Selanjutnya Metode *Penetration Testing* pada Keamanan Jaringan *Wireless Wardriving* PT. Puma Makmur Aneka *Engineering* Bekasi [14]. Penelitian ini membahas tentang kerentanan yang dapat ditemukan dalam menguji keamanan jaringan *wireless*. Dan Penelitian berikutnya yang berjudul *Penetration Testing* Pada Jaringan *Wifi* Menggunakan Kali Linux [15]. Penelitian ini menjelaskan tentang metode dan hasil penelitian yang dilakukan dalam menganalisis keamanan jaringan *wireless* menggunakan kali linux. Dari tinjauan ini, dapat disimpulkan bahwa serangan sinyal *jamming* merupakan ancaman serius bagi jaringan nirkabel. Berbagai penelitian telah mengeksplorasi jenis-jenis serangan *jamming*, dampaknya terhadap jaringan, serta teknik-teknik untuk mendeteksi dan mengurangi dampak serangan tersebut [16]. Melalui langkah-langkah ini penelitian dapat digunakan untuk meningkatkan keamanan jaringan *wireless*, melindungi data pribadi, dan meningkatkan kesadaran tentang pentingnya keamanan jaringan.

Metode

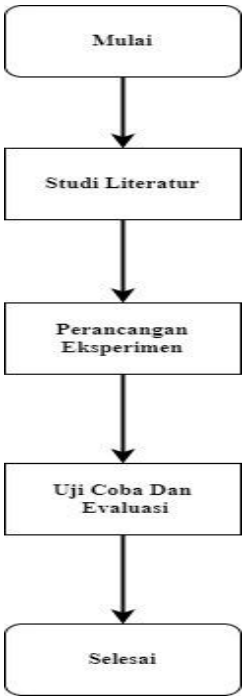
Metode yang digunakan dalam penelitian ini adalah *Penetration testing*. *Penetration testing*, Juga dikenal dengan bahasa lain Pengujian Penetrasi adalah suatu metode yang digunakan untuk menguji keamanan sistem komputer atau jaringan dengan cara yang sama seperti cara yang digunakan oleh penyerang [17]. Tujuan utama dari *penetration testing* adalah untuk mengidentifikasi kelemahan keamanan dan memberikan rekomendasi untuk meningkatkan keamanan sistem, Namun, pelaksanaan uji ini menuntut investasi waktu yang signifikan, sumber daya manusia yang kompeten, serta pemahaman mendalam untuk mengatasi tingkat kerumitan lingkungan pengujian. [18], [19]. Penelitian ini secara khusus mengeksplorasi penggunaan *penetration testing* dengan sistem operasi Kali Linux, yang dilengkapi dengan berbagai alat untuk menguji kekuatan enkripsi, mendeteksi kerentanan, dan melakukan serangan simulasi terhadap WPA *Key* jaringan nirkabel. Gambar 1. mendeskripsikan metode *penetration testing.*



Gambar 1. *Penetration Testing Metode*

Dalam Pengujian Metode *Penetration Testing* diperlukan *tools Fluxion*. Pengujian ini dapat Menggunakan *Fluxion tools* dalam Menganalisis *Wi–Fi*, Untuk memindai Jaringan nirkabel dan Mengidentifikasi celah keamanan dalam jaringan pribadi maupun bisnis [20].

Perancangan



Gambar 2. Alur Penelitian

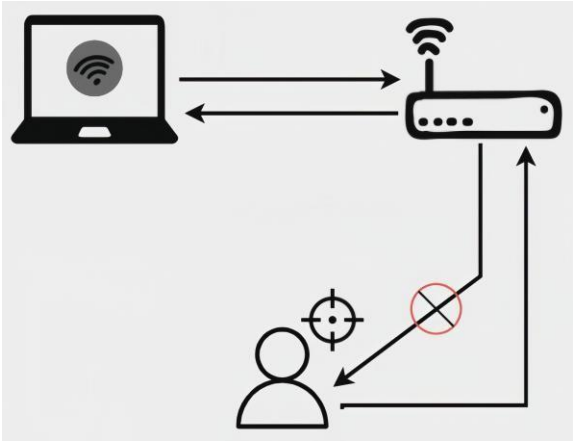
A. Studi Literatur
Pada tahapan ini, Peneliti mengumpulkan sumber dari Jurnal dan Penelitian sebelumnya. Tujuannya adalah untuk memahami kondisi pengetahuan saat ini mengenai serangan *jammer* dan Metode yang digunakan untuk mengatasinya. Hasilnya, Peneliti dapat mengidentifikasi celah – celah penelitian yang belum terjawab.

B. Perancangan Eksperimen
Peneliti merancang eksperimen untuk menguji secara lansung dampak serangan *jammer.* Langkah ini melibatkan pemilihan perangkat yang tepat, menyiapkan lingkungan pengujian yang menyerupai keadaan sebenarnya, dan memutuskan indikator kinerja yang akan dilacak. Peneliti juga akan merancang skenario serangan untuk melihat bagaimana jaringan beraksi.

C. Uji Coba Dan Evaluasi
Dalam tahap uji coba dan evaluasi dalam analisis serangan *jammer* pada jaringan *wireless*, langkah-langkah yang dilakukan sangat penting untuk memahami cara serangan *jammer* yang dapat mengganggu kinerja jaringan. Pertama, *Penetration Testing* Aktif dilakukan dengan menggunakan perangkat bantu keamanan seperti Kali Linux untuk menguji tingkat keamanan jaringan. Dalam percobaan ini, perangkat *jammer* digunakan untuk mengganggu sinyal jaringan *wireless*, sehingga dapat dilihat bagaimana jaringan bereaksi terhadap gangguan tersebut. Selanjutnya, Evaluasi Risiko dilakukan untuk menilai dampak serangan *jammer* pada jaringan, termasuk identifikasi potensi kerugian dan gangguan yang dapat terjadi pada jarak dan kekuatan sinyal yang dibutuhkan untuk mematikan fungsi *access point*, serta identifikasi kelemahan keamanan jaringan yang dapat dimanfaatkan oleh penyerang. Dengan demikian, hasil evaluasi ini dapat digunakan untuk menyimpulkan jenis serangan *jammer* yang dan memberikan rekomendasi untuk meningkatkan keamanan jaringan *wireless* untuk melawan serangan *jammer*.

Pemodelan

A. Topologi Jaringan
Pemodelan dalam konteks serangan *jammer* pada jaringan *wireless* bertujuan untuk memahami dan menganalisis dampak serangan ini terhadap kinerja jaringan . Dengan begitu Kita dapat menilai tingkat gangguan komunikasi yang disebabkan oleh serangan *jammer* dan penerapan teknik mitigasi yang dapat diterapkan melalui simulasi. Dibawah ini merupakan gambarannya :

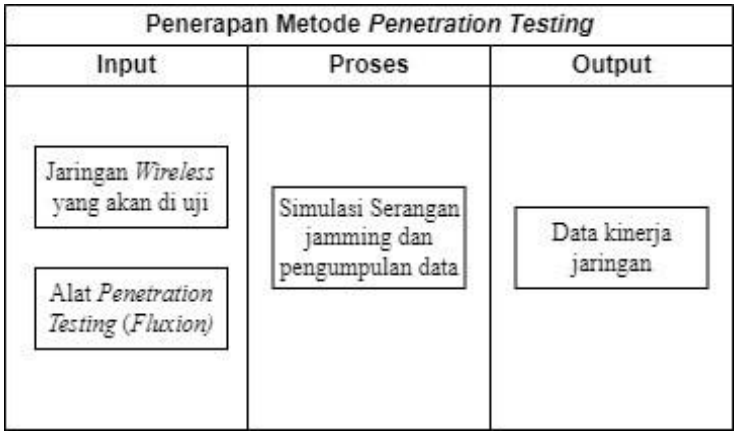


Gambar 3. Topologi Serangan *Jammer*

Gambar 3 menjelaskan skenario umum serangan *jammer* pada jaringan *wireless*. Yang dimana Laptop Berfungsi sebagai perangkat yang mencoba mengakses internet atau sumber daya lainnya saat terhubung ke jaringan *Wi–fi.* Selanjutnya *Router Wi–Fi* yang berfungsi sebagai titik akses dan pemancar sinyal *Wi–Fi.* Lalu *Jammer* yang berfungsi sebagai perangkat yang dengan sengaja merusak sinyal *Wi–fi* dengan mengirimkan sinyal pada frekuensi yang sama atau mirip. *Jammer* dilambangkan dengan Simbol "Dilarang" untuk menunjukkan bahwa *Jammer* ini mengganggu komunikasi normal. Dan Pengguna sebagai target dari serangan tersebut.

B. Perancangan Sistem

Dalam penelitian ini untuk melakukan proses Serangan *jammer* pada jaringan *wireless*, Tools Fluxion digunakan untuk melakukan serangan *jammer* pada jaringan *wireless* dengan menggunakan penetration testing. Untuk lebih jelas dan lengkapnya skema yang digunakan dapat dilihat di bawah ini :



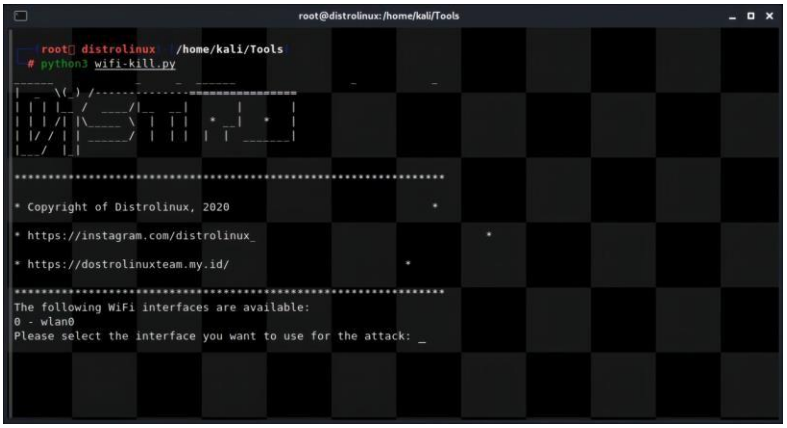
Gambar 4. Penerapan Metode *Penetration Testing*

Gambar 4 merupakan diagram blok yang menjelaskan langkah-langkah Penerapan metode *penetration testing* untuk menganalisis serangan jamming pada jaringan *wireless*, mulai dari input yang dibutuhkan, proses yang dilakukan, hingga output yang dihasilkan. Output dari proses ini adalah data yang penting untuk memahami dampak serangan dan untuk merancang strategi mitigasi yang efektif.

1. Input

   Pada bagian ini Peneliti memilih Jaringan target yang dipilih untuk melakukan serangan, atau jaringan nirkabel yang akan diuji. Kemudian, memasukkan alat pengujian penetrasi seperti *Fluxion*. Serangan dilakukan melalui program ini, yang memungkinkan pengujian dan pemodelan berbagai jenis serangan jamming pada jaringan nirkabel. Masukan ini menyiapkan segala sesuatunya agar serangan dapat terjadi. Seperti yang ditunjukkan pada Gambar 5 dan Gambar 6 berikut.

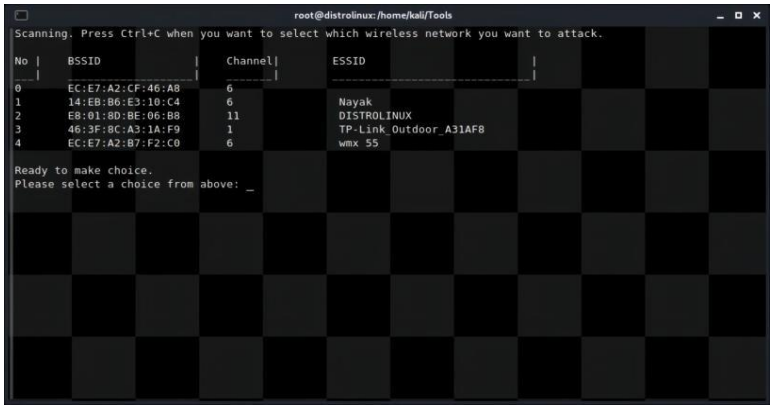
Gambar 5. Jaringan *Wireless* yang akan di uji



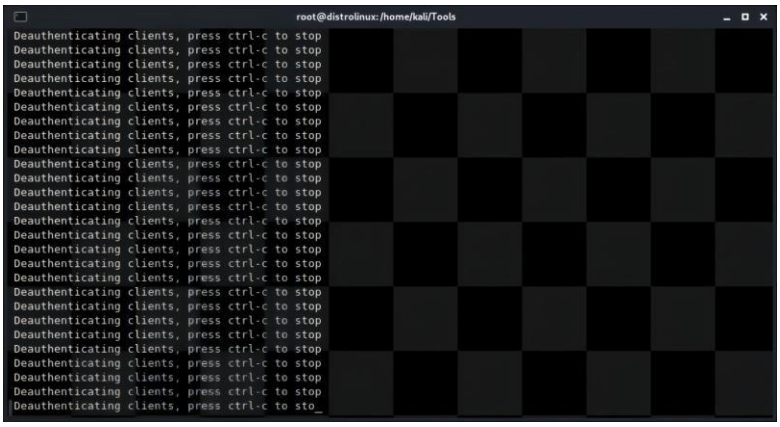
Gambar 6. Alat *Penetration Testing (Fluxion)*

2. Proses

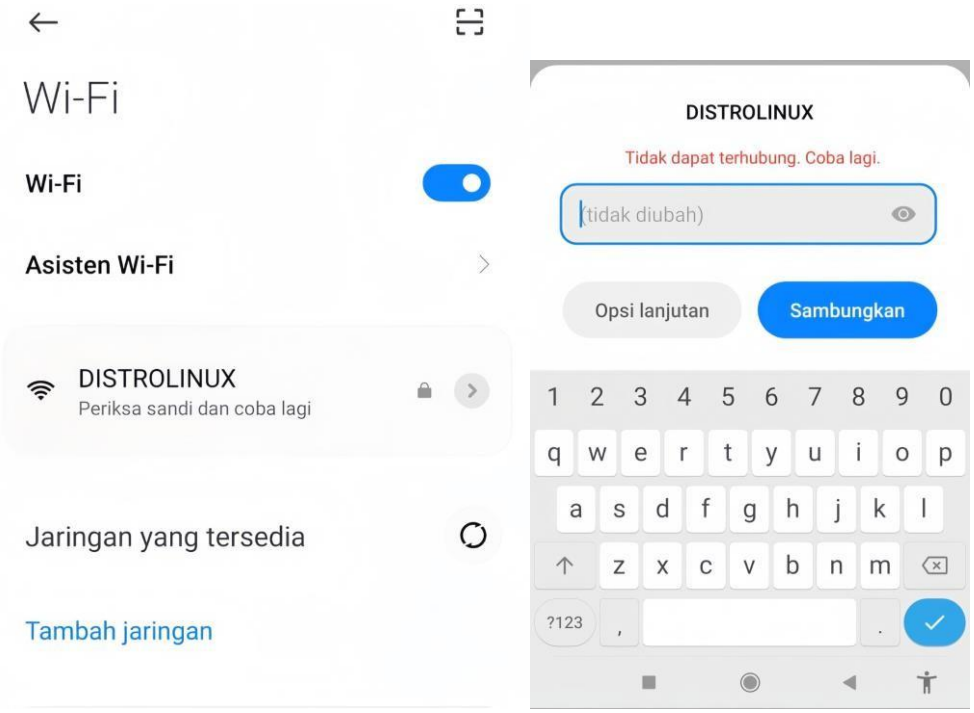
Proses yang dilakukan adalah melakukan simulasi serangan *jammer* pada jaringan *wireless* dengan menggunakan *Tools Fluxion.* Pada tahap ini perangkat penyerang memancarkan sinyal interfrensi untuk mengganggu koneksi antara klien dan *accest point* (AP). Proses ini adalah inti dari pengujian, di mana dampak serangan terhadap jaringan dieksplorasi. Berikut ini adalah prosesnya:



Gambar 7. Simulasi Penyerangan



Gambar 8. Pemisahan Klien



Gambar 9. Klien terputus

Pada Gambar 7, Dilakukan scanning ke jaringan *wireless* yang dipilih untuk melakukan simulasi penyerangan.Lalu Gambar 8, mengirimkan paket serangan ke klien dan titik akses point yang diserang. Dan Gambar 9, memperlihatkan bahwa klien sudah terputus dari Titik *Accest Point* (AP) dan sudah tidak dapat terhubung.

3. Output

Output kinerja jaringan dari penelitian ini menggambarkan bagaimana performa jaringan berubah sebelum, selama, dan setelah serangan jamming. Sebelum serangan, jaringan biasanya stabil dengan kecepatan dan koneksi yang andal. Namun, saat serangan jamming terjadi, performa jaringan menurun drastis, menyebabkan gangguan signifikan seperti penurunan kecepatan transfer, Pemutusan koneksi Accest Point(AP), Bahkan kehilangan data. Setelah serangan dihentikan, jaringan mulai pulih, tetapi pemulihan mungkin tidak langsung, dan beberapa dampak dari serangan Masih dapat dirasakan. Analisis ini menyoroti pentingnya strategi mitigasi untuk menjaga keamanan dan keandalan jaringan *wireless* dalam menghadapi serangan jamming. Dan Untuk mendeteksi dan mengatasi serangan *Jammer* pada jaringan *wireless* adalah dengan cara memperhatikan tanda-tanda seperti penurunan kecepatan internet atau seringnya koneksi terputus, serta menggunakan aplikasi pemantauan jaringan untuk mendeteksi interferensi. Jika terdeteksi, bisa mengubah saluran *Wi-fi*, memperkuat sinyal dengan penguat sinyal, atau menggunakan antena terarah untuk fokus pada sinyal yang lebih kuat.

Mengamankan jaringan dengan enkripsi kuat seperti WPA3, menggunakan VPN, dan menjaga router di tempat yang aman juga dapat membantu melindungi jaringan dari serangan jamming.

Kesimpulan

Teknologi nirkabel telah menjadi bagian penting dalam kehidupan modern, namun rentan terhadap serangan gangguan seperti jamming. Penelitian ini mengeksplorasi dampak serangan jamming pada jaringan *wireless* dengan menggunakan metode *Penetration Testing*. Melalui simulasi jaringan WPA *Key* dan pemanfaatan *Tools Fluxion* pada sistem operasi Linux, studi ini mengidentifikasi kerentanan jaringan terhadap gangguan sinyal. Hasil penelitian menunjukkan bahwa serangan jamming dapat menyebabkan penurunan kinerja jaringan, seperti kecepatan dan stabilitas koneksi. Berdasarkan temuan ini, penelitian memberikan rekomendasi untuk meningkatkan keamanan jaringan nirkabel, sehingga dapat meminimalisir dampak negatif dari serangan jamming.

Daftar Pustaka

[1] F. Tan, J. B. Budiman, dan Skynyrd, "Perbandingan Perkembangan Teknologi Berbasis Nirkabel di Daerah Pelosok dan Daerah Kota," *Jurnal Sains, Nalar, dan Aplikasi Teknologi Informasi*, vol. 2, no. 2, hlm. 25–31, Sep 2023, doi: 10.20885/snati.v2i2.23.

[2] S. Danuasmo, N. Nazuarsyah, dan R. B. Ginting, "Rancang Bangun Jaringan Wireless Lan Dan Internet Berbasis Cloud Pada Universitas Bina Bangsa Getsempena," *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, vol. 7, no. 1, hlm. 15–24, 2023.

[3] F. P. E. Putra, Moh. Riski, M. S. Yahya, dan Moh. H. Ramadhan, "Mengenal Teknologi Jaringan Nirkabel Terbaru Teknologi 5G," *Jurnal Sistim Informasi dan Teknologi*, vol. 5, no. 2, hlm. 167–174, 2023, doi: 10.37034/jsisfotek.v5i1.233.

[4] G. A. N. Pongdatu, A. Michael, dan E. E. Patalo, "Analisis Keamanan Jaringan Wireless menggunakan Metode Penetration Testing di SMK Xyz Tana Toraja," *INFINITY: UKI Toraja Journal of Information Technology*, vol. 2, no. 2, hlm. 17–23, 2022.

[5] A. Faidlatul Habibah dan I. Irwansyah, "Era Masyarakat Informasi sebagai Dampak Media Baru," *Jurnal Teknologi Dan Sistem Informasi Bisnis*, vol. 3, no. 2, hlm. 350–363, Jul 2021, doi: 10.47233/jteksis.v3i2.255.

[6] K. Pahlavan dan P. Krishnamurthy, "Evolution and Impact of Wi-Fi Technology and Applications: A Historical Perspective," *Int J Wirel Inf Netw*, vol. 28, no. 1, hlm. 3–19, Mar 2021, doi: 10.1007/s10776-020-00501-8.

[7] N. Sitohang, "Analisis kelemahan keamanan pada jaringan wireless," Prodi Teknik Informatika, 2020.

[8] A. Suwardi, B. F. Halawa, R. Toro, dan R. Syahputri, "Serangan Sinyal Jamming Menggunakan Wemos D1 Mini Pada Wireless IEEE 802.11 i," dalam *Prosiding Seminar Nasional Sinergitas Multidisiplin Ilmu Pengetahuan dan Teknologi*, 2020, hlm. 151–160.

[9] M. Jufri dan H. Heryanto, "Peningkatan Keamanan Jaringan Wireless Dengan Menerapkan Security Policy Pada Firewall," *JOISIE (Journal Of Information Systems And Informatics Engineering)*, vol. 5, no. 2, hlm. 98–108, Des 2021, doi: 10.35145/joisie.v5i2.1759.

[10] W. Najib, S. Sulistyo, dan Widyawan, "Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things (Review on Security Threat and Solution of Internet of Things Technology)," *Jurnal Nasional Teknik Elektro dan Teknologi Informasi* |, vol. 9, no. 4, hlm. 375–384, Nov 2020.

[11] R. Ferreira, J. Gaspar, P. Sebastião, dan N. Souto, "A Software Defined Radio Based Anti-UAV Mobile System with Jamming and Spoofing Capabilities," *Sensors*, vol. 22, no. 4, 2022, doi: 10.3390/s22041487.

[12] M. Hafizh Ridwan, A. Solehudin, dan C. Rozikin, "Analisis Quality of Service (QOS) Jaringan Wireless Dengan Penerapan PCQ," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 8, no. 3, hlm. 3293–3309, Mei 2024, doi: 10.36040/jati.v8i3.9663.

[13] S. I. Jasim, O. K. Hamid, dan N. J. Alhyani, "A review of jamming attacks in wireless systems," *Int. J. Latest Technol. Eng. Manag*, vol. 8, no. 1, hlm. 16–22, 2023.

[14] R. W. Ismail dan R. Pramudita, "Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT. Puma Makmur Aneka Engineering Bekasi," *Jurnal Mahasiswa Bina Insani*, vol. 5, no. 1, hlm. 53–62, 2020.

[15] M. I. Rusdi dan D. Prasti, "Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux," *Seminar Nasional Teknologi Informasi dan Komputer*, hlm. 260–269, 2019.

[16] W. Najib, S. Sulistyo, dan Widyawan, "Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things," *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, vol. 9, no. 4, hlm. 375–

384, Des 2020, doi: 10.22146/jnteti.v9i4.539.
[17] Yudiana, A. Elanda, dan R. L. Buana, "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma Dengan Menggunakan OWASP TOP 10," *Journal of Computer Enginerring System and Science*, vol. 6, no. 2, hlm. 185–191, 2021.
[18] M. Akil, E. I. Alwi, dan S. M. Abdullah, "Analisa Keamanan Website Terhadap Serangan HTML Injection Menggunakan Metode Penetration Testing," *VARIABLE RESEARCH JOURNAL*, vol. 01, no. 1, hlm. 42–50, Apr 2024, [Daring]. Tersedia pada: https://jakartaglobe.id/
[19] Y. Mulyanto, M. T. A. Zaen, Y. Yuliadi, dan S. Sihab, "Analisis Keamanan Website SMA Negeri 2 Sumbawa Besar Menggunakan Metode Penetration Testing (Pentest)," *Journal of Information System Research (JOSH)*, vol. 4, no. 1, hlm. 202–209, Okt 2022, doi: 10.47065/josh.v4i1.2335.
[20] K. Kashyap, A. Noor, R. Saraswat, dan V. Sharma, "Learning of Penetration Testing Using Open Source Tools for Beginner," Maret 2021. doi: 10.35629/5252-031212871305.