Prosiding Seminar Hasil Penelitian Informatika dan Komputer 2025
SPINTER 2025
Vol. 2 No. 1 2025 **E-ISSN : 3031-9692**
Institut Teknologi dan Bisnis STIKOM Bali, 8 Maret 2025

Analisis Keamanan Jaringan Dengan Menggunakan Metode Penetration Testing (Studi Kasus ITB STIKOM Bali)

Ambrosius Milenius Dian Marly[1)], I Wayan Ardiyasa[2)], I Wayan Karang Utama[3)]
Teknologi Informasi[1), 2)], Sistem Informasi[3)]
Institut Teknologi dan Bisnis STIKOM Bali
Denpasar, Indonesia
e-mail: 200040010@stikom-bali.ac.id[1)], ardi@stikom-bali.ac.id[2)], karang_utama@stikom-bali.ac.id[3)]

Abstrak

Keamanan jaringan menjadi salah satu aspek krusial dalam era digital saat ini, terutama perilaku cybercrime yang membahayakan semua individu yang membuka akses dalam lingkup jaringan. Maka dari itu diperlukan cara menemukan zebuah kelemahan di dalam system web server yang dapat berakibat hacker dapat dengan mudah meretas system web server. Penelitian ini bertujuan untuk menganalisis keamanan jaringan di ITB STIKOM Bali memakai metode penetration testing, yang merupakan pendekatan denan melakukan penyerangan yang dirancang agar dapat mengidentifikasi dan mengatasi kerentanan dalam sistem jaringan. Pengujian dilakukan menggunakan alat seperti Kali Linux, Aircrack-ng, dan VirtualBox, dengan fokus pada tiga tahap utama ialah; cracking encryption, bypassing MAC Address authentication dan attacking the infrastructure. Hasil pengujian ini menunjukkan bahwa metode cracking encryption dan attacking the infrastructure berhasil dilakukan, yang mengindikasikan adanya kelemahan dalam enkripsi jaringan serta potensi serangan berbasis lalu lintas data berlebih (DDoS). Sementara itu, pengujian bypassing MAC address authentication tidak berhasil, yang menunjukkan efektivitas fitur autentikasi MAC dalam mencegah akses tidak sah.

Kata kunci: *Keamanan Jaringan, Penetration Testing, Kali Linux, Hacker, Cybercriminal*

1. Pendahuluan

Kemajuan teknologi informasi, terutama dalam jaringan komputer, telah memberikan dampak signifikan bagi kehidupan manusia. Saat ini, internet telah menjadi bagian esensial yang mendukung berbagai aktivitas sehari-hari, seperti pendidikan, hiburan, dan pekerjaan. Namun, seiring dengan meningkatnya penggunaan jaringan komputer, ancaman terhadap keamanannya juga semakin berkembang.

Di era modern ini, internet ini telah menjadi elemen penting dalam kehidupan serta gaya hidup masyarakat di berbagai belahan dunia [1]. Kemajuan teknologi informasi, terutama dalam jaringan komputer, memungkinkan transfer informasi yang berlangsung dengan cepat [2]. Cepatmya arus informasi menuntut manusia untuk dapat mengelola berbagai informasi yang tersedia guna mendapatkan data yang sesuai dengan kebutuhan [3]. Yang membuat jaringan jadi tidak konsisten dan semua perangkat yang terhubung ke dalam jaringan *router mikrotik* akan terputus secara mendadak [5].

Keamanan jaringan semakin penting seiring dengan meningkatnya jumlah data yang dipertukarkan melalui internet. Masing-masing organisasi ataupun perusahaan diwajibkan untuk terus menjaga kerahasiaan, integritas, dan keaslian data pada web server sesuai dengan standar keamanan internasional [6]. Maka dari itu butuh suatu metode untuk mengidentifikasi kelemahan pada *system web server* yang dapat berakibat para *hacker* untuk meretas sistem tersebut [8]. Semakin pesatnya perkembangan teknologi komunikasi dan informasi melalui komunikasi data nirkabel, keamanan data dalam lalu lintas jaringan *wireless LAN* menjadi semakin krusial dan mendapat perhatian khusus. Pada dasarnya, jaringan yang terhubung ke internet tidak sepenuhnya aman dan selalu berisiko dieksploitasi oleh peretas. [9].

Keamanan jaringan merupakan aspek yang sangat penting untuk menjaga kerahasiaan, integritas, dan ketersediaan data dalam sistem komputer. Salah satu cara untuk meningkatkan keamanan jaringan adalah dengan melakukan pengujian menggunakan metode *penetration testing*. Dalam konteks ini, ITB STIKOM Bali menjadi objek penelitian untuk menganalisis keamanan jaringan mereka. Studi ini bertujuan untuk mengidentifikasi kerentanan pada infrastruktur jaringan kampus dan memberikan rekomendasi perbaikan guna meningkatkan keamanan jaringan.

2. Metode Penelitian

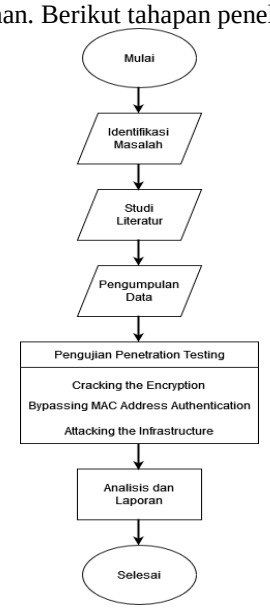
Penelitian ini menerapkan metode pengujian penetrasi untuk mengidentifikasi potensi celah keamanan yang dapat dieksploitasi [4]. Penetration testing merupakan teknik untuk menilai tingkat keamanan suatu sistem komputer atau jaringan dengan mensimulasikan serangan siber [5]. Penetrasi merupakan sebuah upaya resmi dan legal untuk mengeksploitasi sistem komputer guna mengidentifikasi kelemahan pada server web serta meningkatkan keamanan sistem [6].

Penetration testing memberikan wawasan mengenai ancaman keamanan yang nyata dan berpotensi dieksploitasi, terutama jika mencakup alur serta proses keamanan dalam organisasi [8]. Metode pengujian penetrasi yang digunakan memakai sistem operasi *Kali Linux* [9].

Metode penelitian yang digunakan dalam studi ini mencakup beberapa tahapan sebagai berikut:

2.1. Alur Penelitian

Alur penelitian meliputi tahapan mulai dari identifikasi masalah hingga pelaporan hasil, disajikan dalam diagram yang memudahkan pemahaman. Berikut tahapan penelitian yang akan dilaksanakan:



Gambar 1. Alur Penelitian

a. Identifikasi Masalah
Tahap ini melibatkan identifikasi permasalahan yang ada terkait keamanan jaringan di ITB STIKOM Bali. Permasalahan dirumuskan untuk memberikan arah dan tujuan penelitian.

b. Studi Literatur
Mengkaji teori, jurnal, dan penelitian sebelumnya yang relevan untuk memperkuat landasan penelitian serta memperluas wawasan mengenai metode yang akan digunakan, khususnya metode *penetration testing*.

c. Pengumpulan Data
Data yang telah dikumpulkan lewat observasi dan wawancara dengan pihak yang terkait. Observasi dilakukan dengan mempelajari infrastruktur jaringan di ITB STIKOM Bali, sedangkan wawancara dilakukan dengan *administrator* jaringan untuk mendapatkan informasi tambahan.

d. Pengujian *Penetration Testing*
Penelitian menggunakan metode *penetration testing* untuk menganalisis kerentanan jaringan. Pengujian melibatkan beberapa tahap:
   1) *Cracking the Encryption*: Mencoba menembus enkripsi jaringan untuk mengevaluasi keamanannya.
   2) *Bypassing MAC Address Authentication*: Menguji kerentanan sistem terhadap penggantian *MAC Address*.
   3) *Attacking the Infrastructure*: Simulasi serangan terhadap infrastruktur jaringan untuk mengidentifikasi potensi ancaman.

e. Analisis dan Pelaporan

Pada tahap ini akan dilakukan analisa dari hasil pengujian dari tahap sebelumnya akan dianalisis dan dirangkum dalam sebuah laporan.

2.2. Perangkat yang Digunakan

Penelitian ini menggunakan kombinasi hardware dan software, untuk melakukan analisis keamanan jaringan. Perangkat yang dipakai meliputi hal-hal berikut:

a. Perangkat Keras (*Hardware*)

Perangkat keras yang dibutuhkan dalam penelitian ini tercantum dalam tabel dibawah ini:

Tabel 1. Perangkat Keras (*Hardware*)

No.	Perangkat Keras	Spesifikasi	Keterangan
1	Laptop	Laptop	*ASUS X441M*
		CPU	*Intel Celeron N4020, up to 2.8 GHz*
		RAM	*4 GB*
		HDD	*1 TB*
2	*Wireless USB Adapter*	*Interface*	*USB 2.0*
		Frequency	*2.400-2.4835GHz*
		Security	*WEP, WPA/WPA2, WPA-PSK,/WPA2-PSK*

b. Perangkat Lunak (*Software*)

Perangkat lunak yang dibutuhkan dalam penelitian ini tercantum dalam tabel berikut:

Tabel 2. Perangkat Lunak (*Software*)

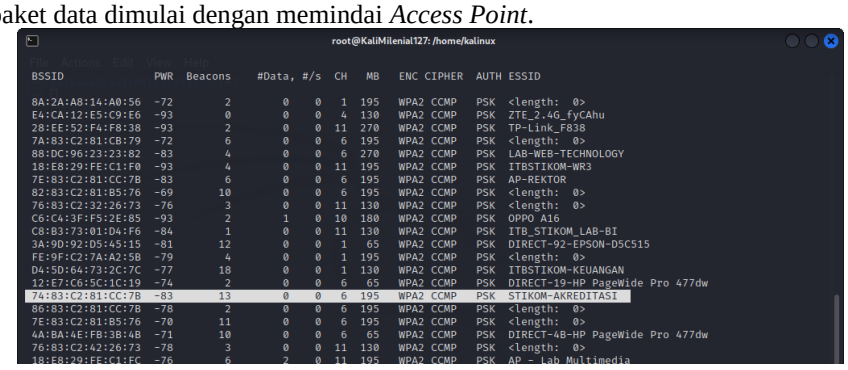
No.	Perangkat Lunak	Fungsi
1	Sistem Operasi Windows	Sebagai pengelola dan mengatur sumber daya komputer seperti *CPU, RAM,* dan *Hard Disk*
2	*VirtualBox*	Menjadi *Virtualisasi System*
3	*Aircrack-ng*	Menjadi *Tools* untuk Menjalankan *Eksploitasi*
4	*Airodump-ng*	Mengumpulkan Data Serangan Jaringan yang Dilindungi *WPA2*
5	*Aireplay-ng*	Mengirimkan Paket *deauth* ke Perangkat Dalam Jaringan *Wi-Fi*
6	*Macchanger*	Menjadi *Tools* untuk Menggantikan *MAC Address* Sementara
7	*DDoS Attack*	Mengirim Paket ke Server Secara Banyak

3. Hasil dan Pembahasan

Penelitian ini dilaksanakan untuk mengidentifikasi celah keamanan pada jaringan ITB STIKOM Bali menggunakan metode *Penetration Testing*. Jadi perlu dilakukan tiga tahap utama dalam pengujian kali ini yaitu:

3.1 *Cracking the Encryption*

Pada tahap awal, penulis memakai perangkat lunak *aircrack-ng* untuk mengaktifkan *mode monitoring* dan mengumpulkan *MAC Address*. Alat *aircrack-ng* untuk mengidentifikasi dan mengumpulkan paket data dimulai dengan memindai *Access Point*.

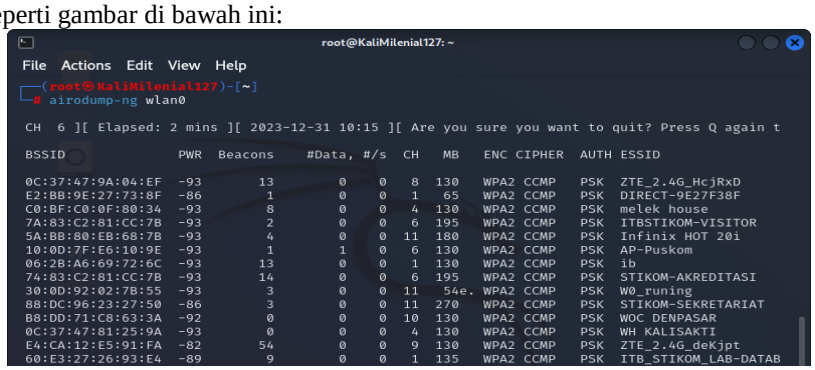


Gambar 2. Proses *Scanning*

Gambar di atas menunjukkan proses *scanning* yang dilakukan terhadap jaringan "ITB STIKOM Bali", dimana data paket yang dikumpulkan akan menjadi dasar untuk tahap selanjutnya. Hasil dari

scanning ini menunjukkan data mentah berhasil dikumpulkan dan siap untuk *didekripsi*, menyoroti potensi kelemahan dalam *mekanisme enkripsi*.

Untuk melakukan *handshake*, gunakan *tools airodump-ng wlan0*. Jika betul, muncul tampilan *mode handshake* seperti gambar di bawah ini:



Gambar 3. *Mode Handshake*

3.2 *Bypassing MAC Address Authentication*

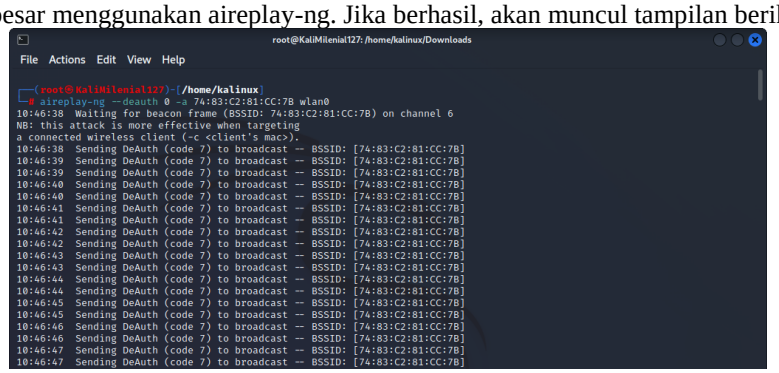
Tahap kedua berfokus pada evaluasi efektivitas *MAC address filtering* di jaringan "ITB STIKOM Bali". Proses ini untuk memantau lalu lintas jaringan dan mengidentifikasi *MAC Address* dari perangkat yang aktif dalam jaringan.

Gambar 4. *Bypassing MAC Address*

Gambar di atas menampilkan bagaimana *MAC Address* dari jaringan "ITB STIKOM Bali" tidak berhasil digunakan untuk melewati *filter MAC*. Hasil pengujian menunjukkan bahwa *MAC filtering* yang diterapkan cukup kuat untuk mencegah akses yang tidak sah.

3.3 *Attacking the Infrastructure*

Pada tahap ini, akan dilakukan serangan DDoS, yaitu suatu bentuk serangan dengan membanjiri lalu lintas jaringan melalui pengiriman sejumlah besar paket data. Penulis akan mencoba mengirimkan paket dalam jumlah besar menggunakan aireplay-ng. Jika berhasil, akan muncul tampilan berikut:



Gambar 5. *Serangan DOS* (*Denial of Service*)

Gambar di atas mengilustrasikan serangan *DoS* yang diterapkan pada jaringan "ITB STIKOM Bali", dimana serangan ini berhasil memutuskan koneksi perangkat lain yang terhubung. Pengujian ini memungkinkan gangguan signifikan.

Penetration Testing yang diterapkan memberikan wawasan mengenai kelemahan yang ada dalam sistem keamanan jaringan. Tabel di bawah ini menyajikan hasil dari metode *Penetration Testing* yang digunakan, memberikan gambaran umum mengenai temuan dan potensi risiko yang diidentifikasi selama evaluasi jaringan ini.

Tabel 3. Hasil Pengujian

Jenis Serangan	Informasi yang Diperlukan	Keterangan
Cracking the Encryption	*Database Password*, *Handshake*, *Channel* dan *MAC Address* yang Digunakan *Access Point*	Berhasil
Bypassing MAC Address Authentication	*List User* Dalam Jaringan yang Sama	Gagal
Attacking the Infrastructure	*WPA Key* Hasil *Attacking WPA Key*	Berhasil

4. Kesimpulan

Hasil penelitian menunjukkan bahwa sistem keamanan jaringan ITB STIKOM Bali memiliki beberapa celah yang dapat dimanfaatkan untuk serangan tertentu. Dari tiga tahap pengujian serangan pada router, hanya satu yang tidak berhasil, yaitu bypassing autentikasi MAC Address. Sementara itu, dua tahap lainnya, yakni cracking enkripsi dan menyerang infrastruktur, berhasil dilakukan. Keberhasilan serangan ini disebabkan oleh konfigurasi router yang masih menggunakan pengaturan default dari vendor, baik dalam hal kata sandi maupun firewall..

Maka dari itu, aspek keamanan pada router perlu ditingkatkan.. Pada tahap *cracking the encryption*, enkripsi jaringan berhasil ditembus, menunjukkan adanya potensi kelemahan dalam mekanisme keamanan yang diterapkan. Sementara itu, pengujian *bypassing MAC address authentication* gagal, yang mengindikasikan bahwa *filter MAC Address* cukup efektif dalam mencegah akses yang tidak sah. Namun, pada tahap *attacking the infrastructure*, serangan *DDoS* berhasil dilakukan, membuktikan bahwa infrastruktur jaringan masih rentan terhadap serangan berbasis lalu lintas data berlebih.

Daftar Pustaka

[1] I. Supratman, “Analisa Keamanan Jaringan LAN Menggunakan Snort Dengan Metode Penetration Test di Labor Teknik Informatika Universitas Islam Riau,” Universitas Islam Riau Pekanbaru, Pekanbaru, 2021. Accessed: Mar. 13, 2024. [Online]. Available: https://repository.uir.ac.id/11032/

[2] Herman, R. Umar, and A. Prasetyo Marsaid, “Analisis Keamanan Jaringan LAN Terhadap Kerentanan Jaringan Ancaman DDoS Menggunakan Metode Penetration Testing,” *JURIKOM (Jurnal Riset Komputer)*, vol. 10, no. 1, pp. 317-329, Feb. 2023. [Onine]. Avaliable: http://dx.doi.org/10.30865/jurikom.v10i1.5835

[3] R. Rachman, “Analisis Keamanan Jaringan Wireless LAN (WLAN) Dengan Metode Penetration Testing Pada PT.PLN (Persero) Sektor Pengendalian Pembangkitan Pekanbaru, ”Universitas Islam Riau Pekanbaru, Pekanbaru, 2021. Accessed: Mar. 13, 2024. [Online]. Available: http://repository.uir.ac.id/id/eprint/11034

[4] A. Kurniadi, “Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: TP-Link Archer A6),” Universitas Internasional Batam, Batam, 2021. Accessed: Mar. 13, 2024. [Online]. Available: http://repository.uib.ac.id/id/eprint/3420

[5] Y. Mulyanto and A. A. Fari, “Analisis Keamanan Login Router Mikrotik Dari Serangan Bruteforce Menggunakan Metode Penetration Testing,” *JINTEKS (Jurnal Informatika Teknologi dan Sains)*, vol. 4, no. 3, pp. 145–155, Aug. 2022, Accessed: Mar. 13, 2024. [Online]. Available: https://doi.org/10.51401/jinteks.v4i3.1897

[6] F. Fachri, A. Fadlil and I. Riadi, “Analisis Keamanan Webserver Menggunakan Penetration Test,” *Jurnal Informatika*, vol. 8, no. 2, pp. 183–190, Sep. 2021, [Online]. Available: http://ejournal.bsi.ac.id/ejournal/index.php/ji

[7] M. F. N. Fermana, “Analisis Kerentanan Keamanan Sistem Pada Windows Server 2022 Menggunakan Metode Penetration Testing Execution Standard,” Politeknik Negeri Jakarta, Jakarta, 2023. Accessed: Mar. 13, 2024. [Online].

Available:https://repository.pnj.ac.id/13642/1/Skripsi%20%20M%20Farhan%20Naufal%20Fermana.pdf
[8] M. Hasibuan and A. M. Elhanafi, "Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux Untuk Mengetahui Kerentanan Keamanan Server Dengan Metode Black Box," *Jurnal Teknik Informatika*, vol. 1, no. 4, pp. 171–177, Des. 2022, Accessed: Mar. 13, 2024. [Online]. Available: https://doi.org/10.56211/sudo.v1i4.160
[9] M. A. Adiguna and B. W. Widagdo, "Analisis Keamanan Jaringan Wpa2-Psk Menggunakan Metode Penetration Testing (Studi Kasus: Router Tp-Link Mercusys Mw302r)," *Jurnal Sistem Komputer dan Kecerdasan Buatan*, vol. 5, no. 2, pp. 1–8, Mar. 2022, Accessed: Mar. 13, 2024. [Online]. Available: https://doi.org/10.47970/siskom-kb.v5i2.268
[10] F. Setyawan, Rasyidah and H. Amnur, "Keamanan Jaringan Wireless Dengan Kali Linux," *Jurnal Ilmiah*, vol. 3, no. 1, pp. 16–22, 2022, [Online]. Available: http://jurnal-itsi.org
[11] M. I. Susanto, A. Hasad and M. A. Bakri, "Sistem Proteksi Jaringan Wlan Terhadap Serangan Wireless Hacking," *Journal of Electrical and Electronics*, vol. 7, no. 1, pp. 25–33, Mar. 2019, Accessed: Mar. 13, 2024. [Online]. Available: https://jurnal.unismabekasi.ac.id/index.php/jrec/article/download/1762/1489
[12] M. M. Ibrahim, "Analisis Keamanan Jaringan Pada Fasilitas Internet (WIFI) Kantor Pemerintahan Kota Batam Terhadap Serangan Packet Sniffing," Universitas Putera Batam, Batam, 2020. Accessed: Mar. 13, 2024. [Online]. Available: http://repository.upbatam.ac.id/2401/1/cover%20s.d%20bab%20III.pdf
[13] F. S. Laksamana, "Analisis Keamanan Jaringan Dalam Smarthome Internet of Things (IoT) Menggunakan Cisco Packet Tracer Dengan Metode Square," Universitas Islam Negeri Syarif Hidayatullah Jakarta, Jakarta, 2019. Accessed: Mar. 13, 2024. [Online]. Available: https://repository.uinjkt.ac.id/dspace/bitstream/123456789/47462/1/Fahrizal%20Satya%20Laksaman-FST.pdf
[14] R. Kurniawan, "Analisis Keamanan Fasilitas Jaringan (Wi-Fi) Terhadap Serangan Packet Sniffing Pada Protocol HTTP dan HTTPS," Universitas Islam Riau Pekanbaru, Pekanbaru, 2021. Accessed: Mar. 13, 2024. [Online]. Available: https://repository.uir.ac.id/17418/
[15] M. Akbar, T. A. Pramana, M. I, and A. Fauzi, "Analisis Keamanan Jaringan Komputer Pada Sekolah Menengah Atas Negeri 04 Bandung," *Jurnal Nasional Komputasi dan Teknologi Informasi*, vol. 4, no. 4, pp. 258–264, Aug. 2021, [Online]. Available: https://doi.org/10.32672/jnkti.v4i4.3106
[16] Y. Hae, and W. Sulistyo, "Analisis Keamanan Jaringan Pada Web Dari Serangan Sniffing Dengan Metode Eksperimen," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 8, no. 4, pp. 2095–2105, Des. 2021, [Online]. Available: https://doi.org/10.35957/jatisi.v8i4.1196
[17] Y. Novaliano, "Analisis Keamanan Jaringan Pada Layanan Internet Publik Menggunakan Metode Penetration Testing Execution Standard (PTES) (Studi Kasus: Klinik Pratama Bhakti Medika)," Univeritas Satya Negara Indonesia, Bekasi, 2020. Accessed: Mar. 13, 2024. [Online]. Available: https://repository.usni.ac.id/index.php?p=fstreampdf&fid=1097&bid=1095
[18] M. Gustiawan, R. J. Yudianto, J. Pratama, and A. Fauzi, "Implementasi Jaringan Hotspot Di Perkantoran Guna Meningkatkan Keamanan Jaringan Komputer," *Jurnal Nasional Komputasi dan Teknologi Informasi*, vol. 4, no. 4, pp. 244–247, Aug. 2021, [Online]. Available: https://doi.org/10.32672/jnkti.v4i4.3098
[19] F. Rizqi Nurdiana, I. Gunawan, R. Cahya Viollita, M. Arip Faizal, and D. Nurcahyadi, "Analisis Keamanan Jaringan Wifi Menggunakan Wireshark," *JES (Jurnal Elektro Smart)*, vol. 1, no. 1, pp. 10–13, Aug. 2021, [Online]. Available: http://searchsecurity.techtarget.com/tip/Wireshark-tutorial-
[20] Michael, I. Ruslianto, and R. Hidayati, "Analisis Perbandingan Sistem Keamanan Jaringan Wi-Fi Protected Access 2-Pre Shared Key (WPA2-PSK) Dan Captive Portal Pada Jaringan Publik Wireless," *Jurnal Komputer dan Aplikasi*, vol. 09, no. 01, pp. 108–118, Aug. 2021, [Online]. Available: http://dx.doi.org/10.26418/coding.v9i01.4590240
[21] Y. Mulyanto, Herfandi, and R. C. Kirana, "Analisis Keamanan Wireless Local Area Network (WLAN) Terhadap Serangan Brute Force Dengan Metode Penetration Testing (Studi Kasus : RS H. Lmanambai Abdulkadir)," *JINTEKS (Jurnal Informatika Teknologi dan Sains)*, vol. 4, no. 1, pp. 26–35, Feb. 2022, doi: 10.51401