CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 8, No. 2, November 2025, hlm. 135-141

Analisis Keamanan Jaringan Wi-Fi Pada SMKN 1 Kota Jantho Menggunakan Metode *Vulnerability Assessment*

Farhan. Y[1], Aulia Syarif Aziz[2]

Email: [1]210212067@student.ar-raniry.ac.id, [2]aulia.aziz@ar-raniry.ac.id
[1,2]Universitas Islam Negeri Ar-Raniry

Abstrak

Keamanan jaringan Wi-Fi di lingkungan pendidikan memiliki peran penting dalam menjaga kerahasiaan dan integritas data. Penelitian ini bertujuan menganalisis tingkat keamanan jaringan Wi-Fi SMKN 1 Kota Jantho dengan menggunakan metode vulnerability assessment berbasis aplikasi open-source, yaitu Kismet dan Airodump-ng. Kismet digunakan untuk mendeteksi dan memantau jaringan secara pasif, sedangkan Airodump-ng berfungsi menangkap handshake WPA/WPA2 serta memantau lalu lintas jaringan secara real-time. Data hasil pemindaian dianalisis menggunakan standar CVSS (Common Vulnerability Scoring System) untuk menentukan tingkat risiko, serta dilakukan simulasi serangan deauthentication guna menguji respons jaringan. Hasil penelitian menunjukkan adanya beberapa kerentanan dengan rata-rata skor CVSS kategori High (7,58), termasuk penggunaan enkripsi lemah (WEP), layanan manajemen tidak aman (Telnet), dan potensi rogue access point. Dibandingkan dengan penelitian terdahulu, penelitian ini memberikan kontribusi praktis berupa pendekatan yang lebih sederhana, murah, dan aplikatif untuk meningkatkan keamanan Wi-Fi di sekolah, tanpa memerlukan perangkat keras khusus maupun aplikasi berlisensi. Temuan ini menegaskan bahwa kombinasi Kismet dan Airodump-ng dapat dijadikan solusi efektif dalam memetakan kerentanan serta mendukung strategi mitigasi keamanan jaringan di lingkungan pendidikan.

Kata kunci: keamanan jaringan, Wi-Fi, *vulnerability assessment*, Kismet, Airodump-ng, CVSS

Wi-Fi Network Security Analysis At SMKN 1 Kota Jantho Using The Vulnerability Assessment Method

Abstrak

Wi-Fi network security in educational environments plays a crucial role in maintaining data confidentiality and integrity. This study aims to analyze the security level of the Wi-Fi network at SMKN 1 Kota Jantho using a vulnerability assessment approach based on open-source applications, namely Kismet and Airodump-ng. Kismet was employed to detect and passively monitor wireless networks, while Airodump-ng was used to capture WPA/WPA2 handshakes and observe network traffic in real-time. The collected data were evaluated using the Common Vulnerability Scoring System (CVSS) to determine risk levels, and a deauthentication attack simulation was conducted to assess the network's resilience. The results revealed several vulnerabilities with an average CVSS score in the High category (7.58), including the use of weak encryption (WEP), insecure management services (Telnet), and the potential for rogue access points. Compared to previous studies, this research provides a practical contribution by offering a simpler, cost-effective, and applicable approach to improving Wi-Fi security in schools without requiring specialized hardware or licensed software. These findings highlight that the combination of Kismet and Airodump-ng can serve as an effective solution for mapping vulnerabilities and supporting security mitigation strategies in educational environments.

Keywords: *network security, Wi-Fi, vulnerability assessment, Kismet, Airodump-ng, CVSS*

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah menjadikan jaringan nirkabel (*wireless network*) sebagai salah satu infrastruktur utama dalam mendukung aktivitas di berbagai sektor, termasuk dunia pendidikan. Wi-Fi menjadi media konektivitas yang efisien dan fleksibel, sehingga banyak digunakan di sekolah untuk menunjang proses belajar-mengajar. Namun, kemudahan akses ini juga membuka potensi kerentanan keamanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab, seperti pencurian data, penyusupan jaringan, atau sabotase layanan. Oleh karena itu, pengujian keamanan jaringan melalui *vulnerability assessment* menjadi langkah penting dalam menjaga integritas, kerahasiaan, dan ketersediaan layanan jaringan sekolah.

Berbagai perangkat lunak telah dikembangkan untuk membantu proses *vulnerability assessment*, di antaranya *Kismet* dan *Airodump-ng*. *Kismet* merupakan aplikasi sumber terbuka yang mampu mendeteksi, memantau, dan menganalisis jaringan Wi-Fi secara pasif, menampilkan informasi detail mengenai *SSID*, *BSSID*, jenis enkripsi, kekuatan sinyal, dan perangkat klien yang terhubung. Sementara itu, *Airodump-ng*, yang merupakan bagian dari paket Aircrack-ng, digunakan untuk memantau lalu lintas jaringan secara real-time dan menangkap data seperti *handshake* WPA/WPA2 untuk analisis keamanan lanjutan.

Penelitian ini bertujuan untuk menguji keamanan jaringan Wi-Fi di SMKN 1 Kota Jantho menggunakan *Kismet* dan *Airodump-ng*, serta membandingkan efektivitas keduanya dalam mengidentifikasi potensi kerentanan. Analisis dilakukan dengan mengacu pada standar *CVSS* (*Common Vulnerability Scoring System*) untuk menentukan tingkat keparahan risiko yang ditemukan. Selain itu, dilakukan simulasi serangan ringan berupa *deauthentication attack* untuk menilai respons jaringan terhadap upaya pemutusan koneksi klien. Hasil penelitian diharapkan dapat memberikan rekomendasi praktis dalam meningkatkan keamanan jaringan Wi-Fi di lingkungan sekolah.

2. METODOLOGI

Penelitian ini menggunakan metode *vulnerability assessment* untuk mengidentifikasi potensi kerentanan pada jaringan Wi-Fi SMKN 1 Kota Jantho. Tahapan penelitian diawali dengan persiapan perangkat keras berupa laptop yang telah terpasang sistem operasi *Kali Linux* dan mendukung mode *monitor* pada antarmuka nirkabel (*wlan0*). Perangkat lunak yang digunakan meliputi *Kismet* dan *Airodump-ng* sebagai alat utama pemantauan dan analisis jaringan. *Kismet* digunakan untuk melakukan deteksi dan analisis jaringan Wi-Fi

secara pasif, mencatat detail seperti *SSID*, *BSSID*, jenis enkripsi, kekuatan sinyal, dan perangkat klien yang terhubung. Sementara itu, *Airodump-ng* digunakan untuk memantau lalu lintas jaringan secara real-time dan menangkap *handshake* WPA/WPA2 untuk analisis keamanan lanjutan.

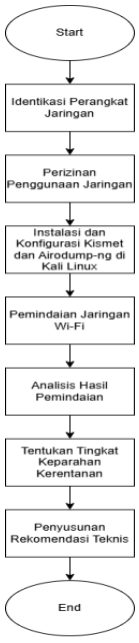
Metode Vulnerability Assessment (VA) dipilih dalam penelitian ini karena mampu mengidentifikasi kelemahan jaringan secara sistematis dengan risiko minimal terhadap stabilitas sistem. Pendekatan ini sangat relevan untuk lingkungan pendidikan, di mana keterbatasan sumber daya dan kebutuhan akan kestabilan layanan Wi-Fi menjadi faktor utama. Secara ilmiah, VA menyediakan pemetaan kerentanan berdasarkan standar internasional seperti CVSS (Common Vulnerability Scoring System) sehingga hasilnya dapat diukur, dibandingkan, dan digunakan sebagai dasar rekomendasi mitigasi.

Jika dibandingkan dengan metode yang lebih baru seperti Penetration Testing, VA lebih aman diterapkan karena penetration testing berfokus pada eksploitasi nyata yang berpotensi mengganggu layanan jaringan dan menimbulkan risiko downtime. Sementara itu, Threat Hunting yang saat ini juga mulai populer membutuhkan infrastruktur pemantauan canggih, analisis log secara real-time, dan keahlian tingkat lanjut, sehingga sulit diimplementasikan pada sekolah dengan keterbatasan teknis maupun biaya. Dengan demikian, meskipun VA sudah sering digunakan, alasan ilmiah pemilihannya dalam penelitian ini adalah karena VA tetap menawarkan keseimbangan antara akurasi deteksi, keamanan proses pengujian, dan keterjangkauan sumber daya, khususnya pada konteks pendidikan menengah.

Agar metodologi penelitian ini dapat diadopsi di tempat lain, maka langkah-langkah penerapannya dapat dijadikan panduan praktis. Tahap pertama adalah persiapan lingkungan uji, yaitu menentukan lokasi jaringan Wi-Fi yang akan dianalisis dengan terlebih dahulu memperoleh izin resmi dari administrator jaringan, serta menyiapkan perangkat laptop berbasis Linux yang dilengkapi adaptor Wi-Fi dengan dukungan mode monitor. Selanjutnya dilakukan instalasi dan konfigurasi aplikasi open-source, yaitu Kismet untuk monitoring jaringan secara pasif dan Airodump-ng untuk akuisisi data teknis seperti handshake WPA/WPA2. Setelah itu, proses pengujian dilaksanakan dengan menjalankan Kismet untuk memetakan SSID, BSSID, channel, jenis enkripsi, dan perangkat yang terhubung, kemudian menggunakan Airodump-ng untuk menangkap handshake serta mencatat aktivitas jaringan. Pada tahap ini juga dapat dilakukan simulasi serangan terbatas, misalnya deauthentication, untuk menguji respons jaringan tanpa mengganggu layanan utama.

Data yang diperoleh kemudian dianalisis dengan mengevaluasi hasil tangkapan dari Kismet maupun Airodump-ng untuk mengidentifikasi kelemahan enkripsi, autentikasi, maupun layanan terbuka. Setiap kerentanan yang ditemukan diberi skor tingkat risiko menggunakan Common Vulnerability Scoring System (CVSS) agar hasilnya dapat terukur dan terstandarisasi. Tahap terakhir adalah menyusun rekomendasi teknis, seperti migrasi ke WPA3, menonaktifkan port yang tidak aman, memperbarui firmware perangkat, serta melakukan monitoring berkala. Dengan demikian, metodologi ini tidak hanya relevan pada studi kasus di SMKN 1 Kota Jantho, tetapi juga dapat direplikasi di sekolah, kampus, maupun institusi lain dengan sumber daya terbatas. Hal ini menunjukkan bahwa penelitian ini menghadirkan kerangka kerja praktis berbasis aplikasi open-source yang dapat diimplementasikan secara efektif dan terjangkau dalam meningkatkan keamanan jaringan Wi-Fi.

Proses penelitian dimulai dengan instalasi dan konfigurasi kedua aplikasi pada perangkat uji, dilanjutkan dengan mengaktifkan antarmuka nirkabel pada mode *monitor* untuk memungkinkan penangkapan paket data. Pemindaian dilakukan dengan menangkap sinyal Wi-Fi pada area jaringan sekolah, kemudian menganalisis hasil tangkapan untuk mengidentifikasi potensi kerentanan, seperti penggunaan enkripsi yang lemah, keberadaan *access point* ilegal, atau konfigurasi keamanan yang tidak memadai. Data yang diperoleh dari kedua aplikasi selanjutnya dianalisis dan diklasifikasikan berdasarkan standar *CVSS* (*Common Vulnerability Scoring System*) untuk menentukan tingkat keparahan risiko. Selain itu, dilakukan simulasi serangan ringan berupa *deauthentication attack* dengan tujuan memutus koneksi perangkat klien dari jaringan, guna menguji respons jaringan terhadap potensi ancaman tersebut. Hasil dari tahapan ini menjadi dasar dalam penyusunan rekomendasi teknis untuk mitigasi risiko keamanan jaringan Wi-Fi.



Gambar 1. Flowchart alur penelitian

Rancangan penelitian diawali dengan tahap persiapan yang mencakup identifikasi perangkat jaringan yang akan dipindai dan perizinan penggunaan jaringan untuk keperluan penelitian. Setelah itu, dilakukan instalasi dan konfigurasi *Kismet* dan *Airodump-ng* melalui sistem operasi *Kali Linux* pada perangkat yang akan digunakan untuk pemindaian. Tahap selanjutnya adalah melakukan pemindaian jaringan Wi-Fi di SMKN 1 Kota Jantho untuk mengidentifikasi kerentanan. Hasil pemindaian kemudian dianalisis untuk menentukan tingkat keparahan setiap kerentanan yang ditemukan. Berdasarkan hasil analisis, dibuat rekomendasi teknis untuk meningkatkan keamanan jaringan.

3. KAJIAN PENELITIAN TERDAHULU

Beberapa penelitian di Indonesia telah dilakukan untuk menganalisis keamanan jaringan Wi-Fi dengan pendekatan dan aplikasi yang berbeda. Hermaduanti (2016) melakukan penelitian mengenai Pengembangan Framework Otomatisasi Mitigasi Kasus Rogue Access Point Pada Jaringan Wireless IEEE 802.1X dengan memanfaatkan Wireshark sebagai tools utama. Penelitian ini berfokus pada analisis paket hasil capture untuk mendeteksi keberadaan rogue access point serta merancang framework mitigasi otomatis guna meningkatkan keamanan jaringan nirkabel. Berbeda dengan penelitian ini, Pamungkas (2021) menggunakan Wireshark untuk menganalisis Quality of Service (QoS) pada jaringan internet berbasis wireless LAN layanan Indihome di Asrama Banten. Fokus penelitian tersebut lebih mengarah pada evaluasi performa jaringan berdasarkan parameter delay, jitter, throughput, dan packet loss sebagai indikator stabilitas serta keamanan jaringan. Sementara itu, Satria (2014) mengembangkan perangkat Wireless Intrusion Detection System (IDS) berbasis embedded system pada studi kasus di Badan Narkotika Nasional. Dalam penelitiannya, Wireshark digunakan untuk menganalisis paket data yang diterima oleh perangkat, sehingga menghasilkan prototipe IDS berbasis hardware yang mampu mendeteksi serangan terhadap jaringan Wi-Fi.

Jika dibandingkan dengan penelitian-penelitian tersebut, penelitian ini memiliki persamaan dalam hal fokus kajian, yaitu sama-sama menyoroti aspek keamanan jaringan nirkabel dengan memanfaatkan tools open-source untuk proses analisis. Namun, terdapat perbedaan dari sisi pendekatan maupun output yang dihasilkan. Hermaduanti lebih menitikberatkan pada mitigasi otomatis terhadap rogue access point, Pamungkas menekankan pada analisis kualitas layanan (QoS) jaringan, dan Satria menghasilkan prototipe perangkat IDS berbasis embedded system. Penelitian ini sendiri mengambil pendekatan berbeda dengan menggunakan kombinasi Kismet dan Airodump-ng, yang berfungsi saling melengkapi antara monitoring pasif dan akuisisi paket handshake WPA/WPA2. Dengan demikian, penelitian ini berkontribusi pada penguatan studi keamanan jaringan Wi-Fi di Indonesia dengan pendekatan teknis yang lebih terfokus pada proses deteksi kerentanan dan uji penetrasi enkripsi jaringan.

4. PEMBAHASAN

Hasil penelitian ini menunjukkan bahwa penggunaan aplikasi *Kismet* dan *Airodump-ng* mampu memberikan gambaran keamanan jaringan Wi-Fi secara komprehensif. Kismet lebih unggul dalam menampilkan informasi terstruktur dan mudah dipahami, sedangkan Airodump-ng berfungsi baik untuk menangkap data teknis seperti handshake

WPA/WPA2 yang penting dalam analisis keamanan. Temuan ini memiliki keterkaitan dengan penelitian Hermaduanti (2016) yang menggunakan Wireshark untuk mendeteksi *rogue access point* pada jaringan IEEE 802.1X. Meskipun fokus penelitian Hermaduanti lebih kepada pembuatan framework mitigasi otomatis, hasil penelitian ini memperkuat temuan tersebut dengan menunjukkan bahwa kombinasi Kismet dan Airodump-ng juga efektif dalam mendeteksi ancaman, khususnya serangan deauthentication yang berpotensi digunakan untuk penyusupan jaringan.

Perbandingan juga dapat dilihat dengan penelitian Pamungkas (2021) yang menekankan pada analisis *Quality of Service* (QoS) jaringan Wi-Fi berbasis parameter delay, jitter, throughput, dan packet loss. Walaupun keduanya menggunakan aplikasi analisis jaringan, penelitian Pamungkas lebih berorientasi pada aspek performa layanan, sedangkan penelitian ini berfokus pada aspek kerentanan enkripsi dan autentikasi yang berhubungan langsung dengan keamanan jaringan. Dengan demikian, penelitian ini melengkapi penelitian Pamungkas dengan menegaskan bahwa kualitas layanan yang baik tetap harus disertai dengan pengujian kerentanan keamanan untuk mencegah potensi kebocoran data.

Selanjutnya, penelitian ini juga memiliki benang merah dengan penelitian Satria (2014) yang mengembangkan perangkat *Wireless Intrusion Detection System (IDS)* berbasis embedded system untuk mendeteksi serangan jaringan Wi-Fi. Bedanya, penelitian Satria menekankan pembangunan perangkat keras khusus, sedangkan penelitian ini memanfaatkan aplikasi open-source yang lebih mudah diimplementasikan di sekolah atau laboratorium dengan sumber daya terbatas. Hal ini menunjukkan bahwa penelitian ini memberikan kontribusi praktis berupa solusi murah dan efisien, yang sekaligus memperkuat literatur terdahulu dalam upaya peningkatan keamanan jaringan nirkabel.

Secara keseluruhan, hasil penelitian ini tidak hanya mengonfirmasi temuan-temuan sebelumnya mengenai pentingnya deteksi ancaman pada jaringan Wi-Fi, tetapi juga menambahkan perspektif baru bahwa kombinasi aplikasi Kismet dan Airodump-ng dapat menjadi alternatif yang praktis, ekonomis, dan efektif dalam mendukung strategi mitigasi keamanan jaringan, khususnya di lingkungan pendidikan.

Setelah dilakukan pengujian Analisis kemanan jaringan Wi-Fi di SMKN 1 Kota Jantho dan juga dilakukan penyerangan *deauth*. Maka *Kismet* dan *Airodump-ng* mendeteksi adanya serangan secara otomatis pada Wi-Fi yang terpantau oleh aplikasi *Kismet* dan *Airodump-ng*.

4.1. Perbandingan Hasil Penggunaan Aplikasi *Kismet* dan *Airodump-ng*

Berdasarkan hasil pengujian teknis, *Kismet* dan *Airodump-ng* sama-sama terbukti efektif dalam melakukan *vulnerability assessment* jaringan Wi-Fi di SMKN 1 Kota Jantho, namun masing-masing memiliki keunggulan yang berbeda. *Kismet* lebih unggul dalam aspek pemantauan visual dan deteksi ancaman secara real-time, dengan indikator yang jelas seperti peringatan warna merah dan notifikasi *alert* saat terjadi serangan, serta kemampuan mendeteksi *rogue access point* dan *SSID* tersembunyi. Hal ini sesuai dengan preferensi administrator jaringan yang cenderung lebih memilih *Kismet* karena kemudahan identifikasi ancaman dan efektivitasnya dalam memberikan gambaran menyeluruh kondisi jaringan. Sementara itu, *Airodump-ng* lebih unggul dalam aspek teknis pengambilan data mentah, seperti penangkapan *handshake*, informasi detail *SSID*/*BSSID*, *channel*, kekuatan sinyal, dan daftar klien yang terhubung. Keunggulan ini menjadikan *Airodump-ng* sangat berguna dalam analisis lanjutan, misalnya untuk *password cracking* atau pengujian keamanan enkripsi. Meskipun kedua aplikasi memberikan hasil yang saling melengkapi sedangkan *Airodump-ng* digunakan pada situasi yang memerlukan analisis mendalam atau pengujian spesifik. Dengan demikian, kombinasi keduanya dinilai memberikan cakupan keamanan yang optimal, di mana *Kismet* berperan sebagai sistem deteksi dini, dan *Airodump-ng* sebagai alat analisis teknis yang lebih detail.

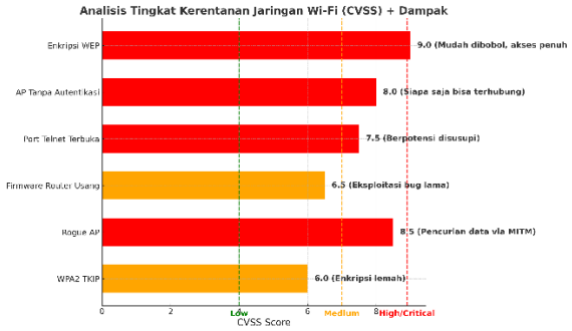
Berikut merupakan perbandingan kedua aplikasi

1. *Kismet* berfungsi untuk mendeteksi, memantau, dan menganalisis jaringan Wi-Fi secara pasif dengan visualisasi real-time, serta mampu mendeteksi *SSID* tersembunyi dan rogue access point melalui tampilan GUI yang interaktif dan notifikasi visual. Keunggulan lainnya adalah kemampuannya memonitor banyak jaringan secara bersamaan tanpa mengganggu koneksi, namun memiliki kelemahan berupa detail teknis yang tidak sedalam *Airodump-ng* serta konfigurasi awal yang cukup kompleks.
2. *Airodump-ng* digunakan untuk pemindaian mendalam dan penangkapan paket (packet capture) untuk analisis teknis, seperti menampilkan informasi lengkap tentang *SSID*, *BSSID*, channel, dan kekuatan sinyal, serta mampu menangkap handshake WPA/WPA2. Keunggulannya adalah proses yang ringan dan cepat, cocok untuk pengujian lanjutan maupun pengujian enkripsi, namun tidak memiliki alert otomatis seperti *Kismet* dan antarmuka CLI yang kurang ramah untuk pengguna non-teknis.

4.2. Analisis Keamanan Jaringan Wi-Fi Berdasarkan *CVSS*

Berdasarkan pemindaian menggunakan *Kismet* dan *Airodump-ng*, serta simulasi serangan *deauthentication* dan identifikasi layanan router, ditemukan sejumlah kerentanan pada jaringan Wi-Fi SMKN 1 Kota Jantho. Evaluasi menggunakan *CVSS*

(*Common Vulnerability Scoring System*) menunjukkan rata-rata skor berada pada kategori High (7,58), yang berarti ancaman terhadap keamanan jaringan cukup serius. Kerentanan tertinggi mencakup penggunaan enkripsi WEP, access point tanpa autentikasi, serta port Telnet terbuka. Kondisi ini menunjukkan jaringan sangat berpotensi menjadi target serangan penyadapan, pencurian kredensial, maupun pengambilalihan perangkat. Gambar 2 memperlihatkan merupakan diagram *CVSS*



Gambar 2 Diagram CVSS

1. Enkripsi WEP: 9.0 (Critical). Mudah dipecahkan menggunakan brute force, sehingga *confidentiality* dan *integrity* sangat rentan. Kerentanan ini paling berbahaya karena memungkinkan penyadapan penuh terhadap lalu lintas Wi-Fi.
2. AP Tanpa Autentikasi (Open Network): 8.0 (High). Memungkinkan siapa saja terhubung tanpa izin, sehingga rawan penyadapan (*man-in-the-middle*) dan injeksi lalu lintas berbahaya.
3. Port Telnet Terbuka: 7.5 (High). Transmisi plaintext membuat kredensial router sangat mudah dicuri.
4. Firmware Router Usang: 6.5 (Medium). Membuka peluang eksploitasi bug lama yang sudah diketahui publik. Risiko ini sedang, tetapi tetap berbahaya bila tidak segera dilakukan pembaruan.
5. Rogue AP (Evil Twin): 8.5 (High). Penyerang dapat membuat access point palsu untuk mengelabui pengguna. Jika korban tersambung, seluruh data dapat dicuri.
6. WPA2-TKIP: 6.0 (Medium). Lebih kuat dari WEP, tetapi sudah deprecated (tidak direkomendasikan IEEE sejak 2012). Lemah terhadap brute-force dan replay attack, sehingga tetap berisiko.

   Rata-rata skor CVSS: 7,58 (High), mayoritas kerentanan yang ditemukan tergolong serius sehingga perlu mitigasi segera.

4.3. Rekomendasi mitigasi:

1. Perbarui protokol enkripsi: Migrasi ke WPA3-SAE atau minimal WPA2-AES.
2. Amankan access point: Hilangkan open SSID, aktifkan PMF, rotasi password.
3. Matikan Telnet: Gunakan SSH terenkripsi dan ubah kredensial default.
4. Update firmware secara rutin: Ikuti rilis resmi vendor untuk menutup bug.
5. Pantau & blok Rogue AP: Gunakan WIDS/WIPS, whitelist SSID resmi.
6. Segmentasi jaringan: Pisahkan VLAN tamu vs internal, tambah firewall rules.
7. Edukasi pengguna: Guru & siswa diberi pelatihan singkat tentang bahaya open Wi-Fi dan pentingnya password kuat.

4.4. Diskusi dan Perbandingan Dengan Penelitian Terdahulu

Jika dilihat dari segi metode, penelitian ini menggunakan pendekatan Vulnerability Assessment dengan aplikasi Kismet dan Airodump-ng. Hal ini berbeda dengan penelitian Hermaduanti (2016) yang menerapkan analisis forensik jaringan berbasis Wireshark untuk mendeteksi *rogue access point*. Hermaduanti berfokus pada perancangan framework mitigasi otomatis, sedangkan penelitian ini lebih menekankan pada pemetaan kerentanan secara real-time dengan mengombinasikan monitoring pasif (Kismet) dan akuisisi handshake (Airodump-ng). Perbedaan signifikan di sini adalah penelitian ini menunjukkan efektivitas penggunaan aplikasi open-source yang lebih sederhana dan praktis tanpa memerlukan framework baru.

Jika dibandingkan dengan penelitian Pamungkas (2021), terdapat perbedaan orientasi hasil. Penelitian Pamungkas menggunakan Wireshark untuk mengevaluasi *Quality of Service (QoS)* jaringan (delay, jitter, throughput, dan packet loss), sehingga fokusnya pada performa layanan. Sementara itu, penelitian ini memusatkan perhatian pada aspek keamanan enkripsi dan autentikasi, yang ditunjukkan melalui temuan adanya kerentanan WEP, open network, port Telnet terbuka, serta risiko serangan deauthentication. Dengan demikian, meskipun keduanya sama-sama menilai jaringan Wi-Fi, penelitian ini memberikan kontribusi berbeda karena hasilnya lebih menyoroti sisi keamanan data dibandingkan stabilitas performa jaringan.

Perbandingan juga dapat dilihat dengan penelitian Satria (2014) yang mengembangkan prototipe Wireless Intrusion Detection System (IDS) berbasis embedded system. Hasil penelitian Satria membuktikan efektivitas IDS dalam mendeteksi serangan jaringan, namun membutuhkan perangkat keras khusus dan implementasi yang lebih kompleks. Sebaliknya, penelitian ini menunjukkan bahwa kombinasi Kismet dan Airodump-ng dapat mencapai fungsi deteksi yang serupa dengan biaya lebih rendah, mudah diimplementasikan, dan dapat langsung diaplikasikan di sekolah. Perbedaan signifikan di sini adalah penelitian ini menghadirkan solusi yang lebih terjangkau dan aplikatif, sehingga relevan untuk konteks pendidikan dengan sumber daya terbatas.

Secara keseluruhan, diskusi ini menunjukkan bahwa metode dan hasil penelitian ini melengkapi literatur yang sudah ada. Perbedaan utama dengan penelitian terdahulu terletak pada pemilihan metode (aplikasi open-source vs framework/IDS khusus) serta orientasi hasil (keamanan data vs performa layanan). Hal ini menegaskan kontribusi penelitian ini dalam menyediakan alternatif yang lebih sederhana, murah, dan efektif untuk meningkatkan keamanan jaringan Wi-Fi di lingkungan pendidikan.

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan di SMKN 1 Kota Jantho, dapat disimpulkan bahwa jaringan Wi-Fi sekolah masih memiliki sejumlah kerentanan yang cukup signifikan. Pengujian menggunakan aplikasi Kismet dan Airodump-ng berhasil mengidentifikasi kelemahan pada aspek enkripsi, autentikasi, serta layanan manajemen jaringan. Kismet menunjukkan keunggulan dalam mendeteksi perangkat dan lalu lintas jaringan secara visual dan real-time, sementara Airodump-ng lebih unggul dalam pengambilan data teknis untuk analisis lanjutan. Simulasi serangan deauthentication membuktikan bahwa jaringan rentan terhadap gangguan layanan (Denial of Service) dan berpotensi dimanfaatkan untuk pencurian data melalui handshake capture. Berdasarkan analisis tingkat risiko menggunakan CVSS, kerentanan yang ditemukan rata-rata berada pada kategori *High*, sehingga memerlukan penanganan segera.

Meskipun penelitian ini masih bersifat aplikatif dengan memanfaatkan aplikasi existing, kontribusi utama yang diberikan adalah pada penerapan praktis metode vulnerability assessment di lingkungan pendidikan menengah. Penelitian ini menunjukkan bahwa kombinasi Kismet dan Airodump-ng dapat menjadi solusi murah, efektif, dan mudah diimplementasikan untuk memetakan kerentanan jaringan Wi-Fi tanpa memerlukan perangkat keras khusus maupun biaya lisensi aplikasi berbayar. Selain itu, penelitian ini juga memberikan rekomendasi teknis berbasis CVSS yang dapat dijadikan panduan oleh administrator jaringan sekolah, seperti migrasi ke WPA3, menonaktifkan layanan yang tidak aman, memperbarui firmware secara berkala, serta melakukan monitoring rutin. Dengan demikian, penelitian ini berkontribusi pada bidang keamanan jaringan dengan menghadirkan studi kasus nyata di sekolah, sekaligus memperluas literatur yang sebelumnya lebih banyak berfokus pada lingkungan kampus atau institusi besar.

5.2. Saran

Untuk meningkatkan keamanan jaringan, pihak sekolah disarankan melakukan pembaruan protokol enkripsi ke WPA3 atau minimal WPA2 dengan AES, serta menonaktifkan metode lama seperti WEP dan TKIP. Autentikasi jaringan perlu diperkuat dengan penggunaan kata sandi yang kompleks dan penggantian secara berkala, serta menghindari jaringan terbuka tanpa proteksi. Layanan manajemen yang tidak aman seperti Telnet sebaiknya dinonaktifkan dan diganti dengan protokol aman seperti SSH. Perangkat jaringan juga perlu diperbarui *firmware*-nya secara rutin untuk menutup celah keamanan yang sudah diketahui publik. Selain itu, penerapan sistem pemantauan dan deteksi intrusi (*Wireless Intrusion Detection System*) akan membantu mengidentifikasi dan memblokir *rogue access point*. Segmentasi jaringan antara internal dan tamu, didukung firewall, dapat membatasi ruang gerak potensi serangan. Tidak kalah penting, sekolah perlu memberikan edukasi kepada guru dan siswa mengenai keamanan jaringan dan pentingnya menjaga kredensial. Kombinasi penggunaan *Kismet* untuk deteksi dini dan *Airodump-ng* untuk investigasi teknis juga direkomendasikan guna menciptakan perlindungan yang lebih komprehensif terhadap ancaman keamanan jaringan.

DAFTAR PUSTAKA

NAJIB, W., 2019. Analisis Keamanan Jaringan Single Sign On (SSO). Analisis Keamanan Jaringan Single Sign, no. 2302–3805, hlm.1–6.

GONDOHANINDIJO, J., 2012. Sistem Keamanan Jaringan Nirkabel. Sistem Keamanan Jaringan Nirkabel, 3, hlm.1–217.

PINEM, S. dan AZIZ, A.S., 2025. Evaluasi Keamanan Jaringan Berbasis Intrusion Detection System (IDS) untuk Melindungi Data Sensitif di Kantor Kecamatan Ketambe, Kabupaten Aceh Tenggara. INNOVATIVE: Journal of Social Science Research, [e-journal] 5(4), hlm. 5138–5146.

Arief, M.R., 2013. Teknologi jaringan tanpa kabel (Wireless). Seminar Nasional Teknologi 2007, vol. 2007, no. November, pp.1–8.

Supriyanto, A., 2006. Tinjauan teknis teknologi perangkat wireless dan standar keamanannya. Teknologi Informasi Dinamika, vol. 11, no. 2, pp.75–83.

HERMADUANTI, N. & RIADI, I., 2016. Automation framework for rogue access point mitigation in IEEE 802.1X-based WLAN. Journal of Theoretical and Applied Information Technology, 93(2), pp. 287–296.

PRASETYO, S. E. & TAN, E., 2021. Analisis Quality of Service (QoS) Jaringan Wireless 2.4 GHz dan 5 GHz di Dalam Ruangan dengan Hambatan Kaca. Jurnal Ilmiah Teknologi Informasi Asia, 15(2), pp. 103–114. DOI: 10.32815/jitika.v15i2.609.

PATTIASINA, G. H. Y., 2016. Analisis Kinerja Wireless Intrusion Detection System (WIDS) terhadap Serangan Man in the Middle (MitM) di Jaringan WLAN.

Ramadhani, 2010. Analisis keamanan jaringan wireless di Universitas Gadjah Mada dengan menggunakan metode wardriving. UGM.

Aristian & Cholil, W., 2022. Analisis vulnerability terhadap website Lembaga Bahasa LIA Palembang menggunakan Nessus, Netsparker dan Acunetic. Jurnal Pendidikan dan Konseling, vol. 4, pp.1707–1715.

Ruswanti, D., Susilo, D., F. Sains & Universitas Setia Budi Surakarta, 2023. Uji keamanan WPA2 dengan Wi-Fi deauther menggunakan Aerowpa 1.2. Tekinkom, vol. 6, pp.860–866. https://doi.org/10.37600/tekinkom.v6i2.776

Rustam, Y.W.A. & Novi, R., 2015. Jurnal Informasi, vol. VII, no. 1, pp.58–82.

Komputer, K.J., 2020. Jaringan komputer. Yogyakarta: Penerbit Andi. vol. 231, no. April 2019, p.11

Susila, A., Riadi, I. & Prayudi, Y., 2017. Wi-Fi security level analysis for minimizing cybercrime. International Journal of Computer Applications, vol. 164, no. 7, pp.35–39.

Fatimah, F., Mary, T. & Pernanda, A.Y., 2022. Analisis keamanan jaringan Wi-Fi terhadap serangan packet sniffing di Universitas PGRI Sumatera Barat. JURTEII Jurnal Teknologi Informasi, vol. 1, no. 2, pp.7–11.

Nurdiana, F.R., Gunawan, I., Viollita, R.C., Faizal, M. & Nurcahyadi, D., 2021. Analisis keamanan jaringan Wi-Fi menggunakan Wireshark. JES (Jurnal Elektro Smart), vol. 1, no. 1, pp.10–12.

Tania, A.M. et al., 2018. Keamanan website menggunakan vulnerability assessment. Informatics Education Professional, vol. 2, no. 2, pp.171–180.

Fajri, A., B. Siber & B. Siber, 2019. Pemindaian kinerja dan keamanan jaringan Wi-Fi menggunakan teknik wardriving (Studi kasus di Kota Batam), pp.24–25.

Azmi, A.Y.F., Gusti, J.A.G. & Wahyudi, E., 2022. Analisis network security pada layanan Wi-Fi Indihome terhadap serangan denial of service (DoS). Jurnal Litek: Jurnal List. Telekomunikasi dan Elektronika, vol. 19, no. 1, pp.8–12.

Mulya, B.W.R. & Tarigan, A., 2018. Pemeringkatan risiko keamanan sistem jaringan komputer Politeknik Kota Malang menggunakan CVSS dan FMEA. Ilkom Jurnal Ilmiah, vol. 10, no. 2, pp.190–200.

Margareth, S. et al., 2024. Uji penetration testing web server XYZ menggunakan metode OWASP TOP 10 dan CVSS, pp.1173–1182.

Pratiwi, P.A., Mashalani, F., Hafizhah, M. & Batrisyia, A., 2024. Mengungkap metode observasi yang efektif menurut pra-pengajar EFL. Mutiara Jurnal Penelitian dan Karya Ilmiah, vol. 2, no. 1, pp.133–149.

Pranatawijaya, V.H., Widiatry, W., Priskila, R. & Putra, P.B.A.A., 2019. Penerapan skala Likert dan skala dikotomi pada kuesioner online. Jurnal Sains dan Informatika, vol. 5, no. 2, pp.128–137.

Vi, T., 2018. Tugas VI mata kuliah keamanan jaringan komputer.

Wibowo, R.M. & Sulaksono, A., 2021. Web vulnerability through cross site scripting (XSS) detection with OWASP Security Shepherd. Indonesian Journal of Information Systems, vol. 3, no. 2, pp.149–159.

Rahmawati, A.F. & Susetyo, Y.A., 2023. Analisis quality code menggunakan Sonarqube dalam suatu aplikasi berbasis Laravel. IT-Explore: Jurnal Penerapan Teknologi Informasi dan Komunikasi, vol. 2, no. 2, pp.99–103.

Purwanza, S.W. et al., 2022. Metodologi Penelitian Kuantitatif, Kualitatif, dan Kombinasi.

Astuti, E.P., 2016. Analisis faktor-faktor profitabilitas perusahaan menggunakan purposive sampling dan regresi berganda. Jurnal Riset Akuntansi Terpadu, vol. 9, no. 1, pp.105–114.