KAJIAN LITERATUR ANALISIS KEAMANAN JARINGAN

Raga Sakti Pratikno [1], Cakra Trinata [2], Galuh Boy Hertantyo[3]
[1,2,3]Politeknik Pengayoman Indonesia
Alamat e-mail : [1]ragasakti59@gmail.com, [2]cakra.trinata@poltekim.ac.id,
[3]galuhboyh@poltekim.ac.id

ABSTRACT

Wireless network security is an important aspect in maintaining the operational continuity of an organization, especially with the increasing cyber threats to network infrastructure. This study aims to analyze the methods that have been used in securing Wireless Access Points (WAP) through the Systematic Literature Review (SLR) approach. The review process was carried out using the PRISMA method, which involves selecting literature based on certain inclusion criteria from various academic sources such as Google Scholar. From the selection results, 30 scientific journals were analyzed to identify the methods used in testing wireless network security. The research findings show that Penetration Testing is the most common method used in network security analysis. In addition, other techniques such as Deauthentication Attack, Port Scanning, Wardriving Attack, and Wireless Intrusion Detection System (WIDS) are also applied in various studies. The results of this review confirm that WAP security requires a comprehensive and sustainable testing strategy to anticipate evolving cyber threats.

Keywords: Network Security, Wireless Access Point, Penetration Testing, Systematic Literature Review, PRISMA.

ABSTRAK

Keamanan jaringan nirkabel merupakan aspek penting dalam menjaga kelangsungan operasional suatu organisasi, terutama dengan meningkatnya ancaman siber terhadap infrastruktur jaringan. Penelitian ini bertujuan untuk menganalisis metode yang telah digunakan dalam mengamankan Wireless Access Point (WAP) melalui pendekatan Systematic Literature Review (SLR). Proses tinjauan dilakukan dengan metode PRISMA, yang melibatkan pemilihan literatur berdasarkan kriteria inklusi tertentu dari berbagai sumber akademik seperti Google Scholar. Dari hasil seleksi, sebanyak 30 jurnal ilmiah dianalisis untuk mengidentifikasi metode yang digunakan dalam pengujian keamanan jaringan nirkabel. Temuan penelitian menunjukkan bahwa Penetration Testing merupakan metode yang paling umum digunakan dalam analisis keamanan jaringan. Selain itu, teknik lain seperti Deauthentication Attack, Port Scanning, Wardriving Attack, dan

Wireless Intrusion Detection System (WIDS) juga diterapkan dalam berbagai penelitian. Hasil tinjauan ini menegaskan bahwa keamanan WAP memerlukan strategi pengujian yang komprehensif dan berkelanjutan untuk mengantisipasi ancaman siber yang terus berkembang.

Kata kunci: Keamanan Jaringan, Wireless Access Point, Penetration Testing, Systematic Literature Review, PRISMA.

A. Pendahuluan (12 pt dan Bold)

Di era digital saat ini, jaringan nirkabel telah menjadi infrastruktur penting dalam lingkungan kantor untuk mendukung komunikasi, kolaborasi, dan produktivitas kerja. Oleh karena itu, perlindungan terhadap jaringan kantor menjadi prioritas utama untuk mencegah berbagai ancaman yang dapat mengganggu dan merugikan kantor. Serangan siber seperti peretasan, malware, ransomware, dan pencurian data dapat menargetkan jaringan kantor yang kurang terlindungi.

Keamanan jaringan dalam suatu kantor memainkan peran krusial dalam mendukung kelancaran administrasi dan menjaga stabilitas kantor tersebut. Jika sistem keamanan jaringan memiliki celah, semua informasi penting bisa jatuh ke tangan pihak yang tidak bertanggung jawab. Selain itu, serangan jaringan dapat menyebabkan gangguan operasional, kehilangan data, bahkan memperlambat kinerja pegawai.

Salah satu cara untuk melindungi keamanan jaringan yaitu menemukan celah pada jaringan nirkabel kantor dengan melakukan uji coba penyerangan terhadap jaringan nirkabel secara legal dengan mendapatkan persetujuan dari kantor tersebut. *Wireless* (nirkabel) adalah teknologi yang menghubungkan dua piranti untuk bertukar data tanpa media kabel. Adapun *Wireless Fidelity (WiFi)*, yaitu perangkat standar yang digunakan untuk komunikasi jaringan local tanpa kabel (*Wireless Local Area Network*/WLAN) yang didasari pada spesifikasi IEEE 802.11 (Samsumar, 2018). *Wireless Access Point* (WAP) merupakan perangkat jaringan yang menghubungkan perangkat-perangkat jaringan yang menuju jaringan *wireless* ataupun yang berasal dari jaringan *wireless*. Perangkat ini berfungsi sebagai *hub* atau *switch*

pada jaringan *wireless* atau nirkabel, dan saat ini ada yang dapat difungsikan sebagai *router* untuk menjembatani antar jaringan yang berbeda seperti menghubungkan jaringan lokal dengan *Internet Service Provider* (ISP)(Duskarnaen & Nurfalah, 2017).

Terdapat banyak metodologi yang dilakukan dalam melakukan uji coba penyerangan keamanan jaringan nirkabel.

B. Metode Penelitian (Huruf 12 dan Ditebalkan)

Penelitian ini melakukan survei secara menyeluruh terhadap penelitian tentang berita hoax di media sosial dan membuat protokol penelitian tinjauan sistematis dengan PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-analysis) (Moher et al., 2009). Proses ini diklasifikasikan menjadi lima tahap, yaitu: Penetapan Kriteria Kelayakan, Penetapan Sumber Informasi, Pemilihan Literatur, Pengumpulan Data, dan Pemilihan Item Data.

A. Tahap 1 : Kriteria kelayakan artikel. Ditentukan oleh Inclusion Criteria (IC), yaitu:

a. IC1: artikel harus merupakan penelitian asli yang telah dipelajari dan ditulis dalam bahasa Inggris dan Indonesia.

b. IC2: artikel diterbitkan antara tahun 2013 hingga 2025.

c. IC3: artikel bertujuan untuk menganalisis metode yang digunakan peneliti lain dalam menganalisis keamanan jaringan.

B. Tahap 2 : Penetapan sumber literatur

a. Literatur dicari pada basis data daring dengan repositori signifikan untuk studi akademis yaitu Google Scholar.

b. Pada artikel-artikel yang memenuhi syarat untuk IC, dicari juga penelitian lain yang berhubungan dengan penelitian ini.

C. Tahap 3 : Pemilihan Literatur

a. Kata Kunci penentuan pertama adalah “Keamanan Jaringan” dan “Wireless Access Point”.

b. Untuk mengeksplorasi dan memilih judul, abstrak dan artikel.

c. Kata kunci diperoleh dari hasil pencarian kelayakan kriteria yang telah ditentukan sebelumnya.

d. Baca artikel yang tidak dihilangkan dari sebelumnya tahap,

penuh atau sebagian, untuk menentukan item tersebut memenuhi syarat untuk peninjauan berikutnya.

D. Tahap 4 : Pengumpulan Data

Data dikumpulkan secara manual dengan membuat formulir ekstraksi data. Penelitian ini memfilter 18.200 jurnal berdasarkan kata kunci "Keamanan Jaringan" dan 417.000 jurnal berdasarkan kata kunci "Wireless Access Point" dari seluruh sumber dan kriteria dan seluruh artikel, 46 jurnal ilmiah layak menjadi calon referensi menurut judul dan abstrak untuk menjawab pertanyaan penelitian atau research question. Setelah dilakukan penelitian lebih lanjut, hanya terdapat 30 jurnal terpilih yang memenuhi syarat untuk penelitian ini. Tabel 1 menunjukkan data yang telah dikumpulkan.

Tabel 1. Hasil Seleksi Jurnal Penelitian

Sumber	**Kata Kunci**		**Kandidat**	**Terpilih**
	Analisis Keamanan Jaringan	***Wireless Network***		
Science Direct	3	99.315	18	0
Google Scholar	18.200	417.000	38	30
Total			**63**	**30**

SLR ini memberikan jawaban atas beberapa Research Question seperti berikut :

Tabel 2. Pertanyaan Penelitian

ID	**Pertanyaan Penelitian**	**Latar Belakang**
RQ	Metode apa yang pernah diusulkan peneliti sebelumnya untuk melakukan analisis keamanan jaringan?	Mengidentifikasi metode yang pernah digunakan oleh peneliti sebelumnya terkait analisis keamanan jaringan

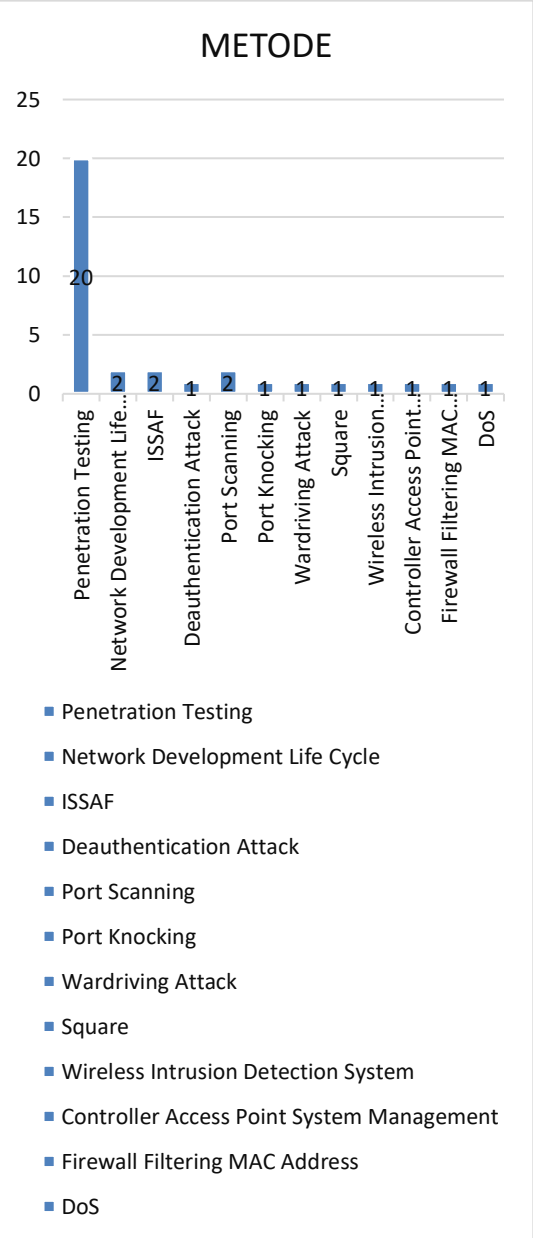
C.Hasil Penelitian dan Pembahasan (Huruf 12 dan Ditebalkan)

Tabel 3. Hasil Tinjauan Literatur

No	**Judul**	**Tahun**	**Metode**
1.	Analisa…(Hutabarat, 2020)	2019	Penetration Testing

2.	Analisis…(Kurniawan, 2015)	2015	Network Development Life Cycle
3.	Analisis…(Silmina et al, 2022)	2022	Penetration Testing & ISSAF
4.	Analisis…(Fikri & Majapahit, 2023)	2023	Deauthentication Attack
5.	Analisis…(Saputra et al., 2023)	2023	Penetration Testing
6.	Analisis…(Y, 2022)	2022	Penetration Testing
7.	Implementasi…(Rusydianto, 2017)	2017	Port Scanning
8.	Kali Linux…(Walidin, 2024)	2024	Penetration Testing
9.	Keamanan…(Rasyidah, 2022)	2022	Penetration Testing
10.	Penetration…(Quroturohman, 2020)	2020	Penetration Testing
11.	Analisis…(Albar & Putra, 2022)	2022	Port Knocking
12.	Analisis…(Okario, 2023)	2023	Penetration Testing
13.	Analisa…(Yusnanto et al., 2022)	2022	Penetration Testing
14.	Pengujian…(Dwi Purnomo & Chusyairi, 2024)	2024	Penetration Testing
15.	Analisis…(Faishol, 2024)	2024	Penetration Testing
16.	Analisis…(Samsumar & Gunawan, 2017)	2017	Penetration Testing
17.	Analisis…(Dayan et al., 2023)	2023	Penetration Testing
18.	Analisis…(Hamza et al., 2023)	2023	Penetration Testing, Wardriving Attack, dan Square
19.	Analisis…(Adiguna & Widagdo, 2022)	2022	Penetration Testing
20.	Analisis…(Kurniadi, 2021)	2021	Penetration Testing
21.	Analisis…(Fachri et al., 2021)	2021	Penetration Testing
22.	Evaluasi…(Zein, 2022)	2022	ISSAF
23.	Evaluasi…(Pujiarto & Utami, 2013)	2013	Penetration Testing
24.	Implementasi…(Gustiawan et al., 2021)	2021	Network Development Life Cycle
25.	Implementasi…(Mauluddin & Desyani, 2024)	2024	Penetration Testing
26.	Keamanan…(Santoso, 2019)	2019	Wireless Intrusion Detection System
27.	Manajemen…(Rifai & Sudibyo, 2018)	2018	Controller Access Point System Management

28.	Optimalisasi…(Purnama, 2019)	2019	Firewall Filtering MAC Address
29.	Pencegahan…(Alfian et al., 2024)	2024	Penetration Testing
30.	Analisis…(Yunanri et al., 2023)	2023	Port Scanning & DoS



Gambar 1 Tabel Hasil Analisis Metode

Langkah awal adalah melakukan analisis terhadap aspek yang dibandingkan yaitu metode analisis keamanan jaringan. Aspek tersebut merupakan Research Question yang perlu dianalisis berdasarkan alasan mengapa peneliti terdahulu menggunakan itu. Sehingga dapat dijadikan dasar yang kuat untuk melakukan analisis keamanan jaringan oleh peneliti yang akan dilaksanakan. Adapun metode yang digunakan oleh peneliti terdahulu adalah sebagai berikut:

Dari grafik tersebut, terdapat enam metode yang pernah diusulkan oleh peneliti terdahulu. Adapun metode Penetration Testing adalah metode yang paling sering digunakan peneliti terdahulu dalam analisis keamanan jaringan. Penetration Testing adalah pendekatan metode komprehensif yang digunakan dalam pengujian penetrasi untuk mengidentifikasi kerentaan dalam seluruh postur

keamanan organisasi. Tujuan dari Penetration Testing adalah untuk identifikasi kerentaan pada keamanan, evaluasi dari pengaruh control keamanan, dan menguji ketahanan sistem dari serangan.

E. Kesimpulan

Kesimpulan dari penelitian ini menunjukkan bahwa keamanan jaringan nirkabel, khususnya Wireless Access Point (WAP), merupakan aspek krusial dalam infrastruktur teknologi informasi kantor. Berdasarkan tinjauan literatur yang dilakukan, metode yang paling umum digunakan dalam analisis keamanan jaringan adalah Penetration Testing, yang bertujuan untuk mengidentifikasi kerentanan keamanan, mengevaluasi kontrol keamanan, serta menguji ketahanan sistem terhadap serangan siber.

Dari hasil penelitian sebelumnya, berbagai teknik pengujian keamanan telah diterapkan, termasuk Deauthentication Attack, Port Scanning, Wardriving Attack, serta penggunaan Wireless Intrusion Detection System (WIDS). Penelitian ini juga menegaskan pentingnya evaluasi berkala terhadap keamanan jaringan guna mengantisipasi perkembangan ancaman siber yang semakin kompleks.

Dengan demikian, penerapan metode uji keamanan yang komprehensif dan berkelanjutan sangat diperlukan untuk menjaga integritas, ketersediaan, serta kerahasiaan data dalam lingkungan jaringan nirkabel.

DAFTAR PUSTAKA

Adiguna, Mochamad Adhari, and Bambang Wisnu Widagdo. 2022. "Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus : Router Tp-Link Mercusys Mw302r)." *Jurnal SISKOM-KB (Sistem Komputer dan Kecerdasan Buatan)* 5(2):1–8. doi:10.47970/siskom-kb.v5i2.268.

Albar, Rizka, and Rian Okta Putra. 2022. "ANALISIS KEAMANAN JARINGAN MENGGUNAKAN METODE SNIFFING DAN IMPLEMENTASI KEAMANAN JARINGAN PADA MIKROTIK ROUTER OS V6.48.3 MENGGUNAKAN METODE PORT KNOCKING." 8(1).

Alfian, Alfian, Mardiana Purwaningsih, and Fandan Dwi Nugroho Wicaksono. 2024. "Pencegahan Kerentanan Keamanan Jaringan Komputer Mikrotik Menggunakan Metode Penetration Testing." *Jurnal Ilmiah FIFO* 16(2):121. doi:10.22441/fifo.2024.v16i2.003.

Dayan, Rozi, Yusuf Muhyidin, and Dayan Singasatia. 2023. "ANALISIS KEAMANAN JARINGAN PADA WIRELESS LOCAL AREA NETWORK TERHADAP SERANGAN BRUTE

FORCE MENGGUNAKAN METODE PENETRATION TESTING." *JATI (Jurnal Mahasiswa Teknik Informatika)* 7(3):2051–56. doi:10.36040/jati.v7i3.7097.

Duskarnaen, M. Ficky, and Febri Nurfalah. 2017. "Analisis, Perancangan, Dan Implementasi Jaringan Wireless Point To Point Antara Kampus A Dan Kampus B Universitas Negeri Jakarta." *PINTER : Jurnal Pendidikan Teknik Informatika dan Komputer* 1(2):134–41. doi:10.21009/pinter.1.2.6.

Dwi Purnomo, Marcell, and Ahmad Chusyairi. 2024. "Pengujian Keamanan Sistem Mengunakan Metode Penetration Testing di Website Diskominfostandi Kota Bekasi." *Sistematis : Jurnal Ilmiah Sistem Informasi* 1(1):92–101. doi:10.69533/100hxk38.

Fachri, Fahmi, Abdul Fadlil, and Imam Riadi. 2021. "Analisis Keamanan Webserver menggunakan Penetration Test." *Jurnal Informatika* 8(2):183–90. doi:10.31294/ji.v8i2.10854.

Faishol, Dimas Erisma, Triawan Adi Cahyanto, and Miftahur Rahman. 2024. "Analisis Dan Evaluasi Protokol Keamanan Jaringan Nirkabel Wi-Fi Protected Access 3 dengan Metode Penetration Testing." 9.

Fikri, Lalu Muhammad Zahirul, and Jl Majapahit. 2023. "Analisis Keamanan Jaringan Wi-Fi Dengan Metode Deauthentication Attack Pada Access point Di Lingkungan Universitas Mataram."

Gustiawan, Mokhamad, Ristu Juli Yudianto, Johanes Pratama, and Abdurahman Fauzi. 2021. "Implementasi Jaringan Hotspot Di Perkantoran Guna Meningkatkan Keamanan Jaringan Komputer." *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)* 4(4):244–47. doi:10.32672/jnkti.v4i4.3098.

Hamza, Sahriar, Nur Humaira Abri, and Abdul Haris Muhammad. 2023. "Analisis Keamanan Jaringan Wireless Lan Menggunakan Tiga Metode Penetration Testing, Wardriving Attack, And Square Studi Kasus : PT. Telekomunikasi Cabang Ternate." *Jurnal Teknik Informatika (J-Tifa)* 6(1):7–11. doi:10.52046/j-tifa.v6i2.1599.

Hutabarat, Ari Prayoga. 2020. "Analisa Dan Perancangan Keamanan Jaringan End User Dari Serangan Exploit Menggunakan Metode Penetration."

Kurniadi, Arif. 2021. "Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode PenetrationTesting(Studi Kasus : TP-Link Archer A6)." 1(1).

Mauluddin, Eka Rahmat, and Teti Desyani. 2024. "Implementasi Pengamanan Jaringan Dengan Teknik Penetration Testing Menggunakan Metode Deauther Dan Evil Twin Pada Wireless Tl-WR840N." 3(4).

Mochamad Teguh Kurniawan, Ramadhan Triyanto Prabowo. 2015. "Analisis Dan Desain Keamanan Jaringan Komputer Dengan Metode Network Development Cycle (Studi Kasus :Universitas Telkom)."

Moher, David, Alessandro Liberati, Jennifer Tetzlaff, and Douglas G. Altman. 2009. "Preferred Reporting Items for Systematic Reviews and Meta-analyses: The PRISMA Statement." *Open Medicine*.

Okario, Albert. 2023. "Analisis Celah Keamanan Jaringan WPA dan WPA2 Dengan Menggunakan Metode Penetration Testing." 1.

Prana Walidin, Adamsyach, Fahra Pebiana Putri, and Dedy Kiswanto. 2024. "KALI LINUX SEBAGAI ALAT ANALISIS KEAMANAN JARINGAN MELALUI PENGGUNAAN NMAP, WIRESHARK, DAN METASPLOIT." *JATI (Jurnal Mahasiswa Teknik Informatika)* 9(1):1188–96. doi:10.36040/jati.v9i1.12661.

Pujiarto, Bambang, and Ema Utami. 2013. "EVALUASI KEAMANAN WIRELESS LOCAL AREA NETWORK MENGGUNAKAN METODE PENETRATION TESTING (KASUS : UNIVERSITAS MUHAMMADIYAH MAGELANG)." 14(2).

Purnama, Rachmat Adi. 2019. "Optimalisasi Keamanan Jaringan Wireless Menggunakan Firewall Filtering MAC Address." 8(4).

Quroturohman, Denis. 2020. "PENETRATION TESTING DALAM FORENSIK DIGITAL PADA JARINGAN FAKULTAS TEKNIK UNIVERSITAS IBN KHALDUN BOGOR DENGAN PING OF DEATH."

Rasyidah, Fajar Setyawan, and Hidra Amnur. 2022. "Keamanan Jaringan Wireless Dengan Kali Linux." *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi* 3(1):16–22. doi:10.30630/jitsi.3.1.57.

Rifai, Bakhtiar, and Aji Sudibyo. 2018. "MANAJEMEN WIRELESS ACCESS POINT PADA HOTSPOT SERVER MENGGUNAKAN CONTROLLER ACCESS POINT SYSTEM MANAGEMENT."

Rusydianto, Muhammad Rizqi, Edy Budiman, and Hario Jati Setyadi. 2017. "IMPLEMENTASI TEKNIK HACKING WEB SERVER DENGAN PORT SCANNING DALAM SISTEM OPERASI KALI LINUX." 2(2).

Samsumar, Lalu Delsi. 2018. "PENGEMBANGAN JARINGAN KOMPUTER NIRKABEL (WiFi) MENGGUNAKAN MIKROTIK ROUTER (STUDI KASUS PADA SMA PGRI AIKMEL)." *METHODIKA: Jurnal Teknik Informatika dan Sistem Informasi* 4(1):1–9. doi:10.46880/mtk.v4i1.59.

Samsumar, Lalu Delsi, and Karya Gunawan. 2017. "ANALISIS DAN EVALUASI TINGKAT KEAMANAN JARINGAN KOMPUTER NIRKABEL (WIRELESS LAN); STUDI KASUS DI KAMPUS STMIK MATARAM." *Jurnal Ilmiah Teknologi Infomasi Terapan* 4(1). doi:10.33197/jitter.vol4.iss1.2017.152.

Santoso, Joko Dwi. 2019. "KEAMANAN JARINGAN NIRKABEL MENGGUNAKAN WIRELESS INTRUSION DETECTION SYSTEM." 1(3).

Satria Galang Saputra, Bita Parga Zen, and Abdurahman. 2023. "Analisis Keamanan Jaringan Wireless menggunakan Metode Penetration Testing Execution Standard (PTES)." *Jurnal Sistem Informasi Galuh* 1(2):43–51. doi:10.25157/jsig.v1i2.3152.

Silmina, Esi Putri, Arizona Firdonsyah, and Rovalia Adhella Attya Amanda. 2022. "ANALISIS KEAMANAN JARINGAN SISTEM INFORMASI SEKOLAH MENGGUNAKAN PENETRATION TEST DAN ISSAF." *Transmisi* 24(3):83–91. doi:10.14710/transmisi.24.3.83-91.

Y, Arya Kukuh, Geraldo Alfaren, and Indra Gunawan. 2022. "Analisis Serangan Penetration Testing: Sebuah Review Sistematik." *JIIFKOM (Jurnal Ilmiah Informatika dan Komputer)* 1(2):21–26. doi:10.51901/jiifkom.v1i2.231.

Yunanri, Yuliadi, Shinta Esabella, and Yasinta Bella Fitriana. 2023. "Analisis Keamanan Jaringan Menggunakan Metode Security Policy Development Life Cycle (SPDLC)."

Yusnanto, Tri, Muhammad Abdul Muin, and Sugeng Wahyudiono. 2022. "Analisa Infrastruktur Jaringan Wireless dan Local Area Network (WLAN) Meggunakan Wireshark Serta Metode Penetration Testing Kali Linux." *Journal on Education* 4(4):1470–76. doi:10.31004/joe.v4i4.2175.

Zein, Afrizal. 2022. "EVALUASI KEAMANAN WIRELESS LAN MENGGUNAKAN ISSAF (INFORMATION SYSTEM SECURITY ASSESSMENT FRAMEWORK)." *SAINSTECH: JURNAL PENELITIAN DAN PENGKAJIAN SAINS DAN TEKNOLOGI* 32(2):29–35. doi:10.37277/stch.v32i2.1294.